Д.А.Супруненко

ГРУППЫ МАТРИЦ

ОГЛАВЛЕНИЕ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ПРЕДИСЛОВИЕ

В настоящей книге изложены классические результаты о строении нормальных делителей полной линейной группы над телом, теоремы Бернсайда и Шура о периодических линейных группах, теорема о нормальном строении $SL(n, Z)$ при $n > 2$. Кроме того, здесь содержится теория разрешимых, нильпотентных и локально нильпотентных линейных групп. Более полное представление о содержании дает следующий обзор ее глав.

В первой главе речь идет о группах подстановок (конечных и бесконечных). После изложения начальных сведений устанавливается связь теории примитивных разрешимых групп подстановок (не обязательно конечной степени) с теорией разрешимых линейных групп над простыми полями. Здесь же изучаются нильпотентные и локально нильпотентные группы подстановок. Дано, например, полное описание максимальных нильпотентных подгрупп симметрической группы конечной степени. Доказана, в частности, сопряженность максимальных транзитивных нильпотентных подгрупп конечной симметрической группы.

Значительная часть второй главы посвящена теории определителей матриц над телом и строению нормальных делителей полной линейной группы над телом; в основу изложения положены статья Ж. Дьедонне [1] и книга Э. Артина [1]. Здесь же рассматриваются некоторые свойства эндоморфизмов модуля над ассоциативным кольцом. В частности, устанавливаются перестановочные свойства трансвекций модуля.

В третьей главе описываются нормальные делители предельной полной линейной группы над произвольным ассоциативным кольцом (теорема Х. Басса [1] и нормальные делители $SL(n, Z)$, $n > 2$, (Х. Басс, М. Лазар, Ж.-П. Сэрр [1] и И. Менннике [1]). Предельной (или стабильной) полной линейной группой $GL(\Delta)$ над кольцом Δ называется объединение следующей бесконечной возрастающей цепи групп:

$$GL(1, \Delta) \subset GL(2, \Delta) \subset \ldots \subset GL(n, \Delta) \subset \ldots$$

В четвертой главе доказывается локальная теорема А. И. Мальцева об условиях точной линейной представимости группы и теоремы Клиффорда о нормальных делителях неприводимой линейной группы. Исследуются свойства импримитивных линейных групп и условия полной приводимости линейных групп.

В пятой главе рассматриваются разрешимые группы матриц над полем. Основное внимание уделено строению примитивных максимальных разрешимых подгрупп группы $GL(n, \Delta)$ для произвольного поля Δ. Детально рассматривается инвариантный ряд

$$G \supset V \supset A \supset F \supset (E_n), \tag{α}$$

где G — примитивная максимальная разрешимая подгруппа группы $GL(n, \Delta)$, F — максимальный абелев нормальный делитель G, V — централизатор F в G, а A/F — подгруппа фактор-группы G/F, максимальная среди инвариантных абелевых подгрупп G/F, содержащихся в V/F. Ряд (α) однозначно определяется группой G. Изучение ряда (α) позволяет в некоторых случаях классифицировать максимальные неприводимые разрешимые подгруппы $GL(n, \Delta)$. Из свойств ряда (α) просто выводятся теоремы Г. Цассенхауза и А. И. Мальцева о линейных разрешимых группах. Построение максимальных разрешимых подгрупп полной линейной группы над алгебраически замкнутым полем сведено к построению разрешимых подгрупп симплектической группы над конечным простым полем. Приведен каталог максимальных неприводимых разрешимых групп простой степени над алгебраически замкнутым полем. Перечислены также все максимальные неприводимые разрешимые группы простой степени над конечным полем. Устанавливаются условия полной приводимости разрешимой линейной группы. В частности, разрешимая линейная группа над полем нулевой характеристики тогда и только тогда вполне приводима, когда вполне приводима любая ее циклическая подгруппа.

Шестая глава в основном посвящена периодическим линейным группам над полем. Доказывается критерий Бернсайда конечности линейной группы, теорема Шура о локальной конечности периодической линейной группы над произвольным полем, теорема Шура о существовании у комплексной периодической линейной группы абелева нормального делителя конечного индекса. Изучаются p-подгруппы Силова и П-подгруппы Силова группы $GL(n, \Delta)$. Приводятся структурные теоремы В. П. Платонова о периодических линейных группах: теорема о сопряженности p-подгрупп Силова в периодической линейной группе, аналог теоремы Шура — Цассенхауза для периодических линейных групп. Рассматриваются свойства линейной группы, уже не обязательно периодической, связанные со свойствами характеристических полиномов ее матриц.

В главе седьмой изучаются нильпотентные и локально нильпотентные группы матриц над полем. Здесь полностью описаны все максимальные локально нильпотентные подгруппы полной линейной группы над алгебраически замкнутым полем. В частности, для алгебраически замкнутого поля Δ доказано следующее. Если $\operatorname{char}\Delta$ делит число n, то в $GL(n, \Delta)$ нет неприводимых локально нильпотентных подгрупп, если же $\operatorname{char}\Delta = 0$, либо $\operatorname{char}\Delta = p$, но p не делит n, в $GL(n, \Delta)$ с точностью до сопряженности имеется единственная максимальная неприводимая локально нильпотентная подгруппа. Для алгебраически замкнутого основного поля описаны также полностью максимальные неприводимые метабелевы (нильпотентные класса 2) подгруппы полной линейной группы. В случае произвольного основного поля классификация максимальных неприводимых локально нильпотентных подгрупп полной линейной группы сведена к описанию p-подгрупп Силова проективной группы $PGL(p^{\alpha}, \Delta)$. Для совершенного поля дается канонический вид локально нильпотентных приводимых неразложимых линейных групп.

Теоремы, предложения, леммы и формулы нумеруются в каждом параграфе автономно. При ссылке к номеру теоремы (леммы, предложения) приписывается слева номер параграфа. Например, если теорема 5 из § 7 упоминается не в § 7, то она именуется теорема 7.5. При ссылке на следствие 1 теоремы 7.5 пишется «следствие 7.5.1». Если эта ссылка делается в самом § 7, то пишем «следствие 5.1».

Автор с благодарностью вспоминает А. И. Мальцева, по настоянию которого была начата работа над книгой. Хочется выразить признательность редактору Ф. И. Кизнер и моим ученикам: Г. П. Жавриду, В. С. Конюху, Л. П. Луговской, Н. Н. Метельскому, О. М. Нерославскому, В. П. Юфереву, помогавшим мне при подготовке рукописи.

ГЛАВА I

ЭЛЕМЕНТЫ ТЕОРИИ ГРУПП ПОДСТАНОВОК

§ 1. Свойства отображений

1. Отображения. Пусть X и Y — произвольные непустые множества. Говорят, что определено *отображение множества X в множество Y*, если каждому элементу $x \in X$ приведен в соответствие единственный элемент $y \in Y$.

Отображения множества X в множество Y будем записывать в виде f: $X \to Y$, g: $X \to Y$ и т. д. Образ множества X при отображении f будем обозначать $f(X)$ или $\operatorname{Im} f$. Запись $x \mapsto y$ означает, что $y = f(x)$ — образ элемента $x \in X$ при отображении f. Если f: $X \to Y$, а $B \subset Y$ *), то $f^{-1}(B) = \{x \mid x \in X;\ f(x) \in B\}$.

Два отображения f: $X \to Y$ и f_1: $X_1 \to Y_1$ считаются ***равными***, если $X = X_1$, $Y = Y_1$ и для каждого элемента $x \in X$ $f(x) = f_1(x)$.

Пусть $\varnothing \neq A \subset X$. Отображение φ: $A \to Y$ называется *ограничением отображения f: $X \to Y$ на множестве A*, если для каждого $a \in A$ $\varphi(a) = f(a)$.

Ограничение отображения f на множестве A будем часто обозначать символом $f|A$. Если H — какое-либо множество отображений X в Y, то символом $H|A$ будем обозначать множество всех ограничений $h|A$, $h \in H$.

Отображение f: $X \to Y$ называется *инъективным*, если для любых элементов x_1 и x_2 множества X

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

(здесь $\Rightarrow$, как обычно, — знак следования).

Отображение f: $X \to Y$ называется *сюръективным*, если для всякого $y \in Y$ $f^{-1}(y) \neq \varnothing$.

---

*) Значок $\subset$ используется в книге для обозначения нестрогого включения, т. е. не исключается совпадение множеств.

Отображение $f\colon X \to Y$ называется *биективным*, или *биекцией*, если оно сюръективно и инъективно.

2. Умножение отображений. Пусть $f\colon X \to Y, g\colon Z \to U$, $Y \subset Z$. Отображение

$$gf\colon X \to U, \qquad x \mapsto g(f(x)),$$

называется *произведением* отображений g и f.

Под воздействием отображения gf элемент $x \in X$ переходит в $g(y)$, где $y = f(x)$.

Произведение gf двух отображений g и f определено лишь тогда, когда второе множество второго отображения есть подмножество первого множества первого отображения.

Теорема 1. *Пусть f, g, h — такие отображения, что существует хотя бы одно из двух произведений $f(gh)$ или $(fg)h$. Тогда существуют оба эти произведения и*

$$f(gh) = (fg)h. \tag{1}$$

Доказательство. Пусть существует, например, $f(gh)$. Тогда существует gh и, следовательно, g и h имеют вид $g\colon X \to Y$, $h\colon Z \to U$, $U \subset X$. Отсюда следует, что $gh\colon Z \to Y$, $f\colon V \to W$ и $Y \subset V$. Поэтому fg существует и имеет вид $fg\colon X \to W$. Так как $U \subset X$, то существует и $(fg)h$.

Докажем теперь равенство (1). Очевидно, $f(gh)\colon Z \to W$, $(fg)h\colon Z \to W$. Пусть $z \in Z$, $a = f(gh)$, $b = (fg)h$. Тогда $a(z) = f(gh)(z) = f(gh(z)) = f(g(h(z)))$, $b(z) = (fg)h(z) = fg(h(z)) = f(g(h(z))) = a(z)$, $b = a$. ■

Пусть теперь $\Sigma(X)$ — множество всех отображений X в X. Тогда, очевидно, произведение существует для любой пары отображений из $\Sigma(X)$ и, в силу теоремы 1, $\Sigma(X)$ *является полугруппой. Тождественное отображение*

$$e\colon X \to X, \qquad x \mapsto x,$$

служит единицей этой полугруппы.

Полугруппу $\Sigma(X)$ будем называть *симметрической полугруппой, действующей на множестве X*, а группу $S(X)$ всех ее обратимых элементов — *симметрической группой, действующей на X*. Всякую подгруппу в $S(X)$ будем называть *группой подстановок множества X*.

Мощность $\operatorname{card} X$ множества X назовем *степенью* группы подстановок множества X.

Если $\operatorname{card} X = n < \infty$, то будем иногда вместо $S(X)$ писать S_n.

Теорема 2. *Отображение из полугруппы $\Sigma(X)$ тогда и только тогда обратимо, когда оно биективно.*

Доказательство. Пусть $f\colon X \to X$ — биекция. Если x по одному разу пробегает все точки множества X, то $f(x) = y$ также пробегает все эти точки по одному разу. Следовательно, существует $g \in \Sigma(X)$ такое, что $g(y) = x$. Очевидно, $fg(y) = f(x) = y$, $gf(x) = g(y) = x$, т. е. $fg = gf = e$. Таким образом, из биективности отображения f следует его обратимость в полугруппе $\Sigma(X)$.

Пусть теперь $f \in S(X)$, т. е. в полугруппе $\Sigma(X)$ есть такое отображение g, что $fg = gf = e$. Для произвольного элемента y множества X $fg(y) = e(y) = y, f(g(y)) = y$. Следовательно, f — сюръективное отображение. Если $x_1, x_2 \in X$ и $f(x_1) = f(x_2)$, то $gf(x_1) = gf(x_2)$, $e(x_1) = e(x_2)$, $x_1 = x_2$. Доказана биективность отображения f. ∎

3. Подобие. Пусть $A \subset \Sigma(X)$, $B \subset \Sigma(Y)$. Будем говорить, что множество A *подобно* множеству B, если существуют такие биекции $\gamma\colon X \to Y$, $\varphi\colon A \to B$, что для любых $a \in A$ и $x \in X$ верно равенство

$$\varphi(a)(\gamma(x)) = \gamma(a(x)). \tag{2}$$

Если

$$\varphi(a) = b, \qquad \gamma(x) = y, \tag{3}$$

то $b(y) = \gamma(a(x)) = \gamma a \gamma^{-1}(y)$, откуда

$$b = \gamma a \gamma^{-1}. \tag{4}$$

Очевидно, совокупность равенств (3) и (4) влечет за собой равенство (2), так что *множество A подобно множеству B тогда и только тогда, когда существует такая биекция $\gamma\colon X \to Y$, что отображение*

$$\varphi\colon A \to B, \qquad a \mapsto \gamma a \gamma^{-1},$$

также является биекцией. Если множества A и B подобны, то $B = \gamma A \gamma^{-1}$.

4. Представление отображениями. Пусть A — произвольное непустое множество. Любое отображение

$$g\colon A \to \Sigma(X) \tag{5}$$

будем называть *представлением множества A отображениями.*

Два представления g: $A \to \Sigma(X)$ и h: $A \to \Sigma(Y)$ будем называть *эквивалентными*, если существует такая биекция γ: $X \to Y$, что для любых $a \in A$, $x \in X$ верно равенство

$$h(a)(\gamma(x)) = \gamma(g(a)(x)). \tag{6}$$

Положив $y = \gamma(x)$, из (6) получим

$$h(a)(y) = \gamma g(a)\gamma^{-1}(y), \qquad h(a) = \gamma g(a)\gamma^{-1}.$$

Следовательно, *множества* $\operatorname{Im} g$ *и* $\operatorname{Im} h$ *подобны.*

Ниже рассмотрим два таких представления полугруппы (в частности, группы), одно из которых есть гомоморфизм, а другое — инверсный гомоморфизм.

5. Регулярное представление. Пусть A — полугруппа с единицей 1. Каждый элемент a этой полугруппы определяет два отображения:

$$\sigma_a\colon\ A \to A, \qquad x \mapsto ax, \qquad x \in A,$$

и

$$\tau_a\colon\ A \to A, \qquad x \mapsto xa, \qquad x \in A.$$

Введем два представления:

$$\lambda\colon\ A \to \Sigma(A), \qquad a \mapsto \sigma_a,$$

и

$$\rho\colon\ A \to \Sigma(A), \qquad a \mapsto \tau_a.$$

Представление λ назовем *левым регулярным представлением* полугруппы A, а ρ — ее *правым регулярным представлением.*

Теорема 3. (i) *λ и ρ — инъективные отображения, причем λ — гомоморфизм, а ρ — инверсный гомоморфизм.*

(ii) $\operatorname{Im}\rho$ — *централизатор полугруппы* $\operatorname{Im}\lambda$, *а* $\operatorname{Im}\lambda$ — *централизатор* $\operatorname{Im}\rho$ *в* $\Sigma(A)$.

Доказательство. (i) Рассмотрим, например, ρ. Пусть $\rho(a) = \rho(b)$; $a, b \in A$. Тогда $\tau_a = \tau_b$, $\tau_a(1) = \tau_b(1)$, $a = b$. Следовательно, ρ — инъективное отображение. Далее,

$$\rho(ab) = \tau_{ab}, \qquad \tau_{ab}(x) = xab = \tau_a(x)\,b = \tau_b\tau_a(x).$$

Значит,

$$\tau_{ab} = \tau_b\tau_a, \qquad \rho(ab) = \rho(b)\rho(a).$$

Аналогично устанавливаются инъективность отображения λ и равенство $\lambda(ab) = \lambda(a)\lambda(b)$.

(ii) Положим $\operatorname{Im}\lambda = A_\lambda$, $\operatorname{Im}\rho = A_\rho$. Пусть $Z(A_\lambda)$ — централизатор множества A_λ в полугруппе $\Sigma(A)$. Для $a, b \in A$

$$\sigma_a\tau_b(x) = axb = \tau_b\sigma_a(x),$$

следовательно, $Z(A_\lambda) \supset A_\rho$. Для $\varphi \in Z(A_\lambda)$

$$\varphi\sigma_x = \sigma_x\varphi, \qquad \varphi\sigma_x(1) = \sigma_x\varphi(1),$$

или $\varphi(x) = xc$, где $c = \varphi(1)$. Отсюда

$$\varphi(x) = \tau_c(x), \qquad \varphi = \tau_c, \qquad \varphi \in A_\rho, \qquad Z(A_\lambda) = A_\rho.$$

Аналогично доказывается равенство $Z(A_\rho) = A_\lambda$. ∎

Следствие 1. *Если A — коммутативная полугруппа с единицей, то $\operatorname{Im}\lambda = \operatorname{Im}\rho$ — максимальная коммутативная подполугруппа в $\Sigma(A)$.*

Следствие 2. *Если A — абелева группа, то $\operatorname{Im}\lambda = \operatorname{Im}\rho$ — максимальная абелева подгруппа в $S(A)$.*

Теорема 4. *Левое регулярное представление полугруппы A с единицей эквивалентно ее правому регулярному представлению тогда и только тогда, когда A коммутативна.*

Доказательство. Для коммутативной полугруппы A

$$\sigma_a(x) = ax = xa = \tau_a(x), \qquad \sigma_a = \tau_a.$$

Пусть, с другой стороны, $\gamma\colon A \to A$ — такая биекция, что для любого $a \in A$ $\tau_a = \gamma\sigma_a\gamma^{-1}$. Тогда $\tau_a\gamma = \gamma\sigma_a$, $\tau_a\gamma(1) = \gamma\sigma_a(1)$. Положив $\gamma(1) = c$, получим

$$\tau_a(c) = \gamma(a), \qquad \gamma(a) = ca, \qquad \gamma = \sigma_c.$$

Далее,

$$\sigma_a = \gamma^{-1}\tau_a\gamma = \gamma^{-1}\gamma\tau_a = \tau_a.$$

Для $b \in A$

$$\sigma_a(b) = ab, \qquad \tau_a(b) = ba.$$

Значит, $ab = ba$, A — коммутативная полугруппа. ∎

§ 2. Транзитивность

1. Орбиты. Пусть Γ — группа подстановок множества X. Установим в X бинарное отношение R, положив для $x, y \in X$ xRy тогда и только тогда, когда в группе есть такой элемент g, что $g(x) = y$. Так как Γ — группа, то R — отношение эквивалентности. Пусть теперь

$$X = \bigcup X_\alpha, \qquad \alpha \in I, \tag{1}$$

— разбиение множества X, определяемое этим отношением. Тогда множества X_α, $\alpha \in I$, назовем *орбитами* группы Γ. Если группа Γ обладает только одной орбитой, т. е. для любых x, $y \in X$ xRy, то будем называть эту группу *транзитивной*. Если же $\operatorname{card} I > 1$, то назовем группу Γ *интранзитивной*. Если $A \subset X$, $g \in \Gamma$ и $\Gamma(A) = A$, то $\Gamma|A$ будем иногда трактовать как подгруппу $S(A)$, совпадающую с Γ на A, а $g|A$ — как элемент $S(A)$, совпадающий с g на A.

Будем говорить, что две группы G_1 и G_2 подстановок множества X имеют *один и тот же орбитальный тип*, если существует такая биекция φ: $X \to X$, которая переводит всякую орбиту группы G_1 в орбиту группы G_2.

Пусть s, $t \in S(X)$, $x_1 \in X$. Если $t(x_1) = x_2$, то

$$sts^{-1}(s(x_1)) = s(x_2).$$

Отсюда следует, в частности, что если (1) — разбиение множества X на орбиты группы Γ, то $X = \bigcup s(X_\alpha)$, $\alpha \in I$, — его разбиение на орбиты группы $s\Gamma s^{-1}$. Следовательно, *сопряженные подгруппы группы $S(X)$ имеют один и тот же орбитальный тип.*

2. Циклы подстановок. Цикленный тип. Пусть $a \in S(X)$, а X_α — одна из орбит циклической группы (a). Тогда ограничение $a_\alpha = a|X_\alpha$ называется *циклом* подстановки a. Мощность $\operatorname{card} X_\alpha$ называется *длиной цикла* a_α.

Ясно, что *любая орбита группы (a) есть множество всех точек вида $x_k = a^k(x_0)$, $k = 0, \pm 1, \pm 2, \ldots, x_0 \in X$.* Отсюда следует, что *длина любого цикла конечна или счетна. В последнем случае $x_k \neq x_l$, если $k \neq l$.*

Если группа (a) транзитивна, то подстановку a назовем *полным циклом.*

Очевидно, *в группе $S(X)$ лишь тогда есть полные циклы, когда множество X конечно или счетно.*

Если лишь одна орбита группы (a) имеет отличную от 1 мощность, то подстановка a называется *циклической.*

Будем говорить, что подстановки a и b из $S(X)$ имеют *один и тот же цикленный тип*, если циклические группы (a) и (b) имеют один и тот же орбитальный тип.

Теорема 1. *Две подстановки группы $S(X)$ тогда и только тогда сопряжены в $S(X)$, когда они имеют один и тот же цикленный тип.*

Доказательство. Пусть a и b — подстановки из $S(X)$, и пусть $b = tat^{-1}$, где $t \in S(X)$. Тогда $(b) = t(a)t^{-1}$. Как отмечалось выше, сопряженные подгруппы имеют один и тот же орбитальный тип. Следовательно, a и b имеют один и тот же цикленный тип.

Необходимость доказана. Установим достаточность. Пусть подстановки a и b из $S(X)$ имеют один и тот же цикленный тип. Тогда есть такая подстановка φ из $S(X)$, что для любой орбиты X_α, $\alpha \in I$, группы (a) множество $\varphi(X_\alpha)$ является орбитой Y_α группы (b). Очевидно, $\operatorname{card} X_\alpha = \operatorname{card} Y_\alpha$, $X_\alpha = \{x_{k\alpha} \mid x_{k\alpha} = a^k(x_\alpha)\}$, $Y_\alpha = \{y_{k\alpha} \mid y_{k\alpha} = b^k(y_\alpha)\}$. Для каждого $\alpha \in I$ построим биекцию t_α: $X_\alpha \to Y_\alpha$, $x_{k\alpha} \mapsto y_{k\alpha}$. Теперь построим такую биекцию t: $X \to X$, что $t|X_\alpha = t_\alpha$ для любого $\alpha \in I$. Тогда $tat^{-1} = b$. Действительно, для любого $y_{k\alpha} \in Y_\alpha$ имеем

$$tat^{-1}(y_{k\alpha}) = tat^{-1}t(x_{k\alpha}) = ta(x_{k\alpha}) = t(x_{k+1,\alpha}) = y_{k+1,\alpha} = b(y_{k\alpha}). \blacksquare$$

3. Кратная транзитивность. Пусть Γ — группа подстановок множества X, а U_k — множество всех таких точек $(x_1, \ldots, x_k)$ декартова произведения $X^k = X \times \ldots \times X$, что $x_i \neq x_j$ при $i \neq j$. В частности, если $\operatorname{card} X = n$ — натуральное число, то $\operatorname{card} U_k = n(n-1)\ldots(n-k+1)$. Зададим в U_k бинарное отношение R_k, положив aR_kb для элементов $a = (x_1, \ldots, x_k)$, $b = (y_1, \ldots, y_k)$ множества U_k тогда и только тогда, когда в группе Γ есть такой элемент g, что $g(x_i) = y_i$, $i = 1, \ldots, k$. Очевидно, при $k = 1$ R_k совпадает с R, заданным выше. Очевидно также, что R_k есть отношение эквивалентности.

Группу Γ назовем *k раз транзитивной*, если для любых двух точек $a, b \in U_k$ aR_kb.

Группа Γ, действующая на множестве X, определяет изоморфную ей группу $\mathfrak{G}$ подстановок $\bar{g}$ множества U_k: подстановке $g \in \Gamma$ соответствует $\bar{g} \in S(U_k)$ по формуле

$$\bar{g}(a) = (g(x_1), \ldots, g(x_k)), \qquad a = (x_1, \ldots, x_k) \in U_k.$$

Очевидно, *группа* Γ *тогда и только тогда* k *раз транзитивна, когда группа* $\mathfrak{G}$ *транзитивна.*

4. Стационарная подгруппа. Пусть Γ — группа подстановок множества X, а a — фиксированная точка этого множества. Множество Γ_a всех элементов группы Γ, оставляющих точку a неподвижной, является, очевидно, подгруппой. Подгруппа Γ_a называется *стационарной подгруппой группы* Γ, или *стабилизатором точки* a *в группе* Γ.

Теорема 2. *Пусть* X_α — *орбита группы* Γ, $a \in X_\alpha$, Γ_α — *стационарная подгруппа. Для каждой точки* $x \in X_\alpha$ *выберем в группе* Γ *одну такую подстановку* g_x, *что* $g_x(a) = x$. *Тогда* $\Gamma = \bigcup g_x\Gamma_a$, $x \in X_\alpha$, — *разбиение группы* Γ *на левые смежные классы по подгруппе* Γ_a.

Доказательство. Пусть g — произвольный элемент группы Γ. Тогда $g(a) = x \in X_\alpha$. Очевидно,

$$g_x^{-1}g \in \Gamma_a, \qquad g \in g_x\Gamma_a.$$

С другой стороны, классы $g_x\Gamma_a$ и $g_y\Gamma_a$ при различных x и y из X_α различны, ибо $g_x\Gamma_a(a) = x$, $g_y\Gamma_a(a) = y$. ■

Следствие 1. *Порядок группы подстановок конечного множества делится на мощность любой ее орбиты. В частности, порядок транзитивной группы подстановок конечного множества делится на ее степень.*

Следствие 2. *Порядок* k *раз транзитивной группы натуральной степени* n *делится на число* $n(n-1)\ldots$ $\ldots(n-k+1)$.

Теорема 3. *Пусть* X_α — *орбита группы* Γ, *а* $\mathfrak{K}_\alpha$ — *семейство всех стационарных подгрупп* Γ_a, *где* $a \in X_\alpha$. *Тогда система всех различных подгрупп из семейства* $\mathfrak{K}_\alpha$ *есть класс сопряженных подгрупп группы* Γ.

Доказательство. Пусть $a \in X_\alpha$, $g \in \Gamma$. Рассмотрим группу $g\Gamma_a g^{-1}$. Так как X_α — орбита группы Γ, то $g(a) = b \in X_\alpha$. Далее, $g\Gamma_a g^{-1}(b) = b$, значит, $g\Gamma_a g^{-1} \subset \Gamma_b$. Так как $g^{-1}(b) = a$, то

$$g^{-1}\Gamma_b g \subset \Gamma_a, \qquad \Gamma_b \subset g\Gamma_a g^{-1}, \qquad \Gamma_b = g\Gamma_a g^{-1}.$$

Отсюда вытекает, что семейство $\mathfrak{K}_\alpha$ вместе с группой Γ_a содержит и $g\Gamma_a g^{-1}$ и что любые две подгруппы из $\mathfrak{K}_\alpha$ сопряжены в группе Γ. ■

Следствие 1. *Если* Γ — *транзитивная группа, а* $\mathfrak{K}$ — *семейство всех ее стационарных подгрупп, то мно-*

жество всех различных подгрупп из этого семейства есть класс сопряженных в Γ подгрупп.

Следствие 2. *Пусть Γ — группа подстановок, все подгруппы которой инвариантны, X_α — одна из ее орбит. Тогда для любых $a, b \in X_\alpha$ $\Gamma_a = \Gamma_b$.*

Группа подстановок называется *регулярной*, если она транзитивна, а ее стационарная подгруппа совпадает с единичной.

Следствие 3. *Транзитивная группа подстановок, все подгруппы которой инвариантны, регулярна.*

Следствие 4. *Транзитивная группа подстановок множества X, все подгруппы которой инвариантны, не содержится в другой группе подстановок этого множества, все подгруппы которой инвариантны. В частности, абелева транзитивная подгруппа группы $S(X)$ максимальна среди абелевых подгрупп $S(X)$.*

Следствие 5. *Порядок транзитивной группы подстановок конечного множества, все подгруппы которой инвариантны, равен ее степени.*

§ 3. Импримитивность

1. Системы импримитивности. Пусть Γ — транзитивная группа подстановок множества X. Если существует разбиение

$$X = \bigcup X_\alpha, \qquad \alpha \in I, \tag{1}$$

множества X *), удовлетворяющее следующим условиям:

(i) $\operatorname{card} I > 1$;

(ii) существует такое $\alpha \in I$, что $\operatorname{card} X_\alpha > 1$;

(iii) для любых $\alpha \in I$, $g \in \Gamma$ найдется такое $\beta \in I$, что $g(X_\alpha) \subset X_\beta$,

то (1) называется *разбиением* множества X *на системы импримитивности* группы Γ, а группа Γ — *импримитивной*. Если же такого разбиения не существует, то группа Γ называется *примитивной*.

Лемма 1. *Если (1) — разбиение множества X на системы импримитивности группы Γ, то все множества X_α*

*) Разбиением множества X называют представление его в виде объединения непересекающихся подмножеств, т. е. в равенстве (1) $X_\alpha \cap X_\beta = \varnothing$ при $\alpha \neq \beta$.

имеют одну и ту же мощность. Для $\alpha \in I$, $g \in \Gamma$ *существует такое* $\beta \in I$, *что*

$$g(X_\alpha) = X_\beta. \tag{2}$$

Доказательство. Рассмотрим $g(X_\alpha)$. Согласно (iii) $g(X_\alpha) \subset X_\beta$, $\beta \in I$, и, значит, $X_\alpha \subset g^{-1}(X_\beta)$. Если $x \in g(X_\alpha)$, то $g^{-1}(x) \in X_\alpha$. Отсюда и из (iii) вытекает $g^{-1}(X_\beta) \subset X_\alpha$. Следовательно, (2) доказано. Так как группа Γ транзитивна, то для любых γ, $\delta \in I$ в ней есть такая подстановка h, что $h(X_\gamma) \subset X_\delta$. В силу (2) $h(X_\gamma) = X_\delta$, значит, множества X_γ и X_δ равномощны. ■

Следствие 1. *Транзитивная группа подстановок простой степени примитивна.*

Теорема 1. *Дважды транзитивная группа подстановок примитивна.*

Доказательство. Пусь Γ — импримитивная группа подстановок множества X, (1) — разбиение этого множества на системы импримитивности группы Γ, a, $a_1 \in X_\alpha$, $b \in X_\beta$, $a \neq a_1$, $\alpha \neq \beta$. Если бы группа Γ была дважды транзитивной, то в ней нашлась бы такая подстановка g, что

$$g(a) = a, \tag{3}$$

$$g(a_1) = b. \tag{4}$$

Из (3) тогда следовало бы $g(X_\alpha) = X_\alpha$, а из (4) — $g(X_\alpha) = X_\beta$. Полученное противоречие доказывает теорему.

Заметим, что *разбиение множества X на системы импримитивности группы Γ определяет некоторый гомоморфизм этой группы.* Действительно, введем отображение

$$\varphi\colon \Gamma \to S(I), \quad g \mapsto \tilde{g}, \quad \tilde{g}(\alpha) = \beta, \quad \text{если} \quad g(X_\alpha) = X_\beta. \tag{5}$$

Очевидно, φ — гомоморфизм; будем его называть *гомоморфизмом, определяемым разбиением* (1). Ядро этого гомоморфизма $\operatorname{Ker}\varphi$ *состоит из всех таких подстановок* $g_0 \in \Gamma$, *что* $g_0(X_\alpha) = X_\alpha$ *для любого* $\alpha \in I$. Так как Γ транзитивна, то $\operatorname{Im}\varphi$ *является транзитивной подгруппой группы* $S(I)$.

Для фиксированного $\alpha_1 \in I$ с разложением (1) свяжем две следующие подгруппы:

$$H_{\alpha_1} = \{g \mid g \in \Gamma,\ g(X_{\alpha_1}) = X_{\alpha_1}\}, \qquad H_{\alpha_1} \subset \Gamma,$$
$$F_{\alpha_1} = H_{\alpha_1} \mid X_{\alpha_1}, \qquad F_{\alpha_1} \subset S(X_{\alpha_1}).$$

Пусть $\{g_\alpha\}$, $\alpha \in I$, — *такое множество элементов из* Γ, *что* $g_\alpha(X_{\alpha_1}) = X_\alpha$. *Тогда*

$$\Gamma = \bigcup g_\alpha H_{\alpha_1}, \quad \alpha \in I,$$

— *разбиение группы* Γ *на левые смежные классы по* H_{α_1}.

Действительно, при $\alpha \neq \beta$

$$g_\alpha H_{\alpha_1} \neq g_\beta H_{\alpha_1},$$

ибо $g_\alpha H_{\alpha_1}(X_{\alpha_1}) = X_\alpha$, $g_\beta H_{\alpha_1}(X_{\alpha_1}) = X_\beta$. Если теперь $g \in \Gamma$, то $g(X_{\alpha_1}) = X_\alpha$ при некотором $\alpha \in I$. Далее, $g_\alpha^{-1} g(X_{\alpha_1}) = X_{\alpha_1}$. Следовательно, $g_\alpha^{-1} g \in H_{\alpha_1}$, $g \in g_\alpha H_{\alpha_1}$. ■

Отметим, что F_{α_1} — *транзитивная подгруппа группы* $S(X_{\alpha_1})$. Это следует из транзитивности группы Γ и определения группы F_{α_1}.

2. Критерий примитивности.

Теорема 2. *Транзитивная группа тогда и только тогда примитивна, когда ее стационарная подгруппа максимальна.*

Доказательство. Пусть Γ — транзитивная группа подстановок множества X, $a \in X$, Γ_a — стационарная подгруппа в Γ, и пусть Γ_a не максимальна в Γ, т. е. существует промежуточная подгруппа U:

$$\Gamma \supset U \supset \Gamma_a, \qquad \Gamma \neq U, \qquad U \neq \Gamma_a.$$

Выведем отсюда импримитивность группы Γ. С этой целью напишем разбиение группы Γ на левые смежные классы по подгруппе U:

$$\Gamma = \bigcup g_\alpha U = \bigcup U_\alpha, \qquad U_\alpha = g_\alpha U, \qquad \alpha \in I, \tag{6}$$

и положим $X_\alpha = U_\alpha(a)$. Так как группа Γ транзитивна, то

$$X = \bigcup X_\alpha, \qquad \alpha \in I. \tag{7}$$

Покажем, что (7) — разбиение, т. е. что $X_\alpha \cap X_\beta = \varnothing$ при $\alpha \neq \beta$. Действительно, пусть $u(a) = v(a)$, $u \in U_\alpha$, $v \in U_\beta$. Тогда $u^{-1}v(a) = a$, $u^{-1}v \in \Gamma_a$, $v \in u\Gamma_a \subset U_\alpha$. Последнее противоречит разбиению (6). Итак, (7) — разбиение. Покажем теперь, что (7) — разбиение на системы импримитивности группы Γ. Рассмотрим $g(X_\alpha)$, $g \in \Gamma$:

$$g(X_\alpha) = gU_\alpha(a) = gg_\alpha U(a) = g_\beta U(a) = U_\beta(a) = X_\beta,$$

т. е.

$$g(X_\alpha) = X_\beta. \tag{8}$$

Так как $U \neq \Gamma_a$, то $\operatorname{card} X_\alpha > 1$; $U \neq \Gamma$, следовательно, $\operatorname{card} I > 1$. Отсюда и из (8) вытекает, что (7) — разбиение множества X на системы импримитивности группы Γ.

Обратно. Пусть Γ — импримитивная группа. Докажем существование промежуточной подгруппы U:

$$\Gamma \supset U \supset \Gamma_a, \quad \Gamma \neq U, \quad U \neq \Gamma_a. \tag{9}$$

Пусть $a \in X_\alpha$, где X_α — одна из систем импримитивности группы Γ. Введем множество U всех таких подстановок $h \in \Gamma$, что $h(X_\alpha) = X_\alpha$. Так как Γ — транзитивная группа, $X_\alpha \neq \{a\}$ и $X_\alpha \neq X$, то U — промежуточная между Γ и Γ_a подгруппа. (9) доказано. ■

Следствие 1. *Регулярная группа подстановок либо импримитивна, либо имеет простой порядок.*

Следствие 2. *Транзитивная группа подстановок, все подгруппы которой инвариантны, почти всегда импримитивна. Исключение составляют группы, порядок и степень которых есть одно и то же простое число.*

Следствие 3. *Стационарная подгруппа симметрической группы максимальна.*

Из первой части доказательства теоремы вытекает

Следствие 4. *Пусть Γ — транзитивная подгруппа в $S(X)$, $a \in X$, а Γ_a — стабилизатор точки a в Γ. Если U — такая подгруппа группы Γ, что $\Gamma \supset U \supset \Gamma_a$, $\Gamma \neq U$, $U \neq \Gamma_a$, то $U(a)$ — одна из систем импримитивности группы Γ.*

3. Продолжение разбиения на системы импримитивности. Пусть Γ — импримитивная группа подстановок множества X,

$$X = \bigcup X_\alpha, \quad \alpha \in I, \quad X = \bigcup Y_\beta, \quad \beta \in B \tag{10}$$

— два разбиения множества X на системы импримитивности группы Γ. Если каждое множество Y_β является истинным подмножеством некоторого множества X_α, то второе разбиение называется *продолжением* первого.

Лемма 2. *Если для какого-либо* $\beta_1 \in B$

$$Y_{\beta_1} \subset X_{\alpha_1}, \qquad \alpha_1 \in I, \tag{11}$$

— строгое включение, то второе разбиение (10) *есть продолжение первого.*

Доказательство. Пусть $\beta \in B$. В силу транзитивности группы Γ в ней есть такая подстановка g, что $g(Y_{\beta_1}) = Y_\beta$. Из включения (11) следует, что

$$Y_\beta = g(Y_{\beta_1}) \subset g(X_{\alpha_1}) = X_\alpha, \qquad \alpha \in I,$$

— строгое включение. ■

Если для некоторого разбиения множества X на системы импримитивности группы Γ нет продолжения, то оно называется *непродолжаемым*.

С помощью группы F_{α_1}, введенной в начале параграфа, сформулируем одно условие непродолжаемости разбиения на системы импримитивности.

Лемма 3. *Первое из двух разбиений* (10) *тогда и только тогда непродолжаемо, когда группа* F_{α_1} *примитивна.*

Доказательство. Пусть второе из разбиений (10) есть продолжение первого. Тогда

$$X_{\alpha_1} \supset Y_{\beta_1}, \qquad \beta_1 \in B, \qquad X_{\alpha_1} \neq Y_{\beta_1}. \tag{12}$$

Положим

$$H = \{h \mid h \in \Gamma,\ h(Y_{\beta_1}) = Y_{\beta_1}\}.$$

Тогда, так как X_{α_1} — одна из систем импримитивности группы Γ, то из (12) следует

$$H \subset H_{\alpha_1} = \{g \mid g \in \Gamma,\ g(X_{\alpha_1}) = X_{\alpha_1}\}.$$

Группа F_{α_1} транзитивна, следовательно, $H \mid X_{\alpha_1} \subset F_{\alpha_1}$ — строгое включение. Если теперь $y_1 \in Y_{\beta_1}$, а $(F_{\alpha_1})_{y_1}$ — стабилизатор точки y_1 в группе F_{α_1}, то $(F_{\alpha_1})_{y_1} \subset H \mid X_{\alpha_1}$ — тоже строгое включение. Согласно критерию примитивности F_{α_1} импримитивна.

Обратно, если F_{α_1} импримитивна, то первое из двух разбиений (10) продолжаемо. Действительно, пусть F_α

импримитивна, а Y_{β_1} — одна из ее систем импримитивности. Положим

$$V = \{v \mid v \in F_{\alpha_1},\ v(Y_{\beta_1}) = Y_{\beta_1}\}.$$

Тогда

$$F_{\alpha_1} \supset V \supset (F_{\alpha_1})_a,$$

где $(F_{\alpha_1})_a$ — стабилизатор $a \in Y_{\beta_1}$ в группе F_{α_1}, причем оба включения строгие. Положим

$$U = \{u \mid u \in \Gamma,\ u(X_{\alpha_1}) = X_{\alpha_1},\ u \mid X_{\alpha_1} \in V\}.$$

Тогда для стабилизатора Γ_a точки a в Γ имеем $\Gamma \supset U \supset \Gamma_a$, где оба включения строгие. Очевидно, $U(a) = Y_{\beta_1}$. Следовательно, Y_{β_1} — система импримитивности группы Γ. Так как $Y_{\beta_1} \subset X_{\alpha_1}$ и включение строгое, то, в силу леммы 2, первое разложение (10) продолжаемо. ■

Очевидно, что *если множество X конечно, то для любой импримитивной подгруппы в $S(X)$ существует непродолжаемое разбиение множества X на ее системы импримитивности.*

4. Импримитивные группы и сплетения. Среди импримитивных групп подстановок отличаются особой «правильностью» группы, получаемые с помощью сплетения транзитивных групп. Определение сплетения групп подстановок принадлежит Л. А. Калужнину (см. Калужнин [1], [2], [3]).

Дадим определение сплетения групп подстановок. Пусть $X = A \times B$ — декартово произведение множеств A и B, $\operatorname{card} A > 1$, $\operatorname{card} B > 1$, F — группа подстановок множества A, G — группа подстановок множества B, а Π — множество всех отображений π: $B \to F$. Каждую пару $h = \langle g, \pi \rangle$, где $g \in G$, $\pi \in \Pi$, отождествим с отображением

$$h\colon X \to X,\quad x = (a, b) \mapsto (f_b(a), g(b)),\quad f_b = \pi(b), \tag{13}$$
$$a \in A,\quad b \in B.$$

На множестве Π введем аддитивную операцию $+$, положив для $\pi_1, \pi_2 \in \Pi$, $b \in B$

$$(\pi_1 + \pi_2)(b) = f_1 f_2,\qquad f_1 = \pi_1(b),\qquad f_2 = \pi_2(b).$$

Тогда $\langle \Pi, + \rangle$ — *группа, изоморфная полному прямому произведению ν экземпляров группы F, где* $\nu = \operatorname{card} B$.

Очевидно, *для* $g \in G$, $\pi \in \Pi$ *произведение отображений* πg *существует и* $\pi g \in \Pi$.

Лемма 4. *Пусть* $g, g_1 \in G$, $\pi, \pi_1 \in \Pi$. *Тогда*

$$\langle g, \pi\rangle \langle g_1, \pi_1\rangle = \langle gg_1, \pi g_1 + \pi_1\rangle.$$

Доказательство. Положим $h = \langle g, \pi\rangle$, $h_1 = \langle g_1, \pi_1\rangle$. Тогда, согласно (13),

$$hh_1(a, b) = h(\pi_1(b)(a), g_1(b)) = (\pi g_1(b)\pi_1(b)(a), gg_1(b)) =$$
$$= ((\pi g_1 + \pi_1)(b)(a), gg_1(b)) = \langle gg_1, \pi g_1 + \pi_1\rangle (a, b). \blacksquare$$

С помощью леммы 4 легко заключить, что *совокупность всех отображений* $h = \langle g, \pi\rangle$ *является* некоторой *подгруппой группы* $S(X)$. Действительно, в силу леммы 4 эта совокупность есть полугруппа с единицей $\langle e, 0\rangle$, где e — единица G, а 0 — нуль $\langle \Pi, +\rangle$. В силу той же леммы

$$\langle g, \pi\rangle^{-1} = \langle g^{-1}, -\pi g^{-1}\rangle.$$

Группа всех отображений $h = \langle g, \pi\rangle$ называется *полным сплетением* групп F и G и обозначается $F \operatorname{Wr} G$.

Лемма 5. *Группа* $F \operatorname{Wr} G$ *обладает таким нормальным делителем* N, *что*

(i) $$(F \operatorname{Wr} G)/N \cong G,$$

(ii) N — *полное прямое произведение* ν *экземпляров группы* F, *где* $\nu = \operatorname{card} B$.

Доказательство. Рассмотрим отображение

$$\gamma\colon F \operatorname{Wr} G \to G, \qquad \langle g, \pi\rangle \mapsto g.$$

В силу леммы 4 отображение γ — сюръективный гомоморфизм. Очевидно, $\operatorname{Ker}\gamma = N = \{\langle e, \pi\rangle\}$. Следовательно, $(F \operatorname{Wr} G)/N \cong G$. Согласно лемме 4 $\langle e, \pi\rangle\langle e, \pi_1\rangle = \langle e, \pi + \pi_1\rangle$. Отсюда $N \cong \langle \Pi, +\rangle$. $\blacksquare$

Следствие 1. *Если* $\operatorname{card} A = \mu$, $\operatorname{card} B = \nu$, *где* μ *и* ν — *натуральные числа, то* $F \operatorname{Wr} G$ — *группа подстановок порядка* $(\operatorname{card} G)(\operatorname{card} F)^{\nu}$ *степени* $\mu\nu$.

С помощью формулы (13) легко проверяется

Лемма 6. *Группа* $F \operatorname{Wr} G$ *тогда и только тогда транзитивна, когда транзитивны обе группы* F *и* G.

Пусть группы F и G транзитивны. Положим для $b \in B$ $X_b = A \times b$. Тогда, очевидно, $X = \bigcup X_b$, $b \in B$, — разбиение множества X на системы импримитивности группы $F \operatorname{Wr} G$. В этом случае группа G описывает то, как перемещает $F \operatorname{Wr} G$ системы импримитивности, а F — описывает действие $F \operatorname{Wr} G$ внутри системы импримитивности.

Следующая теорема показывает, что любая импримитивная группа подстановок содержится в полном сплетении двух групп.

Теорема 3. *Пусть* Γ — *импримитивная подгруппа группы* $S(Y)$, $Y = \bigcup Y_\alpha$, $\alpha \in I$, — *разбиение множества* Y *на системы импримитивности группы* Γ, φ: $\Gamma \to S(I)$ — *гомоморфизм, определяемый этим разбиением. Для фиксированного* $\alpha_1 \in I$ *положим*

$$H = \{h \mid h \in \Gamma,\ h(Y_{\alpha_1}) = Y_{\alpha_1}\}, \quad F = H \mid Y_{\alpha_1}, \quad G = \operatorname{Im} \varphi.$$

Тогда Γ *является подгруппой полного сплетения* $F \operatorname{Wr} G$.

Доказательство. Положим $A = Y_{\alpha_1}$. Для каждого $\alpha \in I$ выберем в Γ одну такую подстановку g_α, что $g_\alpha(Y_{\alpha_1}) = Y_\alpha$, а $g_{\alpha_1} = e$. Каждое $y_\alpha \in Y_\alpha$ представимо в виде $y_\alpha = g_\alpha(a)$, $a \in A$. Положим $y_\alpha = (a, \alpha)$. Тогда $Y_\alpha = A \times \alpha$. Следовательно, $Y = A \times I$. Как мы видели выше (см. начало параграфа), $\{g_\alpha \mid \alpha \in I\}$ — полная система представителей левых смежных классов группы Γ по подгруппе H. Для $y \in Y$, $v \in \Gamma$ можно написать

$$v(y) = v(a, \alpha) = v g_\alpha(a, \alpha_1) = g_\beta h_\alpha(a, \alpha_1), \tag{14}$$

где $h_\alpha \in H$. Положим $f_\alpha = h_\alpha \mid Y_{\alpha_1}$. Тогда из (14) получим

$$v(y) = g_\beta h_\alpha(a, \alpha_1) = g_\beta f_\alpha(a, \alpha_1) = g_\beta(f_\alpha(a), \alpha_1) =$$
$$= (f_\alpha(a), \beta) = (f_\alpha(a), \varphi(v)(\alpha)), \qquad \varphi(v) \in G.$$

Следовательно, $v(a, \alpha) = \langle g, \pi\rangle(a, \alpha)$, где $g = \varphi(v)$, π: $I \to F$, $a \to f_\alpha$. Таким образом, $v = (g, \pi) \in F \operatorname{Wr} G$. ■

5. Нормальные делители транзитивных групп.

Теорема 4. *Пусть* Γ — *транзитивная группа подстановок множества* X, *а* H — *ее отличный от* (e) *интранзитивный нормальный делитель. Тогда разбиение множества* X *на орбиты группы* H *является его разбиением на системы импримитивности группы* Γ.

Доказательство. Пусть $X = \bigcup X_\alpha$, $\alpha \in I$, — разбиение множества X на орбиты группы H. Так как $H \neq (e)$, то существует такое $\alpha \in I$, что $\operatorname{card} X_\alpha > 1$. Так как группа H интранзитивна, то $\operatorname{card} I > 1$. Остается показать, что для $g \in \Gamma$

$$g(X_\alpha) \subset X_\beta, \qquad \alpha, \beta \in I. \tag{15}$$

Если $a_1, b_1 \in g(X_\alpha)$, то $a_1 = g(a)$, $b_1 = g(b)$, где $a, b \in \in X_\alpha$; $b = h(a)$, где $h \in H$. Далее, $h_1 = ghg^{-1} \in H$, $h_1(a_1) = b_1$, $a_1, b_1 \in X_\beta$. Отсюда следует включение (15). ■

Следствие 1. *Отличный от (e) нормальный делитель примитивной группы подстановок транзитивен.*

Следствие 2. *Отличный от (e) абелев нормальный делитель H примитивной группы подстановок — характеристически простая группа, т. е. в H нет нетривиальных характеристических подгрупп.*

Доказательство. Пусть F — нетривиальная характеристическая подгруппа группы H. Согласно предыдущему следствию F — транзитивная абелева группа. В силу следствия 2.3.4 группа F максимальна среди абелевых подгрупп симметрической группы. Последнее противоречит строгому включению $F \subset H$. ■

Следствие 3. *Аддитивная группа ассоциативного тела характеристически проста.*

Доказательство. Пусть T — ассоциативное тело. В симметрической группе $S(T)$ выделим подгруппу Γ, состоящую из всех подстановок f вида $f(x) = \alpha x + \beta$, x, α, $\beta \in T$, $\alpha \neq 0$. Очевидно, Γ — дважды транзитивная группа. Согласно теореме 1 группа Γ примитивна. Все подстановки h вида $h(x) = x + \tau$, $x, \tau \in T$, составляют абелев нормальный делитель H группы Γ. По предыдущему следствию группа H характеристически проста. Очевидно, наконец, что аддитивная группа тела T и группа H изоморфны. ■

Теорема 5. *Транзитивная группа подстановок Γ, имеющая отличный от (e) центр, почти всегда импримитивна. Исключение составляет случай, когда порядок и степень группы Γ есть одно и то же простое число.*

Доказательство. Пусть Γ — примитивная группа, Z — ее центр, $Z \neq (e)$. Согласно следствию 4.1 группа Z транзитивна. Для любого $g \in \Gamma$ $(g)Z$ — транзитивная абелева группа. По следствию 2.3.4 $(g)Z = Z$, $g \in Z$, $\Gamma = Z$. В силу следствия 2.2 порядок и степень группы Γ есть одно и то же простое число. ■

Следствие 1. *Если множество X содержит не менее трех точек, то группа $S(X)$ — без центра.*

Пусть Γ — транзитивная подгруппа в $S(X)$, H — интранзитивный нормальный делитель в Γ, а $X = \bigcup X_\alpha$, $\alpha \in I$, — разбиение множества X на орбиты группы H. Введем транзитивные представления r_α группы H:

$$r_\alpha\colon\ H \to S(X_\alpha), \qquad h \mapsto h_\alpha = h \mid X_\alpha. \tag{16}$$

Систему всех орбит X_α группы H разобьем на классы, относя X_α и X_β к одному и тому же классу тогда и только тогда, когда представления r_α и r_β эквивалентны. Объединяя орбиты каждого класса, получим разбиение множества X:

$$X = \bigcup Y_\lambda, \qquad \lambda \in K, \tag{17}$$

где K — множество всех классов, $Y_\lambda = \bigcup X_\alpha$, $\alpha \in I_\alpha$, $I = \bigcup I_\lambda$, $\lambda \in K$, а r_α и r_β тогда и только тогда эквивалентны, когда индексы α и β принадлежат одному и тому же I_λ. При этих обозначениях справедлива

Теорема 6. (i) *Группы $H_\alpha = H \mid X_\alpha$, $\alpha \in I$, попарно подобны.*

(ii) *Если* $\operatorname{card} K > 1$, *то* (17) *есть разбиение на системы импримитивности группы* Γ.

Доказательство. Пусть $\alpha, \beta \in I$. Докажем существование такой биекции $\gamma\colon X_\alpha \to X_\beta$, что

$$H_\beta = \gamma H_\alpha \gamma^{-1}. \tag{18}$$

Так как группа Γ транзитивна, то в ней есть такая подстановка g, что $g(X_\alpha) = X_\beta$. Построим отображение

$$\gamma\colon\ X_\alpha \to X_\beta, \qquad x_\alpha \mapsto g(x) = x_\beta.$$

Очевидно, γ — биекция. Любую точку $x_\beta \in X_\beta$ запишем в виде $x_\beta = \gamma(x_\alpha)$, $x_\alpha \in X_\alpha$. Для $h_\alpha \in H_\alpha$ можно написать

$$\gamma h_\alpha \gamma^{-1}(x_\beta) = \gamma h_\alpha(x_\alpha) = gh(x_\alpha) = \bar{h}\gamma(x_\alpha) = \bar{h}(x_\beta) = \bar{h}_\beta(x_\beta),$$

где $\bar{h} = ghg^{-1}$, $\bar{h}_\beta = \bar{h} \mid X_\beta \in H_\beta$. Следовательно,

$$\gamma h_\alpha \gamma^{-1} \in H_\beta, \qquad \gamma H_\alpha \gamma^{-1} \subset H_\beta.$$

Меняя местами α с β, γ с γ^{-1} и g с g^{-1}, находим

$$\gamma^{-1} H_\beta \gamma \subset H_\alpha.$$

Отсюда вытекает (18), а равенство (18) означает подобие групп H_α и H_β. (i) доказано

Докажем (ii). Пусть два представления r_α и r_β эквивалентны. Тогда, по определению эквивалентности, существует такая биекция γ: $X_\alpha \to X_\beta$, что для любого $h \in H$

$$r_\beta(h) = \gamma r_\alpha(h)\gamma^{-1},$$

т. е.

$$h_\beta = \gamma h_\alpha \gamma^{-1}, \tag{19}$$

где $h_\alpha = h|X_\alpha$, $h_\beta = h|X_\beta$. Пусть теперь $g \in \Gamma$, $g(X_\alpha) = X_\sigma$, $g(X_\beta) = X_\tau$. Покажем эквивалентность представлений r_σ и r_τ. С этой целью построим отображение

$$f\colon X_\sigma \to X_\tau, \qquad f\colon g(x_\alpha) \mapsto g(\gamma(x_\alpha)), \tag{20}$$

где x_α — произвольная точка из X_α. Очевидно, что f — биекция. Положим $x_\sigma = g(x_\alpha)$, $\bar h = g^{-1}hg$ для любого $h \in H$, $\bar h_\alpha = \bar h|X_\alpha$. Тогда из (19) и (20) получим следующие равенства, верные при любом $h \in H$:

$$h_\tau f(x_\sigma) = h_\tau f(g(x_\alpha)) = h_\tau g(\gamma(x_\alpha)) = hg(\gamma(x_\alpha)) = g\bar h(\gamma(x_\alpha)) =$$
$$= g\bar h_\beta(\gamma(x_\alpha)) = g\gamma\bar h_\alpha\gamma^{-1}(\gamma(x_\alpha)) = g\gamma\bar h_\alpha(x_\alpha) = g\gamma\bar h(x_\alpha) =$$
$$= f(g(\bar h(x_\alpha))) = f(hg(x_\alpha)) = fh(x_\sigma) = fh_\sigma(x_\sigma).$$

Отсюда

$$h_\tau f = fh_\sigma, \qquad h_\tau = fh_\sigma f^{-1}$$

для любого $h \in H$. Следовательно, представления r_σ и r_τ эквивалентны. Отсюда вытекает, что для любых $\lambda \in K$ и $g \in G$

$$g(Y_\lambda) \subset Y_\mu \tag{21}$$

при некотором $\mu \in K$. Из (21) следует, что (17) — разбиение множества X на системы импримитивности группы G. ■

Так как группа G транзитивна, то вместо (21) можно написать $g(Y_\lambda) = Y_\mu$. Если $Y_\lambda = \bigcup X_\alpha$, $\alpha \in I_\lambda$, то $Y_\mu = \bigcup g(X_\alpha)$, $\alpha \in I_\lambda$. Таким образом, справедливо

Следствие 1. *Мощность множества орбит группы H, входящих в Y_λ, одна и та же для всех $\lambda \in K$. Иными словами, все представления r_α имеют одну и ту же кратность.*

Следствие 2. *Если* $\operatorname{card} I = m < \infty$, *то число неэквивалентных представлений* r_α *делит число* m.

Теорема 7. *Примитивная группа подстановок имеет не более одного отличного от* (e) *абелева нормального делителя.*

Доказательство. Пусть H и F — отличные от (e) абелевы нормальные делители примитивной группы подстановок. Согласно следствию 4.1 H и F — транзитивные группы. Рассмотрим пересечение $D = H \cap F$. Возможны два случая: $D = (e)$ и $D \neq e$. Если $D = (e)$, то HF — абелев нормальный делитель, содержащий группу H. В силу следствия 2.3.4 $HF = H$, $F \subset H$, что противоречит равенству $D = (e)$. Если же $D \neq (e)$, то, по следствию 4.1, D — транзитивная группа. По следствию 2.3.4 $D = H$, $D = F$ и, значит, $H = F$. ∎

§ 4. Группы подстановок, имеющие регулярный нормальный делитель. Примитивные разрешимые группы

1. Регулярные группы. Пусть F — регулярная подгруппа в $S(X)$, а 0 — некоторая фиксированная точка множества X. Зададим биекцию

$$\lambda\colon X \to F, \quad a \mapsto f_a, \qquad f_a(0) = a. \tag{1}$$

С помощью этой биекции на множестве X зададим операцию $+$, положив для $a, b \in X$

$$a + b = f_a f_b(0). \tag{2}$$

Тогда это множество станет аддитивной группой $\langle X, +\rangle$, изоморфной группе F. Полагая в (2) $b = x$, найдем $f_a(x) = a + x$ для любого $x \in X$. Отсюда и из (1) вытекает, что отображение λ есть левое регулярное представление группы $\langle X, +\rangle$. Следовательно, доказана

Лемма 1. *Всякая регулярная группа подстановок есть образ левого регулярного представления.*

Лемма 2. (i) *Изоморфные регулярные группы подстановок множества* X *сопряжены в* $S(X)$.

(ii) *Пусть* $+$ *и* $+_1$ — *групповые операции на множестве* X, $\gamma\colon \langle X, +\rangle \to \langle X, +_1\rangle$ — *изоморфизм,* $\lambda\colon \langle X, +\rangle \to S(X)$ *и* $\lambda_1\colon \langle X, +_1\rangle \to S(X)$ — *левые регулярные представления групп* $\langle X, +\rangle$ *и* $\langle X, +_1\rangle$, $G = \operatorname{Im} \lambda$, $\overline{G} = \operatorname{Im} \lambda_1$. *Тогда* $\overline{G} = \gamma G \gamma^{-1}$.

Доказательство. В силу леммы 1 из (ii) следует (i). Докажем (ii). Положим $\lambda(a)=g_a$, $\lambda_1(a)=\bar{g}_a$. Для $\bar{g}_a\in\bar{G}$ и $x\in X$

$$\bar{g}_a\gamma(x)=a+{}_1\gamma(x)=\gamma(\gamma^{-1}(a)+x)=\gamma(g_{\gamma^{-1}(a)}(x)).$$

Следовательно,

$$\bar{g}_a\gamma=\gamma g_{\gamma^{-1}(a)},\quad \bar{g}_a=\gamma g_{\gamma^{-1}(a)}\gamma^{-1},\quad \bar{G}=\gamma G\gamma^{-1}. \blacksquare$$

Очевидно, образ регулярного представления любой группы — регулярная группа подстановок. Поэтому, *если A — такая абстрактная группа, что* $\operatorname{card} A=\operatorname{card} X$, *то в группе $S(X)$ есть*, согласно лемме 2, *единственная с точностью до сопряженности регулярная подгруппа F, изоморфная группе A. С помощью формулы* (2) *группа F определяет группу $\langle X,+\rangle$, изоморфную A.*

2. Теорема о централизаторе транзитивной группы.

Теорема 1. *Пусть B — транзитивная подгруппа группы $S(X)$, а C — централизатор группы B в $S(X)$.*

(i) *Если группа C транзитивна, то $B\cong C$ и на множестве X можно задать такую групповую операцию $+$, что группа B окажется образом левого регулярного представления группы $\langle X,+\rangle$, а C — образом правого регулярного представления группы $\langle X,+\rangle$.*

(ii) *Если группа C интразитивна и*

$$X=\bigcup X_\alpha,\qquad \alpha\in I, \tag{3}$$

— разбиение множества X на ее орбиты, то для любого $\alpha\in I$ представление r_α: $C\to S(X_\alpha)$, $f\mapsto f|X_\alpha$, является точным и для любых $\alpha,\beta\in I$ представления r_α и r_β эквивалентны.

Доказательство. Пусть группа C транзитивна, $a\in X$, B_a — стационарная подгруппа группы B. Для любого $x\in X$ в группе C есть такая подстановка f, что $f(a)=x$. Если $g\in B_a$, то $gf=fg$, $gf(a)=fg(a)$, $g(x)=f(a)=x$, $B_a=(e)$. Тогда B — регулярная группа. Согласно лемме 1 на множестве X можно задать такую групповую операцию $+$, что группа B окажется образом левого регулярного представления группы $\langle X,+\rangle$. Тогда, по теореме 1.3, C — образ правого регулярного представления группы $\langle X,+\rangle$. Отсюда следует, что группы B и C инверсно изоморфны. (i) доказано.

Пусть теперь группа C интранзитивна. Тогда C — интранзитивный нормальный делитель группы $\Gamma = BC$. Если $C = (e)$, то утверждение (ii) тривиально. Пусть $C \neq (e)$. Тогда, согласно теореме 3.4, (3) — разбиение множества X на системы импримитивности группы Γ. Пусть ε — фиксированный индекс из I. Так как группа B транзитивна, то для любого $\alpha \in I$ можно выбрать в ней такую подстановку g_α, что $g_\alpha(X_\varepsilon) = X_\alpha$. В качестве g_ε возьмем e. Пусть теперь $f \in C$. Тогда $f(X_\alpha) = X_\alpha$. Положим $f_\alpha = f \mid X_\alpha = r_\alpha(f)$, $\gamma_\alpha = g_\alpha \mid X_\varepsilon$. Очевидно, γ_α: $X_\varepsilon \to X_\alpha$ — биекция. Для $x_\alpha \in X_\alpha$ $x_\alpha = g_\alpha(x_\varepsilon) = \gamma_\alpha(x_\varepsilon)$. Далее, $r_\alpha(f)\gamma_\alpha(x_\varepsilon) = f_\alpha g_\alpha(x_\varepsilon) = fg_\alpha(x_\varepsilon) = g_\alpha f(x_\varepsilon) = \gamma_\alpha(r_\varepsilon(f)(x_\varepsilon))$. Отсюда $r_\alpha(f)\gamma_\alpha(x_\varepsilon) = \gamma_\alpha(r_\varepsilon(f)(x_\varepsilon))$ для любого $x_\varepsilon \in X_\varepsilon$. Следовательно, представления r_α и r_ε эквивалентны.

Итак, представления r_α, $\alpha \in I$, попарно эквивалентны. В частности, если для каких-либо $\alpha \in I$ и $f \in C$ $r_\alpha(f) = f_\alpha$ совпадает с тождественной подстановкой $e_\alpha \in S(X_\alpha)$, то и $r_\beta(f_\beta) = e_\beta$, т. е. $f = e$. Следовательно, каждое представление r_α точное. ■

Следствие 1. *Централизатор C примитивной подгруппы B группы $S(X)$ в $S(X)$ почти всегда совпадает с (e). Исключение составляет случай, когда* $\operatorname{card} X = p$ *— простое число, а B — группа порядка p.*

Доказательство. Пусть $C \neq (e)$. C — нормальный делитель примитивной группы BC, поэтому, согласно следствию 3.4.1, C — транзитивная группа. В силу теоремы 1 группа B регулярна. По следствию 3.2.1 B — группа простого порядка и простой степени p. ■

Следствие 2. *Пусть C — централизатор транзитивной подгруппы B группы $S(X)$ в $S(X)$, а H — подгруппа в C.*

(i) *Если группа H транзитивна, то $H = C$.*

(ii) *Если группа H интразитивна и $X = \bigcup X_\alpha$, $\alpha \in I$, — разбиение множества X на ее орбиты, то представления r_α: $H \to S(X_\alpha)$, $h \mapsto h \mid X_\alpha$, $\alpha \in I$, попарно эквивалентны и точны.*

Доказательство. (i) непосредственно вытекает из теоремы 1, (ii) доказывается так же, как в теореме 1. ■

Следствие 3. *Если h — подстановка из группы $S(X)$, перестановочная с каждой подстановкой транзитивной группы B, то ее циклы имеют одну и ту же дли-*

ну. В частности, если $\operatorname{card} X < \infty$, *то порядок подстановки* h *делит* $\operatorname{card} X$.

Лемма 3. *Пусть транзитивная подгруппа* Γ *группы* $S(X)$ *представима в виде произведения* $\Gamma = HF$ *таких своих подгрупп* H *и* F, *что* H *интранзитивна и взаимный коммутант* (H, F) *равен* (e). *Пусть, далее,*

$$X = \bigcup X_\alpha, \qquad \alpha \in I, \tag{4}$$

— разбиение множества X *на орбиты группы* H, *а* r_α: $H \to S(X_\alpha)$, $r_\alpha(h) = h|X_\alpha$. *Тогда представления* r_α *попарно эквивалентны.*

Доказательство. Так как группа H инвариантна в Γ, то (4) — разбиение множества X на системы импримитивности группы Γ. Пусть α и β — произвольные индексы из I. Тогда в F есть такая подстановка f_β, что $f_\beta(X_\alpha) = X_\beta$. Положим $\varphi = f_\beta|X_\alpha$. Очевидно, что φ: $X_\alpha \to X_\beta$ — биекция. Для $x_\alpha \in X_\alpha$, $h \in H$ можно написать $r_\beta(h)(\varphi(x_\alpha)) = r_\beta(h)(f_\beta(x_\alpha)) = h_\beta f_\beta(x_\alpha) = hf_\beta(x_\alpha) = f_\beta h(x_\alpha) = f_\beta h_\alpha(x_\alpha) = \varphi(r_\alpha(h))(x_\alpha)$. Следовательно, $r_\beta(h)\varphi = \varphi r_\alpha(h)$. Эквивалентность r_α и r_β доказана. ■

3. Группы, имеющие регулярный нормальный делитель. Пусть F — регулярная подгруппа группы $S(X)$, N — нормализатор F в $S(X)$, 0 — нуль группы $\langle X, +\rangle$ (см. формулы (1), (2)), а N_0 — стабилизатор точки 0 в N. Тогда верна

Теорема 2 (теорема о голоморфе). (i) $N = FN_0$.

(ii) $N_0 = \operatorname{Aut}\langle X, +\rangle$ — *группа всех автоморфизмов группы* $\langle X, +\rangle$.

(iii) *Для любого автоморфизма* ψ *группы* F *в* N_0 *есть такой элемент* g_0, *что* $\psi(f) = g_0 f g_0^{-1}$ *при всяком* $f \in F$.

Доказательство. (i) следует из теормы 2.2. Докажем (ii). Пусть $g_0 \in N_0$. Тогда для $a, b \in \langle X, +\rangle$

$$g_0(a) = g_0 f_a(0) = g_0 f_a g_0^{-1}(0) = f_c(0) = c,$$

$$g_0(b) = g_0 f_b(0) = f_d(0) = d,$$

где $f_c = g_0 f_a g_0^{-1}$, $f_d = g_0 f_b g_0^{-1}$. Далее,

$$g_0(a+b) = g_0(f_a f_b(0)) = g_0 f_a f_b g_0^{-1}(0) =$$
$$= f_c f_d(0) = c + d = g_0(a) + g_0(b).$$

Следовательно, $g_0 \in \mathrm{Aut}\langle X, +\rangle$, $N_0 \subset \mathrm{Aut}\langle X, +\rangle$. Пусть теперь $\varphi \in \mathrm{Aut}\langle X, +\rangle$. Тогда

$$\varphi(0) = 0, \qquad \varphi(a) = \varphi f_a \varphi^{-1}(0) = b = f_b(0),$$

где a, $b \in X$, f_a, $f_b \in F$. Докажем, что для любого $x \in X$

$$\varphi f_a \varphi^{-1}(x) = f_b(x). \tag{5}$$

Положим $x = \varphi(y)$, $y \in X$. Тогда

$$\varphi f_a \varphi^{-1}(x) = \varphi f_a(y) = \varphi f_a f_y(0) =$$
$$= \varphi(a + y) = \varphi(a) + \varphi(y) = b + x = f_b(x).$$

Равенство (5) доказано, следовательно, $\varphi f_a \varphi^{-1} = f_b \in F$ при любом φ из $\mathrm{Aut}\langle X, +\rangle$, т. е. $\varphi \in N$. Так как $\varphi(0) = (0)$, то $\varphi \in N_0$, $\mathrm{Aut}\langle X, +\rangle \subset N_0$. Отсюда и из предыдущего включения следует $N_0 = \mathrm{Aut}\langle X, +\rangle$.

Остается доказать (iii). Пусть ψ — автоморфизм группы F, а x пробегает множество X. Если $\psi(f_x) = f_{\bar{x}}$, то отображение φ: $x \mapsto \bar{x}$ — автоморфизм группы $\langle X, +\rangle$, ибо (1) — изоморфизм групп $\langle X, +\rangle$ и F. В силу (ii) $\varphi \in N_0$. Следовательно,

$$\psi(f_x) = f_{\varphi(x)}, \tag{6}$$

где $\varphi \in N_0$. Далее,

$$\varphi f_x \varphi^{-1}(0) = \varphi(x) = f_{\varphi(x)}(0). \tag{7}$$

Так как $f_{\varphi(x)}$ и $\varphi f_x \varphi^{-1}$ — элементы регулярной группы F, то из (7) вытекает равенство $\varphi f_x \varphi^{-1} = f_{\varphi(x)}$. Отсюда и из (6) следует

$$\psi(f_x) = \varphi f_x \varphi^{-1}, \qquad \varphi \in N_0. \ ■$$

Из теоремы 2 вытекает

Теорема 3. *Пусть Γ — подгруппа группы $S(X)$, содержащая регулярный нормальный делитель F, а $\langle X, +\rangle$ — группа, определяемая формулами* (2). *Тогда*

(i) $\Gamma = \Gamma_0 F$, $F \cap \Gamma_0 = (e)$, *где* Γ_0 — *стабилизатор нуля* 0 *группы* $\langle X, +\rangle$ *в* Γ,

(ii) Γ_0 — *подгруппа в* $\mathrm{Aut}\langle X, +\rangle$.

Введем одно определение. Пусть A — произвольная группа, а H — подгруппа в $\mathrm{Aut}\,A$. Подгруппа B группы A называется *H-допустимой*, если $h(B) = B$ для каждого h из H. Подгруппа H в $\mathrm{Aut}\,A$ называется *не-*

приводимой, если единственными *H-допустимыми* подгруппами группы A являются A и (e).

Теорема 4. *Подгруппа* Γ *группы* $S(X)$, *содержащая регулярный нормальный делитель* F, *тогда и только тогда примитивна, когда* Γ_0 (см. теорему 3) — *неприводимая подгруппа группы* $\mathrm{Aut}\langle X, +\rangle$. *В частности, нормализатор* N *регулярной подгруппы* F *в* $S(X)$ *тогда и только тогда примитивен, когда* F *характеристически проста.*

Доказательство. Пусть $\Gamma = F\Gamma_0$ импримитивна. Тогда, по критерию примитивности, в Γ есть промежуточная подгруппа U, $\Gamma \supset U \supset \Gamma_0$, $\Gamma \neq U \neq \Gamma_0$. Положим $F_1 = U \cap F$. Тогда $F_1 \neq (e)$, $F_1 \neq F$ и для $g \in \Gamma_0$ $gUg^{-1} = U$. Следовательно, для любого $g \in \Gamma_0$

$$gF_1g^{-1} = F_1. \tag{8}$$

Положим теперь $X_1 = \lambda^{-1}(F_1)$ (см. отображение (1)) и покажем, что X_1 является Γ_0-допустимой подгруппой в $\langle X, +\rangle$. Для $x_1 \in X_1$ и $g \in \Gamma_0$ можно написать

$$g(x_1) = gf_{x_1}(0) = gf_{x_1}g^{-1}(0) = f_{x_2}(0) = x_2,$$

где f_{x_2}, в силу (8), принадлежит подгруппе F_1. Следовательно, $x_2 \in X_1$, а X_1 есть Γ_0-допустимая подгруппа группы $\langle X, +\rangle$.

Обратно, пусть в группе $\langle X, +\rangle$ есть нетривиальная Γ_0-допустимая подгруппа X_1. Положим $F_1 = \lambda(X_1)$. Очевидно, что F_1 — промежуточная между F и (e) подгруппа. Для $y \in X_1$, $g \in \Gamma_0$

$$gf_yg^{-1}(0) = gf_y(0) = g(y) = y_1 \in X_1.$$

Следовательно,

$$gf_yg^{-1} = f_{y_1} \in \lambda(X_1) = F_1,$$

т. е.

$$gF_1g^{-1} = F_1.$$

Значит, $F_1\Gamma_0$ — подгруппа в Γ. Очевидно, $F_1\Gamma_0$ — промежуточная между Γ и Γ_0 подгруппа. По критерию примитивности 3.2 группа Γ импримитивна. ∎

Доказанную теорему можно сформулировать, не прибегая к группе $\langle X, +\rangle$:

Пусть Γ — *группа подстановок, имеющая регулярный нормальный делитель* F, Γ_1 — *какая-либо ее стационарная* *подгруппа, H — группа всех автоморфизмов h группы F вида*

$$h(f)=g_1 f g_1^{-1}, \qquad g_1 \in \Gamma_1, \qquad f \in F.$$

Группа Γ тогда и только тогда примитивна, когда H — неприводимая подгруппа в $\operatorname{Aut} F$.

4. Примитивные группы, имеющие абелев нормальный делитель.

Теорема 5. *Пусть F — отличная от (e) абелева подгруппа группы $S(X)$, N — ее нормализатор в $S(X)$, A и B — примитивные подгруппы в N, содержащие группу F, A_0, B_0, N_0 — стационарные подгруппы групп A, B, N, оставляющие неподвижной одну и ту же точку $0 \in X$. Группы A и B тогда и только тогда сопряжены в $S(X)$, когда A_0 и B_0 сопряжены в N_0.*

Доказательство. Из примитивности группы A вытекает, в силу следствия 3.4.1, транзитивность группы F. Отсюда и из коммутативности группы F следует ее регулярность (см. следствие 2.3.3). Тогда, согласно теоремам 2 и 3,

$$N=FN_0, \qquad A=FA_0, \qquad B=FB_0. \tag{9}$$

Если в группе N_0 есть такой элемент v, что $vA_0v^{-1}=B_0$, то, используя (9), получим

$$vAv^{-1}=vFA_0v^{-1}=vFv^{-1}vA_0v^{-1}=FB_0=B.$$

Обратно, пусть в группе $S(X)$ есть такая подстановка r, что $rAr^{-1}=B$. Тогда rFr^{-1} — абелев нормальный делитель в B. Согласно теореме 3.5 $rFr^{-1}=F$. Следовательно, $r \in N$. В силу (9) $r=vf$, где $v \in N_0$, $f \in F$. Тогда

$$rAr^{-1}=vAv^{-1}=FB_0.$$

Очевидно, стационарная подгруппа группы vAv^{-1}, оставляющая на месте точку 0, совпадает с группой vA_0v^{-1}. Следовательно,

$$B_0=vA_0v^{-1}. \blacksquare$$

Теорема 6. *Пусть Γ и G — две такие примитивные подгруппы в $S(X)$, что каждая из них обладает отличным от (e) абелевым нормальным делителем. Тогда изоморфизм групп Γ и G влечет за собой их сопряженность в $S(X)$.*

Доказательство. Пусть $\Phi \neq (e)$ — абелев нормальный делитель группы Γ, а $F \neq (e)$ — абелев нормальный делитель в G. Так как Γ и G — примитивные группы, а Φ и F — абелевы, то, согласно теореме 3.4, Φ и F суть регулярные подгруппы в $S(X)$. В силу теоремы 3 $\Gamma = \Gamma_0\Phi$, $G = G_0F$, где Γ_0 и G_0 — стационарные подгруппы групп Γ и G. Пусть теперь $\psi\colon \Gamma \to G$ — изоморфизм. Тогда $\psi(\Phi)$ — абелев нормальный делитель в G, совпадающий, по теореме 3.5, с группой F. Значит, $\Phi \cong F$. Согласно лемме 2 в группе $S(X)$ есть такая подстановка t, что $t\Phi t^{-1} = F$. Положим $A = t\Gamma t^{-1}$; A — примитивная группа, изоморфная группе G. По теореме 3 $A = A_0F$, где A_0 — стационарная подгруппа группы A. Если $\varphi : A \to G$ — изоморфизм, то, согласно теореме 3.5, $\varphi(F) = F$. Следовательно, $\varphi|F$ — автоморфизм группы F. Пусть теперь N — нормализатор группы F в $S(X)$. Тогда $N = N_0F$, где N_0 — стационарная подгруппа группы N. По теореме 2 в группе N_0 есть такая подстановка d, что для любого $f \in F$ $\varphi(f) = dfd^{-1}$. Построим теперь изоморфизм $\gamma\colon A \to \gamma(A)$, $x \mapsto d^{-1}\varphi(x)d$. В силу выбора d ограничение $\gamma|F$ является единицей группы $\operatorname{Aut} F$. Для любых $f \in F$, $a \in A$ имеем

$$afa^{-1} \in F. \tag{10}$$

Отсюда

$$\gamma(a)f\gamma(a)^{-1} = afa^{-1}. \tag{11}$$

Следовательно, для любого $f \in F$ $a^{-1}\gamma(a)f = fa^{-1}\gamma(a)$. Согласно следствию 2.3.4 $a^{-1}\gamma(a) \in F$. Далее, $\gamma(a) = af_1$, $f_1 \in F$, $\gamma(A) = \gamma(A_0F) = A_0F = A$. С другой стороны, $\gamma(A) = d^{-1}\varphi(A)d = d^{-1}Gd$. Следовательно, $t\Gamma t^{-1} = A = d^{-1}Gd$. ■

Если отличная от (e) абелева группа F является нормальным делителем примитивной группы, то F характеристически проста. Характеристически простые абелевы группы легко обозримы.

Лемма 4. *Аддитивные группы линейных пространств над простыми полями и только они являются характеристически простыми абелевыми группами* *).

---

*) Очевидно, что простое поле здесь можно заменить любым. Но нам удобнее приведенная формулировка.

Доказательство. Если A — характеристически простая аддитивная абелева группа, то, очевидно, все отличные от нуля ее элементы имеют один и тот же простой порядок p, либо A — группа без кручения. Ясно, что в первом случае A — аддитивная группа линейного пространства над полем $GF(p)$, содержащим точно p элементов. Рассмотрим второй случай. Очевидно, уравнение $mx = na$, где m и n — произвольные целые числа, $m > 0$, имеет в A единственное решение. Положим $\frac{n}{m} a = x$. Прямые вычисления показывают, что A с введенным таким образом умножением на рациональные числа — линейное пространство над полем рациональных чисел.

С другой стороны, *полная линейная группа* $GL(V)$ всех обратимых линейных преобразований пространства V над любым полем транзитивна (см. гл. II, § 7), так что аддитивная группа линейного пространства характеристически проста. ■

Известно также, что абелева группа тогда и только тогда характеристически проста, когда она изоморфна аддитивной группе некоторого поля.

Лемма 5. *Пусть V — линейное пространство над простым полем Δ, а A — аддитивная группа пространства V. Тогда $\operatorname{Aut} A$ совпадает с полной линейной группой $GL(V)$.*

Доказательство. $GL(V)$ состоит из всех таких биекций $g\colon V \to V$, что для любых $x, y \in V$, $\lambda \in \Delta$ $g(x+y) = g(x) + g(y)$, $g(\lambda x) = \lambda g(x)$. Следовательно, $GL(V) \subset \operatorname{Aut} A$.

Верно и включение $\operatorname{Aut} A \subset GL(V)$. Действительно, пусть $x \in A$, $\lambda \in \Delta$, $\varphi \in \operatorname{Aut} A$. Если Δ — простое поле простой характеристики, то $\lambda x = lx$, где l — целое число, зависящее только от λ. Следовательно, $\varphi(\lambda x) = \varphi(lx) = l\varphi(x) = \lambda\varphi(x)$, $\varphi \in GL(V)$. Пусть теперь Δ — простое поле нулевой характеристики, т. е. поле рациональных чисел, а $\lambda \neq 0$. Тогда $\lambda = \frac{k}{l}$, где k и l — целые числа. Положим $\lambda x = y$. Ясно, что $kx = ly$, $\varphi(kx) = \varphi(ly)$, $k\varphi(x) = l\varphi(y)$, $\varphi(y) = \lambda\varphi(x)$, $\varphi(\lambda x) = \lambda\varphi(x)$, $\varphi \in GL(V)$. ■

Очевидно, что линейное пространство $V \neq (0)$ над полем Δ тогда и только тогда не имеет подгрупп, не являющихся подпространствами, когда Δ — простое поле простой характеристики. Следовательно, *если A — аддитивная группа линейного пространства V над Δ, то для $\Delta = GF(p)$ класс всех неприводимых подгрупп группы* $\operatorname{Aut} A$ *совпадает с классом всех неприводимых подгрупп группы* $GL(V)$ *), *а для $\Delta = Q$, где Q — поле рациональных чисел, класс неприводимых подгрупп группы* $\operatorname{Aut} A$ *строго включается в класс неприводимых подгрупп группы* $GL(V)$.

Теорема 7. *Пусть Γ — примитивная подгруппа в $S(X)$, обладающая абелевым нормальным делителем $F \neq (e)$. Тогда:*

(i) *F изоморфна аддитивной группе некоторого линейного пространства V над простым полем Δ и состоит из всех параллельных переносов f_a пространства V,*

$$f_a(x) = x + a, \quad a, x \in V = X, \quad f_a \in F;$$

(ii) $\Gamma = \Gamma_0 F$, $\Gamma_0 \cap F = (e)$, *где 0 — нуль аддитивной группы $\langle X, +\rangle$ пространства V, а Γ_0 — стабилизатор точки 0 в Γ;*

(iii) *Γ_0 — подгруппа в $GL(V)$, неприводимая как подгруппа в* $\operatorname{Aut}\langle X, +\rangle$ **).

Доказательство. Из примитивности группы Γ следует транзитивность группы F. Отсюда и из коммутативности группы F вытекает ее регулярность. В силу теоремы 4 группа F характеристически проста. Отсюда и из леммы 4 следует (i). (ii) вытекает из теоремы 3, (iii) следует из теоремы 3, теоремы 4 и леммы 5. ■

5. Примитивные разрешимые группы. Применим теперь полученные результаты к разрешимым примитивным группам подстановок. Пусть Γ — разрешимая примитивная подгруппа в $S(X)$. Тогда, в силу разрешимости, Γ обладает отличным от (e) абелевым нормальным делителем F (см. Курош [1], стр. 361). Следовательно, к группе Γ применима теорема 7, т. е.

$$\Gamma = \Gamma_0 F, \tag{12}$$

*) О неприводимых линейных группах см. § 14.

**) Как уже отмечалось, для $\Delta = Q$ неприводимости Γ_0 как подгруппы в $GL(V)$ недостаточно.

где F — группа параллельных переносов некоторого линейного пространства V над простым полем Δ, Γ_0 — стабилизатор нуля 0 аддитивной группы $\langle X, +\rangle$ пространства V в группе Γ. Согласно теореме 7 Γ_0 — подгруппа в $GL(V)$, неприводимая как подгруппа группы $\mathrm{Aut}\langle X, +\rangle$. Укажем один способ задания всех примитивных разрешимых подгрупп группы $S(X)$.

Обозначим буквой $\mathfrak{A} = \{A_\alpha\}$, $\alpha \in I$, класс всех таких характеристически простых абелевых групп A_α, что $\mathrm{card}\, A_\alpha = \mathrm{card}\, X$. Для каждой группы $A_\alpha \in \mathfrak{A}$ построим на базе X аддитивную группу $\langle X, +_\alpha\rangle \cong A_\alpha$ и регулярное представление λ_α: $\langle X, +_\alpha\rangle \to S(X)$. Положим $F_\alpha = \mathrm{Im}\,\lambda_\alpha$. Пусть, далее, $\mathfrak{G}_\alpha$ — класс неприводимых разрешимых подгрупп группы $\mathrm{Aut}\,\langle X, +_\alpha\rangle$ такой, что каждая неприводимая разрешимая подгруппа группы $\mathrm{Aut}\,\langle X, +_\alpha\rangle$ сопряжена в $\mathrm{Aut}\,\langle X, +_\alpha\rangle$ с одной и только одной подгруппой из класса $\mathfrak{G}_\alpha$. Так как, по теореме 2, $\mathrm{Aut}\,\langle X, +_\alpha\rangle$ содержится в нормализаторе группы F_α в $S(X)$, то для $\Gamma_{0\alpha} \in \mathfrak{G}_\alpha$

$$\Gamma = \Gamma_{0\alpha} F_\alpha \tag{13}$$

является группой. Пусть $\mathfrak{M}_\alpha$ — класс всех групп вида (13). Положим

$$\mathfrak{M} = \bigcup \mathfrak{M}_\alpha, \qquad \alpha \in I. \tag{14}$$

Теорема 8. (i) *Каждая группа из класса $\mathfrak{M}$ является примитивной разрешимой подгруппой в $S(X)$.*

(ii) *Любая примитивная разрешимая подгруппа группы $S(X)$ сопряжена в $S(X)$ с одной и только одной группой из класса $\mathfrak{M}$.*

Доказательство. Пусть $\Gamma \in \mathfrak{M}$. Тогда согласно (13), $\Gamma = \Gamma_{0\alpha} F_\alpha$, $\Gamma_{0\alpha} \in \mathfrak{G}_\alpha$. $\Gamma_{0\alpha}$ — разрешимая подгруппа группы Γ, а F_α — абелев нормальный делитель, поэтому Γ — разрешимая группа. По теореме 4 группа Γ примитивна, ибо $\Gamma_{0\alpha}$ — неприводимая подгруппа группы $\mathrm{Aut}\,\langle X, +_\alpha\rangle$. (i) доказано.

Перейдем к (ii). Докажем сперва, что две различные группы B и C из класса $\mathfrak{M}$ не сопряжены в группе $S(X)$. В силу (13) и (14) $B = H_\alpha F_\alpha$, $C = G_\beta F_\beta$, где $H_\alpha \in \mathfrak{G}_\alpha$, $G_\beta \in \mathfrak{G}_\beta$ и для $\alpha \neq \beta$ $F_\alpha \not\cong F_\beta$. Согласно теореме 3.5 сопряженность групп B и C в $S(X)$ влечет за собой сопряженность групп F_α и F_β. Поэтому при

$\alpha \neq \beta$ группы B и C не сопряжены в группе $S(X)$. Пусть теперь $\alpha = \beta$. Группы H_α и G_α, по построению класса $\mathfrak{G}_\alpha$, не сопряжены в группе $\mathrm{Aut}\langle X, +_\alpha\rangle$. Поэтому, по теореме 5, группы B и C не сопряжены в группе $S(X)$.

Остается теперь доказать, что всякая примитивная разрешимая погруппа Γ группы $S(X)$ сопряжена в $S(X)$ с какой-нибудь группой из класса $\mathfrak{M}$. Согласно теореме 7 $\Gamma = \Gamma_0 F$, где F — регулярная абелева подгруппа группы $S(X)$, Γ_0 — неприводимая разрешимая подгруппа в $\mathrm{Aut}\langle X, +\rangle$, а $\langle X, +\rangle$ — группа, определяемая группой F с помощью формулы (2). По построению класс $\mathfrak{A}$ содержит группу $A_\alpha \cong F \cong \langle X, +\rangle$. Следовательно, для некоторого $\alpha \in I$ $\langle X, +\rangle \cong \langle X, +_\alpha\rangle$. В силу леммы 2 в группе $S(X)$ есть такая подстановка u, что u: $\langle X, +\rangle \to \langle X, +_\alpha\rangle$ — изоморфизм, а $F_\alpha = uFu^{-1}$. Если теперь $N_0 = \mathrm{Aut}\langle X, +\rangle$, то $uN_0u^{-1} = \mathrm{Aut}\langle X, +_\alpha\rangle$. Тогда

$$u\Gamma u^{-1} = u\Gamma_0 u^{-1} F_\alpha, \qquad u\Gamma_0 u^{-1} \subset \mathrm{Aut}\langle X, +_\alpha\rangle.$$

$u\Gamma_0 u^{-1}$ — разрешимая неприводимая подгруппа группы $\mathrm{Aut}\langle X, +_\alpha\rangle$. Следовательно, $u\Gamma_0 u^{-1}$ сопряжена в $\mathrm{Aut}\langle X, +_\alpha\rangle$ с некоторой подгруппой из класса $\mathfrak{G}_\alpha$. Тогда, по теореме 5, группа $u\Gamma u^{-1}$ сопряжена в $S(X)$ с одной из групп класса $\mathfrak{M}_\alpha$. ■

В связи с доказанной теоремой отметим, что для любого $\alpha \in I$ (см. (14)) подкласс $\mathfrak{M}_\alpha$ не пуст. Действительно, характеристически простая группа A_α изоморфна аддитивной группе некоторого поля Ω (см. замечание после леммы 4). Следовательно, в подклассе $\mathfrak{M}_\alpha$ есть группа Γ всех отображений вида

$$g_{\lambda,\mu}\colon\ \Omega \to \Omega, \quad g_{\lambda,\mu}(x) = \lambda x + \mu, \quad x, \lambda, \mu \in \Omega, \quad \lambda \neq 0. \tag{15}$$

Добавим, наконец, что в случае разрешимых групп теорема 6 принимает следующий вид.

Теорема 6а. *Если две разрешимые примитивные подгруппы группы $S(X)$ изоморфны, то они сопряжены в $S(X)$.*

6. Примитивные разрешимые группы конечной степени.

Теорема 9. *Пусть X — конечное множество. В группе $S(X)$ тогда и только тогда есть примитивные* *разрешимые подгруппы, когда* card X — *степень простого числа.*

Доказательство. Пусть card $X = m$, а Γ — примитивная разрешимая подгруппа в S_m. Согласно теоремам 7 и 8 в группе Γ есть абелев нормальный делитель F порядка m, являющийся аддитивной группой линейного пространства над простым полем Σ. Следовательно, $\Sigma = GF(p)$, где p — простое число, $m = p^n$.

Обратно, пусть card $X = p^n$. Возьмем в качестве множества X поле $\Delta = GF(p^n)$. Тогда группа всех подстановок вида (15) — примитивная разрешимая подгруппа группы $S(X)$. ■

Лемма 6. *Примитивная разрешимая группа* Γ *тогда и только тогда максимальна среди разрешимых подгрупп группы* $S(X)$, *когда* Γ_0 (см. (12)) *максимальна среди разрешимых подгрупп группы* $GL(V)$. *Если* Γ *и* G — *примитивные разрешимые подгруппы группы* $S(X)$ *и* $G \supset \Gamma$, *то абелев нормальный делитель группы* Γ *является нормальным делителем группы* G.

Доказательство. Докажем сначала второе утверждение леммы. Группы Γ и G запишем в виде $\Gamma = F\Gamma_0$, $G = HG_0$, где F и H — регулярные абелевы нормальные делители, а Γ_0 и G_0 — стабилизаторы точки 0 в группах Γ и G соответственно. Очевидно, $\Gamma \cap H$ — нормальный делитель группы Γ. Следовательно, в силу теоремы 3.7, либо $\Gamma \cap H = F$, либо $\Gamma \cap H = 1$. В первом случае $H \supset F$, а отсюда и из регулярности групп H и F и вытекает равенство $H = F$. Покажем невозможность второго случая. Пусть $\Gamma \cap H = 1$. Тогда построим группу $U = H\Gamma$ и запишем ее в виде $U = HU_0$, где U_0 — стабилизатор точки 0 в U. Так как $\Gamma \cap H = 1$, то U_0 изоморфна группе Γ. Следовательно, U_0 обладает абелевым нормальным делителем порядка $p^n =$ card X. В силу примитивности U группа U_0 — неприводимая подгруппа группы $GL(n, p) \equiv GL(V)$, где V есть n-мерное линейное пространство над $GF(p)$. По первой теореме Клиффорда (теорема 16.1) U_0 не может обладать нормальным делителем порядка p^n. Следовательно, второй случай невозможен.

Теперь легко доказать первое утверждение леммы. Если Γ — максимальная примитивная разрешимая подгруппа в $S(X)$, то, очевидно, Γ_0 максимальна среди разрешимых подгрупп в $GL(V)$. Обратно, пусть $\Gamma = F\Gamma_0$, Γ_0 — максимальная разрешимая подгруппа в $GL(V)$, а $F \subset G$, где G — разрешимая подгруппа в $S(X)$. Тогда, согласно второму утверждению леммы, $G = FG_0$ и F — нормальный делитель группы G. Следовательно, $GL(V) \supset G_0 \supset \Gamma_0$. Из максимальности группы Γ_0 вытекает $G_0 = \Gamma_0$, $G = \Gamma$. ■

Если Γ — примитивная разрешимая подгруппа в $S(X)$, $\operatorname{card} X = p^n$, $F \neq (e)$ — абелев нормальный делитель в Γ, то, как отмечалось выше, группу $\langle X, +\rangle$ можно трактовать как аддитивную группу пространства Σ^n над полем $\Sigma = GF(p)$. Тогда группа F становится группой всех параллельных переносов f_a вида

$$f_a = a + x, \qquad a,\ x \in \Sigma^n,$$

пространства Σ^n. Согласно теореме 8 $\Gamma = \Gamma_0 F$, где Γ_0 — разрешимая неприводимая подгруппа в группе $GL(\Sigma^n)$. Отсюда и из теорем 7 и 5 вытекает

Теорема 10. (i) *Группа*

$$\Gamma = AF, \tag{16}$$

где F — группа параллельных переносов пространства Σ^n, $\Sigma = GF(p)$, а A — неприводимая разрешимая подгруппа группы $GL(\Sigma^n)$, является примитивной разрешимой подгруппой симметрической группы S_{p^n}.

(ii) *Любая примитивная разрешимая подгруппа группы S_{p^n} сопряжена в S_{p^n} с одной из групп вида* (16).

(iii) *Две примитивные разрешимые подгруппы $\Gamma = AF$ и $\Phi = BF$ вида* (16) *тогда и только тогда сопряжены в группе S_{p^n}, когда группы A и B сопряжены в $GL(\Sigma^n)$.*

(iv) *Группа* (16) *тогда и только тогда максимальна среди разрешимых подгрупп группы S_{p^n}, когда группа A максимальна среди разрешимых подгрупп группы $GL(\Sigma^n)$.*

Теорема 10 полностью редуцирует проблему построения примитивных разрешимых подгрупп группы S_{p^n} к построению неприводимых разрешимых подгрупп группы $GL(\Sigma^n)$.

В случае групп простой степени, т. е. при $n=1$, вопрос полностью решает

Теорема 11. (i) *В группе S_p есть лишь одна, с точностью до сопряженности, максимальная разрешимая транзитивная подгруппа Γ_p. Порядок группы Γ_p равен $p(p-1)$; она состоит из всех подстановок $h_{\alpha\beta}$ вида*

$$h_{\alpha\beta}(x)=\beta x+\alpha, \quad \alpha,\ \beta,\ x\in GF(p),\ \beta\neq 0.$$

(ii) *Пусть $\tau=\tau(p-1)$ — число всех положительных делителей числа $p-1$. Тогда система всех разрешимых транзитивных подгрупп группы S_p разбивается на τ классов сопряженных в S_p подгрупп. Представителями этих классов служат группы $\Gamma_{p,s}$, $s\mid p-1$*), $s>0$; порядок группы $\Gamma_{p,s}$ равен ps, она состоит из всех подстановок h_s вида*

$$h_s(x)=\beta^{\frac{p-1}{s}}x+\alpha, \qquad \alpha,\ \beta,\ x\in GF(p), \qquad \beta\neq 0.$$

Доказательство. Теорема следует из теоремы 10, ибо при $n=1$ пространство Σ^n сводится к $\Sigma=GF(p)$, а группа $GL(\Sigma^n)$ — к группе подстановок вида $g(x)=\beta x$, $\beta, x\in GF(p)$, $\beta\neq 0$. Кроме того, согласно следствию леммы 3.1, транзитивная группа подстановок простой степени примитивна. ∎

7. Импримитивные разрешимые группы конечной степени. Пусть θ — какое-либо абстрактное теоретико-групповое свойство, удовлетворяющее следующим условиям:

1. Если группа обладает свойством θ, то ее подгруппы и гомоморфные образы также обладают этим свойством.

2. Если нормальный делитель N группы Γ и фактор-группа Γ/N обладают свойством θ, то и сама Γ обладает этим свойством.

Группы, обладающие свойством θ, будем называть здесь θ-группами. θ-группами являются, в частности, разрешимые группы и Π-группы.

---

*) Здесь и далее мы используем стандартное обозначение: запись $m\mid n$ означает, что число m делит число n; будем использовать также перечеркнутую вертикальную черту для обозначения отрицания отношения делимости.

Теорема 12. *Пусть* Γ — *транзитивная подгруппа группы* S_n, *максимальная среди ее* θ-*подгрупп (свойство* θ *фиксировано). Тогда либо* Γ *примитивна, либо* $\Gamma = F \operatorname{Wr} G$, *где* F — *максимальная примитивная* θ-*подгруппа группы* S_m, G — *максимальная транзитивная* θ-*подгруппа группы* S_l, $lm = n$, $1 < l < n$.

Утверждение теоремы следует из определения θ-группы и теоремы 3.3.

Выбирая в качестве свойства θ разрешимость, получим, учитывая еще теорему 9

Следствие 1. *Максимальная разрешимая транзитивная подгруппа* Γ *группы* S_n *либо примитивна, либо* $\Gamma = F \operatorname{Wr} G$, *где* F — *максимальная примитивная разрешимая подгруппа группы* S_{p^α}, G — *максимальная транзитивная разрешимая подгруппа группы* S_l, $p^\alpha l = n$, p — *простое число, а* α — *натуральное.*

Выбирая в качестве θ-групп Π-группы, получим

Следствие 2. *Транзитивная* Π-*подгруппа Силова* Γ *группы* S_n *либо примитивна, либо* $\Gamma = F \operatorname{Wr} G$, *где* F — *примитивная* Π-*подгруппа Силова группы* S_m, G — *транзитивная* Π-*подгруппа Силова группы* S_l, $ml = n$, $1 < l < n$.

Так как конечная p-группа, где p — простое число, имеет нетривиальный центр, то из теоремы 12 и теоремы 3.6 вытекает

Следствие 3. p-*подгруппа Силова* $\mathfrak{P}_{p^\alpha}$ *группы* S_{p^α} *представима в виде*

$$\mathfrak{P}_{p^\alpha} = \mathfrak{P}_p \operatorname{Wr} \mathfrak{P}_{p^{\alpha-1}} = \mathfrak{P}_p \operatorname{Wr} (\mathfrak{P}_p \operatorname{Wr} \mathfrak{P}_p \operatorname{Wr} \ldots \operatorname{Wr} \mathfrak{P}_p).$$

Порядок группы $\mathfrak{P}_{p^\alpha}$ *равен* p^ω, *где* $\omega = (p^\alpha - 1)(p - 1)^{-1}$.

§ 5. Нильпотентные и локально нильпотентные группы подстановок

1. Предварительные леммы. Группа G называется *N-группой*, или *группой с нормализаторным условием*, если любая ее истинная подгруппа отлична от своего нормализатора в G.

Лемма 1. *Пусть транзитивная подгруппа* Γ *группы* $S(X)$ *удовлетворяет нормализаторному условию. Если* $\operatorname{card} X > 1$ *и не является простым числом, то группа* Γ *импримитивна.*

Доказательство. Пусть $\operatorname{card} X > 1$ и Γ — примитивная группа. Рассмотрим стационарную подгруппу Γ_a группы Γ. Так как группа Γ является N-группой, то в ней есть подгруппа U, содержащая Γ_a в качестве нетривиального нормального делителя. Согласно критерию примитивности 3.2 $U = \Gamma$. Отсюда и из транзитивности группы Γ следует, в силу следствия 3.4.1, что $\Gamma_a = (e)$, т. е. Γ — регулярная группа. По следствию 3.2.1 $\operatorname{card} X$ — простое число. ∎

Лемма 2. *Пусть $\operatorname{card} X > 1$, а Γ — транзитивная N-подгруппа группы $S(X)$. Если $a \in X$, то в множестве X есть такая точка $b \neq a$, что $\Gamma_b = \Gamma_a$.*

Доказательство. Пусть U — нормализатор группы Γ_a в Γ. Для $h \in U \setminus \Gamma_a$ $h(a) = b \neq a$, $\Gamma_a = h\Gamma_a h^{-1} = \Gamma_b$. ∎

Следствие. *Дважды транзитивная подгруппа группы $S(X)$ не является N-группой.*

Лемма 3. *Если n — натуральное число, а Γ — транзитивная нильпотентная подгруппа группы S_n, то $\Pi(\Gamma) = \Pi(n)$* *).

Доказательство. Пусть сперва $n = p$ — простое число. Тогда группа Γ примитивна и, следовательно, ее центр $Z(\Gamma)$, по следствию 3.4.1, транзитивен. Так как абелева транзитивная подгруппа максимальна среди абелевых подгрупп в S_n, то $\Gamma = Z(\Gamma)$. Следовательно, Γ — циклическая группа порядка p. Для $n = p$ лемма доказана.

Воспользуемся теперь индукцией по числу $\tau(n)$ делителей числа n. Для $\tau(n) = 2$ лемма верна. Пусть $\tau(n) > 2$, и лемма верна для всех таких n_1, что $\tau(n_1) < \tau(n)$. Согласно лемме 1 группа Γ импримитивна. Разбиение множества X, где действует группа Γ, на ее системы импримитивности определяет гомоморфизм $\varphi\colon \Gamma \to S_m$, где m — число систем разбиения. $\overline{\Gamma} = \operatorname{Im} \varphi$ — нильпотентная транзитивная группа степени m, где $m \mid n$, $\tau(m) < \tau(n)$. По индуктивному предположению всякий простой делитель порядка группы $\overline{\Gamma}$ делит число m. Группа $K = \operatorname{Ker} \varphi$ содержится в прямом про-

*) Здесь $\Pi(n)$ — множество всех простых делителей числа n, а $\Pi(\Gamma)$ — множество всех простых чисел, входящих в порядки элементов (периодической) группы Γ. Такие обозначения будут употребляться и далее.

изведении m нильпотентных транзитивных групп степени nm^{-1}, следовательно, по индуктивному предположению, каждый простой делитель числа $\operatorname{card} \underline{K}$ делит число nm^{-1}. Так как $\operatorname{card} \Gamma = (\operatorname{card} K)(\operatorname{card} \overline{\Gamma})$, то каждый простой делитель числа $\operatorname{card} \Gamma$ делит число n. В силу транзитивности группы Γ число $\operatorname{card} \Gamma$ делится на n. ■

Следствие 1. *Транзитивная нильпотентная подгруппа группы S_{p^ν}, где p — простое число, является p-подгруппой.*

Следствие 2. *Максимальная транзитивная нильпотентная подгруппа группы S_{p^ν}, где p — простое число, является ее p-подгруппой Силова.*

2. Максимальные транзитивные нильпотентные подгруппы группы S_n. Здесь мы полностью изучим строение максимальных нильпотентных транзитивных подгрупп симметрической группы S_n; в частности, докажем их сопряженность в S_n.

Пусть

$$n = p_1^{\nu_1} \ldots p_k^{\nu_k} \tag{1}$$

— каноническое разложение числа n. При $k = 1$ $(n = p^\nu)$, согласно следствию 2 леммы 3, максимальная транзитивная нильпотентная подгруппа группы S_{p^ν} является ее p-подгруппой Силова. Следовательно, в силу теоремы Силова, *все максимальные транзитивные нильпотентные подгруппы группы S_{p^ν} сопряжены в ней.*

Пусть теперь $k > 1$, $q_j = p_j^{\nu_j}$, а X_j — множество, состоящее из q_j точек, $j = 1, \ldots, k$. Ниже мы построим одну нильпотентную транзитивную подгруппу N_n группы S_n и покажем, что любая транзитивная нильпотентная подгруппа группы S_n сопряжена в S_n с некоторой подгруппой группы N_n. Очевидно, что число точек декартова произведения $X_1 \times \ldots \times X_k = X$ равно n. Следовательно, можно считать, что $S_n = S(X)$. Пусть N_{q_j} — одна из p_j-подгрупп Силова группы $S(X_j)$, а g_j — произвольная подстановка из N_{q_j}, $j = 1, \ldots, k$. Пусть еще N_n — множество всех подстановок $g \in S(X)$ вида

$$g(x) = g(x_1, \ldots, x_k) = (g_1(x_1), \ldots, g_k(x_k)), \tag{2}$$

где $x = (x_1, \ldots, x_k) \in X$, $g_j \in N_{q_j}$, $j = 1, \ldots, k$.

Очевидно, что N_n является группой, изоморфной прямому произведению групп $N_{q_1}, \ldots, N_{q_k}$. Так как группы N_{q_j} транзитивны и нильпотентны, то и N_n — транзитивная нильпотентная группа, причем

$$\operatorname{card} N_n = p_1^{\omega_1} \ldots p_k^{\omega_k},$$

где $\omega_j = \left(p_j^{\nu_j} - 1\right)\left(p_j - 1\right)^{-1}$, $j = 1, \ldots, k$.

Пусть теперь N — любая транзитивная нильпотентная подгруппа в $S(X)$. Тогда, согласно лемме 3,

$$\operatorname{card} N = p_1^{\alpha_1} \ldots p_k^{\alpha_k}, \quad \alpha_j \geqslant \nu_j.$$

Следовательно, группа N — прямое произведение $N = H \times F$, где H — подгруппа порядка $p_1^{\alpha_1}$, а F — подгруппа порядка $p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

Лемма 4. *Множество X можно записать в виде декартова произведения $X = Y \times Z$ таких множеств Y и Z, что:*

(i) $\operatorname{card} Y = p_1^{\nu_1}$, $\operatorname{card} Z = np_1^{-\nu_1}$;

(ii) *для* $h \in H$, $f \in F$

$$h(y, z) = (\bar{h}(y), z), \qquad f(y, z) = (y, \bar{f}(z)),$$
$$\bar{h} \in S(Y), \qquad \bar{f} \in S(Z), \qquad (y, z) \in Y \times Z;$$

(iii) $h \mapsto \bar{h}$ *— точное транзитивное представление группы H, а $f \mapsto \bar{f}$ — точное транзитивное представление группы F.*

Доказательство. Так как $n \nmid \operatorname{card} F$, то F — интранзитивная группа. Пусть $X = X_1 \cup \ldots \cup X_s$ — разбиение множества X на орбиты группы F. Согласно лемме 4.3 представления r_i: $f \mapsto f_i = f \mid X_i$, $i = 1, \ldots, s$, попарно эквивалентны. Очевидно, что $\operatorname{Im} r_i$ — транзитивная нильпотентная подгруппа в $S(X_i)$. Следовательно, в силу леммы 3, $\Pi(\operatorname{card} X_i) = \Pi(\operatorname{card} F)$. Так как $N = H \times F$ — транзитивная группа, то группа H транзитивно перемещает орбиты $X_1, \ldots, X_s$ группы F. Следовательно, $s \mid \operatorname{card} H$. Отсюда находим

$$s = p_1^{\beta_1}, \qquad \operatorname{card} X_i = p_2^{\beta_2} \ldots p_k^{\beta_k}.$$

Так как $(\operatorname{card} X_i)s = n$, то

$$s = p_1^{\nu_1}, \qquad \operatorname{card} X_i = p_2^{\nu_2} \dots p_k^{\nu_k}.$$

Положим $t = \operatorname{card} X_i$ и обозначим точки орбиты X_1 парами чисел $(1, 1)$, $(1, 2)$, ..., $(1, t)$. Пусть теперь $h_1 = e$, h_2, ..., h_s — такие подстановки из группы H, что $h_y(X_1) = X_y$. Запишем точки орбиты X_y в виде $(y, 1)$, $(y, 2)$, ..., (y, t), положив $(y, z) = h_y(1, z)$, $z = 1, \dots, t$. Очевидно, $X = Y \times Z$, где $Y = \{1, \dots, s\}$, $Z = \{1, \dots, t\}$. Для $f \in F$ имеем

$$f(y, z) = fh_y(1, z) = h_y f(1, z) = h_y(1, \bar{f}(z)) = (y, \bar{f}(z)),$$

где $\bar{f} \in S(Z)$ и зависит только от f. Рассмотрим теперь $h(y, z)$, $h \in H$. Имеем $h(1, z) = (y_1, z_1)$, $1 \leqslant y_1 \leqslant s$. Если $z_1 \neq z$, то

$$h_{y_1}^{-1} h(1, z) = h_{y_1}^{-1}(y_1, z_1) = (1, z_1) \neq (1, z),$$

т. е.

$$h_{y_1}^{-1} h \,|\, X_1 = h_0$$

— отличная от e подстановка из группы $S(X_1)$. Положим теперь $F_0 = F | X_1$. Тогда h_0 перестановочна с каждой подстановкой из группы F_0. Следовательно, $(h_0)F_0$ — транзитивная нильпотентная подгруппа в $S(X_1)$. Согласно лемме 3 простые делители порядка элемента h_0 делят число t. Последнее невозможно. Следовательно, $z_1 = z$ и

$$h(1, z) = (y_1, z). \tag{3}$$

Рассмотрим теперь $h(y, z)$. С помощью равенства (3) получим

$$h(y, z) = hh_y(1, z) = (y', z) = (\bar{h}(y), z),$$

где $\bar{h} \in S(Y)$ и зависит только от h. ■

Из леммы 4 следует

Теорема 1. *Любая транзитивная нильпотентная подгруппа симметрической группы S_n сопряжена в S_n с некоторой подгруппой группы N_n, задаваемой формулами* (2).

Из этой теоремы, в свою очередь, вытекает

Теорема 2. *Любые две максимальные транзитивные нильпотентные подгруппы группы S_n сопряжены в S_n.*

Если (1) *— каноническое разложение числа n, то максимальная транзитивная нильпотентная подгруппа в S_n изоморфна прямому произведению p_j-подгрупп Силова симметрических групп $S_{p_j^{\nu_j}}$, $j=1, \ldots, k$.*

Докажем еще одну теорему о транзитивных нильпотентных подгруппах в S_n.

Теорема 3. *Пусть m — произведение всех различных простых делителей числа n, Γ — максимальная транзитивная нильпотентная подгруппа в $S_n = S(X)$, Γ_a — стационарная подгруппа группы Γ, а U — ее нормализатор в Γ. Тогда индекс подгруппы Γ_a в группе U равен m, или* (символически)

$$U:\Gamma_a = m.$$

Прежде чем доказывать эту теорему, заметим, что она равносильна следующему утверждению:

Если $Y = \{y \mid y \in X,\ \Gamma_a(y) = y\}$, то $\operatorname{card} Y = m$.

Теореме 3 можно еще придать такой вид:

Число различных стационарных подгрупп группы Γ равно nm^{-1}.

Доказательство теоремы 3. Для $n=1$ теорема тривиальна. Будем считать, что $n>1$ и положим $U:\Gamma_a = t$. Так как группа Γ является N-группой, то $t>1$. Очевидно, что $t \mid n$.

Докажем сперва, что при $n = p^\nu$, где p — простое число, $t = p$. Пусть $l = p^{\nu-1}$. Группа Γ является p-подгруппой Силова в S_{p^ν} и содержит, в частности, подстановки вида

$$d_1^{s_1} d_2^{s_2} \ldots d_l^{s_l},$$

где d_j — попарно независимые p-членные циклы, $0 \leqslant s_j \leqslant p$. Если $d_1(a) \neq a$, то подстановка $d_2 \ldots d_l \in \Gamma_a$ и оставляет на месте ровно p точек. Следовательно, $t \leqslant p$. Так как $t>1$ и $t \mid p^\nu$, то $t=p$.

Пусть теперь (1) — каноническое разложение числа n и $k>1$. Можно считать, что $\Gamma = N_n$, где N_n задается формулами (2). Рассмотрим стационарную подгруппу Γ_a

группы N_n, где $a=(a_1, \ldots, a_k) \in X = X_1 \times \ldots \times X_k$. Если $g \in \Gamma_a$, то компоненты g_j подстановки g таковы, что $g_j(a_j) = a_j$. Когда g пробегает группу Γ_a, то g_j независимо друг от друга пробегают стационарные подгруппы $\left(N_{q_j}\right)_{a_j}$ групп N_{q_j}. Согласно доказанному выше группа $\left(N_{q_j}\right)_{a_j}$ оставляет на месте точно p_j точек. Следовательно, группа Γ_a оставляет неподвижными точно $p_1 \ldots p_k = m$ точек. ■

3. **Интранзитивные максимальные нильпотентные подгруппы в S_n.** Пусть Γ — одна из интранзитивных максимальных нильпотентных подгрупп в $S_n = S(X)$, а $X = Y_1 U \ldots U Y_k$ — разбиение множества X на орбиты группы Γ. Тогда $\Gamma_j = \Gamma | Y_j$, $j=1, \ldots, k$, — транзитивная максимальная нильпотентная подгруппа в $S(Y_j)$, а Γ — прямое произведение своих ограничений Γ_j. Отсюда и из теоремы 2 следует, что *интранзитивная максимальная нильпотентная подгруппа группы S_n с точностью до сопряженности в S_n задается аддитивным представлением числа n:*

$$n = n_1 + \ldots + n_k, \tag{4}$$

где $k > 1$, $n_j = \operatorname{card} Y_j$, $j=1, \ldots, k$, Y_j — орбита группы Γ. Иными словами, *с точностью до сопряженности в S_n максимальная нильпотентная подгруппа группы S_n задается своим орбитальным типом.*

Однако не для каждого представления (4) в группе S_n есть интранзитивная максимальная нильпотентная подгруппа, орбиты которой имеют мощности

$$n_1, \ldots, n_k. \tag{5}$$

Пусть (4) — представление числа n, n_j — натуральные числа, а

$$X = Y_1 \cup \ldots \cup Y_k \tag{6}$$

— такое разбиение множества X, что $\operatorname{card} Y_j = n_j$, $j = 1, \ldots, k$. Построим такую группу $H = H(n_1, \ldots, n_k)$, что (6) — разбиение множества X на ее орбиты, $H_j = H | Y_j$ — транзитивная максимальная нильпотентная подгруппа в $S(Y_j)$, $j = 1, \ldots, k$, а группа H — прямое произведение своих ограничений на орбитах. Выясним, для каких разложений (4) подгруппа $H(n_1, \ldots, n_k)$ максимальна среди нильпотентных подгрупп в S_n.

Лемма 5. *Если числа* (5) *все различны, то группа* $H(n_1, \ldots, n_k)$ *максимальна среди нильпотентных подгрупп в* S_n.

Доказательство. Пусть числа (5) все различны, а группа $H = H(n_1, \ldots, n_k)$ содержится в другой нильпотентной подгруппе группы S_n. Тогда H — истинная инвариантная подгруппа некоторой нильпотентной группы U из S_n. Очевидно, что некоторая орбита Y группы U является объединением нескольких орбит группы H. Транзитивная группа $U|Y$ обладает интранзитивным нормальным делителем $H|Y$. Согласно теореме 3.4 орбиты группы $H|Y$ суть системы импримитивности группы $U|Y$. Следовательно, орбиты группы H, входящие в Y, имеют одну и ту же мощность, что противоречит условию леммы. ■

Лемма 6. *Пусть в* (4) $n_1 = n_2 = \ldots = n_k = m > 1$, $k > 1$. *Группа* $H = H(n_1, \ldots, n_k)$ *тогда и только тогда содержится в транзитивной нильпотентной подгруппе группы* S_n, *когда* $m = p^\alpha$, $k = p^\beta$, *где* p — *простое число.*

Доказательство. Пусть $H \subset G$, где G — транзитивная нильпотентная подгруппа в S_n. Можно считать, что G максимальна среди нильпотентных подгрупп в S_n. Положим $m = p^\alpha t$, $(t, p) = 1$, $\alpha > 0$, p — простое число. Найдем показатель u, с каким число p входит в $d = \operatorname{card} H$. Сперва рассмотрим порядок d_1 группы $H|Y_1$. Согласно теореме 2 число p входит в d_1 с показателем $\omega = (p^\alpha - 1)(p-1)^{-1}$. Следовательно, $u = k\omega = k(p^\alpha - 1)(p-1)^{-1}$. Если теперь $k = p^\beta r$, $(p, r) = 1$, то в порядок группы G число p входит с показателем $v = (p^{\alpha+\beta} - 1)(p-1)^{-1}$, ибо $n = km = p^{\alpha+\beta} rt$, $(p, rt) = 1$. Так как H — подгруппа в G, то $u \leqslant v$, следовательно,

$$u^{-1}v = \frac{p^{\alpha+\beta} - 1}{(p^\alpha - 1)p^\beta r} = f(r) \geqslant 1. \tag{7}$$

При фиксированных p, α и β $f(r)$ зависит только от r. Ясно, что $f(r)$ убывает с возрастанием r. С другой стороны, $f(2) < 1$. Отсюда и из (7) вытекает, что $r = 1$, т. е.

$$k = p^\beta. \tag{8}$$

Легко показать, что $m = p^\alpha$. Действительно, пусть простое число $q \neq p$ и $q \mid m$. Тогда, подобно равенству (8), получим $k = q^{\gamma}$. Последнее противоречит (8). Необходимость доказана.

Пусть теперь $m = p^{\alpha}$, $k = p^{\beta}$. Тогда $H = H(n_1, \ldots, n_k)$, где $n_1 = \ldots = n_k = p^{\alpha}$, является p-подгруппой группы $S_n = S_{p^{\alpha+\beta}}$. Следовательно, H содержится в p-подгруппе Силова $N_{p^{\alpha+\beta}}$ группы $S_{p^{\alpha+\beta}}$. Как мы видели раньше, $N_{p^{\alpha+\beta}}$ — транзитивная подгруппа группы $S_{p^{\alpha+\beta}}$. ■

Заметим еще, что если среди чисел (5) имеется по меньшей мере две единицы, то группа $H(n_1, \ldots, n_k)$ содержится в другой нильпотентной подгруппе группы S_n. Действительно, пусть $n_1 = n_2 = 1$. Тогда $H(n_1, n_2, \ldots, n_k)$ — истинная подгруппа в $H(2, n_3, \ldots, n_k)$.

Из лемм 5, 6 и последнего замечания вытекает

Теорема 4. *Всякая интранзитивная максимальная нильпотентная подгруппа группы S_n сопряжена в ней с группой вида $H(n_1, \ldots, n_k)$.*

Группа $H(n_1, \ldots, n_k)$ тогда и только тогда максимальна среди нильпотентных подгрупп в S_n, когда одновременно выполняются следующие два условия:

(i) *полином $(x - n_1)(x - n_2) \ldots (x - n_k) = \varphi(x)$ не делится на $(x - 1)^2$;*

(ii) *если p^{α}, где $\alpha > 0$, p — простое число, есть корень полинома $\varphi(x)$, то его кратность меньше p.*

Теорема 4 вместе с теоремами 1 и 2 полностью описывает максимальные нильпотентные подгруппы симметрической группы S_n.

4. О нильпотентных и локально нильпотентных группах подстановок бесконечной степени. Пусть X — бесконечное множество. Введем группу $SF(X)$, состоящую из всех таких $f \in S(X)$, что $f(x) \neq x$ только для конечного множества точек $x \in X$.

Легко видеть, что *$SF(X)$ — локально конечный нормальный делитель группы $S(X)$.*

Так как любая отличная от единицы подстановка из регулярной подгруппы группы $S(X)$ фактически перемещает все точки множества X, то пересечение любой регулярной подгруппы группы $S(X)$ с группой $SF(X)$ есть единичная группа. В частности, *в группе $SF(X)$ нет транзитивных абелевых подгрупп*. Следовательно, *орбиты ее абелевых подгрупп конечны.*

Лемма 7. *Центр транзитивной подгруппы группы $SF(X)$ совпадает с единичной подгруппой.*

Доказательство. Пусть H — транзитивная подгруппа в $SF(X)$, а Z — центр группы H. Все орбиты группы Z конечны. Следовательно, если

$$X = \bigcup X_\alpha, \quad \alpha \subset I, \tag{9}$$

— разбиение множества X на орбиты группы Z, то I — бесконечное множество. Пусть теперь $Z \neq (e)$, $c \in Z$, $c \neq e$. Тогда, согласно теореме 4.1, для любого $\alpha \in I$ $c|X_\alpha \neq e$. Отсюда вытекает, что подстановка c фактически перемещает бесконечное множество точек, т. е. не входит в группу $SF(X)$. ■

Из этой леммы вытекает

Теорема 5. *Орбиты нильпотентной подгруппы группы $SF(X)$ конечны.*

Доказательство. Пусть Γ — нильпотентная подгруппа в $SF(X)$, а X_α — какая-либо из ее орбит. Тогда $\Gamma_\alpha = \Gamma|X_\alpha$ — нильпотентная группа. Если $\operatorname{card} X_\alpha > 1$, то центр группы Γ_α отличен от (e). В силу леммы 7 множество X_α конечно. ■

Теорема 6. *Транзитивную подгруппу Γ группы $SF(X)$ нельзя представить в виде произведения двух неединичных поэлементно перестановочных нормальных делителей. В частности, Γ неразложима в прямое произведение.*

Доказательство. Пусть транзитивная подгруппа Γ группы $SF(X)$ представима в виде произведения $\Gamma = HF$ своих нетривиальных нормальных делителей H и F, причем $(H, F) = (e)$. Тогда возможны два случая: 1) группы H и F транзитивны, 2) хотя бы одна из них интранзитивна. Покажем, что оба случая приводят к противоречию. В силу теоремы 4.1 в первом случае H и F — регулярные группы, что противоречит включению $H \subset SF(X)$. Рассмотрим теперь второй случай. Пусть, например, группа H интранзитивна, а (9) — разбиение множества X на ее орбиты. Тогда, согласно лемме 4.3, представления r_α: $H \to S(X_\alpha), h \mapsto h|X_\alpha$, $\alpha \in I$, попарно эквивалентны. Отсюда и из включения $H \subset SF(X)$ вытекает конечность множества I. Следовательно, орбиты группы H бесконечны. С другой стороны, так как H — нормальный делитель в Γ, то, по теореме 3.4, (9) есть разбиение множества X на системы импримитивности группы Г. Очевидно, системы импримитивности транзитивной подгруппы в $SF(X)$ не могут быть бесконечны. ■

Из теоремы 6 вытекает

Теорема 7. *Локально нильпотентная транзитивная подгруппа группы $SF(X)$ является р-группой.*

Доказательство. Пусть Г — транзитивная локально нильпотентная подгруппа в $SF(X)$. Тогда Г, будучи периодической локально нильпотентной группой, есть прямое произведение своих подгрупп Силова. Но, по теореме 6, группа Г неразложима, значит, она есть p-группа. ■

Из теоремы 7 следует

Теорема 8. *Максимальная локально нильпотентная транзитивная подгруппа группы $SF(X)$ является ее р-подгруппой Силова.*

Строение p-подгрупп Силова группы $SF(X)$ изучил Иванюта [1], [2]. В частности, им показано, что *при* $\operatorname{card} X > \aleph_0$ *в группе $SF(X)$ нет транзитивных р-подгрупп, а при счетном множестве X транзитивные р-подгруппы Силова группы $SF(X)$ попарно сопряжены.* Отсюда и из теоремы 7 вытекает, что *орбиты локально нильпотентной подгруппы группы $SF(X)$ либо конечны, либо счетны.*

В связи с теоремой 6 сформулируем следующую проблему. *При каких условиях локально конечная группа изоморфна некоторой транзитивной подгруппе группы $SF(X)$? Какие локально конечные группы допускают изоморфное вложение в группы $SF(X)$?*

ГЛАВА II

ПОЛНАЯ ЛИНЕЙНАЯ ГРУППА

§ 6. Некоторые определения. Предварительные предложения

1. Мультипликативная группа кольца. Некоторые свойства тел. Всюду в этой главе термин *кольцо* будет означать ассоциативное кольцо с единицей, содержащее хотя бы два элемента.

Пусть Δ — кольцо, а 1 — единица в Δ. Элемент α из Δ называется *обратимым* в Δ, если в Δ существует такой элемент β, что $\alpha\beta = \beta\alpha = 1$. Очевидно, множество всех обратимых в Δ элементов есть группа относительно умножения. Эта группа называется *мультипликативной группой кольца* Δ и обозначается символом Δ^*. Если $\gamma \in \Delta \setminus \Delta^*$, то γ называется *необратимым* в Δ элементом.

Элемент η кольца Δ называется *унипотентным*, если $\eta - 1$ — нильпотентный элемент, т. е. $(\eta - 1)^k = 0$ для некоторого натурального k. Обозначим буквой U множество всех унипотентных элементов в Δ. *Унипотентный элемент* η *обратим* в Δ. В самом деле, $\eta = 1 + \theta$, $\theta^k = 0$,

$$(1+\theta)\left[1-\theta+\theta^2- \ldots +(-1)^{k-1}\theta^{k-1}\right]=1-\theta^k=1.$$

Элемент

$$\theta_1 = \sum_{\nu=1}^{k-1}(-1)^\nu\theta^\nu$$

нильпотентен, ибо

$$\theta_1^k = \theta^k\left[\sum_{\nu=1}^{k-1}(-1)^\nu\theta^{\nu-1}\right]^k = 0.$$

Следовательно $\eta^{-1} = 1 + \theta_1$ — также унипотентный элемент.

Очевидно, *произведение двух перестановочных унипотентных элементов также является унипотентным элементом*, так что *для коммутативного кольца* Δ *множество* U — *подгруппа в* Δ^*.

Пусть $\Delta = T$ — тело.

Предложение 1. *Периодическая абелева подгруппа* G *мультипликативной группы тела* T *локально циклическая. В частности, мультипликативная группа конечного поля* $GF(q)$ *есть циклическая группа порядка* $q-1$.

Доказательство. Будучи периодической абелевой группой, G локально конечна. Поэтому достаточно показать, что каждая конечная подгруппа H в G циклична. Порядки элементов абелевой конечной группы суть делители максимального среди них, следовательно, все элементы группы H — корни уравнения

$$x^d = 1, \tag{1}$$

где d — порядок некоторого элемента h группы H. Очевидно, что группа H содержится в некотором поле $\Sigma \subset T$. В поле Σ уравнение (1) имеет не больше чем d корней. С другой стороны, $1, h, h^2, \ldots, h^{d-1}$ — корни этого уравнения, принадлежащие группе H. Следовательно, $H = (h)$ — циклическая группа. ∎

Предложение 2. *Пусть тело* T *не является полем характеристики 2, или* T — *поле характеристики 2, не содержащее трансцендентных относительно своего простого подполя элементов. Пусть, далее,* S — *подгруппа аддитивной группы тела* T, *порожденная произведениями квадратов из* T. *Тогда* $S = T$.

Доказательство. S — множество всех элементов тела T вида

$$\sum \pm \alpha_1^2 \ldots \alpha_k^2, \qquad \alpha_i \in T.$$

Если характеристика тела отлична от 2, $\operatorname{char} T \neq 2$, то совпадение S и T следует из равенства

$$\alpha = \left(\frac{\alpha+1}{2}\right)^2 - \left(\frac{\alpha-1}{2}\right)^2, \qquad \alpha \in T.$$

Пусть теперь $\operatorname{char} T = 2$, T — некоммутативное тело, $Z(T)$ — его центр. Если $\alpha \in T \setminus Z(T)$, то найдется такой элемент $\beta \in T$, что $\gamma = \alpha\beta - \beta\alpha \neq 0$. Далее, элемент

$$\gamma = \alpha\beta + \beta\alpha \tag{2}$$

принадлежит S, ибо $\gamma = (\alpha + \beta)^2 - \alpha^2 - \beta^2$. Элемент $\gamma\alpha = \alpha(\beta\alpha) + (\beta\alpha)\alpha \in S$, так как он имеет вид (2). Очевидно, что множество S замкнуто относительно умножения, поэтому $\gamma^{-1} = \gamma(\gamma^{-1})^2 \in S$, $\alpha = \gamma^{-1}(\gamma\alpha) \in S$. Таким образом, $T \setminus Z(T) \subset S$.

Если $\delta \in Z(T)$, то $\delta\gamma = \alpha(\delta\beta) + (\delta\beta)\alpha \in S$, $\delta \in S$. Значит, $Z(T) \subset S$, $S = T$.

Остается рассмотреть тот случай, когда T — поле характеристики 2, все элементы которого алгебраические относительно содержащегося в нем простого подполя. Каждый отличный от нуля элемент ε поля T имеет нечетный порядок, так как он входит в мультипликативную группу некоторого конечного поля $GF(2^k)$. Поэтому $\varepsilon = (\varepsilon^\nu)^2 \in S$. ■

Как показывает простой пример поля $\Delta(x)$ рациональных дробей, где $\Delta = GF(2)$, предложение 2 может оказаться неверным, если T — поле характеристики 2, содержащее трансцендентные элементы.

2. Модуль. Пусть Δ — кольцо. Множество M называется *правым Δ-модулем*, если оно удовлетворяет следующим условиям:

1) M — аддитивная абелева группа;

2) для любых $\alpha \in \Delta$, $a \in M$ определен элемент $a\alpha \in M$, причем если $b \in M$, $\beta \in \Delta$, то

$$(a+b)\alpha = a\alpha + b\alpha, \qquad a(\alpha+\beta) = a\alpha + a\beta,$$
$$a(\alpha\beta) = (a\alpha)\beta, \qquad a \cdot 1 = a.$$

Аналогично определяется *левый Δ-модуль* M:

1) M — аддитивная абелева группа;

2) для $\alpha \in \Delta$, $a \in M$ определено произведение $\alpha a \in M$, причем если $b \in M$, $\beta \in \Delta$, то

$$\alpha(a+b) = \alpha a + \alpha b, \qquad (\alpha+\beta)a = \alpha a + \beta a,$$
$$(\alpha\beta)a = \alpha(\beta a), \qquad 1 \cdot a = a.$$

Подмножество $N \subset M$ называется *подмодулем* Δ-модуля M, если N — подгруппа аддитивной группы M и для любых $\alpha \in \Delta$, $c \in N$ $c\alpha \in N$.

Например, для любого $a \in M$ множество $a\Delta = \{a\alpha \mid \alpha \in \Delta\}$ есть подмодуль в M.

Подмодуль P Δ-модуля M называется *гиперплоскостью* модуля M, если модуль M представляется в виде прямой суммы: $M = P \dotplus v\Delta$, $v \in M$, $v \neq 0$. Система B элементов модуля M называется *линейно независимой над* Δ, если для любой ее конечной подсистемы $b_1, \ldots, b_k$

$$b_1\lambda_1 + \ldots + b_k\lambda_k = 0,\ \lambda_j \in \Delta \Rightarrow \lambda_1 = \ldots = \lambda_k = 0.$$

Элемент u Δ-модуля M называется *свободным над* Δ, если из равенства $u\lambda = 0$, где $\lambda \in \Delta$, следует $\lambda = 0$. Если Δ-модуль M обладает такой линейно независимой системой элементов B, что каждый элемент M есть линейная комбинация конечного множества элементов из B, то B называется *Δ-базисом* модуля M, а M — *свободным Δ-модулем*. Нулевой модуль также называется свободным.

Часто мы опускаем Δ и пишем просто «базис», «модуль» и т. д.

Символом Δ^n будем обозначать правый свободный Δ-модуль, состоящий из элементов вида $(\alpha_1, \ldots, \alpha_n)$, $\alpha_j \in \Delta$, причем

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n),$$
$$(\alpha_1, \ldots, \alpha_n)\gamma = (\alpha_1\gamma, \ldots, \alpha_n\gamma), \qquad \gamma \in \Delta.$$

Элементы $(1, 0, \ldots, 0)$, $(0, 1, \ldots, 0)$, $\ldots$, $(0, 0, \ldots, 1)$ составляют один из базисов этого модуля.

Символом Δ_L^n будем обозначать левый свободный Δ-модуль, отличающийся от Δ^n тем, что вместо $(\alpha_1, \ldots, \alpha_n)\gamma$ определено $\gamma(\alpha_1, \ldots, \alpha_n) = (\gamma\alpha_1, \ldots, \gamma\alpha_n)$.

В тех случаях, когда мощность Δ-базиса свободного модуля M над кольцом Δ не зависит от выбора базиса, эта мощность называется *размерностью* модуля M. Пусть Δ — область главных идеалов, а M — свободный Δ-модуль. Тогда любые два Δ-базиса модуля M имеют одну и ту же мощность, каждый подмодуль модуля M свободен и его размерность не больше размерности модуля M (Ленг [1], стр. 432).

Если, в частности, Δ — тело, то Δ-модуль называется *векторным пространством над* Δ. Всякое векторное пространство M над Δ является свободным модулем, мощность его базиса является инвариантом и называется *размерностью* векторного пространства (и обозначается $M:\Delta$). Справедлива теорема Штейница о линейной зависимости. Подмодули Δ-модуля M над телом Δ называются *подпространствами* векторного пространства M. Всякое подпространство векторного пространства M есть прямое слагаемое пространства M. Всякая линейно независимая система элементов содержится в некотором базисе пространства (см. Курош [2], гл. 5, § 3).

§ 7. Эндоморфизмы

1. End$M$. Пусть M — правый Δ-модуль. Отображение h: $M \to M$ называется *эндоморфизмом* модуля M, если для x, $y \in M$, $\alpha \in \Delta$

$$h(x+y)=h(x)+h(y), \qquad h(x\alpha)=h(x)\alpha. \tag{1}$$

Обозначим символом $\operatorname{End} M$ множество всех эндоморфизмов модуля M. Произведение gh двух эндоморфизмов g и h определим как произведение отображений. Сумму $g+h$ определим, положив для любого x из M

$$(g+h)(x)=g(x)+h(x). \tag{2}$$

Лемма 1. $\operatorname{End} M$ — *кольцо с единицей.*

Доказательство. Так как M — аддитивная абелева группа, то, в силу (1) и (2), $\operatorname{End} M$ — также аддитивная абелева группа. Ассоциативность умножения в $\operatorname{End} M$ следует из ассоциативности умножения отображений. Рассмотрим $f(g+h)$, f, g, $h \in \operatorname{End} M$. Для $x \in M$

$$f(g+h)(x)=f(g(x)+h(x))=fg(x)+fh(x)=(fg+fh)(x).$$

Следовательно, $f(g+h)=fg+fh$. Аналогично проверяется равенство $(g+h)f=gf+hf$.

Очевидно, что единицей кольца $\operatorname{End} M$ служит тождественное отображение. ■

Вместо $\operatorname{End} M$ иногда будем писать $\operatorname{Hom}(M, M)$.

Эндоморфизм левого Δ-модуля M определяется как отображение h: $M \to M$, при котором для x, $y \in M$, $\alpha \in \Delta$, $(x+y)h=xh+yh$, $(\alpha x)h=\alpha(xh)$. Умножение эндоморфизмов g и h задается формулой $x(gh)=(xg)h$.

Как легко проверить, справедлива

Лемма 2. *Пусть M — свободный Δ-модуль, B — его базис. Тогда любое отображение $f\colon B \to M$ однозначно продолжается до эндоморфизма модуля M.*

2. Полная линейная группа. Биективный эндоморфизм модуля M называется его *автоморфизмом*. Очевидно, *множество* $\operatorname{Aut} M$ *всех автоморфизмов модуля M есть группа относительно умножения. Это мультипликативная группа кольца* $\operatorname{End} M$.

Группа всех автоморфизмов свободного правого Δ-модуля M называется *полной линейной группой* и обозначается символом $GL(M)$.

Лемма 3. *Пусть M — свободный Δ-модуль, h — его эндоморфизм, B — базис модуля M. Эндоморфизм h тогда и только тогда является автоморфизмом, когда $h(B)$ — базис модуля M и*

$$B \to h(B), \qquad b \mapsto h(b), \qquad b \in B, \tag{3}$$

— биекция.

Доказательство. Если отображение (3) удовлетворяет условию леммы, то обратное ему отображение $h(b) \mapsto b$ однозначно, в силу леммы 2, продолжается до эндоморфизма g модуля M; $gh = hg = e$ — тождественный автоморфизм. Таким образом, $h \in \operatorname{Aut} M$.

Обратно, пусть h — автоморфизм модуля M. Тогда $h(M) = M$. Следовательно, каждый элемент модуля M есть линейная комбинация конечной системы элементов вида $d = h(b)$, $b \in B$. Любая конечная система $d_1 = h(b_1), \ldots, d_n = h(b_n)$, $b_i \in B$, линейно независима:

$$d_1\lambda_1 + \ldots + d_n\lambda_n = 0 \Rightarrow h(a) = 0,$$

где $\lambda_i \in \Delta$, $a = b_1\lambda_1 + \ldots + b_n\lambda_n$; но h — биекция, поэтому $a = 0$, $\lambda_i = 0$ для $i = 1, \ldots, n$. Следовательно, $h(B)$ — базис модуля. ■

Из предыдущих двух лемм вытекает, очевидно,

Лемма 4. *Для любой пары A и B равномощных базисов свободного модуля M существует автоморфизм этого модуля, переводящий A на B. Любая биекция $A \to B$ однозначно продолжается до автоморфизма модуля M.*

Отсюда следует, в частности, что если M — векторное пространство, то для любой пары a и b ненулевых векторов существует автоморфизм пространства M, переводящий a в b, т. е. *группа* $GL(M)$ *транзитивна на множестве* $M \setminus \{0\}$.

Пример. Пусть M — n-мерное пространство над конечным полем $GF(q)$. Тогда $GL(M)$ — конечная группа порядка

$$(q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}).$$

3. Гомотетии. Пусть M — правый Δ-модуль. Рассмотрим отображение

$$\rho_\alpha\colon M \to M, \quad x \mapsto x\alpha, \quad x \in M, \quad \alpha \in \Delta.$$

Очевидно, что ρ_α не всегда является эндоморфизмом модуля M. Однако $\rho_\alpha \in \operatorname{End} M$, если $\alpha \in Z(\Delta)$, где $Z(\Delta)$ — центр кольца Δ. Вообще верна

Лемма 5. *Если в модуле M есть свободный элемент, то*

$$\rho_\alpha \in \operatorname{End} M \tag{4}$$

тогда и только тогда, когда $\alpha \in Z(\Delta)$.

Доказательство. Пусть верно (4). Тогда для $v \in M$, $\lambda \in \Delta$ $\rho_\alpha(v\lambda) = \rho_\alpha(v)\lambda = v(\alpha\lambda)$. С другой стороны, $\rho_\alpha(v\lambda) = (v\lambda)\alpha = v(\lambda\alpha)$. Отсюда $v(\alpha\lambda - \lambda\alpha) = 0$. Если теперь v — свободный элемент, то $\alpha\lambda = \lambda\alpha$, $\alpha \in Z(\Delta)$. ■

Очевидно, *все автоморфизмы* ρ_α, где $\alpha \in Z(\Delta)^*$, *составляют группу* $H(M)$, *изоморфную группе* $Z(\Delta)^*$. Будем называть $H(M)$ *группой гомотетий модуля* M, а ее элементы — *гомотетиями*.

Подмодуль N модуля M называется *инвариантным относительно эндоморфизма* f, если $f(N) \subset N$.

Лемма 6. *Пусть Δ — кольцо без делителей нуля, M — правый свободный Δ-модуль, содержащий хотя бы два линейно независимых элемента, σ — автоморфизм модуля M. Если каждый подмодуль модуля M вида $w\Delta$ инвариантен относительно автоморфизма σ, то $\sigma \in H(M)$.*

Доказательство. Для любых u и v из M

$$\sigma(u) = u\alpha, \quad \sigma(v) = v\beta, \quad \sigma(u+v) = (u+v)\gamma, \quad \alpha, \beta, \gamma \in \Delta.$$

С другой стороны,

$$\sigma(u+v) = \sigma(u) + \sigma(v) = u\alpha + v\beta.$$

Следовательно,

$$u\gamma + v\gamma = u\alpha + v\beta.$$

Если теперь u и v линейно независимы, то отсюда следует $\alpha = \gamma = \beta$.

Так как кольцо Δ без делителей нуля, то из линейной независимости u и v следует линейная независимость w и v, где $w = u\lambda$, $\lambda \neq 0$, $\lambda \in \Delta$. Поэтому

$$\sigma(w) = w\alpha = u\lambda\alpha.$$

С другой стороны,

$$\sigma(w) = \sigma(u\lambda) = u\alpha\lambda.$$

Следовательно,

$$u(\lambda\alpha - \alpha\lambda) = 0, \qquad \lambda\alpha - \alpha\lambda = 0, \qquad \alpha \in Z(\Delta),$$

где $Z(\Delta)$ — центр кольца Δ.

В частности, если B — базис модуля M, то для всех $b \in B$, $\sigma(b) = b\alpha$, $\alpha \in Z(\Delta)$. Тогда для любого $a \in M$ $\sigma(a) = a\alpha$, $\sigma \in H(M)$. ■

4. Трансвекции. Эндоморфизм τ Δ-модуля M называется *трансвекцией*, если в M есть такая гиперплоскость P, каждый элемент которой неподвижен при τ, что $\tau(a) - a \in P$ для любого $a \in M$.

Множество всех трансвекций, связанных с фиксированной гиперплоскостью P, обозначим символом $K(P)$.

Согласно определению гиперплоскости модуль M можно представить в виде прямой суммы

$$M = P \dotplus v\Delta, \qquad v \in M, \qquad v \neq 0. \tag{5}$$

Очевидно, что *эндоморфизм τ модуля M тогда и только тогда принадлежит $K(P)$, когда выполняются следующие два условия*:

(i) *для любого $a \in P$ $\tau(a) = a$;*

(ii) $\tau(v) = v + p$, $p \in P$.

Теорема 1. *Для произвольной гиперплоскости P Δ-модуля M множество $K(P)$ — группа, изоморфная аддитивной группе модуля P.*

Доказательство. В силу (ii) при фиксированном разложении (5) автоморфизм $\tau \in K(P)$ задается элементом p из P. Положим $\tau = \tau_p$. Для $a \in P$, p, $q \in P$

$$\tau_p\tau_q(a) = a, \qquad \tau_p\tau_q(v) = \tau_p(v + q) = v + p + q.$$

Следовательно,

$$\tau_p\tau_q = \tau_{p+q}.$$

Очевидно, что отображение

$$\gamma\colon\ K(P)\to P, \qquad \tau_p \longmapsto p,$$

биективно. Так как

$$\gamma(\tau_p\tau_q) = \gamma(\tau_p) + \gamma(\tau_q),$$

то γ — изоморфизм. ∎

Заметим, что *трансвекция — унипотентный элемент кольца* End M. В самом деле,

$$(\tau_p - e)(v) = v + p - v = p,$$

далее,

$$(\tau_p - e)^2(v) = (\tau_p - e)(p) = p - p = 0,$$

откуда

$$(\tau_p - e)^2 = 0.$$

Теорема 2. *Пусть правый Δ-модуль M допускает представление* (5), *где v — свободный элемент и P содержит свободный элемент. Тогда*:

(i) *централизатор подгруппы $K(P)$ в* $\mathrm{Aut}\, M$ *равен произведению $K(P)H(M)$*;

(ii) *$K(P)H(M)$ — максимальная абелева подгруппа группы* $\mathrm{Aut}\, M$;

(iii) *множество U всех унипотентных элементов группы $K(P)H(M)$ есть группа, равная произведению $K(P)H_u$, где H_u — группа всех унипотентных гомотетий. Если, в частности, в центре кольца Δ нет неединичных унипотентных элементов, то $U = K(P)$.*

Доказательство. Пусть автоморфизм σ перестановочен с каждой трансвекцией из $K(P)$, $\tau_p \in K(P)$. Так как

$$\sigma(v) = a + v\lambda, \qquad a \in P, \qquad \lambda \in \Delta,$$

то из

$$\tau_p(a + v\lambda) = \sigma(v + p)$$

получим

$$a + (v + p)\lambda = a + v\lambda + \sigma(p),$$

т. е.

$$\sigma(p) = p\lambda$$

для любого $p \in P$. Далее, для $\delta \in \Delta$

$$\sigma(p\delta) = (p\delta)\lambda = \sigma(p)\delta = p\lambda\delta.$$

Если p — свободный элемент, то отсюда следует $\delta\lambda = \lambda\delta$, т. е. λ принадлежит центру $Z(\Delta)$ кольца Δ. Итак,

$$\sigma(p) = p\lambda, \quad p \in P, \quad \sigma(v) = a + v\lambda, \quad a \in P, \quad \lambda \in Z(\Delta). \tag{6}$$

Автоморфизм σ^{-1} также перестановочен с каждой трансвекцией из $K(P)$, поэтому, согласно (6),

$$\sigma^{-1}(p) = p\mu, \quad \sigma^{-1}(v) = v\mu + b, \quad \mu \in Z(\Delta), \quad b \in P.$$

Далее,

$$v = e(v) = \sigma^{-1}\sigma(v) = \sigma^{-1}(a + v\lambda) = a\mu + v\mu\lambda + b\lambda,$$

откуда

$$v(1 - \mu\lambda) - (a\mu + b\lambda) = 0. \tag{7}$$

Так как (5) — прямая сумма, то из (7) следует $v(1 - \mu\lambda) = 0$. Но v — свободный элемент, значит, $1 = \mu\lambda$, $\lambda \in Z(\Delta)^*$.

Рассмотрим теперь произведение $\tau^{-1}\sigma$, где $\tau = \tau_{a\lambda^{-1}}$. Для $p \in P$

$$\tau^{-1}\sigma(p) = \tau^{-1}(p\lambda) = p\lambda.$$

Так как $\tau^{-1} = \tau_{-a\lambda^{-1}}$, то

$$\tau^{-1}\sigma(v) = \tau^{-1}(a + v\lambda) = a + (v - a\lambda^{-1})\lambda = v\lambda.$$

Далее,

$$\tau^{-1}\sigma(v\delta) = (v\lambda)\delta = (v\delta)\lambda, \qquad \delta \in \Delta.$$

Поэтому

$$\tau^{-1}\sigma(x) = x\lambda$$

для любого элемента x модуля M, т. е. $\tau^{-1}\sigma \in H(M)$. Отсюда $\sigma \in K(P)H(M)$.

С другой стороны, каждый элемент группы $K(P)H(M)$ перестановочен, очевидно, с каждой трансвекцией из $K(P)$. Таким образом, (i) доказано.

Очевидно, что $K(P)H(M)$ — абелева группа. Отсюда и из (i) вытекает (ii).

Пусть теперь $\sigma \in K(P)H(M)$. Тогда для $p \in P$

$$\sigma(p) = p\lambda, \quad \sigma(v) = v\lambda + a_1, \quad a_1 \in P, \quad \lambda \in Z(\Delta)^*.$$

Далее, $(\sigma - e)(v) = v(\lambda - 1) + a_1$,

$$(\sigma - e)^k(v) = v(\lambda - 1)^k + a_k, \quad a_k \in P. \tag{8}$$

Если σ — унипотентный элемент, то $(\sigma - e)^k = 0$ для некоторого k. Из (8) тогда следует $v(\lambda - 1)^k = 0$ и, так как v — свободный элемент, $(\lambda - 1)^k = 0$, т. е. λ — унипотентный элемент. С другой стороны, произведение трансвекции τ и унипотентной гомотетии ρ является также унипотентным элементом, ибо τ и ρ перестановочны. ∎

Теорема 2 верна, в частности, для свободного модуля, один из базисов которого содержит не менее двух элементов.

Следствие 1. *Если Δ — кольцо без делителей нуля, а Δ-модуль M допускает два таких представления $M = P \dotplus v\Delta$, $M = Q \dotplus w\Delta$, что v и w — свободные элементы, гиперплоскости P и Q содержат хотя бы по одному свободному элементу и $P + Q = M$, то централизатор C объединения $K(P) \cup K(Q)$ в $\operatorname{Aut} M$ есть $H(M)$.*

Доказательство. $C = K(P)\,H(M) \cap K(Q)\,H(M)$. Если $\sigma \in C$, то $\sigma = \tau_p\rho$, $\rho \in H(M)$, $p \in P$. Но $H(M) \subset C$, поэтому $\tau_p \in C$ и, значит,

$$\tau_p = \bar\tau_q\rho_\alpha, \qquad q \in Q, \qquad \bar\tau_q \in K(Q), \qquad \rho_\alpha \in H(M).$$

Так как $P + Q = M$, то в гиперплоскости P есть такой элемент a, что $a = b + w\delta$, $b \in Q$, $\delta \in \Delta$, $\delta \neq 0$. Далее,

$$a = \tau_p(a) = \bar\tau_q\rho_\alpha(a) = \rho_\alpha\bar\tau_q(b + w\delta) = (b + (w + q)\delta)\,\alpha.$$

Следовательно, $b + w\delta = (b + (w + q)\delta)\,\alpha$, $b - b\alpha - q\delta\alpha = w\delta(\alpha - 1)$. Отсюда вытекает, $w\delta(\alpha - 1) = 0$ и, так как w — свободный элемент, $\alpha = 1$. Следовательно,

$$\tau_p = \bar\tau_q = e, \qquad \sigma = \rho, \qquad C = H(M). \ ∎$$

Следствие 2. *Пусть Δ — произвольное кольцо, M — свободный Δ-модуль с базисом $B = \{a, b, \ldots\}$, содержащим не менее двух элементов, P и Q — гиперплоскости, порожденные, соответственно, множествами $B \setminus a$ и $B \setminus b$. Тогда централизатор C объединения $K(P) \cup K(Q)$ совпадает с группой $H(M)$.*

Доказательство. $M = P \dotplus a\Delta$, $P \ni b$ и $M = Q \dotplus b\Delta$. Поэтому, согласно теореме 2, $C = K(P)H(M) \cap K(Q)H(M)$. Пусть $\sigma \in C$. Тогда $\sigma = \tau_p\rho$, $p \in P$, $\rho \in H(M)$. Так как $H(M) \subset C$, то $\tau_p \in C$. Отсюда

$$\tau_p = \rho_\alpha\bar\tau_q, \qquad \rho_\alpha \in H(M), \qquad q \in Q, \qquad \bar\tau_q \in K(Q).$$

Далее, $a = \tau_p(a) = \rho_\alpha \bar{\tau}_q(a) = a\alpha$. Так как a — свободный элемент, то

$$\alpha = 1, \quad \tau_p = \bar{\tau}_q.$$

Значит, трансвекция τ оставляет неподвижными все точки модулей P и Q. Но $P + Q = M$, следовательно, $\tau_p = e$, $\sigma = \rho \in H(M)$, $C = H(M)$. ∎

Пусть либо $Z(\Delta^*) = Z(\Delta)^*$, либо в M есть такой базис B, что $\operatorname{card} B > 1$. Тогда верно

Следствие 3. *Центр полной линейной группы $GL(M)$ совпадает с группой $H(M)$.*

Доказательство. Если $M = u\Delta$, где u — свободный элемент, то отображение $\gamma \longmapsto \sigma_\gamma$, где $\sigma_\gamma(u) = u\gamma$, есть изоморфизм группы Δ^* на $GL(M)$. Следовательно, $H(M)$ — центр группы $GL(M)$. Если же какой-либо базис модуля M содержит более одного элемента, то требуемое утверждение вытекает из следствия 2. ∎

Пусть теперь $\Delta = T$ — тело, а M — векторное пространство над T размерности > 1. Тогда верна

Лемма 7. *Любые две отличные от e трансвекции пространства M сопряжены в группе $GL(M)$.*

Доказательство. Пусть

$$M = P \dotplus vT = Q \dotplus wT, \quad \tau_p \in K(P), \quad \bar{\tau}_q \in K(Q),$$
$$\tau_p, \ \bar{\tau}_q \neq e.$$

Модуль M имеет такие базисы $\{A, v\}$ и $\{B, w\}$, что A — базис подпространства P, B — базис Q, причем $p \in A$, $q \in B$. В силу леммы 4 в группе $GL(M)$ есть такой автоморфизм σ, что $\sigma(A) = B$, $\sigma(p) = q$, $\sigma(v) = w$. Легко видеть, что

$$\sigma\tau_p\sigma^{-1} = \bar{\tau}_q.$$

В самом деле,

$$\sigma\tau_p\sigma^{-1}(b) = \sigma\tau_p(a) = \sigma(a) = b, \quad a = \sigma^{-1}(b), \quad b \in B$$

и

$$\sigma\tau_p\sigma^{-1}(w) = \sigma\tau_p(v) = \sigma(v + p) = w + q. \ ∎$$

§ 8. Матричное представление эндоморфизма

1. Матрица эндоморфизма. Пусть M — правый свободный Δ-модуль, обладающий конечным базисом

$$u_1, \ldots, u_n. \tag{1}$$

Если σ — эндоморфизм модуля M, то

$$\sigma(u_\nu) = \sum_{\mu=1}^{n} u_\mu \alpha_{\mu\nu}, \quad \alpha_{\mu\nu} \in \Delta, \quad \nu = 1, \ldots, n. \tag{2}$$

Положим $a = \|\alpha_{\mu\nu}\|$. Матрицу a назовем *матрицей эндоморфизма* σ *в базисе* (1).

Обозначим символом Δ_n множество всех $n \times n$-матриц над кольцом Δ и введем отображение

$$\varphi\colon \operatorname{End} M \to \Delta_n, \qquad \sigma \mapsto a. \tag{3}$$

В силу леммы 7.2 φ — биекция.

Теорема 1. *Отображение* φ — *изоморфизм колец* $\operatorname{End} M$ *и* Δ_n.

Доказательство. Пусть $\sigma, \tau \in \operatorname{End} M$,

$$\varphi(\sigma) = a = \|\alpha_{\mu\nu}\|, \qquad \varphi(\tau) = b = \|\beta_{\mu\nu}\|.$$

Из (3) следует, что

$$\varphi(\sigma + \tau) = a + b = \varphi(\sigma) + \varphi(\tau).$$

Для $\sigma\tau$ можно написать

$$\sigma\tau(u_\nu) = \sigma\left(\sum_{\mu=1}^{n} u_\mu \beta_{\mu\nu}\right) =$$
$$= \sum_{\mu=1}^{n} \sigma(u_\mu)\beta_{\mu\nu} = \sum_{\mu=1}^{n} \left(\sum_{k=1}^{n} u_k \alpha_{k\mu}\right)\beta_{\mu\nu} =$$
$$= \sum_{k=1}^{n} u_k \left(\sum_{\mu=1}^{n} \alpha_{k\mu}\beta_{\mu\nu}\right) = \sum_{k=1}^{n} u_k \gamma_{k\nu},$$

где $\|\gamma_{k\nu}\| = ab$. Следовательно,

$$\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau). \ \blacksquare$$

Мультипликативную группу кольца Δ_n обозначим $GL(n, \Delta)$. Так как мультипликативные группы изоморфных колец изоморфны, то из теоремы 1 вытекает

Следствие 1. $GL(M) \cong GL(n, \Delta)$.

Группу $GL(n, \Delta)$ будем называть *полной линейной группой* степени n над кольцом Δ. В дальнейшем изложении мы не будем делать большого различия между группами $GL(M)$ и $GL(n, \Delta)$.

Лемма 1а. *Матрица из* Δ_n *тогда и только тогда обратима в* Δ_n, *когда ее столбцы составляют некоторый базис правого свободного модуля* Δ^n.

Доказательство. Пусть $a = \varphi(\sigma)$ (см. 3)). Матрица a обратима в Δ_n тогда и только тогда, когда σ — автоморфизм, т. е. когда

$$\sigma(u_1), \ldots, \sigma(u_n) \tag{4}$$

— базис модуля M. Если

$$a_1, \ldots, a_n \tag{5}$$

— столбцы матрицы a, то, в силу (2), равенства

$$\sigma(u_1)\gamma_1 + \ldots + \sigma(u_n)\gamma_n = \\ = u_1\lambda_1 + u_2\lambda_2 + \ldots + u_n\lambda_n, \qquad \gamma_i, \lambda_k \in \Delta$$

и

$$a_1\gamma_1 + \ldots + a_n\gamma_n = \begin{bmatrix} \lambda_1 \\ \cdot \\ \cdot \\ \cdot \\ \lambda_n \end{bmatrix}$$

равносильны. Поэтому (4) — базис модуля M тогда и только тогда, когда (5) — базис модуля Δ^n. ■

С помощью аналогичных рассуждений, проведенных для левых модулей, доказывается

Лемма 1б. *Матрица a из Δ_n тогда и только тогда обратима в Δ_n, когда ее строки составляют базис левого Δ-модуля Δ^n_L.*

Теорема 2. *Если a — матрица эндоморфизма σ в базисе* (1), *а b — матрица автоморфизма τ в том же базисе, то $b^{-1}ab$ — матрица эндоморфизма σ в базисе*

$$\tau(u_1), \ldots, \tau(u_n). \tag{6}$$

Доказательство. Положим $\sigma_1 = \tau^{-1}\sigma\tau$. Согласно теореме 1 $b^{-1}ab$ — матрица эндоморфизма σ_1 в базисе (1). С другой стороны, матрица эндоморфизма σ в базисе (6) совпадает с матрицей эндоморфизма σ_1 в базисе (1). Действительно, $\sigma = \tau\sigma_1\tau^{-1}$, и если

$$\sigma_1(u_\nu) = \sum_{\mu=1}^{n} u_\mu\lambda_{\mu\nu},$$

то

$$\tau\sigma_1\tau^{-1}(\tau(u_\nu)) = \tau\sigma_1(u_\nu) = \tau\left(\sum_{\mu=1}^{n} u_\mu\lambda_{\mu\nu}\right) = \sum_{\mu=1}^{n} \tau(u_\mu)\lambda_{\mu\nu}.$$

Отсюда и вытекает теорема. ■

2. Теорема Бернсайда.

Теорема 3 (Бернсайд [3]). *Пусть Δ — область главных идеалов, Σ — поле отношений кольца Δ, а G — подгруппа группы $GL(n, \Sigma)$, обладающая следующим свойством: в кольце Δ найдется такой отличный от нуля элемент δ, что для каждого $g \in G$ $g\delta \in \Delta_n$. Тогда в группе $GL(n, \Sigma)$ есть такая матрица t, что*

$$t^{-1}Gt \subseteq GL(n, \Delta).$$

Доказательство. Отметим в пространстве Σ^n какой-нибудь базис

$$u_1, \ldots, u_n \tag{7}$$

и не будем отличать матрицы $g \in G$ от автоморфизмов пространства Σ^n, определяемых ими в базисе (7). Для $g \in G$

$$g(u_j) = \sum_{i=1}^{n} u_i\gamma_{ij}, \quad \gamma_{ij} \in \Sigma, \quad \gamma_{ij}\delta \in \Delta, \quad j = 1, \ldots, n. \tag{8}$$

Введем правый свободный Δ-модуль M с базисом (7). Пространство Σ^n также можно рассматривать как Δ-модуль. С помощью формул (8) каждый элемент g группы G определяет гомоморфизм Δ-модулей:

$$g\colon M \to \Sigma^n. \tag{9}$$

Пусть теперь N — подмножество всех таких $v \in M$, что для любого $g \in G$ $g(v) \in M$. Очевидно, что N есть подмодуль модуля M. В Δ-модуле N есть n линейно независимых элементов

$$u_1\delta, \ldots, u_n\delta.$$

Так как Δ — область главных идеалов, то N — свободный Δ-модуль размерности n. Наконец, подмодуль N инвариантен относительно группы G, ибо для $v \in N$, $h, g \in G$ имеем

$$g(v) \in M, \qquad hg(v) \in M,$$

т. е.

$$g(v) \in N.$$

Если
$$v_1, \ldots, v_n \tag{10}$$
— Δ-базис модуля N, то элементы (10) линейно независимы над Σ. В самом деле, всякий элемент $\sigma \in \Sigma$ имеет вид $\delta\nu^{-1}$, где $\delta, \nu \in \Delta$. Если
$$v_1\delta_1\nu_1^{-1} + \ldots + v_n\delta_n\nu_n^{-1} = 0 \tag{11}$$
и $\delta_n \neq 0$, то, умножая (11) на $\nu_1\nu_2 \ldots \nu_n$, получим
$$v_1x_1 + \ldots + v_nx_n = 0, \quad x_i \in \Delta, \quad x_n \neq 0. \tag{12}$$
Последнее невозможно. Итак, (10) — базис пространства Σ^n. Так как
$$g(v_j) = \sum_{i=1}^{n} v_i\alpha_{ij}, \quad \alpha_{ij} \in \Delta, \quad j = 1, \ldots, n,$$
то теорема вытекает теперь из теоремы 2. ■

Следствие 1. *Если Δ — область главных идеалов, Σ — поле отношений кольца Δ, а G — конечная подгруппа группы $GL(n, \Sigma)$, то в $GL(n, \Sigma)$ есть такая матрица t, что $t^{-1}Gt \subset GL(n, \Delta)$.*

3. Элементарные матрицы $t_{ij}(\lambda)$. Специальная линейная группа. Пусть правый свободный Δ-модуль M обладает базисом
$$u_1, \ldots, u_n, \quad n > 1. \tag{13}$$
Рассмотрим трансвекцию
$$\tau = \tau_{ij}(\lambda), \quad i \neq j,$$
задаваемую равенствами
$$\tau(u_\alpha) = u_\alpha, \qquad \alpha \neq j,$$
$$\tau(u_j) = u_j + u_i\lambda, \quad \lambda \in \Delta.$$
Очевидно, матрицей трансвекции τ в базисе (13) служит
$$t_{ij}(\lambda) = E + e_{ij}\lambda, \tag{14}$$
где E — единичная матрица, а $e_{ij} = \|a_{\mu\nu}\|$, $a_{ij} = 1$, $a_{\mu\nu} = 0$, если $\mu \neq i$ или $\nu \neq j$. Матрицы (14) будем называть *элементарными*.

В частности, $E = t_{ij}(0)$.

Подгруппа $SL(n, \Delta)$ группы $GL(n, \Delta)$, порожденная всеми элементарными матрицами $t_{ij}(\lambda)$, называется *специальной линейной группой.* Можно трактовать специальную линейную группу и как подгруппу $SL(M)$ в $GL(M)$, порожденную всеми трансвекциями $\tau_{ij}(\lambda)$.

Если P_j — подмодуль модуля M с базисом

$$u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n$$

(см. (13)), то

$$M = P_j \dotplus u_j\Delta$$

и для $p_j \in P_j$

$$p_j = \sum_{i \neq j} u_i\lambda_i, \qquad \lambda_i \in \Delta.$$

Следовательно, для любой трансвекции τ_{p_j} из $K(P_j)$

$$\tau_{p_j} = \prod_{i \neq j} \tau_{ij}(\lambda_i).$$

Отсюда и из следствия 7.2.1 вытекает

Лемма 2. *Централизатор множества всех трансвекций вида $\tau_{ij}(\lambda)$ в группе $GL(M)$ совпадает с группой $H(M)$.*

Из этой леммы следует

Теорема 4. *Если $n > 1$, то централизатор группы $SL(n, \Delta)$ в группе $GL(n, \Delta)$ совпадает с $Z(\Delta)^*E_n$, где $Z(\Delta)$ — центр кольца Δ.*

Лемма 3 (Басс [1]). *Если $n > 2$, а i, j, k — три различных индекса, не превосходящих n, то*

$$t_{ij}(\lambda\mu) = t_{ik}(\lambda)\, t_{kj}(\mu)\, t_{ik}^{-1}(\lambda)\, t_{kj}^{-1}(\mu).$$

В частности,

$$t_{ij}(\lambda) = t_{ik}(\lambda)\, t_{kj}(1)\, t_{ik}^{-1}(\lambda)\, t_{kj}^{-1}(1).$$

Действительно, если $i \neq j$, то

$$t_{ij}(\lambda)\, t_{ij}(\mu) = t_{ij}(\lambda + \mu), \qquad t_{ij}^{-1}(\lambda) = t_{ij}(-\lambda).$$

Далее,

$$\begin{aligned} t_{ik}(\lambda)\, t_{kj}(\mu) &= E + e_{ik}\lambda + e_{kj}\mu + e_{ij}\lambda\mu, \\ t_{ik}(-\lambda)\, t_{kj}(-\mu) &= E - e_{ik}\lambda - e_{kj}\mu + e_{ij}\lambda\mu. \end{aligned} \tag{15}$$

Для доказательства леммы остается перемножить равенства (15). ■

Из леммы 3 вытекает, очевидно,

Теорема 5. *Если $n > 2$, то $SL(n, \Delta)$ совпадает со своим коммутантом и содержится, следовательно, в коммутанте группы $GL(n, \Delta)$.*

Обратимся теперь к случаю $n = 2$.

Лемма 4. *Если в Δ^* есть такой элемент α, что $\alpha - 1 \in \Delta^*$, то любая элементарная матрица из $GL(2, \Delta)$ является коммутатором в $GL(2, \Delta)$.*

Доказательство. Если

$$a = \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}, \quad b = \begin{bmatrix} 1 & \mu \\ 0 & 1 \end{bmatrix}, \quad \mu = (\alpha - 1)^{-1} \lambda,$$

то

$$t_{12}(\lambda) = aba^{-1}b^{-1}.$$

Пусть теперь

$$c = t_{21}(\gamma), \qquad \gamma = -\lambda(\alpha - 1)^{-1}, \qquad d = a^{-1},$$

тогда

$$t_{21}(\lambda) = c\,dc^{-1}d^{-1}. \ \blacksquare$$

Следствие 1. *Если $\Delta = T$ — тело, отличное от $GF(2)$, то любая элементарная матрица из группы $GL(2, T)$ является в этой группе коммутатором.*

Напротив, если $T = GF(2)$, то отличная от единичной элементарная матрица из $GL(2, T)$ не есть коммутатор.

Следствие 2. *Если в Δ^* есть такой элемент α, что $\alpha - 1 \in \Delta^*$, то группа $SL(2, \Delta)$ содержится в коммутанте группы $GL(2, \Delta)$.*

Лемма 5. *Если (13) — базис модуля M, то для любой пары α, β, $1 \leqslant \alpha \leqslant n, 1 \leqslant \beta \leqslant n$, $\alpha \neq \beta$, в группе $SL(M)$ есть такой элемент $s_{\alpha\beta}$, что*

$$s_{\alpha\beta}(u_\alpha) = u_\beta, \quad s_{\alpha\beta}(u_\beta) = -u_\alpha, \quad s_{\alpha\beta}(u_i) = u_i, \qquad i \neq \alpha, \beta.$$

Доказательство. Положим

$$s_{\alpha\beta} = \tau_{\beta\alpha}(1)\,\tau_{\alpha\beta}(-1)\,\tau_{\beta\alpha}(1).$$

Очевидно, что такой элемент обладает требуемыми свойствами. $\blacksquare$

Заметим, что если $a \in GL(n, \Delta)$, то $s_{\alpha\beta}^{-1} a s_{\alpha\beta}$ получается из a перестановкой ее α-й и β-й строк с последующим умножением β-й строки на -1.

Пусть t — подстановка, действующая на множестве $\{u_1, \ldots, u_n\}$ базисных элементов модуля M. Подстановка t однозначно продолжается до автоморфизма f модуля M. Можно вложить симметрическую группу S_n в $GL(n, \Delta)$, если отождествить t с матрицей автоморфизма f в базисе (13). В частности, цикл длины 3 $(u_\alpha, u_\beta, u_\gamma)$ можно представить в виде

$$(u_\alpha, u_\beta, u_\gamma) = s_{\alpha\beta}^3 s_{\alpha\gamma} \in SL(n, \Delta).$$

Поэтому из леммы 5 вытекает

Следствие 1. *Всякая четная подстановка содержится в группе $SL(n, \Delta)$. Если t — нечетная подстановка, то* $t = f_\alpha s$; $f_\alpha(u_\alpha) = -u_\alpha$, $f_\alpha(u_i) = u_i$, $i \neq \alpha$, $s \in SL(n, \Delta)$.

4. Формальные леммы. Пусть Δ^n — правый свободный Δ-модуль столбцов. Если $x \in \Delta^n$, $c \in \Delta_n$, то $cx \in \Delta^n$. Как легко проверить, отображение

$$h\colon \Delta^n \to \Delta^n, \qquad x \mapsto cx,$$

является эндоморфизмом модуля Δ^n. Пусть $c = \|\gamma_{ij}\|$. Векторы

$$b_1 = \begin{bmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad b_2 = \begin{bmatrix} 0 \\ 1 \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \ \ldots, \ b_n = \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ 1 \end{bmatrix} \tag{16}$$

составляют базис модуля Δ^n.

Далее,

$$h(b_\nu) = cb_\nu = \begin{bmatrix} \gamma_{1\nu} \\ \gamma_{2\nu} \\ \cdot \\ \cdot \\ \cdot \\ \gamma_{n\nu} \end{bmatrix} = b_1\gamma_{1\nu} + b_2\gamma_{2\nu} + \ldots + b_n\gamma_{n\nu},$$
$$\nu = 1, \ldots, n.$$

Следовательно, матрица эндоморфизма h в базисе (16) совпадает с c. Обратно, любой эндоморфизм h модуля Δ^n сводится к умножению столбцов на матрицу h в базисе (16). Это дает возможность не различать эндоморфизм и его матрицу в базисе (16).

Лемма 6 (Басс [1]). *При $n > 1$ аддитивная группа, порождаемая $SL(n, \Delta)$, совпадает с аддитивной группой полного матричного кольца Δ_n.*

Доказательство. Пусть D — аддитивная группа, порождаемая $SL(n, \Delta)$. Для $i \neq j$ и произвольного $\lambda \in \Delta$ $e_{ij}\lambda = t_{ij}(\lambda) - E_n \in D$. Далее, $e_{ii}\lambda = t_{ij}(\lambda)t_{ij}(1) - t_{ij}(\lambda) - e_{ij} \in D$. ■

Если Φ — подгруппа аддитивной группы кольца Δ, то символом Φ^n будем обозначать подгруппу аддитивной группы модуля Δ^n, состоящую из всех столбцов

$$\begin{bmatrix} \varphi_1 \\ \cdot \\ \cdot \\ \cdot \\ \varphi_n \end{bmatrix}, \quad \varphi_\nu \in \Phi.$$

Лемма 7 (Басс [1]). *Пусть $n > 1$. Подгруппа L аддитивной группы модуля Δ^n тогда и только тогда инвариантна относительно $SL(n, \Delta)$, когда $L = \Phi^n$, где Φ — некоторый левый идеал кольца Δ.*

Доказательство. В силу предыдущего утверждения в формулировке леммы можно $SL(n, \Delta)$ заменить кольцом Δ_n. Пусть L — инвариантная относительно Δ_n подгруппа аддитивной группы модуля Δ^n. Рассмотрим отображение

$$\pi_\nu\colon L \to \Delta, \quad x = \begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix} \mapsto x_\nu.$$

Положим $\operatorname{Im}(\pi_\nu) = \Phi_\nu$. Ясно, что Φ_ν — подгруппа аддитивной группы кольца Δ. Φ_ν — левый идеал в Δ. Действительно, пусть $a_\nu \in \Phi_\nu$. Тогда в L есть столбец

$$a = \begin{bmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_\nu \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{bmatrix}.$$

Для $\lambda \in \Delta$, $(e_{\nu\nu}\lambda)a \in L$. Но $(e_{\nu\nu}\lambda)a = b_\nu(\lambda\alpha_\nu)$. Следовательно, $\lambda\alpha_\nu \in \Phi_\nu$, Φ_ν — левый идеал. Пусть снова $\alpha_\nu \in \Phi_\nu$,

$$a = \begin{bmatrix} \alpha_1 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_\nu \\ \cdot \\ \cdot \\ \cdot \\ \alpha_n \end{bmatrix} \in L.$$

Тогда для любого $i = 1, \ldots, n$

$$e_{i\nu}a \in L, \qquad e_{i\nu}a = b_i\alpha_\nu.$$

Следовательно, $\alpha_\nu \in \Phi_i$. Таким образом,

$$\Phi_1 = \ldots = \Phi_n = \Phi.$$

Очевидно, что

$$L \subset b_1\Phi + \ldots + b_n\Phi = \Phi^n.$$

С другой стороны, если $\alpha_\nu \in \Phi$, то

$$a = \begin{bmatrix} \alpha_1 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_\nu \\ \cdot \\ \cdot \\ \cdot \\ \alpha_n \end{bmatrix} \in L, \quad e_{\nu\nu}a = b_\nu\alpha_\nu \in L, \qquad L = \Phi^n.$$

Необходимость доказана.

Докажем достаточность. Пусть Φ — произвольный левый идеал кольца Δ. Покажем, что аддитивная подгруппа Φ^n группы Δ^n инвариантна относительно Δ_n. Пусть

$$b = \begin{bmatrix} \beta_1 \\ \cdot \\ \cdot \\ \cdot \\ \beta_n \end{bmatrix} \in \Phi^n.$$

Тогда $\beta_j \in \Phi$, $(e_{ij}\lambda)\,b = b_i(\lambda\beta_j) \in \Phi^n$, так как $\lambda\beta_j \in \Phi$. ■

5. Аффинная группа. Пусть Aff (n, Δ) — множество всех пар вида

$$\langle g, a\rangle, \quad g \in GL(n, \Delta), \quad a \in \Delta^n. \tag{17}$$

Пару (17) будем трактовать как отображение

$$\langle g, a\rangle \colon \Delta^n \to \Delta^n, \quad x \mapsto gx + a.$$

Очевидно, что (17) — биекция, т. е. $\mathrm{Aff}(n, \Delta) \subset S(\Delta^n)$. Если $\langle h, b\rangle$ — другая пара из $\mathrm{Aff}(n, \Delta)$, то

$$\langle g, a\rangle \langle h, b\rangle (x) = \langle g, a\rangle (hx + b) = ghx + gb + a = \\ = \langle gh, gb + a\rangle (x),$$

т. е.

$$\langle g, a\rangle \langle h, b\rangle = \langle gh, gb + a\rangle. \tag{18}$$

Из (18) следует, что $\mathrm{Aff}(n, \Delta)$ — группа. Будем называть ее *аффинной группой.*

Очевидно, что $\langle E_n, (0)\rangle$ — единица группы $\mathrm{Aff}(n, \Delta)$ и

$$\langle g, a\rangle^{-1} = \langle g^{-1}, -g^{-1}a\rangle. \tag{19}$$

Из (18) также видно, что

$$\gamma \colon \mathrm{Aff}(n, \Delta) \to GL(n, \Delta), \quad \langle g, a\rangle \mapsto g, \tag{20}$$

— сюръективный гомоморфизм. Далее,

$$\mathrm{Ker}\,\gamma = \{\langle E_n, a\rangle \mid a \in \Delta^n\} = \langle E_n, \Delta^n\rangle\,^{*)},$$

так что

$$GL(n, \Delta) \cong \mathrm{Aff}(n, \Delta)/\langle E_n, \Delta^n\rangle.$$

Пару $\langle g, a\rangle \in \mathrm{Aff}(n, \Delta)$ можно трактовать так же, как $(n+1)\times(n+1)$-матрицу

$$\begin{bmatrix} \gamma_{11} & \dots & \gamma_{1n} & \alpha_1 \\ \cdot & \cdot & \cdot & \cdot \\ \gamma_{n1} & \dots & \gamma_{nn} & \alpha_n \\ 0 & \dots & 0 & 1 \end{bmatrix}, \quad \|\gamma_{ij}\| = g, \quad \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = a,$$

которую условимся записывать так:

$$\begin{bmatrix} g & a \\ 0 & 1 \end{bmatrix}.$$

---

*) В дальнейшем без особых оговорок мы будем пользоваться обозначениями вида $\langle G, L\rangle = \{\langle g, l\rangle \mid g \in G,\ l \in L\}$.

Такое представление элементов аффинной группы имеет смысл, так как

$$\begin{bmatrix} g & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} h & b \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} gh & gb+a \\ 0 & 1 \end{bmatrix}.$$

Таким образом, $\mathrm{Aff}(n, \Delta) \subset GL(n+1, \Delta)$. Элементы $\langle E_n, a\rangle \in \langle E_n, \Delta^n\rangle$ изображаются при этом матрицами вида

$$\begin{bmatrix} E_n & a \\ 0 & 1 \end{bmatrix},$$

так что $\langle E_n, \Delta^n\rangle \subset SL(n+1, \Delta)$.

Из (18) и (19) легко получить формулу

$$\langle g, 0\rangle \langle E_n, a\rangle \langle g, 0\rangle^{-1} = \langle E_n, ga\rangle,$$

откуда вытекает

Лемма 8. *Пусть L — подгруппа аддитивной группы модуля Δ^n, а H — подгруппа группы $GL(n, \Delta)$. Подгруппа $\langle H, (0)\rangle$ тогда и только тогда принадлежит нормализатору подгруппы $\langle E_n, L\rangle$ в* $\mathrm{Aff}(n, \Delta)$, *когда $HL = L$.*

В дальнейшем мы будем часто употреблять выражение вида «подгруппа A *нормализуется* подгруппой B в группе G» в смысле «B содержится в нормализаторе подгруппы A в G».

Лемма 9 (Басс [1]). *Пусть G — подгруппа в* $\mathrm{Aff}(n, \Delta)$, *γ — гомоморфизм* (20), *$H = \mathrm{Im}\,\gamma$.*

(i) *Тогда взаимный коммутант K групп G и $\langle E_n, \Delta^n\rangle$ удовлетворяет соотношению:*

$$K = (G, \langle E_n, \Delta^n\rangle) = (\langle H, (0)\rangle, \langle E_n, \Delta^n\rangle) = \langle E_n, A\rangle,$$

где

$$A = \sum (h - E_n)\Delta^n, \qquad h \in H,$$

— аддитивная группа, порождаемая всеми столбцами $(h - E_n)a$, $h \in H$, $a \in \Delta^n$.

(ii) *Если группа G нормализуется группой $\langle E_n, \Delta^n\rangle$ и*

$$G \cap \langle E_n, \Delta^n\rangle = \langle E_n, (0)\rangle, \tag{21}$$

то $G = \langle E_n, (0)\rangle$.

(iii) *Если группа G нормализуется группой $\langle SL(n,\Delta),\ (0)\rangle$, то $K = \langle E_n, \Phi^n\rangle$, где Φ — левый идеал кольца Δ.*

Доказательство. В силу формул (18) и (19) для $\langle h, b\rangle \in G$, $\langle E_n, a\rangle \in \langle E_n, \Delta^n\rangle$

$$\langle h,\ b\rangle\langle E_n,\ a\rangle\langle h,\ b\rangle^{-1}\langle E_n,\ a\rangle^{-1} = \langle E_n,\ (h - E_n)\,a\rangle,$$

откуда и вытекает (i).

(ii) следует из (i). Действительно, если A нормализуется группой $\langle E_n, \Delta^n\rangle$, то

$$K \subset A \cap \langle E_n,\ \Delta^n\rangle.$$

Если, сверх того, имеет место (21), то, в силу (i),

$$H = (E_n), \qquad A \subset \langle E_n,\ \Delta^n\rangle, \qquad A = \langle E_n,\ (0)\rangle.$$

Докажем (iii). Пусть A нормализуется группой $\langle SL(n,\Delta),\ (0)\rangle$. В силу леммы 8 $\langle E_n\Delta^n\rangle$ также нормализуется этой группой. Тогда и группа K ею нормализуется. В силу (i) $K = \langle E_n,\ D\rangle$, а $SL(n,\ \Delta)D = D$ согласно лемме 8. Следовательно, по лемме 7, $D = \Phi^n$, где Φ — левый идеал кольца Δ. ■

§ 9. Определитель Дьедонне

1. Матрицы $d(\mu)$. Пусть $\Delta = T$, где T = тело. Введем матрицы $d(\mu) \in GL(n, T)$, $n > 1$, положив

$$d(\mu) = \operatorname{diag}[1,\ \ldots,\ 1,\ \mu], \qquad \mu \in T^*, \tag{1}$$

т. е. $d(\mu)$ — это диагональная матрица с элементами $1, \ldots, 1, \mu$ на главной диагонали.

Лемма 1. *Если $a \in GL(n,T)$, то $a = sd(\mu)$, $s \in SL(n,T)$.*

Доказательство. Умножение слева матрицы a на элементарную матрицу $t_{ij}(\lambda)$ равносильно следующей элементарной операции: прибавлению к i-й строке матрицы a ее j-й строки, умноженной слева на λ. Лемма будет доказана, если установить, что матрицу $a = \|\alpha_{ij}\|$ из $GL(n,T)$ можно привести к виду (1) с помощью подобных элементарных операций.

Согласно лемме 8.1а столбцы матрицы $a = \|\alpha_{ij}\|$ образуют базис пространства T^n. Следовательно, в первом столбце есть отличный от нуля элемент. Мы можем считать, что $\alpha_{21} \neq 0$. Прибавляя к первой строке матрицы a вторую, умноженную слева

$$(1-\alpha_{11})\alpha_{21}^{-1},$$

получим матрицу с 1 на позиции $(1, 1)$. Прибавляя затем первую строку, умноженную слева на подходящий множитель, к каждой из других строк, мы приведем матрицу a к виду

$$\begin{bmatrix} 1 & \alpha_{12} \; \ldots \; \alpha_{1n} \\ 0 & \\ \cdot & \\ \cdot & A_{n-1} \\ \cdot & \\ 0 & \end{bmatrix} = a_1.$$

Но $a_1 \in GL(n, T)$, поэтому столбцы этой матрицы составляют базис пространства T^n. Учитывая вид матрицы a_1, отсюда заключаем, что в первом столбце матрицы A_{n-1} есть элемент из T^*. Если $n-1 > 1$, то к матрице A_{n-1} применимы предыдущие рассуждения. Таким образом, при $n > 2$ можно считать, что первый столбец матрицы A_{n-1} имеет вид

$$\begin{bmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}.$$

С помощью элементарной операции можно устранить α_{12}. Поступая аналогично, мы придем к матрице вида

$$a_2 = \begin{bmatrix} 1 & 0 & \ldots & 0 & \alpha_{1n} \\ 0 & 1 & \ldots & 0 & \alpha_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 & \alpha_{n-1, n} \\ 0 & 0 & \ldots & 0 & \alpha_{nn} \end{bmatrix}.$$

Так как $a_2 \in GL(n, T)$, то столбцы матрицы a_2 образуют базис пространства T^n, поэтому

$$\alpha_{nn} = \mu \neq 0.$$

Очевидно, что матрицу a_2 можно элементарными операциями привести к виду (1). ■

Следствие 1. *Матрицы $t_{ij}(\lambda)$ вместе с матрицами $d(\mu)$ составляют систему образующих группы $GL(n, T)$.*

Лемма 2. *Пусть $n > 1$, α, $\beta \in T^*$, $\mu = \alpha\beta\alpha^{-1}\beta^{-1}$. Тогда $d(\mu) \in SL(n, T)$.*

Доказательство. В последовательности

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ \alpha^{-1} & 1 \end{bmatrix}, \begin{bmatrix} 0 & -\alpha \\ \alpha^{-1} & 1 \end{bmatrix}, \begin{bmatrix} 0 & -\alpha \\ \alpha^{-1} & \beta^{-1} \end{bmatrix},$$

$$\begin{bmatrix} \alpha\beta\alpha^{-1} & 0 \\ \alpha^{-1} & \beta^{-1} \end{bmatrix}, \begin{bmatrix} \alpha\beta\alpha^{-1} & 0 \\ 1 & \beta^{-1} \end{bmatrix}, \begin{bmatrix} 0 & -\mu \\ 1 & \beta^{-1} \end{bmatrix},$$

$$\begin{bmatrix} 0 & -\mu \\ 1 & \mu \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & \mu \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & \mu \end{bmatrix}$$

каждая матрица получается из предыдущей с помощью одной элементарной операции. Следовательно, E_n при $n > 1$ можно с помощью элементарных операций привести к виду $d(\mu)$. Отсюда и вытекает лемма. ■

2. Определитель матрицы над телом. Пусть $\overline{T}^*$ — фактор-группа группы T^* по ее коммутанту. К группе $\overline{T}^*$ присоединим $\overline{0}$ внешним образом: $\overline{0}\overline{T}^* = \overline{T}^*\overline{0} = \overline{0}$. Полученную коммутативную полугруппу обозначим символом $\overline{T}$. Если $T^* \to \overline{T^*}$ — естественный гомоморфизм, то образ элемента $\alpha \in T^*$ будем обозначать $\bar{\alpha}$. Расширяя это отображение, положим $\bar{\alpha} = \overline{0}$ для $\alpha = 0$. Тогда для α, $\beta \in T$

$$\overline{\alpha\beta} = \bar{\alpha}\bar{\beta} = \bar{\beta}\bar{\alpha} = \overline{\beta\alpha}.$$

Очевидно, что $\overline{1}$ — единица полугруппы $\overline{T}$.

Наша цель — доказать существование отображения

$$\delta\colon T_n \to \overline{T}, \tag{2}$$

удовлетворяющего трем условиям:

I. *Если матрица b получается из матрицы a умножением слева одной из строк на α, то*

$$\delta(b) = \bar{\alpha}\delta(a).$$

II. *Если матрица b получается из матрицы a прибавлением к одной строке другой, то*

$$\delta(b) = \delta(a).$$

III. $\delta(E) = \bar{1}$.

Если существует отображение δ, удовлетворяющее условиям I, II, III, *то оно обладает следующими свойствами:*

1) *Если $s \in SL(n, T)$, то $\delta(sa) = \delta(a)$.*

2) *Если $a = sd(\mu)$, $s \in SL(n, T)$, то $\delta(a) = \bar{\mu}$.*

3) *Если какая-либо строка матрицы a состоит из нулей, то $\delta(a) = \bar{0}$.*

4) $a \in T_n \setminus GL(n, T) \Leftrightarrow \delta(a) = \bar{0}$ (здесь $\Leftrightarrow$, как обычно, — знак эквивалентности).

5) $\delta(ab) = \delta(a)\delta(b)$.

6) *Если матрица b получается из матрицы a транспозицией двух строк, то $\delta(b) = -\bar{1}\delta(a)$.*

Доказательство. 1) Так как s — произведение элементарных матриц вида $t_{ij}(\lambda)$, то достаточно показать, что

$$\delta(t_{ij}(\lambda)a) = \delta(a). \tag{3}$$

Пусть $\lambda \neq 0$, а матрица b получается из матрицы a заменой j-й строки a_j строкой λa_j. Тогда, согласно I, $\delta(b) = \bar{\lambda}\delta(a)$. С другой стороны, если матрица c получается из матрицы b прибавлением к i-й строке j-й, то

$$\delta(c) = \delta(b) = \bar{\lambda}\delta(a) = \bar{\lambda}(\delta(t_{ij}(\lambda)a)). \tag{4}$$

Так как $\bar{\lambda} \in \overline{T^*}$, то (4) $\Rightarrow$ (3).

2) вытекает из 1), I и III. 3) следует из I.

4) Пусть

$$a \in T_n \setminus GL(n, T). \tag{5}$$

Тогда, в силу леммы 8.1б, какая-либо строка этой матрицы есть левая линейная комбинация других ее строк. Поэтому в группе $SL(n, T)$ есть такая матрица s, что матрица sa содержит нулевую строку. Поэтому $\delta(a) = \delta(sa) = \bar{0}$. Таким образом, (5) влечет $\delta(a) = \bar{0}$. Обратная импликация следует из 2) и леммы 1.

5) Если матрица a необратима, то, в силу леммы 8.1а, ее столбцы линейно зависимы справа. Столбцы

матрицы ab — правые линейные комбинации столбцов матрицы a. По теореме Штейница они также линейно зависимы и, значит, матрица ab необратима. Тогда

$$\delta(ab) = \bar{0} = \delta(a)\delta(b).$$

Пусть теперь $a \in GL(n, T)$. Тогда, в силу леммы 1, $a = sd(\mu)$, $s \in SL(n, T)$,

$$\delta(ab) = \delta(sd(\mu)b) = \delta(d(\mu)b).$$

Матрица $d(\mu)b$ получается из b после умножения последней строки слева на μ. Поэтому

$$\delta(d(\mu)b) = \bar{\mu}\delta(b) = \delta(a)\delta(b).$$

6) следует из 1) и I. ∎

Теорема 1. *Существует единственное отображение* (2), *удовлетворяющее условиям* I, II, III. *Это отображение — сюръективный гомоморфизм.*

Доказательство Из свойств 2) и 4) вытекает, что существует не более одного отображения (2), удовлетворяющего условиям I, II, III. Поэтому достаточно построить такое отображение и показать, что оно — сюръективный гомоморфизм. Воспользуемся индукцией по числу n. Для $n = 1$ положим $\delta(\alpha) = \bar{\alpha}$. Условия I, II, III, очевидно, выполняются. Пусть теперь $n > 1$ и уже построено отображение

$$\delta\colon T_{n-1} \to \bar{T},$$

удовлетворяющее условиям I, II, III. Построим отображение (2). Пусть $a \in T_n$. Если матрица a необратима, то положим

$$\delta(a) = \bar{0}.$$

Если же a обратима, то ее строки $a_1, \ldots, a_n$ составляют базис пространства T_L^n. Следовательно, существует единственный вектор $(\lambda_1, \ldots, \lambda_n) \in T^n$ такой, что

$$\sum_{\nu=1}^{n} \lambda_\nu a_\nu = (1, 0, \ldots, 0). \tag{6}$$

Строку a_i запишем в виде

$$a_i = (\alpha_{i1}, b_i), \qquad b_i \in T_L^{n-1}.$$

Тогда из (6) получим

$$\sum_{\nu=1}^{n} \lambda_\nu b_\nu = (0, \ldots, 0). \tag{7}$$

Пусть

$$f = \begin{bmatrix} b_1 \\ b_2 \\ \cdot \\ \cdot \\ \cdot \\ b_n \end{bmatrix},$$

а $c_i \in T_{n-1}$ получается из матрицы f вычеркиванием i-й строки. Если $\lambda_i \neq 0$, $\lambda_j \neq 0$ и $i \neq j$, то введем еще две матрицы g и h из T_{n-1} следующим образом: g получается из c_i заменой b_j на $\lambda_j b_j$, а h — заменой b_j на b_i. Тогда, согласно I,

$$\delta(c_i) = \overline{\lambda_j^{-1}}\delta(g).$$

Прибавив теперь к строке $\lambda_j b_j$ матрицы g каждую из других строк b_ν, умноженную слева на λ_ν, получим, в силу (7), вместо строки $\lambda_j b_j$ строку $-\lambda_i b_i$. Следовательно,

$$\delta(g) = -\overline{\lambda_i}\delta(h).$$

Отсюда

$$\delta(c_i) = \overline{\lambda_j^{-1}}(-\overline{\lambda_i})\,\delta(h). \tag{8}$$

Заметим теперь, что матрицу h можно получить из матрицы c_j перестановкой строк. Подсчитав число нужных для этого транспозиций, найдем

$$\delta(h) = \overline{(-1)^{j-i-1}}\,\delta(c_j).$$

Отсюда и из (8)

$$\overline{(-1)^{i+1}}\,\overline{\lambda_i^{-1}}\delta(c_i) = \overline{(-1)^{j+1}\,\lambda_j^{-1}}\delta(c_j).$$

Последнее равенство показывает, что величина

$$\overline{(-1)^{i+1}\,\lambda_i^{-1}}\delta(c_i)$$

принимает одно и то же значение для всех таких i, что $\lambda_i \neq 0$.

Положим

$$\delta(a) = \overline{(-1)^{i+1}\lambda_i^{-1}\delta(c_i)}, \qquad \lambda_i \neq 0. \tag{9}$$

Итак, мы построили отображение (2): $\delta(a) = \overline{0}$, *если матрица a необратима, для обратимой матрицы a $\delta(a)$ определяется формулой* (9). Покажем теперь, что это отображение удовлетворяет условиям I, II, III.

Пусть $a \in T_n$, $\mu \in T^*$, а матрица b получается из матрицы a умножением i-й строки слева на μ. Если матрица a необратима, то необратима и b и

$$\delta(b) = \overline{0} = \bar{\mu}\delta(a).$$

Если же a обратима, то обратима b и, значит, $\delta(a)$ и $\delta(b)$ надо вычислять по формуле (9). Очевидно, при переходе от $\delta(a)$ к $\delta(b)$ множитель λ_i надо заменить на $\lambda^i\mu^{-1}$, а другие λ_ν оставить прежними. Если $\lambda_i \neq 0$, то

$$\delta(b) = \overline{(-1)^{i+1}\mu\lambda_i^{-1}\delta(c_i)} = \bar{\mu}\delta(a),$$

ибо c_i при переходе от a к b не меняется. Если же

$$\lambda_i = 0, \qquad \lambda_\nu \neq 0,$$

то $\delta(c_\nu)$ при переходе от a к b умножается на $\bar{\mu}$ и, значит,

$$\delta(b) = \bar{\mu}\delta(a).$$

Пусть теперь матрица b получается из матрицы a заменой строки a_i на строку $a_i + a_j$. Если a необратима, то и b необратима и $\delta(b) = \overline{0} = \delta(a)$. Если же матрица a обратима, то обратима и b. Так как $\lambda_i(a_i + a_j) + (\lambda_j - \lambda_i)a_j = \lambda_i a_i + \lambda_j a_j$, то при переходе от a к b λ_j заменяется на $\lambda_j - \lambda_i$, а другие λ_ν не изменяются. Очевидно, и $\delta(c_\nu)$ с $\nu \neq j$ не изменяются при этом переходе. Следовательно, если $\lambda_\nu \neq 0$, то

$$\delta(a) = (-1)^{\nu+1}\lambda_\nu^{-1}\delta(c_\nu) = \delta(b).$$

Если же всегда при $\nu \neq j$ $\lambda_\nu = 0$, то, согласно (7), $\lambda_j b_j = (0, \ldots, 0)$, $b_j = (0, \ldots, 0)$. Поэтому при переходе от матрицы a к матрице b строка b_i переходит в $b_i + b_j = b_i$, т. е. матрица c_j не изменяется. Так как $\lambda_i = 0$, то λ_j также не изменяется и снова $\delta(b) = \delta(a)$.

Остается проверить условие III. Пусть $a = E_n$. Тогда $\lambda_1 = 1$, $\lambda_\nu = 0$ для $\nu > 1$, $c_1 = E_{n-1}$. По формуле (9) находим $\delta(E_n) = \delta(a) = \delta(E_{n-1}) = 1$.

Итак, отображение δ удовлетворяет условиям I, II, III. Согласно 5) δ — гомоморфизм. Сюръективность отображения δ следует из 2) и 4). ■

Если тело T коммутативно (при этом $\overline{T^*} = T^*$ и можно считать $\bar{T} = T$), *то $\delta(a)$ совпадает с обычным определителем* $\det a$ *матрицы a над полем.* В самом деле, пусть $a = sd(\mu)$, $s \in SL(n, T)$. Тогда, очевидно, $\det a = \mu$. С другой стороны, $\delta(a) = \bar{\mu} = \mu$.

Будем теперь в случае произвольного тела T называть $\delta(a)$ *определителем матрицы* $a \in T_n$ и обозначать $\det a$.

Рассмотрим примеры.

1. Пусть

$$a = \begin{bmatrix} \alpha_{11} & 0 \ \ldots \ 0 \\ \alpha_{21} & \\ \vdots & A_{n-1} \\ \alpha_{n1} & \end{bmatrix} \in GL(n, T).$$

Тогда, по формуле (9),

$$\det a = \bar{\alpha}_{11} \det A_{n-1}.$$

Следовательно, для

$$a = \begin{bmatrix} \alpha_{11} & 0 & \ldots & 0 \\ \alpha_{21} & \alpha_{22} & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{bmatrix}$$

$$\det a = \overline{\alpha_{11} \ldots \alpha_{nn}}.$$

2. Пусть $c \in GL(n, T)$ — мономиальная матрица (т. е. матрица, имеющая в каждой строке и в каждом столбце по одному ненулевому элементу),

$$\alpha_{i_1 1}, \ \ldots, \ \alpha_{i_n n}$$

— все ее ненулевые элементы. Тогда

$$\det c = \overline{(-1)^t \alpha_{i_1 1} \ldots \alpha_{i_n n}},$$

где t — число инверсий в перестановке $i_1, i_2, \ldots, i_n$.

Теорема 2. *При $n \geqslant 2$ $SL(n, T)$ — множество всех матриц из T_n с определителем, равным $\overline{1}$.*

Доказательство. Если $a \in SL(n, T)$, то $\det a = \overline{1}$ в силу 1) и III. Пусть теперь $\det a = \overline{1}$. Тогда, согласно 4), a — обратимая матрица и, следовательно, $a = sd(\mu)$, где $s \in SL(n, T)$, $\bar{\mu} = \overline{1}$. Отсюда вытекает, что

$$\mu = \mu_1 \ldots \mu_k,$$

где μ_j — коммутатор в T^*. В силу леммы 2 $d(\mu_j) \in SL(n, T)$ и, значит,

$$d(\mu) = d(\mu_1) \ldots d(\mu_n) \in SL(n, T), \qquad a \in SL(n, T). \ \blacksquare$$

Очевидно, что

$$\delta(GL(n, T)) = \overline{T^*}.$$

Отсюда и из теоремы 2 вытекает

Теорема 3. *Если $n \geqslant 2$, то $SL(n, T)$ — инвариантная подгруппа группы $GL(n, T)$, фактор-группа по которой изоморфна $\overline{T^*}$.*

Теорема 4. *Пусть $n > 2$, либо $n = 2$, но $T \neq GF(2)$. Тогда $SL(n, T)$ — коммутант группы $GL(n, T)$.*

Доказательство. Согласно теореме 3 группа $SL(n, T)$ содержит коммутант группы $GL(n, T)$. В силу же теоремы 8.5 и следствия 1 леммы 8.4 $SL(n, T)$ содержится в коммутанте. $\blacksquare$

Следствие 1. *При $n \geqslant 2$ всякая подгруппа в $GL(n, T)$, содержащая $SL(n, T)$, инвариантна.*

Если M — правое пространство над телом T, а h — эндоморфизм этого пространства, то положим $\det h = \det a$, где a — матрица эндоморфизма h в некотором базисе. Так как в любом другом базисе матрица эндоморфизма h имеет вид $c^{-1}ac$ и $\det(c^{-1}ac) = \det a$, то $\det h$ не зависит от выбора базиса. $SL(M)$ можно теперь определить как группу всех автоморфизмов пространства M с определителем, равным $\overline{1}$.

§ 10. Инвариантные подгруппы в $GL(M)$

Пусть M—правое n-мерное пространство над телом T. Согласно результатам § 8 группа $GL(M)$ всех автоморфизмов пространства M изоморфна группе $GL(n, T)$ всех обратимых $n \times n$-матриц над телом T. Из свойств определителя следует, что $GL(n, T)$ есть множество всех таких матриц $a \in T_n$, что $\det a \neq \overline{0}$, а $SL(n, T)$ есть множество всех матриц из T_n с определителем, равным $\overline{1}$. Но $\det h$ определен и для любого эндоморфизма h пространства M. Пусть $SL(M)$ — группа всех таких h из $\operatorname{End} M$, что $\det h = \overline{1}$. Если

$$\psi\colon GL(M) \to GL(n, T)$$

— такой изоморфизм, что $\psi(h)$ — матрица автоморфизма h, то

$$\psi(SL(M)) = SL(n, T), \qquad \psi^{-1}(SL(n, T)) = SL(M).$$

В дальнейшем мы часто будем отождествлять $GL(n, T)$ с $GL(M)$, $SL(n, T)$ с $SL(M)$.

Лемма 1. *Множество всех трансвекций пространства M является системой образующих группы $SL(M)$.*

Доказательство. По лемме 7.7 любая неединичная трансвекция τ из $GL(M)$ сопряжена с трансвекцией $\tau_{ij}(\lambda)$, $\lambda \in T^*$. Далее, $\det(\tau_{ij}(\lambda)) = \det(t_{ij}(\lambda)) = \overline{1}$, поэтому $\det \tau = \overline{1}$ и, значит, $\tau \in SL(M)$.

С другой стороны, множество всех элементарных матриц $t_{ij}(\lambda)$ порождает группу $SL(n, T)$. Следовательно, множество всех трансвекций $\tau_{ij}(\lambda)$ порождает группу $SL(M)$. ■

Лемма 2. *Если $n > 2$, то централизатор любой трансвекции τ в группе $GL(M)$ содержит полную систему представителей смежных классов $GL(M)$ по $SL(M)$.*

Доказательство. По лемме 7.7 любые две неединичные трансвекции сопряжены в группе $GL(M)$, поэтому достаточно доказать лемму для одной из них, скажем, для $\tau_{12}(1)$. Очевидно, что при любом $\mu \in T^*$ матрица $d(\mu)$ перестановочна с $t_{12}(1)$, поэтому централизатор матрицы $t_{12}(1)$ в $GL(n, T)$ содержит полную систему представителей смежных классов группы $GL(n, T)$ по $SL(n, T)$. ■

Лемма 3. *Если $n > 2$, то любые две неединичные трансвекции сопряжены в группе $SL(M)$.*

Доказательство. Пусть τ_1 и τ_2 — две неединичные трансвекции. По лемме 7.7 $\tau_1 = g\tau_2 g^{-1}$, $g \in GL(M)$. Пусть c — элемент централизатора τ_2 в $GL(M)$, входящий в тот же смежный класс группы $GL(M)$ по $SL(M)$, что и g. Тогда

$$\tau_1 = (gc^{-1})\tau_2(gc^{-1})^{-1}, \qquad gc^{-1} \in SL(M). \blacksquare$$

Теорема 1. *Если $n > 2$, то всякая подгруппа Γ в $GL(M)$, нормализуемая группой $SL(M)$, либо содержит $SL(M)$, либо содержится в центре группы $GL(M)$.*

Доказательство. Пусть Γ не входит в центр группы $GL(M)$. В силу леммы 3 достаточно доказать, что Γ содержит неединичную трансвекцию. Согласно следствию 7.2.3 и лемме 7.6 найдутся такие $\sigma \in \Gamma$ и $a \in M$, что a и $b = \sigma(a)$ линейно независимы. Пространство M можно представить в виде $M = P \dotplus bT$, где P — гиперплоскость, содержащая a. Рассмотрим трансвекцию τ:

$$\tau(p) = p, \qquad p \in P, \qquad \tau(b) = b + a.$$

Пусть

$$\tau_1 = \sigma\tau\sigma^{-1}.$$

Тогда $\tau_1(b) = b$, $\tau_1 \neq \tau$ и, значит,

$$\rho = \tau_1\tau^{-1} \neq e.$$

Так как $\rho = \sigma\tau\sigma^{-1}\tau^{-1}$ и группа Γ инвариантна относительно $SL(M)$, то $\rho \in \Gamma$. Для $x \in M$ $x = p + b\lambda$, $\tau(x) = p + (b + a)\lambda = x + a\lambda$,

$$\tau(x) - x \in aT. \tag{1}$$

Аналогично,

$$\tau_1(x) - x \in bT. \tag{2}$$

Если теперь $Q = aT + bT$, то, в силу (1) и (2), для $x \in M$

$$\rho(x) - x \in Q. \tag{3}$$

Так как $n > 2$, то Q содержится в некоторой гиперплоскости H и из (3) следует

$$\rho(x) - x \in H, \qquad \rho(H) = H. \tag{4}$$

Теперь возможны два случая:

1) ρ перестановочно с каждой трансвекцией из $K(H)$;

2) в $K(H)$ существует трансвекция φ, не перестановочная с ρ.

В первом случае, по теореме 7.2, $\rho = \rho_\alpha\tau_\alpha$, где $\rho_\alpha \in H(M)$, $\tau_\alpha \in K(H)$, $\tau_\alpha(c) = c \dotplus h$, $M = H \dotplus cT$. Далее,

$\rho(c) - c = (c+h)\alpha - c = c(\alpha - 1) + h\alpha \in H$. Поэтому $c(\alpha - 1) = 0$, $\alpha - 1 = 0$, $\rho_\alpha = e$, $\rho = \tau_\alpha \in K(H)$, τ_α — принадлежащая группе Γ неединичная трансвекция.

Во втором случае $\varphi_1 = \rho\varphi\rho^{-1}\varphi^{-1} \in \Gamma$. Далее, $\rho\varphi\rho^{-1} \in K(\rho(H)) = K(H)$. Поэтому и $\varphi_1 \in K(H)$. ■

Легко проверить, что теорема 1 не распространяется на группы $GL(2, 2)$ и $GL(2, 3)$. Однако это единственное исключение; доказательству этого факта мы предпошлем три леммы.

Лемма 4. *Пусть M — двумерное пространство над телом T, а P и Q — его одномерные подпространства. Тогда группы $K(P)$ и $K(Q)$ сопряжены в $SL(M)$.*

Доказательство. Очевидно, надо рассматривать случай, когда $P \neq Q$. Пусть $P = pT$, $Q = qT$. Тогда

$$p,\ q \tag{5}$$

— базис пространства M. Пусть теперь автоморфизм σ задается равенствами $\sigma(p) = q$, $\sigma(q) = p(-1)$. В базисе (5) этот автоморфизм имеет матрицу

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$\det\sigma = \overline{1}$, $\sigma \in SL(M)$. Если τ — произвольная трансвекция из $K(P)$, то

$$\tau(p) = p, \quad \tau(q) = q + p\lambda, \quad \lambda \in T, \quad \tau = \tau_\lambda.$$

Тогда

$$\sigma\tau\sigma^{-1}(q) = q, \quad \sigma\tau\sigma^{-1}(p) = \sigma\tau(q(-1)) =$$
$$= \sigma(q(-1) + p(-\lambda)) = p + q(-\lambda).$$

Следовательно, $\sigma\tau_\lambda\sigma^{-1} \in K(Q)$. Когда λ пробегает T, то $\sigma\tau_\lambda\sigma^{-1}$ пробегает $K(Q)$, т. е.

$$\sigma K(P)\sigma^{-1} = K(Q). \ ■$$

Следствие 1. *Пусть M — двумерное пространство над телом T, P — одномерное подпространство пространства M. Если подгруппа Γ группы $GL(M)$, содержащая $K(P)$, нормализуется группой $SL(M)$, то $\Gamma \supset SL(M)$.*

Лемма 5. *Пусть M — двумерное пространство над телом T, причем тело T или не является полем характеристики 2, или, будучи полем характеристики 2, не со-*

держит трансцендентных относительно своего простого подполя элементов. Если подгруппа Γ *группы* $GL(M)$ *нормализуется группой* $SL(M)$ *и содержит неединичную трансвекцию, то* $\Gamma \supset SL(M)$.

Доказательство. Пусть $\tau \in \Gamma$ — неединичная трансвекция. Для некоторого базиса a, b пространства M можно написать

$$\tau(a) = a, \quad \tau(b) = a\lambda + b, \quad \lambda \in T. \tag{6}$$

Пусть $\sigma \in GL(M)$ определяется формулами

$$\sigma(a) = a\alpha, \quad \sigma(b) = b\gamma.$$

Тогда

$$\sigma^{-1}(a) = a\alpha^{-1}, \quad \sigma^{-1}(b) = b\gamma^{-1}$$

и

$$\sigma\tau\sigma^{-1}(a) = a, \quad \sigma\tau\sigma^{-1}(b) = a\alpha\lambda\gamma^{-1} + b. \tag{7}$$

Если

$$\gamma = \lambda^{-1}\alpha^{-1}\lambda, \tag{8}$$

то

$$\det\sigma = \overline{\alpha\lambda^{-1}\alpha^{-1}\lambda} = \overline{1}, \quad \sigma \in SL(2, T).$$

Подставив (8) в (7), получим

$$\sigma\tau\sigma^{-1}(a) = a, \quad \sigma\tau\sigma^{-1}(b) = a\alpha^2\lambda + b. \tag{9}$$

Положим $\tau = \tau_\lambda$. Тогда, в силу (9),

$$\sigma\tau_\lambda\sigma^{-1} = \tau_{\alpha^2\lambda} \in \Gamma. \tag{10}$$

Пусть $L = \{\lambda \in T \mid \tau_\lambda \in \Gamma\}$. Очевидно, что L — подгруппа аддитивной группы тела T. Из (10) вытекает, что $\alpha^2 L \subset \subset L$ для любого $\alpha \in T$. Следовательно,

$$\alpha_1, \ldots, \alpha_k \in T \Rightarrow \alpha_1^2 \ldots \alpha_k^2 L \subset L.$$

Если S — подгруппа аддитивной группы тела T, порожденная произведениями квадратов из T, то $SL \subset L$. В силу предложения 6.2 $S = T$. Значит, $TL \subset L$, $L = T$. Очевидно, что множество всех τ_λ, где $\lambda \in T$, есть группа $K(aT)$. Таким образом, $K(aT) \subset \Gamma$. В силу леммы 4 Γ тогда содержит все трансвекции и, значит, $\Gamma \supset SL(M)$. ■

Лемма 6. *Пусть* M — *двумерное пространство над телом* T, a, b — *базис пространства* M, σ — *элемент вида*

$$\sigma(a) = a\alpha, \quad \sigma(b) = a\beta + b\gamma,$$

Γ — подгруппа группы $GL(M)$, нормализуемая группой $SL(M)$ и содержащая σ. Если γ не принадлежит центру $Z(T)$ тела T или $\gamma \in Z(T)$, но $\gamma \neq \alpha$, то $SL(M) \subset \Gamma$.

Доказательство. Пусть τ — трансвекция вида (6). Тогда

$$\rho = \sigma\tau\sigma^{-1}\tau^{-1} \in \Gamma, \quad \tau^{-1}(a) = a, \quad \tau^{-1}(b) = a(-\lambda) + b.$$

Отсюда находим

$$\rho(a) = a, \quad \rho(b) = a(\alpha\lambda\gamma^{-1} - \lambda) + b,$$

т. е. $\rho \in K(aT)$.

Теперь рассмотрим два случая: 1) тело T некоммутативно, 2) T — поле.

В первом случае, согласно лемме 5, достаточно выбрать так λ, что

$$\alpha\lambda\gamma^{-1} - \lambda \neq 0. \tag{11}$$

Если $\alpha \neq \gamma$, то условие (11) выполняется при $\lambda = 1$. Если же $\alpha \doteq \gamma$, то, по условию леммы, $\gamma \notin Z(T)$. Тогда существует в T такое λ, что $\gamma\lambda \neq \lambda\gamma$ и, значит,

$$\gamma\lambda\gamma^{-1} - \lambda \neq 0.$$

Рассмотрим второй случай. По условию $\alpha \neq \gamma$,

$$\alpha\lambda\gamma^{-1} - \lambda = (\alpha\gamma^{-1} - 1)\lambda \neq 0.$$

Когда λ пробегает поле T, $(\alpha\gamma^{-1} - 1)\lambda$ также пробегает T. Поэтому $K(aT) \subset \Gamma$. Согласно следствию леммы 4 $SL(M) \subset \Gamma$. ■

Теорема 2. *Пусть M — двумерное пространство над телом T, содержащим хотя бы четыре элемента. Тогда всякая подгруппа группы $GL(M)$, нормализуемая группой $SL(M)$, либо содержит $SL(M)$, либо содержится в центре группы $GL(M)$.*

Доказательство. Пусть Γ — нормализуемая группой $SL(M)$ подгруппа в $GL(M)$, не содержащаяся в центре $GL(M)$. Тогда найдутся такие $a \in M$, $\sigma \in \Gamma$, что

$$a, \ b = \sigma(a) \tag{12}$$

— базис пространства M. Элемент σ имеет вид

$$\sigma(a) = b, \quad \sigma(b) = a\beta + b\gamma, \quad \beta \neq 0.$$

Пусть автоморфизм τ определяется равенствами

$$\tau(a) = a\gamma\mu + b(-\mu), \qquad \tau(b) = a\mu^{-1}, \qquad \mu \in T^*.$$

Матрицей его в базисе (12) служит

$$\begin{bmatrix} \gamma\mu & \mu^{-1} \\ -\mu & 0 \end{bmatrix}.$$

Следовательно, $\tau \in SL(M)$ и

$$\rho = (\tau^{-1}\sigma^{-1}\tau)\,\sigma \in \Gamma.$$

Далее, находим

$$\rho(a) = a(-\mu^{-1}\beta^{-1}\mu^{-1}),$$
$$\rho(b) = a\mu^{-1}\beta^{-1}(-\gamma\mu\beta - \mu^{-1}\gamma) + b(-\mu^2\beta).$$

Попытаемся теперь подобрать параметр μ так, чтобы можно было применить лемму 6.

Если $\beta \notin Z(T)$ и $\mu = 1$, то $-\mu^2\beta \notin Z(T)$ и применима лемма 6.

Если $\beta \in Z(T)$, но T — некоммутативное тело, то, в силу предложения 6.2, найдется такое $\mu \in T$, что $\mu^2 \notin Z(T)$. Тогда $-\mu^2\beta \notin Z(T)$ и снова применима лемма 6.

Остается рассмотреть случай, когда T — поле. Для применимости леммы 6 нужно так подобрать параметр μ, чтобы $-\mu^{-1}\beta^{-1}\mu^{-1} \neq -\mu^2\beta$. Последнее равносильно условию

$$\mu^4 \neq \beta^{-2}. \tag{13}$$

Уравнение

$$x^4 = \beta^{-2} \tag{14}$$

в поле T имеет не более четырех решений. Следовательно, если в T^* более четырех элементов, то при любом β в T^* есть элемент μ, удовлетворяющий условию (13). Таким образом, остается рассмотреть лишь два случая: 1) $T = GF(4)$, 2) $T = GF(5)$. В поле $GF(4)$ уравнение (14) имеет только одно решение $x = \beta^{-2}$. Полагая $\mu \neq \beta^{-2}$, получим нужное значение параметра. Пусть теперь $T = GF(5)$. Для $\beta \in T^*$ $\mu^4 = 1$. Следовательно, при $\beta \neq \pm 1$ условие (13) выполняется для любого $\mu \in T^*$. Если же $\beta = \pm 1$, то условие (13) не может быть выполнено. В этом случае выберем μ так, чтобы $\mu^2\beta = 1$. Тогда ρ примет вид $\rho(a) = a(-1)$, $\rho(b) = a(-2\gamma) + b(-1)$.

Далее, $\rho^2(a) = a$, $\rho^2(b) = a(4\gamma) + b$. Если $\gamma \neq 0$, то ρ^2 — неединичная трансвекция, принадлежащая группе Γ. В силу леммы 5 $\Gamma \supset SL(M)$. Остается случай $\gamma = 0$, $\beta = \pm 1$. Если $\beta = 1$, то $\sigma(a) = b$, $\sigma(b) = a$. Перейдем к новому базису c, d, где $c = a + b$, $d = a - b$. Тогда

$$\sigma(c) = c, \quad \sigma(d) = d(-1). \tag{15}$$

Если же $\beta = -1$, то положим $c = a + 2b$, $d = a - 2b$. Тогда

$$\sigma(c) = c(-2), \quad \sigma(d) = d2. \tag{16}$$

В случаях (15) и (16) применима лемма 6 ($\gamma \neq \alpha$). ■

Объединяя теоремы 1 и 2 и следствие 9.4.1, получим следующую теорему.

Теорема 3. *Пусть M есть n-мерное пространство над телом T, $n > 1$. Тогда всякая подгруппа в $GL(M)$, содержащая $SL(M)$ или содержащаяся в $H(M)$, инвариантна. Если $n > 2$ или $n = 2$, но $T \neq GF(2)$, $T \neq GF(3)$, то всякая инвариантная в $GL(M)$ подгруппа содержит $SL(M)$ или содержится в центре группы $GL(M)$.*

Эта теорема позволяет получить одну серию простых групп. Обозначим символом $Z(SL(M))$ центр группы $SL(M)$, а символом $PSL(M)$ — фактор-группу $SL(M)/Z(SL(M))$.

Теорема 4. *Пусть M есть n-мерное пространство над телом T и $n > 2$ или $n = 2$, но T содержит более трех элементов. Тогда $PSL(M)$ — простая группа.*

Доказательство. Пусть Γ — истинная инвариантная подгруппа в $PSL(M)$. Тогда $\Gamma = U/Z(SL(M))$, где U — нормальный делитель в $SL(M)$, содержащий $Z(SL(M))$. По теореме 3 U содержится в центре группы $GL(M)$. Но $U \subset SL(M)$, поэтому $U = Z(SL(M))$. Отсюда следует простота группы $PSL(M)$. ■

Результаты §§ 9, 10 принадлежат Дьедонне [1]. Изложение здесь близко к изложению Артина [1].

Приведем еще без доказательства теоремы Розенберга [1] о строении $GL(M)$ для случая бесконечной размерности пространства M над телом T.

Пусть $M:T = \aleph_\delta$, $\delta \geqslant 0$, $L = \operatorname{End} M$, $G = GL(M)$, e — единица кольца L. Положим

$$\Sigma = \{s \in L \mid (s - e)^2 = 0\}.$$

Тогда Σ — система образующих группы G. Группа G совпадает со своим коммутантом.

Для кардинала $\aleph_\nu$, $0 \leqslant \nu \leqslant \delta$, положим

$$F_\nu = \{f \in L \mid \operatorname{Im} f : T < \aleph_\nu\};$$

F_ν — двусторонний идеал кольца L. Введем группы G_0 и $G_\nu(1)$: $G_0 = Z^* e + F^0$, где Z — центр тела T, $G_\nu(1) = e + F_\nu$.

Пусть N — истинный нормальный делитель группы G. Тогда либо $N \subset G_0$, либо $N = HG_\nu(1)$, где H — подгруппа группы $Z^* e$.

ГЛАВА III

НОРМАЛЬНОЕ СТРОЕНИЕ ГРУПП $GL(\Delta)$ И $GL(n, Z)$, $n > 2$

§ 11. Нормальные делители предельной полной линейной группы

1. Предельная полная линейная группа. Пусть Δ — ассоциативное кольцо с единицей 1. Отождествляя матрицу $a \in GL(n, \Delta)$ с матрицей $\mathrm{diag}[a, 1] \in GL(n+1, \Delta)$, получим бесконечную возрастающую цепь подгрупп

$$GL(1, \Delta) \subset GL(2, \Delta) \subset \ldots \subset GL(n, \Delta) \subset \ldots$$

Объединение групп этой цепи назовем *предельной полной линейной группой над кольцом* Δ и обозначим символом $GL(\Delta)$.

Таким образом, *каждый элемент* $a \in GL(\Delta)$ *принадлежит группе* $GL(n, \Delta)$ *при некотором* $n = n(a)$.

Подгруппу $SL(\Delta)$ группы $GL(\Delta)$, порожденную всеми элементарными матрицами

$$t_{ij}(\lambda) = E + e_{ij}(\lambda), \qquad \lambda \in \Delta,$$

назовем *предельной специальной линейной группой над кольцом* Δ.

Теорема 1. (Лемма Уайтхеда.) *Коммутант группы* $GL(\Delta)$ *совпадает с* $SL(\Delta)$.

Доказательство. Пусть K — коммутант группы $GL(\Delta)$. Так как каждая элементарная матрица — коммутатор (лемма 8.3), то $SL(\Delta) \subset K$. Пусть теперь x, $y \in GL(\Delta)$. Тогда для некоторого натурального n $x, y \in GL(n, \Delta)$. Очевидно, что

$$xyx^{-1}y^{-1} = \mathrm{diag}[xyx^{-1}y^{-1}, E_n] = \\ = \mathrm{diag}[x, x^{-1}]\,\mathrm{diag}[y, y^{-1}]\,\mathrm{diag}[(yx)^{-1}, yx]. \qquad (1)$$

Далее,

$$\operatorname{diag}[x, x^{-1}] = \\ = \begin{bmatrix} E_n & -x \\ 0 & E_n \end{bmatrix} \begin{bmatrix} E_n & 0 \\ x^{-1} - E_n & E_n \end{bmatrix} \begin{bmatrix} E_n & E_n \\ 0 & E_n \end{bmatrix} \begin{bmatrix} E_n & 0 \\ x - E_n & E_n \end{bmatrix}.$$

С другой стороны, матрицы вида

$$\begin{bmatrix} E_n & a \\ 0 & E_n \end{bmatrix}, \quad \begin{bmatrix} E_n & 0 \\ a & E_n \end{bmatrix}$$

являются произведениями элементарных матриц, ибо

$$\begin{bmatrix} E_n & a_1 \\ 0 & E_n \end{bmatrix} \begin{bmatrix} E_n & a_2 \\ 0 & E_n \end{bmatrix} = \begin{bmatrix} E_n & a_1 + a_2 \\ 0 & E_n \end{bmatrix}.$$

Таким образом,

$$\begin{bmatrix} E_n & a \\ 0 & E_n \end{bmatrix}, \quad \begin{bmatrix} E_n & 0 \\ a & E_n \end{bmatrix} \in SL(\Delta). \tag{2}$$

Из (1) и (2) вытекает

$$xyx^{-1}y^{-1} \in SL(\Delta), \qquad K \subset SL(\Delta).$$

Следовательно, $K = SL(\Delta)$. ■

2. Конгруэнц-подгруппа. Пусть N — двусторонний идеал кольца Δ. Очевидно, естественный гомоморфизм колец

$$\gamma_N\colon \Delta \to \Delta/N = \bar{\Delta}$$

можно продолжить до сюръективного гомоморфизма матричных колец

$$h_N\colon \Delta_n \to \bar{\Delta}_n, \qquad \|\alpha_{ij}\| \mapsto \|\bar{\alpha}_{ij}\|, \qquad \bar{\alpha}_{ij} = \gamma_N(\alpha_{ij}).$$

Этот гомоморфизм, в свою очередь, определяет гомоморфизм групп

$$g_N\colon GL(n, \Delta) \to GL(n, \bar{\Delta}), \qquad x \mapsto h_N(x).$$

Будем называть g_N *гомоморфизмом Минковского*. Ядро $CL(n, \Delta, N)$ этого гомоморфизма назовем *N-конгруэнц-подгруппой группы* $GL(n, \Delta)$.

Если $N = (0)$, то $\bar{\Delta} = \Delta$, g_N — тождественный автоморфизм. Следовательно,

$$CL(n, \Delta, (0)) = (1).$$

При $N = \Delta$ положим $GL(n, \bar{\Delta}) = 1$. Тогда

$$CL(n, \Delta, \Delta) = GL(n, \Delta).$$

Введем еще группу $E(n, \Delta, N)$, порожденную всеми элементарными матрицами из $CL(n, \Delta, N)$. Следующие три леммы принадлежат Б а с с у [1].

Л е м м а 1. *Если $n > 2$, то*

(i) $E(n, \Delta, N) \lhd SL(n, \Delta)$ *);

(ii) $E(n, \Delta, N) = (SL(n, \Delta), E(n, \Delta, N))$.

Д о к а з а т е л ь с т в о. По определению группа $E(n, \Delta, N)$ порождается всеми элементарными матрицами $t_{ij}(\mu)$, где $\mu \in N$. Согласно лемме 8.3

$$t_{ik}(\lambda)\, t_{kj}(\mu)\, t_{ik}^{-1}(\lambda)\, t_{kj}^{-1}(\mu) = t_{ij}(\lambda\mu) \in E(n, \Delta, N), \tag{3}$$

где i, j, k попарно различны. Следовательно, для $\lambda \in \Delta$, $\mu \in N$

$$t_{ik}(\lambda)\, t_{kj}(\mu)\, t_{ik}^{-1}(\lambda) \in E(n, \Delta, N). \tag{4}$$

Аналогично,

$$t_{ij}(\lambda)\, t_{kj}(\mu)\, t_{ij}^{-1}(\lambda) \in E(n, \Delta, N). \tag{5}$$

Если теперь $\alpha \neq \beta$, $(\alpha - j)(\beta - k) \neq 0$, то

$$t_{\alpha\beta}(\lambda)\, t_{kj}(\mu)\, t_{\alpha\beta}^{-1}(\lambda) = t_{kj}(\mu) \in E(n, \Delta, N). \tag{6}$$

Из (4) — (6) следует, что для любого $a \in SL(n, \Delta)$

$$a t_{kj}(\mu)\, a^{-1} \in E(n, \Delta, N), \qquad \mu \in N,$$

и, значит, $E(n, \Delta, N) \lhd SL(n, \Delta)$.

Докажем (ii). Из (i) вытекает включение

$$K = (SL(n, \Delta), E(n, \Delta, N)) \subset E(n, \Delta, N).$$

Полагая в (3) $\lambda = 1$, получим $t_{ij}(\mu) \in K$. Следовательно,

$$K = E(n, \Delta, N). \blacksquare$$

---

*) Если B — подгруппа группы A, то $B \lhd A$ означает, что B — нормальный делитель в A.

Лемма 2. $(GL(n, \Delta), CL(n, \Delta, N)) \subset E(2n, \Delta, N)$.

Доказательство. Пусть $x \in GL(n, \Delta)$, $y \in CL(n, \Delta, N)$. Тогда $y = E_n + y_1$, где y_1 — матрица над N. Введем матрицы t_1, t_2, t_3, положив

$$t_1 = \begin{bmatrix} E_n & (yx)^{-1} y_1 \\ 0 & E_n \end{bmatrix}, \qquad t_2 = \begin{bmatrix} E_n & -x^{-1}y_1 \\ 0 & E_n \end{bmatrix},$$

$$t_3 = \begin{bmatrix} E_n & 0 \\ -y^{-1}y_1x & E_n \end{bmatrix}.$$

Очевидно, что $t_1, t_2, t_3 \in E(2n, \Delta, N)$. Если

$$s = \begin{bmatrix} E_n & 0 \\ x & E_n \end{bmatrix},$$

то $s \in SL(2n, \Delta)$. Отсюда, в силу леммы 1, вытекает включение

$$t = t_1 s^{-1} t_2 s t_3 \in E(2n, \Delta, N). \tag{7}$$

Положим

$$a = \operatorname{diag}[yx, E_n], \qquad b = \operatorname{diag}[x, y].$$

Тогда

$$at_1 = \begin{bmatrix} yx & y_1 \\ 0 & E_n \end{bmatrix}, \qquad at_1s^{-1} = \begin{bmatrix} x & y_1 \\ -x & E_n \end{bmatrix},$$

$$at_1s^{-1}t_2 = \begin{bmatrix} x & 0 \\ -x & y \end{bmatrix}, \qquad at_1s^{-1}t_2s = \begin{bmatrix} x & 0 \\ y_1x & y \end{bmatrix},$$

$$at = \operatorname{diag}[x, y] = b. \tag{8}$$

В частности, из (7) и (8) вытекает, что

$$u = \operatorname{diag}[y^{-1}, y] \in E(2n, \Delta, N). \tag{9}$$

Для доказательства достаточно положить $x = y^{-1}$. Пусть теперь $c = \operatorname{diag}[xy, E_n]$. Тогда

$$cu = b. \tag{10}$$

Из (9) и (10) следует

$$y^{-1}x^{-1}yx = \operatorname{diag}[y^{-1}x^{-1}yx, E_n] = c^{-1}a = ut^{-1} \in E(2n, \Delta, N),)$$

откуда и вытекает лемма. ■

Положим теперь

$$CL(\Delta, N) = \bigcup_n CL(n, \Delta, N), \qquad E(\Delta, N) = \bigcup_n E(n, \Delta, N).$$

Лемма 3. $E(\Delta, N) = (SL(\Delta), E(\Delta, N)) = (GL(\Delta), CL(\Delta, N)) = (GL(\Delta), E(\Delta, N))$.

Доказательство. Согласно леммам 1 и 2

$$E(n, \Delta, N) = (SL(n, \Delta), E(n, \Delta, N)) \subset \subset (GL(n, \Delta), CL(n, \Delta, N)) \subset E(2n, \Delta, N).$$

Переходя к предельным группам $E(\Delta, N)$, $SL(\Delta)$, $GL(\Delta)$ и $CL(\Delta)$, получим требуемые равенства. ∎

3. Нормальные делители группы $GL(\Delta)$.

Лемма 4. *Пусть $n > 2$, H — подгруппа в $GL(n, \Delta)$, нормализуемая группой $SL(n, \Delta)$, а N — множество всех таких $\nu \in \Delta$, что хотя бы одна элементарная матрица $t_{ij}(\nu) \in H$. Тогда N — двусторонний идеал кольца Δ, а $H \supset E(n, \Delta, N)$.*

Доказательство. $t_{ij}(0) = E_n \in H$, так что $0 \in \in N$, $N \neq \varnothing$. Далее, пусть $t_{kl}(\alpha) \in H$. Для $\delta \in \Delta$ и $j \neq \neq l, k$, согласно лемме 8.3,

$$t_{kj}(\alpha\delta) = t_{kl}(\alpha)\, t_{lj}(\delta)\, t_{kl}^{-1}(\alpha)\, t_{lj}^{-1}(\delta) \in H. \tag{11}$$

Для $\gamma \in \Delta$ и $i \neq k, j$

$$t_{ij}(\gamma\alpha\delta) = t_{ik}(\gamma)\, t_{kj}(\alpha\delta)\, t_{ik}^{-1}(\gamma)\, t_{kj}^{-1}(\alpha\delta) \in H. \tag{12}$$

Следовательно, истинна импликация

$$t_{kl}(\alpha) \in H \Rightarrow t_{ij}(\gamma\alpha\delta) \in H; \quad i \neq k; \quad j \neq l, k; \quad \gamma, \delta \in \Delta. \tag{13}$$

Из (13) следует истинность импликации

$$\alpha \in N \Rightarrow \gamma\alpha\delta \in N, \qquad \gamma, \delta \in \Delta. \tag{14}$$

Кроме того, положив в (13) $\gamma = \delta = 1$, получим

$$t_{kl}(\alpha) \in H \Rightarrow t_{ij}(\alpha) \in H, \tag{15}$$

где $i \neq j$. Пусть теперь $\alpha, \beta \in N$. Тогда $t_{kl}(\alpha)$, $t_{ij}(\beta) \in H$. В силу (15)

$$t_{kl}(\beta) \in H, \quad t_{kl}(\alpha - \beta) = t_{kl}(\alpha)\, t_{kl}^{-1}(\beta) \in H, \quad \alpha - \beta \in N. \tag{16}$$

Из (14) и (16) следует, что N — двусторонний идеал кольца Δ. В силу (15) $E(n, \Delta, N) \subset H$. ∎

Теорема 2. (i) *Пусть подгруппа H группы $GL(\Delta)$ нормализуется группой $SL(\Delta)$. Тогда существует единственный двусторонний идеал $N = N(H)$ кольца Δ такой, что*

$$E(\Delta, N) \subset H \subset CL(\Delta, N). \tag{17}$$

(ii) *Всякая подгруппа H группы $GL(\Delta)$, удовлетворяющая условиям* (17), *инвариантна в* $GL(\Delta)$.

Доказательство. Пусть подгруппа H в $GL(\Delta)$ нормализуется группой $SL(\Delta)$, а N — двусторонний идеал кольца Δ, порождаемый элементами всех матриц $h-1$, $h \in H$. Тогда, очевидно, $H \subset CL(\Delta, N)$. Покажем, что

$$E(\Delta, N) \subset H. \tag{18}$$

Если $H=(1)$, то $N=(0)$, $CL(\Delta, (0))=(1)=E(\Delta, (0))$ и (18) тривиально. Будем считать $H \neq (1)$. Рассмотрим группу

$$H_n = H \cap GL(n, \Delta)$$

и двусторонний идеал N_n, порождаемый элементами матриц

$$h-E_n, \quad h \in H_n.$$

Для достаточно больших n $H_n \neq (E_n)$, $N_n \neq (0)$. Очевидно, что

$$H_n \subset \mathrm{Aff}(n, \Delta),$$

и так как H нормализуется группой $SL(\Delta)$, то $H_n = \langle H_n, (0)\rangle$ нормализуется группой $SL(n, \Delta) = \langle SL(n, \Delta, (0)\rangle$ (см. § 8). Согласно лемме 8.9

$$K = (\langle H_n, (0)\rangle, \langle E_n, \Delta^n\rangle) = \langle E_n, \Phi^n\rangle,$$

где Φ — левый идеал кольца Δ. С другой стороны, по той же лемме

$$K = \langle E_n, A\rangle, \quad A = \Sigma(h-E_n)\Delta^n, \quad h \in H_n.$$

Следовательно, Φ содержит любой элемент матрицы $h-E_n$, $h \in H_n$. Далее, так как H нормализуется группой

$$SL(\Delta) \supset \langle E_n, \Delta^n\rangle,$$

то

$$K \subset H \cap GL(n+1, \Delta) = H_{n+1}.$$

Таким образом, группа H_{n+1} содержит элементарные матрицы $t_{ij}(\nu)$, где ν — элементы матриц $h-E_n$, $h \in H_n$. В силу леммы 4

$$H_{n+1} \supset E(n+1, \Delta, N_n).$$

Переходя к предельным группам, отсюда получим (17).

Остается показать единственность $N = N(H)$ и (ii). Пусть подгруппа H группы $GL(\Delta)$ удовлетворяет условиям (17). Тогда

$$(GL(\Delta),\ E(\Delta,\ N)) \subset (GL(\Delta),\ H) \subset (GL(\Delta),\ CL(\Delta,\ N)).$$

Отсюда и из леммы 3 получаем

$$(GL(\Delta),\ H) = E(\Delta,\ N) \subset H. \tag{19}$$

Из (19) вытекает единственность N и инвариантность группы H в $GL(\Delta)$. ■

О строении $\operatorname{Aut} M$, где M — свободный модуль с базисом произвольной бесконечной мощности над коммутативным кольцом, см. статью Максвелла [1].

4. Теорема Минковского. Возвратимся снова к конгруэнц-подгруппе $CL(n, \Delta, N)$.

Теорема 3. (Теорема Минковского.) *Пусть Δ — гауссово кольцо нулевой характеристики, q — такой неразложимый элемент этого кольца, что $q \nmid 2$ и для всякого простого целого рационального p $q^2 \nmid p$, а $N = q\Delta$. Тогда $CL(n, \Delta, N)$ — группа без кручения.*

Доказательство. Пусть в группе $CL(n, \Delta, N)$ есть отличные от E_n элементы конечного порядка. Тогда в ней найдется элемент a простого порядка p. Очевидно, что

$$a = E_n + qb, \qquad b \in \Delta_n, \qquad b \neq 0.$$

Далее,

$$a^p = (E_n + qb)^p = \\ = E_n + pqb + \frac{p(p-1)}{2} q^2 b^2 + \ldots + q^p b^p = E_n.$$

Отсюда

$$pb + \frac{p(p-1)}{2} qb^2 + \ldots + q^{p-1} b^p = 0. \tag{20}$$

Возможны два случая: $q \nmid p$ и $q \mid p$. В первом случае из (20) вытекает, что $q \mid b$, т. е. q делит каждый элемент матрицы b. Пусть

$$q^\alpha \mid b, \qquad q^{\alpha+1} \nmid b, \qquad \alpha > 0. \tag{21}$$

В силу (21) слагаемые в (20), начиная со второго, делятся на $q^{2\alpha+1}$. Следовательно, pb и b делятся на $q^{2\alpha+1}$. Последнее противоречит (21). Во втором случае, в силу условия теоремы, $p > 2$, $q^2 \nmid p$. Следовательно, $p = qr$,

$r \in \Delta$, $(r, q) = 1$. Формуле (20) можно придать следующий вид:

$$qrb = q^2 b^2 c, \tag{22}$$

где $c \in \Delta_n$. Так как $(r, q) = 1$, то из (22) следует, что $q \mid b$. Пусть $q^\alpha \mid b$, $q^{\alpha+1} \nmid b$. Тогда правая часть равенства (22) делится на $q^{2\alpha+2}$, а левая не делится на $q^{\alpha+2}$. Это противоречие и доказывает теорему во втором случае. ■

Следствие 1. *Пусть Δ и $N = q\Delta$ имеют тот же смысл, что и в теореме 3. Тогда $CL(\Delta, N)$ — группа без кручения.*

Следствие 2. *Периодические подгруппы группы $GL(n, Z)$ над кольцом Z целых рациональных чисел конечны. Для любого простого $p > 2$ и любой конечной подгруппы H группы $GL(n, Z)$ в $GL(n, Z/p)$ существует группа, изоморфная H.*

Следствие 3. *Пусть Σ — поле нулевой характеристики, а x — переменная. Тогда всякая периодическая подгруппа группы $GL(n, \Sigma[x])$ изоморфна некоторой подгруппе группы $GL(n, \Sigma)$.*

Для доказательства достаточно в теореме 3 положить $\Delta = \Sigma[x]$, $q = q(x) = x$.

Следствие 4. *Пусть Σ — поле нулевой характеристики, а $x_1, \ldots, x_m$ — независимые переменные. Тогда всякая конечная подгруппа группы $GL(n, \Sigma(x_1, \ldots, x_m))$ изоморфна некоторой подгруппе группы $GL(n, \Sigma)$.*

Доказательство. Рассмотрим сперва конечную подгруппу G группы $GL(n, \Sigma(x))$. Согласно теореме Бернсайда (теорема 8.3) G изоморфна некоторой подгруппе группы $GL(n, \Sigma[x])$, а в силу следствия 3 — некоторой подгруппе группы $GL(n, \Sigma)$. Отсюда индукцией по числу переменных получаем требуемое. ■

Теорема 4. Пусть Δ — *дедекиндово кольцо нулевой характеристики, а $\mathfrak{P}$ — такой простой идеал кольца Δ, что $\mathfrak{P} \not\supset (2)$ и для любого простого $p \in Z$ $\mathfrak{P}^2 \not\supset (p)$. Тогда $CL(n, \Delta, \mathfrak{P})$ — группа без кручения.*

Доказательство. Пусть $a \in CL(n, \Delta, \mathfrak{P})$ — элемент простого порядка p. Тогда

$$a = E_n + b, \qquad b \in \mathfrak{P}_n, \qquad b = \| \beta_{ij} \| \neq 0, \qquad \beta_{ij} \in \mathfrak{P}$$

и

$$pb + \frac{p(p-1)}{2} b^2 + \ldots + b^p = 0, \tag{23}$$

$b^k = \|\beta_{ij}^k\|$, $\beta_{ij}^k \in \mathfrak{P}$. Пусть число l таково, что для всех i, j $\beta_{ij} \in \mathfrak{P}^l$, но для некоторой пары μ, ν $\beta_{\mu\nu} \notin \mathfrak{P}^{l+1}$. Из (23) находим

$$p\beta_{\mu\nu} + C_p^2\beta_{\mu\nu}^2 + \ldots + \beta_{\mu\nu}^p = 0. \tag{24}$$

Возможны два случая: $\mathfrak{P} \not\supset (p)$ и $\mathfrak{P} \supset (p)$. В первом случае

$$p\beta_{\mu\nu} \in \mathfrak{P}^l \setminus \mathfrak{P}^{l+1},$$

что противоречит (24). Во втором случае

$$p \neq 2, \qquad p\beta_{\mu\nu} \in \mathfrak{P}^{l+1} \setminus \mathfrak{P}^{l+2},$$

а остальные слагаемые (24) принадлежат идеалу $\mathfrak{P}^{2l+1}$. Это противоречие и доказывает теорему. ■

В связи с теоремами 3 и 4 представляется интересным выяснить, для каких колец Δ и идеалов N группа $CL(n, \Delta, N)$ является группой без кручения.

§ 12. Нормальные делители группы $GL(n, Z)$ при $n > 2$. Подгруппы конечного индекса

1. Предварительные леммы. Пусть сперва Δ — произвольное ассоциативное кольцо с единицей. Докажем две леммы (см. Басс [1]).

Лемма 1. *Пусть $n > 2$, H — подгруппа в $GL(n, \Delta)$, нормализуемая группой $SL(n, \Delta)$ и удовлетворяющая одному из следующих условий*):*

(i) $H \cap \langle E_{n-1}, \Delta^{n-1}\rangle \neq (E_n)$;

(ii) $H \cap Z(\Delta)^* \langle E_{n-1}, \Delta^{n-1}\rangle \not\subset Z(\Delta)^* E_n$, *где* $Z(\Delta)^*$ — *мультипликативная группа центра кольца* Δ;

(iii) *существуют такие* $h \in H$, $\mu \in Z(\Delta)^*$, *что матрица* $h - \mu E_n$ *имеет нулевую строку или нулевой столбец, но* $h - \mu E_n \neq 0$;

(iv) *существует такая матрица* $h \in H$, $h \neq \gamma E_n$, $\gamma \in Z(\Delta)^*$, *что при всяком* $\delta \in \Delta$ *матрицы* $t_{12}(\delta)$ *и* h *перестановочны.*

Тогда

$$H \supset E(n, \Delta, N), \qquad N \neq (0).$$

---

*) См. конец § 8.

Доказательство. (i) Очевидно, имеет место равенство

$$H \cap \langle E_{n-1}, \Delta^{n-1}\rangle = A = \langle E_{n-1}, B\rangle,$$

где $B \neq (0)$ — подгруппа аддитивной группы модуля Δ^{n-1}. Так как H нормализуется группой $SL(n, \Delta) \supset \supset \langle SL(n-1, \Delta), (0)\rangle$ и $\langle E_{n-1}, \Delta^{n-1}\rangle$ нормализуется группой $\langle SL(n-1, \Delta), (0)\rangle$, то и $A = \langle E_{n-1}, B\rangle$ нормализуется группой $\langle SL(n-1, \Delta), (0)\rangle$. Согласно леммам 8.7 и 8.8

$$B = \Phi^{n-1},$$

$\Phi \neq 0$ — левый идеал кольца Δ. Поэтому для $\varphi \in \Phi$ $t_{1n}(\varphi) \in A \subset H$. Тогда по лемме 11.4

$$H \supset E(n, \Delta, N), \qquad N \neq (0).$$

(ii) Пусть

$$\mu \in Z(\Delta)^*, \qquad d = \mu\langle E_{n-1}, a\rangle \in H, \qquad a \neq (0).$$

Тогда для $s \in SL(n-1, \Delta)$

$$\langle s, 0\rangle d \langle s, 0\rangle^{-1} = \mu\langle E_{n-1}, sa\rangle = d_1 \in H.$$

Очевидно, матрицу s можно выбрать так, что $sa \neq a$. Тогда

$$dd_1^{-1} \neq E_n, \qquad dd_1^{-1} \in H \cap \langle E_{n-1}, \Delta^{n-1}\rangle,$$

т. е. группа H удовлетворяет условию (i).

(iii) Можно считать, что матрица $h - \mu E_n$ имеет нулевую строку,

$$h \in H, \qquad \mu \in Z(\Delta)^*, \qquad h \neq \mu E_n.$$

В самом деле, если бы столбец матрицы $h - \mu E_n$ был нулевым, то мы перешли бы к группе ${}^tH$, получающейся из H транспонированием всех ее матриц, так как ${}^tH$ нормализуется группой $SL(n, \Delta)$, а ${}^tE(n, \Delta, N) = E(n, \Delta, N)$. Итак, пусть одна из строк матрицы $h - \mu E_n$ нулевая. Трансформируя $h - \mu E_n$ элементом из группы $SL(n, \Delta)$, можно добиться того, чтобы нулевой была последняя строка. Поэтому можно считать, что $h \in Z(\Delta)^*\mathrm{Aff}(n-1, \Delta)$. Рассмотрим пересечение

$$H \cap Z(\Delta)^* \,\mathrm{Aff}\,(n-1, \Delta) = A.$$

Так как $h \neq \mu E_n$, то $A \not\subset Z(\Delta)^* E_n$. Если $A \subset Z(\Delta)^* \langle E_{n-1}, \Delta^{n-1}\rangle$, то группа H удовлетворяет условию (ii). Если же $A \not\subset Z(\Delta)^* \langle E_{n-1}, \Delta^{n-1}\rangle$, то рассмотрим взаимный коммутант

$$K = (A, \langle E_{n-1}, \Delta^{n-1}\rangle) = (A, Z(\Delta)^* \langle E_{n-1}, \Delta^{n-1}\rangle).$$

Ясно, что $K \subset H$, ибо $\langle E_{n-1}, \Delta^{n-1}\rangle \subset SL(n, \Delta)$. Согласно теореме 7.2. $Z(\Delta)^* \langle E_{n-1}, \Delta^{n-1}\rangle$ — максимальная абелева подгруппа в $GL(n, \Delta)$, поэтому $K \neq (E_n)$. Очевидно,

$$K = (A_1, \langle E_{n-1}, \Delta^{n-1}\rangle),$$

где A_1 — некоторая подгруппа в $\mathrm{Aff}(n-1, \Delta)$. Следовательно,

$$K \subset \langle E_{n-1}, \Delta^{n-1}\rangle, \qquad K \neq (E_n),$$

т. е. группа H удовлетворяет условию (i).

(iv) Пусть $h \in H$ и для любого $\delta \in \Delta$

$$t_{12}(\delta) h = h t_{12}(\delta).$$

Тогда первый столбец матрицы h имеет вид

$$\begin{bmatrix} \gamma \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \qquad \gamma \in Z(\Delta)^*,$$

т. е. группа H удовлетворяет условию (iii). ■

Лемма 2. *Пусть $n > 2$, H — подгруппа в $GL(n, \Delta)$, нормализуемая группой $SL(n, \Delta)$ и содержащая матрицу h, не принадлежащую центру группы $GL(n, \Delta)$ и такую, что хотя бы один из ее элементов — нуль. Тогда*

$$H \supset E(n, \Delta, N), \qquad N \neq (0).$$

Доказательство. Пусть $h = \|\gamma_{ij}\|$, $\gamma_{kl} = 0$. Возможны два случая: $k \neq l$ и $k = l$. В первом случае, согласно лемме 8.5, в группе $SL(n, \Delta)$ есть такая матрица c, что

$$chc^{-1} = \|\alpha_{ij}\|, \qquad \alpha_{n1} = 0.$$

Если же $k = l$, то в $SL(n, \Delta)$ есть такая матрица c, что

$$chc^{-1} = \|\alpha_{ij}\|, \qquad \alpha_{11} = 0.$$

Следовательно, можно считать $\gamma_{n1} = 0$ или $\gamma_{11} = 0$. Учитывая лемму 1 (iv), достаточно рассмотреть тот случай, когда есть такое $\alpha \in \Delta$, что

$$r = ht_{12}(\alpha) h^{-1} t_{12}^{-1}(\alpha) \neq E_n.$$

Очевидно, $r \in H$. Далее,

$$ht_{12}(\alpha) h^{-1} = E_n + he_{12}\alpha h^{-1} = E_n + u\alpha v,$$

где u — первый столбец матрицы h, а v — вторая строка матрицы h^{-1}. Следовательно,

$$r = t_{12}^{-1}(\alpha) + u\alpha v t_{12}^{-1}(\alpha) = t_{12}^{-1}(\alpha) + uc, \qquad c = \alpha v t_{12}^{-1}(\alpha).$$

Теперь рассмотрим отдельно два случая: 1) $\gamma_{n1} = 0$ и 2) $\gamma_{11} = 0$. Очевидно, в первом случае последняя строка матрицы uc нулевая. Следовательно, последняя строка матрицы r имеет вид $[0 \ldots 0\,1]$ и группа H удовлетворяет условию (iii) предыдущей леммы. Если же $\gamma_{11} = 0$, то первая строка матрицы r совпадает с первой строкой матрицы $t_{12}^{-1}(\alpha)$, т. е. имеет вид $[1\ {-\alpha}\ 0 \ldots 0]$. Ясно, что $r = \|\rho_{ij}\|$ — нецентральный элемент и $\rho_{13} = 0$. Мы пришли к случаю, когда $k \neq l$. ■

Далее Δ — *коммутативное евклидово кольцо.*

Лемма 3. *Для произвольного столбца*

$$a = \begin{bmatrix} \alpha_1 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_n \end{bmatrix} \in \Delta^n, \qquad n > 1,$$

в группе $SL(n, \Delta)$ есть такая матрица s, что

$$sa = \begin{bmatrix} \mu \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \qquad \mu\Delta = \alpha_1\Delta + \ldots + \alpha_n\Delta.$$

Доказательство. Если $a = (0)$, то $\mu = 0$, $s = E_n$. Пусть теперь $a \neq (0)$. Очевидно,

$$t_{ij}(\delta)\, a = \begin{bmatrix} \alpha_1 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_{i-1} \\ \alpha_i + \delta\alpha_j \\ \alpha_{i+1} \\ \cdot \\ \cdot \\ \cdot \\ \alpha_n \end{bmatrix}. \tag{1}$$

Пусть O — орбита группы $SL(n, \Delta)$, содержащая столбец a. Среди отличных от нуля координат векторов орбиты O пусть μ — наименьшая по норме. Если b — вектор из O, одна из координат которого есть μ, то, в силу (1), все его координаты делятся на μ. Значит, O содержит вектор

$$\begin{bmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ \mu \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix},$$

а с ним и вектор

$$\begin{bmatrix} \mu \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}.$$

Кроме того, из (1) следует, что для $s \in SL(n, \Delta)$ координаты векторов a и sa порождают один и тот же идеал кольца Δ. Значит, $\alpha_1\Delta + \ldots + \alpha_n\Delta = \mu\Delta$. ■

Следствие 1. *Векторы a и b из Δ^n тогда и только тогда входят в одну орбиту группы $SL(n, \Delta)$, когда координаты вектора a и координаты вектора b порождают один и тот же идеал кольца Δ.*

Доказательство. Необходимость, очевидно, следует из леммы 3. Докажем достаточность. Пусть

$$a = \begin{bmatrix} \alpha_1 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_n \end{bmatrix}, \quad b = \begin{bmatrix} \beta_1 \\ \cdot \\ \cdot \\ \cdot \\ \beta_n \end{bmatrix},$$

$$\alpha_1\Delta + \ldots + \alpha_n\Delta = \beta_1\Delta + \ldots + \beta_n\Delta.$$

Тогда, согласно лемме 3, в группе $SL(n, \Delta)$ есть такие матрицы s_1 и s_2, что

$$s_1 a = \begin{bmatrix} \mu_1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad s_2 b = \begin{bmatrix} \mu_2 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad (\mu_1) = (\mu_2).$$

Если $\mu_1 = 0$, то $\mu_2 = 0$, $a = b = 0$. Пусть $\mu_1 \neq 0$. Тогда

$$\mu_2 = \varepsilon\mu_1, \quad \varepsilon \in \Delta^*.$$

Пусть $O(a)$ и $O(b)$ — орбиты группы $SL(n, \Delta)$, содержащие, соответственно, a и b. Далее,

$$t_{21}(\varepsilon) \begin{bmatrix} \mu_1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} = \begin{bmatrix} \mu_1 \\ \mu_2 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} \in O(a);$$

$\mu_1 = \varepsilon^{-1}\mu_2$, $\varepsilon^{-1} \in \Delta^*$. Следовательно,

$$\begin{bmatrix} \mu_2 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} \in O(a),$$

т. е. $O(a) = O(b)$. ■

Лемма 4. *Пусть* $n>2$, $h=\|\gamma_{ij}\|\in\Delta_n$. *Тогда в группе* $SL(n, \Delta)$ *найдется такая матрица* s, *что*

$$shs^{-1}=g=\|\beta_{ij}\|,$$

где

$$\begin{bmatrix}\beta_{21}\\ \beta_{31}\\ \cdot\\ \cdot\\ \cdot\\ \beta_{n1}\end{bmatrix}=\begin{bmatrix}\mu\\ 0\\ \cdot\\ \cdot\\ \cdot\\ 0\end{bmatrix},\quad \mu\Delta=\gamma_{21}\Delta+\ldots+\gamma_{n-1}\Delta,\quad \beta_{11}=\gamma_{11}. \qquad (2)$$

Доказательство. Согласно лемме 3 найдется такая матрица $s_1\in SL(n-1, \Delta)$, что

$$s_1\begin{bmatrix}\gamma_{21}\\ \cdot\\ \cdot\\ \cdot\\ \gamma_{n1}\end{bmatrix}=\begin{bmatrix}\mu\\ 0\\ \cdot\\ \cdot\\ \cdot\\ 0\end{bmatrix}.$$

Полагая

$$s=\operatorname{diag}[1, s_1],$$

получим равенства (2), $s\in SL(n, \Delta)$. ■

Теорема 1. *Пусть* $n>2$, H — *подгруппа в* $GL(n, \Delta)$, *нормализуемая группой* $SL(n, \Delta)$ *и не содержащаяся в группе* $Z(\Delta)^*E_n$. *Тогда* $H\supset E(n, \Delta, N)$ *для некоторого ненулевого идеала* N *кольца* Δ.

Доказательство. Пусть $g\in H$ и $g\notin Z(\Delta)^*E_n$. Тогда, согласно лемме 4, в группе H есть матрица

$$h=\|\gamma_{ij}\|=sgs^{-1},\quad s\in SL(n, \Delta),$$

такая, что $\gamma_{n1}=0$. Ясно, что $h\notin Z(\Delta)^*E_n$. Из леммы 2 тогда следует, что $H\supset E(n, \Delta, N)$, $N\neq(0)$. ■

2. **Группа $CSL(n, Z, N)$.** Пусть Δ — ассоциативное кольцо с единицей, а N — его двусторонний идеал. Введем группу $CSL(n, \Delta, N)$, положив

$$CSL(n, \Delta, N)=CL(n, \Delta, N)\cap SL(n, \Delta).$$

Очевидно, $CSL(n, \Delta, N)$ — нормальный делитель в $SL(n, \Delta)$ и в $GL(n, \Delta)$. Из определения группы $CSL(n, \Delta, N)$ следует включение $E(n, \Delta, N)\subset\subset CSL(n, \Delta, N)$.

Ниже будем рассматривать случай, когда Δ совпадает с кольцом Z целых рациональных чисел. По определению $SL(n, Z)$ — группа матриц, порожденная всеми элементарными матрицами

$$t_{ij}(\lambda), \qquad \lambda \in Z.$$

Так как

$$t_{ij}(\lambda) = (t_{ij}(1))^{\lambda},$$

то *группа $SL(n, Z)$ порождается $n(n-1)$ элементарными матрицами вида $t_{ij}(1)$, $i, j = 1, \ldots, n$.*

Теорема 2. *$SL(n, Z)$ есть группа всех $n \times n$-матриц над кольцом Z с определителем, равным* 1.

Доказательство. Так как $\det t_{ij}(\lambda) = 1$, то $\det g = 1$ для любой матрицы $g \in SL(n, Z)$. С другой стороны, пусть $h \in Z_n$ и $\det h = 1$. С помощью элементарных преобразований, т. е. умножая справа или слева на элементарные матрицы, матрицу h можно привести к виду

$$t_1 h t_2 = \operatorname{diag}[\pm 1, \ldots, \pm 1] = b, \qquad t_1, t_2 \in SL(n, Z),$$

где -1 фигурирует на диагонали матрицы b четное число раз. Покажем, что

$$b \in SL(n, Z).$$

Для этого рассмотрим матрицу $c = \operatorname{diag}[-1, 1, \ldots, 1, -1]$. Применяя к ней элементарные преобразования, будем последовательно получать

$$\begin{bmatrix} -1 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 0 \\ . & . & . & . & . \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 0 \\ . & . & . & . & . \\ 0 & 0 & \ldots & 1 & 0 \\ -1 & 0 & \ldots & 0 & -1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 0 \\ . & . & . & . & . \\ 0 & 0 & \ldots & 1 & 0 \\ -1 & 0 & \ldots & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 0 \\ . & . & . & . & . \\ 0 & 0 & \ldots & 1 & 0 \\ -1 & 0 & \ldots & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ . & . & . & . & . \\ 0 & 0 & \ldots & 1 & 0 \\ -1 & 0 & \ldots & 0 & 1 \end{bmatrix}, \quad E_n.$$

Отсюда вытекает, что $c \in SL(n, Z)$. Следовательно, и $h \in SL(n, Z)$. ■

Рассмотрим теперь $CSL(n, Z, N) = CL(n, Z, N) \cap \cap SL(n, Z)$. На множестве $CSL(n, Z, N)$ определим бинарное отношение R, положив для g, $h \in CSL(n, Z, N)$ gRh, если h получается из g применением конечного числа операций трех следующих видов: умножение на элемент из группы $E(n, Z, N)$ справа или слева, трансформирование элементом из $SL(n, Z)$. Очевидно, R — *отношение эквивалентности.*

Лемма 5 (Бреннер [1]). *Пусть $n > 2$. Тогда для любой матрицы $a = \|\alpha_{ij}\| \in CSL(n, Z, N)$ существует такая матрица*

$$b = \operatorname{diag}[c, 1], \qquad c \in CSL(n-1, Z, N), \tag{3}$$

что aRb.

Доказательство. Если $N = Z$, то $CL(n, Z, N) = GL(n, Z)$, $CSL(n, Z, N) = SL(n, Z) = E(n, Z, N)$ и лемма тривиальна. Тривиальна она и при $N = (0)$, ибо $CL(n, Z, (0)) = CSL(n, Z, (0)) = E(n, Z, (0)) = (E_n)$. Пусть теперь $N = (\nu)$, $\nu \in Z$, $\nu > 1$. Лемма почти очевидна, если при некотором i, $1 \leqslant i \leqslant n$, $\alpha_{ii} = 1$. В самом деле, при $k \neq i$ $\alpha_{ki} \in N$ и, значит,

$$t_{ki}(\alpha_{ki}) \in E(n, Z, N).$$

С другой стороны, пусть

$$d = t_{ki}(-\alpha_{ki})a.$$

Ясно, что на позиции (k, i) матрицы d расположен нуль. Таким образом, умножая матрицу a слева на матрицы из группы $E(n, Z, N)$, можно обратить в нуль все недиагональные элементы i-го столбца. Таким же приемом можно обратить в нуль все недиагональные элементы i-й строки. Наконец, согласно лемме 8.5, в группе $SL(n, Z)$ есть матрица, трансформирующая полученную матрицу к виду (3).

Пусть теперь матрица $r = \|\rho_{ij}\| \in CSL(n, Z, N)$ удовлетворяет условиям

$$(\rho_{21}\nu^{-1}, \rho_{32}\nu^{-1}) = 1, \qquad \rho_{31} = 0 \tag{4}$$

(здесь в левой части первого равенства используется обычная запись наибольшего общего делителя двух чисел). Тогда существует такая матрица r_1 с 1 на позиции (2,2), что rRr_1. В самом деле, $\rho_{22}=1+\nu\lambda$, а из (4) вытекает существование таких целых δ_1 и δ_2, что

$$\nu\lambda=\rho_{21}\delta_1+\rho_{32}\delta_2. \qquad (5)$$

Если теперь

$$t=t_{12}(\delta_1)\,t_{23}(-\delta_2), \qquad r_1=trt^{-1},$$

то rRr_1 и, в силу (5), на позиции (2,2) матрицы r_1 расположена 1.

Для доказательства леммы остается показать существование матрицы

$$r=\|\rho_{ij}\|,$$

удовлетворяющей условиям (4) и такой, что aRr. При этом можно считать $\alpha_{11}\neq\pm1$. Тогда наибольший общий делитель недиагональных элементов первого столбца матрицы a имеет вид $\mu=\lambda\nu>0$. Так как $\det a=1$, то

$$(\alpha_{11}, \lambda)=1.$$

Согласно лемме 4 матрица a сопряжена в группе $SL(n,Z)$ с матрицей

$$f=\|\gamma_{ij}\|, \qquad \gamma_{11}=\alpha_{11}, \qquad \gamma_{21}=\lambda\nu, \qquad \gamma_{i1}=0 \text{ для } i>2.$$

Очевидно, что существует $i>1$ такое, что $\gamma_{3i}\neq 0$. Поэтому можно считать

$$\gamma_{32}\neq 0.$$

Так как

$$(\gamma_{11}, \lambda)=(\alpha_{11}, \lambda)=1,$$

то, по теореме Дирихле о простых числах в арифметической прогрессии, существует такое $\gamma\in Z$, что

$$(\gamma_{11}\gamma+\lambda, \ \gamma_{32}\nu^{-1})=1.$$

Положим

$$r=\|\rho_{ij}\|=t_{21}(\gamma_\nu)f.$$

Тогда fRr и

$$\rho_{21}=\gamma_{21}+\gamma_{11}\gamma\delta=\lambda\nu+\gamma_{11}\gamma\nu=(\gamma_{11}\gamma+\lambda)\,\nu,$$
$$\rho_{32}=\gamma_{32}, \qquad \rho_{31}=0.$$

В силу выбора γ

$$(\rho_{32}\nu^{-1}, \ \rho_{21}\nu^{-1})=1.$$

Следовательно, aRr и r удовлетворяет условиям (4). ■

Лемма 6. *Пусть* $n > 2$. *Тогда истинна следующая импликация*:

$$E(n, Z, N) \neq CSL(n, Z, N) \Rightarrow \\ \Rightarrow E(n-1, Z, N) \neq CSL(n-1, Z, N).$$

Доказательство. Пусть

$$CSL(n, Z, N) \neq E(n, Z, N). \tag{6}$$

Тогда $D = CSL(n, Z, N) \setminus E(n, Z, N) \neq \varnothing$. Пусть $a \in D$ и aRb. Так как обе части неравенства (6) инвариантны в группе $SL(n, Z)$, то $b \in D$. Согласно лемме 5 существует матрица b вида $b = \operatorname{diag}[c, 1]$, aRb. Так как $b \notin E(n, Z, N)$, то $c \notin E(n-1, Z, N)$. Следовательно, $c \in CSL(n-1, Z, N) \setminus E(n-1, Z, N)$. ■

3. Совпадение групп $E(3, Z, N)$ и $CSL(3, Z, N)$. Введем естественный гомоморфизм

$$f\colon SL(3, Z) \to SL(3, Z)/E(3, Z, N)$$

и положим $\Gamma = CSL(3, Z, N)$.

Лемма 7. $f(\Gamma)$ *содержится в центре группы* $\operatorname{Im} f$.

Доказательство. Если gRh и $f(h)$ принадлежит центру C группы $\operatorname{Im} f$, то $f(g) = f(h) \in C$. Пусть $g \in \Gamma$. Тогда, согласно лемме 3, существует такая матрица

$$h = \begin{bmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \Gamma,$$

что gRh. Рассмотрим

$$h_1 = ht_{13}(1)\, h^{-1} t_{13}^{-1}(1) = \begin{bmatrix} 1 & 0 & \alpha \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{bmatrix} t_{13}(-1) = t_{13}(\alpha - 1)\, t_{23}(\gamma).$$

Так как $\alpha - 1$, $\gamma \in N$, то $h_1 \in E(3, Z, N)$. Таким же путем устанавливается принадлежность группе $E(3, Z, N)$ и других коммутаторов $\bar{h}$ вида

$$ht_{ij}(1)\, h^{-1} t_{ij}^{-1}(1),$$

где $(i, j) \neq (1, 2)$ или $(2, 1)$. Поэтому $f(\bar{h}) = E(3, Z, N)$, $f(h)$ перестановочно с $f(t_{ij}(1))$. Далее,

$$t_{12}(1) = t_{13}(1)\, t_{32}(1)\, t_{13}(-1)\, t_{32}(-1),$$
$$t_{21}(1) = t_{23}(1)\, t_{31}(1)\, t_{23}(-1)\, t_{31}(-1),$$

так что группа $SL(3, Z)$ порождается матрицами $t_{ij}(1)$, где $(i, j) \neq (1, 2)$ или $(2, 1)$. Поэтому $f(h) \in C$. Следовательно, и $f(g) \in C$. ∎

Лемма 8. *Пусть*

$$x = \begin{bmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \Gamma, \qquad y = f(x),$$

а $k \geqslant 1$ — целое число. Тогда в группе Γ есть такая матрица x_k вида

$$x_k = \begin{bmatrix} \alpha & \beta^k & 0 \\ (-1)^{k+1}\gamma^k & \delta_k & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

что $f(x_k) = y^k$.

Доказательство. Воспользуемся индукцией по числу k. Для $k = 1$ лемма верна, $x_1 = x$, $\delta_1 = \delta$. Пусть лемма верна для k, докажем ее справедливость для $k + 1$. Положим

$$\bar{x} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{bmatrix} x \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} \delta & 0 & -\gamma \\ 0 & 1 & 0 \\ -\beta & 0 & \alpha \end{bmatrix}.$$

Согласно лемме 7 $f(x) \in C$. Следовательно, $f(\bar{x}) = y$. По индуктивному предположению $f(x_k\bar{x}) = f(x_k)f(\bar{x}) = y^{k+1}$. Умножая матрицу

$$x_k\bar{x} = \begin{bmatrix} \alpha\delta & \beta^k & -\alpha\gamma \\ (-1)^{k+1}\gamma^k\delta & \delta_k & (-1)^{k+2}\gamma^{k+1} \\ -\beta & 0 & \alpha \end{bmatrix}$$

последовательно на элементарные матрицы из группы $E(3, Z, N)$, получим

$$x_k\bar{x}, \quad \begin{bmatrix} 1 & \beta^k & 0 \\ (-1)^{k+1}\gamma^k\delta & \delta_k & (-1)^{k+2}\gamma^{k+1} \\ -\beta & 0 & \alpha \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ (-1)^{k+1}\gamma^k & \delta_{k+1} & (-1)^{k+2}\gamma^{k+1} \\ -\beta & \beta^{k+1} & \alpha \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & \delta_{k+1} & (-1)^{k+2}\gamma^{k+1} \\ 0 & \beta^{k+1} & \alpha \end{bmatrix}.$$

Трансформируя последнюю матрицу элементом группы $SL(3, Z)$ (лемма 8.5), получим x_{k+1}. По построению

$$f(x_{k+1}) = y^{k+1}. \blacksquare$$

Лемма 9. *Пусть*

$$x = \begin{bmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \Gamma,$$

а k таково, что $\beta^k \equiv \varepsilon (\mathrm{mod}\, \alpha)$, где $\varepsilon = \pm 1$. Тогда

$$x^k \in E(3, Z, N).$$

Доказательство. Рассмотрим $u_k = x_k t_{12}(\lambda\nu)$, $(\nu) = N$:

$$u_k = \begin{bmatrix} \alpha & \alpha\lambda\nu + \beta^k & 0 \\ \gamma' & \delta' & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Так как $x \in CSL(3, Z)$, то $\alpha = 1 + \mu\nu$, $\nu \mid \beta$. Следовательно,

$$\nu \mid \beta^k + \varepsilon\mu\nu.$$

С другой стороны,

$$\beta^k = \varepsilon + \rho\alpha, \quad \beta^k + \varepsilon\mu\nu = \varepsilon + \rho\alpha + \varepsilon(\alpha - 1) = (\rho + \varepsilon)\alpha.$$

Следовательно, $\nu \mid (\rho + \varepsilon)\alpha$, и так как $(\nu, \alpha) = 1$, то $\nu \mid \rho + \varepsilon$. Тогда $\nu\alpha \mid (\rho + \varepsilon)\alpha$, т. е.

$$\nu\alpha \mid \beta^k + \varepsilon\mu\nu.$$

Значит, уравнение

$$\alpha\lambda\nu + \beta^k = -\varepsilon\mu\nu$$

разрешимо в Z относительно λ. Подставив его решение в u_k, получим

$$u_k = \begin{bmatrix} \alpha & -\varepsilon\mu\nu & 0 \\ \gamma' & \delta' & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Далее,

$$t_{21}(-\varepsilon) u_k t_{21}(\varepsilon) = \begin{bmatrix} 1 & -\varepsilon\mu\nu & 0 \\ \gamma'' & \delta'' & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Очевидно, последняя матрица принадлежит группе $E(3, Z, N)$. Следовательно,

$$x_k \in E(3, Z, N).$$

Согласно лемме 8

$$f(x^k) = f(x_k) = E(3, Z, N), \qquad x^k \in E(3, Z, N). \blacksquare$$

Лемма 10 (Меннике [1]). $CSL(3, Z, N) = E(3, Z, N)$.

Доказательство. Пусть $x \in \Gamma$. Покажем, что $x \in E(3, Z, N)$. Так как при xRy $x \in E(3, Z, N) \Leftrightarrow y \in E(3, Z, N)$, то, в силу леммы 5, можно считать, что

$$x = \begin{bmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Для $\tau_i \in Z$

$$t_{21}^{-1}(\tau_i)\, x t_{21}(\tau_i) = \begin{bmatrix} \alpha + \tau_i\beta & \beta & 0 \\ \gamma' & \delta' & 0 \\ 0 & 0 & 1 \end{bmatrix} = x_i.$$

Если

$$\alpha_i = \alpha + \tau_i\beta,$$

а k_i — такое целое число, что

$$\beta^{k_i} \equiv \pm 1 \pmod{\alpha_i}, \tag{7}$$

то, согласно лемме 9,

$$x_i^{k_i} \in E(3, Z, N).$$

Но

$$x_i^{k_i} = t_{21}^{-1}(\tau_i)\, x^{k_i} t_{21}(\tau_i),$$

так что $x_i^{k_i} R x^{k_i}$ и, значит,

$$x^{k_i} \in E(3, Z, N). \tag{8}$$

Пусть теперь $i = 1, 2$, (k_1, k_2) — наибольший общий делитель чисел k_1 и k_2. В силу (8)

$$x^{(k_1, k_2)} \in E(3, Z, N).$$

Остается теперь доказать существование таких чисел α_1 и α_2 в прогрессии

$$\alpha + \tau\beta \tag{9}$$

и таких взаимно простых k_1 и k_2 в Z, которые удовлетворяют условиям (7).

Покажем сначала существование такого простого числа p, что

$$p \equiv -1 \pmod 4 \tag{10}$$

и p или $-p$ находится в прогрессии (9). Так как $\det x = 1$, $(\alpha, \beta) = 1$.

Пусть $\alpha \equiv -1 \pmod 4$. Тогда $(\alpha, 4\beta) = 1$, поэтому, по теореме Дирихле об арифметических прогрессиях, в прогрессии $\alpha + 4\beta\tau$ есть простое число p.

Аналогично, если $\alpha \equiv 1 \pmod 4$, то в прогрессии $-\alpha + \tau(-\beta)$ есть такое простое число p, что $p \equiv -\alpha \equiv -1 \pmod 4$. Тогда $-p$ находится в прогрессии (9).

Остается рассмотреть случай четного α. Тогда $\beta \equiv 1 \pmod 2$ и сравнение

$$\alpha + k\beta \equiv -1 \pmod 4$$

имеет единственное решение k. Рассмотрим прогрессию $\alpha + \tau\beta$, где $\tau \equiv k \pmod 4$:

$$\alpha + \tau\beta = \alpha + (4l + k)\beta = (\alpha + k\beta) + 4\beta l. \tag{11}$$

Так как $(\alpha + k\beta,\ 4\beta) = 1$, в прогрессии (11) есть простое число p.

Пусть простое число p удовлетворяет условию (10) и p или $-p$ принадлежит прогрессии (9). Пусть, далее,

$$p - 1 = 2^l q_1^{l_1} \ldots q_s^{l_s}$$

— каноническое разложение,

$$m = \beta q_1 \ldots q_s \quad \text{или} \quad m = \beta \quad \text{при} \quad p - 1 = 2^l.$$

По теореме Дирихле существует такое простое число n, что $n \equiv (-1) \pmod m$. Далее, так как $(p, m) = 1$, то существует такое простое число r, что $r \equiv -p \pmod m$. Пусть a — показатель числа β по модулю p, а k_2 — показатель числа β по модулю nr. Тогда

$$a \mid p - 1, \quad k_2 \mid \varphi(nr),$$

где $\varphi(x)$ — функция Эйлера. В силу выбора чисел n и r отсюда вытекает, что a и k_2 не имеют общих нечетных простых делителей. Так как p удовлетворяет условию (10), то a нечетно, либо при четном a нечетно $\frac{a}{2}$. Положим теперь $\alpha_1 = \pm p$, $\alpha_2 = \pm nr$ так, чтобы α_1 и α_2 принадлежали прогрессии (9). Пусть

$$k_1 = a, \text{ если } a \text{ нечетно,}$$

$$k_1 = \frac{a}{2}, \text{ если } a \text{ четно.}$$

Тогда α_1 и α_2 входят в прогрессию (9), а числа k_1 и k_2 удовлетворяют условиям (7). ■

Из лемм 6 и 10 вытекает

Теорема 3. *При* $n > 2$ $CSL(n, Z, N) = E(n, Z, N)$.

4. Нормальные делители групп $GL(n, Z)$ и $SL(n, Z)$ при $n > 2$. Подгруппы конечного индекса. Применяя к случаю $\Delta = Z$ теорему 1 и учитывая теорему 3, получим следующее утверждение:

Теорема 4 (Менникe [1]). *Пусть* $n > 2$, H — *подгруппа в* $GL(n, Z)$, *нормализуемая группой* $SL(n, Z)$ *и не содержащаяся в группе* Z^*E_n. *Тогда для некоторого ненулевого идеала* N *кольца* Z

$$H \supset CSL(n, Z, N).$$

Следствие 1. *Пусть* $n > 2$, $\Gamma = GL(n, Z)$ *или* $\Gamma = SL(n, Z)$, $H \lhd \Gamma$ *и* H *не содержится в центре группы* Γ. *Тогда* H — *подгруппа конечного индекса.*

Так как всякая подгруппа конечного индекса содержит нормальный делитель группы конечного же индекса, то из теоремы 4 вытекает

Теорема 5 (Басс, Лазар, Серр [1], Менникe [1]). *Пусть* $n > 2$, *а* G — *подгруппа группы* $SL(n, Z)$ *конечного индекса. Тогда при некотором* $N \neq (0)$

$$G \supset CSL(n, Z, N).$$

Условие $n > 2$ в теоремах 4 и 5 является существенным. Еще в 1887 году были найдены примеры нормальных делителей конечного индекса группы $SL(2, Z)$, не содержащих группу $CSL(2, Z, N)$ ни при каком $N \neq (0)$. Серию таких примеров построил Райнер в [1].

Подгруппы конечного индекса в $SL(n, \Delta)$, где $n > 2$, а Δ — кольцо целых алгебраических чисел конечного расширения поля рациональных чисел, изучаются в работе Басса, Милнора и Серра [1].

В этом случае, теорема 5 остается верной тогда и только тогда, когда для любого идеала N кольца Δ фактор-группа $C_N = CSL(n, \Delta, N)/E(n, \Delta, N)$ является единичной группой. Если поле K имеет вещественное нормирование, то $C_N = 1$ для любого идеала N. Если же поле K вполне мнимо, то C_N изоморфна некоторой подгруппе порядка $r = r(N)$ группы корней из 1, лежащих в K. В частности, если m — число корней из 1 в поле K, а m^2 делит идеал N, то $r(N) = m$.

ГЛАВА IV

ПРИВОДИМОСТЬ И ИМПРИМИТИВНОСТЬ

§ 13. Абелевы группы с операторами. Строение полупростых алгебр

Здесь приводятся, в основном без доказательств, нужные для дальнейшего изложения свойства операторных абелевых групп и теоремы о строении ассоциативных полупростых алгебр.

1. Операторная абелева группа. Пусть A — операторная абелева аддитивная группа с областью операторов Ω. Тогда по определению для любых $\omega \in \Omega$, $x \in A$ задано $\omega x \in A$, причем $\omega(a+b) = \omega a + \omega b$ для $a, b \in A$. Подгруппа B группы A называется *допустимой*, если $\omega b \in B$ для любых $\omega \in \Omega$, $b \in B$. Очевидно, что A и (0) — допустимые подгруппы группы A. Если отличная от (0) группа A обладает лишь этими двумя тривиальными допустимыми подгруппами, то A называется *операторно простой.*

Если B — допустимая подгруппа группы A, то фактор-группу A/B можно считать операторной группой с той же областью операторов Ω, положив $\omega(a+B) = \omega a + B$ для $a \in A$.

Композиционным рядом операторной группы A называется конечный ряд

$$A_0 = A \supset A_1 \supset \ldots \supset A_k = (0)$$

допустимых подгрупп, факторы которого

$$F_i = A_i/A_{i+1}, \quad i = 0, 1, \ldots, k-1,$$

операторно просты.

Пусть A и $\bar{A}$ — операторные группы с одной и той же областью операторов Ω. Будем называть A и $\bar{A}$ ***операторно изоморфными***, если существует такое **биективное** отображение $f\colon A \to \bar{A}$, что $f(x+y) = f(x) + f(y)$, $f(\omega x) = \omega f(x)$ для любых $x, y \in A$, $\omega \in \Omega$.

Если операторная группа A обладает композиционным рядом, то его факторы F_i определены однозначно с точностью до операторного изоморфизма и нумерации (теорема Жордана — Гельдера).

Предложение 1. *Пусть группа A — прямая сумма*

$$A = B_1 \dotplus \ldots \dotplus B_k \tag{1}$$

операторно простых допустимых подгрупп B_i. Тогда всякая нетривиальная допустимая подгруппа B группы A операторно изоморфна прямой сумме

$$B_{i_1} \dotplus \ldots \dotplus B_{i_r},$$

а группа A представима в виде

$$A = B \dotplus B_{i_{r+1}} \dotplus \ldots \dotplus B_{i_k},$$

где

$$i_1, \ldots, i_r, i_{r+1}, \ldots, i_k$$

— некоторая перестановка чисел $1, \ldots, k$.

Предложение 2. *Пусть*

$$A = B_1 \dotplus \ldots \dotplus B_k = C_1 \dotplus \ldots \dotplus C_l, \tag{2}$$

где

$$B_1, \ldots, B_k, \quad C_1, \ldots, C_l$$

— операторно простые допустимые подгруппы группы A. Тогда $k = l$ и при подходящей нумерации слагаемых подгруппы B_j и C_j операторно изоморфны ($j = 1, \ldots, k$).

Из этих двух предложений следует

Предложение 3. *Пусть* (2) *— два разложения группы A в прямую сумму операторно простых допустимых подгрупп, H — операторно простая допустимая подгруппа группы A, $B(H)$ — прямая сумма всех B_j из* (2), *операторно изоморфных H, а $C(H)$ — прямая сумма всех C_j из* (2), *операторно изоморфных H. Тогда $H \subset B(H)$* и $B(H) = C(H)$.

Предложение 4. *Группа A, обладающая композиционным рядом, тогда и только тогда представляется в виде прямой суммы операторно простых допустимых подгрупп, когда каждая ее допустимая операторно простая подгруппа прямо дополняема допустимой подгруппой.*

Группа A называется *разложимой*, если ее можно представить в виде прямой суммы двух нетривиальных допустимых подгрупп. В противном случае группа A называется *неразложимой.*

Предложение 5. *Операторная группа A, обладающая композиционным рядом, либо неразложима, либо — прямая сумма конечной системы неразложимых допустимых подгрупп. Если (2) — два представления группы A в виде прямой суммы неразложимых допустимых подгрупп, то $k = l$ и при подходящей нумерации слагаемых группы B_j и C_j операторно изоморфны ($j = 1, \ldots, k$).*

2. Гомоморфизмы операторных абелевых групп. Пусть операторные абелевы аддитивные группы A и B имеют одну и ту же область операторов Ω. Символом $\mathrm{Hom}(A, B)$ обозначим множество всех операторных гомоморфизмов A в B, т. е. множество всех таких отображений $h\colon A \to B$, что

$$h(x+y) = h(x) + h(y), \qquad h(\omega x) = \omega h(x)$$

для любых $x, y \in A$, $\omega \in \Omega$. Для элементов g и h из $\mathrm{Hom}(A, B)$ определим сложение, положив $(g+h)(x) = g(x) + h(x)$. Тогда, очевидно, $\mathrm{Hom}(A, B)$ станет аддитивной абелевой группой. Ясно, что для $h \in \mathrm{Hom}(A, B)$ $\mathrm{Ker}\, h$ — допустимая подгруппа группы A, а $\mathrm{Im}\, h$ — допустимая подгруппа в B.

При $B = A$ элементы из $\mathrm{Hom}(A, B) = \mathrm{Hom}(A, A)$ можно, кроме того, перемножать как отображения. Непосредственная проверка показывает, что $\mathrm{Hom}(A, A)$ — *ассоциативное кольцо с единицей.*

Лемма 1. (Лемма Шура.) *Пусть A и B — операторно простые абелевы группы с одной и той же областью операторов, а $h \in \mathrm{Hom}(A, B)$. Тогда h — либо нуль группы $\mathrm{Hom}(A, B)$, либо операторный изоморфизм.*

Доказательство. Пусть $h \neq 0$. Тогда $\mathrm{Ker}\, h \neq A$. Так как группа A операторно проста, то $\mathrm{Ker}\, h = (0)$. Так как $h \neq 0$, то $\mathrm{Im}\, h \neq (0)$. Отсюда и из операторной простоты B вытекает, что $\mathrm{Im}\, h = B$. Следовательно, h — операторный изоморфизм. ■

Следствие 1. *Если A — операторно простая группа, то $\mathrm{Hom}(A, A)$ есть тело. Если A и B — неизоморфные операторно простые группы, то $\mathrm{Hom}(A, B) = (0)$.*

Лемма 2. *Пусть A задается формулой* (1), *где B_j — операторно простые попарно операторно изоморфные группы. Тогда кольцо* $\mathrm{Hom}(A, A)$ *изоморфно полному матричному кольцу T_k над телом* $T = \mathrm{Hom}\,(B_1, B_1)$.

Доказательство. Будем считать, что A — прямая сумма k экземпляров группы

$$B = B_1,$$

и записывать $a \in A$ в виде

$$a = (a_1, \ldots, a_k), \qquad a_j \in B,$$

так что в B_j входят все элементы вида

$$(0, \ldots, 0, a_j, 0, \ldots, 0),$$

где элемент a_j находится на j-м месте. Введем k^2 операторных эндоморфизмов $\varepsilon_{\mu\nu}$, где $\mu, \nu = 1, \ldots, k$, вида

$$\varepsilon_{\mu\nu}(a_1, \ldots, a_k) = (0, \ldots, a_\nu, \ldots, 0),$$

где элемент a_ν занимает μ-е место. Например,

$$\varepsilon_{21}(a_1, \ldots, a_k) = (0, a_1, 0, \ldots, 0).$$

Пусть $T = \mathrm{Hom}(B, B)$. Для $t \in T$ положим

$$t(a_1, \ldots, a_k) = (ta_1, \ldots, ta_k).$$

Следовательно, t можно трактовать как эндоморфизм группы A. Отсюда вытекает, что любой элемент h вида

$$h = \sum_{\alpha, \beta=1}^{k} t_{\alpha\beta}\varepsilon_{\alpha\beta}, \qquad t_{\alpha\beta} \in T, \tag{3}$$

является операторным эндоморфизмом группы A.

Из определения $\varepsilon_{\mu\nu}$ следует

$$\varepsilon_{\alpha\beta}\varepsilon_{\mu\nu} = \delta_\mu^\beta \varepsilon_{\alpha\nu},$$

где δ_μ^β — символ Кронекера.

Очевидно, что

$$t\varepsilon_{\mu\nu} = \varepsilon_{\mu\nu}t, \qquad t \in T.$$

Эндоморфизмы $\varepsilon_{\alpha\beta}$ линейно независимы над T. Действительно, пусть $h = 0$. Тогда, умножая равенство (3) на $\varepsilon_{\nu\nu}$ справа и на $\varepsilon_{\mu\mu}$ слева, получим

$$t_{\mu\nu}\varepsilon_{\mu\nu} = 0.$$

Отсюда

$$t_{\mu\nu} = 0.$$

Итак, эндоморфизмы h вида (3) составляют кольцо, изоморфное полному матричному кольцу T_k.

Остается теперь показать, что любой элемент $g \in \operatorname{Hom}(A, A)$ имеет вид (3). При фиксированных g, i, j определим следующим образом отображение t_{ij}: $B \to B$. Пусть $b \in B$,

$$b_j = (0, \ldots, b, \ldots, 0), \qquad gb_j = (c_1, \ldots, c_k).$$

Тогда положим

$$t_{ij} b = c_i.$$

Очевидно, $t_{ij} \in T$. Покажем, что

$$g = \sum_{i,\, j} t_{ij} \varepsilon_{ij}. \tag{4}$$

Для $a = (a_1, \ldots, a_k) \in A$ можно написать

$$ga = g(a_1, \ldots, a_k) = \sum_{j=1}^{k} g(0, \ldots, a_j, \ldots, 0),$$

причем в каждом j-м слагаемом элемент a_j находится на j-м месте. Далее,

$$g(0, \ldots, a_j, \ldots, 0) = (t_{1j} a_j, \ldots, t_{kj} a_j).$$

Следовательно,

$$ga = \sum_{i,\, j} (0, \ldots, t_{ij} a_j, \ldots, 0),$$

где элемент $t_{ij} a_j$ расположен на i-м месте. С другой стороны,

$$t_{ij} \varepsilon_{ij}(a) = t_{ij}(0, \ldots, a_j, \ldots, 0) = (0, \ldots, t_{ij} a_j, \ldots, 0),$$

где a_j и $t_{ij} a_j$ находятся на i-м месте. Таким образом,

$$ga = \sum_{i,\, j} t_{ij} \varepsilon_{ij}(a).$$

Отсюда вытекает равенство (4). ■

Теорема 1. *Пусть A — прямая сумма*

$$A = B_{11} \dotplus \ldots \dotplus B_{1r_1} \dotplus B_{21} \dotplus \ldots \dotplus B_{2r_2} \dotplus \ldots$$
$$\ldots \dotplus B_{s1} \dotplus \ldots \dotplus B_{sr_s}$$

допустимых операторно простых групп B_{ij} таких, что $B_{i\alpha}$ и $B_{i\beta}$ при любых i, α, β операторно изоморфны, а $B_{i\alpha}$ и $B_{j\beta}$ при $i \neq j$ операторно не изоморфны. Тогда кольцо $\mathrm{Hom}(A, A)$ *есть прямая сумма s колец $R_1, \ldots, R_s$ таких, что $R_iR_j = (0)$ при $i \neq j$, кольцо R_j $(j = 1, \ldots, s)$ изоморфно полной матричной алгебре $T^j_{r_j}$ степени r_j над телом* $T^j = \mathrm{Hom}\,(B_{j1}, B_{j1})$.

Доказательство. Пусть

$$A_j = B_{j1} \dotplus \ldots \dotplus B_{jr_j}, \qquad j = 1, \ldots, s.$$

Тогда

$$A = A_1 \dotplus \ldots \dotplus A_s.$$

Для любого $h \in R = \mathrm{Hom}\,(A, A)$

$$h(A_j) \subset A_j. \tag{5}$$

Действительно, рассмотрим отображение

$$\bar{h}\colon\ B_{j\alpha} \to h(B_{j\alpha}), \qquad x \mapsto h(x), \qquad x \in B_{j\alpha}.$$

Так как h — гомоморфизм и группа $B_{j\alpha}$ операторно проста, то $h(B_{j\alpha})$ — либо (0), либо группа, операторно изоморфная $B_{j\alpha}$. Согласно предложению 3

$$h(B_{j\alpha}) \subset A_j$$

и, следовательно, верно (5).

Введем теперь эндоморфизмы π_j, $j = 1, \ldots, s$, положив

$$\pi_j\colon\ x \mapsto x_j, \qquad x \in A, \qquad x = x_1 + \ldots + x_s, \qquad x_j \in A_j.$$

Очевидно, что

$$\pi_1 + \ldots + \pi_s = 1,$$

где 1 — тождественный автоморфизм группы A. Для $R = \mathrm{Hom}\,(A, A)$ можно написать

$$R = (\pi_1 + \ldots + \pi_s) R = \pi_1 R + \ldots + \pi_s R = R_1 + \ldots + R_s,$$

где

$$R_j = \pi_j R.$$

Из включения (5) вытекает:

$$R(A_j) = A_j, \qquad \pi_i R(A_i) = A_i, \qquad \pi_i R(A_j) = (0) \quad \text{при} \quad i \neq j.$$

Следовательно, при $i \neq j$ $R_i \cap R_j = (0)$, $R_i R_j = (0)$. Отсюда

$$R = R_1 \dotplus \ldots \dotplus R_s.$$

Очевидно, что

$$R_j \mid A_j = \mathrm{Hom}(A_j, A_j).$$

Так как при $i \neq j$ $R_j(A_i) = (0)$, то

$$R_j \cong \mathrm{Hom}(A_j, A_j).$$

Отсюда и из леммы 2 следует утверждение теоремы. ■

3. Полупростые алгебры над полем. Пусть A — линейное пространство над полем Δ, и пусть на A задана операция умножения векторов, т. е. для любых a и b из A определено произведение $ab \in A$. Если A образует кольцо относительно сложения и умножения векторов, причем $(ab)\lambda = (a\lambda)b = a(b\lambda)$ для любых a, $b \in A$, $\lambda \in \Delta$, то A называется *алгеброй над полем* Δ. Если умножение векторов подчинено ассоциативному закону, то алгебра A называется *ассоциативной*. Размерность линейного пространства алгебры A называется *размерностью* (или *рангом*) алгебры A. *Идеалом* алгебры A называется всякий идеал кольца алгебры, выдерживающий умножение на элементы поля Δ.

В настоящем пункте буквой A обозначена ассоциативная алгебра конечной размерности над полем Δ, обладающая единицей e. Идеал N (левый, правый или двусторонний) алгебры A называется *нильпотентным*, если существует такое натуральное число l, что произведение l произвольных элементов из N равно нулю. Так как в A есть единица, то всякий идеал алгебры A является подпространством пространства алгебры.

Пусть R — идеал максимальной размерности над Δ среди нильпотентных идеалов алгебры A. Тогда R — двусторонний идеал A и любой нильпотентный идеал алгебры A содержится в R. Отсюда вытекает, что идеал R определяется однозначно алгеброй A. R называется *радикалом алгебры* A. Алгебра A называется *полупростой*, если ее радикал $R = (0)$. Алгебра A называется *простой*, если в A только два двусторонних идеала: A и (0).

Алгебру A удобно иногда рассматривать как абелеву операторную группу $W(A)$, область операторов которой тоже A, а результат действия оператора a из A на элемент x из A есть произведение ax. Очевидно, система всех допустимых подгрупп абелевой аддитивной группы $W(A)$ совпадает с системой всех левых идеалов алгебры A, а операторно простые подгруппы группы $W(A)$ суть минимальные левые идеалы алгебры A. Строение полупростых алгебр полностью описывается следующими теоремами.

Теорема 2. *Алгебра A тогда и только тогда полупроста, когда*

$$A = L_1 \dotplus \ldots \dotplus L_t, \tag{6}$$

где L_j, $j = 1, \ldots, t$, — минимальные левые идеалы A. Иными словами, алгебра A тогда и только тогда полупроста, когда операторная группа $W(A)$ есть прямая сумма операторно простых допустимых подгрупп.

Теорема 3. *Алгебра A тогда и только тогда полупроста, когда A представима в виде прямой суммы*

$$A = A_1 \dotplus \ldots \dotplus A_s, \tag{7}$$

где A_j — двусторонние идеалы алгебры A, $A_iA_j = (0)$ при $i \neq j$, $A_j \cong T^j_{r_j}$, T^j — тело, центр которого содержит Δ.

В силу предложения 2 слагаемые L_j в разложении (6) определяются алгеброй A однозначно с точностью до операторного изоморфизма и нумерации. Разложение (7) определяется алгеброй A однозначно с точностью до нумерации слагаемых A_j. Разложения (6) и (7) связаны следующим образом. Число слагаемых s в (7) есть число попарно операторно изоморфных слагаемых в (6). Размерности над Δ слагаемых из (6) суть числа

$$n_i = (T^i : \Delta)\, r_i, \qquad i = 1, \ldots, s,$$

ибо A_i — прямая сумма r_i операторно изоморфных минимальных левых идеалов размерности n_i.

В частности, условия простоты алгебры A имеют вид

1) *Алгебра A тогда и только тогда проста, когда*

$$A = L_1 \dotplus \ldots \dotplus L_r,$$

где L_j — попарно операторно изоморфные минимальные левые идеалы A.

2) *Алгебра A тогда и только тогда проста, когда $A \cong T_r$, где T — тело.*

4. О нильпотентных кольцах и нильпотентных группах. Пусть A — ассоциативное кольцо, а B и C — двусторонние идеалы A. *Произведением* BC называется идеал кольца A, состоящий из всех сумм вида

$$b_1c_1 + \ldots + b_tc_t,$$

где t — любое целое положительное число, $b_i \in B$, $c_i \in C$. Легко видеть, что умножение идеалов ассоциативно. Это определение позволяет ввести степени A^ν, $\nu \geqslant 1$, кольца $A : A^2 = AA$, $A^3 = AAA$ и т. д.

Пусть кольцо A *нильпотентно*, т. е. пусть для некоторого целого положительного k $A^k = 0$. Если k — наименьшее положительное число, для которого $A^k = 0$, то k называется *классом нильпотентности* кольца A. Легко видеть, что имеют место следующие строгие включения:

$$A \supset A^2 \supset \ldots \supset A^{k-1} \supset 0.$$

Пусть снова A — произвольное ассоциативное кольцо. На множестве A зададим операцию $\circ$, положив

$$a \circ b = a + b + ab, \qquad a, b \in A.$$

Очевидно, *относительно этой операции A образует полугруппу $\langle A, \circ \rangle$, единицей которой служит нуль кольца A. Полугруппа $\langle A, \circ \rangle$* называется *присоединенной* полугруппой кольца A.

Теорема 4. *Пусть A — нильпотентное кольцо класса нильпотентности k. Тогда присоединенная полугруппа $G = \langle A, \circ \rangle$ является нильпотентной группой, класс нильпотентности которой не превосходит числа $k - 1$.*

Доказательство. Для $a \in A$ имеем $a^\nu = 0$, $\nu \leqslant k$. Положим $a_1 = \sum\limits_{j=1}^{\nu-1} (-1)^j a^j$. Тогда $a \circ a_1 = a_1 \circ a = 0$, т. е. a — обратимый в G элемент. Следовательно, $G = \langle A, \circ \rangle$ является группой. Покажем, что G нильпотентна, а класс нильпотентности G не больше $k - 1$. Положим $G_0 = G$, $G_j = (G, G_{j-1})$, где $j > 0$, а (G, G_{j-1}) — взаимный коммутант. Надо доказать, что G_{k-1} является единичной группой, т. е. $G_{k-1} = 0$. Покажем, что при любом j $G_j \subset A^{j+1}$, и теорема будет доказана. Для $j = 0$ включение $G_j \subset A^{j+1}$ очевидно. Пусть $G_{j-1} \subset A^j$, $j > 0$. Далее, $G_j = (G, G_{j-1})$ порождается коммутаторами вида

$c = a \circ b \circ a_1 \circ b_1$, где $a \in G$, $b \in G_{j-1}$, $a \circ a_1 = 0$, $b \circ b_1 = 0$. Для c имеем

$$c = (a + b + ab) \circ (a_1 + b_1 + a_1 b_1) = a + b + ab + \\ + a_1 + b_1 + a_1 b_1 + (a + b + ab)(a_1 + b_1 + a_1 b_1) \equiv \\ \equiv a + b + a_1 + b_1 + (a + b)(a_1 + b_1) \equiv \\ \equiv a + a_1 + aa_1 + b + b_1 + bb_1 \pmod{A^{j+1}}.$$

Следовательно, $a \circ b \circ a_1 \circ b_1 = c \in A^{j+1}$, $G_j \subset A^{j+1}$. ■

Пусть теперь Δ — произвольное ассоциативное кольцо с единицей. В кольце Δ_n выделим подкольцо $N(n, \Delta)$ всех матриц вида

$$a = \begin{bmatrix} 0 & \alpha_{12} & \alpha_{13} & \ldots & \alpha_{1n} \\ 0 & 0 & \alpha_{23} & \ldots & \alpha_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & \alpha_{n-1, n} \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}, \qquad \alpha_{ij} \in \Delta.$$

Как легко видеть, произведение любых n матриц из $N(n, \Delta)$ равно нулю. С другой стороны, $e_{12}e_{23} \ldots e_{n-1, n} = e_{1n} \neq 0$. Следовательно, $N(n, \Delta)$ — нильпотентное кольцо класса нильпотентности n.

Теорема 5. *$G = E_n + N(n, \Delta)$ — нильпотентная группа класса $n - 1$.*

Доказательство. Отображение f: $N(n, \Delta) \to E_n + N(n, \Delta)$, где $f(x) = E_n + x$, является изоморфизмом присоединенной группы кольца $N(n, \Delta)$ и группы G. Действительно, f биективно, и $f(x \circ y) = f(x + y + xy) = E_n + x + y + xy = (E_n + x)(E_n + y) = f(x) f(y)$. Следовательно, по теореме 4, группа G нильпотентна и класс нильпотентности G не больше $n - 1$. С другой стороны, если положить $t_{ij}(1) = t_{ij}$, то $t_{13} = (t_{12}, t_{23}) \in G_1$, $t_{14} = (t_{13}, t_{34}) \in G_2$, $\ldots$, $t_{1n} = (t_{1, n-1}, t_{n-1, n}) \in G_{n-2}$, где $G_0 = G$, $G_j = (G, G_{j-1})$. Следовательно, $G_{n-2} \neq E_n$; группа G нильпотентна класса $n - 1$. ■

Если в качестве кольца Δ взять тело T, то верна

Теорема 6. *Пусть N — нильпотентное подкольцо кольца T_n. Тогда в $GL(n, T)$ найдется такой элемент d, что*

$$d^{-1} N d \subset N(n, T).$$

Доказательство. T_n будем трактовать как кольцо эндоморфизмов пространства T^n. Пусть $N^k = 0$,

$N^{k-1} \neq 0$, $k > 1$. Введем подпространство Q_ν, где $0 < \nu < k$, пространства T^n, взяв в качестве Q_ν линейную T-оболочку множества векторов $N^\nu T^n$. Очевидно, что

$$Q_{k-1} \subset Q_{k-2} \subset \ldots \subset Q_1 \subset T^n = Q_0.$$

Из построения Q_ν следует, что для $g \in N$ и $\nu < k-1$ имеем

$$g(Q_\nu) \subset Q_{\nu+1}, \qquad g(Q_{k-1}) = 0, \qquad N^{k-\nu} Q_\nu = 0.$$

Можно показать, что все включения $Q_\nu \subset Q_{\nu-1}$, $\nu = 1, \ldots, k-1$, являются строгими. Действительно, пусть $Q_\nu = Q_{\nu-1}$. Тогда $N(Q_{\nu-1}) = N(Q_\nu) \subset Q_{\nu+1}$, отсюда

$$N^{k-1}T^n = N^{k-\nu}(N^{\nu-1}T^n) \subset N^{k-\nu}Q_{\nu-1} = V^{k-\nu}Q_\nu = 0.$$

Однако $N^{k-1}T^n \neq 0$, ибо k — класс нильпотентности N. Теперь легко доказать теорему. Построим T-базис пространства T^n следующим образом. Базис Q_{k-1} дополним до базиса Q_{k-2}, полученный базис Q_{k-2} дополним до базиса Q_{k-3} и т. д. Очевидно, в построенном базисе матрица элемента g из N имеет вид

$$\begin{bmatrix} 0 & a_{12} & \ldots & a_{1k} \\ 0 & 0 & \ldots & a_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 0 \end{bmatrix}.$$

Это и доказывает теорему. ■

Следствие 1. *Кольцо $N(n, T)$ максимально среди нильпотентных подколец кольца T_n. Если N_1 и N_2 — максимальные нильпотентные подкольца кольца T_n, то в $GL(n, T)$ найдется такой элемент d, что $d^{-1}N_1 d = N_2$.*

§ 14. Линейные представления. Приводимость и неприводимость линейных групп

1. Линейные представления. Пусть M — правый свободный модуль над кольцом Λ, а Y — произвольное непустое множество. Любое отображение

$$d\colon Y \to \operatorname{Hom}(M, M) \qquad (1)$$

называется *линейным представлением множества Y*.

Для заданного представления (1) модуль M будем рассматривать как операторную абелеву аддитивную группу $M(\Omega)$ с областью операторов $\Omega = Y \cup \Delta$, где действие оператора $\omega \in \Omega$ на элемент $u \in M$ задается следующим образом. Если $\omega = y \in Y$, то положим $\omega u = \sigma u$, где $\sigma = d(y)$. Если же $\omega = \lambda \in \Delta$, то положим $\omega u = u\lambda$. Очевидно, каждая допустимая подгруппа операторной группы $M(\Omega)$ является подмодулем модуля M. Пусть M_1 и M_2 — свободные правые модули над кольцом Δ. Два представления

$$d_1\colon\ Y \to \operatorname{Hom}(M_1, M_1), \qquad d_2\colon\ Y \to \operatorname{Hom}(M_2, M_2) \tag{2}$$

множества Y называются *эквивалентными*, если группы $M_1(\Omega)$ и $M_2(\Omega)$ операторно изоморфны.

Лемма 1. *Представления* (2) *эквивалентны тогда и только тогда, когда существует такой изоморфизм модулей*

$$\psi\colon\ M_1 \to M_2, \tag{3}$$

что для любого $y \in Y$ выполняется равенство

$$d_2(y) = \psi d_1(y)\psi^{-1}. \tag{4}$$

Доказательство. Пусть представления (2) эквивалентны. Тогда существует операторный изоморфизм

$$\psi\colon\ M_1(\Omega) \to M_2(\Omega).$$

Очевидно, что ψ — изоморфизм модулей M_1 и M_2. Покажем справедливость формулы (4). Пусть x_1 пробегает модуль M_1. Тогда $x_2 = \psi(x_1)$ пробегает модуль M_2. Для любого $y \in Y$ можно написать

$$d_2(y)(x_2) = y\psi(x_1) = \psi(yx_1) = \psi(d_1(y)(x_1)).$$

Отсюда

$$\begin{gathered}(d_2(y)\psi)(x_1) = (\psi d_1(y))(x_1),\\ d_2(y)\psi = \psi d_1(y).\end{gathered} \tag{5}$$

Из (5) следует (4). Необходимость доказана.

Докажем достаточность. Пусть существует изоморфизм модулей (3) и верна формула (4). Покажем, что ψ — операторный изоморфизм групп $M_1(\Omega)$ и $M_2(\Omega)$. Очевидно, из (4) вытекает (5). Для любого $x \in M$ из (5) находим

$$\psi d_1(y)(x) = d_2(y)\psi(x), \qquad \psi(yx) = y\psi(x).$$

Следовательно, ψ — операторный изоморфизм. ■

В случае, когда модули M_1 и M_2 обладают конечными базисами, лемму 1 можно сформулировать следующим образом.

Представления (2) *тогда и только тогда эквивалентны, когда модули* M_1 *и* M_2 *обладают такими базисами* B_1 *и* B_2 *соответственно, что для любого* $y \in Y$ *матрица эндоморфизма* $d_1(y)$ *в базисе* B_1 *совпадает с матрицей эндоморфизма* $d_2(y)$ *в базисе* B_2.

В случае, когда в (1) множество Y является группой, мы будем предполагать, что выполняются два условия:

$$d(y_1y_2) = d(y_1)\,d(y_2)$$

для любых $y_1, y_2 \in Y$, а $\operatorname{Im} d$ есть подгруппа группы $GL(M)$. Представление $d\colon G \to \operatorname{Hom}(M, M)$ группы G называется *точным*, если отображение d инъективно.

Пусть M_1, M_2 — свободные модули над кольцом Δ, H_1 — подгруппа $GL(M_1)$, а H_2 — подгруппа $GL(M_2)$. Будем говорить, что H_1 и H_2 *подобны как линейные группы*, если существует изоморфизм модулей

$$\varphi\colon M_1 \to M_2,$$

для которого

$$H_2 = \varphi H_1 \varphi^{-1}.$$

Если d_1 и d_2 — эквивалентные прдставления группы G, то, в силу леммы 1, $\operatorname{Im} d_1$ и $\operatorname{Im} d_2$ подобны как линейные группы.

Будем теперь рассматривать частный случай представления (1), когда $M = V$, где V — линейное пространство над телом T,

$$d\colon Y \to \operatorname{Hom}(V, V). \tag{6}$$

Вместо $M(\Omega)$ будем писать в этом случае $V(\Omega)$. Представление (6) называется *неприводимым*, если группа $V(\Omega)$ операторно проста. Если же $V(\Omega)$ обладает нетривиальной допустимой подгруппой, то представление (6) называется *приводимым*. Представление (6) называется *вполне приводимым*, если $V(\Omega)$ — прямая сумма операторно простых допустимых подгрупп. Представление (6) называется *разложимым* (*неразложимым*), если операторная группа $V(\Omega)$ разложима (неразложима).

Пусть теперь размерность V над телом T конечна и равна n. Так как каждая допустимая подгруппа группы $V(\Omega)$ является подпространством пространства V, то операторная группа $V(\Omega)$ обладает композиционным рядом

$$V(\Omega) = V_0(\Omega) \supset V_1(\Omega) \supset \ldots \supset V_k(\Omega) = 0, \qquad k \leqslant n. \tag{7}$$

Положим

$$U_j(\Omega) = V_{j-1}(\Omega)/V_j(\Omega), \qquad j = 1, \ldots, k.$$

Группы $U_j(\Omega)$ операторно просты и представление (6) вместе с композиционным рядом (7) определяет k неприводимых линейных представлений множества Y

$$d_j\colon Y \to \mathrm{Hom}(U_j, U_j), \qquad j = 1, \ldots, k,$$

где

$$d_j(y) = \sigma_j, \qquad \sigma_j(u) = yu, \qquad u \in U_j, \qquad y \in Y. \tag{8}$$

Представления (8) называются *неприводимыми частями представления* (6). В силу теоремы Жордана — Гельдера неприводимые части заданного представления (6) определяются однозначно с точностью до эквивалентности и нумерации.

Пусть теперь H — какое-либо подмножество кольца $\mathrm{Hom}(V, V)$. Введем тривиальное линейное представление

$$D\colon H \to \mathrm{Hom}(V, V), \qquad h \mapsto h.$$

Неприводимые части представления D будем называть *неприводимыми частями множества* H.

Если Y — алгебра над полем Λ, а V — линейное пространство над Λ, то будем предполагать, что d в (6) является гомоморфизмом алгебр Y и $\mathrm{Hom}(V,V)$.

2. Локальная теорема Мальцева. Множество Σ подгрупп группы G называется *локальной системой группы* G, если выполняются два требования:

1) $$G = \bigcup H_\alpha, \qquad H_\alpha \in \Sigma;$$

2) для любых H_α и H_β из Σ существует в Σ такая H_γ, что

$$H_\alpha \subset H_\gamma, \qquad H_\beta \subset H_\gamma.$$

Например, совокупность всех подгрупп группы G, порождаемых конечными подмножествами G, есть локальная система группы G.

Целью настоящего пункта является доказательство следующей теоремы Мальцева:

Теорема 1 (Мальцев [1]). *Пусть Σ — локальная система группы G. Если каждая H_α из Σ обладает точным линейным представлением степени n над некоторым полем Δ_α, то и группа G обладает точным линейным представлением степени n над некоторым полем Δ.*

Доказательству теоремы предпошлем несколько определений и лемм, относящихся к свойствам ультрапроизведений.

Пусть I — непустое множество. Совокупность $\mathfrak{F}$ подмножеств множества I называется *фильтром* над I, если $\mathfrak{F}$ обладает следующими свойствами:

1) $\varnothing \notin \mathfrak{F}$,

2) $X, Y \in \mathfrak{F} \Rightarrow X \cap Y \in \mathfrak{F}$,

3) $(I \supset Y \supset X \in \mathfrak{F}) \Rightarrow Y \in \mathfrak{F}$.

Фильтр $\mathfrak{F}$ над I называется *ультрафильтром* над I, если выполняется условие

4) для каждого $X \subset I$ либо $X \in \mathfrak{F}$, либо $I \setminus X \in \mathfrak{F}$. Из 1) и из 4) вытекает, что $I \in \mathfrak{F}$ для любого ультрафильтра $\mathfrak{F}$ над I. Если совокупность $\mathfrak{F}$ подмножеств I подчинена лишь условиям 1) и 2), то $\mathfrak{F}$ называется *центрированной системой* над I. Очевидно, всякая центрированная система над I содержится в некотором фильтре над I. Нетрудно доказать, что *всякий фильтр над I содержится в некотором ультрафильтре над I* (см. Мальцев [5], стр. 196).

Пусть $\mathfrak{F}$ — ультрафильтр над I, и пусть каждому $\alpha \in I$ поставлено в соответствие множество A_α. Построим декартово произведение

$$\prod A_\alpha, \quad \alpha \in I, \tag{9}$$

элементы которого будем записывать в виде

$$a = \{a_\alpha\}, \quad a_\alpha \in A_\alpha.$$

На множестве (9) зададим бинарное отношение $\equiv_{\mathfrak{F}}$, положив

$$a \equiv_{\mathfrak{F}} b \Leftrightarrow I_1 = \{\alpha \in I \mid a_\alpha = b_\alpha\} \in \mathfrak{F}.$$

Так как $I \in \mathfrak{F}$, то отношение $\equiv_{\mathfrak{F}}$ рефлексивно. Из определения отношения $\equiv_{\mathfrak{F}}$ вытекает его симметричность. Покажем транзитивность $\equiv_{\mathfrak{F}}$. Пусть $a \equiv_{\mathfrak{F}} b$ и $b \equiv_{\mathfrak{F}} c$. Тогда

$$I_2 = \{\alpha \in I \mid b_\alpha = c_\alpha\} \in \mathfrak{F}.$$

Далее, согласно 2), $I_1 \cap I_2 \in \mathfrak{F}$. С другой стороны,

$$I_1 \cap J_2 \subset \{\alpha \in I \mid a_\alpha = c_\alpha\} = I_3.$$

Следовательно, $I_3 \in \mathfrak{F}$ и

$$a \equiv_{\mathfrak{F}} c.$$

Таким образом, $\equiv_{\mathfrak{F}}$ есть отношение эквивалентности на (9). Множество классов эквивалентных элементов обозначим символом

$$\prod A_\alpha/\mathfrak{F} \tag{10}$$

и назовем ультрапроизведением множеств A_α. Класс, содержащий элемент $a = \{a_\alpha\}$, будем обозначать символом $\bar{a} = \overline{\{a_\alpha\}}$. Если все A_α являются группами (кольцами, модулями), то можно задать естественным образом операцию на ультрапроизведении (10) и превратить его в группу (кольцо, модуль). Пусть, например, $A_\alpha = \Delta_\alpha$ — кольцо. Для

$$\lambda = \{\lambda_\alpha\}, \quad \mu = \{\mu_\alpha\}, \qquad \lambda_\alpha, \ \mu_\alpha \in \Delta_\alpha,$$

положим

$$\bar{\lambda} + \bar{\mu} = \overline{\{\lambda_\alpha + \mu_\alpha\}}, \qquad \bar{\lambda}\bar{\mu} = \overline{\{\lambda_\alpha \mu_\alpha\}}.$$

Классы $\bar{\lambda} + \bar{\mu}$ и $\bar{\lambda}\bar{\mu}$ не зависят от выбора представителей λ и μ классов $\bar{\lambda}$ и $\bar{\mu}$. Действительно, пусть $\bar{\lambda} = \bar{\rho}$, $\bar{\mu} = \bar{\sigma}$. Тогда

$$X_1 = \{\alpha \in I \mid \lambda_\alpha = \rho_\alpha\} \in \mathfrak{F}, \qquad X_2 = \{\alpha \in I \mid \mu_\alpha = \sigma_\alpha\} \in \mathfrak{F},$$
$$Y = X_1 \cap X_2 \in \mathfrak{F}.$$

Для $\alpha \in Y$

$$\lambda_\alpha + \mu_\alpha = \rho_\alpha + \sigma_\alpha, \qquad \lambda_\alpha \mu_\alpha = \rho_\alpha \sigma_\alpha.$$

Следовательно,

$$Y \subset \{\alpha \in I \mid \lambda_\alpha + \mu_\alpha = \rho_\alpha + \sigma_\alpha\} \in \mathfrak{F},$$
$$Y \subset \{\alpha \in I \mid \lambda_\alpha \mu_\alpha = \rho_\alpha \sigma_\alpha\} \in \mathfrak{F},$$

т. е. $\bar\lambda + \bar\mu = \bar\rho + \bar\sigma$, $\bar\lambda\bar\mu = \bar\rho\bar\sigma$. Очевидно, что

$$\Delta = \prod \Delta_\alpha/\mathfrak{F} \tag{11}$$

— кольцо. Это кольцо называется *ультрапроизведением колец* Δ_α. Совершенно аналогично определяются ультрапроизведения групп, модулей и других алгебраических систем.

Если каждое кольцо Δ_α, $\alpha \in I$, *является полем, то и кольцо* (11) — *тоже поле*. Действительно, Δ — кольцо с единицей и нулем

$$\bar 1 = \overline{\{1_\alpha\}} \quad \text{и} \quad \bar 0 = \overline{\{0_\alpha\}},$$

где 1_α и 0_α — единица и, соответственно, нуль поля Δ_α. Пусть

$$\bar\lambda = \overline{\{\lambda_\alpha\}} \in \Delta, \quad \bar\lambda \neq \bar 0.$$

Тогда

$$X = \{\alpha \in I \mid \lambda_\alpha = 0_\alpha\} \notin \mathfrak{F}, \qquad Y = I \setminus X \in \mathfrak{F}.$$

Положим

$$\bar\mu = \overline{\{\mu_\alpha\}},$$

где

$$\mu_\alpha = \lambda_\alpha^{-1}, \qquad \alpha \in Y,$$
$$\mu_\alpha = 1_\alpha, \qquad \alpha \in X.$$

Тогда

$$\bar\lambda\bar\mu = \overline{\{\lambda_\alpha\mu_\alpha\}}, \qquad \{\alpha \in I \mid \lambda_\alpha\mu_\alpha = 1_\alpha\} = Y \in \mathfrak{F}.$$

Следовательно,

$$\bar\lambda\bar\mu = \bar 1,$$

т. е. Δ — поле. ■

Пусть теперь каждому $\alpha \in I$ поставлены в соответствие: поле Δ_α, n-мерное линейное пространство V_α над Δ_α и подгруппа G_α группы $GL(V_\alpha)$. Построим ультрапроизведения

$$\Delta = \prod \Delta_\alpha/\mathfrak{F}, \qquad V = \prod V_\alpha/\mathfrak{F}, \qquad G = \prod G_\alpha/\mathfrak{F}.$$

Мы уже видели, что Δ — поле. Покажем, что V — линейное пространство размерности n над полем Δ.

Для $\bar\lambda = \overline{\{\lambda_\alpha\}} \in \Delta$, $\bar u = \overline{\{u_\alpha\}} \in V$, $\bar v = \overline{\{v_\alpha\}} \in V$ имеем

$$\bar u + \bar v = \overline{\{u_\alpha + v_\alpha\}}, \qquad \bar u\bar\lambda = \overline{\{u_\alpha\lambda_\alpha\}},$$

откуда видно, что V — линейное пространство над Δ. Пусть

$$b_{\alpha 1}, \ldots, b_{\alpha n} \tag{12}$$

— базис V_α над Δ_α. Положим $b_1 = \{b_{\alpha 1}\}, \ldots, b_n = \{b_{\alpha n}\}$. Тогда

$$\bar{b}_1, \ldots, \bar{b}_n \tag{13}$$

— базис пространства V над Δ. В самом деле, для любого $\bar{v} \in V$ можно написать

$$\bar{v} = \overline{\{b_{\alpha 1}\lambda_{\alpha 1} + \ldots + b_{\alpha n}\lambda_{\alpha n}\}} = \bar{b}_1\bar{\lambda}_1 + \ldots + \bar{b}_n\bar{\lambda}_n.$$

С другой стороны, система (13) линейно независима над Δ, ибо из равенства

$$\bar{b}_1\bar{\lambda}_1 + \ldots + \bar{b}_n\bar{\lambda}_n = \bar{0}$$

вытекает

$$\{\alpha \in I \mid b_{\alpha 1}\lambda_{\alpha 1} + \ldots + b_{\alpha n}\lambda_{\alpha n} = 0_\alpha\} \in \mathfrak{F},$$

где 0_α — нулевой вектор пространства V_α. Так как (12) — базис пространства V_α, то для $j = 1, \ldots, n$

$$X_j = \{\alpha \in I \mid \lambda_{\alpha j} = 0_\alpha\} \in \mathfrak{F},$$

где 0_α — нуль поля Δ_α. Следовательно,

$$\bar{\lambda}_j = \overline{\{\lambda_{\alpha j}\}} = \bar{0}.$$

Таким образом, V есть n-мерное линейное пространство над Δ.

Легко видеть, что

$$G = \prod G_\alpha/\mathfrak{F}$$

— подгруппа группы $GL(V)$. Действительно, пусть $\bar{g} = \overline{\{g_\alpha\}} \in G$. Для $\bar{\lambda} \in \Delta$, $\bar{u}, \bar{v} \in V$ можно написать

$$\bar{g}(\bar{u}\bar{\lambda}) = \overline{\{g_\alpha(u_\alpha\lambda_\alpha)\}} = \overline{\{g_\alpha(u_\alpha)\lambda_\alpha\}} = \overline{\{g_\alpha\}}\,\overline{\{u_\alpha\}}\,\bar{\lambda} = \bar{g}(\bar{u})\,\bar{\lambda},$$

$$\bar{g}(\bar{u} + \bar{v}) = \bar{g}(\bar{u}) + \bar{g}(\bar{v}).$$

Следовательно, $G \subset \mathrm{Hom}(V, V)$. Так как G — группа и единица группы G совпадает с единицей $\mathrm{Hom}(V, V)$, то G — подгруппа в $GL(V)$. Итак, верна

Лемма 2. *Ультрапроизведение линейных групп G_α степени n над полями Δ_α есть линейная группа степени n над некоторым полем Δ.*

Лемма 3. *Пусть G — произвольная группа, а Σ — ее локальная система. Тогда G изоморфна некоторой подгруппе ультрапроизведения всех подгрупп системы Σ при подходящем фильтре над Σ.*

Доказательство. Построим сперва одну центрированную систему подмножеств множества Σ. Для каждого конечного подмножества F группы G положим

$$\Sigma_F = \{H \in \Sigma \mid H \supset F\}. \tag{14}$$

Если F_1 и F_2 — два конечных подмножества группы G, то из (14) следует

$$\Sigma_{F_1 \cup F_2} = \Sigma_{F_1} \cap \Sigma_{F_2}. \tag{15}$$

Так как $G = \bigcup H_\alpha$, $H_\alpha \in \Sigma$, то для одноэлементных множеств $F = \{g\}$

$$\Sigma_g = \Sigma_F \neq \varnothing.$$

Пусть теперь $\operatorname{card} F = m > 1$ и для подмножеств F_j группы G мощности, меньшей m, неравенство

$$\Sigma_{F_j} \neq \varnothing$$

доказано. Множество F можно записать в виде

$$F = F_1 \cup F_2, \qquad \operatorname{card} F_j < m.$$

Тогда

$$\Sigma_F = \Sigma_{F_1} \cap \Sigma_{F_2}, \qquad \Sigma_{F_j} \neq \varnothing.$$

Пусть $R \in \Sigma_{F_1}$, $S \in \Sigma_{F_2}$. Так как Σ — локальная система, то в Σ есть группа H такая, что $H \supset R$, $H \supset S$. Очевидно, что $H \supset F = F_1 \cup F_2$. Следовательно,

$$\Sigma_F \neq \varnothing. \tag{16}$$

Пусть Φ — совокупность всех Σ_F, где F — любое конечное подмножество группы G. Из (15) и (16) следует, что Φ — центрированная система подмножеств над Σ. Как мы заметили выше, Φ содержится в некотором ультрафильтре $\mathfrak{F}$ над Σ. Покажем, что G изоморфно вкладывается в ультрапроизведение

$$\prod S_\alpha/\mathfrak{F}, \qquad S_\alpha \in \Sigma.$$

Введем отображение

$$\varphi\colon\ G \to \prod S_\alpha/\mathfrak{F}, \qquad g \mapsto \overline{\{g_\alpha\}},$$

где $g_\alpha = g$, $g \in S_\alpha$; $g_\alpha = 1$, $g \notin S_\alpha$. Покажем, что φ — гомоморфизм. Действительно,

$$\varphi(gh) = \overline{\{(gh)_\alpha\}}.$$

Очевидно, для g и h из G

$$\Sigma_{\{g,\,h\}} \subset \{S_\alpha \in \Sigma \mid (gh)_\alpha = g_\alpha h_\alpha\} = X.$$

Так как $\Sigma_{\{g,\,h\}} \in \mathfrak{F}$, то $X \in \mathfrak{F}$. Следовательно,

$$\varphi(gh) = \overline{\{(gh)_\alpha\}} = \overline{\{g_\alpha\}}\,\overline{\{h_\alpha\}} = \varphi(g)\,\varphi(h).$$

Остается доказать инъективность φ. Пусть $g \in G$, $g \neq 1$, а $\varphi(g) = \overline{1}$. Тогда

$$\{S_\alpha \in \Sigma \mid g_\alpha = 1\} \in \mathfrak{F}, \qquad X = \{S_\alpha \in \Sigma \mid g \notin S_\alpha\} \in \mathfrak{F},$$
$$\Sigma_g = \Sigma \setminus X \notin \mathfrak{F}.$$

Однако по построению $\mathfrak{F}$ содержит все Σ_F, где F — конечное подмножество группы G. ■

Сформулированная выше теорема Мальцева вытекает из лемм 2 и 3 (ср. Кегель [1]).

3. Полупростота и полная приводимость. Пусть A — алгебра конечной размерности над полем Δ с единицей e, а V — конечномерное линейное пространство над Δ. Мы будем рассматривать такие линейные представления

$$d\colon\ A \to \mathrm{Hom}(V,\ V),$$

что $d(e)$ совпадает с единицей кольца $\mathrm{Hom}(V, V)$. Примером представления такого рода может служить *левое регулярное представление* ρ алгебры A с единицей e:

$$\rho\colon\ A \to \mathrm{Hom}(W,\ W),$$

где W — линейное пространство алгебры A,

$$\rho(a) = \sigma_a, \qquad \sigma_a\colon\ A \to A, \qquad \sigma_a(x) = ax.$$

Как легко проверить,

$$\rho(a+b) = \sigma_{a+b} = \sigma_a + \sigma_b,$$
$$\rho(ab) = \sigma_{ab} = \sigma_a\sigma_b,$$
$$\mathrm{Ker}\,\rho = (0).$$

Следовательно, ρ — точное линейное представление алгебры A. Очевидно, $\rho(e)$ — единица Hom (W, W). Операторную аддитивную группу, определяемую представлением ρ, будем обозначать $W(A)$. Ясно, что допустимыми подгруппами группы $W(A)$ будут левые идеалы алгебры A. Из теоремы 13.2 вытекает, что *представление* ρ *тогда и только тогда вполне приводимо, когда алгебра* A *полупроста.*

В теории представлений хорошо известна

Теорема 2. *Пусть алгебра* A *полупроста. Тогда каждое представление вида* d *вполне приводимо, а любая неприводимая часть представления* d *эквивалентна некоторой неприводимой части левого регулярного представления* ρ (см., например, Ван-дер-Варден [2], стр. 197).

Если, в частности, A — простая алгебра над Δ, то минимальные левые идеалы A попарно операторно изоморфны. Отсюда и из теоремы 2 вытекает

Следствие 1. *Пусть* A — *простая алгебра над полем* Δ. *Тогда* A *обладает с точностью до эквивалентности единственным неприводимым представлением над* Δ.

Теорема 3. *Пусть* V — *пространство конечной размерности над полем* Δ, *а* A — *подалгебра алгебры* Hom(V, V), *причем единица* e *алгебры* A *совпадает с единицей* Hom(V, V). *Тогда из неприводимости* A *следует простота* A, *а из полной приводимости* A *полупростота* A.

Доказательство. Пусть подалгебра A алгебры Hom(V, V) вполне приводима как множество эндоморфизмов пространства V. Пусть, далее, W — линейное пространство алгебры A. Будем рассматривать две операторные группы: пространство $W(A)$ левого регулярного представления ρ алгебры A и пространство $V(A)$ тривиального представления D алгебры A. Так как A имеет конечную размерность над Δ, то в $W(A)$ есть операторно простые допустимые подгруппы. Пусть W_1 — произвольная операторно простая допустимая подгруппа группы $W(A)$. Так как $V(A)$ — прямая сумма допустимых операторно простых подгрупп, то в $V(A)$ есть такая допустимая операторно простая подгруппа V_1, что $W_1V_1 \neq (0)$. Следовательно, найдется такой вектор

$v_1 \in V$, что
$$W_1 v_1 \neq (0). \tag{17}$$
Введем отображение
$$\gamma_1\colon\ W_1 \to V_1, \qquad x \mapsto x v_1.$$
Для $x, y \in W$, $a \in A$ имеем
$$\gamma_1(x + y) = \gamma_1(x) + \gamma_1(y), \qquad \gamma_1(ax) = a\gamma_1(x).$$
Следовательно, γ_1 — операторный гомоморфизм. Так как W_1 и V_1 операторно просты, то, в силу (17), γ_1 — операторный изоморфизм, причем
$$V_1 = W_1 v_1. \tag{18}$$
Если $W_1 = W(A)$, то теорема доказана, ибо в этом случае алгебра A проста (см. конец § 13).

Пусть теперь
$$W_1 \neq W(A). \tag{19}$$
В силу (18) в W_1 найдется такой элемент e_1, что $e_1 v_1 = v_1$. Так как группа W_1 операторно проста, то
$$W_1 = Ae_1.$$
Отсюда и из (19) следует, что
$$e_1 \neq e.$$
Для любого x из W_1 можно написать
$$\gamma_1(xe_1) = xe_1 v_1 = x v_1 = \gamma_1(x).$$
Отсюда и из инъективности γ_1 вытекает, что
$$xe_1 = x$$
для любого $x \in W_1$. В частности, $e_1^2 = e_1$. Следовательно, пространство $W(A) = W$ можно записать в виде
$$W(A) = A = Ae = Ae_1 \dotplus A(e - e_1) = W_1 \dotplus A(e - e_1).$$
Ясно, что $A(e - e_1)$ — допустимая подгруппа группы $W(A)$. Итак, любая операторно простая допустимая подгруппа W_1 группы $W(A)$ прямо дополняема допустимой подгруппой. Согласно предложению 13.4 $W(A)$ — прямая сумма операторно простых допустимых подгрупп, т. е. алгебра A полупроста. Если, в частности, A

неприводима, то в (17) $V_1 = V$, а любая операторно простая допустимая подгруппа W_1 операторно изоморфна группе $V(A)$, т. е. алгебра A проста. ■

4. Линейная оболочка вполне приводимой группы. Пусть V есть n-мерное линейное пространство над полем Δ, а G — какое-либо множество эндоморфизмов из $\mathrm{Hom}(V, V)$. *Линейной Δ-оболочкой* $[G]_\Delta$ множества G называется множество всех линейных комбинаций вида

$$g_1\lambda_1 + \ldots + g_k\lambda_k, \qquad g_i \in G, \qquad \lambda_i \in \Delta.$$

Если, в частности, G — *полугруппа относительно умножения, то, очевидно,* $[G]_\Delta$ *является алгеброй над* Δ. Пространство V можно рассматривать как аддитивную операторную группу $V(\Omega)$ с областью операторов $\Omega = \Delta \cup G$. Очевидно, в этом случае допустимыми подгруппами $V(\Omega)$ окажутся подпространства V, инвариантные относительно множества эндоморфизмов G. Ясно, что система допустимых подгрупп $V(\Omega)$ не изменится, если заменить область операторов $\Omega = \Delta \cup G$ областью

$$\Omega_1 = \Delta \cup [G]_\Delta,$$

т. е. всякая допустимая подгруппа операторной группы $V(\Omega)$ является допустимой подгруппой операторной группы $V(\Omega_1)$ и наоборот. При переходе от допустимых подгрупп группы $V(\Omega)$ к допустимым подгруппам группы $V(\Omega_1)$ сохраняется также отношение операторного изоморфизма, т. е. две допустимые подгруппы операторной группы $V(\Omega_1)$ тогда и только тогда операторно изоморфны, когда они операторно изоморфны как подгруппы из $V(\Omega)$.

В частности, если G — вполне приводимая группа из $GL(V)$, то $[G]_\Delta$ — вполне приводимая подалгебра алгебры $\mathrm{Hom}(V, V)$.

Теорема 4. *Пусть G — вполне приводимая подгруппа группы $GL(V)$, где V — линейное пространство над полем Δ, $n_1, \ldots, n_s$ — степени всех попарно неэквивалентных неприводимых частей G, а $A = [G]_\Delta$. Тогда*

$$A = R_1 \dotplus \ldots \dotplus R_s,$$

где $R_j \cong T^j_{r_j}$, T^j — тело, центр которого содержит Δ, $(T^j : \Delta) r_j = n_j$, $R_i R_j = (0)$ при $i \neq j$. В частности, если

G неприводима, то $A = T_r$, $(T:\Delta)r = n$, где T — тело, n — размерность пространства V над Δ.

Доказательство. Так как $A = [G]_\Delta$ вполне приводима, то, по теореме 3, A полупроста. В силу приведенных выше замечаний числа

$$n_1, \ldots, n_s \tag{20}$$

суть степени всех попарно неэквивалентных частей алгебры A. По теореме 2 каждая неприводимая часть A эквивалентна некоторой неприводимой части левого регулярного представления алгебры A. Следовательно, в алгебре A имеется по меньшей мере s операторно неизоморфных операторно простых левых идеалов. С другой стороны, если L — любой операторно простой левый идеал алгебры

$$A = [G]_\Delta = \mathrm{Hom}(V, V),$$

то среди допустимых подгрупп группы

$$V(\Omega_1) \qquad (\Omega_1 = \Delta \cup A)$$

есть подгруппа, операторно изоморфная L. Действительно, так как $L \neq (0)$, то в V есть такой вектор v, что

$$V_1 = L(v) \neq (0);$$

V_1 и есть искомая допустимая подгруппа. Таким образом, в A имеется точно s операторно неизоморфных операторно простых левых идеалов, размерности которых равны числам (20). Отсюда и из теоремы 13.3 вытекает требуемое. ■

Очевидно, что в подходящем базисе пространства V матрицы g группы G из теоремы 4 одновременно принимают следующий вид:

$$g = \mathrm{diag}[g_1, \ldots, g_1, \ldots, g_j, \ldots, g_j, \ldots, g_s, \ldots, g_s],$$

где γ_j: $g \mapsto g_j$ — неприводимое представление группы G степени n_j, $n = n_1k_1 + \ldots + n_sk_s$, k_j — число повторений g_j. При $i \neq j$ представления γ_i и γ_j не эквивалентны. Пусть

$$G_j = \mathrm{Im}\,\gamma_j, \qquad A_j = [G_j]_\Delta, \qquad j = 1, \ldots, s.$$

Тогда теорему 4 можно сформулировать так:

Теорема 4а. *Алгебра* $A = [G]_\Delta$ *состоит из всех матриц вида*

$$\operatorname{diag}[a_1, \ldots, a_1, \ldots, a_s, \ldots, a_s],$$

где $a_1, \ldots, a_s$ *независимо друг от друга пробегают, соответственно, алгебры* $A_1, \ldots, A_s$. *Следовательно,* $A : \Delta = A_1 : \Delta + \ldots + A_s : \Delta$.

Как хорошо известно, тело конечной размерности над алгебраически замкнутым полем P совпадает с P. Следовательно, в теореме 4 для алгебраически замкнутого поля Δ

$$T^i : \Delta = 1, \qquad n_i = r_i.$$

Если G неприводима, то при алгебраически замкнутом Δ имеем

$$A = [G]_\Delta = \Delta_n, \qquad A : \Delta = n^2.$$

Пусть Δ — произвольное поле, а Σ — надполе поля Δ. Тогда, очевидно, любая подгруппа группы $GL(n, \Delta)$ является подгруппой группы $GL(n, \Sigma)$. Подгруппа G группы $GL(n, \Delta)$ называется *абсолютно неприводимой*, если при любом расширении Σ поля Δ G является неприводимой подгруппой группы $GL(n, \Sigma)$.

Следствие 1. *Подгруппа* G *группы* $GL(n, \Delta)$ *тогда и только тогда абсолютно неприводима, когда ее линейная* Δ-*оболочка совпадает с* Δ_n.

Доказательство. Если Σ — надполе поля Δ, то

$$[G]_\Delta : \Delta = [G]_\Sigma : \Sigma,$$

ибо система линейно независимых над Δ матриц из Δ_n остается линейно независимой и над Σ. По известной теореме из теории полей поле Δ является подполем некоторого алгебраически замкнутого поля P. Если теперь G абсолютно неприводима, то

$$n^2 = [G]_P : P = [G]_\Delta : \Delta.$$

Следовательно,

$$[G]_\Delta = \Delta_n, \tag{21}$$

т. е. из абсолютной неприводимости группы G вытекает равенство (21). Обратное утверждение очевидно. ■

Доказанное следствие можно сформулировать еще так:

Следствие 2. *Подгруппа G группы $GL(n, \Delta)$ тогда и только тогда абсолютно неприводима, когда в G существует n^2 линейно независимых матриц над Δ.*

Приведем еще некоторые свойства неприводимых групп и алгебр.

Лемма 4. *Пусть G — неприводимая подгруппа группы $GL(n, \Sigma)$, где Σ — такое расширение поля Δ, что $\Sigma : \Delta = m$, $\Sigma \subset \Delta_m$. Положив $n = ml$ и заменив в матрицах группы G элементы σ поля Σ матрицами из Δ_m, группу G будем трактовать как подгруппу группы $GL(n, \Delta)$. Если теперь*

$$[G]_\Delta \supset \Sigma E_l, \tag{22}$$

то G — неприводимая подгруппа группы $GL(n, \Delta)$.

Доказательство. n-мерное пространство Δ^n над Δ, где действует группа G, можно рассматривать как l-мерное пространство Σ^l над Σ. Пусть $L \neq (0)$ — инвариантное относительно $[G]_\Delta$ подпространство пространства Δ^n. В силу (22) L является подпространством пространства Σ^l. По условию G — неприводимая подгруппа $GL(l, \Sigma)$. Следовательно,

$$L = \Sigma^l = \Delta^n,$$

т. е. G — неприводимая подгруппа группы $GL(n, \Delta)$. ■

Лемма 4а. *Пусть тело T содержится в Δ_m, где Δ — поле, центр тела T содержит ΔE_m, $T : \Delta = m$,*

$$B = T_r. \tag{23}$$

Положим $n = mr$ и будем трактовать B как подалгебру алгебры Δ_n. Тогда B — неприводимая подалгебра алгебры Δ_n.

Доказательство. Из (23) следует, согласно теореме 13.3, что B — простая алгебра над Δ и размерность операторно простого левого идеала над Δ равна $rm = n$. Следовательно, по теореме 2, степень неприводимого представления алгебры B матрицами над полем Δ равна n. Но $B \subset \Delta_n$. Следовательно, тривиальное представление D: $B \to B$, $x \mapsto x$, степени n неприводимо. Таким образом, B — неприводимая подалгебра алгебры Δ_n. ■

Ниже нам понадобится еще правое регулярное представление алгебры A над полем Δ с единицей e.

Пусть W — пространство алгебры A. *Правым регулярным представлением* A называется отображение

$$\rho_1\colon\ A \to \mathrm{Hom}(W, W),$$

$$\rho_1(a) = \tau_a, \qquad \tau_a\colon\ A \to A, \qquad \tau_a(x) = xa.$$

Как легко проверить,

$$\begin{aligned} &\rho_1(a+b) = \tau_{a+b} = \tau_a + \tau_b,\\ &\rho_1(ab) = \tau_{ab} = \tau_b\tau_a,\\ &\rho_1(a\lambda) = \tau_{a\lambda} = \tau_a\lambda,\ \lambda \in \Delta,\\ &\mathrm{Ker}\,\rho_1 = (0). \end{aligned}$$

Таким образом, ρ_1 — инверсный инъективный гомоморфизм алгебры A в алгебру $\mathrm{Hom}(W, W)$. В силу теоремы 1.3, $\mathrm{Im}\,\rho_1$ является централизатором $\mathrm{Im}\,\rho$ в $\mathrm{Hom}(W, W)$, а $\mathrm{Im}\,\rho$ — централизатором $\mathrm{Im}\,\rho_1$ в $\mathrm{Hom}(W, W)$. Отсюда вытекает, что

$$\mathrm{Im}\,\rho \cap \mathrm{Im}\,\rho_1 = Z(\mathrm{Im}\,\rho) = Z(\mathrm{Im}\,\rho_1), \tag{24}$$

где $Z(\mathrm{Im}\,\rho)$, $Z(\mathrm{Im}\,\rho_1)$ — центры $\mathrm{Im}\,\rho$ и $\mathrm{Im}\,\rho_1$.

Теорема 5. *Пусть A — неприводимая подалгебра с единицей E_n алгебры Δ_n, где Δ — поле. Тогда в $GL(n, \Delta)$ найдется такая матрица g, что $A = gT_rg^{-1}$, где T — тело, причем $\Delta_m \supset T \supset \Delta E_m$, $T : \Delta E_m = m$, $n = mr$. Далее, централизатор A в Δ_n совпадает с $gT'E_rg^{-1}$,* где *T' — тело, инверсно изоморфное телу T, центр тела T' совпадает с центром тела T и равен $T' \cap T$.*

Доказательство. По теореме 3 A — простая подалгебра алгебры Δ_n, следовательно, по теореме 13.3, A изоморфна алгебре Φ_r, где Φ — тело конечной размерности m над полем Δ. Введем левое и правое регулярные представления ρ и ρ_1 тела Φ:

$$\rho\colon\ \Phi \to \Delta_m, \qquad \rho_1\colon\ \Phi \to \Delta_m.$$

Положим

$$T = \mathrm{Im}\,\rho, \qquad T' = \mathrm{Im}\,\rho_1.$$

Тогда тела T и T' инверсно изоморфны, центр тела T' совпадает с центром тела T и равен $T \cap T'$ (см. (24)).

Заменив в матрицах алгебры Φ_r элементы φ тела Φ элементами $\rho(\varphi) \in T$, получим алгебру T_r, изоморфную A. Очевидно, что T_r — подалгебра алгебры Δ_{mr}. Согласно лемме 4а, T_r — неприводимая подалгебра алгебры Δ_{mr}. Так как простая алгебра A обладает единственным с точностью до эквивалентности неприводимым представлением, то $mr = n$,

$$A = gT_r g^{-1},$$

где $g \in GL(n, \Delta)$. Первая часть доказана. Так как T' — централизатор T в Δ_m, то $T'E_r$ — централизатор T_r в Δ_n, а $gT'E_r g^{-1}$ — централизатор A в Δ_n. ■

Теорема 6. *Пусть G — неприводимая подгруппа группы $GL(n, \Delta)$, Z' — центр группы G. Тогда $[Z']_\Delta = \Sigma$ — расширение поля Δ, степень $\Sigma : \Delta$ делит число n.*

Доказательство. Пусть V — линейное пространство над Δ, где действует G. Так как G неприводима, то аддитивная операторная группа $V(\Omega)$ с областью операторов $\Omega = G \cup \Delta$ операторно проста. Элементы $\sigma \in \Sigma$ являются эндоморфизмами операторной группы $V(\Omega)$. В силу следствия 1 леммы 13.1 Σ содержится в некотором теле $T \supset \Delta$. Следовательно, Σ — коммутативная алгебра без делителей нуля конечной размерности над Δ. Отсюда вытекает, что Σ — поле. Покажем, что степень $m = \Sigma : \Delta$ делит число n. Очевидно, V можно рассматривать как линейное пространство над Σ. Если $k = V : \Sigma$, то $mk = n$. ■

В связи с доказательством теоремы 6 заметим, что для любых $\sigma \in \Sigma$, $x \in V$, $g \in G$ $g(\sigma(x)) = \sigma g(x)$. Таким образом, G можно рассматривать как подгруппу группы $GL(k, \Sigma)$.

5. θ-подгруппы. Пусть θ — некоторое абстрактное групповое свойство, подчиненное следующему условию: если подгруппа Γ группы G обладает свойством θ, а C — абелева подгруппа из G, лежащая в централизаторе группы Γ в G, то ΓC тоже обладает свойством θ. В качестве свойства θ можно взять, например, разрешимость, коммутативность, локальную нильпотентность, нильпотентность заданного класса. Подгруппу Γ группы G, обладающую свойством θ, назовем θ-подгруппой.

Теорема 7. *Пусть Δ — произвольное поле, а G — максимальная неприводимая θ-подгруппа группы*

$GL(n, \Delta)$. Тогда существует такое расширение Σ степени m поля Δ, что m делит число n, G — абсолютно неприводимая максимальная θ-подгруппа группы $GL(r, \Sigma)$, $r = nm^{-1}$, а центр группы G совпадает с $\Sigma^* E_r$.

Доказательство. В силу теоремы 5 можно считать, что

$$[G]_\Delta = T_r,$$

где T — тело, $(T : \Delta) r = n$, а централизатор T_r в Δ_n совпадает с $T' E_r$, где T' — тело, инверсно изоморфное телу T, причем $T' = T$ тогда и только тогда, когда T коммутативно. Покажем, что T коммутативно. Пусть T и, значит, T' некоммутативны. Если a — нецентральный элемент из T', то

$$a \notin T, \qquad aE_r \notin G \subset T_r.$$

С другой стороны, по определению θ-группы, $(a) E_r G$ есть θ-группа,

$$(a) E_r G \neq G.$$

Последнее противоречит максимальности G среди θ-подгрупп группы $GL(n, \Delta)$. Следовательно, $T = \Sigma$, где Σ — поле. В силу максимальности G

$$\Sigma^* E_r \subset G.$$

Итак,

$$[G]_\Delta = \Sigma_r,$$

$\Sigma^* E_r$ — центр G. В силу следствия 4.1 G — абсолютно неприводимая подгруппа группы $GL(r, \Sigma)$. Очевидно, что

$$m = \Sigma : \Delta = nr^{-1}. \ \blacksquare$$

§ 15. Примитивность и импримитивность

1. Определение импримитивности и простейшие свойства импримитивных групп. Пусть V — линейное пространство над телом T, а G — подгруппа группы $GL(V)$. Если V представимо в виде прямой суммы

$$V = \dot{\sum} Q_\nu, \qquad \nu \in I, \tag{1}$$

подпространств $Q_\nu \neq (0)$, где $\operatorname{card} I > 1$ и для любых $\alpha \in I$, $g \in G$

$$g(Q_\alpha) \subset Q, \qquad \beta \in I, \tag{2}$$

то группа G называется *импримитивной*, разложение (1) — *разложением пространства V на системы импримитивности группы G*, а подпространства Q_ν — *системами импримитивности группы G*. В противном случае, группа называется *примитивной*.

Лемма 1. *Пусть* (1) — *разложение V на системы импримитивности группы G. Тогда из включения* (2) *следует равенство*

$$g(Q_\alpha) = Q_\beta.$$

Доказательство. Из (2) и из определения импримитивности находим

$$Q_\alpha \subset g^{-1}(Q_\beta) \subset Q_\gamma, \qquad \gamma \in I. \tag{3}$$

Так как Q_ν — прямые слагаемые, то из (3) вытекает

$$Q_\alpha = Q_\gamma, \qquad g^{-1}(Q_\beta) = Q_\alpha, \qquad g(Q_\alpha) = Q_\beta. \blacksquare$$

Пусть (1) — разложение пространства V на системы импримитивности группы G. Из леммы 1 следует, что каждый элемент группы G осуществляет некоторую подстановку $\bar{g}$ над системами импримитивности Q_ν, $\nu \in I$, т. е. разложение (1) определяет сюръективный гомоморфизм

$$\gamma\colon\ G \to \Gamma, \qquad g \longmapsto \bar{g}, \tag{4}$$

где

$$\bar{g}\colon\ Q_\nu \longmapsto g(Q_\nu), \qquad \nu \in I,$$

а Γ — множество всех $\bar{g}$. Ясно, что Γ — подгруппа симметрической группы $S(X)$, где X — множество всех Q_ν из (1). Пусть теперь ν — фиксированный индекс из I, а Γ_{Q_ν} — стабилизатор точки $Q_\nu \in X$ в группе Γ. Пользуясь гомоморфизмом (4), введем подгруппу H_ν группы G, положив

$$H_\nu = \gamma^{-1}(\Gamma_{Q_\nu}). \tag{5}$$

Очевидно, что

$$H_\nu = \{h \mid h \in G,\ h(Q_\nu) = Q_\nu\}.$$

При этих обозначениях верна

Теорема 1. *Пусть G — неприводимая импримитивная подгруппа группы $GL(V)$, а (1) — разложение пространства V на системы импримитивности G. Тогда:*

(i) *группа Γ транзитивна;*

(ii) *совокупность всех различных подгрупп H_ν, $\nu \in I$, есть класс сопряженных подгрупп группы G;*

(iii) *для любого $\nu \in I$ ограничение $G_\nu = H_\nu \mid Q_\nu$ есть неприводимая подгруппа группы $GL(Q_\nu)$;*

(iv) *для любых $\alpha, \beta \in I$ G_α и G_β подобны как линейные группы.*

Доказательство. Пусть Y — орбита группы Γ. Тогда сумма W всех подпространств Q_ν, принадлежащих Y, есть инвариантное относительно G подпространство пространства V. Отсюда и из неприводимости G вытекает $W = V$, $Q_\nu \in Y$ при любом $\nu \in I$, т. е. Γ транзитивна. (i) доказано. Докажем (ii). Так как Γ транзитивна, то совокупность всех различных стабилизаторов Γ_x составляет класс сопряженных подгрупп группы Γ (следствие 2.3.1). Отсюда и из (5) вытекает (ii). Переходим к доказательству (iii). В силу (i) для фиксированного $\alpha \in I$ мы можем построить такое множество

$$\{g_\nu\}, \quad \nu \in I, \tag{6}$$

элементов из G, что

$$g_\alpha = e, \qquad g_\nu(Q_\alpha) = Q_\nu.$$

Так как $\{\gamma(g_\nu)\}$, $\nu \in I$, — полная система представителей левых смежных классов группы Γ по подгруппе Γ_{Q_α}, то (6) — полная система представителей левых смежных классов G по H_α.

Пусть R_α — нетривиальное инвариантное относительно группы G_α подпространство пространства Q_α. Тогда

$$R_\nu = g_\nu(R_\alpha) \subset Q_\nu.$$

Положим

$$R = \dot{\sum} R_\nu, \qquad \nu \in I.$$

Для $g \in G$ имеем

$$gg_\nu = g_\mu h, \qquad h \in H_\alpha.$$

Поэтому

$$g(R_\nu) = gg_\nu(R_\alpha) = g_\mu h(R_\alpha) \subset g_\mu(R_\alpha) = R_\mu.$$

Следовательно, $g(R) \subset R$. Так как $R \neq V$, то последнее противоречит неприводимости группы G. (iii) доказано. Остается доказать (iv). С помощью элементов (6) зададим отображение

$$\varphi\colon Q_\alpha \to Q_\beta, \quad x \mapsto g_\beta(x), \quad x \in Q_\alpha.$$

Так как $g_\beta(Q_\alpha) = Q_\beta$, то φ — изоморфизм подпространств Q_α и Q_β. Как легко проверить,

$$H_\beta = g_\beta H_\alpha g_\beta^{-1}.$$

Для $b \in G_\beta = H_\beta | Q_\beta$ имеем

$$b = g_\beta h_\alpha g_\beta^{-1} | Q_\beta = \varphi a \varphi^{-1}, \quad a \in G_\alpha.$$

Следовательно,

$$G_\beta \subset \varphi G_\alpha \varphi^{-1}.$$

С другой стороны, $G_\alpha \subset \varphi^{-1} G_\beta \varphi$. Отсюда

$$G_\beta = \varphi G_\alpha \varphi^{-1}.$$

(iv) доказано. ■

Пусть G — неприводимая импримитивная подгруппа в $GL(V)$, а (1) — разложение V на системы импримитивности группы G. Разложение (1) называется *непродолжаемым*, если группы G_ν из теоремы 1 примитивны.

Лемма 2. *Пусть для неприводимой импримитивной подгруппы G группы $GL(V)$ существует такое разложение* (1) *пространства V над телом T на системы импримитивности G, что*

$$Q_\nu : T < \infty, \quad \nu \in I. \tag{7}$$

Тогда имеется непродолжаемое разложение V на системы импримитивности G.

Доказательство. Если группы G_ν примитивны, то (1) — непродолжаемое разбиение. Пусть группа G_α импримитивна и

$$Q_\alpha = Q_{\alpha 1} \dotplus \ldots \dotplus Q_{\alpha m}$$

— разложение Q_α на системы импримитивности группы G_α. С помощью элементов (6) построим систему подпространств

$$Q_{\nu l} = g_\nu (Q_{\alpha l}).$$

Пространство V можно представить в виде

$$V = \dot{\sum} Q_{\nu j}, \quad \nu \in I, \quad j = 1, \ldots, m. \tag{8}$$

Для $g \in G$ имеем

$$g(Q_{\nu j}) = gg_\nu (Q_{\alpha j}) = g_\mu h(Q_{\alpha j}) = g_\mu (Q_{\alpha k}) = Q_{\mu k}, \qquad h \in H_\alpha.$$

Следовательно, (8) также является разложением пространства V на системы импримитивности группы G, причем

$$Q_{\alpha j} : T < Q_\alpha : T < \infty.$$

Отсюда и вытекает лемма. ■

Следствие 1. *Для неприводимой импримитивной подгруппы G группы $GL(V)$, где V — пространство конечной размерности, всегда есть непродолжаемое разложение V на системы импримитивности G.*

Если для группы G существует такое разложение (1) на ее системы импримитивности, что все подпространства Q_ν одномерны, то группа G называется *мономиальной*.

Теорема 2. *Пусть G — неприводимая импримитивная подгруппа группы $GL(V)$, и пусть существует такое разложение* (1) *пространства V на системы импримитивности группы G, что* $\operatorname{card} I = k$, *где k — натуральное число. Тогда G обладает нормальным делителем N, индекс которого в G делит $k!$ и делится на k.*

Доказательство. Пусть $N = \operatorname{Ker} \gamma$ (см. (4)). Тогда, по теореме 1, $\Gamma \cong G/N$ — транзитивная подгруппа симметрической группы S_k. Отсюда и следует теорема. ■

В случае, когда V имеет конечную размерность n над телом T, верна

Теорема 3. (Критерий импримитивности.) *Неприводимая подгруппа G группы $GL(V)$ тогда и только тогда импримитивна, когда существует такое подпространство Q пространства V, что $Q : T = m < n$, $m \mid n$, а индекс подгруппы $H = \{h \mid h \in G,\ h(Q) = Q\}$ в G равен nm^{-1}.*

Доказательство. Пусть G — импримитивная неприводимая подгруппа $GL(V)$, а (1) — разложение V на системы импримитивности G. Полагая

$$Q = Q_\alpha, \qquad H = H_\alpha,$$

видим, что $Q:T=m$, $m|n$, а $G:H=nm^{-1}$. Необходимость доказана. Докажем достаточность. Пусть группа G неприводима, а подпространство Q в V удовлетворяет условиям теоремы, $k=nm^{-1}$,

$$b_1=e,\ b_2,\ \ldots,\ b_k$$

— полная система представителей левых смежных классов G по H. Построим подпространство

$$R=Q+b_2(Q)+\ \ldots\ +b_k(Q). \tag{9}$$

Для $g\in G$ имеем

$$g(b_\mu(Q))=b_\nu h(Q)=b_\nu(Q),\qquad h\in H.$$

Следовательно, $g(R)=R$. Так как группа G неприводима, то $R=V$. Но размерность R равна n только тогда, когда (9) — прямая сумма $b_\mu(Q)$. С другой стороны,

$$g(b_\mu(Q))=b_\nu(Q).$$

Таким образом, (9) — разложение V на системы импримитивности группы G. ■

2. Сплетение линейной группы и группы подстановок. Пусть U — линейное пространство над телом T, G_1 — подгруппа группы $GL(U)$, а Γ — подгруппа симметрической группы S_k, перемещающей числа $1, \ldots, k$, $k>1$. Декартову степень

$$U^k=V_1$$

будем трактовать как линейное пространство над телом T, произвольный вектор $v\in V$ будем записывать в виде

$$v=(u_1,\ \ldots,\ u_k),\qquad u_j\in U.$$

Для любых $f_1, \ldots, f_k\in G_1$, $s\in\Gamma$ определим отображение

$$f\colon V_1\to V_1,\qquad f=\langle f_1,\ \ldots,\ f_k,\ s\rangle,$$

положив

$$f(v)=f(u_1,\ \ldots,\ u_k)=\bar v\in V_1, \tag{10}$$

где $s(\nu)$-я компонента вектора $\bar v$ равна

$$f_\nu(u_\nu),\qquad \nu=1,\ \ldots,\ k.$$

Очевидно, что f — автоморфизм пространства V_1. Множество всех таких автоморфизмов f обозначим буквой F. Пусть $g = \langle g_1, \ldots, g_k, r\rangle \in F$. Тогда

$$gf(v) = g(\bar{v}) = (\bar{\bar{v}}) \in V_1,$$

где $rs(\bar{\bar{\nu}})$-я компонента вектора v равна

$$g_{s(\nu)}f_\nu(u_\nu), \qquad \nu = 1, \ldots, k.$$

Следовательно,

$$gf = \langle g_{s(1)}f_1, \ldots, g_{s(k)}f_k, rs\rangle \in F. \tag{11}$$

Из (11) вытекает, что F — подгруппа группы $GL(V_1)$. Группу F назовем *сплетением линейной группы* G_1 *и группы подстановок* Γ и обозначим $G_1 \wr \Gamma$.

Группа $F = G_1 \wr \Gamma$ *импримитивна*. Действительно, пусть подпространство Q_j пространства $V_1 = U^k$ состоит из всех векторов вида $(0, \ldots, u_j, \ldots, 0)$, где $u_j \in U$ является j-й компонентой ($j = 1, \ldots, k$). Тогда, очевидно,

$$V_1 = Q_1 \dotplus \ldots \dotplus Q_k. \tag{12}$$

В силу (10), для $f \in F$ имеем

$$f(Q_j) = Q_{s(j)}.$$

Следовательно, группа F импримитивна, а (12) — разложение пространства V_1 на системы импримитивности группы F.

Очевидно, что отображение

$$\tilde{\gamma}\colon F \to \Gamma, \qquad \langle f_1, \ldots, f_k, s\rangle \longmapsto s$$

является сюръективным гомоморфизмом, причем $\operatorname{Ker}\tilde{\gamma}$ — прямое произведение k экземпляров группы G_1. Следовательно, F — расширение прямого произведения k экземпляров группы G_1 с помощью группы Γ.

Лемма 3. *Пусть* G_1 *и* H — *сопряженные подгруппы группы* $GL(U)$, *а* Γ *и* Φ — *сопряженные подгруппы группы* S_k. *Тогда* $G_1 \wr \Gamma$ *и* $H \wr \Phi$ — *сопряженные подгруппы группы* $GL(U) \wr S_k$.

Доказательство. Пусть

$$H = aG_1a^{-1}, \qquad \Phi = b\Gamma b^{-1}, \qquad a \in GL(U), \qquad b \in S_k.$$

Возьмем в $GL(U) \wr S_k$ элемент $c = \langle a, \ldots, a, b \rangle$. Тогда

$$H \wr \Phi = c (G_1 \wr \Gamma) c^{-1}.$$

Действительно, из (11) вытекает

$$c^{-1} = \langle a^{-1}, \ldots, a^{-1}, b^{-1} \rangle.$$

Для $f \in F$ с помощью (11) находим

$$fc^{-1} = \langle f_{b^{-1}(1)} a^{-1}, \ldots, f_{b^{-1}(k)} a^{-1}, sb^{-1} \rangle,$$

$$cfc^{-1} = \langle af_{b^{-1}(1)} a^{-1}, \ldots, af_{b^{-1}(k)} a^{-1}, bsb^{-1} \rangle =$$

$$= \langle h_1, \ldots, h_k, \varphi \rangle, \quad h_j \in H, \quad \varphi \in \Phi.$$

Следовательно,

$$cfc^{-1} \in H \wr \Phi, \quad c (G_1 \wr \Gamma) c^{-1} \subset H \wr \Phi.$$

Таким же приемом докажем, что

$$c^{-1} (H \wr \Phi) c \subset G_1 \wr \Gamma.$$

Отсюда

$$c (G_1 \wr \Gamma) c^{-1} = H \wr \Phi. \blacksquare$$

Лемма 4. *Пусть G_1 — неприводимая подгруппа группы $GL(U)$, а Γ — транзитивная подгруппа симметрической группы S_k, $k > 1$. Тогда группа $F = G_1 \wr \Gamma$ почти всегда неприводима. Единственным исключением служит случай, когда U — одномерное пространство над полем $GF(2)$.*

Доказательство. Пусть выполняются условия леммы, U не является одномерным пространством над $GF(2)$, $R \neq (0)$ — инвариантное относительно F подпространство пространства V_1, $v \in R$, $v \neq 0$. Тогда

$$v = q_1 + \ldots + q_k, \quad q_j \in Q_j, \quad q_\alpha \neq 0.$$

Так как F содержит прямое произведение k экземпляров группы G_1, а U содержит, по меньшей мере, два различных ненулевых вектора, то в F есть такой элемент f, что

$$f(q_\nu) = q_\nu \quad \text{для} \quad \nu \neq \alpha,$$

$$f(q_\alpha) = p_\alpha \in Q_\alpha, \quad p_\alpha \neq q_\alpha.$$

Далее, $f(v) - v \in R$, следовательно,

$$v_\alpha = p_\alpha - q_\alpha \in R, \quad v_\alpha \neq 0, \quad v_\alpha \in Q_\alpha.$$

Так как группа G неприводима, то $Q_\alpha \subset R$. В силу транзитивности группы Γ отсюда вытекает, что

$$Q_\nu \subset R, \quad \nu = 1, \ldots, k.$$

Следовательно,

$$R = V_1,$$

т. е. группа F неприводима.

Остается рассмотреть случай, когда U — одномерное пространство над $GF(2)$. В этом случае в Q_j есть единственный ненулевой вектор q_j, и для $f \in F$ имеем

$$f(q_j) = q_{s(j)}, \quad s \in \Gamma.$$

Следовательно, для $v = q_1 \dotplus \ldots \dotplus q_k$ $f(v) = v$. Отсюда вытекает приводимость F. ■

Пусть теперь G — неприводимая импримитивная подгруппа $GL(V)$, где V — конечномерное линейное пространство над телом T,

$$V = Q_1 \dotplus \ldots \dotplus Q_k \tag{13}$$

— разложение V на системы импримитивности группы G, а

$$\gamma\colon G \to \Gamma \tag{14}$$

— гомоморфизм, определяемый разложением (13) (см. (4)). Так как группа Γ транзитивна, то в G можно выбрать такие элементы

$$g_1 = e, \ g_2, \ \ldots, \ g_k, \tag{15}$$

что

$$g_\nu(Q_1) = Q_\nu, \quad \nu = 1, \ldots, k.$$

Положим, как выше,

$$H_\nu = \{h \mid h \in G, \ h(Q_\nu) = Q_\nu\}, \quad G_\nu = H_\nu \mid Q_\nu, \quad \nu = 1, \ldots, k. \tag{16}$$

Если $\varphi_\nu = g_\nu \mid Q_1$, то, как следует из доказательства утверждения (iv) теоремы 1,

$$G_\nu = \varphi_\nu G_1 \varphi_\nu^{-1}. \tag{17}$$

Следовательно, если

$$v_{11}, \ldots, v_{1m} \tag{18}$$

— какой-либо базис пространства Q_1, а

$$v_{\nu j} = g_\nu(v_{1j}), \quad j = 1, \ldots, m,$$

то группа G_ν в базисе

$$v_{\nu 1}, \ldots, v_{\nu m} \tag{19}$$

задается той же группой A_1 матриц над T, что и группа G_1 в базисе (18).

При этих обозначениях верна

Лемма 5. *Группа G подобна как линейная группа некоторой подгруппе сплетения $G_1 \wr \Gamma$.*

Доказательство. Сперва построим подгруппу B группы $GL(V)$, изоморфную прямому произведению групп $G_1, \ldots, G_k$. Положим

$$B = B_1 \times \ldots \times B_k, \quad B_j \mid Q_j = G_j,$$

а $B_j \mid Q_i$ — единичная группа при $i \neq j$. Тогда для любого $g \in G$

$$gBg^{-1} = B.$$

Действительно, в силу (13),

$$g(Q_j) = Q_\nu.$$

Если $x \in Q_\nu$, $b_j \in B_j$, то

$$gb_jg^{-1}(x) = ga_jg^{-1}(x) = a_\nu(x) = b_\nu(x),$$

где $a_j \in G_j$, $a_\nu \in G_\nu$, $b_\nu \in B_\nu$. Если же $x \in Q_\mu$, $\mu \neq \nu$, то $g^{-1}(x) \in Q_i$, $i \neq j$, следовательно,

$$gb_jg^{-1}(x) = gb_j(g^{-1}(x)) = gg^{-1}(x) = x.$$

Отсюда

$$gB_jg^{-1} = B_\nu, \quad gBg^{-1} = B.$$

Рассмотрим теперь группу $\bar{F} = BG$. Так как для $b \in B$

$$b(Q_j) = Q_j,$$

то группа $\bar{F}$ тоже импримитивна и (13) есть разложение пространства V на системы импримитивности группы $\bar{F}$. Покажем, что группы $\bar{F}$ и $G_1 \wr \Gamma$ подобны как линейные группы. В качестве T-базиса V возьмем систему векторов

$$v_{11}, \ldots, v_{1m}, \ldots, v_{k1}, \ldots, v_{km} \tag{20}$$

(см. (18) и (19)). Для $g \in \bar{F}$ имеем

$$g(v_{\nu\mu}) = \sum_{j=1}^{m} v_{i_\nu j} \alpha_{j\mu}^{\nu}, \qquad \alpha_{j\mu}^{\nu} \in T, \tag{21}$$

где $i_1, \ldots, i_k$ — перестановка чисел $1, \ldots, k$. Из (21), в силу выбора базиса (20), находим

$$g_\nu g_{i_\nu}^{-1} g(v_{\nu\mu}) = \sum_{j=1}^{m} v_{\nu j} \alpha_{j\mu}^{\nu} = h^{\nu}(v_{\nu\mu}), \qquad h^{\nu} \in H_\nu. \tag{22}$$

Из (21) и (22) вытекает

$$a_\nu = \| \alpha_{j\mu}^{\nu} \| \in A_1. \tag{23}$$

Соотношения (21) и (23) показывают, что $\bar{F}$ подобна как линейная группа группе $G_1 \wr \Gamma$. Так как $\bar{F} \supset G$, то лемма доказана. ■

Пусть теперь $\bar{\theta}$ — какое-либо абстрактное теоретико-групповое свойство, подчиненное двум следующим условиям:

1) Если группа обладает свойством $\bar{\theta}$, то любая ее подгруппа и фактор-группа тоже обладают свойством $\bar{\theta}$.

2) Если нормальный делитель N группы H и фактор-группа H/N обладают свойством $\bar{\theta}$, то и H обладает свойством $\bar{\theta}$.

Группу, обладающую свойством $\bar{\theta}$, будем кратко называть $\bar{\theta}$-*группой*. $\bar{\theta}$-группами являются, например, разрешимые группы, П-группы и, в частности, p-группы. Из определения $\bar{\theta}$-группы следует, что сплетение $G_1 \wr \Gamma$ тогда и только тогда является $\bar{\theta}$-группой, когда G_1 и Γ суть $\bar{\theta}$-группы.

Теорема 4. *Пусть G — неприводимая максимальная $\bar{\theta}$-подгруппа группы $GL(V)$, где V — линейное пространство конечной размерности n над телом T. Тогда G либо примитивна, либо подобна как линейная группа сплетению $G_1 \wr \Gamma$, где G_1 — максимальная примитивная $\bar{\theta}$-подгруппа группы $GL(Q)$, а Γ — максимальная транзитивная $\bar{\theta}$-подгруппа симметрической группы S_k, Q — подпространство пространства V, $(Q:T)k = n$.*

Доказательство. Если группа G примитивна, то теорема очевидна. Пусть G импримитивна. Тогда, в силу леммы 2, для G существует непродолжаемое разложение (13) пространства V на системы импримитивности группы G. Так как G является θ-группой, то группы G_1 и Γ, связанные с разложением (13), — тоже θ-группы. Согласно лемме 5 группа G подобна как линейная группа группе $G_1 \wr \Gamma$, причем G_1 примитивна, а Γ транзитивна. Так как G максимальна среди θ-подгрупп $GL(V)$, а $G_1 \wr \Gamma$ есть θ-подгруппа, то G подобна $G_1 \wr \Gamma$. Из максимальности G также следует максимальность G_1 в $GL(Q)$ и максимальность Γ в S_k среди θ-подгрупп. ■

3. Кронекерово произведение линейных преобразований. Пусть X — пространство линейных форм над полем Δ с переменными

$$x_1, \ldots, x_n, \tag{24}$$

Y — пространство линейных форм над Δ с переменными

$$y_1, \ldots, y_m, \tag{25}$$

а V есть nm-мерное пространство билинейных форм над Δ с базисом

$$x_1y_1, \ldots, x_ny_1, \ldots, x_1y_m, \ldots, x_ny_m. \tag{26}$$

Пусть, далее, $f \in \mathrm{Hom}(X, X)$, $g \in \mathrm{Hom}(Y, Y)$, $a = \| \alpha_{ij} \|$ — матрица f в базисе (24), а $b = \| \beta_{kl} \|$ — матрица g в базисе (25). *Кронекеровым произведением эндоморфизмов* f и g назовем эндоморфизм $f \dot{\times} g$ пространства V, определяемый формулами

$$(f \dot{\times} g)(x_iy_j) = f(x_i)\, g(y_j), \tag{27}$$
$$i = 1, \ldots, n, \quad j = 1, \ldots, m.$$

Очевидно, что

$$(f \dot{\times} g)(x_iy_j) = \sum_{k=1}^{n} \sum_{l=1}^{m} x_k y_l \alpha_{ki} \beta_{lj}, \tag{28}$$
$$i = 1, \ldots, n, \quad j = 1, \ldots, m.$$

Как легко проверить, nm-матрица над Δ

$$\begin{bmatrix} a\beta_{11} & \ldots & a\beta_{1m} \\ \cdot & \cdot \; \cdot \; \cdot & \cdot \\ a\beta_{m1} & \ldots & a\beta_{mm} \end{bmatrix} = a \dot{\times} b \tag{29}$$

служит матрицей эндоморфизма $f \dot{\times} g$ в базисе (26). Матрица $a \dot{\times} b$, определяемая равенством (29), называется *кронекеровым произведением матриц* a и b.

Пусть теперь $\alpha \in \Delta$, a и c — матрицы из Δ_n, а b и d — из Δ_m. Тогда из (29) вытекают следующие равенства:

$$\left.\begin{aligned} (a \dot{\times} b)\alpha &= a\alpha \dot{\times} b = a \dot{\times} b\alpha, \\ (a+c) \dot{\times} b &= a \dot{\times} b + c \dot{\times} b, \\ a \dot{\times} (b+d) &= a \dot{\times} b + a \dot{\times} d, \\ (a \dot{\times} b)(c \dot{\times} d) &= ac \dot{\times} bd, \\ a \dot{\times} E_m &= \operatorname{diag}[a, \ldots, a] \in \Delta_{nm}, \\ E_n \dot{\times} b &= \begin{bmatrix} \beta_{11}E_n & \ldots & \beta_{1m}E_n \\ \cdot & \cdot \cdot \cdot & \cdot \\ \beta_{m1}E_n & \ldots & \beta_{mm}E_n \end{bmatrix}. \end{aligned}\right\} \quad (30)$$

В частности, для обратимых матриц a и b имеем

$$a^{-1} \dot{\times} b^{-1} = (a \dot{\times} b)^{-1}.$$

Из (29) следует, что

$$a \dot{\times} b = E_{nm} \Leftrightarrow a = \alpha E_n, \quad b = \beta E_m, \quad \alpha\beta = 1, \quad \alpha, \beta \in \Delta. \quad (31)$$

Если A — подмножество Δ_n, а B — подмножество Δ_m, то *кронекеровым произведением* $A \dot{\times} B$ назовем множество всех $a \dot{\times} b$, где $a \in A$, $b \in B$.

Кронекерово произведение определяет сюръективный гомоморфизм

$$h\colon\ GL(n, \Delta) \times GL(m, \Delta) \to GL(n, \Delta) \dot{\times} GL(m, \Delta),$$

где $GL(n, \Delta) \times GL(m, \Delta)$ — прямое произведение групп, а $h\colon \langle a, b\rangle \mapsto a \dot{\times} b$. Из (31) следует, что $\operatorname{Ker} h$ состоит из всех пар вида

$$\langle \alpha E_n, \alpha^{-1}E_m\rangle, \quad \alpha \in \Delta^*,$$

т. е.

$$\operatorname{Ker} h \cong \Delta^*.$$

Отсюда вытекает

Лемма 6. *Пусть A — подгруппа $GL(n, \Delta)$, а B — подгруппа $GL(m, \Delta)$. Тогда*

$$A \dot{\times} B \cong (A \times B)/M,$$

где $A \times B$ — *прямое произведение, а* M — *подгруппа группы* $A \times B$, *изоморфная некоторой подгруппе группы* Δ^*.

Лемма 7. *Пусть* G — *абсолютно неприводимая подгруппа* $GL(n, \Delta)$. *Тогда централизатор* C *группы* $G \dot{\times} E_m$ *в* $GL(nm, \Delta)$ *совпадает с* $E_n \dot{\times} GL(m, \Delta)$.

Доказательство. Запишем матрицы группы $GL(nm, \Delta)$ как $m \times m$-матрицы $c = \|c_{ij}\|$ над Δ_n. Если $c \in C$, то все c_{ij}, в силу (30), принадлежат централизатору G в Δ_n. Так как G абсолютно неприводима, то

$$c_{ij} = \gamma_{ij} E_n, \qquad \gamma_{ij} \in \Delta.$$

Отсюда и из последнего равенства (30) вытекает требуемое. ■

Лемма 8. *Пусть* A — *подгруппа* $GL(n, \Delta)$, *а* B — *подгруппа* $GL(m, \Delta)$. *Группа* $A \dot{\times} B$ *тогда и только тогда абсолютно неприводима, когда обе группы* A *и* B *абсолютно неприводимы.*

Доказательство. Рассмотрим линейную Δ-оболочку $[A \dot{\times} B]_\Delta$ группы $A \dot{\times} B$. Из (30) следует включение

$$[A \dot{\times} B]_\Delta \supset [A]_\Delta \dot{\times} [B]_\Delta. \tag{32}$$

Пусть A и B абсолютно неприводимы. Тогда

$$[A]_\Delta = \Delta_n, \qquad [B]_\Delta = \Delta_m.$$

Если теперь e_{ij} $(i, j = 1, \ldots, n)$ — канонический базис пространства Δ_n, ε_{kl} $(k, l = 1, \ldots, m)$ — канонический базис в Δ_m, то, как вытекает из (29), произведения $e_{ij} \dot{\times} \varepsilon_{kl}$ составят базис алгебры Δ_{nm}. Отсюда и из (32) следует

$$[A \dot{\times} B]_\Delta = \Delta_{nm}.$$

Достаточность доказана. Докажем необходимость. Пусть

$$a_1, \ldots, a_k$$

— максимальная система линейно независимых элементов в A,

$$b_1, \ldots, b_l$$

— максимальная система линейно независимых элементов в B. Тогда, в силу (30), любой элемент группы

$A \dot{\times} B$ есть линейная комбинация kl элементов вида

$$a_i \dot{\times} b_j, \quad i=1, \ldots, k, \quad j=1, \ldots, l.$$

Следовательно, из абсолютной неприводимости $A \dot{\times} B$ вытекает абсолютная неприводимость групп A и B. ■

Заметим, что в лемме 8 абсолютно неприводимые группы нельзя заменить неприводимыми. Неприводимость $A \dot{\times} B$ всегда влечет за собой неприводимость A и B, но, как показывает следующий пример, группа $A \dot{\times} B$ может оказаться приводимой, когда обе группы неприводимы. Действительно, пусть R — поле вещественных чисел, $A=B$ — группа всех вещественных матриц вида

$$\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}, \quad \alpha^2+\beta^2 \neq 0.$$

Очевидно, $A \dot{\times} A$ — абелева подгруппа группы $GL(4, R)$. Но в $GL(4, R)$ нет неприводимых абелевых подгрупп.

Возвратимся снова к произвольному полю Δ.

Лемма 9. *Из примитивности группы $A \dot{\times} B$ следует примитивность групп A и B.*

Доказательство. Пусть группа A импримитивна, а

$$u_{11}, \ldots, u_{1r}; \ldots; u_{s1}, \ldots, u_{sr}$$

— базисы s систем импримитивности группы A. Построим подпространство Q_i размерности r_m пространства V с базисом

$$u_{ik}y_j, \quad k=1, \ldots, r; \quad j=1, \ldots, m.$$

Очевидно, что

$$V=Q_1+\ldots+Q_s$$

— разложение V на системы импримитивности $A \dot{\times} B$. Таким же приемом доказывается, что импримитивность B влечет импримитивность $A \dot{\times} B$. ■

§ 16. О нормальных делителях вполне приводимых групп

1. Леммы о нормализаторе. Пусть V — конечномерное линейное пространство над телом T, H — подгруппа группы $GL(V)$, а G — нормализатор подгруппы H в $GL(V)$. Будем рассматривать пространство V как операторную аддитивную группу $V(\Omega)$ с областью операторов $\Omega = T \cup H$. Таким образом, допустимыми подгруппами группы $V(\Omega)$ окажутся такие подпространства W пространства V, что $h(W) = W$ для h из H. При этих предположениях докажем две следующие леммы.

Лемма 1. *Пусть $g \in G$, а W — допустимая подгруппа группы $V(\Omega)$. Тогда верны три утверждения:*

(i) *$g(W)$ — допустимая подгруппа группы $V(\Omega)$;*

(ii) *группа $H|g(W)$ подобна группе $H|W$;*

(iii) *$g(W)$ тогда и только тогда операторно проста, когда W операторно проста.*

Доказательство. По условию $h(W) = W$ для любого h из H. С другой стороны, каждый элемент $\bar{h}$ группы H можно записать в виде

$$\bar{h} = ghg^{-1}, \qquad h \in H.$$

Отсюда

$$\bar{h}(g(w)) = gh(w) = g(w).$$

(i) доказано. Для доказательства (ii) рассмотрим отображение γ: $W \to g(W)$, $x \mapsto g(x)$. Так как $g \in GL(V)$, то γ — изоморфизм подпространств W и $g(W)$ (операторность изоморфизма γ не утверждается!). Группа $H|g(W)$ есть множество всех отображений вида $\bar{h}|g(W)$, где $\bar{h} = ghg^{-1}$, $h \in H$. Для $x \in W$

$$\bar{h}(g(x)) = ghg^{-1}g(x).$$

Полагая $h|W = h_W$, отсюда находим

$$\bar{h}(g(x)) = \gamma h_W \gamma^{-1}(g(x)), \qquad \bar{h}\,|\,g(W) = \gamma h_W \gamma^{-1}.$$

Следовательно, группа $H|g(W)$ подобна $H|W$. Утверждение (iii) легко получить из (i). ■

Лемма 2. *Пусть $g \in G$, а W_1 и W_2 — операторно изоморфные допустимые подгруппы группы $V(\Omega)$. Тогда $g(W_2)$ операторно изоморфна группе $g(W_1)$.*

Доказательство. Пусть

$$f\colon W_1 \to W_2$$

— операторный изоморфизм. Тогда для $\lambda \in T$, $x, y \in W_1$, $h \in H$ имеем

$$f(x+y) = f(x) + f(y), \qquad f(x\lambda) = f(x)\lambda, \qquad f(hx) = hf(x).$$

Введем отображение

$$f_1\colon g(W_1)\to g(W_2), \qquad g(x)\mapsto g(f(x)).$$

Очевидно, f_1 биективно. Для f_1 находим

$$f_1(g(x)+g(y))=f_1(g(x+y))=g(f(x+y))=$$
$$=g(f(x)+f(y))=gf(x)+gf(y)=$$
$$=f_1(g(x))+f_1(g(y)),$$
$$f_1(g(x)\lambda)=f_1(g(x\lambda))=g(f(x\lambda))=g(f(x)\lambda)=$$
$$=g(f(x))\lambda=f_1(g(x))\lambda.$$

Для любого $h\in H$ положим

$$h_1=g^{-1}hg.$$

Тогда

$$f_1[h(g(x))]=f_1[g(h_1(x))]=g[f(h_1(x))]=g(h_1f(x))=$$
$$=gh_1(f(x))=hg(f(x))=hf_1(g(x)).$$

Следовательно, f_1 — операторный изоморфизм. ■

Приведем еще одну простую лемму о централизаторе группы H в $GL(V)$.

Лемма 3. *Если g принадлежит централизатору группы H в группе $GL(V)$, а W — допустимая подгруппа группы $V(\Omega)$, то подгруппы W и $g(W)$ операторно изоморфны.*

Доказательство. Отображение $\gamma\colon W\to g(W)$, где $\gamma(x)=g(x)$ для $x\in W$, является операторным изоморфизмом. Действительно, для любого h из H можно написать

$$\gamma(h(x))=gh(x)=hg(x)=h\gamma(x).\ ■$$

2. Теоремы Клиффорда. Пусть, как и выше, V — конечномерное линейное пространство над телом T.

Теорема 1. (Первая теорема Клиффорда.) *Пусть G — неприводимая подгруппа группы $GL(V)$, а H — нормальный делитель группы G. Тогда справедливы два следующих утверждения:*

(i) *H вполне приводим;*

(ii) *для любых двух инвариантных неприводимых относительно H подпространств W_1 и W_2 пространства V группы $H|W_1$ и $H|W_2$ подобны.*

Доказательство. Пусть L_1 — неприводимое инвариантное относительно H подпространство пространства V. Если $L_1 = V$, то теорема доказана. Если $L_1 \neq V$, то в G найдется такой элемент g_2, что

$$g_2(L_1) \neq L_1. \tag{1}$$

В силу леммы 1 $g_2(L_1)$ — инвариантное неприводимое относительно H подпространство. Так как верно (1), то $L_1 + g_2(L_1)$ — прямая сумма. Пусть теперь

$$g_2, \ldots, g_r \tag{2}$$

— такие элементы группы G, что

$$L = L_1 \dotplus g_2(L_1) \dotplus \ldots \dotplus g_r(L_1)$$

— прямая сумма, а для каждого $g \in G$ сумма $L + g(L_1)$ уже не является прямой. Так как размерность пространства V конечна, то такие элементы (2) существуют. Из построения пространства L и неприводимости пространства $g(L_1)$ относительно H находим

$$g(L_1) \cap L \neq (0), \qquad g(L_1) \subset L, \qquad gg_j(L_1) \subset L, \qquad g(L) = L.$$

Отсюда и из неприводимости группы G вытекает равенство $L = V$. Следовательно,

$$V = L_1 \dotplus g_2(L_1) \dotplus \ldots \dotplus g_r(L_1), \tag{3}$$

т. е. (i) доказано. Согласно предложению 13.1 любая операторно простая подгруппа W вполне приводимой группы $V(\Omega)$, где $\Omega = T \cup H$, операторно изоморфна одному из слагаемых $g_j(L_1)$ из (3). Отсюда и из леммы 1 вытекает (ii). ■

Следствие 1. *Нормальный делитель вполне приводимой подгруппы группы $GL(V)$ вполне приводим.*

Сохраняя обозначения теоремы 1, обратимся к разложению (3) и положим

$$L_\nu = g_\nu(L_1), \qquad \nu = 2, \ldots, r.$$

Очевидно, что

$$L_1, \ldots, L_r \tag{4}$$

— операторно простые допустимые подгруппы группы $V(\Omega)$, $\Omega = T \cup H$. Разобьем систему подпространств (4) на классы, относя L_μ и L_ν к одному классу тогда и только тогда, когда L_μ и L_ν операторно изоморфны.

Пусть k — число этих классов. Построим k прямых сумм

$$Q_1, \ldots, Q_k$$

подпространств (4), входящих в один класс. Тогда, очевидно,

$$V = Q_1 \dotplus \ldots \dotplus Q_k. \tag{5}$$

Теорема 2. (Вторая теорема Клиффорда.) *Если $k > 1$, то (5) — разложение пространства V на системы импримитивности группы G.*

Доказательство. Пусть $g \in G$, рассмотрим

$$g(Q_i), \quad i = 1, \ldots, k.$$

Согласно лемме 2 $g(Q_i)$ — прямая сумма операторно простых операторно изоморфных подгрупп. В силу предложения 13.3 каждая операторно простая подгруппа группы $V(\Omega)$ содержится в одной из подгрупп Q_j, $j = 1, \ldots, k$, причем две операторно простые операторно изоморфные подгруппы попадают в одну и ту же группу Q_j. Следовательно,

$$g(Q_i) \subset Q_j.$$

Отсюда и из определения импримитивности (см. § 15) вытекает, что (5) — разложение пространства V на системы импримитивности группы G, если $k > 1$. ■

С помощью подпространств (4) введем неприводимые части группы H, т. е. неприводимые представления d_j вида

$$d_j\colon H \to GL(L_j), \quad h \mapsto h \mid L_j, \quad j = 1, \ldots, r. \tag{6}$$

Из теоремы 2 вытекает

Следствие 1. *Неприводимые части нормального делителя H примитивной неприводимой группы G попарно эквивалентны.*

Число представлений d_j (см. (6)), эквивалентных фиксированному представлению d_ν, назовем *кратностью представления* d_ν.

Следствие 2. *Неприводимые части нормального делителя H неприводимой группы G имеют одну и ту же кратность.*

Доказательство. В силу леммы 15.1 Q_j имеют одну и ту же размерность. Подпространства L_i также одной и той же размерности. Следовательно, все неприводимые части группы H имеют одну и ту же кратность, равную

$$(Q_1 : T)(L_1 : T)^{-1}. \blacksquare$$

Следствие 3. *Если степень и кратность неприводимой части группы H равны 1, то G мономиальна.*

Лемма 4. *Пусть неприводимая подгруппа G группы $GL(V)$ представима в виде*

$$G = HF, \tag{7}$$

где H и F — поэлементно перестановочные нормальные делители G. Тогда неприводимые части группы $H(F)$ попарно эквивалентны.

Доказательство. Пусть L_1 — операторно простая допустимая подгруппа группы $V(\Omega)$, $\Omega = T \cup H$. Тогда, согласно (3) и предложению 13.1, любая операторно простая допустимая подгруппа группы $V(\Omega)$ операторно изоморфна группе вида $g(L_1)$, где $g \in G$. В силу (7)

$$g(L_1) = f(L_1), \quad f \in F.$$

Отсюда и из леммы 3 вытекает требуемое. $\blacksquare$

Применим теперь лемму 4 к случаю, когда $T = \Delta$, где Δ — поле, а G — абсолютно неприводимая подгруппа $GL(n, \Delta)$.

Лемма 5. *Пусть абсолютно неприводимая подгруппа G группы $GL(n, \Delta)$ представима в виде (7), l — степень неприводимой части группы H, m — степень неприводимой части F, причем $lm \leqslant n$. Тогда $lm = n$, а неприводимые части групп H и F абсолютно неприводимы.*

Доказательство. По условию

$$[G]_\Delta : \Delta = n^2.$$

Согласно лемме 4

$$[H]_\Delta : \Delta \leqslant l^2, \quad [F]_\Delta : \Delta \leqslant m^2.$$

С другой стороны, в силу (7),

$$n^2 = [G]_\Delta : \Delta \leqslant ([H]_\Delta : \Delta)([F]_\Delta : \Delta) \leqslant l^2 m^2.$$

Отсюда

$$n \leqslant lm, \qquad n = lm, \qquad [H]_\Delta : \Delta = l^2, \qquad [F]_\Delta : \Delta = m^2.$$

Следовательно, неприводимые части групп H и F абсолютно неприводимы. ■

Теорема 3. *Пусть абсолютно неприводимая подгруппа G группы $GL(n, \Delta)$ представима в виде* (7), l — *степень неприводимой части H, m — степень неприводимой части F и $lm \leqslant n$. Тогда группа G сопряжена в $GL(n, \Delta)$ с группой матриц*

$$\bar{G} = \bar{H} \dot{\times} \bar{F},$$

где $\bar{H}$ — абсолютно неприводимая подгруппа группы $GL(l, \Delta)$, $\bar{F}$ — абсолютно неприводимая подгруппа $GL(m, \Delta)$; $\bar{H} \cong H$, $\bar{F} \cong F$.

Доказательство. Согласно лемме 5 $lm = n$. В силу леммы 4 матрицы h группы H в некотором базисе B пространства Δ^n имеют вид

$$h = \bar{h} \dot{\times} E_m,$$

где $\bar{h}$ пробегает неприводимую подгруппу $\bar{H}$ группы $GL(l, \Delta)$, изоморфную H. В силу леммы 5 $\bar{H}$ абсолютно неприводима. Отсюда и из леммы 15.8 вытекает, что матрицы f группы F в базисе B имеют вид

$$f = E_l \dot{\times} \bar{f},$$

где $\bar{f}$ пробегает абсолютно неприводимую подгруппу $\bar{F}$ группы $GL(m, \Delta)$, изоморфную группе F. Следовательно, матрицы группы G в базисе B имеют вид $\bar{h} \dot{\times} \bar{f}$, причем любая матрица $\bar{h} \dot{\times} \bar{f}$ принадлежит G. ■

3. О нормализаторе вполне приводимой группы. Пусть снова V — конечномерное линейное пространство над телом T, а H — вполне приводимая подгруппа группы $GL(V)$. Как и выше, V будем рассматривать как аддитивную операторную группу $V(\Omega)$ с областью операторов $\Omega = T \cup H$. Пусть

$$V = L_1 \dotplus \ldots \dotplus L_m \tag{8}$$

— разложение $V(\Omega)$ в прямую сумму операторно простых допустимых подгрупп

$$L_j, \quad j = 1, \ldots, m. \tag{9}$$

Разобьем систему подгрупп (9) на классы, помещая L_i и L_j в один и тот же класс тогда и только тогда, когда L_i и L_j операторно изоморфны. Пусть k — число таких классов, а $Q_1, \ldots, Q_k$ — прямые суммы подгрупп L_j, входящих в один и тот же класс. Очевидно,

$$V = Q_1 \dotplus \ldots \dotplus Q_k. \tag{10}$$

Построим еще одно разложение пространства V в прямую сумму допустимых подгрупп. С этой целью систему подгрупп (9) разобьем на классы другим способом. Подгруппы L_i и L_j будем относить к одному и тому же классу тогда и только тогда, когда группы $H|L_i$ и $H|L_j$ подобны. Пусть l — число новых классов, а $W_1, \ldots, W_l$ — суммы подгрупп L_j, входящих в один и тот же класс. Тогда

$$V = W_1 \dotplus \ldots \dotplus W_l. \tag{11}$$

В силу предложения 13.3 разложение (10) не зависит от разложения (8) и определяется группой $V(\Omega)$ единственным образом с точностью до перестановки слагаемых, а любые операторно простые операторно изоморфные подгруппы группы $V(\Omega)$ содержатся в одной и той же группе Q_j.

Аналогичными свойствами обладает и разложение (11).

Лемма 6. *Разложение* (11) *единственно с точностью до перестановки слагаемых. Пусть P и P_1 — операторно простые подгруппы группы $V(\Omega)$ такие, что группы $H|P$ и $H|P_1$ подобны. Тогда для некоторого* μ

$$P \subset W_\mu, \quad P_1 \subset W_\mu. \tag{12}$$

Доказательство. Докажем справедливость включений (12). Согласно предложению 13.1 P операторно изоморфна некоторой группе L_i из разложения (8); P_1 — группе L_j. Так как ограничения $H|P$ и $H|P_1$ подобны, то отсюда следует, что и группы $H|L_i$ и $H|L_j$ также подобны. Пусть

$$L_i \subset Q_\lambda, \quad L_j \subset Q_\nu.$$

Тогда, в силу приведенных свойств разложения (10),

$$P \subset Q_\lambda, \quad P_1 \subset Q_\nu.$$

Так как $H|L_i$ и $H|L_j$ подобны, то найдется такое μ, $1 \leqslant \mu \leqslant l$, что

$$Q_\nu \subset W_\mu, \quad Q_\lambda \subset W_\mu.$$

Следовательно,

$$P \subset W_\mu, \quad P_1 \subset W_\mu.$$

(12) доказано. Из построения разложения (11) и из предложения 13.1 вытекает, что для любых операторно простых подгрупп U_1 и U_2 из W_μ группы $H|U_1$ и $H|U_2$ подобны. Отсюда и из (12) вытекает единственность разложения (11). ■

Пусть теперь $N(H)$ — нормализатор H в $GL(V)$, а $C(H)$ — централизатор H в $GL(V)$.

Лемма 7. *Каждое слагаемое W_μ разложения* (11) *является инвариантным подпространством относительно группы $N(H)$, а каждое слагаемое Q_j разложения* (10) *является инвариантным подпространством относительно группы $C(H)$.*

Доказательство. Пусть $g \in N(H)$, а P — операторно простая допустимая подгруппа W_μ. Согласно лемме 1 группы $H|P$ и $H|g(P)$ подобны. В силу леммы 6 $g(P) \subset W_\mu$. Следовательно,

$$g(W_\mu) = W_\mu.$$

Аналогично из леммы 3 вытекает вторая часть леммы 7. ■

Лемма 8. *Пусть $g \in N(H)$. Тогда*

$$g(Q_i) = Q_j \tag{13}$$

при некотором j.

Доказательство. По построению Q_i — прямая сумма операторно простых операторно изоморфных подгрупп группы $V(\Omega)$. В силу леммы 2 $g(Q_i)$ — тоже прямая сумма операторно простых операторно изоморфных подгрупп группы $V(\Omega)$. Следовательно,

$$g(Q_i) \subset Q_j$$

при некотором j. Ясно, что

$$Q_i \subset g^{-1}(Q_j) \subset Q_\lambda.$$

Так как Q_i и Q_λ — прямые слагаемые, то

$$\lambda = i, \quad g^{-1}(Q_j) = Q_i, \quad g(Q_i) = Q_j. \ ■$$

Очевидно, из построения разложений (10) и (11) вытекает, что каждое слагаемое W_μ разложения (11) является прямой суммой некоторых слагаемых Q_j разложения (10).

Из лемм 7 и 8 следует

Лемма 9. *Пусть $Q_j \subset W_\mu$, а U — прямая сумма всех Q_ν, входящих в W_μ и имеющих ту же размерность, что и Q_j. Тогда U — инвариантное относительно $N(H)$ подпространство пространства V.*

В заключение рассмотрим случай, когда $T = \Delta$, где Δ — алгебраически замкнутое поле, а неприводимые части группы H попарно эквивалентны. При этих условиях в подходящем базисе пространства $V = \Delta^n$ матрицы $h \in H$ принимают вид

$$h = h_1 \dot{\times} E_l, \tag{14}$$

где h_1 пробегает неприводимую подгруппу H_1 группы $GL(m, \Delta)$, изоморфную H, $ml = n$.

Лемма 10. *Пусть подгруппа H группы $GL(n, \Delta)$ состоит из матриц вида* (14). *Тогда ее нормализатор $N(H)$ в $GL(n, \Delta)$ совпадает с группой $N_1 \dot{\times} GL(l, \Delta)$, где N_1 — нормализатор H_1 в $GL(m, \Delta)$.*

Доказательство. Непосредственная проверка показывает, что

$$N_1 \dot{\times} GL(l, \Delta) \subset N(H). \tag{15}$$

Пусть теперь $g \in N(H)$, $h \in H$. Тогда

$$ghg^{-1} = g(h_1 \dot{\times} E_l)g^{-1} = \bar{h}_1 \dot{\times} E_l, \qquad \bar{h}_1 \in H_1.$$

Очевидно, отображение

$$\gamma_1 \colon h_1 \mapsto \bar{h}_1$$

является автоморфизмом группы H_1; его можно продолжить до автоморфизма

$$\gamma \colon [H_1]_\Delta \to [H_1]_\Delta.$$

Так как группа H_1 неприводима и поле Δ алгебраически замкнуто, то

$$[H_1]_\Delta = \Delta_m.$$

Следовательно, γ — внутренний автоморфизм Δ_m, и поэтому для $g \in N(H)$ в $GL(m, \Delta)$ найдется такой элемент g_1, что при любом $h_1 \in H_1$

$$g(h_1 \dot{\times} E_l) g^{-1} = g_1 h_1 g_1^{-1} \dot{\times} E_l.$$

Отсюда вытекает, что $g_1 \in N_1$. Ясно, что для любого $h \in H$

$$ghg^{-1} = (g_1 \dot{\times} E_l) h (g_1 \dot{\times} E_l)^{-1}.$$

Следовательно, $(g_1 \dot{\times} E_l)^{-1} g$ принадлежит централизатору $C(H)$ группы H в $GL(n, \Delta)$. Согласно лемме 15.8

$$C(H) = E_m \dot{\times} GL(l, \Delta).$$

Отсюда

$$g \in (g_1 \dot{\times} E_l)(E_m \dot{\times} GL(l, \Delta)) \subset N_1 \dot{\times} GL(l, \Delta).$$

Последнее включение вместе с (15) доказывает лемму. ■

§ 17. Некоторые условия полной приводимости линейной группы над полем

1. Полупростые матрицы и d-матрицы. d-группы. Пусть Δ — произвольное поле, V — линейное пространство размерности n над Δ, а $a \in \operatorname{End} V$. Очевидно, *эндоморфизм a тогда и только тогда неприводим* (т. е. в V нет нетривиальных инвариантных относительно a подпространств), *когда его характеристический полином неприводим в* $\Delta[x]$. Хорошо также известно, что *эндоморфизм a тогда и только тогда вполне приводим* (т. е. V — прямая сумма неприводимых инвариантных относительно a подпространств), *когда минимальный полином $m(x)$ эндоморфизма a не имеет в кольце $\Delta[x]$ кратных множителей.* Вполне приводимые эндоморфизмы из $\operatorname{End} V$ называют также *полупростыми* эндоморфизмами. Матрицы полупростых эндоморфизмов будем называть полупростыми матрицами. Иными словами, матрица a из Δ_n называется *полупростой* над Δ, если в $GL(n, \Delta)$ есть такая матрица t, что

$$t^{-1}at = \operatorname{diag}[a_1, \ldots, a_k],$$

где a_j — матрица с неприводимым в $\Delta[x]$ характеристическим полиномом, $j = 1, \ldots, k$.

Введем еще одно определение. Матрица $a \in \Delta_n$ называется *d-матрицей*, если существует такое расширение Σ поля Δ и такая матрица $t \in GL(n, \Sigma)$, что

$$t^{-1}at = \operatorname{diag}[\lambda_1, \ldots, \lambda_n], \quad \lambda_j \in \Sigma; \quad j = 1, \ldots, n.$$

Ясно, что в качестве Σ здесь можно взять поле разложения характеристического полинома матрицы a.

Из определения d-матрицы и свойств минимальных полиномов матриц вытекает, что *матрица a из Δ_n тогда и только тогда является d-матрицей, когда ее минимальный полином $m(x)$ взаимно прост с производной $m'(x)$. Следовательно, всякая d-матрица полупроста. Для совершенных полей Δ класс d-матриц совпадает с классом полупростых матриц. В случае же несовершенного поля Δ класс полупростых матриц над Δ шире класса d-матриц над Δ.*

Подгруппа G группы $GL(n, \Delta)$ называется *d-группой*, если каждый элемент из G является d-матрицей.

Лемма 1. *Пусть A — множество попарно перестановочных d-матриц из Δ_n. Тогда существуют такое конечное расширение Σ поля Δ и такая матрица $t \in GL(n, \Sigma)$, что все матрицы множества $t^{-1}At$ диагональны.*

Доказательство. Очевидно, достаточно рассмотреть лишь случай конечного A, ибо в A есть конечная максимальная система линейно независимых матриц. Пусть A конечно, а Σ — поле разложения полинома $f(x) \in \Delta[x]$, где $f(x)$ — произведение характеристических полиномов матриц A. Доказывать будем индукцией по степени n. Для $n = 1$ лемма очевидна. Пусть $n > 1$, и пусть для матриц степени, меньшей n, лемма доказана. Если все матрицы a из A скалярны, то лемма тоже очевидна. Пусть в A есть нескалярная матрица a. Так как a является d-матрицей, то в $GL(n, \Sigma)$ есть такая матрица u, что

$$u^{-1}au = \operatorname{diag}[\lambda_1 E_{n_1}, \ldots, \lambda_k E_{n_k}], \quad k > 1,$$
$$\lambda_i \neq \lambda_j \quad \text{при} \quad i \neq j.$$

Следовательно, матрицы b множества $u^{-1}Au$ имеют вид

$$b = \operatorname{diag}[b_1, \ldots, b_k], \quad b_j \in \Sigma_{n_j}; \quad j = 1, \ldots, k.$$

Очевидно, b_j является d-матрицей, причем b_j пробегает некоторое множество B_j попарно перестановочных матриц из Σ_{n_j}, когда b пробегает $B = u^{-1}Au$. Так как $n_j < n$, то, по индуктивному предположению, в $GL(n_j, \Sigma)$ есть такая матрица t_j, что все матрицы $t_j^{-1}B_jt_j$ диагональны. Следовательно, все матрицы множества $t^{-1}At$, где

$$t = u \cdot \mathrm{diag}\,[t_1, \ldots, t_k],$$

диагональны. ■

Лемма 2. *Множество A попарно перестановочных d-матриц из Δ_n вполне приводимо.*

Доказательство. Пусть Σ — поле, существование которого утверждается в лемме 1, A_1 — подалгебра алгебры Δ_n, порождаемая E_n и A, а A_2 — подалгебра алгебры Σ_n, порождаемая E_n и A. В силу леммы 1 в A_2 нет ненулевых нильпотентных элементов. Следовательно, их нет и в $A_1 \subset A_2$, т. е. A_1 полупроста и A вполне приводимо. ■

Как вытекает из леммы 1, для любых перестановочных d-матриц $a, b \in \Delta_n$ и любых $\lambda, \mu \in \Delta$ матрицы ab и $\lambda a + \mu b$ — тоже d-матрицы. Ниже приводится простой пример, показывающий, что ни это замечание, ни лемма 2 не переносятся на полупростые матрицы. Пусть p — простое число, $x^p - \delta$ — неприводимый полином из $\Delta[x]$, где Δ — поле характеристики p. Рассмотрим множество A, состоящее из двух матриц a и b степени $n = 2p$:

$$a = \begin{bmatrix} c & c \\ 0 & c \end{bmatrix}, \quad b = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix},$$

где c — матрица из Δ_p, характеристический полином которой совпадает с $x^p - \delta$. Очевидно, $ab = ba$. Далее,

$$a^p = \left(b + \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix}\right)^p = b^p = \delta E_n.$$

Следовательно, $x^p - \delta$ — минимальный полином матрицы a, т. е. a и b — полупростые матрицы. Очевидно, что A — приводимое множество матриц. A неразложимо. Действительно, если бы A было разложимым, то A было бы и вполне приводимым. Однако группа G, порождаемая матрицами a и b, содержит нормальный делитель (u),

$$u=\begin{bmatrix} E_p & E_p \\ 0 & E_p \end{bmatrix},$$

и по теореме Клиффорда не может быть вполне приводимой. Итак, A — неразложимое приводимое множество перестановочных полупростых матриц. Матрицы ab^{-1}, $a-b$ не полупросты, хотя a, b, b^{-1} полупросты.

Лемма 3. *Пусть G — группа полупростых матриц из $GL(n, \Delta)$, $\gamma_1, \ldots, \gamma_k$ — неприводимые части группы G. Если все группы $\operatorname{Im}\gamma_j$, $j=1, \ldots, k$, абелевы, то группа G тоже абелева.*

Доказательство. Если все $\operatorname{Im}\gamma_j$ абелевы, то все матрицы коммутанта G' группы G унипотентны. Так как каждая матрица из G полупроста, то $G'=(E)$. ■

Лемма 4. *Периодическая группа G матриц над полем Δ тогда и только тогда является d-группой, когда* $\operatorname{char}\Delta \notin \Pi(G)$.

Доказательство. Пусть G есть d-группа, $g\in G$, k — порядок элемента g. Тогда для любого простого делителя q числа k и некоторого расширения Σ поля Δ в группе Σ^* есть элемент порядка q. Следовательно, $\operatorname{char}\Delta \notin \Pi(G)$. Обратно. Пусть $\operatorname{char}\Delta\notin\Pi(G)$. Тогда для любого g из G $\operatorname{char}\Delta$ не делит порядок k элемента g. Минимальный полином матрицы g делит полином $\psi(x)=x^k-1$, $(\psi(x), \psi'(x))=1$. Следовательно, g является d-матрицей, а G является d-группой. ■

Следствие 1. *Конечная группа матриц над полем Δ тогда и только тогда является d-группой, когда* $\operatorname{char}\Delta$ *не делит ее порядок.*

Лемма 5. *Пусть группа G матриц над полем Δ имеет такой нормальный делитель H, что H является d-группой, G/H — периодическая группа, а* $\operatorname{char}\Delta\notin\Pi(G/H)$. *Тогда G является d-группой.*

Доказательство. Для $g\in G$ существует такое целое $k>0$, что $g^k=h\in H$, $\operatorname{char}\Delta\notin\Pi(k)$. Так как H есть d-группа, то минимальный полином $m(x)$ матрицы h взаимно прост с $m'(x)$. Очевидно, что $m(x^k)$ — аннулирующий матрицу g полином.

Так как

$$(m(x^k),\ km'(x^k)\,x^{k-1})=1,$$

то полином $m(x^k)$ не имеет кратных корней ни в каком расширении поля Δ. Следовательно, g является d-матрицей. ■

2. Об условиях полной приводимости.

Теорема 1 (Дж. Диксон [1]). *Пусть G — подгруппа группы $GL(n, \Delta)$, а H — вполне приводимая подгруппа группы G конечного индекса j, причем* $\operatorname{char}\Delta = 0$ *или* $(\operatorname{char}\Delta, j) = 1$. *Тогда группа G вполне приводима.*

Доказательство. Пусть G действует в пространстве Δ^n, а $Q \neq (0)$ — подпространство пространства Δ^n, инвариантное относительно G. Покажем, что Q обладает инвариантным относительно G дополнением. Тем самым будет доказана теорема. Так как H — вполне приводимая подгруппа группы G, то $\Delta^n = Q \dotplus L$, где L — инвариантное относительно H подпространство Δ^n. Введем эндоморфизм π пространства Δ^n, положив,

$$\pi \mid Q = 0, \qquad \pi \mid L = e,$$

где e — единица $\operatorname{Hom}(L, L)$. Пусть B — полная система представителей левых смежных классов группы G по подгруппе H. Построим эндоморфизм σ_B пространства Δ^n, положив

$$\sigma_B = \frac{1}{j} \sum_{x \in B} x\pi x^{-1}. \tag{1}$$

Подпространство $P = \operatorname{Im}\sigma_B = \sigma_B\Delta^n$ не зависит от выбора системы B. Действительно,

$$x\pi x^{-1}\Delta^n = x\pi\Delta^n = xL.$$

Следовательно, если $y = xh$, $h \in H$, то

$$y\pi y^{-1}\Delta^n = y\pi\Delta^n = yL = xhL = xL.$$

Легко видеть, что для $g \in G$ множество gB также является полной системой представителей левых смежных классов группы G по подгруппе H и справедливо равенство

$$g\sigma_B = \frac{1}{j}\left(\sum_{x \in B} (gx)\,\pi\,(gx)^{-1}\right) g = \sigma_{gB}g. \tag{2}$$

Подпространство P инвариантно относительно G. Действительно, из (2) получаем

$$gP = g\sigma_B\Delta^n = \sigma_{gB}g\Delta^n = \sigma_{gB}\Delta^n = \sigma_B\Delta^n = P.$$

Эндоморфизм σ_B обладает следующими двумя свойствами:

$$\operatorname{Ker}\sigma_B = Q, \qquad P \cap Q = \operatorname{Im}\sigma_B \cap \operatorname{Ker}\sigma_B = (0). \tag{3}$$

Действительно, для $q \in Q$ $x\pi x^{-1}q = 0$. Следовательно,

$$Q \subset \operatorname{Ker}\sigma_B. \tag{4}$$

Пусть теперь $u = q + l$, $q \in Q$, $l \in L$. Тогда

$$x^{-1}(q + l) = q_1 + l_1, \qquad q_1 \in Q, \qquad l_1 \in L.$$

Отсюда

$$x(q_1 + l_1) = q_1' + x(l_1) = q + l, \qquad q_1' \in Q.$$

Следовательно,

$$x(l_1) = q_2 + l, \qquad q_2 \in Q,$$

$$x\pi x^{-1}(q + l) = x\pi(q_1 + l_1) = x(l_1) = q_2 + l.$$

Отсюда

$$\sigma_B(q + l) = q_3 + l, \qquad q_3 \in Q. \tag{5}$$

Если $\sigma_B(q + l) = 0$, то, в силу (5), $l = 0$. Отсюда и из (4) получаем

$$\operatorname{Ker}\sigma_B = Q.$$

Если $\sigma_B(q + l) \in Q$, то, в силу (5), $l = 0$. Следовательно, $P \cap Q = (0)$, т. е. (3) доказано. Из (3) получаем $\Delta^n = Q \dotplus P$, где P — инвариантное относительно G подпространство. ∎

Следствие 1. *Если порядок конечной группы матриц над полем Δ не делится на* $\operatorname{char}\Delta$, *то группа вполне приводима.*

Следствие 2. *Конечная d-группа матриц G над произвольным полем Δ вполне приводима.*

Доказательство. В силу леммы 4 $\operatorname{char}\Delta$ не делит порядок группы G. Отсюда и из следствия 1 вытекает следствие 2. ∎

Теорема 2 (Платонов [7]). *Пусть Δ — произвольное поле, G — подгруппа в $GL(n, \Delta)$, обладающая таким вполне приводимым нормальным делителем H,* *что G/H — локально конечная группа и* $\operatorname{char}\Delta \notin \Pi(G/H)$. *Тогда группа G вполне приводима.*

Доказательство. Пусть $g_1, \ldots, g_r$ — максимальная линейно независимая система матриц из G, G_1 — группа, порожденная $g_1, \ldots, g_r$, H. Из локальной конечности группы G/H следует конечность группы G_1/H. $\operatorname{char}\Delta$ не делит индекс $G_1:H$, следовательно по теореме 1, группа G_1 вполне приводима. Так как линейные оболочки групп G_1 и G совпадают, то G тоже вполне приводима. ■

Лемма 6. *Пусть Δ — поле простой характеристики p, а b — такая d-матрица из Δ_n, что матрица b^p диагональна. Тогда b тоже диагональна.*

Доказательство. Положим

$$a = b^p = \operatorname{diag}\left[\lambda_1 E_{n_1}, \ldots, \lambda_k E_{n_k}\right], \ \lambda_j \in \Delta, \ \lambda_i \neq \lambda_j \text{ при } i \neq j.$$

Так как $ab = ba$, то

$$b = \operatorname{diag}[b_1, \ldots, b_k], \qquad b_j \in \Delta_{n_j}; \qquad j = 1, \ldots, k.$$

Докажем, что все b_j скалярны. Для b_j можно написать

$$b_j^p = \lambda_j F_{n_j}. \tag{6}$$

Очевидно, что b_j есть d-матрица. Следовательно, существует такое расширение Σ_j поля Δ, что в $GL(n_j, \Sigma_j)$ найдется матрица t_j, для которой

$$t_j b_j t_j^{-1} = \operatorname{diag}\left[\rho_1, \ldots, \rho_{n_j}\right].$$

Из (6) находим

$$b_j^p = t_j b_j^p t_j^{-1} = \operatorname{diag}\left[\rho_1^p, \ldots, \rho_{n_j}^p\right] = \lambda_j E_{n_j},$$

где $\rho_1^p = \ldots = \rho_{n_j}^p = \lambda_j$. Так как $p = \operatorname{char}\Delta$, то $\rho_1 = \ldots$ $\ldots = \rho_{n_j} = \rho$,

$$t_j b_j t_j^{-1} = \rho E_{n_j}, \qquad b_j = \rho E_{n_j}, \qquad \rho \in \Delta.$$

Следовательно, все b_j скалярны, а матрица b диагональна. ■.

Теорема 3. *Пусть Δ — произвольное поле, а G есть d-подгруппа группы $GL(n, \Delta)$, обладающая таким абелевым нормальным делителем F, что фактор-группа G/F локально конечна. Тогда G вполне приводима.*

Доказательство. Если $\operatorname{char}\Delta = 0$, то теорема следует из теоремы 2. Пусть $\operatorname{char}\Delta = p$, где p — простое число. Достаточно рассматривать случай, когда группа G/F конечна. Пусть G/F конечна. Согласно лемме 1 существует такое расширение Σ поля Δ и такая матрица $t \in GL(n, \Sigma)$, что группа tFt^{-1} состоит из диагональных матриц. Положим

$$F_1 = tFt^{-1}, \qquad G_1 = tGt^{-1}.$$

Очевидно, что G_1 и F_1 — подгруппы в $GL(n, \Sigma)$. Рассмотрим еще группу F_2 всех диагональных матриц из $GL(n, \Sigma)$, содержащихся в группе G_1. Очевидно,

$$G_1 \supset F_2 \supset F_1.$$

По условию G_1/F_1 — конечная группа. Пусть теперь cF_1 — элемент порядка p^α фактор-группы G_1/F_1. Тогда $c \in F_2$. Действительно, рассмотрим элементы

$$c, c^p, \ldots, c^{p^{\alpha-1}}, c^{p^\alpha}.$$

В силу выбора c $c^{p^\alpha} \in F_1$. Согласно лемме 6 $c^{p^{\alpha-1}}$ — диагональная матрица, следовательно, $c^{p^{\alpha-1}} \in F_2$. Применяя несколько раз лемму 6, получим, $c \in F_2$, т. е.

$$cF \in F_2/F_1.$$

Таким образом, F_2/F_1 содержит p-подгруппу Силова группы G_1/F_1. Отсюда вытекает, что индекс $G_1 : F_2$ не делится на p. F_2 — вполне приводимая подгруппа $GL(n, \Sigma)$. Так как

$$t^{-1}F_2(t) \subset G \subset GL(n, \Delta),$$

то $t^{-1}F_2t$ — вполне приводимая подгруппа в G, индекс которой взаимно прост с $\operatorname{char}\Delta$. По теореме 1 группа G вполне приводима. ■

Отметим без доказательства еще одно условие полной приводимости:

Теорема 4 (Супруненко [16]). *Пусть Δ — совершенное поле, а G — подгруппа группы $GL(n, \Delta)$, имеющая вполне приводимый нормальный делитель N. Если фактор-группа G/N периодическая и* $\operatorname{char}\Delta \notin \Pi(G/N)$, *то группа G вполне приводима.*

Известны примеры приводимых, но неразложимых d-групп (см. Платонов, Залесский [1], Мерзляков [2]).

ГЛАВА V

РАЗРЕШИМЫЕ ГРУППЫ МАТРИЦ

§ 18. Приводимые разрешимые группы

1. Специальная треугольная группа. Пусть Δ — ассоциативное кольцо с единицей 1. Группу всех матриц вида

$$\begin{bmatrix} 1 & \alpha_{12} & \alpha_{13} & \ldots & \alpha_{1n} \\ 0 & 1 & \alpha_{23} & \ldots & \alpha_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix},$$

где α_{ij} — произвольные элементы кольца Δ, $n > 1$, будем называть *специальной треугольной группой* и обозначать $T(n, \Delta)$.

Здесь мы покажем, что группа $T(n, \Delta)$ разрешима, а длина ряда ее коммутантов зависит только от n. Очевидна

Лемма 1. *Любые две матрицы вида*

$$\begin{bmatrix} E_m & B \\ 0 & E_{n-m} \end{bmatrix},$$

где B есть $m \times (n-m)$-матрица над кольцом Δ, перестановочны.

Введем теперь число $\mu = \mu(n)$, положив

$$\mu(n) = [\log_2(n-1)] + 1.$$

Очевидно, число μ определяется неравенствами:

$$2^{\mu} > n - 1 \geqslant 2^{\mu-1}.$$

Теорема 1. *Группа $T(n, \Delta)$ разрешима. Длина ряда коммутантов группы $T(n, \Delta)$ равна $\mu(n) = [\log_2(n-1)] + 1$.*

Доказательство. Положим $T(n, \Delta) = G_n$ и покажем сперва, что μ-й коммутант $G_n^{(\mu)}$ группы G_n равен (E_n). Доказывать равенство

$$G_n^{(\mu)} = (E_n) \tag{1}$$

будем индукцией по числу μ. Если $\mu(n) \leqslant 2$, то $n \leqslant 4$, а для $n \leqslant 4$ равенство (1) легко проверяется. Пусть $\mu(n) > 2$, и для $\mu - 1$ равенство доказано. Положим $m = 2^{\mu-1}$. Тогда

$$2^{\mu-1} > m - 1 > 2^{\mu-2}, \qquad \mu(m) = \mu(n) - 1 = \mu - 1.$$

Следовательно, по индуктивному предположению,

$$G_m^{(\mu-1)} = (E_m).$$

Из последнего равенства вытекает, что матрицы a группы $G_n^{(\mu-1)}$ имеют такой вид, что $m-1$ диагоналей матрицы a, находящихся над главной диагональю, состоят из нулей. Так как $n - m \leqslant m$, то матрицу a удобно записать так:

$$a = \begin{bmatrix} E_m & B \\ 0 & E_{n-m} \end{bmatrix}. \tag{2}$$

В силу леммы 1 из (2) вытекают коммутативность группы $G_n^{(\mu-1)}$ и равенство (1). Теперь надо показать, что

$$G_n^{(\mu-1)} \neq (E_n). \tag{3}$$

Из определения $\mu = \mu(n)$ находим

$$n \geqslant 2^{\mu-1} + 1.$$

Положим $2^{\mu-1} + 1 = \alpha$. В группе G_n есть элементарная матрица

$$t_{1\alpha} = t_{1\alpha}(1) = E_n + e_{1\alpha}.$$

Неравенство (3) можно получить с помощью следующей таблицы:

$$\begin{array}{llllll}
t_{12} & t_{13} & t_{15} & t_{19} & \ldots\ t_{1,\,2^{\mu-2}+1} & t_{1\alpha} \\
t_{23} & t_{24} & t_{26} & t_{2,\,10} & \ldots\ t_{2^{\mu-2}+1,\,\alpha} & \\
t_{34} & t_{35} & t_{37} & t_{3,\,11} & \ldots & \\
\cdot & \cdot & \cdot & \cdot & & \\
t_{\alpha-1,\,\alpha} & t_{\alpha-2,\,\alpha} & t_{\alpha-4,\,\alpha} & t_{\alpha-8,\,\alpha} & &
\end{array}$$

где $t_{ij} = t_{ij}(1)$. Действительно, по лемме 8.3, элементы второго столбца этой таблицы — коммутаторы элементов первого столбца, элементы третьего столбца — коммутаторы элементов второго и т. д., следовательно,

$$t_{13} \in G_n^{(1)}, \quad t_{15} \in G_n^{(2)}, \quad \ldots, \quad t_{1,\,2^\beta+1} \in G_n^{(\beta)}.$$

В частности,

$$t_{1\alpha} = t_{1,\,2^{\mu-1}+1} \in G_n^{(\mu-1)}, \qquad G_n^{(\mu-1)} \neq (E_n). \ \blacksquare$$

Рассмотрим теперь группу $T(n_1, \ldots, n_k, \Delta)$, состоящую из всех матриц вида

$$a = \begin{bmatrix} E_{n_1} & a_{12} & \ldots & a_{1k} \\ 0 & E_{n_2} & \ldots & a_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & E_{n_k} \end{bmatrix}, \tag{4}$$

где $n_1 + n_2 + \ldots + n_k = n$, a_{ij} — произвольная $n_i \times n_j$-матрица над кольцом Δ.

Теорема 2. *Длина ряда коммутантов группы* $T(n_1, \ldots, n_k, \Delta)$ *равна* $\mu(k) = [\log_2(k-1)] + 1$.

Доказательство. Положим

$$H_k = T(n_1, \ldots, n_k, \Delta)$$

и покажем сперва, что

$$H_k^{(\mu)} = (E_n), \tag{5}$$

где $\mu = \mu(k)$. Равенство (5) будем доказывать индукцией по числу μ. Для $\mu = 1, 2$ оно очевидно. Пусть $\mu > 2$ и для $\mu - 1$ (5) доказано. Для k верны неравенства

$$2^{\mu-1} + 1 \leqslant k < 2^\mu + 1.$$

Положим $l = 2^{\mu-1}$. Тогда

$$2^{\mu-2} + 1 < l < 2^{\mu-1} + 1$$

и, по индуктивному предположению,

$$H_l^{(\mu-1)} = (E_n).$$

Отсюда следует, что матрицы группы $H_k^{(\mu-1)}$ имеют вид

$$b=\begin{bmatrix} E_{n_1} & 0 & \ldots & 0 & b_{1,l+1} & \ldots & \ldots & \ldots & b_{1k} \\ 0 & E_{n_2} & 0 & \ldots & 0 & b_{2,l+2} & \ldots & \ldots & b_{2k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \ldots & \ldots & 0 & E_{n_{k-l}} & 0 & \ldots & 0 & b_{k-l,k} \\ 0 & \ldots & \ldots & \ldots & 0 & E_{n_{k-l+1}} & 0 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & E_{n_k} \end{bmatrix}. \tag{6}$$

В силу выбора числа l имеем $2l\geqslant k$, $k-l\leqslant l$. Из последнего неравенства вытекает

$$n_1+n_2+\ldots+n_{k-l}+n_{l+1}+\ldots+n_k\leqslant$$
$$\leqslant n_1+n_2+\ldots+n_{k-l}+n_{k-l+1}+n_{k-l+2}+\ldots+n_k=n.$$

Следовательно, матрицу (6) можно записать в виде

$$b=\begin{bmatrix} E_s & B_{st} \\ 0 & E_t \end{bmatrix},$$

где

$$s=n_1+\ldots+n_{k-l}, \qquad t=n-s.$$

Отсюда и из леммы 1 следует, что $H_k^{(\mu-1)}$ — абелева группа, т. е.

$$H_k^{(\mu)}=(E_n).$$

Теперь остается показать, что

$$H_k^{(\mu-1)}\neq(E_n). \tag{7}$$

Введем матрицы T_{ij}. Матрицу вида (4) такую, что

$$a_{ij}=\begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 0 \end{bmatrix}=\varepsilon_{ij},$$

а остальные $a_{\lambda\nu}=0$, обозначим символом T_{ij}. Положим $\alpha=2^{\mu-1}+1$ и составим следующую таблицу:

$$\left.\begin{array}{llllll} T_{12} & T_{13} & T_{15} & \ldots & T_{1,\,2^{\mu-2}+1} & T_{1,\,\alpha} \\ T_{23} & T_{24} & T_{26} & \ldots & T_{2^{\mu-2}+1,\,\alpha} & \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & & & \\ T_{\alpha-1,\,\alpha} & T_{\alpha-2,\,\alpha} & T_{\alpha-4,\,\alpha} & & & \end{array}\right\} \tag{8}$$

В этой таблице матрицы второго столбца — коммутаторы матриц первого, матрицы третьего столбца — коммутаторы матриц второго и т. д. Действительно, как легко проверить,

$$\varepsilon_{ij}\varepsilon_{jl}=\varepsilon_{il}.$$

Если теперь положить

$$T_{ij}-E_n=\hat{E}_{ij},$$

то

$$\hat{E}_{ij}\hat{E}_{jl}=\hat{E}_{il},$$

а при $\lambda\neq j$

$$\hat{E}_{ij}\hat{E}_{\lambda l}=0.$$

Отсюда находим

$$\left.\begin{aligned} T_{ik}T_{kj}&=E_n+\hat{E}_{ik}+\hat{E}_{kj}+\hat{E}_{ij},\\ T_{ik}^{-1}T_{kj}^{-1}&=E_n-\hat{E}_{ik}-\hat{E}_{kj}+\hat{E}_{ij}, \end{aligned}\right\} \tag{9}$$

где i, j, k — попарно различные числа.

Перемножая равенства (9), получим

$$T_{ik}T_{kj}T_{ik}^{-1}T_{kj}^{-1}=E_n+\hat{E}_{ij}=T_{ij}. \tag{10}$$

Из (10) и следует отмеченное свойство таблицы (8). Таким образом,

$$T_{13}\in H_k^{(1)},\quad T_{15}\in H_k^{(2)},\ \ldots,\ T_{1,\,2^{\beta}+1}\in H_k^{(\beta)},$$
$$T_{1,\,2^{\mu-1}+1}\in H_k^{(\mu-1)}.$$

Следовательно, верно (7). ■

2. Редукция к примитивным группам. Пусть теперь Δ — поле, а G — произвольная подгруппа группы

$GL(n, \Delta)$. Тогда в подходящем базисе пространства Δ^n матрицы g группы G принимают вид

$$g = \begin{bmatrix} a_1(g) & a_{12}(g) & \dots & a_{1k}(g) \\ 0 & a_2(g) & \dots & a_{2k}(g) \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & a_k(g) \end{bmatrix}, \tag{11}$$

где отображение

$$\gamma_i\colon\ G \to GL(n_i, \Delta), \qquad g \mapsto a_i(g),$$

— неприводимое представление группы G степени n_i, а $a_{ij}(g)$ есть $n_i \times n_j$-матрица над Δ, $n_1 + n_2 + \dots$ $\dots + n_k = n$ (см. § 14).

Теорема 3. *Группа G матриц вида* (11) *тогда и только тогда разрешима, когда разрешимы все группы*

$$G_i = \operatorname{Im}\gamma_i, \qquad i = 1, \dots, k. \tag{12}$$

Доказательство. Необходимость. Пусть группа G разрешима. Тогда разрешим любой ее гомоморфный образ. Следовательно, все группы (12) разрешимы.

Достаточность. Пусть разрешимы все группы (12). Рассмотрим гомоморфизм

$$f\colon\ G \to GL(n, \Delta) \tag{13}$$

$$f(g) = \operatorname{diag}[a_1(g), \dots, a_k(g)], \qquad g \in G.$$

Очевидно, группа $\operatorname{Im} f$ разрешима. С другой стороны, матрицы из $\operatorname{Ker} f$ имеют вид (4). Следовательно,

$$\operatorname{Ker} f \subset T(n_1, \dots, n_k, \Delta).$$

Отсюда вытекает разрешимость группы $\operatorname{Ker} f$ и разрешимость группы G. ■

Если группа G матриц вида (11) — максимальная разрешимая подгруппа группы $GL(n, \Delta)$, то группы (12) являются максимальными разрешимыми подгруппами групп $GL(n_i, \Delta)$, группа $\operatorname{Im} f$ изоморфна прямому произведению групп (12), а элементы $a_{ij}(g)$ суть произвольные $n_i \times n_j$-матрицы над полем Δ. Таким образом, максимальная разрешимая подгруппа группы $GL(n, \Delta)$ задается последовательностью групп $G_1, \dots, G_k$, где

G_i — максимальная разрешимая неприводимая подгруппа группы $GL(n_i, \Delta)$,

$$n_1 + n_2 + \ldots + n_k = n.$$

Теорема 4. *Пусть максимальная разрешимая подгруппа* $\mathfrak{G}$ *группы* $GL(n, \Delta)$ *приводима. Тогда* $\mathfrak{G}$ *сопряжена в* $GL(n, \Delta)$ *с полупрямым произведением*

$$HT(n_1, \ldots, n_k, \Delta) \tag{14}$$

групп H *и* $T(n_1, \ldots, n_k, \Delta)$, *где* H — *группа всех матриц вида* $h = \operatorname{diag}[h_1, \ldots, h_k]$, $h_j \in G_j$, G_j — *максимальная разрешимая неприводимая подгруппа группы* $GL(n_j, \Delta)$, $j = 1, \ldots, k$, H — *прямое произведение групп* $G_1, \ldots, G_k$.

Доказательство. Согласно теореме 3 группа (14) разрешима. Группа $\mathfrak{G}$ сопряжена в $GL(n, \Delta)$ с группой G матриц вида (11). Очевидно, что любой элемент $g \in G$ представим в виде

$$g = f(g)\,u, \qquad u \in T(n_1, \ldots, n_k, \Delta), \qquad f(g) \in H.$$

Следовательно,

$$G \subset HT(n_1, \ldots, n_k, \Delta).$$

Так как G — максимальная разрешимая подгруппа группы $GL(n, \Delta)$, то

$$G = HT(n_1, \ldots, n_k, \Delta). \blacksquare$$

Теорема 5. *Пусть* G — *неприводимая разрешимая подгруппа группы* $GL(n, \Delta)$. *Тогда* G *либо примитивна, либо сопряжена в* $GL(n, \Delta)$ *с некоторой подгруппой сплетения*

$$\bar{G} \wr \Gamma, \tag{15}$$

где $\bar{G}$ — *примитивная разрешимая подгруппа в* $GL(m, \Delta)$, Γ — *транзитивная разрешимая подгруппа симметрической группы* S_k, *а* $km = n$. *В частности, максимальная разрешимая неприводимая подгруппа группы* $GL(n, \Delta)$ *либо примитивна, либо сопряжена в* $GL(n, \Delta)$ *с группой* (15), *где* $\bar{G}$ — *максимальная примитивная разрешимая подгруппа группы* $GL(m, \Delta)$, *а* Γ — *максимальная транзитивная подгруппа группы* S_k.

Эта теорема следует из теоремы 15.4.

§ 19. Примитивные разрешимые группы. Ограниченность длины ряда коммутантов разрешимой линейной группы

1. Абелев нормальный делитель примитивной разрешимой группы. Пусть Δ — произвольное поле, G — примитивная разрешимая подгруппа группы $GL(n, \Delta)$, а H — абелев нормальный делитель группы G.

Лемма 1. *В $GL(n, \Delta)$ есть разрешимая группа $\mathfrak{G}$, обладающая максимальным абелевым нормальным делителем F, такая, что $\mathfrak{G} \supset G$, $F \supset H$, F является мультипликативной группой поля K, K — расширение поля ΔE_n, $\Delta E_n \subset K \subset \Delta_n$, $K : \Delta$ делит число n.*

Доказательство. Согласно теоремам Клиффорда (§ 16) H вполне приводима и ее неприводимые части попарно эквивалентны. Если m_1 — степень неприводимой части группы H, то m_1 делит n, а линейная Δ-оболочка $[H] = \Sigma_1$ есть поле, степень которого над Δ равна m_1.

Положим $H_1 = \overset{*}{\Sigma}_1$. Тогда для $g \in G$

$$gH_1g^{-1} = H_1.$$

Следовательно,

$$G_1 = H_1G$$

— разрешимая группа, а H_1 — ее абелев нормальный делитель. Если H_1 — максимальный абелев нормальный делитель в G_1, то лемма доказана, ибо в качестве $\mathfrak{G}$ можно взять G_1, в качестве F — группу H_1. Если же H_1 содержится в другом абелевом нормальном делителе H_1' группы G_1, то строим разрешимую группу

$$G_2 = H_2G_1,$$

где

$$H_2 = \overset{*}{\Sigma}_2, \qquad \Sigma_2 = [H_1'], \qquad \Sigma_2 \supset \Sigma_1, \qquad \Sigma_2 \neq \Sigma_1.$$

Если H_2 — максимальный абелев нормальный делитель группы G_2, то лемма доказана. Если же $H_2 \subset H_2'$, где H_2' — другой абелев нормальный делитель группы G_2, то строим группу

$$G_3 = H_3G_2, \qquad H_3 = \overset{*}{\Sigma}_3, \qquad \Sigma_3 = [H_2'], \qquad \Sigma_3 \supset \Sigma_2, \qquad \Sigma_3 \neq \Sigma_2$$

и т. д. Так как степени полей Σ_1, Σ_2, Σ_3, ... суть делители числа n и включения

$$\Sigma_1 \subset \Sigma_2 \subset \Sigma_3 \subset \ldots$$

строгие, то процесс построения полей Σ_j конечен и для некоторого j группа

$$H_j = \Sigma_j^*$$

есть максимальный абелев нормальный делитель группы

$$G_j = H_j G_{j-1}.$$

Полагая

$$\mathfrak{G} = G_j, \qquad F = H_j,$$

получим требуемое. ■

Пусть теперь G — примитивная разрешимая подгруппа в $GL(n, \Delta)$, обладающая таким максимальным абелевым нормальным делителем F, что

$$F = K^*, \qquad \Delta E_n \subset K \subset \Delta_n, \tag{1}$$

K — расширение поля ΔE_n, $K : \Delta = m$, $m \mid n$. Обозначим буквой V централизатор группы F в G, а символом $\mathcal{G}(K/\Delta)$ — группу всех автоморфизмов поля K, оставляющих неподвижным каждый элемент поля ΔE_m. Тогда верна

Теорема 1. *Фактор-группа G/V изоморфна некоторой разрешимой подгруппе группы $\mathcal{G}(K/\Delta)$.*

Доказательство. Рассмотрим отображение

$$f\colon\ G \to \mathcal{G}(K/\Delta), \qquad g \mapsto \sigma_g, \tag{2}$$

где $\sigma_g\colon K \to K$, $\sigma_g(x) = gxg^{-1}$, $x \in K$. Так как $F = K^*$, то $\operatorname{Ker} f = V$. Отсюда

$$G/V \cong \operatorname{Im} f \subset \mathcal{G}(K/\Delta). \ ■$$

Следствие 1. $G : V \leqslant K : \Delta = m$.

При рассмотрении группы V пространство Δ^n, где она действует, удобно трактовать как пространство размерности $r = n/m$ над полем K. Так как каждый элемент v из V перестановочен с каждым элементом λ из K, то $V \subset GL(r, K)$. Ясно, что $GL(r, K)$ есть централизатор группы F в $GL(n, \Delta)$. В частности, если

$$K : \Delta = n,$$

то
$$F = K^* = GL(1, K) = V.$$

Отсюда и из теоремы 1 вытекает

Следствие 2. *Если $K : \Delta = n$, то $V = F$, а группа G/F изоморфна разрешимой подгруппе группы $\mathscr{G}(K/\Delta)$, $G : F \leqslant n$.*

2. Абелев нормальный делитель фактор-группы G/F. Здесь мы сохраняем обозначения первого пункта. Будем предполагать, что
$$V \neq F. \tag{3}$$

При условии (3) фактор-группа G/F обладает отличным от единицы абелевым нормальным делителем A/F, содержащимся в V/F. Таким, например, будет предпоследний член ряда коммутантов фактор-группы V/F.

Итак, пусть A/F — неединичный абелев нормальный делитель фактор-группы G/F, содержащийся в группе V/F.

Лемма 2. *Центр группы A совпадает с F.*

Доказательство. $F \subset A \subset V$. Следовательно, F содержится в центре $Z_1(A)$ группы A. С другой стороны, $Z_1(A)$ — абелев нормальный делитель в G. Так как F — максимальный абелев нормальный делитель группы G, то $Z_1(A) = F$. ■

Лемма 3. (i) *Порядок каждого элемента фактор-группы A/F конечен и является делителем числа $r = n/m$.*

(ii) *Пусть ν — порядок элемента aF из A/F. Тогда классом элементов, сопряженных с a в группе A, является следующая совокупность:*
$$a,\ \gamma a,\ \gamma^2 a,\ \ldots,\ \gamma^{\nu-1} a,$$
где γ — элемент порядка ν из K^*. В группе A найдется такой элемент b, что порядок коммутатора $(a, b) = aba^{-1}b^{-1}$ равен ν.

(iii) *Коммутант A' группы A есть конечная циклическая группа, порядок которой совпадает с экспонентой группы A/F.*

Доказательство. Для любых a и b из A
$$ab = \lambda ba, \quad \lambda \in K^*, \quad a^t b = \lambda^t b a^t.$$

Далее, $ab \in GL(r, K)$,

$$\det(ab) = \det(\lambda ba) = \lambda^r \det(ab).$$

Следовательно,

$$\lambda^r = 1, \qquad a^r b = b a^r. \tag{4}$$

Из (4), в силу леммы 2, получаем

$$a^r \in F, \qquad (aF)^r = F.$$

Следовательно, порядок ν элемента aF является делителем числа r. (i) доказано.

Если теперь $c, d \in A$, то, очевидно,

$$(a, c)(a, d) = (a, cd), \qquad (a, c)^r = 1, \qquad (a, c) \in K^*.$$

Следовательно, множество всех коммутаторов вида (a, c), где c пробегает группу A, а элемент a фиксирован, есть конечная циклическая группа (γ). Пусть τ — порядок группы (γ). Тогда для любого $c \in A$

$$(a^\tau, c) = (a, c)^\tau = 1.$$

Следовательно,

$$a^\tau \in F, \qquad (aF)^\tau = F, \qquad \nu \mid \tau.$$

С другой стороны,

$$(a, c)^\nu = (a^\nu, c) = 1,$$

значит, $\tau \mid \nu$, $\nu = \tau$, т. е. порядок элемента γ равен ν. Отсюда следует (ii). Действительно,

$$cac^{-1} = (c, a)\, a = \gamma^t a.$$

С другой стороны, $(a, b) = \gamma$ при некотором b.

Остается доказать (iii). Из (4) следует, что A' — конечная циклическая подгруппа группы K^*. Пусть теперь ν_1 — экспонента группы A/F. Тогда в A есть такой элемент a_1, что порядок a_1F из A/F равен ν_1. Для любого $a \in A$ порядок ν элемента $aF \in A/F$ делит число ν_1. Согласно (ii) для любого $c \in C$ порядок элемента $(a, c) = \gamma^t$ делит число ν. Следовательно, для любой пары u и v из A

$$(u, v)^\nu = (u, v)^{\nu_1} = 1.$$

С другой стороны, в группе A есть такой элемент b_1, что порядок элемента $\gamma_1 = (a_1, b_1)$ равен ν_1. Значит,

$$\gamma_1 \in A', \qquad (u, v) \in (\gamma_1), \qquad A' = (\gamma_1),$$

т. е. порядок группы A' равен ν_1. ∎

Рассмотрим теперь линейную K-оболочку $[A]$ группы A.

Лемма 4. $A : F = [A] : K$.

Доказательство. Если $c_1, \ldots, c_k$ — линейно независимые над K элементы группы A, то, очевидно, они принадлежат различным смежным классам A по F. Пусть, обратно,

$$d_1, \ldots, d_\mu \tag{5}$$

— представители μ различных смежных классов группы A по F. Покажем, что они линейно независимы над K. Для любого элемента a группы A

$$ad_ja^{-1} = f_jd_j, \qquad f_j \in F, \tag{6}$$

причем при $i \neq j$ найдется такой элемент $a \in A$, что в (6) $f_i \neq f_j$. Действительно, пусть $f_i = f_j$ для каждого $a \in A$, т. е.

$$ad_ia^{-1}d_i^{-1} = ad_ja^{-1}d_j^{-j}, \qquad (a, d_j^{-1}d_i) = 1.$$

Отсюда следует, что $d_j^{-1}d_i \in F$, $d_i \in d_jF$, ибо F — центр группы A. Последнее противоречит выбору элементов (5). Пусть теперь система (5) линейно зависима над K и

$$\lambda_1d_1 + \ldots + \lambda_\mu d_\mu = 0, \qquad \lambda_i \in K, \tag{7}$$

— нетривиальное соотношение с наименьшим из возможных количеством ненулевых коэффициентов. Можно считать, что $\lambda_1, \lambda_2 \neq 0$. Пусть a — такой элемент группы A, что

$$ad_1a^{-1}d_1^{-1} = f_1 \neq f_2 = ad_2a^{-1}d_2^{-1}.$$

Тогда из (7) получим

$$f_1(\lambda_1d_1 + \ldots + \lambda_\mu d_\mu) - a(\lambda_1d_1 + \ldots + \lambda_\mu d_\mu)a^{-1} = 0,$$
$$\lambda_2(f_1 - f_2)d_2 + \ldots + \lambda_\mu(f_1 - f_\mu)d_\mu = 0, \qquad \lambda_2(f_1 - f_2) \neq 0.$$

Последнее противоречит выбору соотношения (7). Теперь уже легко доказать лемму. Пусть

$$u_1, \ldots, u_k \tag{8}$$

— максимальная линейно независимая над K система элементов группы A. Тогда (8) есть K-базис алгебры $[A]$, все элементы (8) принадлежат различным классам группы A по F. С другой стороны, в силу предыдущего замечания, (8) — полная система представителей смежных классов группы A по F. ■

Так как $A \subset GL(r, K)$, $[A] \subset K_r$, то из леммы 4 вытекает

$$A : F = [A] : K \leqslant r^2 = \frac{n^2}{m^2}. \tag{9}$$

Теорема 2. *В группе A есть пары элементов $a_1, b_1, a_2, b_2, \ldots, a_t, b_t$, обладающие следующими свойствами:*

(i) *$(a_i, b_i) = \varepsilon_i$ — элемент группы F порядка ν_i, $\nu_{i+1} \mid \nu_i$;*

(ii) *элементы, принадлежащие двум разным парам, перестановочны;*

(iii) *каждый элемент a группы A единственным образом представляется в виде $a = fa_1^{\alpha_1}b_1^{\beta_1} \ldots a_t^{\alpha_t}b_t^{\beta_t}$, $f \in F$, $0 \leqslant \alpha_i < \nu_i$, $0 \leqslant \beta_i < \nu_i$.*

Доказательство. Пусть ν_1 — наибольшее число среди порядков элементов группы A/F. Тогда, согласно лемме 3, в группе A есть такая пара элементов a_1, b_1, что $(a_1, b_1) = \varepsilon_1$ — элемент порядка ν_1. Группу A можно представить в виде

$$A = (a_1)(b_1)A_1, \tag{10}$$

где A_1 — централизатор множества $\{a_1, b_1\}$ в A. В самом деле, число элементов группы A, сопряженных с a_1, равно ν_1. Следовательно,

$$A : A_1 \leqslant \nu_1^2.$$

С другой стороны, ν_1^2 произведений $a_1^{\alpha_1}b_1^{\beta_1}$, $0 \leqslant \alpha_1 < \nu_1$, $0 \leqslant \beta_1 < \nu_1$, принадлежат различным смежным классам группы A по A_1, поскольку

$$(a_1^{\alpha_1}b_1^{\beta_1}, b_1) = \varepsilon_1^{\alpha_1}, \qquad (a_1, a_1^{\alpha_1}b_1^{\beta_1}) = \varepsilon_1^{\beta_1}.$$

Следовательно,

$$A : A_1 = \nu_1^2$$

и верно (10).

Если группа A_1 абелева, то

$$A_1 = F, \qquad A = (a_1)(b_1)F$$

и теорема доказана. Пусть $A_1 \neq F$, а ν_2 — наибольшее число среди порядков элементов фактор-группы A_1/F. В силу выбора числа ν_1 имеем $\nu_2 | \nu_1$. Согласно лемме 3 и равенству (10) в группе A_1 есть такая пара элементов a_2, b_2, что $(a_2, b_2) = \varepsilon_2$, ε_2 — элемент группы F порядка ν_2. Тогда

$$A_1 = (a_2)(b_2)A_2,$$

где A_2 — централизатор множества $\{a_1, b_1, a_2, b_2\}$ в группе A. Отсюда

$$A = (a_1)(b_1)(a_2)(b_2)A_2,$$

причем элементы $a_1^{\alpha_1}b_1^{\beta_1}a_2^{\alpha_2}b_2^{\beta_2}$, $0 \leqslant \alpha_i < \nu_i$, $0 \leqslant \beta_i < \nu_i$, $i = 1, 2$, принадлежат различным смежным классам группы A по A_2. Так как A/F — конечная группа, то после конечного числа шагов мы придем к равенству

$$A = (a_1)(b_1) \ldots (a_t)(b_t)F,$$

где элементы $a_1^{\alpha_1}b_1^{\beta_1} \ldots a_t^{\alpha_t}b_t^{\beta_t}$, $0 \leqslant \alpha_i < \nu_i$, $0 \leqslant \beta_i < \nu_i$, $i = 1, \ldots, t$, лежат в разных смежных классах группы A по F. ■

Следствие 1. $A : F = \nu_1^2 \ldots \nu_t^2$.

3. Конечность индекса максимального абелева нормального делителя. До сих пор мы считали, что A/F — произвольный отличный от единицы абелев нормальный делитель группы G/F, содержащийся в V/F. Пусть теперь A/F — такая подгруппа в G/F, что выполняются три следующих условия:

1) A/F — абелев нормальный делитель группы G/F;
2) $A/F \subset V/F$;
3) группа A/F максимальна среди подгрупп группы G/F, обладающих свойствами 1) и 2).

Тогда справедлива

Теорема 3. *Группа A/F совпадает со своим централизатором в группе V/F.*

Доказательство. Пусть B/F — централизатор A/F в V/F, а C — централизатор A в V. Так как A/F — нормальный делитель в G/F, то B — нормальный делитель группы G. Очевидно, выполняются следующие включения: $B \supset C \supset F$. Покажем сперва, что

$$B = AC. \tag{11}$$

Для $a \in A$ и $b \in B$, очевидно, $(a, b) \in F$. В частности, $(a_j, b) \in F$, $(b, b_j) \in F$, где a_j, b_j — элементы A, обладающие свойствами (i), (ii), (iii), сформулированными в теореме 2. Далее, так как $a_j^{\nu_j} b_j^{\nu_j} \in F$, то

$$\left(a_j^{\nu_j}, b\right) = \left(a_j, b\right)^{\nu_j} = 1, \qquad \left(b, b_j^{\nu_j}\right) = \left(b, b_j\right)^{\nu_j} = 1.$$

Следовательно,

$$\left(a_j, b\right) = \varepsilon_j^{\beta_j}, \qquad \left(b, b_j\right) = \varepsilon_j^{\alpha_j},$$

где $j = 1, \ldots, t$, $0 \leqslant \beta_j < \nu_j$, $0 \leqslant \alpha_j < \nu_j$. С другой стороны, элемент $a = a_1^{\alpha_1} b_1^{\beta_1} \ldots a_t^{\alpha_t} b_t^{\beta_t}$ удовлетворяет условиям

$$\left(a_j, a\right) = \varepsilon_j^{\beta_j}, \qquad \left(a, b_j\right) = \varepsilon_j^{\alpha_j}, \qquad j = 1, \ldots, t.$$

Отсюда

$$(a_j, a^{-1}b) = (a^{-1}b, b_j) = 1,$$

где $j = 1, \ldots, t$; следовательно, $a^{-1}b \in C$, $b \in aC$, $B \subset AC$ что влечет (11).

Пусть теперь $B/F \neq A/F$. Тогда предпоследний член D/F ряда коммутантов группы B/F отличен от единицы. D/F — абелев нормальный делитель в G/F, но группа D/F не может быть абелевой в силу максимальности группы A/F. Следовательно, группа D содержит такие элементы d, d_1, что

$$(d, d_1) \notin F. \tag{12}$$

Согласно (11)

$$d = ac, \qquad d_1 = a'c', \qquad a, a' \in A, \qquad c, c' \in C.$$

Следовательно, $(d, d_1) = (a, a')(c, c') \in C$. Так как $(d, d_1) \in A$, то

$$(d, d_1) \in A \cap C = F,$$

что противоречит (12). ■

Следствие 1. *Централизатор группы A в группе V совпадает с F.*

Следствие 2. *Централизатор группы A в G совпадает с F.*

Теорема 4.

$$G : F \leqslant \rho(n) = n^2(n^2-1)(n^2-2)\ldots(n^2-2^{l-1}), \quad (13)$$

где $l = [2\log_2 n]$.

Доказательство. Возможны два случая: $V = F$ и $V \neq F$. В первом случае, в силу теоремы 1,

$$G : F \leqslant m \leqslant n < \rho(n).$$

Во втором случае

$$G : F = (G : V)(V : A)(A : F). \quad (14)$$

Оценим индекс $V : A = (V : F) : (A : F)$. Согласно теореме 3 группа A/F совпадает со своим централизатором в V/F. Следовательно, фактор-группа $V/F/A/F$ изоморфна некоторой разрешимой подгруппе группы $\mathrm{Aut}(A/F)$. Так как $\mathrm{card}(A/F) \leqslant r^2 = n^2/m^2$, то

$$\mathrm{card}\ \mathrm{Aut}(A/F) \leqslant (r^2-1)(r^2-2)\ldots(r^2-2^{k-1}),$$

где $k = [2\log_2 r]$. Отсюда и из (13) получим

$$G : F \leqslant m(r^2-1)(r^2-2)\ldots(r^2-2^{k-1})\frac{n^2}{m^2} =$$

$$= \frac{n^2}{m}(r^2-1)\ldots(r^2-2^{k-1}) \leqslant \rho(n). \ \blacksquare$$

Теорема 5. *Всякая примитивная разрешимая подгруппа $\mathfrak{G}$ группы $GL(n, \Delta)$ обладает абелевым нормальным делителем, индекс которого не больше числа $\rho(n)$* (см. (13)). *Индекс максимального абелева нормального делителя группы $\mathfrak{G}$ не больше $\rho(n)$.*

Доказательство. Пусть $\mathfrak{H}$ — максимальный абелев нормальный делитель группы $\mathfrak{G}$. Согласно лемме 1, группа $\mathfrak{G}$ содержится в разрешимой группе G, максимальный абелев нормальный делитель F которой есть мультипликативная группа поля K, а $\mathfrak{H} \subset F$. Так как

$$\mathfrak{G}F : F \leqslant G : F \leqslant \rho(n), \qquad \mathfrak{G}F : F = \mathfrak{G} : (\mathfrak{G} \cap F),$$

то

$$\mathfrak{G} : (\mathfrak{G} \cap F) \leqslant \rho(n).$$

Очевидно, $\mathfrak{G} \cap F$ — абелев нормальный делитель группы $\mathfrak{G}$. Так как $\mathfrak{H} \subset F$, то $\mathfrak{G} \cap F \supset \mathfrak{H}$. Из максимальности $\mathfrak{H}$ тогда следует $\mathfrak{G} \cap F = \mathfrak{H}$. Значит, $\mathfrak{G} : \mathfrak{H} \leqslant \rho(n)$. ∎

Теорема 6. *Неприводимая разрешимая подгруппа группы $GL(n, \Delta)$ обладает абелевым нормальным делителем, индекс которого не больше числа $\rho_1(n)$, зависящего только от n.*

Доказательство. В силу теоремы 5 надо рассматривать лишь импримитивные неприводимые разрешимые подгруппы группы $GL(n, \Delta)$. Пусть $\mathfrak{G}$ — импримитивная неприводимая разрешимая подгруппа в $GL(n, \Delta)$. Тогда, согласно теореме 18.5, мы можем считать, что $\mathfrak{G}$ — подгруппа сплетения $\overline{G} \wr \Gamma$, где $\overline{G}$ — примитивная разрешимая подгруппа группы $GL(m_1, \Delta)$, а Γ — транзитивная разрешимая подгруппа в S_{k_1}, $k_1 m_1 = n$. Ввиду теоремы 5 $\overline{G}$ обладает абелевым нормальным делителем, индекс которого не превышает числа $\rho(m_1)$. Следовательно, прямое произведение k_1 экземпляров группы $\overline{G}$ обладает абелевым нормальным делителем, индекс которого не больше числа $(\rho(m_1))^{k_1}$. Отсюда следует, что $\overline{G} \wr \Gamma$ обладает абелевым нормальным делителем, индекс которого не превышает числа

$$k_1!\,(\rho(m_1))^{k_1} < n!\,\rho(n)^n = \rho_1(n).$$

Так как $\mathfrak{G}$ — подгруппа в $\overline{G} \wr \Gamma$, то $\mathfrak{G}$ тоже обладает абелевым нормальным делителем, индекс которого не больше $\rho_1(n)$. ∎

Теорема 7 (Мальцев [3], Колчин [1]). *Разрешимая подгруппа группы $GL(n, \Sigma)$, где Σ — алгебраически замкнутое поле, обладает таким нормальным делителем N, что индекс N не больше числа $\rho_2(n)$, зависящего только от n, а матрицы из N одновременным трансформированием приводятся к треугольному виду.*

Доказательство. В силу теоремы 6, алгебраической замкнутости поля Σ и теоремы 16.2 неприводимая разрешимая подгруппа группы $GL(n, \Sigma)$ обладает нормальным делителем, индекс которого не больше $\rho_1(n)$, а матрицы одновременно трансформируются к диагональному виду. Отсюда и вытекает теорема 7. ∎

4. Ограниченность длины ряда коммутантов.

Теорема 8 (Цассенхауз [1]). *Пусть Δ — произвольное поле. Длина ряда коммутантов любой разрешимой подгруппы $\mathfrak{G}$ группы $GL(n, \Delta)$ не превышает некоторого числа $l(n)$, зависящего только от n.*

Доказательство. Пусть $\lambda(\mathfrak{G})$ — длина ряда коммутантов группы $\mathfrak{G}$. Если группа $\mathfrak{G}$ примитивна, то, в силу теоремы 5, в $\mathfrak{G}$ есть абелев нормальный делитель $\mathfrak{H}$ такой, что $\mathfrak{G} : \mathfrak{H} \leqslant \rho(n)$. Следовательно,

$$\lambda(\mathfrak{G}) \leqslant [\log_2 \rho(n)] + 1 = l_1(n). \tag{15}$$

Пусть теперь $\mathfrak{G}$ — неприводимая импримитивная подгруппа в $GL(n, \Delta)$. Тогда, согласно теореме 18.5, $\mathfrak{G}$ — подгруппа сплетения $\bar{G} \wr \Gamma$, где $\bar{G}$ — примитивная разрешимая подгруппа в $GL(nk_1^{-1}, \Delta)$, а Γ — транзитивная разрешимая подгруппа симметрической группы S_{k_1}. Следовательно,

$$\lambda(\mathfrak{G}) \leqslant \lambda(\bar{G} \wr \Gamma) \leqslant \lambda(\bar{G}) + \lambda(\Gamma) \leqslant$$
$$\leqslant [\log_2 k_1!] + \left[\log_2 \rho\left(\frac{n}{k_1}\right)\right] + 1.$$

Отсюда

$$\lambda(\mathfrak{G}) \leqslant [\log_2 n!] + [\log_2 \rho(n)] + 1 = l_2(n). \tag{16}$$

Пусть, наконец, $\mathfrak{G}$ — приводимая разрешимая подгруппа группы $GL(n, \Delta)$. Тогда матрицы из $\mathfrak{G}$ можно одновременно привести к виду (11) из § 18. В силу теоремы 18.2 можно написать

$$\lambda(\mathfrak{G}) \leqslant [\log_2 (k-1)] + 1 + \lambda(\operatorname{Im} \gamma_j),$$

где γ_j — некоторая неприводимая часть группы $\mathfrak{G}$, степень γ_j равна $n_j < n$. В силу (16)

$$\lambda(\operatorname{Im} \gamma_j) \leqslant l_2(n_j) \leqslant l_2(n).$$

Следовательно,

$$\lambda(\mathfrak{G}) \leqslant [\log_2 (k-1)] + 1 + l_2(n) \leqslant [\log_2 (n-1)] + 1 + l_2(n) =$$
$$= [\log_2 (n-1)] + [\log_2 n!] + [\log_2 \rho(n)] + 2 = l(n). \tag{17}$$

Из (15) — (17) для любой разрешимой подгруппы $\mathfrak{G}$ группы $GL(n, \Delta)$ имеем $\lambda(\mathfrak{G}) \leqslant l(n)$. ■

Заметим, что формула (17) дает весьма грубую оценку $\lambda(\mathfrak{G})$ разрешимой подгруппы $\mathfrak{G}$ группы $GL(n, \Delta)$.

Дж. Диксон в [2] доказывает, что

$$\lambda(\mathfrak{G}) \leqslant n+2. \tag{18}$$

Группа G называется *локально разрешимой*, если любое ее конечное подмножество элементов порождает разрешимую подгруппу группы G.

Теорема 9 (Цассенхауз [1]). *Пусть Λ — произвольное поле. Тогда любая локально разрешимая подгруппа $\mathfrak{G}$ группы $GL(n, \Delta)$ разрешима.*

Доказательство. Для произвольной группы G индуктивно введем коммутаторы D^j, положив

$$D^1(g_1, g_2) = g_1 g_2 g_1^{-1} g_2^{-1},$$

$$D^j = D^j(g_1, \ldots, g_{2^j}) =$$

$$= D^1\left(D^{j-1}(g_1, \ldots, g_{2^{j-1}}), D^{j-1}(g_{2^{j-1}+1}, \ldots, g_{2^j})\right),$$

$j > 1$, $g_i \in G$. Пусть k — натуральное число. *Группа G тогда и только тогда разрешима и $\lambda(G) \leqslant k$, когда*

$$D^k = 1 \tag{19}$$

для любых 2^k элементов из G. Действительно, если $\lambda(G) \leqslant k$, то, очевидно, равенство (19) верно. Пусть теперь для любых 2^k элементов группы G имеет место (19). При $k=1$ группа G абелева и $\lambda(G)=1$. Пусть $k>1$ и для $k-1$ утверждение доказано. Рассмотрим подгруппу N группы G, порождаемую всеми D^{k-1}. Очевидно, N — абелев нормальный делитель группы G. Для любых 2^{k-1} элементов фактор-группы G/N имеем $D^{k-1}=1$. Следовательно,

$$\lambda(G/N) \leqslant k-1, \qquad \lambda(G) \leqslant k.$$

Теперь нетрудно доказать теорему.

По условию любая подгруппа $\mathfrak{H}$ группы $\mathfrak{G}$, порожденная конечным множеством ее элементов, разрешима. По теореме 8 $\lambda(\mathfrak{H}) \leqslant l(n) = l$. Следовательно, для любых 2^l элементов группы $\mathfrak{G}$

$$D^l = 1.$$

Отсюда $\lambda(\mathfrak{G}) \leqslant l$. ■

Теорема 10. ***Любая разрешимая подгруппа $\mathfrak{G}$ группы $GL(n, \Delta)$ содержится в некоторой максимальной разрешимой подгруппе группы $GL(n, \Delta)$.***

Доказательство. $\mathfrak{G}$ содержится в максимальной локально разрешимой подгруппе $\mathfrak{G}_1$ группы $QL(n, \Delta)$. По теореме 9 $\mathfrak{G}_1$ разрешима. ■

Разрешимым радикалом группы G называется ее максимальный разрешимый нормальный делитель.

Так как произведение двух разрешимых нормальных делителей группы есть разрешимый нормальный делитель, то группа либо вовсе не имеет радикала, либо имеет единственный радикал.

Теорема 11. *Подгруппа $\mathfrak{G}$ группы $GL(n, \Delta)$ имеет разрешимый радикал.*

Доказательство. Пусть $\mathfrak{M}$ — класс всех разрешимых нормальных делителей группы $\mathfrak{G}$. Совокупность $\mathfrak{N}$ всех произведений вида

$$a_1 a_2 \ldots a_r, \qquad a_j \in H_j \in \mathfrak{M}$$

является, очевидно, нормальным делителем группы $\mathfrak{G}$. Каждое конечное множество элементов из $\mathfrak{N}$ содержится в произведении конечного множества групп $H \in \mathfrak{M}$. Следовательно, $\mathfrak{N}$ — локально разрешимая подгруппа в $GL(n, \Delta)$. По теореме 9 $\mathfrak{N}$ — разрешимый нормальный делитель в $\mathfrak{G}$. Очевидно, для $H \in \mathfrak{M}$, $H \subset \mathfrak{N}$. Следовательно, $\mathfrak{N}$ — разрешимый радикал группы $\mathfrak{G}$. ■

§ 20. Максимальные примитивные разрешимые подгруппы полной линейной группы

1. Фактор-группа G/V. Неприводимость V. Пусть Δ — произвольное поле, G — максимальная примитивная разрешимая подгруппа группы $GL(n, \Delta)$, F — максимальный абелев нормальный делитель группы G, а V — централизатор F в G. Тогда из леммы 19.1 вытекает

$$F = K^*, \qquad \Delta E_n \subset K \subset \Delta_n, \tag{1}$$

где K — расширение поля Δ, $K : \Delta = m$, $m \mid n$. С группой G связано еще одно поле. Согласно теореме 14.7 существует такое расширение Σ поля Δ, что G — подгруппа $GL(l, \Sigma)$,

$$[G]_\Delta = \Sigma_l, \qquad (\Sigma : \Delta)\, l = n, \tag{2}$$

Σ^*E_l — центр группы G. Так как F — максимальный абелев нормальный делитель группы G, то

$$\Sigma^*E_l \subset F, \qquad \Sigma E_l \subset K.$$

Следовательно, поле ΣE_l совпадает с совокупностью всех элементов поля K, перестановочных с каждым элементом группы G. Таким образом, для гомоморфизма f, определяемого формулой (2) § 19, справедливо соотношение

$$\operatorname{Im} f \subset \mathcal{G}(K/\Sigma) \subset \mathcal{G}(K/\Delta), \tag{3}$$

где $\mathcal{G}(K/\Sigma)$ — группа всех автоморфизмов поля K, оставляющих неподвижным каждый элемент поля ΣE_l. Так как $\operatorname{Ker} f = V$, то

$$G/V \cong \operatorname{Im} f \subset \mathcal{G}(K/\Sigma), \qquad G : V \leqslant K : \Sigma. \tag{4}$$

Лемма 1. $[G]_\Delta : \Delta = (G : V)([V]_\Delta : \Delta)$.

Доказательство. Пусть

$$g_1, \ldots, g_\tau \tag{5}$$

— полная система представителей смежных классов группы G по V. Тогда система (5) линейно независима над кольцом $[V] = [V]_\Delta$. Действительно, пусть

$$g_1 v_1 + g_2 v_2 + \ldots + g_\tau v_\tau = 0, \qquad v_j \in [V], \tag{6}$$

— нетривиальное соотношение, содержащее наименьшее число ненулевых слагаемых. Мы можем считать, что $v_1 \neq 0$, $v_2 \neq 0$. Так как g_1 и g_2 принадлежат двум различным смежным классам G по V, а V — централизатор F в G, то в F есть такой элемент λ, что $\lambda_1 \neq \lambda_2$, где $\lambda_j = g_j^{-1}\lambda g_j$, $j = 1, \ldots, \tau$. Очевидно, $\lambda g_j = g_j \lambda_j$, $j = 1, \ldots, \tau$. Отсюда и из (6) находим:

$$\lambda(g_1 v_1 + g_2 v_2 + \ldots + g_\tau v_\tau) - \\ - (g_1 v_1 + g_2 v_2 + \ldots + g_\tau v_\tau)\lambda_1 = 0,$$

$$g_2 v_2 (\lambda_2 - \lambda_1) + \ldots + g_\tau v_\tau (\lambda_\tau - \lambda_1) = 0.$$

Последнее равенство противоречит выбору соотношения (6). Следовательно, система (5) линейно независима над $[V]$. Так как любой элемент алгебры $[G] = [G]_\Delta$ имеет вид $g_1 v_1 + \ldots + g_\tau v_\tau$, $v_j \in [V]$, то

$$[G] : \Delta = (G : V)([V] : \Delta). \blacksquare$$

Теорема 1. (i) $G/V \cong \mathcal{G}(K/\Sigma)$; (ii) K — *нормальное сепарабельное расширение поля* Σ *с разрешимой группой Галуа* $\mathcal{G}(K/\Sigma)$; (iii) V — *абсолютно неприводимая подгруппа группы* $GL(r, K)$.

Доказательство. Из (2) следует равенство

$$[G]:\Delta = l^2(\Sigma:\Delta) = \frac{n^2}{\Sigma:\Delta}. \tag{7}$$

Согласно (4)

$$G:V \leqslant K:\Sigma, \tag{8}$$

причем равенство $G:V = K:\Sigma$ имеет место лишь тогда, когда справедливы утверждения (i) и (ii). Так как $V \subset GL(r, K)$, то

$$[V]:\Delta \leqslant r^2(K:\Delta) = \frac{n^2}{m}. \tag{9}$$

Очевидно, равенство $[V]:\Delta = \frac{n^2}{m}$ имеет место только тогда, когда V — абсолютно неприводимая подгруппа группы $GL(r, K)$. Из леммы 1 и из формул (8) и (9) следует

$$[G]:\Delta = (G:V)([V]:\Delta) \leqslant (K:\Sigma)\frac{n^2}{m} = \frac{(K:\Sigma)n^2}{(K:\Sigma)(\Sigma:\Delta)} = \frac{n^2}{\Sigma:\Delta}.$$

В силу (7) отсюда и из (8) и (9) вытекает

$$G:V = K:\Sigma, \qquad [V]:\Delta = \frac{n^2}{m}. \tag{10}$$

Из (10) следуют (i), (ii), (iii). ■

Теорема 2. $V = F \Leftrightarrow K:\Delta = n$.

Доказательство. Согласно следствию 19.1.2, $K:\Delta = n \Rightarrow V = F$. Покажем справедливость обратной импликации. Пусть $V = F$. Тогда, заменяя в (10) V на F, получим

$$K:\Delta = \frac{n^2}{K:\Delta}, \qquad K:\Delta = n. \ ■$$

2. Фактор-группа A/F. Теперь мы будем предполагать, что $V \neq F$, и будем рассматривать фактор-группу A/F, подчиненную следующим требованиям:

(i) A/F — абелев нормальный делитель группы G/F;

(ii) $A/F \subset V/F$;

(iii) A/F — максимальная среди подгрупп фактор-группы G/F, обладающих свойствами (i) и (ii).

Группу G будем изучать с помощью инвариантного ряда

$$G \supset V \supset A \supset F \supset (E_n). \qquad (\alpha)$$

Лемма 2. *Линейная Δ-оболочка $[A]$ группы A есть простая алгебра над полем K. Центр алгебры $[A]$ совпадает с полем K.*

Доказательство. Очевидно, $[A]_\Delta = [A]_K$, ибо $A \supset F$, $[A]_\Delta \supset K$. Так как A — нормальный делитель примитивной группы G, то, в силу теорем Клиффорда (§ 16, п. 2), группа A вполне приводима, а ее неприводимые части эквивалентны. Следовательно, по теореме 14.4, $[A]_\Lambda$ — простая алгебра над Λ. Так как $[A]_\Lambda = [A]_K$, то $[A] = [A]_\Delta$ — простая алгебра над K.

Покажем, что K — центр алгебры $[A]$. Любой ненулевой элемент c из $[A]$ имеет вид

$$c = f_1 d_1 + \ldots + f_\nu d_\nu, \qquad f_j \in F,$$

где d_j — элементы различных смежных классов группы A по F. Если теперь c принадлежит центру алгебры $[A]$, то для любого $a \in A$

$$c - aca^{-1} = 0, \quad a d_j a^{-1} = \lambda_j d_j, \quad \lambda_j \in F, \quad j = 1, \ldots, \nu.$$

Следовательно,

$$f_1 (1 - \lambda_1) d_1 + \ldots + f_\nu (1 - \lambda_\nu) d_\nu = 0.$$

Согласно лемме 19.4 $d_1, \ldots, d_\nu$ линейно независимы над K. Отсюда $\lambda_j = 1$, $j = 1, \ldots, \nu$. Так как a — произвольный элемент A, то $\nu = 1$, $d_1 \in F$, $c = f_1 d_1 \in F$, центр $[A]$ совпадает с K. ∎

Лемма 3. $[A]_\Delta = [V]_\Lambda$.

Доказательство. Положим $[A] = [A]_\Lambda$. Вместе с элементом $v \in V$ рассмотрим отображение

$$\varphi_v \colon [A] \to [A], \qquad x \to v^{-1} x v. \qquad (11)$$

Так как $v^{-1} A v = A$, то φ_v — автоморфизм алгебры $[A]$. Очевидно, для $\lambda \in K$ имеем $\varphi_v(\lambda) = \lambda$. Согласно лемме 2, $[A]$ — простая алгебра над K, а поле K — ее центр. Как известно, автоморфизм простой алгебры, оставляющий неподвижными элементы ее центра, есть внутренний автоморфизм (Ван-дер-Варден [2], стр. 234).

Таким образом, для любого $v \in V$ в группе $[A]^*$ обратимых элементов алгебры $[A]$ найдется такой элемент u, что

$$u^{-1}xu = v^{-1}xv \tag{12}$$

при всяком $x \in [A]$. Так как K — центр алгебры $[A]$, то элемент u при фиксированном v определяется равенством (12) с точностью до множителя из группы $F = K^*$. Следовательно, (12) задает отображение

$$\psi\colon V \to [A]^*/F, \qquad v \mapsto uF.$$

Как легко видеть, ψ — гомоморфизм. Согласно следствию 19.3.1, централизатор A в V равен F, следовательно, $\operatorname{Ker}\psi = F$. Пусть теперь $\operatorname{Im}\psi = U/F$. Тогда

$$U/F \cong V/F.$$

Так как U и V — подгруппы группы $GL(r, K)$, то для u и v, связанных условием (12), имеем

$$u = dv, \tag{13}$$

где $d \in GL(r, K)$ перестановочно с каждым элементом группы A. Очевидно, элемент d из (13) определяется элементом v с точностью до множителя из F. Следовательно, (12) и (13) задают отображение

$$\psi_1\colon V/F \to GL(r, K)/F, \qquad vF \mapsto dF.$$

ψ_1 — гомоморфизм. Действительно, если $vF = dFuF$, $v_1F = d_1Fu_1F$, то $vv_1F = dd_1Fuu_1F$. Поэтому группа D, где $D/F = \operatorname{Im}\psi_1$, разрешима.

Далее, для $g \in G$ имеем

$$g^{-1}Dg = D. \tag{14}$$

В самом деле, из (13) находим

$$v_1 = g^{-1}vg = g^{-1}dgg^{-1}ug = d_1u_1, \quad d_1 = g^{-1}dg, \quad u_1 = g^{-1}ug,$$

где $v_1 \in V$, $u_1 \in g^{-1}[A]g = [A]$. Элемент d_1 перестановочен с каждым элементом $[A] = g^{-1}[A]g$. Следовательно, u_1 и v_1 определяют один и тот же автоморфизм алгебры $[A]$, т. е. равенство $v_1 = d_1u_1$ есть равенство вида (13), $\psi_1(v_1F) = d_1F$, $d_1 \in D$. Отсюда следует (14).

Покажем, что $D = F$. Действительно, в силу (14) группа GD разрешима. Следовательно, $D \subset G$. D содержится в централизаторе группы A в G. В силу следствия 19.3.2 $D = F$. Теперь легко доказать лемму. Из (13) $v = du \in F[A] = [A]$, $V \subset [A]$, $[V] = [A]$. ■

Теорема 3. $A : F = \frac{n^2}{m^2}$, $[A] = K_r$.

Доказательство. Ввиду теоремы 1 $[V] = K_r$. Отсюда, в силу леммы 3,

$$[A] : K = [V] : K = K_r : K = r^2 = \frac{n^2}{m^2}.$$

С другой стороны, согласно лемме 19.4, $A : F = [A] : K$. Следовательно, $A : F = \frac{n^2}{m^2}$. ■

Следствие 1. *Для любого простого делителя q числа n/m в $K^* = F$ найдется элемент порядка q. В частности,* $\operatorname{char} \Delta \notin \Pi(n/m)$.

Доказательство. Очевидно, коммутант A' группы A является подгруппой группы $K^* = F$. В силу леммы 19.3 порядок A' совпадает с экспонентой группы A/F. Следовательно, любой простой делитель числа $A : F$ делит порядок A'. Отсюда и из теоремы 3 вытекает требуемое. ■

Следствие 2. *Пусть n — нечетное число, а R — поле всех вещественных чисел. Тогда любая неприводимая разрешимая подгруппа $GL(n, R)$ мономиальна.*

Доказательство. Достаточно показать, что при нечетном $n > 1$ в $GL(n, R)$ нет максимальных примитивных разрешимых подгрупп. Пусть $n > 1$ — нечетное число, а G — максимальная примитивная разрешимая подгруппа $GL(n, R)$. Тогда $F = K^* = R^*E_n$. Согласно следствию 1 для любого простого делителя q числа n в R^* есть элемент порядка q. Так как q — нечетное число, то последнее невозможно. ■

Следствие 3. *Пусть n — нечетное число, а Q — поле рациональных чисел. Если G — максимальная примитивная разрешимая подгруппа $GL(n, Q)$, то $V = F$, т. е. $K : Q = n$.*

Доказательство. Пусть $K : Q = m < n$. Тогда, согласно следствию 1, в K^* есть элемент η порядка $q > 2$, где q — простой делитель числа n/m. Следовательно, $K \supset Q(\eta)$. Так как $Q(\eta) : Q = q - 1$, то $K : Q$ делится на 2. Но $K : Q$ не может делиться на 2, ибо $K : Q$ делит n, а n — нечетное число. ■

Следствие 4. *Пусть n — нечетное число, G — максимальная разрешимая примитивная подгруппа $GL(n, Q)$, а $F = K^*$ — максимальный абелев нормальный делитель G. Тогда G совпадает с нормализатором F в $GL(n, Q)$, а фактор-группа G/F изоморфна группе всех автоморфизмов поля K относительно поля Δ.*

Доказательство. Согласно предыдущему следствию $K : Q = n$. Следовательно, $K = Q(\theta)$, где θ — матрица из $GL(n, Q)$ с неприводимым характеристическим полиномом. Так как $K^* = F$ — нормальный делитель группы G, то G содержится в нормализаторе $N(F)$ группы F в $GL(n, Q)$. Пусть $\mathcal{G}$ — группа всех автоморфизмов поля K относительно Q. Совокупность всех элементов поля, оставляемых неподвижными каждым автоморфизмом из $\mathcal{G}$, образует поле Σ, $K \supset \Sigma \supset QE_n$. Как легко видеть, K является нормальным расширением поля Σ, а $\mathcal{G}$ совпадает с группой Галуа $\mathcal{G}(K/\Sigma)$. Так как n нечетно, а порядок $\mathcal{G}$ равен $K : \Sigma$ и делит n, то группа $\mathcal{G}$ разрешима. Каждый элемент a из $N(F)$ определяет автоморфизм σ_a поля K: $\sigma_a(x) = axa^{-1}$, $x \in K$. Очевидно, что $\sigma_a \in \mathcal{G}$, $\sigma_{ab} = \sigma_a \sigma_b$. Следовательно, имеет место гомоморфизм

$$\gamma\colon N(F) \to \mathcal{G}, \qquad a \mapsto \sigma_a.$$

Так как $F = K^*$, а $K : Q = n$, то $\operatorname{Ker}\gamma = F$. Так как группа $\mathcal{G}$ разрешима, то группа $N(F)$ тоже разрешима. Следовательно, $G = N(F)$. Остается доказать, что $G/F \cong \mathcal{G}$. Для этого достаточно установить сюръективность гомоморфизма γ. Пусть σ — произвольный элемент из $\mathcal{G}$. Ясно, что σ вполне задается матрицей $\theta_1 = \sigma(\theta)$. Матрицы θ и θ_1 имеют одну и ту же общую нормальную форму, следовательно, в $GL(n, Q)$ есть такая матрица t, что $t\theta t^{-1} = \theta_1$. Очевидно, $tKt^{-1} = K$, $tFt^{-1} = F$. Следовательно, $t \in N(F)$, т. е. гомоморфизм γ сюръективен. Отсюда $G/F = N(F)/F \cong \mathcal{G}$. ∎

Теорема 4. *A/F совпадает со своим централизатором в $GL(r, K)/F$.*

Доказательство. Пусть C/F — централизатор A/F в $GL(r, K)/F$, а $c \in G$. Тогда для $a \in A$

$$(c, a) \in F, \qquad (c, a)^r = 1.$$

В частности, для элементов a_j, b_j из теоремы 19.2 имеем

$$(c, b_j)=\varepsilon_j^{\alpha_j}, \quad (a_j, c)=\varepsilon_j^{\beta_j}, \quad j=1, \ldots, t.$$

Положим $c_1=a_1^{\alpha_1}b_1^{\beta_1} \ldots a_t^{\alpha_t}b_t^{\beta_t}$. Тогда при $j=1, \ldots, t$

$$(c_1, b_j)=(c, b_j); \quad (a_j, c_1)=(a_j, c);$$
$$(cc_1^{-1}, b_j)=(a_j, cc_1^{-1})=1.$$

Следовательно, элемент cc_1^{-1} перестановочен с каждым элементом группы A. В силу теоремы 3 $cc_1^{-1}\in F$,

$$c\in c_1F\subset A, \quad C/F=A/F. \blacksquare$$

Теорема 5. *Пусть*

$$r=q_1^{l_1} \ldots q_k^{l_k} \tag{15}$$

— каноническое разложение числа r, а Q_j/F есть q_j-подгруппы Силова группы A/F, $j=1, \ldots, k$. Тогда Q_j/F — прямое произведение $2l_j$ групп порядка q_j.

Доказательство. Очевидно, что Q_j/F — абелев нормальный делитель порядка $g_j^{2l_j}$ фактор-группы G/F. Надо показать, что экспонента, Q_j/F равна q_j. Пусть, вопреки теореме, экспонента Q_j/F равна q_j^α, $\alpha>1$. Тогда $\beta=q_j^{\alpha-1}>1$. Рассмотрим группу D/F, состоящую из всех элементов вида $(uF)^\beta$, где uF пробегает Q_j/F. Очевидно, $D\neq F$, D — нормальный делитель группы G. Для любых u и v из Q_j имеем

$$(u^\beta, v^\beta)=(u, v)^{\beta^2}=(u, v)^{q_j^{2\alpha_j-2}}=1,$$

ибо порядок коммутанта Q_j' группы Q_j равен q_j^α. Следовательно, D — абелев нормальный делитель группы G. Последнее противоречит максимальности F. $\blacksquare$

В силу теоремы 19.2 из теоремы 5 вытекает

Следствие 1. *Группа Q_j представима в виде*

$$Q_j=(u_1)(v_1) \ldots (u_{l_j})(v_{l_j})F,$$

где

$$(u_i, v_i)=\eta, \quad \eta_i^{q_j}=1, \quad \eta\neq 1, \quad \eta\in F; \quad u_i^{q_j}, v_i^{q_j}\in F,$$

а элементы, принадлежащие различным парам, перестановочны.

Ясно, что теоремы 3 и 5 полностью определяют строение фактор-группы A/F как группы порядка n^2/m^2, представимой в виде прямого произведения групп простых порядков.

Ниже группы Q_j, $j = 1, \ldots, k$, теоремы 5 рассматриваются как подгруппы $GL(r, K)$.

Лемма 4. (i) *Для $\nu \neq j$ группы Q_ν и Q_j поэлементно перестановочны.*

(ii) *Неприводимые части группы Q_j попарно эквивалентны и абсолютно неприводимы. Степени неприводимых частей группы Q_j равны числу $q_j^{l_j}$.*

Доказательство. Пусть $\nu \neq j$, $a \in Q_\nu$, $b \in Q_j$. Тогда $(a, b) = \lambda \in F$, $(a, b)^{q_\nu} = (a^{q_\nu}, b) = \lambda^{q_\nu} = 1$, $(a, b)^{q_j} = (a, b^{q_j}) = \lambda^{q_j} = 1$. Отсюда $\lambda = 1$, $ab = ba$. (i) доказано. Очевидно, что $A = Q_1 \ldots Q_k$. Отсюда и из (i) вытекает, что $A = Q_j U_j$, где U_j — подгруппа группы A, каждый элемент которой перестановочен с каждым элементом из Q_j. Так как Q_j — нормальный делитель неприводимой группы A, то группа Q_j вполне приводима. В силу леммы 16.4 из равенства $A = Q_j U_j$ вытекает эквивалентность неприводимых частей группы Q_j. Следовательно, $[Q_j]_K = T_\rho$, где T — тело. Пусть σ — степень неприводимой части группы Q_j. Тогда

$$\rho (T : K) = \sigma, \qquad T_\rho : K = \rho^2 (T : K) = \rho\sigma.$$

С другой стороны, в силу леммы 19.4,

$$[Q_j]_K : K = Q_j : F = q_j^{2l_j}.$$

Отсюда

$$\rho\sigma = q_j^{2l_j}. \tag{16}$$

Так как σ делит число r, то из (16) вытекает

$$\rho \leqslant \sigma \leqslant q_j^{l_j}. \tag{17}$$

Из (16) и (17) находим $\rho = \sigma = q_j^{l_j}$, $[Q_j]_K : K \cong K_{q_j^{l_j}}$, т. е. степени неприводимых частей группы Q_j равны $q_j^{l_j}$, а неприводимые части группы Q_j абсолютно неприводимы. (ii) доказано. ■

Теорема 6. *Существует такой K-базис пространства K^r, при котором группы Q_j, $j = 1, \ldots, k$, одновременно принимают вид*

$$Q_j = E_{q_1^{l_1} \ldots q_{j-1}^{l_{j-1}}} \dot{\times} Q^j \dot{\times} E_{rq_1^{-l_1} \ldots q_j^{-l_j}},$$

где Q^j — абсолютно неприводимая подгруппа $GL(q_j^{l_j}, K)$, изоморфная группе Q_j, а $\dot{\times}$ — знак кронекерова произведения.

Доказательство. Согласно лемме 4 неприводимые части группы Q_1 абсолютно неприводимы, попарно эквивалентны и их степени равны $q_1^{l_1}$. Следовательно, в некотором K-базисе K^r группа Q_1 принимает вид

$$Q_1 = Q^1 \dot{\times} E_{rq_1^{-l_1}}, \tag{18}$$

где Q^1 — абсолютно неприводимая подгруппа группы $GL(q_1^{l_1}, K)$, изоморфная группе Q_1. Рассмотрим теперь группу $U_1 = Q_2 \ldots Q_k$. Группы U_1 и Q_1 поэлементно перестановочны. В силу (18) U_1 имеет вид

$$U_1 = E_{q_1^{l_1}} \dot{\times} U^1, \tag{19}$$

где U^1 — подгруппа группы $GL(rq_1^{-l_1}, K)$, изоморфная группе U. В частности, $Q_2 = E_{q_1^{l_1}} \dot{\times} \bar{Q}_2$,

$$\bar{Q}_2 \cong Q_2, \qquad \bar{Q}_2 \subset GL(rq_1^{-l_1}, K).$$

К группе $\bar{Q}_2$ применимы те же рассуждения, что и к группе Q_1. Неприводимые части $\bar{Q}_2$ попарно эквивалентны, их степени равны $q_2^{l_2}$. Следовательно, в некотором K-базисе K^r одновременно выполняется (18) и

$$Q_2 = E_{q_1^{l_1}} \dot{\times} Q^2 \dot{\times} E_{rq_1^{-l_1} q_2^{-l_2}}, \tag{20}$$

где Q^2 — абсолютно неприводимая подгруппа группы $GL(q_2^{l_2}, K)$, изоморфная Q_2. Так как $Q^1 \dot{\times} Q^2$ — абсолютно неприводимая подгруппа группы $GL(q_1^{l_1}q_2^{l_2}, K)$, то из (18) и (20) следует

$$Q_3 = E_{q_1^{l_1}q_2^{l_2}} \dot{\times} \overline{Q}_3.$$

Поступая так дальше, получим требуемое. ■

Следствие 1. *В подходящем K-базисе пространства K^r группу A можно записать в виде*

$$A = Q^1 \dot{\times} \ldots \dot{\times} Q^k,$$

где Q^j — абсолютно неприводимая подгруппа группы $GL(q_j^{l_j}, K)$, изоморфная группе Q_j.

Теорема 7. *Пусть P/F — подгруппа фактор-группы Q_j/F, а C — централизатор P в Q_j. Тогда*

$$Q_j : C = P : F.$$

Доказательство. Пусть $P:F = q_j^{\nu}$. Тогда $P = (u_1) \ldots (u_{\nu})F$, P/F — прямое произведение ν циклических групп (u_jF) порядка q_j. Согласно лемме 19.3 индекс централизатора элемента u_j в группе Q_j равен q_j. Следовательно,

$$i_1 = Q_j : C \leqslant q_j^{\nu}.$$

Далее,

$$Q_j = PP_1, \quad P_1 : F = q_j^{2l_j - \nu}.$$

Если i_2 — индекс централизатора P_1 в Q_j, то

$$i_2 \leqslant q_j^{2l_j - \nu}.$$

Так как центр Q_j равен F, $Q_j : F = q_j^{2l_j}$, то $q_j^{2l_j} \leqslant i_1 i_2$. Отсюда $i_1 = q_j^{\nu} = Q_j : C$. ■

В следующей теореме использованы обозначения теоремы 19.2.

Теорема 8. *Пусть пары элементов $u_1, v_1, \ldots, u_t, v_t$ алгебры $[A]_K = K_r$ подчинены трем условиям:* (i) $(u_j, v_j) = (a_j, b_j)$, $j = 1, \ldots, t$; (ii) *элементы, принадлежащие двум различным парам, перестановочны;* (iii) $u_j^{\nu_j} = a_j^{\nu_j}$, $v_j^{\nu_j} = b_j^{\nu_j}$, $j = 1, \ldots, t$. *Тогда в $GL(r, K)$ имеется такой элемент x, что*

$$xa_jx^{-1} = u_j, \quad xb_jx^{-1} = v_j, \quad j = 1, \ldots, t.$$

Доказательство. Рассмотрим r^2 элементов

$$u_1^{\alpha_1} \ldots v_t^{\beta_t}, \quad 0 \leqslant \alpha_j < \nu_j, \quad 0 \leqslant \beta_j < \nu_j. \tag{21}$$

Если $(\alpha_1, \ldots, \beta_t) \neq (\gamma_1, \ldots, \delta_t)$, то при некотором j, $1 \leqslant j \leqslant t$, либо

$$\left(u_j, u_1^{\alpha_1} \ldots v_t^{\beta_t}\right) \neq \left(u_j, u_1^{\gamma_1} \ldots v_t^{\beta_t}\right),$$

либо

$$\left(v_j, u_1^{\alpha_1} \ldots v_t^{\beta_t}\right) \neq \left(v_j, u_1^{\gamma_1} \ldots v_t^{\delta_t}\right).$$

Как и при доказательстве леммы 19.4, пользуясь этими неравенствами, можно доказать, что элементы (21) линейно независимы над K. Следовательно, отображение θ: $K_r \to K_r$,

$$\sum \lambda_{\alpha_1 \ldots \beta_t} a_1^{\alpha_1} \ldots b_t^{\beta_t} \longmapsto \sum \lambda_{\alpha_1 \ldots \beta_t} u_1^{\alpha_1} \ldots v_t^{\beta_t},$$

где $\lambda_{\alpha_1 \ldots \beta_t} \in K$, биективно. В силу условий (i)—(iii) θ — автоморфизм алгебры K_r. Очевидно, $\theta(\lambda) = \lambda$ для $\lambda \in K$. Следовательно, θ — внутренний автоморфизм алгебры K_r. Отсюда и вытекает теорема. ■

3. Единственность инвариантного ряда (α).

Теорема 9. *Максимальная примитивная разрешимая подгруппа G группы $GL(n, \Delta)$ обладает единственным максимальным абелевым нормальным делителем.*

Доказательство. Пусть F и $F_1 \neq F$ — максимальные абелевы нормальные делители группы G. Тогда, согласно лемме 19.1, $F = K^*$, $F_1 = K_1^*$, где K и K_1 — конечные расширения поля Δ. Как уже отмечалось выше (см. формулу (2)), G является абсолютно неприводимой подгруппой группы $GL(l, \Sigma)$, где $\Sigma^* E_l$ — центр G. По теореме 1 K — нормальное сепарабельное расширение поля Σ. Следовательно, $K = \Sigma(\theta)$, где θ — примитивный элемент поля K. Так как F и F_1 максимальны и $F \neq F_1$, то $K \neq \Sigma E_l$, $K_1 \neq \Sigma E_l$. Пусть $\varphi(x)$ из $\Sigma[X]$ — минимальный полином матрицы θ. Тогда $\varphi(x) = 0$ — нормальное уравнение и поле разложения $\overline{K}$ полинома $\varphi(x)$ изоморфно полю K. Положим $K : \Sigma = \mu$, $l\mu^{-1} = \rho$ и будем G рассматривать как подгруппу группы $GL(l, \overline{K})$. Матрица θ над $\overline{K}$ принимает вид

$$\theta = \operatorname{diag}[\theta_1 E_\rho, \ldots, \theta_\mu E_\rho],$$

где θ_j — корни $\varphi(x)$. Следовательно, f из F имеет вид

$$f = \operatorname{diag}[\alpha_1 E_\rho, \ldots, \alpha_\mu E_\rho].$$

Группа G как подгруппа $GL(l, \overline{K})$ импримитивна. По теореме 16.2, для пространства $\overline{K}^l$, имеется разложение

$$\overline{K}^l = Q_1 \dotplus \ldots \dotplus Q_\mu \tag{22}$$

на системы импримитивности группы G, причем оператор θ векторы Q_j умножает на θ_j. Очевидно, в F_1 есть элемент f_1, не перестановочный с θ. Так как $F_1 = K_1^*$, а $e + f_1 \neq 0$, то $e + f_1 \in F$. Так как $f_1\theta \neq \theta f_1$, то при некотором j $f_1(Q_j) = Q_i$, $i \neq j$. Отсюда $(e + f_1)(Q_j) = Q_j + Q_i$. Последнее противоречит разложению (22) пространства $\overline{K}^l$ на системы импримитивности G. ■

Добавим, что теорема 9 остается верной, если примитивность G заменить неприводимостью (см. теорему 14 в книге Супруненко [8]).

Теорема 10. *Пусть B/F — нормальный делитель группы G/F, содержащийся в Q/F, где Q/F есть q-подгруппа Силова группы A/F. Тогда группа Q/F представима в виде прямого произведения $Q/F = B/F \times U/F$, где U/F — нормальный делитель в G/F, причем взаимный коммутант (B, U) равен единичной группе.*

Доказательство. Пусть U — централизатор группы B в Q. Так как U является пересечением централизатора B в G с Q, то U — нормальный делитель в G. Центр группы B совпадает с F. Следовательно, $U \cap B = F$, т. е. $B/F \cap U/F = 1$. Согласно теореме 7 $Q : U = B : F$. Так как

$$Q : F = (Q : U)(U : F),$$

то

$$Q : F = (B : F)(U : F).$$

Следовательно, Q/F — прямое произведение своих подгрупп B/F и U/F. ■

Теорема 11. *Группа A инвариантного ряда (α) однозначно определяется группой G.*

Доказательство. Пусть группа B обладает свойствами:

(i) B/F — абелев нормальный делитель группы G/F;

(ii) $B/F \subset V/F$;

(iii) группа B/F максимальна среди подгрупп в G/F, удовлетворяющих условиям (i) и (ii).

Надо показать, что $B = A$. Пусть q — простой делитель числа r, P/F есть q-подгруппа Силова группы A/F, а Q/F есть q-подгруппа Силова группы B/F. Положим

$$D/F = P/F \cap Q/F.$$

Очевидно, что D/F — нормальный делитель группы G/F. Согласно теореме 10

$$P/F = D/F \times U/F, \qquad Q/F = D/F \times W/F,$$

где прямые множители U/F и W/F являются нормальными делителями группы G/F, причем $(D, U) = (D, W) = 1$, где (D, V) и (D, W) — взаимные коммутанты. Очевидно, $U/F \cap W/F = 1$. Следовательно, UW/F — абелев нормальный делитель группы G/F;

$$R/F = D/F \times UW/F$$

— также ее абелев нормальный делитель. Группа R/F содержится в V/F и является q-группой. Очевидно,

$$R/F \supset P/F, \qquad R/F \supset Q/F.$$

Отсюда вытекает

$$R/F = P/F, \quad R/F = Q/F, \quad P = Q.$$

Так как q — произвольный простой делитель числа r, то $A = B$. ■

Из теорем 9 и 11 следует, что *группа G обладает единственным инвариантным рядом вида* (α).

Теорема 12. *Пусть $\mathfrak{N}$ — нормализатор группы A в $GL(n, \Delta)$, а G_1 — другая максимальная примитивная разрешимая подгруппа группы $GL(n, \Delta)$ такая, что*

$$G_1 \supset V_1 \supset A \supset F \supset (E_n)$$

— ее инвариантный ряд вида (α). Если группы G и G_1 сопряжены в $GL(n, \Delta)$, то они сопряжены и в $\mathfrak{N}$.

Доказательство. Пусть

$$tGt^{-1} = G_1, \qquad t \in GL(n, \Delta).$$

Рассмотрим группы: tFt^{-1}, tVt^{-1} и tAt^{-1}. Группа tFt^{-1} — максимальный абелев нормальный делитель группы $tGt^{-1} = G_1$. По теореме 9 $tFt^{-1} = F$. Следовательно,

$tVt^{-1} = V_1$, $tAt^{-1} \subset V_1$ и tAt^{-1}/F — максимальная подгруппа среди абелевых нормальных делителей группы G_1/F, содержащихся в V_1/F. По теореме 11 $tAt^{-1} = A$. Отсюда $t \in \mathfrak{N}$. ∎

4. Фактор-группа V/A. Введем сперва две группы. Пусть P — произвольное поле, а $HSp(2l, P)$ — совокупность всех таких матриц h из P_{2l}, что

$$^{t}h\Phi_l h = \lambda\Phi_l,$$

где $\lambda \in P^*$, ^{t}h — матрица, транспонированная к h,

$$\Phi_l = \begin{bmatrix} 0 & E_l \\ -E_l & 0 \end{bmatrix}.$$

Если

$$^{t}h_1\Phi_l h_1 = \lambda_1\Phi_l, \qquad \lambda_1 \in P^*,$$

то

$$^{t}(h_1 h)\Phi_l(h_1 h) = \lambda\lambda_1\Phi_l.$$

Очевидно, что $HSp(2l, P)$ является подгруппой группы $GL(2l, P)$. Отображение $h \longmapsto \lambda$ — гомоморфизм групп $HSp(2l, P) \to P^*$. Ядро этого гомоморфизма состоит из всех таких матриц $h \in P_{2l}$, что

$$^{t}h\Phi_l h = \Phi_l. \tag{23}$$

Группу $Sp(2l, P)$ всех матриц h из P_{2l}, удовлетворяющих условию (23), назовем *симплектической группой* степени $2l$ над полем P. Группу $HSp(2l, P)$ будем называть *гиперсимплектической группой*.

Запишем матрицу $h \in P_{2l}$ в виде

$$h = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1l} & \beta_{11} & \dots & \beta_{1l} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_{l1} & \dots & \alpha_{ll} & \beta_{l1} & \dots & \beta_{ll} \\ \gamma_{11} & \dots & \gamma_{1l} & \delta_{11} & \dots & \delta_{1l} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \gamma_{l1} & \dots & \gamma_{ll} & \delta_{l1} & \dots & \delta_{ll} \end{bmatrix}$$

и введем $2l$-мерные векторы u_i, v_i, x_μ, y_μ $(i, \mu = 1, \dots, l)$ над полем P, положив

$$\begin{aligned} u_i &= (\alpha_{1i}, \gamma_{1i}, \dots, \alpha_{li}, \gamma_{li}), \\ v_i &= (\beta_{1i}, \delta_{1i}, \dots, \beta_{li}, \delta_{li}), \\ x_\mu &= (\gamma_{1\mu}, -\alpha_{1\mu}, \dots, \gamma_{l\mu}, -\alpha_{l\mu}), \\ y_\mu &= (\delta_{1\mu}, -\beta_{1\mu}, \dots, \delta_{l\mu}, -\beta_{l\mu}). \end{aligned} \tag{24}$$

Под скалярным произведением двух векторов вида **(24)** будем понимать сумму произведений их одноименных компонент.

Лемма 5. *Матрица h из P_{2l} тогда и только тогда принадлежит группе $HSp(2l, P)$, когда скалярные произведения векторов* (24) *подчинены следующим требованиям*:

1) $u_i x_\mu = 0$, 2) $u_i y_i = \lambda$,

3) $\mu \neq i \Rightarrow u_i y_\mu = 0$, 4) $v_i y_\mu = 0$,

где $\lambda = \lambda(h) \in P^*$.

Доказательство. Заметим сперва, что для любой матрицы h из P_{2l}

$$v_i x_\mu = -u_\mu y_i. \tag{25}$$

Обратимся к матрице ${}^t h \Phi_l h$.

$$\begin{gathered}{}^t h \Phi_l h = {}^t h (\Phi_l h) = \\ = \begin{bmatrix} \alpha_{11} \dots \alpha_{l1} & \gamma_{11} \dots \gamma_{l1} \\ \dots\dots\dots & \dots\dots\dots \\ \alpha_{1l} \dots \alpha_{ll} & \gamma_{1l} \dots \gamma_{ll} \\ \beta_{11} \dots \beta_{l1} & \delta_{11} \dots \delta_{l1} \\ \dots\dots\dots & \dots\dots\dots \\ \beta_{1l} \dots \beta_{ll} & \delta_{1l} \dots \delta_{ll} \end{bmatrix} \begin{bmatrix} \gamma_{11} \dots \gamma_{1l} & \delta_{11} \dots \delta_{1l} \\ \dots\dots\dots & \dots\dots\dots \\ \gamma_{l1} \dots \gamma_{ll} & \delta_{l1} \dots \delta_{ll} \\ -\alpha_{11} \dots -\alpha_{1l} & -\beta_{11} \dots -\beta_{1l} \\ \dots\dots\dots & \dots\dots\dots \\ -\alpha_{l1} \dots -\alpha_{ll} & -\beta_{l1} \dots -\beta_{ll} \end{bmatrix} = \\ = \begin{bmatrix} R & S \\ T & U \end{bmatrix},\end{gathered}$$

где R, S, T, U — матрицы порядка l,

$$R = \| \rho_{i\mu} \|, \quad \rho_{i\mu} = u_i x_\mu; \quad S = \| \sigma_{i\mu} \|, \quad \sigma_{i\mu} = u_i y_\mu;$$
$$T = \| \tau_{i\mu} \|, \quad \tau_{i\mu} = v_i x_\mu, \quad U = \| \theta_{i\mu} \|, \quad \theta_{i\mu} = v_i y_\mu.$$

Матрица h тогда и только тогда принадлежит $HSp(2l, P)$, когда $R = U = 0$, $S = -T = \lambda E_l$. Отсюда и из (25) следует лемма. ■

Ясно, что *лемма* 5 *остается верной, если в ее формулировке λ заменить единицей, а группу $HSp(2l, P)$ — группой $Sp(2l, P)$*.

Лемма 6. $Sp(2, P) = SL(2, P)$, $HSp(2, P) = GL(2, P)$.

Доказательство. Пусть

$$h=\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in P_2.$$

Тогда

$$ {}^t h \Phi_1 h = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = $$

$$ = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \begin{bmatrix} \gamma & \delta \\ -\alpha & -\beta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \det h.$$

Отсюда и следует лемма. ■

В случае, когда $P = GF(q)$, вместо $Sp(2l, P)$ мы будем писать $Sp(2l, q)$.

Перейдем теперь к изучению фактор-группы V/A. Ввиду следствия 6.1 мы будем считать, что группа A представлена в виде кронекерова произведения

$$A = Q^1 \dot{\times} \ldots \dot{\times} Q^k. \tag{26}$$

Ясно, что V является подгруппой нормализатора группы A в группе $GL(r, K)$. Пусть N — нормализатор A_j в $GL(r, K)$, а N_j — нормализатор Q в $GL\left(q_j^{l_j}, K\right)$, $j = 1, \ldots, k$. Тогда верна

Теорема 13. $N = N_1 \dot{\times} \ldots \dot{\times} N_k$.

Доказательство. Для любого $h \in N$ имеем

$$hQ_j h^{-1} = Q_j,$$

$$h\left(E_{q_1^{l_1}} \dot{\times} \ldots \dot{\times} Q^j \dot{\times} \ldots \dot{\times} E_{q_k^{l_k}}\right) h^{-1} = $$
$$= E_{q_1^{l_1}} \dot{\times} \ldots \dot{\times} Q_{q_j^{l_j}} \dot{\times} \ldots \dot{\times} E_{q_k^{l_k}}.$$

Отсюда, переходя к $[Q_j]_K$, получаем

$$h\left(E_{q_1^{l_1}} \dot{\times} \ldots \dot{\times} K_{q_j^{l_j}} \dot{\times} \ldots \dot{\times} E_{q_k^{l_k}}\right) h^{-1} = $$
$$= E_{q_1^{l_1}} \dot{\times} \ldots \dot{\times} K_{q_j^{l_j}} \dot{\times} \ldots \dot{\times} E_{q_k^{l_k}},$$

$$h\left(E_{q_1^{l_1}} \dot{\times} \ldots \dot{\times} x_j \dot{\times} \ldots \dot{\times} E_{q_k^{l_k}}\right) h^{-1} = $$
$$= E_{q_1^{l_1}} \dot{\times} \ldots \dot{\times} x_j' \dot{\times} \ldots \dot{\times} E_{q_k^{l_k}}, \tag{27}$$

где x_j, $x'_j \in K_{q_j^{l_j}}$. Последнее равенство определяет автоморфизм σ_j алгебры $K_{q_j^{l_j}}$

$$\sigma_j\colon K_{q_j^{l_j}} \to K_{q_j^{l_j}}, \qquad x_j \mapsto x'_j, \tag{28}$$

причем $\sigma_j(Q^j) = Q^j$, $\sigma_j(\lambda E) = \lambda E$ для $\lambda \in K$. Следовательно, в $GL\left(q_j^{l_j}, K\right)$ есть такая матрица h_j, что $\sigma_j(x_j) = h_j x_j h_j^{-1}$ при всяком x_j из $K_{q_j^{l_j}}$. Так как $\sigma_j(Q^j) = h_j Q^j h_j^{-1} = Q^j$, то $h_j \in N_j$. Положим теперь $g = h_1 \dot{\times} \ldots \dot{\times} h_k$. Тогда для любого a из A имеем $gag^{-1} = hah^{-1}$. Отсюда $g^{-1}h = \lambda \in F$, $h = \lambda h_1 \dot{\times} \ldots \dot{\times} h_k \in N_1 \dot{\times} \ldots \dot{\times} N_k$, $N \subset N_1 \dot{\times} \ldots \dot{\times} N_k$. С другой стороны, включение $N_1 \dot{\times} \ldots \dot{\times} N_k \subset N$ очевидно. ■

Теорема 14. *Фактор-группа N/A изоморфна прямому произведению $N_1/Q^1 \times \ldots \times N_k/Q^k$.*

Доказательство. Положим

$$M_j = E_{q_1^{l_1} \ldots q_{j-1}^{l_{j-1}}} \dot{\times} N_j \dot{\times} E_{rq_1^{-l_1} \ldots q_j^{-l_j}}. \tag{29}$$

Тогда, в силу теоремы 13, $N = M_1 \ldots M_k$. Для любого $j = 1, \ldots, k$

$$M_j \cap M_1 \ldots M_{j-1} M_{j+1} \ldots M_k = F.$$

Следовательно, получаем прямое произведение

$$N/F = M_1/F \times M_2/F \times \ldots \times M_k/F. \tag{30}$$

С другой стороны,

$$A/F = Q_1/F \times \ldots \times Q_k/F. \tag{31}$$

Из (30) и (31) следует, что N/A изоморфна прямому произведению $M_1/Q_1 \times \ldots \times M_k/Q_k$. В силу (29) $M_j/Q_1 \cong N_j/Q^j$. ■

Рассмотрим теперь фактор-группу N_j/Q^j. Для упрощения обозначений положим $l_j = l$, $q_j = q$. Согласно теореме 5 Q^j можно записать в виде

$$Q^j = (c_1)(d_1) \ldots (c_l)(d_l) K^*, \tag{32}$$

где c_ν^q, $d_\nu^q \in K^*$, $(c_\nu, d_\nu) = \eta$, $\eta^q = 1$, $\eta \neq 1$, $\eta \in K^*$, а элементы, принадлежащие к двум разным парам, перестановочны.

Каждый элемент x из N_l определяет автоморфизм σ_x группы Q^l: $\sigma_x(u) = xux^{-1}$, $u \in Q^l$. Введем теперь гомоморфизм

$$\varphi: \quad N_l \to \operatorname{Aut}(Q^l/K^*), \tag{33}$$

положив

$$\varphi: x \longmapsto \bar\sigma_x, \quad \bar\sigma_x(uK^*) = \sigma_x(u) K^*, \quad x \in N_l, \quad u \in Q^l.$$

В силу теоремы 4 централизатор Q^l/K^* в N_l/K^* совпадает с Q^l/K^*. Следовательно,

$$\operatorname{Ker}\varphi = Q^l, \qquad N_l/Q^l \cong \operatorname{Im}\varphi. \tag{34}$$

Применим теперь автоморфизм σ_x к элементам c_i и d_i (см. 32)):

$$\begin{aligned} \sigma_x(c_i) = c_i' = \lambda_i c_1^{\alpha_{1i}} \ldots c_l^{\alpha_{li}} d_1^{\gamma_{1i}} \ldots d_l^{\gamma_{li}}, \\ \sigma_x(d_i) = d_i' = \mu_i c_1^{\beta_{1i}} \ldots c_l^{\beta_{li}} d_1^{\delta_{1i}} \ldots d_l^{\delta_{li}}, \end{aligned} \tag{35}$$

где λ_i, $\mu_i \in K^*$, $0 \leqslant \alpha_{\rho i} < q$, $0 \leqslant \beta_{\rho i} < q$, $0 \leqslant \gamma_{\rho i} < q$, $0 \leqslant \delta_{\rho i} < q$, i, $\rho = 1, \ldots, l$. Переходя к $\bar\sigma_x$, из (35) получим

$$\begin{aligned} \bar\sigma_x(c_i K^*) = c_1^{\alpha_{1i}} \ldots c_l^{\alpha_{li}} d_1^{\gamma_{1i}} \ldots d_l^{\gamma_{li}} K^*, \\ \bar\sigma_x(d_i K^*) = c_1^{\beta_{1i}} \ldots c_l^{\beta_{li}} d_1^{\delta_{1i}} \ldots d_l^{\delta_{li}} K^*, \end{aligned} \tag{36}$$

где показатели $\alpha_{\rho i}$, $\beta_{\rho i}$, $\gamma_{\rho i}$, $\delta_{\rho i}$ можно считать элементами поля $GF(q)$. Так как $\bar\sigma_x$ — автоморфизм, то, в силу (32), элементы c_i', d_i' из (35) подчинены следующим условиям:

$$\begin{gathered} (c_i', d_i') = \eta, \quad (c_i', c_\mu') = 1, \quad (d_i', d_\mu') = 1, \\ \mu \neq i \Rightarrow (c_i', d_\mu') = 1, \end{gathered} \tag{37}$$

$$c_i'^q = c_i^q, \qquad d_i'^q = d_i^q. \tag{38}$$

Из равенства $(c_i, d_i) = \eta$ находим

$$(c_i^\alpha, d_i^\delta) = \eta^{\alpha\delta}, \qquad (d_i^\gamma c_i^\beta) = \eta^{-\beta\gamma}.$$

Отсюда

$$(c_i^\alpha d_i^\gamma, c_i^\beta d_i^\delta) = \eta^{\alpha\delta - \beta\gamma}. \tag{39}$$

Из (39) вытекает, что условия (37) эквивалентны следующим сравнениям:

$$\left.\begin{array}{ll}
1) & \displaystyle\sum_{\rho=1}^{l} (\alpha_{\rho i}\delta_{\rho i} - \beta_{\rho i}\gamma_{\rho i}) \equiv 1,\\
2) & \displaystyle\sum_{\rho=1}^{l} (\alpha_{\rho i}\gamma_{\rho\mu} - \alpha_{\rho\mu}\gamma_{\rho i}) \equiv 0,\\
3) & \displaystyle\sum_{\rho=1}^{l} (\beta_{\rho i}\delta_{\rho\mu} - \beta_{\rho\mu}\delta_{\rho i}) \equiv 0,\\
4) & \mu \neq i \Rightarrow \displaystyle\sum_{\rho=1}^{l} (\alpha_{\rho i}\delta_{\rho\mu} - \beta_{\rho\mu}\gamma_{\rho i}) \equiv 0.
\end{array}\right\} \pmod q. \qquad (40)$$

Лемма 7. *Матрица*

$$h(x) = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1l} & \beta_{11} & \dots & \beta_{1l} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_{l1} & \dots & \alpha_{ll} & \beta_{l1} & \dots & \beta_{ll} \\ \gamma_{11} & \dots & \gamma_{1l} & \delta_{11} & \dots & \delta_{1l} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \gamma_{l1} & \dots & \gamma_{ll} & \delta_{l1} & \dots & \delta_{ll} \end{bmatrix}, \qquad (41)$$

элементы которой — показатели, фигурирующие в формулах (36), *принадлежит симплектической группе* $Sp(2l, q)$.

Доказательство. Эти показатели мы условились рассматривать как элементы поля $GF(q)$. Если воспользоваться скалярными произведениями векторов (24), то условия (40) можно переписать в виде

$$1)\ u_i y_i = 1, \qquad 2)\ u_i x_\mu = 0,$$
$$3)\ v_i y_\mu = 0, \qquad 4)\ \mu \neq i \Rightarrow u_i y_\mu = 0.$$

Отсюда и из леммы 5 вытекает лемма 7. ■

Введем, наконец, отображение

$$\psi \colon N_l \to Sp(2l, q), \qquad x \mapsto h(x) \qquad (42)$$

(см. (41)).

Лемма 8. *Отображение* ψ *является гомоморфизмом*, $\operatorname{Ker}\psi = Q^j$. *Следовательно, фактор-группа* N_j/Q^j *изоморфна некоторой подгруппе группы* $Sp(2l, q)$.

Доказательство. Непосредственные вычисления показывают, что для $x, y \in N_j$ $h(xy) = h(x)h(y)$. С другой стороны, из формул (36) и (41) следует, что матрица $h(x)$ тогда и только тогда является единичной, когда $\bar{\sigma}_\nu$ — тождественный автоморфизм. Отсюда и из теоремы 4 следует, что $\operatorname{Ker}\psi = Q^j$. ∎

Из теоремы 14 и леммы 8 вытекает

Теорема 15. *Фактор-группа N/A изоморфна прямому произведению k групп H_j, $j = 1, \ldots, k$, где H_j — некоторая подгруппа группы $Sp(2l_j, q_j)$. Фактор-группа V/A изоморфна некоторой разрешимой подгруппе прямого произведения k симплектических групп $Sp(2l_j, q_j)$, $j = 1, \ldots, k$.*

Возвратимся к гомоморфизму (42).

Теорема 16. *Пусть элементы c_ν, d_ν группы Q^j* (см. формулу (32)) *можно выбрать так, что $c_\nu^q = d_\nu = 1$ $\nu = 1, \ldots, l$, и пусть при $q = 2$ в K^* имеется элемент 4-го порядка. Тогда гомоморфизм ψ сюръективен.*

Доказательство. Пусть $h \in Sp(2l, q)$. По формулам (35) построим элементы c_i', d_i', где в качестве показателей α, β, γ, δ взяты элементы матрицы h. Возможны два случая: 1) $q > 2$, 2) $q = 2$.

При $q > 2$ положим $\lambda_i = \mu_i = 1$. Тогда c_i', d_i' удовлетворяют условиям (37) и (38). В силу теоремы 8 существует такой элемент $g \in GL(q^l, K)$, что $gc_ig^{-1} = c_i'$, $gd_ig^{-1} = d_i'$, $i = 1, \ldots, k$. Очевидно, что $g \in N_j$, $\psi(g) = h$. Для $q > 2$ теорема доказана.

Пусть теперь $q = 2$. Так как в K^* имеется элемент 4-го порядка, то λ_i и μ_i можно подобрать так, что $c_i'^2 = d_i'^2 = 1$. Следовательно, и в этом случае выполняются условия (37) и (38) и тоже применима теорема 8. ∎

Очевидно, что условия теоремы 16 заведомо выполняются, если поле K алгебраически замкнуто.

Теорема 17. *Пусть $F = \Delta^* E_n$, а*

$$n = q_1^{l_1} \ldots q_k^{l_k}$$

— каноническое разложение числа n. Тогда G абсолютно неприводима и сопряжена в $GL(n, \Delta)$ с группой

$$G_1 \dot{\times} \ldots \dot{\times} G_k,$$

где G_j — максимальная примитивная разрешимая абсолютно неприводимая подгруппа группы $GL\left(q_j^{l_j}, \Delta\right)$, $j = 1, \ldots, k$.

Доказательство. Так как $F = \Delta^* E_n$, то F совпадает с центром группы G. Отсюда, в силу теоремы 14.7, $[G]_\Delta = \Delta_n$. Следовательно, G абсолютно неприводима. Из равенства $F = \Delta^* E_n$ вытекает, что $G = V$. Следовательно, согласно теореме 13, группа G сопряжена в $GL(n, \Delta)$ с некоторой подгруппой $\overline{G}$ группы $N = N_1 \dot{\times} \ldots \dot{\times} N_k$, где $N_j \subset GL\left(q_j^{l_j}, \Delta\right)$. Так как $\overline{G}$ — максимальная разрешимая подгруппа группы $GL(n, \Delta)$, то

$$\overline{G} = G_1 \dot{\times} \ldots \dot{\times} G_k,$$

где G_j — максимальная разрешимая подгруппа $GL\left(q_j^{l_j}, \Delta\right)$. В силу леммы 15.8 подгруппа G_j абсолютно неприводима, а в силу леммы 15.9 — примитивна. ■

5. Случай алгебраически замкнутого поля. Пусть теперь поле Δ алгебраически замкнуто. Тогда $F = \Delta^* E_n$, $V = G$, и мы будем вместо ряда (α) писать ряд

$$G \supset A \supset F \supset (E_n). \qquad (\alpha_1)$$

В силу теоремы 3 $A : F = n^2$. Согласно лемме 19.3 $\operatorname{char} \Delta \notin \Pi(n)$. К группе G применима теорема 17, следовательно, мы можем считать, что

$$G = G_1 \dot{\times} \ldots \dot{\times} G_k,$$

где G_j — максимальная примитивная разрешимая подгруппа группы $GL\left(q_j^{l_j}, \Delta\right)$, $j = 1, \ldots, k$, $n = q_1^{l_1} \ldots q_k^{l_k}$ — каноническое разложение числа n. Поэтому мы будем считать, что $n = q^l$, где q — простое число, а G — максимальная примитивная разрешимая подгруппа группы $GL(q^l, \Delta)$. Согласно следствию 5.1 группа A представима в виде

$$A = (u_1)(v_1) \ldots (u_l)(v_l) F, \qquad (43)$$

где $(u_1, v_1) = \eta E_n$, $\eta^q = 1$, $\eta \neq 1$, $\eta \in \Delta^*$, $u_i^q, v_i^q \in F$, элементы из двух разных пар перестановочны.

Лемма 9. *В подходящем базисе пространства Δ^n группа A имеет вид*

$$A = (c_1)(d_1) \ldots (c_l)(d_l) F,$$

где

$$
\begin{aligned}
c_i &= E_{q^{i-1}} \dot{\times} \operatorname{diag}[1, \eta, \ldots, \eta^{q-1}] \dot{\times} E_{q^{l-i}},\\
d_i &= E_{q^{i-1}} \dot{\times} \begin{bmatrix} 0 & 1 \\ E_{q-1} & 0 \end{bmatrix} \dot{\times} E_{q^{l-i}}.
\end{aligned} \tag{44}
$$

Доказательство. Для элементов u_i и v_i (см. формулы (43)) можно написать $u_i, v_i \in \Delta^* E_n$. Так как поле Δ алгебраически замкнуто, то в Δ^* есть такие элементы ρ_i, τ_i, что

$$(\rho_i u_i)^q = (\tau_i v_i)^q = E_n, \quad i = 1, \ldots, l.$$

Полагая $a_i = \rho_i u_i$, $b_i = \tau_i v_i$, $i = 1, \ldots, l$, получим

$$A = (a_1)(b_1) \ldots (a_l)(b_l) F,$$

где $(a_i, b_i) = \eta E_n$, $a_i^q = b_i^q = E_n$, $i = 1, \ldots, l$, а элементы из двух различных пар перестановочны.

С другой стороны, очевидно, элементы c_i и d_i таковы, что $(c_i, d_i) = \eta E_n$, $c_i^q = d_i^q = E_n$, $i = 1, \ldots, l$, а элементы из двух различных пар перестановочны.

В силу теоремы 8 в $GL(n, \Delta)$ найдется такая матрица t, что

$$t a_i t^{-1} = c_i, \quad t b_i t^{-1} = d_i, \quad i = 1, \ldots, l.$$

Отсюда и вытекает лемма 9. ■

До конца § 20 будем считать, что

$$A = (c_1)(d_1) \ldots (c_l)(d_l) F,$$

где c_i и d_i задаются формулами (44), а N — нормализатор A в $GL(q^l, \Delta)$. Любая максимальная примитивная разрешимая подгруппа G группы $GL(q^l, \Delta)$ сопряжена в $GL(q^l, \Delta)$ с некоторой максимальной разрешимой подгруппой группы N. Для любого элемента x из N имеем

$$
\begin{aligned}
x c_i x^{-1} &= \lambda_i c_1^{\alpha_{1i}} \ldots c_l^{\alpha_{li}} d_1^{\gamma_{1i}} \ldots d_l^{\gamma_{li}},\\
x d_i x^{-1} &= \mu_i c_1^{\beta_{1i}} \ldots c_l^{\beta_{li}} d_1^{\delta_{1i}} \ldots d_l^{\delta_{li}},
\end{aligned}
$$

где λ_i, $\mu_i \in \Delta^*$, $\alpha_{\rho i}$, $\beta_{\rho i}$, $\gamma_{\rho i}$, $\delta_{\rho i} \in GF(q)$, $i = 1, \ldots, l$. Положим, далее,

$$\psi(x) = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1l} & \beta_{11} & \ldots & \beta_{1l} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_{l1} & \ldots & \alpha_{ll} & \beta_{l1} & \ldots & \beta_{ll} \\ \gamma_{11} & \ldots & \gamma_{1l} & \delta_{11} & \ldots & \delta_{1l} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \gamma_{l1} & \ldots & \gamma_{ll} & \delta_{l1} & \ldots & \delta_{ll} \end{bmatrix}.$$

Тогда, согласно лемме 7, $\psi(x) \in Sp(2l, q)$, а по теореме 16 отображение

$$\psi\colon\ N \to Sp(2l, q)$$

сюръективно. В силу теоремы 4 $\operatorname{Ker}\psi = A$, следовательно,

$$N/A \cong Sp(2l, q). \tag{45}$$

Лемма 10. *Пусть $\mathfrak{G}_1$ и $\mathfrak{G}_2$ — такие две максимальные примитивные разрешимые подгруппы группы $GL(q^l, \Delta)$, что*

$$A \lhd \mathfrak{G}_1, \qquad A \lhd \mathfrak{G}_2.$$

Группы $\mathfrak{G}_1$ и $\mathfrak{G}_2$ тогда и только тогда сопряжены в $GL(q^l, \Delta)$, когда $H_1 = \psi(\mathfrak{G}_1)$ и $H_2 = \psi(\mathfrak{G}_2)$ сопряжены в $Sp(2l, q)$.

Доказательство. Пусть $\mathfrak{G}_1$ и $\mathfrak{G}_2$ сопряжены в $GL(q^l, \Delta)$. Тогда, по теореме 12, в N есть такая матрица t, что $t\mathfrak{G}_1 t^{-1} = \mathfrak{G}_2$. Применяя к последнему равенству отображение ψ, получим $uH_1u^{-1} = H_2$, где $u = \psi(t)$. Обратно, пусть H_1 и H_2 сопряжены в $Sp(2l, q)$. Очевидно, $\psi^{-1}(H_1)$ и $\psi^{-1}(H_2)$ — разрешимые подгруппы группы N. Так как $\mathfrak{G}_i$ — максимальные разрешимые подгруппы N, то $\mathfrak{G}_i = \psi^{-1}(H_i)$, $i = 1, 2$. Так как ψ сюръективно, то из сопряженности H_1 и H_2 в $Sp(2l, q)$ вытекает сопряженность $\psi^{-1}(H_1)$ и $\psi^{-1}(H_2)$ в N. Следовательно, $\mathfrak{G}_1$ и $\mathfrak{G}_2$ сопряжены в $GL(q^l, \Delta)$. ∎

Теперь будем искать условия, при которых подгруппа группы N примитивна.

Лемма 11. *Пусть B — подгруппа группы N, содержащая A. Группа B тогда и только тогда импримитивна, когда она обладает таким приводимым нормальным* *делителем $D \subset A$, среди неприводимых частей которого есть неэквивалентные.*

Доказательство. Достаточность вытекает из теоремы 16.2. Докажем необходимость. Пусть

$$\Delta^n = L_1 \dotplus \ldots \dotplus L_\mu, \qquad \mu > 1, \qquad n = q^l, \tag{46}$$

— разложение пространства Δ^n на системы импримитивности группы B. Разложение (46) определяет гомоморфизм

$$\gamma\colon\ B \to S_\mu.$$

Так как $B \supset A$, то (46) есть разложение Δ^n на системы импримитивности группы A. Пусть γ_1 — ограничение γ на A, $\operatorname{Ker}\gamma_1 = D$. Тогда $D = A \cap \operatorname{Ker}\gamma$ — инвариантная подгруппа в B. Так как A неприводима, то $\gamma_1(A)$ — транзитивная подгруппа симметрической группы S_μ. С другой стороны, $D \supset F$ и, следовательно, $\gamma_1(A) \cong A/D$ — абелева группа. Поэтому порядок $\gamma_1(A)$ равен μ, $A : D = \mu$, $D : F = q^{2l}\mu^{-1}$. Неприводимые части группы D имеют одну и ту же степень $\rho \leqslant q^l\mu^{-1}$. Пусть σ — число неэквивалентных неприводимых частей группы D. Тогда

$$\sigma \leqslant q^l\rho^{-1}, \qquad [D] : \Delta = \rho^2\sigma = D : F = q^{2l}\mu^{-1}.$$

Отсюда

$$q^{2l}\mu^{-1} = \rho^2\sigma \leqslant \rho^2 q^l \rho^{-1} = \rho q^l \leqslant q^l\mu^{-1}q^l = q^{2l}\mu^{-1}.$$

Следовательно,

$$\rho = q^l\mu^{-1}, \qquad \sigma = q^l\rho^{-1} = \mu.$$

Таким образом, D имеет $\mu > 1$ неэквивалентных неприводимых частей. ∎

Лемма 12. *Пусть B — подгруппа группы N, содержащая группу A, а D — приводимый нормальный делитель группы B, обладающий двумя следующими свойствами:*

1) $F \subset D \subset A$,

2) *среди неприводимых частей группы D есть неэквивалентные.*

Тогда центр $Z(D)$ группы D отличен от F.

Доказательство. Если группа D абелева, то лемма вытекает из свойства 2). Пусть группа D неабелева. Тогда, как и при доказательстве теоремы 19.2, имеем

$$D=(u_1)(v_1)\ \dots\ (u_k)(v_k)D_k,$$

где D_k — центр D, $(u_j, v_j) = \eta E_n, u_j^q = v_j^q = 1$, $j=1, \dots$ $\dots, k$, элементы, принадлежащие различным парам, перестановочны. D_k не может совпадать с F. Действительно, пусть $D_k = F$, и W — централизатор D в A. Тогда $D:F = q^{2k}$. В силу теоремы 7

$$W:F = q^{2(l-k)}.$$

Так как $D_k = F$, то $D \cap W = F$. Следовательно, $A = DW$, $(D, W) = 1$. Отсюда вытекает попарная эквивалентность неприводимых частей группы D (см. лемму 16.4). Последнее противоречит свойству 2) группы D. Отсюда $Z(D) \neq F$. ■

Лемма 13. *Пусть B — подгруппа группы N, содержащая A. Группа B тогда и только тогда примитивна, когда F является максимальным абелевым нормальным делителем в B.*

Необходимость вытекает из теорем 16.1 и 16.2, а достаточность — из двух предыдущих лемм.

Лемма 14. *Пусть C — такая абелева подгруппа группы A, что $C \supset F$, $C:F = q^\nu$, $C = (u_1)\ \dots\ (u_\nu)F$, $u_j^q = 1$, $j=1, \dots, \nu$. Тогда $\nu \leqslant l$, и в группе A есть такие элементы $u_{\nu+1}, \dots, u_l$, $v_1, \dots, v_l$, что $u_j^q = v_j^q = 1$, $(u_j, v_j) = \eta E_n$, $j=1, \dots, l$, а элементы, принадлежащие двум различным парам u_j, v_j, перестановочны.*

Доказательство. $C:F = q^\nu \Rightarrow [C]:\Delta = q^\nu$. Так как группа C абелева, то $[C]:\Delta = q^\nu \leqslant q^l = n$. Следовательно, $\nu \leqslant l$. В силу теоремы 7 централизатор $Z(u_1, \dots, u_\nu)$ множества $\{u_1, \dots, u_\nu\}$ в группе A есть истинная подгруппа централизатора $Z(u_2, \dots, u_\nu)$. Следовательно, в $Z(u_2, \dots, u_\nu)$ найдется такой элемент v_1, что $(u_1, v_1) = \eta E_n$, $v_1^q = 1$. В $Z(u_1, u_3, \dots, u_\nu, v_1)$ найдется элемент v_2 такой, что $(u_2, v_2) = \eta E_n$, $v_2^q = 1$. Поступая так несколько раз, мы найдем в A ν элементов $v_1, \dots, v_\nu$ таких, что $(v_i, v_j) = 1$, $v_j^q = 1$, $(u_i, v_i) = \eta E_n$, $(u_i, v_j) = 1$, $i \neq j$, $j = 1, \dots, \nu$. Если $\nu = l$, то лемма доказана. Если же $\nu < l$, то в $Z(u_1, v_1, \dots, u_\nu, v_\nu)$

есть такая пара элементов $u_{\nu+1}$, $v_{\nu+1}$, что

$$(u_{\nu+1}, v_{\nu+1}) = \eta E_n, \qquad u_{\nu+1}^q = v_{\nu+1}^q = 1.$$

Отсюда и вытекает лемма. ■

Подгруппу H группы $Sp(2l, q)$ назовем *s-приводимой*, если найдутся такое число, ν, $1 \leqslant \nu \leqslant l$, и такая матрица $t \in Sp(2l, q)$, что матрицы группы $t^{-1}Ht$ имеют вид

$$\begin{bmatrix} \alpha_{11} & \dots & \alpha_{1\nu} & \alpha_{1,\nu+1} & \dots & \alpha_{1,2l} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_{\nu 1} & \dots & \alpha_{\nu\nu} & \alpha_{\nu,\nu+1} & \dots & \alpha_{\nu,2l} \\ 0 & \dots & 0 & \alpha_{\nu+1,\nu+1} & \dots & \alpha_{\nu+1,2l} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 0 & \alpha_{2l,\alpha+1} & \dots & \alpha_{2l,2l} \end{bmatrix}. \tag{47}$$

В противном случае подгруппа H группы $Sp(2l, q)$ называется *s-неприводимой*.

Теорема 18. *Пусть $\mathfrak{G}$ — подгруппа группы N, содержащая группу A. Подгруппа $\mathfrak{G}$ тогда и только тогда примитивна, когда $\psi(\mathfrak{G})$ является s-неприводимой подгруппой группы $Sp(2l, q)$.*

Доказательство. Положим $\psi(\mathfrak{G}) = H$. Тогда $\psi^{-1}(H) = \mathfrak{G}A = \mathfrak{G}$. Пусть группа H s-приводима. Тогда в $Sp(2l, q)$ есть такая матрица t, что все матрицы группы $H_1 = t^{-1}Ht$ имеют вид (47). Если $t_1 \in \psi^{-1}(t)$, то $\mathfrak{G}_1 = t_1^{-1}\mathfrak{G}t_1 = \psi^{-1}(H_1)$. Из определения отображения ψ и вида матриц H_1 вытекает, что для $x \in \mathfrak{G}$

$$xa_ix^{-1} = \lambda_i a_1^{\alpha_{1i}} \dots a_\nu^{\alpha_{\nu i}}, \qquad i = 1, \dots, \nu, \quad \lambda_i \in \Delta^*.$$

Следовательно, $C = (a_1) \dots (a_\nu)F \neq F$ — абелев нормальный делитель группы $\mathfrak{G}_1$. Согласно лемме 13 $\mathfrak{G}_1$ импримитивна. Значит, импримитивна и $\mathfrak{G}$. Обратно, пусть $\mathfrak{G}$ импримитивна. Тогда, в силу лемм 11 и 12, $\mathfrak{G}$ обладает таким абелевым нормальным делителем C_0, что

$$F \subset C_0 \subset A, \qquad C_0 : F = q^\nu, \qquad 1 \leqslant \nu \leqslant l.$$

Запишем C_0 в виде

$$C_0 = (u_1) \dots (u_\nu) F, \qquad u_j^q = 1, \qquad j = 1, \dots, \nu.$$

Согласно лемме 14 в A найдутся такие элементы $u_{\nu+1}, \ldots, u_l, v_1, \ldots, v_l$, что

$$A=(u_1)\ldots(u_l)(v_1)\ldots(v_l),$$
$$u_j^q=v_j^q=1, \quad (u_j, v_j)=\eta E_n, \quad j=1, \ldots, l,$$

а элементы из двух различных пар u_i, v_i перестановочны. Согласно теореме 8 в $GL(q^l, \Delta)$ есть такой элемент t_1, что

$$t_1^{-1}u_jt_1=c_j, \quad t_1^{-1}v_jt_1=d_j, \quad j=1, \ldots, l.$$

Очевидно, что $t_1 \in N$, а группа

$$C=t_1^{-1}C_0t_1=(c_1)\ldots(c_\nu)F$$

— абелев нормальный делитель группы $\mathfrak{G}_1=t_1^{-1}\mathfrak{G}t_1$. Положим $t=\psi(t_1)$. Тогда $\psi(\mathfrak{G})=t^{-1}Ht$. Так как $C \lhd \mathfrak{G}_1$, то матрицы группы $t^{-1}Ht$ имеют вид (47). ■

Теорема 19. *Пусть Δ — алгебраически замкнутое поле, а $n=q^l$, где q — простое число, причем $q \neq \operatorname{char}\Delta$. Пусть, далее,*

$$H_1, \ldots, H_\mu$$

— такая система максимальных s-неприводимых разрешимых подгрупп группы $Sp(2l, q)$, что любая максимальная s-неприводимая разрешимая подгруппа группы $Sp(2l, q)$ сопряжена в ней с одной и только одной подгруппой H_j. Тогда любая максимальная примитивная разрешимая подгруппа группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с одной и только одной из следующих групп:

$$\mathfrak{G}_1=\psi^{-1}(H_1), \ldots, \mathfrak{G}_\mu=\psi^{-1}(H_\mu).$$

Группа $\mathfrak{G}_j$ обладает нормальным делителем

$$A=(c_1)(d_1)\ldots(c_l)(d_l)F,$$

где c_i, d_i задаются формулами (44), $\mathfrak{G}_j/A \cong H_j$, $j=1, \ldots, \mu$.

Доказательство. Так как отображение ψ сюръективно, то $\psi(\mathfrak{G}_j)=H_j$. В силу выбора H_j и леммы 10 группы $\psi^{-1}(H_\alpha)$ и $\psi^{-1}(H_\beta)$ при $\alpha \neq \beta$ не сопряжены в $GL(n, \Delta)$. Пусть теперь $\mathfrak{G}$ — любая максимальная разрешимая подгруппа группы $GL(n, \Delta)$. Согласно лемме 9

$\mathfrak{G}$ сопряжена в $GL(n, \Delta)$ с некоторой максимальной примитивной разрешимой подгруппой $\mathfrak{G}^1$ группы N, причем $\mathfrak{G}^1 \supset A$. Группа $\psi(\mathfrak{G}^1) = H$ — разрешимая подгруппа из $Sp(2l, q)$. Согласно теореме 8 H является s-неприводимой подгруппой группы $Sp(2l, q)$. Так как $\mathfrak{G}^1$ максимальна среди разрешимых подгрупп группы $GL(n, \Delta)$, то H — максимальная s-неприводимая разрешимая подгруппа группы $Sp(2l, q)$ и $\mathfrak{G}^1 = \psi^{-1}(H)$. По условию H сопряжена в $Sp(2l, q)$ с некоторой H_j. Следовательно, $\mathfrak{G}^1$ сопряжена в $GL(n, \Delta)$ с $\psi^{-1}(H_j)$. Отсюда и вытекает теорема. ∎

Заметим, что некоторые утверждения настоящего пункта можно доказать, не требуя алгебраической замкнутости основного поля. В частности, лемме 11 можно придать следующий вид.

Лемма 11а. *Пусть Δ — произвольное поле, $n = q^l$, где q — простое число, A_1 — подгруппа группы $GL(n, \Delta)$, обладающая следующими свойствами*:

1. *Центр A_1 совпадает с $\Delta^* E_n$, фактор-группа $A_1/\Delta^* E_n$ абелева*;

2. $[A_1] = \Delta_n$, $A_1 : F = n^2$.

Пусть, далее, N_1 — нормализатор A_1 в $GL(n, \Delta)$, а B_1 — подгруппа группы N_1, содержащая A_1. Группа B_1 тогда и только тогда импримитивна, когда она обладает нормальным делителем $D_1 \subset A_1$, среди неприводимых частей которого есть неэквивалентные.

Лемма 11а доказывается почти так же, как лемма 11. Надо лишь в доказательстве леммы 11 равенство $[D] : \Delta = \rho^2\sigma$ заменить неравенством $[D] : \Delta \leqslant \rho^2\sigma$.

Из теоремы 19 в силу теорем 17, 18.4 и 18.5 вытекает

Теорема 20. *Пусть Δ — алгебраически замкнутое поле, а n — целое положительное число. Тогда совокупность всех максимальных разрешимых подгрупп группы $GL(n, \Delta)$ разбивается на конечное число классов сопряженных подгрупп; это число не превышает некоторой границы, зависящей только от n*

Для сравнения добавим, что, как доказал Платонов в [14], в любой алгебраической группе имеется лишь конечное множество несопряженных максимальных разрешимых подгрупп.

О вещественных разрешимых линейных группах см. Супруненко [8].

§ 21. Разрешимые группы матриц над конечным полем

1. Случай, когда $m = n$. Будем сперва считать, что Δ — произвольное поле. Пусть G — максимальная разрешимая примитивная подгруппа группы $GL(n, \Delta)$, а $F = K^*$ — максимальный абелев нормальный делитель группы G, где $K:\Delta = n$. Обозначим буквой $\mathcal{G}$ группу всех автоморфизмов поля K относительно поля Δ, а символом $N(F)$ — нормализатор F в $GL(n, \Delta)$.

Лемма 1. *Фактор-группа $N(F)/F$ изоморфна некоторой подгруппе группы $\mathcal{G}$. Если K — простое расширение поля Δ, то $N(F)/F \cong \mathcal{G}$. Группа G максимальна среди разрешимых подгрупп группы $N(F)$, а G/F изоморфна некоторой разрешимой подгруппе группы $\mathcal{G}$. Если K — простое расширение поля Δ, то группа G/F изоморфна максимальной разрешимой подгруппе группы $\mathcal{G}$.*

Доказательство. Ясно, что G является подгруппой группы N/F. Рассмотрим гомоморфизм

$$\gamma\colon N(F) \to G, \qquad g \mapsto \sigma_g,$$

где $\sigma_g\colon K \to K$, $\sigma_g(x) = gxg^{-1}$. По условию $K:\Delta = n$, следовательно, централизатор K в $GL(n, \Delta)$ равен F, т. е. $\operatorname{Ker}\gamma = F$, а фактор-группа $N(F)/F$ изоморфна некоторой подгруппе группы $\mathcal{G}$. Покажем теперь, что в случае, когда K — простое расширение поля Δ, гомоморфизм γ сюръективен. Пусть $K = \Delta(\theta)$, а $\sigma \in \mathcal{G}$. Тогда матрицы θ и $\theta_1 = \sigma(\theta)$ имеют один и тот же неприводимый в $\Delta[x]$ характеристический полином. Следовательно, $\sigma(\theta) = a\theta a^{-1}$, где $a \in GL(n, \Delta)$. Очевидно, что $a \in N(F)$, $\sigma(x) = axa^{-1}$ для $x \in K$. Сюръективность γ доказана. Следовательно, если K — простое расширение Δ, то $N(F)/F \cong \mathcal{G}$. ■

Применим теперь лемму 1 к случаю, когда Δ — конечное поле.

Теорема 1. *Пусть $\Delta = GF(p^t)$, G — максимальная разрешимая примитивная подгруппа группы $GL(n, \Delta)$, $F = K^*$ — максимальный абелев нормальный делитель группы G, где $K:\Delta = n$. Тогда:*

(i) *G — циклическое расширение группы K^* и*

$$\operatorname{card} G = n(p^{nt} - 1); \tag{1}$$

(ii) *если пространство Δ^n отождествить с K, то элементы g группы G можно записать в виде*

$$g(x) = \lambda x^{p^{tu}}, \tag{2}$$

где $x \in K$, $\lambda \in K^*$, $u = 0, 1, \ldots, n-1$.

Доказательство. По условию $\Delta = GF(p^t)$, $K = GF(p^{nt})$. Следовательно, $\mathcal{G} = \mathcal{G}(K, \Delta)$ — циклическая группа порядка n. В силу леммы 1 G/F — циклическая группа порядка n. Отсюда вытекает (i). Докажем (ii). Положим $\Delta^n = K$. Тогда F состоит из всех отображений f вида

$$f\colon K \to K, \quad f(x) = \lambda x, \quad x \in K, \quad \lambda \in K^*.$$

В силу леммы 1 $N(F)\colon F = n$, $N(F) = G$. С другой стороны, число элементов g вида (2) равно $\operatorname{card} N(F)$ и для таких элементов $gFg^{-1} = F$. Следовательно, $G = N(F)$ состоит из всех элементов вида (2). ■

Подгруппу группы $GL(n, \Delta)$, состоящую из всех элементов вида (2), обозначим через

$$G_{n(p^{nt}-1)}. \tag{3}$$

Лемма 2. *Пусть пара $\langle n, \Delta\rangle$, где n — целое число, а $\Delta = GF(p^t)$, подчинена следующему условию:*

(a) *для любого делителя d числа n, где $1 \leqslant d < n$, найдется такой простой делитель q числа n/d, что $q \nmid p^{dt} - 1$. Тогда любая максимальная разрешимая примитивная подгруппа группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с $G_{n(p^{nt}-1)}$.*

Утверждение леммы вытекает из следствия 20.3.2 и теоремы 1.

Теорема 2. *Пусть $\Delta = GF(p^t)$, а для каждого делителя n_1 числа n такого, что $1 < n_1 \leqslant n$, пара $\langle n_1, \Delta\rangle$ подчинена условию* (a) *леммы 2. Тогда любая максимальная неприводимая разрешимая подгруппа G группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ либо с группой $G_{n(p^{nt}-1)}$, либо с группой $G_{n_1(p^{n_1t}-1)} \wr \Gamma$, где $n_1 > 1$ — делитель числа n, Γ — максимальная транзитивная разрешимая подгруппа симметрической группы S_k, $k = nn_1^{-1}$.*

Доказательство. Если G примитивна, то теорема следует из леммы 2. Пусть G импримитивна. Тогда, согласно теореме 18.5, G сопряжена в $GL(n, \Delta)$ с группой $\mathfrak{G} \wr \Gamma$, где $\mathfrak{G}$ — максимальная примитивная разрешимая подгруппа группы $GL(n_1, \Delta)$, Γ — максимальная транзитивная разрешимая подгруппа симметрической группы S_k, $kn_1 = n$. В силу леммы 2 группа $\mathfrak{G}$ сопряжена в $GL(n_1, \Delta)$ с группой $G_{n_1}(p^{n_1 t}-1)$. Следовательно, G сопряжена с $G_{n_1}(p^{n_1 t}-1) \wr \Gamma$. ■

Условия теоремы 2 выполняются, в частности, если $n = q^l$, $\Delta = GF(p^t)$, где q — простое число и $q \nmid p^t - 1$. Действительно, в этом случае, как легко проверить, $(q, p^{nt} - 1) = 1$.

2. Образующие группы Q. *Пусть* Δ — *произвольное* поле, G — максимальная примитивная разрешимая подгруппа группы $GL(n, \Delta)$, A и $F = K^*$ — группы ряда (α) (см. § 20, п. 2), $K : \Delta = m < n$, q — простой делитель числа n/m, а Q/F — q-подгруппа Силова группы A/F. При этих обозначениях справедлива

Лемма 3. *Пусть $Q = BC$, где B и C — такие подгруппы группы Q, что $(B, C) = 1$, $C \supset F$. Если D — нормальный делитель группы C, группа C/D локально циклична, а центр группы D содержится в F, то $(Q, C) = (D, D)$.*

Доказательство. Так как $(B, C) = 1$, то $(Q, C) = (C, C)$. Возможны лишь два случая: 1) $(D, D) = 1$, 2) $(D, D) = (Q, Q)$. Во втором случае лемма очевидна. Рассмотрим первый случай. Пусть $(D, D) = 1$. Тогда, по условию, $Z(D) = D \subset F$. В силу локальной цикличности C/D группа C абелева. Следовательно, $(Q, C) = (C, C) = 1 = (D, D)$. ■

Докажем еще одну лемму о группе Q.

Лемма 4. *Пусть Δ — алгебраическое расширение конечного поля, а $Q_0 = Q \cap SL(n, \Delta)$. Тогда $(Q_0, Q_0) \neq 1$.*

Доказательство. Рассмотрим отображение

$$\delta \colon Q \to \Delta^*, \qquad x \mapsto \det x,$$

при котором, очевидно, $\operatorname{Ker} \delta = Q_0$, $\operatorname{Im} \delta \subset \Delta^*$, $\operatorname{Im} \delta \cong Q/Q_0$. Так как Δ^* — локально циклическая группа, то и фактор-группа Q/Q_0 локально циклична. Очевидно, центр $Z(Q_0)$ группы Q_0 является нормальным делителем в G. Следовательно, $Z(Q_0) \subset F$. Если теперь положить

$B = F$, $C = Q$, $D = Q_0$, то B, C и D будут удовлетворять условиям леммы 3. Согласно лемме 3 $(Q_0, Q_0) = (Q, Q) \neq 1$. ■

В силу следствия 20.5.1 группу Q можно представить в виде

$$Q = (c_1)(d_1)\ \dots\ (c_l)(d_l)\,F, \tag{4}$$

$$(c_j,\ d_j) = \eta,\quad \eta^q = 1,\quad \eta \neq 1,\quad \eta \in F,\quad c_j^q,\, d_j^q \in F, \tag{5}$$

а элементы, принадлежащие различным парам c_j, d_j, перестановочны.

Теорема 3. *Пусть Δ — алгебраическое расширение конечного поля. Тогда образующие c_ν, d_ν группы Q можно выбрать так, что кроме формул* (4) *и* (5) *будут верны равенства*:

$$c_\nu^q = d_\nu^q = 1,\qquad \nu = 1, \dots, l, \tag{6}$$

(*при* $q > 2$) *и*

$$c_\nu^2 = \pm 1,\quad d_\nu^2 = \pm 1,\qquad \nu = 1, \dots, l \tag{7}$$

(*при* $q = 2$).

Доказательство. Положим

$$\left.\begin{aligned} &B = (c_1)(d_1)\ \dots\ (c_{j-1})(d_{j-1})(\eta),\\ &C = (c_j)(d_j)\ \dots\ (c_l)(d_l)\,F,\\ &D = \begin{cases} \{x \mid x \in C,\ x^q = 1\} & \text{при}\quad q > 2,\\ \{x \mid x \in C,\ x^q = \pm 1\} & \text{при}\quad q = 2. \end{cases}\end{aligned}\right\} \tag{8}$$

Тогда $Q = BC$, $(B, C) = 1$, $C \supset F$. Пусть u, $v \in D$. При $q > 2$

$$u^q = v^q = 1,\ vu = \lambda uv,\ \lambda \in F,\ \lambda^q = 1;$$

$$(uv)^q = \lambda^{\frac{q(q-1)}{2}} u^q v^q = 1.$$

Следовательно, $uv \in D$. При $q = 2$

$$u^2 = \pm 1,\quad v^2 = \pm 1,\quad vu = \pm uv,\quad (uv)^2 = \pm 1,$$

т. е. $uv \in D$. Отсюда вытекает, что D — нормальный делитель группы C.

Фактор-группа C/D локально циклична. Действительно, если $q > 2$, то рассмотрим отображение γ: $C \to F$,

$x \longmapsto x^q$. Как легко подсчитать,

$$\gamma(x, y) = (y, x)^{\frac{q(q-1)}{2}} x^q y^q = x^q y^q = \gamma(x)\gamma(y).$$

Следовательно, γ — гомоморфизм, $\operatorname{Im}\gamma \subset F$, $\operatorname{Ker}\gamma = D$. Так как Δ — алгебраическое расширение конечного поля, то $F = K^*$ — локально циклическая группа. Следовательно, при $q > 2$ группа $C/D \cong \operatorname{Im}\gamma$ локально циклична. Если же $q = 2$, то рассмотрим отображение

$$\gamma_1\colon C/\{\pm 1\} \to F/\{\pm 1\}, \qquad \{\pm 1\}x \to \{\pm 1\}x^2.$$

Очевидно, что γ_1 — гомоморфизм, $\operatorname{Ker}\gamma_1 = D/\{\pm 1\}$,

$$C/D \cong C/\{\pm 1\}/D/\{\pm 1\} \cong \operatorname{Im}\gamma_1 \subset F/\{\pm 1\}.$$

Следовательно, группа C/D локально циклична и при $q = 2$. Для применимости леммы 3 надо еще показать, что центр $Z(D)$ группы D содержится в F. Пусть сперва $j = 1$. Тогда $B = (\eta)$, $C = Q$, а группа D инвариантна в G. Следовательно, $Z(D) \subset F$. Итак, при $j = 1$ группы B, C, D удовлетворяют условиям леммы 3, т. е. $(D, D) = (Q, C) = (C, C)$. Отсюда $(D, D) \neq 1$. Тогда мы можем считать, что одна пара c_1, d_1 принадлежит группе D, т. е.

$$c_1^q = d_1^q = 1 \qquad \text{при} \quad q > 2,$$
$$c_1^2 = \pm 1,\ d_1^2 = \pm 1 \qquad \text{при} \quad q = 2.$$

Пусть для $j - 1$ пар $c_1, d_1, \ldots, c_{j-1}, d_{j-1}$ выполняются условия

$$c_1^q = d_1^q = \ldots = c_{j-1}^q = d_{j-1}^q = 1 \qquad \text{при} \quad q > 2,$$
$$c_1^2 = \pm 1,\ d_1^2 = \pm 1,\ \ldots,\ c_{j-1}^2 = \pm 1,\ d_{j-1}^2 = \pm 1 \qquad \text{при} \quad q = 2,$$

а B, C и D заданы формулами (8). Введем еще группу $\bar{Q}$, положив

$$\bar{Q} = \{x \mid x \in Q,\ x^q = 1\} \qquad \text{при} \quad q > 2,$$
$$\bar{Q} = \{x \mid x \in Q,\ x^2 = \pm 1\} \qquad \text{при} \quad q = 2.$$

Группа $\bar{Q}$ инвариантна в G, следовательно, ее центр $Z(\bar{Q})$ содержится в F. Ясно, что $B \subset \bar{Q}$. Пусть $a \in \bar{Q}$, тогда

$$a = bc, \quad b \in B, \quad c \in C. \tag{9}$$

Для c из (9) имеем $c \in D$, т. е. $\bar{Q} = BD$. Так как $(B, D) = 1$, то $Z(D) \subset Z(\bar{Q}) \subset F$. Таким образом, B, C, D удовлетворяют условиям леммы 3. Следовательно, c_j, d_j можно выбрать в D. Отсюда и следует теорема. ■

Доказанная теорема позволяет матрицам группы A придать канонический вид, если основное поле Δ является алгебраическим расширением конечного поля.

Согласно § 20 группа A ряда (α) приводима к виду

$$A = Q^1 \dot{\times} \ldots \dot{\times} Q^k.$$

Следовательно, достаточно рассмотреть группы $Q^j \cong Q_j$.

Теорема 4. *Пусть Δ — алгебраическое расширение конечного поля, а $q_j = q > 2$. Тогда в подходящем базисе пространства K^{q^l} группе Q^j можно придать вид*

$$Q^j = (u_1)(v_1) \ldots (u_l)(v_l) F, \tag{10}$$

при этом

$$\begin{aligned} u_\nu &= E_{q^{\nu-1}} \dot{\times} c \dot{\times} E_{q^{l-\nu}}, \\ v_\nu &= E_{q^{\nu-1}} \dot{\times} d \dot{\times} E_{q^{l-\nu}}, \end{aligned} \tag{11}$$

где

$$c = \operatorname{diag}[1, \eta, \ldots, \eta^{q-1}], \qquad d = \begin{bmatrix} 0 & 1 \\ E_{q-1} & 0 \end{bmatrix},$$

$$\eta^q = 1, \quad \eta \neq 1, \quad \eta \in K^*, \qquad \nu = 1, \ldots, l.$$

Доказательство. Пусть φ: $Q_j \to Q^j$ — изоморфизм, а $\bar{c}_\nu = \varphi(c_\nu)$, $\bar{d}_\nu = \varphi(d_\nu)$, $\nu = 1, \ldots, l$ (см. (4)). По теореме 3

$$\bar{c}_\nu^q = \bar{d}_\nu^q = 1, \qquad \nu = 1, \ldots, l.$$

С другой стороны, как легко проверить,

$$u_\nu^q = v_\nu^q = 1, \qquad (u_\nu, v_\nu) = (\bar{c}_\nu, \bar{d}_\nu) = \eta,$$

а матрицы, принадлежащие различным парам u_ν, v_ν, перестановочны. Следовательно, отображение

$$\bar{c}_\nu \longmapsto u_\nu, \quad \bar{d}_\nu \longmapsto v_\nu, \quad \nu = 1, \ldots, l,$$

можно продолжить до центрального автоморфизма алгебры $[Q^j] = K_{q^l}$. Поэтому в $GL(q^l, K)$ есть такая матрица t, что $t\bar{c}_\nu t^{-1} = u_\nu$, $t\bar{d}_\nu t^{-1} = v_\nu$, $\nu = 1, \ldots, l$. ■

Теорема 5. *Пусть* Δ — *алгебраическое расширение конечного поля, а* $q_j = q = 2$.

(i) *Если в* K^* *есть элемент 4-го порядка, то* Q^j *задается формулами* (10) *и* (11).

(ii) *Если в* K^* *нет элемента 4-го порядка, то возможны два случая*:

1) Q^j *задается формулами* (10) *и* (11), *где надо положить* $q = 2$, $\eta = -1$;

2) Q^j *задается формулой* (10), u_ν *и* v_ν *при* $\nu \neq l$ *определяются формулами* (11), *где надо положить* $q = 2$, $\eta = -1$, *а*

$$u_l = E_{2l-1} \dot{\times} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad v_l = E_{2l-1} \dot{\times} \begin{bmatrix} \gamma & \delta \\ \delta & -\gamma \end{bmatrix},$$

$$\gamma^2 + \delta^2 + 1 = 0, \qquad \gamma,\ \delta \in K.$$

Доказательство. Пусть в K^* есть элемент 4-го порядка. Тогда в теореме 3 можно вместо (7) написать $c_\nu^2 = d_\nu^2 = 1$, $\nu = 1, \ldots, l$. Следовательно, теорема 4 в этом случае верна и при $q = 2$. Итак, (i) доказано. Пусть теперь в K^* нет элемента 4-го порядка. Если $c_\nu^2 = d_\nu^2 = 1, \nu = 1, \ldots, l$, то Q^l задается формулами (10) и (11). Остается рассмотреть случай, когда при некотором ν либо $c_\nu^2 = -1$, либо $d_\nu^2 = -1$. Если $c_\nu^2 = -d_\nu^2 = \pm 1$, то пару c_ν, d_ν можно заменить такой парой c'_ν, d'_ν, что $c'^2_\nu = d'^2_\nu = 1$. Действительно, пусть, например, $c_\nu^2 = -d_\nu^2 = -1$. Тогда заменим пару c_ν, d_ν парой $c_\nu d_\nu$, d_ν, $(c_\nu d_\nu)^2 = -c_\nu^2 d_\nu^2 = 1$. Следовательно, мы можем считать, что $c_\nu^2 = d_\nu^2 = \pm 1$. Покажем теперь, что c_l, d_l можно так выбрать, что $c_j^2 = d_j^2 = 1$, $j = 1, \ldots, l-1$, а $c_l^2 = d_l^2 = -1$. Пусть имеются две пары

$$c_\nu^2 = d_\nu^2 = -1, \qquad c_\mu^2 = d_\mu^2 = -1, \qquad \mu \neq \nu.$$

Тогда пары c_ν, d_ν и c_μ, d_μ заменим парами c_ν, $d_\nu d_\mu$ и $c_\nu c_\mu$, d_μ; $(d_\nu d_\mu)^2 = (c_\nu c_\mu)^2 = 1$. Согласно предыдущему, в свою очередь, две последние пары можно заменить такими парами c'_ν, d'_ν и c'_μ, d'_μ, что $c'^2_\nu = d'^2_\nu = c'^2_\mu = d'^2_\mu = 1$. Следовательно, c_l, d_l можно выбрать так, что

$$c_1^2 = d_1^2 = \ldots = c_{l-1}^2 = d_{l-1}^2 = 1, \qquad c_l^2 = d_l^2 = -1.$$

Тем же условиям подчинены и матрицы u_ν, v_ν из теоремы 5. Отсюда, как и при доказательстве теоремы 4, получаем (ii). ■

3. Неприводимые разрешимые группы простой степени. Здесь мы построим все максимальные неприводимые разрешимые подгруппы группы $GL(q, \Delta)$, где q — простое число, а $\Delta = GF(p^t)$. С самого начала отметим, что группа $GL(q, \Delta)$ разрешима, если $q = 2$, а Δ совпадает либо с $GF(2)$, либо с $GF(3)$, ибо в этом случае порядок $GL(q, \Delta)$ равен либо 6, либо 48.

Пусть G — максимальная неприводимая разрешимая подгруппа группы $GL(q, \Delta)$. Возможны три случая:

1) G импримитивна.

2) G примитивна, ее максимальный абелев нормальный делитель $F = K^*$, где $K = GF(p^{qt})$.

3) G примитивна, ее максимальный абелев нормальный делитель $F = \Delta^* E_q$.

В первом случае группа G мономиальна и, согласно теореме 18.5, G сопряжена в $GL(q, \Delta)$ с $\Delta^* \wr \Gamma$, где Γ — максимальная транзитивная разрешимая подгруппа симметрической группы S_q. В силу теоремы 4.11 максимальные разрешимые транзитивные подгруппы S_q сопряжены в S_q и имеют порядок $q(q-1)$. Следовательно, в этом случае

$$\operatorname{card} G = q(q-1)(p^t-1)^q. \qquad (12)$$

Во втором случае, согласно теореме 1, группа G сопряжена в $GL(q, \Delta)$ с группой $G_{q(p^{qt}-1)}$. Значительно сложнее третий случай. Пусть группа G примитивна, а ее максимальный абелев нормальный делитель $F = \Delta^* E_q$. Тогда G обладает нормальным делителем

$$\begin{gathered} A = (a)(b)F, \quad a^q \in F, \qquad b^q \in F, \\ (a, b) = \eta E_q, \quad \eta^q = 1, \quad \eta \neq 1, \quad \eta \in \Delta. \end{gathered} \qquad (13)$$

Так как из (13) следует, что в Δ^* есть элемент порядка q, то третий случай возможен лишь при условии, когда $q \mid p^t - 1$. Очевидно, что G является подгруппой нормализатора N группы A в $GL(q, \Delta)$. Для $x \in N$ можно написать

$$xax^{-1} = \lambda a^\alpha b^\gamma, \qquad xbx^{-1} = \mu a^\beta b^\delta,$$

где λ, $\mu \in \Delta$, α, β, γ, $\delta \in GF(q)$. Положим

$$\psi\colon N \to Sp(2, q) = SL(2, q), \qquad x \mapsto \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}. \tag{14}$$

Пусть сперва $q = 2$ и в Δ^* есть элемент i 4-го порядка, т. е. $p^t - 1 \equiv 0 \pmod 4$. Тогда, согласно теореме 4, a и b можно выбрать так:

$$a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{15}$$

Согласно теореме 20.16 гомоморфизм $\psi\colon N \to SL(2, 2)$ сюръективен. Так как $\operatorname{Ker}\psi = A$, то $N/A \cong SL(2,2) \cong S_3$. Следовательно, N — разрешимая группа, $G = N$,

$$\operatorname{card} G = 6 \cdot 4(p^t - 1) = 24(p^t - 1). \tag{16}$$

Группа $SL(2, 2)$ порождается двумя матрицами

$$\sigma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad \tau = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Положим

$$g = \operatorname{diag}[1, -i], \qquad h = \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}. \tag{17}$$

Как легко проверить, g, $h \in N$, $\psi(h) = \sigma$, $\psi(h) = \tau$. Следовательно, элементы

$$a,\ b,\ g,\ h,\ \rho E_2, \tag{18}$$

где $\rho \in \Delta^*$ и имеет порядок $p^t - 1$, a и b задаются формулами (15), а g и h — формулами (17), составляют систему образующих группы G.

Пусть теперь $q = 2$, но в Δ^* нет элемента 4-го порядка. В силу леммы 4 элементы a и b в (13) можно выбрать так, что

$$\det a = \det b = 1. \tag{19}$$

Из (19) и из включений a^2, $b^2 \in \Delta^* E_2$ вытекает, что $z^2 + 1$ — минимальный полином матриц a и b. Следовательно, можно положить

$$a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Отсюда и из условий $(a, b) = b^2 = -E_2$ найдем

$$b = \begin{bmatrix} \theta & \omega \\ \omega & -\theta \end{bmatrix}, \qquad \theta^2 + \omega^2 = -1, \qquad \theta, \omega \in \Delta^*.$$

В качестве образующих группы $SL(2, 2)$ возьмем матрицы

$$\sigma \quad \text{и} \quad \tau_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Как легко проверить, матрицы

$$g_1 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \qquad h_1 = \begin{bmatrix} \theta & \omega - 1 \\ \omega + 1 & -\theta \end{bmatrix} \tag{20}$$

подчинены следующим условиям:

$$g_1 a g_1^{-1} = a, \qquad h_1 a h_1^{-1} = b,$$
$$g_1 b g_1^{-1} = ab, \qquad h_1 b h_1^{-1} = a.$$

Следовательно, $g_1, h_1 \in N$ и

$$\psi(g_1) = \sigma, \quad \psi(h_1) = \tau_1, \quad N/A \cong SL(2, 2),$$
$$N = G, \qquad \operatorname{card} G = 24(p^t - 1).$$

Группа G порождается матрицами

$$a, b, g_1, h_1, \rho E_2, \tag{21}$$

где $a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $b = \begin{bmatrix} \theta & \omega \\ \omega & -\theta \end{bmatrix}$, $\theta^2 + \omega^2 = -1$, $\theta, \omega \in \Delta^*$, g_1 и h_1 задаются формулами (20), а ρ — элемент порядка $p^t - 1$ из Δ^*.

Случай $q = 2$ рассмотрен полностью.

Пусть теперь $q > 2$. Тогда, согласно теореме 4, матрицы a и b можно выбрать так:

$$a = \operatorname{diag}[1, \eta, \ldots, \eta^{q-1}], \qquad b = \begin{bmatrix} 0 & 1 \\ E_{q-1} & 0 \end{bmatrix},$$
$$a^q = b^q = E_q, \qquad \eta^q = 1, \quad \eta \neq 1, \quad \eta \in \Delta^*.$$

Согласно теореме 20.16 гомоморфизм ψ сюръективен. Следовательно, $N/A \cong SL(2, q)$, $G = \psi^{-1}(H)$, где H — максимальная разрешимая подгруппа группы $SL(2, q)$.

Лемма 5. *Пусть H — подгруппа группы $SL(2, q)$. Группа $\psi^{-1}(H)$ тогда и только тогда примитивна, когда H неприводима.*

Доказательство. Если H — неприводимая подгруппа группы $SL(2, q)$, то $\psi^{-1}(H)$ примитивна в силу леммы 20.11а. Пусть теперь H — приводимая подгруппа группы $SL(2, q)$. Тогда в $GL(2, q)$ есть такая матрица d, что матрицы группы dHd^{-1} имеют вид

$$\begin{bmatrix} \alpha & \beta \\ 0 & \delta \end{bmatrix}, \qquad \alpha,\ \beta,\ \delta \in GF(q). \tag{22}$$

Матрицу d можно выбрать в $SL(2, q)$. Действительно, пусть $\det d = \delta_1$, $\delta_2\delta_1 = 1$. Тогда

$$d_1 = \begin{bmatrix} 1 & 0 \\ 0 & \delta_2 \end{bmatrix} d \in SL(2,\ q),$$

а матрицы группы $d_1 H d_1^{-1} = H_1$ имеют вид (22). Группа $\psi^{-1}(H_1)$ импримитивна. В самом деле, так как матрицы из H_1 имеют вид (22), то для любого элемента g из $\psi^{-1}(H_1)$

$$gag^{-1} = \lambda a^n, \qquad g(a)Fg^{-1} = (a)F,$$

т. е. $(a)F$ — абелев нормальный делитель группы $\psi^{-1}(H_1)$. В силу теоремы 16.2 группа $\psi^{-1}(H_1)$ импримитивна. Так как H_1 и H сопряжены в $SL(2, q)$, то $\psi^{-1}(H_1)$ и $\psi^{-1}(H)$ сопряжены в N. Следовательно, группа $\psi^{-1}(H)$ тоже импримитивна. ∎

В силу доказанной леммы построение всех максимальных разрешимых примитивных подгрупп группы $GL(q, \Delta)$ сводится к построению системы всех максимальных разрешимых неприводимых подгрупп группы $SL(2, q)$ и разбиению этой системы на классы подгрупп, сопряженных в $SL(2, q)$.

Если $q = 3$, то $SL(2, q)$ — разрешимая группа порядка 24. Следовательно, при $q = 3$ $G = \psi^{-1}(SL(2, 3))$,

$$\operatorname{card} G = 24 \cdot 9 \cdot (p^t - 1) = 216(p^t - 1). \tag{23}$$

Пусть теперь $q > 3$. Найдем максимальные разрешимые неприводимые подгруппы группы $SL(2,\ q)$. Как доказано выше, максимальная разрешимая неприводимая подгруппа группы $GL(2, q)$ сопряжена в $GL(2, q)$ с одной из следующих групп *):

G_1 порядка $2(q-1)^2$ (G_1 импримитивна),
G_2 порядка $2(q^2-1)$ (G_2 примитивна, $\operatorname{card} F = q^2-1$),
G_3 порядка $24(q-1)$ (G_3 примитивна, $\operatorname{card} F = q-1$).

Максимальная разрешимая неприводимая подгруппа группы $SL(2, q)$ есть пересечение максимальной разрешимой неприводимой подгруппы группы $GL(2, q)$ с группой $SL(2, q)$.

Построим пересечение $U_j = G_j \cap SL(2, q)$, $j = 1, 2, 3$. Группа G_1 есть множество всех матриц вида

$$\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^\tau,$$

$$\lambda_1, \lambda_2 \in GF(q), \quad \tau = 0, 1, \quad \lambda_1, \lambda_2 \neq 0.$$

Следовательно, U_1 состоит из всех матриц вида

$$\begin{bmatrix} \lambda & 0 \\ 0 & (-1)^\tau \lambda^{-1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^\tau,$$

$$\lambda \in GF(q), \quad \tau = 0, 1, \quad \lambda \neq 0;$$

$\operatorname{card} U_1 = 2(q-1)$. Группа U_1 порождается двумя матрицами u и v:

$$u = \operatorname{diag}[\rho, \rho^{-1}], \qquad v = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

где ρ — элемент порядка $q-1$ из $GF(q)$. Группа G_2 вида $G_{n\,(p^{nt}-1)}$ (см. (3)) состоит из элементов g вида

$$g(x) = \lambda x^{q^\tau}, \quad x, \lambda \in GF(q^2), \quad \lambda \neq 0, \quad \tau = 0, 1.$$

Группа G_2 порождается двумя элементами g_0 и f_0, где

$$g_0(x) = x^q, \qquad f_0(x) = \mu x, \qquad x \in GF(q^2),$$

μ — элемент порядка q^2-1 из $GF(q^2)$. Найдем $\det g_0$ и $\det f_0$. Пусть $\omega \in GF(q^2) \setminus GF(q)$. Тогда $1, \omega$ — базис

*) Группа G_1 при $q = 5$ не максимальна среди разрешимых подгрупп группы $GL(2,5)$. Действительно, $\operatorname{card} GL(2,5) = 2^5 \cdot 15$, $\operatorname{card} G_1 = 2^5$, $\operatorname{card} G_3 = 2^5 \cdot 3$. Группа G_1 является 2-подгруппой Силова группы $GL(2,5)$ и сопряжена в $GL(2,5)$ с некоторой подгруппой группы G_3.

$GF(q^2)$ над $GF(q)$; $\omega+\omega^q=\nu\in GF(q)$. Далее, так как $g_0(1)=1$, $g_0(\omega)=\omega^q=\nu-\omega$, то g_0 задается матрицей

$$\begin{bmatrix} 1 & \nu \\ 0 & -1 \end{bmatrix}, \qquad \det g_0=-1.$$

Для вычисления $\det f_0$ возьмем в качестве базиса $GF(q^2)$ над $GF(q)$ элементы $1, \mu$:

$$f_0(1)=\mu, \qquad f_0(\mu)=\mu^2=-\mu^{q+1}+(\mu^q+\mu)\mu;$$

$$\det f_0=\begin{vmatrix} 0 & -\mu^{q+1} \\ 1 & \mu^q+\mu \end{vmatrix}=\mu^{q+1}.$$

Следовательно, гомоморфизм

$$G_2\to(GF(q))^*, \qquad x\mapsto\det x$$

сюръективен, его ядро совпадает с U_2. Отсюда

$$\operatorname{card} U_2=2(q+1).$$

Рассмотрим, наконец, G_3 и U_3. Группа G_3 порождается либо элементами (18), либо элементами (21) (в (18) и (21) надо заменить p^t числом q). В первом случае в $GF(q)$ есть элемент i 4-го порядка. Легко видеть, что $\det a$, $\det b$, $\det \rho E_2$ суть квадраты в поле $GF(q)$. Далее, $h^3=(2+2i)E_2$, следовательно, $\det h$ — тоже квадрат в $GF(q)$. В силу (17) $\det g=-i$. Следовательно, $\det g$ — тогда и только тогда квадрат в $GF(q)$, когда $q\equiv 1 \pmod 8$. Пусть теперь G_3 порождается элементами (21), $\det g_1=2$, $\det h_1=2$. Следовательно, $\det x$ является квадратом в $GF(q)$ для всех x из G_3 тогда и только тогда, когда число 2 есть квадратичный вычет по модулю q, т. е. когда $q\equiv\pm 1 \pmod 8$. Отсюда вытекает, что в обоих случаях гомоморфизм

$$G_3\mapsto(GF(q))^*, \qquad x\mapsto\det x$$

тогда и только тогда сюръективен, когда $q\equiv\pm 3 \pmod 8$.

Итак, если $q\equiv\pm 3 \pmod 8$, то $\operatorname{card} U_3=\dfrac{24(q-1)}{q-1}=24$.

Если же $q\equiv\pm 1 \pmod 8$, то $\operatorname{card} U_3=\dfrac{24(q-1)}{(q-1)/2}=48$.

Таким образом, группы $U_j=G_j\cap SL(2, q)$, $j=1, 2, 3$, найдены. Однако надо заметить, что сопряженность двух групп B и B_1 в $GL(n, P)$ не влечет за собой сопряженность в $SL(n, P)$ групп $B \cap SL(n, P)$ и $B_1 \cap SL(n, P)$. Если P — произвольное поле, B — подгруппа группы $GL(n, P)$, а гомоморфизм

$$B \to P^*, \qquad x \mapsto \det x \tag{24}$$

сюръективен, то из сопряженности групп B и B_1 в $GL(n, P)$ следует сопряженность групп $B \cap SL(n, P)$ и $B_1 \cap SL(n, P)$ в $SL(n, P)$. Действительно, пусть $B_1 = tBt^{-1}$, $t \in GL(n, P)$. Так как гомоморфизм (24) сюръективен, то в B есть такая матрица b, что $\det b = (\det t)^{-1}$. Положим $d = tb$. Тогда $\det d = 1$, $dBd^{-1} = B_1$,

$$B_1 \cap SL(n, P) = dBd^{-1} \cap dSL(n, P)d^{-1} = d(B \cap SL(n, P))d^{-1}.$$

Мы видели, что отображение $G_j \to (GF(q))^*$, $x \mapsto \det x$ для $j = 1, 2$ всегда сюръективно, а при $j = 3$ сюръективно лишь при $q \equiv \pm 3 \pmod 8$. Остается рассмотреть группу G_3 при $q \equiv \pm 1 \pmod 8$. Пусть r — такая матрица из $GL(2, q)$, что $\det r$ не является квадратом в $(GF(q))^*$. Как легко видеть, любая группа вида dU_3d^{-1}, где $d \in GL(2, q)$, сопряжена в $SL(2, q)$ с одной из двух групп U_3, $U_4 = rU_3r^{-1}$. Покажем, что U_3 и U_4 не сопряжены в $SL(2, q)$. Пусть $lU_4l^{-1} = U_3$, $l \in SL(2, q)$. Тогда $lrU_3(lr)^{-1} = U_3$. Так как при $q \equiv \pm 1 \pmod 8$ $G_3 = U_3(GF(q))^*$, то $lrG_3(lr)^{-1} = G_3$. Далее, $d = lr \notin G_3$, ибо $\det lr$ не является квадратом. Следовательно, $(d)G$ — разрешимая группа, содержащая G_3 в качестве истинной подгруппы. Последнее противоречит максимальности G_3. Значит, U_3 и U_4 не сопряжены в $SL(2, q)$.

Итак, если $q > 3$, то всякая максимальная примитивная разрешимая подгруппа группы $GL(q, \Delta)$ с максимальным абелевым нормальным делителем $F = \Delta^* E_q$ сопряжена в $GL(q, \Delta)$ с одной из следующих четырех групп:

$$\psi^{-1}(U_j), \qquad j = 1, 2, 3, 4.$$

Отсюда и из предыдущих рассмотрений настоящего пункта вытекает

Теорема 6. *Пусть $\Delta = GF(p^t)$, где p — простое число. Тогда верны следующие утверждения:*

1. *Всякая максимальная неприводимая разрешимая подгруппа группы $GL(2, \Delta)$ сопряжена в $GL(2, \Delta)$ с одной из трех следующих подгрупп:*

$G_{2,1}$ *порядка* $2(p^t - 1)^2$,
$G_{2,2}$ *порядка* $2(p^{2t} - 1)$,
$G_{2,3}$ *порядка* $24(p^t - 1)$.

2. *Всякая максимальная неприводимая разрешимая подгруппа группы $GL(3, \Delta)$ сопряжена в $GL(3, \Delta)$ с одной из трех следующих подгрупп:*

$G_{3,1}$ *порядка* $6(p^t - 1)^3$,
$G_{3,2}$ *порядка* $3(p^{3t} - 1)$,
$G_{3,3}$ *порядка* $216(p^t - 1)$.

3. *Всякая максимальная неприводимая разрешимая подгруппа группы $GL(q, \Delta)$, где q — простое число, $q > 3$, сопряжена в $GL(q, \Delta)$ с одной из следующих шести подгрупп:*

$G_{q,1}$ *порядка* $q(q-1)(p^t-1)^q$,
$G_{q,2}$ *порядка* $q(p^{qt}-1)$,
$G_{q,3}$ *порядка* $2(q-1)q^2(p^t-1)$,
$G_{q,4}$ *порядка* $2(q+1)q^2(p^t-1)$,
$G_{q,5}$ *порядка* $48(p^t-1)q^2$, $q \equiv \pm 1 \pmod 8$,
или порядка $24(p^t-1)q^2$, $q \equiv \pm 3 \pmod 8$,
$G_{q,6}$ *порядка* $48(p^t-1)q^2$;

группы $G_{q,3}$, $G_{q,4}$, $G_{q,5}$, $G_{q,6}$ существуют только при условии $p^t \equiv 1 \pmod q$, а для существования группы $G_{q,6}$, сверх того, должно выполняться сравнение $q \equiv \equiv \pm 1 \pmod 8$, причем

$$G_{q,\,j+2} = \psi^{-1}(U_j), \quad G_{q,\,j+2}/A \cong U_j, \quad j = 1,\ 2,\ 3,\ 4.$$

Примечания к теореме 6. 1) Группы $G_{2,1}$, $G_{3,1}$, $G_{q,1}$ мономиальны. 2) $G_{2,2}$, $G_{3,2}$, $G_{q,2}$ — группы вида $G_{n\,(p^{nt}-1)}$ ($n = 2, 3, q$, см. формулу (3)). 3) Группа $G_{2,3}$ существует при $p > 2$, $G_{2,1}$ — при $p^t > 2$, $G_{3,3}$ — при $3 \mid p^t - 1$. 4) Если $p^t = 2$, то при любом простом q всякая максимальная неприводимая разрешимая подгруппа группы $GL(q, 2)$ сопряжена в $GL(q, 2)$ с группой $G_{q,2}$ порядка $q(2^q - 1)$. 5) Если $p^t = 3$, то группы $G_{2,1}$ и $G_{2,2}$ не максимальны, они содержатся в $G_{2,3} = GL(2, 3)$. 6) Если $p^t = 5$, то группа $G_{2,1}$ не максимальна, она сопряжена с истинной подгруппой группы $G_{2,3}$. 7) В $GL(5, \Delta)$ имеется либо две, либо четыре несопряженные максимальные неприводимые разрешимые подгруппы. Если $5 \nmid p^t - 1$, то это будут $G_{5,1}$ и $G_{5,2}$. Если $5 \mid p^t - 1$, то к ним надо добавить только две группы — $G_{5,4}$ и $G_{5,5}$, ибо, в силу 6), группа $G_{5,3}$ не максимальна, она сопряжена с истинной подгруппой группы $G_{5,5}$, а группы $G_{5,6}$ нет вовсе, так как $5 \not\equiv \pm 1 \pmod 8$. Описание максимальных неприводимых разрешимых подгрупп группы $GL(q, \Delta)$ полностью завершено.

§ 22. Разное

1. Неприводимые разрешимые группы простой степени над алгебраически замкнутым полем. Пусть q — простое число, а Δ — алгебраически замкнутое поле. Используя предыдущие результаты, можно полностью классифицировать максимальные неприводимые разрешимые подгруппы группы $GL(q, \Delta)$. Здесь возможны два случая: 1) $q = \operatorname{char}\Delta$, 2) $q \neq \operatorname{char}\Delta$. В первом случае, в силу следствия 20.3.1, в $GL(q, \Delta)$ нет примитивных разрешимых подгрупп и, следовательно, любая неприводимая разрешимая подгруппа группы $GL(q, \Delta)$ мономиальна. Отсюда вытекает

Теорема 1. *Пусть $q = \operatorname{char}\Delta$. Тогда любая максимальная неприводимая разрешимая подгруппа группы $GL(q, \Delta)$ сопряжена в $GL(q, \Delta)$ с группой*

$$\Delta^* \wr \Gamma, \tag{1}$$

где Γ — максимальная транзитивная разрешимая группа подстановок степени q порядка $q(q-1)$.

Пусть теперь $q \neq \operatorname{char}\Delta$. Найдем максимальные неприводимые разрешимые подгруппы группы $GL(q, \Delta)$. Если такая подгруппа импримитивна, то, очевидно, она сопряжена в $GL(q, \Delta)$ с группой (1). Остается найти максимальные примитивные разрешимые подгруппы группы $GL(q, \Delta)$. Согласно теореме 20.19 всякая такая подгруппа сопряжена в $GL(q, \Delta)$ с группой вида $\psi^{-1}(H)$, где H — максимальная s-неприводимая подгруппа группы $Sp(2, q) = SL(2, q)$, причем сопряженность H и H_1 в $Sp(2, q)$ влечет за собой сопряженность $\psi^{-1}(H)$ и $\psi^{-1}(H_1)$ в $GL(q, \Delta)$. Из определения s-неприводимости следует, что s-неприводимость для подгрупп группы $Sp(2, q)$ равносильна неприводимости. Таким образом, для построения всех максимальных примитивных разрешимых подгрупп группы $GL(q, \Delta)$ надо найти максимальные неприводимые разрешимые подгруппы группы $SL(2, q)$ и разбить их множество на классы сопряженных подгрупп. При доказательстве теоремы 21.6 были найдены максимальные неприводимые разрешимые подгруппы U_1, U_2, U_3, U_4 группы $SL(2, q)$ такие, что любая максимальная разрешимая неприводимая подгруппа группы $SL(2, q)$ сопряжена в $SL(2, q)$ с одной из них. Отсюда и из свойств групп U_1, U_2, U_3, U_4 следует

Теорема 2. *Пусть $q \neq \operatorname{char}\Delta$. Тогда любая максимальная примитивная разрешимая подгруппа группы $GL(q, \Delta)$ сопряжена в $GL(q, \Delta)$ с одной из следующих $k = k(q)$ групп*:

$$G_{q_1}, \ \ldots, \ G_{q_k}. \tag{2}$$

Каждая из групп (2) *обладает нормальным делителем $A = (a)(b)\Delta^*$, где $a = \operatorname{diag}[1, \eta, \ldots, \eta^{q-1}]$, $\eta \in \Delta$, $\eta^q = 1$, $\eta \neq 1$, $b = \begin{bmatrix} 0 & 1 \\ E_{q-1} & 0 \end{bmatrix}$.*

Если $q=2$ или $q=3$, то $k = 1$, $G = G_{q_1}$ есть нормализатор A в $GL(q, \Delta)$, $G = \psi^{-1}(SL(2, q))$, $G/A \cong SL(2, q)$. Если $q = 5$, то $k = 2$, $G_{q_1} = \psi^{-1}(U_2)$, $G_{q_2} = \psi^{-1}(U_3)$, $G_{q_1} : A = 12$, $G_{q_2} : A = 24$. Если $q > 5$, $q \equiv \pm 3 \pmod 8$, то $k = 3$, $G_{q_j} = \psi^{-1}(U_j)$, $j = 1, 2, 3$, $G_{q_1} : A = 2(q-1)$, $G_{q_2} : A = 2(q+1)$, $G_{q_3} : A = 24$. Если $q > 5$, $q \equiv \pm 1 \pmod 8$, то $k = 4$, $G_{q_j} = \psi^{-1}(U_j)$, $j = 1, 2, 3, 4$, $G_{q_1} : A = 2(q-1)$, $G_{q_2} : A = 2(q+1)$, $G_{q_3} : A = G_{q_4} : A = 48$.

Пример. В $GL(2, \Delta)$, где $q \neq \operatorname{char}\Delta$, имеется точно три несопряженные максимальные разрешимые подгруппы:

1) Группа $G^{(1)}$ всех матриц вида

$$\begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix}, \quad \alpha, \gamma \in \Delta^*, \quad \beta \in \Delta.$$

2) Группа $G^{(2)}$ всех матриц вида

$$\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^t, \quad \lambda_1, \lambda_2 \in \Delta^*, \qquad t=0,\ 1.$$

3) Группа $G^{(3)}=\psi^{-1}(SL(2,\ 2))$. Матрицы

$$a=\operatorname{diag}[1,\ -1], \qquad b=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$g=\operatorname{diag}[1,\ -i], \qquad h=\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix},$$

где i — элемент четвертого порядка из Δ^*, вместе с Δ^*E составляют систему образующих группы $G^{(3)}$.

2. О приводимых группах. Пусть теперь Δ — произвольное поле, а M — некоторый класс неприводимых матричных групп над Δ не обязательно одной и той же степени. Будем рассматривать группы матриц степени n над Δ, образы неприводимых частей которых лежат в классе M. Пусть $G_1, \ldots, G_k$ — такие группы из класса M, что $n_1+n_2+\ldots+n_k=n$, n_j — степень G_j. Построим группу $G=T(G_1, \ldots, G_k)$, состоящую из всех матриц g вида

$$g=\begin{bmatrix} a_1 & a_{12} & \ldots & a_{1k} \\ 0 & a_2 & \ldots & a_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & a_k \end{bmatrix}, \tag{3}$$

где $a_j \in Q_j$, a_{ij} — произвольная $n_i \times n_j$-матрица над Δ. Класс всех групп вида $T(G_1, \ldots, G_k)$, где $G_j \in M$, $1 \leqslant k \leqslant n$, обозначим символом $\langle M, n\rangle$. Зафиксируем один и тот же для всех $G \in \langle M, n\rangle$ базис

$$u_1, \ldots, u_n \tag{4}$$

пространства Δ^n. Тогда каждую группу G из $\langle M, n\rangle$ можно трактовать как группу автоморфизмов пространства Δ^n с матрицами вида (3) в базисе (4) (числа k и n_j при переходе от одной группы из $\langle M, n\rangle$ к другой могут меняться).

Пусть $G=T(G_1, \ldots, G_k) \in \langle M, n\rangle$, n_j — степень G_j, $j=1,\ 2,\ \ldots,\ k$. Положим $m_1=n_1$, $m_j=m_{j-1}+n_j$,

$j = 2, \ldots, k$, и построим $k-1$ подпространств пространства Δ^n:

$$L_1, \ldots, L_{k-1}, \tag{5}$$

где L_j — подпространство размерности m_j с базисом

$$u_1, \ldots, u_{m_j}, \quad j = 1, 2, \ldots, k-1.$$

Лемма 1. *$L_1, \ldots, L_{k-1}$ суть единственные нетривиальные инвариантные относительно G подпространства пространства Δ^n.*

Доказательство. Очевидно, подпространства (5) инвариантны относительно G. Введем k подпространств $Q_1, \ldots, Q_k$ размерностей $n_1, \ldots, n_k$ с базисами $u_1, \ldots, u_{n_1}; \ldots; u_{m_{k-1}+1}, \ldots, u_n$. Пусть L — нетривиальное ($L \neq 0$, $L \neq \Delta^n$) инвариантное относительно G подпространство, а $v \in L$, $v \neq 0$. Тогда

$$v = q_1 + \ldots + q_t, \quad q_j \in Q_j, \quad q_t \neq 0, \quad t \leqslant k. \tag{6}$$

Так как G_t — неприводимая подгруппа группы $GL(n_t, \Delta)$, то $G_t(q_t)$ содержит линейно независимую систему, состоящую из n_t векторов. Следовательно, $G_t(q_t)$ вместе с вектором v содержит и векторы

$$v_1 + r_1, \quad v_2 + r_2, \quad \ldots, \quad v_{n_t} + r_{n_t}, \tag{7}$$

где $v_1, \ldots, v_{n_t} \in L_{t-1}$, $r_1, \ldots, r_{n_t}$ — базис подпространства Q_t. Очевидно, в G есть такие элементы $\sigma_1, \ldots, \sigma_{m_{t-1}}$, что $\sigma_1(r_1) = r_1 + l_1, \ldots, \sigma_{m_{t-1}}(r_1) = r_1 + l_{m_{t-1}}$, где $l_1, \ldots, l_{m_{t-1}}$ — базис L_{t-1}, а $\sigma_\nu(v_1) = v_1$, $\nu = 1, \ldots, m_{t-1}$. Следовательно, векторы

$$\sigma_1(r_1 + v_1) = r_1 + l_1 + v_1, \quad r_1 + l_2 + v_1, \quad \ldots, \quad r_1 + l_{m_{t-1}} + v_1$$

принадлежат L. Отсюда и из того, что векторы (7) принадлежат L, вытекает, что $l_1, \ldots, l_{m_{t-1}}$ тоже принадлежат L. Следовательно, $L_{t-1} \subset L$. Так как векторы (7) лежат в L, то из последнего включения вытекает $Q_t \subset L$. Следовательно,

$$L \supset L_{t-1} \dotplus Q_t = L_t. \tag{8}$$

Выберем теперь вектор v в L так, что число t в формуле (6) окажется максимальным. Тогда

$$L \subset L_{t-1} \dotplus Q_t = L_t.$$

Отсюда $L = L_t$. Так как $L \neq \Delta^n$, то $t < k$. ■

Пусть теперь класс M подчинен следующему условию:

(*) Если при каком-либо $m \leqslant n$ группа A класса $\langle M, m\rangle$ сопряжена в $GL(m, \Delta)$ с подгруппой группы $B \in M$, то $A = B$.

Теорема 3. *Пусть $G = T(G_1, \ldots, G_k)$ и $H = T(H_1, \ldots, H_j)$ — группы из класса $\langle M, n\rangle$, где M — класс неприводимых матричных групп над Δ, подчиненный условию* (*). *Если $d^{-1}Gd \subset H$ при $d \in GL(n, \Delta)$, то $G = H$.*

Доказательство. Пусть $d^{-1}Gd \subset H$, (5) — нетривиальные подпространства, инвариантные относительно G, а $U_1 \subset \ldots \subset U_{j-1}$ — нетривиальные подпространства, инвариантные относительно H. Тогда $d(U_1), \ldots, d(U_{j-1})$ инвариантны относительно dHd^{-1}. Так как $G \subset dHd^{-1}$, то, в силу леммы 1, $d(U_1) = L_{i_1}, \ldots$ $\ldots, d(U_{j-1}) = L_{i_{j-1}}$, где $1 \leqslant i_1 < i_2 < \ldots < i_{j-1} \leqslant k$. Следовательно, $U_\nu : \Delta = L_{i_\nu} : \Delta$, $\nu = 1, \ldots, j-1$. Отсюда и из способа построения подпространств L_ν и U_ν вытекает

$$U_\nu = L_{i_\nu}, \quad d(U_\nu) = U_\nu, \qquad \nu = 1, \ldots, j-1.$$

Следовательно, в базисе (4) матрица d имеет вид

$$d = \begin{bmatrix} d_1 & d_{12} & \ldots & d_{1j} \\ 0 & d_2 & \ldots & d_{2j} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & d_j \end{bmatrix}.$$

Отсюда и из включения $d^{-1}Gd \subset H$ вытекают j включений вида

$$d_1^{-1}T(G_1, \ldots, G_{t_1})d_1 \subset H_1; \ldots$$
$$\ldots; d_j^{-1}T(G_{k-t_j+1}, \ldots, G_k)d_j \subset H_j,$$

где $t_1+t_2+\ldots+t_j=k$. Отсюда, в силу условия (*), находим

$$H_1=T\left(G_1, \ldots, G_{t_1}\right), \ldots, H_j=T\left(G_{k-t_j+1}, \ldots, G_k\right).$$

Так как группы H_ν неприводимы, то $j=k$, $H_1=G_1, \ldots$ $\ldots, H_k=G_k$, $H=G$. ■

3. **О приводимых разрешимых группах.** Напомним, что неприводимая разрешимая группа степени n обладает абелевым нормальным делителем, индекс которого не превышает некоторого числа $\rho(n)$, зависящего только от n.

Лемма 2. *Пусть $G_1, \ldots, G_k$ — неприводимые разрешимые группы матриц над полем Δ, $n_1, \ldots, n_k$ — их степени, $k>1$, $n_1+\ldots+n_k=n$, а поле Δ содержит по меньшей мере $\rho(n)+1$ элементов. Тогда $G=$ $=T(G_1, \ldots, G_k)$ не может содержаться в неприводимой разрешимой подгруппе группы $GL(n, \Delta)$.*

Доказательство. Пусть, вопреки утверждению леммы, $G \subset \Phi$, где Φ — неприводимая разрешимая подгруппа группы $GL(n, \Delta)$. Группа Φ обладает абелевым нормальным делителем F таким, что $\Phi: F \leqslant \rho(n)$. В группе F нет унипотентных элементов, ибо F — вполне приводимая абелева группа. Пусть H — группа всех матриц h вида

$$h=\left[\begin{array}{cccc} E_{n_1} & h_{12} & \ldots & h_{1k} \\ 0 & E_{n_2} & \ldots & h_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & E_{n_k} \end{array}\right],$$

где $h_{\mu\nu}$ — произвольная $n_\mu \times n_\nu$-матрица над Δ. Очевидно, что $H \subset G \subset \Phi$ и $F \cap H=1$. Ясно также, что H содержит по меньшей мере $\rho(n)+1$ элементов. С другой стороны, $H \cong H/F \cap H \cong HF/F$ и $HF:F \leqslant \rho(n)$ и, следовательно, $\operatorname{card} H \leqslant \rho(n)$. Это противоречие и доказывает лемму. ■

Теорема 4. *Пусть в поле Δ имеется по меньшей мере $\rho(n)+1$ элементов, а M — класс матричных групп над Δ, обладающий следующими свойствами:*

(i) *для любого $m \leqslant n$ всякая максимальная неприводимая разрешимая подгруппа $GL(m, \Delta)$ сопряжена* *в $GL(m, \Delta)$ с одной и только одной группой из класса M;*

(ii) *каждая группа из класса M степени m максимальна среди разрешимых неприводимых подгрупп группы $GL(m, \Delta)$.*

Тогда каждая группа класса $\langle M, n\rangle$ есть максимальная разрешимая подгруппа группы $GL(n, \Delta)$, каждая максимальная разрешимая подгруппа группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с одной и только одной группой класса $\langle M, n\rangle$.

Доказательство. Очевидно, любая максимальная разрешимая подгруппа группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с некоторой группой из $\langle M, n\rangle$. Из леммы 2 и из (i) следует, что класс M подчинен условию $(*)$ п. 2. Следовательно, в силу теоремы 3, каждая группа из $\langle M, n\rangle$ максимальна среди разрешимых подгрупп группы $GL(n, \Delta)$. Из теоремы 3 также следует, что две различные группы из $\langle M, n\rangle$ не сопряжены в $GL(n, \Delta)$. ■

В частности, из теоремы 4 следует, что если в поле Δ имеется по меньшей мере $\rho(n)+1$ элементов, то группа всех невырожденных треугольных матриц степени n над Δ есть максимальная разрешимая подгруппа группы $GL(n, \Delta)$. Впрочем, справедлив более точный результат.

Группа всех невырожденных треугольных матриц степени n над полем Δ почти всегда максимальна среди разрешимых подгрупп группы $GL(n, \Delta)$. Исключение составляет лишь случай, когда $\Delta = GF(2)$, либо $\Delta = GF(3)$ (Супруненко [23]).

Теорема 5. *Пусть Δ — произвольное поле, а G — разрешимая d-группа матриц над Δ. Тогда группа G вполне приводима.*

Доказательство. Будучи разрешимой группой, G обладает нормальным делителем H конечного индекса таким, что для любой его неприводимой части γ группа $\mathrm{Im}\,\gamma$ абелева. В силу леммы 17.3 группа H абелева. Отсюда и из теоремы 17.3 следует полная приводимость группы G. ■

Группу матриц над полем Δ будем называть *немодулярной*, если либо $\mathrm{char}\,\Delta = 0$, либо $\mathrm{char}\,\Delta = p$, где p — простое число, но в G нет нормальных делителей конечного индекса $j \equiv 0 \pmod p$.

Теорема 6. *Пусть Δ — совершенное поле. Тогда всякая вполне приводимая разрешимая немодулярная группа G матриц над Δ есть d-группа. В частности, разрешимая вполне приводимая группа матриц над полем нулевой характеристики есть d-группа.*

Доказательство. Группа G обладает вполне приводимым абелевым нормальным делителем F конечного индекса. Любая матрица из F полупроста. Так как поле Δ совершенно, то F является d-группой. В силу леммы 17.5 G — тоже d-группа. ■

4. О разрешимых целочисленных матричных группах. Пусть Δ — евклидово кольцо, а Ω — поле отношений кольца Δ. Группу $GL(n, \Delta)$ будем трактовать как группу автоморфизмов n-мерного свободного модуля M над Δ, а $GL(n, \Omega)$ — как группу автоморфизмов n-мерного линейного пространства $V \supset M$ над Ω. Очевидно, что $GL(n, \Delta) \subset GL(n, \Omega)$.

Лемма 3. *Пусть G — подгруппа $GL(n, \Delta)$, а M_1 — подмодуль M, инвариантный относительно G. Тогда в модуле M есть прямое слагаемое M_2, инвариантное относительно G, той же размерности над Δ, что и M_1.*

Доказательство. В силу известных свойств модуля над евклидовым кольцом в M_1 есть такой базис $b_1, \ldots, b_m$, что $b_j = a_j\delta_j$, $j = 1, \ldots, m$, где $\delta_j \in \Delta$, $\delta_j \neq 0$, $a_1, \ldots, a_n$ — некоторый базис модуля M. По условию для $g \in G$ можно написать

$$g(b_j) = b_1\lambda_1 + \ldots + b_m\lambda_m, \qquad \lambda_i \in \Delta. \tag{9}$$

С другой стороны,

$$g(a_j) = a_1\gamma_1 + \ldots + a_n\gamma_n, \qquad \gamma_\nu \in \Delta. \tag{10}$$

Следовательно,

$$g(b_j) = g(a_j)\,\delta_j = (a_1\gamma_1 + \ldots + a_n\gamma_n)\,\delta_j. \tag{11}$$

Сравнивая (9) и (11), находим, что в (10) $\gamma_\nu = 0$, если $j \leqslant m$, а $\nu > m$. Следовательно, подмодуль M_2 с базисом $a_1, \ldots, a_m$ есть прямое слагаемое модуля M, инвариантное относительно G. ■

Лемма 4. *Пусть G — подгруппа $GL(n, \Delta)$, а пространство V обладает инвариантным относительно G подпространством P. Тогда модуль M обладает прямым слагаемым M_2 той же размерности, что и P, инвариантным относительно G.*

Доказательство. Положим $M_1 = M \cap P$. Очевидно, что M_1 — инвариантный относительно G подмодуль модуля M и $M_1 : \Delta = P : \Omega$. Согласно лемме 3 в M есть прямое слагаемое M_2, инвариантное относительно G, размерности $M_1 : \Delta$. ■

Из леммы 4 следует

Лемма 5. *Пусть G — подгруппа группы $GL(n, \Delta)$. Тогда Δ-модуль M обладает таким базисом, что матрицы g из G одновременно принимают вид*

$$g = \begin{bmatrix} a_1(g) & a_{12}(g) & \dots & a_{1k}(g) \\ 0 & a_2(g) & \dots & a_{2k}(g) \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_k(g) \end{bmatrix}, \tag{12}$$

где $a_j(g)$, $a_{ij}(g)$ — матрицы над Δ, причем $a_j(g)$ пробегает неприводимую подгруппу G_j группы $GL(n_j, \Omega)$, когда g пробегает G, $j = 1, \dots, k$; $n_1 + n_2 + \dots + n_k = n$.

Группа называется *полициклической*, если она обладает нормальным рядом, все факторы которого цикличны.

Пусть теперь Z — кольцо целых рациональных чисел, а Q — поле рациональных чисел.

Лемма 6. *Пусть матрицы g группы G имеют вид* (12), *где $\Delta = Z$, $\Omega = Q$, а все группы G_j абелевы, $j = 1, \dots, k$. Тогда G — полициклическая группа.*

Доказательство. Пусть сперва $k = 1$. Тогда G — неприводимая абелева подгруппа группы $GL(n, Q)$, а линейная Q-оболочка $[G] = \Sigma$ является расширением степени n поля Q. Пусть K — кольцо всех целых алгебраических чисел поля Σ. Так как $G \subset GL(n, Z)$, то G — подгруппа K^*. По теореме Дирихле K^* — группа с конечным числом образующих, следовательно, K^* и G — полициклические группы. Теперь легко доказать лемму индукцией по числу k. Пусть $k > 1$ и для групп с меньшим числом неприводимых частей лемма верна.

Рассмотрим гомоморфизмы

$$g \overset{h_1}{\longmapsto} \begin{bmatrix} a_1(g) & 0 & \ldots & 0 \\ 0 & a_2(g) & \ldots & a_{2k}(g) \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & a_k(g) \end{bmatrix} \overset{h_2}{\longmapsto}$$

$$\overset{h_2}{\longmapsto} \begin{bmatrix} a_2(g) & a_{23}(g) & \ldots & a_{2k}(g) \\ 0 & a_3(g) & \ldots & a_{3k}(g) \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & a_k(g) \end{bmatrix}. \quad (13)$$

По индуктивному предположению группа $\operatorname{Im} h_2$ полициклична. Группа $\operatorname{Ker} h_2$ изоморфна подгруппе группы G_1. Следовательно, $\operatorname{Ker} h_2$ — тоже полициклическая группа. Так как $\operatorname{Im} h_1/\operatorname{Ker} h_2 \cong \operatorname{Im} h_2$, то и группа $\operatorname{Im} h_1$ полициклична. Далее, матрицы из $\operatorname{Ker} h_1$ имеют вид

$$\begin{bmatrix} E_{n_1} & a_{12} \ldots a_{1k} \\ 0 & E_{n-n_1} \end{bmatrix}.$$

Следовательно, $\operatorname{Ker} h_1$ — абелева группа с конечным числом образующих, значит, группа $\operatorname{Ker} h_1$ полициклична. Так как $G/\operatorname{Ker} h_1 \cong \operatorname{Im} h_1$, то и группа G полициклична. ■

Теорема 7 (Мальцев [3]). *Разрешимая подгруппа группы $GL(n, Z)$ полициклична.*

Доказательство. Пусть U — разрешимая подгруппа группы $GL(n, Z)$. Будучи разрешимой, U обладает таким нормальным делителем G конечного индекса, что образ любой неприводимой части группы G коммутативен (неприводимость над Q).

В силу леммы 5 существует такой базис свободного Z-модуля, где действует U, что матрицы g нормального делителя G имеют вид (12), где группы G_j абелевы. Согласно лемме 6 группа G полициклична. U/G — конечная разрешимая группа, следовательно U/G — тоже полициклическая группа. Отсюда вытекает и полицикличность группы U. ■

Как доказали Ауслендер [1] и Суон [1], всякая полициклическая группа изоморфно вложима в $GL(n, Z)$. Мерзляков [3] показал, что голоморф полициклической группы тоже допускает точное целочисленное представление.

Заканчивая главу, приведем еще несколько результатов без доказательств.

Группа матриц над произвольным полем тогда и только тогда удовлетворяет нетривиальному тождеству, когда она является конечным расширением разрешимой группы (Платонов [13]). Разрешимые подгруппы мультипликативной группы T^* тела конечного ранга n над своим центром Δ изучались в статье Супруненко [17]. Подгруппа G группы T^* называется *неприводимой*, если ее линейная Δ-оболочка совпадает с телом T. Максимальная разрешимая неприводимая подгруппа G группы T^* обладает единственным максимальным абелевым нормальным делителем F, являющимся мультипликативной группой некоторого коммутативного подтела $\Sigma \supset \Delta$ тела T; Σ — нормальное сепарабельное расширение поля Δ с разрешимой группой Галуа $\mathcal{G}(\Sigma/\Delta)$.

Возможны два случая: 1) $\Sigma : \Delta = \sqrt{n}$, 2) $\Sigma : \Delta < \sqrt{n}$. В первом случае $G/F \cong \mathcal{G}(\Sigma/\Delta)$. Во втором — инвариантный ряд (α) (см. § 20, п. 2)

$$G \supset V \supset A \supset F \supset (e)$$

группы G обладает свойствами:

а) A/F — абелева группа порядка $(T : \Delta)(\Sigma : \Delta)^{-2}$, подгруппы Силова которой элементарны;

б) V/A изоморфна некоторой разрешимой подгруппе группы $\mathrm{Aut}(A/F)$;

в) $V/F \cong \mathcal{G}(\Sigma/\Delta)$.

Пусть, в частности, T — тело вещественных кватернионов с базисом $1, i, j, k$ над полем вещественных чисел R. Тогда всякая максимальная разрешимая подгруппа группы T^* сопряжена в T^* с одной из двух подгрупп G_1 и G_2, где G_1 порождается элементами $i, j, 1+i, 1+k$ и группой R^*, а $G_2 = (j)C^*$, $C = R(i)$.

О максимальных разрешимых подгруппах группы $GL(n, T)$, где T — тело конечного ранга над своим центром, см. статью Залесского [2].

Пусть $\mathfrak{G}$ — алгебраическая алгебра над полем Δ, а G — локально разрешимая подгруппа группы $\mathfrak{G}^*$. Тогда наименьшая подалгебра алгебры $\mathfrak{G}$, содержащая G, локально конечномерна. (Залесский [1]).

ГЛАВА VI

ПЕРИОДИЧЕСКИЕ ЛИНЕЙНЫЕ ГРУППЫ

§ 23. Условия конечности линейной группы. Локальная конечность группы матриц над полем

1. След матрицы. Пусть Δ — произвольное поле. Рассмотрим отображение

$$\mathrm{tr}\colon\ \Delta_n \to \Delta, \qquad a = \| \alpha_{ij} \| \mapsto \sum_{\nu=1}^{n} \alpha_{\nu\nu}. \tag{1}$$

Элемент $\mathrm{tr}\, a \in \Delta$ называется *следом матрицы* a.

Как видно из (1), *отображение* tr *линейно*, т. е. *для* $a,\ b \in \Delta_n,\ \lambda,\ \mu \in \Delta$

$$\mathrm{tr}\,(\lambda a + \mu b) = \lambda\, \mathrm{tr}\,(a) + \mu\, \mathrm{tr}\,(b).$$

Очевидно, что

$$\mathrm{tr}\,(ab) = \mathrm{tr}\,(ba),$$

следовательно, для $c \in GL\,(n,\ \Delta)$

$$\mathrm{tr}\,(cbc^{-1}) = \mathrm{tr}\, b.$$

Заметим, в частности, что *в n^2-мерном унитарном пространстве матриц C_n со скалярным умножением*

$$(a,\ b) = \sum_{i,\ j=1}^{n} \alpha_{ij}\bar{\beta}_{ij}, \qquad a = \| \alpha_{ij} \|, \qquad b = \| \beta_{ij} \|$$

имеет место равенство

$$(a,\ b) = \mathrm{tr}\,(ab^*), \tag{2}$$

где $b^* = \| \beta^*_{ij} \|,\ \beta^*_{ij} = \bar{\beta}_{ij}$.

Если u — унитарная матрица,

$$a_1 = uau^{-1}, \qquad b_1 = ubu^{-1},$$

то, в силу формулы (2),

$$(a_1, b_1) = (a, b).$$

2. Критерий Бернсайда конечности линейной группы.

Лемма 1 (Бернсайд [2]). *Пусть Δ — произвольное поле, $\mathfrak{G}$ — абсолютно неприводимая подгруппа группы $GL(n, \Delta)$, а $\operatorname{tr}(\mathfrak{G})$ — конечное множество мощности m. Тогда $\mathfrak{G}$ — конечная группа,*

$$\operatorname{card} \mathfrak{G} \leqslant m^{n^2}. \tag{3}$$

Доказательство. Группа $\mathfrak{G}$ абсолютно неприводима, поэтому в ней есть n^2 линейно независимых матриц (следствие 14.4.2)

$$a_\nu = \|\alpha_{ij}^\nu\|, \qquad \alpha_{ij}^\nu \in \Delta, \qquad \nu = 1, 2, \ldots, n^2. \tag{4}$$

Для $x = \|x_{ij}\| \in \mathfrak{G}$ имеем

$$\operatorname{tr}(a_\nu x) = \sum_{i, j=1}^{n} \alpha_{ij}^\nu x_{ji} = \tau_\nu \in \operatorname{tr}(\mathfrak{G}). \tag{5}$$

Так как матрицы (4) линейно независимы, то при фиксированных $\tau_1, \ldots, \tau_{n^2}$ система (5) имеет единственное решение $x = \|x_{ij}\|$. Следовательно, верно неравенство (3). ■

Из леммы 1 следует

Лемма 2. *Если порядки всех элементов абсолютно неприводимой подгруппы $\mathfrak{G}$ группы $GL(n, \Delta)$ ограничены некоторым числом μ, то $\mathfrak{G}$ — конечная группа, порядок которой меньше некоторого числа $\nu(\mu, n)$, зависящего лишь от μ и n.*

Доказательство. Корни характеристических полиномов матриц из группы $\mathfrak{G}$ суть корни некоторой фиксированной, зависящей от числа μ, степени из единицы. Поэтому $\operatorname{tr}\mathfrak{G}$ — конечное множество, число элементов которого ограничено числом, зависящим от n и μ. ■

Теорема 1. (Критерий Бернсайда конечности линейной группы.) ***Если $\mathfrak{G}$ — подгруппа группы $GL(n, \Delta)$ над произвольным полем Δ, порядки элементов которой*** *не делятся на* $\operatorname{char}\Delta$ *и ограничены некоторым числом* μ, *то* $\mathfrak{G}$ — *конечная группа, порядок которой меньше некоторого числа* $N(\mu, n)$, *зависящего лишь от* n *и* μ.

Доказательство. Пусть Ω — алгебраически замкнутое расширение поля Δ. Будем трактовать группу $\mathfrak{G}$ как подгруппу группы $GL(n, \Omega)$. В подходящем базисе пространства V над полем Ω матрицы группы $\mathfrak{G}$ имеют вид

$$g = \begin{bmatrix} a_1(g) & a_{12}(g) & \ldots & a_{1k}(g) \\ 0 & a_2(g) & \ldots & a_{2k}(g) \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & a_k(g) \end{bmatrix} = \begin{bmatrix} a_1(g) & * \\ 0 & A_2(g) \end{bmatrix}, \tag{6}$$

где $\gamma_\nu\colon g \mapsto a_\nu(g)$, $\nu = 1, \ldots, k$, — неприводимые представления группы $\mathfrak{G}$. Введем гомоморфизм

$$\gamma\colon \mathfrak{G} \to \overline{\mathfrak{G}}, \quad g \mapsto \operatorname{diag}[a_1(g), \ldots, a_k(g)] \tag{7}$$

и рассмотрим $\operatorname{Ker}\gamma$. Если отличная от E_n матрица имеет специальную треугольную форму, то порядок ее либо бесконечен, либо равен p^α, где $p = \operatorname{char}\Delta$. Поэтому $\operatorname{Ker}\gamma = (E_n)$, γ — изоморфизм. Отсюда и из леммы 2 вытекает критерий. ∎

Простым обобщением критерия Бернсайда является следующая

Теорема 2. *Пусть* Δ — *произвольное поле,* Γ — *подгруппа группы* $GL(n, \Delta)$, *и пусть есть такое натуральное число* k, *что* $\operatorname{char}\Delta \nmid k$ *и для всякого элемента* a *группы* Γ $a^k \in \Delta^* E_n$. *Тогда порядок фактор-группы* $\Gamma/\Gamma \cap \Delta^* E_n$ *не превышает некоторого числа* $\mu(k, n)$, *зависящего лишь от* k *и* n.

Доказательство. Будем трактовать группу Γ как подгруппу группы $GL(n, \Omega)$, где Ω — алгебраически замкнутое расширение поля Δ.

$$\Omega^* E_n \cap \Gamma = \Delta^* E_n \cap \Gamma. \tag{8}$$

Пусть теперь $G = \Gamma\Omega^* E_n$, H — ядро гомоморфизма $\det\colon G \to \Omega^*$. Так как поле Ω алгебраически замкнуто, то для любого элемента g группы G в группе Ω^* есть такое ρ, что $\rho^{-1} g \in H$. Следовательно, $G = H\Omega^* E_n$. Если $h \in H$, то

$$h^k = \lambda E_n, \quad \lambda \in \Omega^*, \quad \lambda^n = 1.$$

Положим

$$\nu = n, \quad \text{если} \quad \operatorname{char}\Delta = 0,$$

$$\nu = np^{-\alpha}, \quad (\nu, p) = 1, \quad \text{если} \quad \operatorname{char}\Delta = p > 0,$$

Тогда $h^{k\nu} = E_n$. Согласно критерию Бернсайда $\operatorname{card} H < N(k\nu, n)$. Далее,

$$G/\Omega^*E_n = H\Omega^*E_n/\Omega^*E_n \cong H/H \cap \Omega^*E_n.$$

Следовательно,

$$G : \Omega^*E_n \leqslant nN(k\nu, n) = \mu(k, n).$$

Так как

$$\Gamma/\Gamma \cap \Omega^*E_n \cong \Gamma\Omega^*E_n/\Omega^*E_n = G/\Omega^*E_n,$$

то, в силу (8),

$$\Gamma : (\Gamma \cap \Delta^*E_n) \leqslant \mu(k, n). \blacksquare$$

Теорема 2а. *Пусть Δ — произвольное поле, Γ — неприводимая подгруппа группы $GL(n, \Delta)$, пусть, далее, существует такое натуральное число k, что* $\operatorname{char}\Delta \nmid k$ *и для любого элемента a группы Γ элемент a^k принадлежит ее центру Z. Тогда*

$$\Gamma : Z \leqslant \mu(k, n). \tag{9}$$

Доказательство. Так как группа Γ неприводима, то $Z \subset \Sigma^*$, где $\Sigma = [Z]_\Delta$ — расширение поля Δ, $\Sigma : \Delta = m$, $m|n$. Следовательно, группу Γ можно трактовать как подгруппу в $GL(r, \Sigma)$, $r = nm^{-1}$. Согласно теореме 1

$$\Gamma : (\Gamma \cap \Sigma^*E_r) \leqslant \mu(k, r) \leqslant \mu(k, n).$$

Очевидно, $\Gamma \cap \Sigma^*E_r = Z$, значит, верно (9). $\blacksquare$

Теорема 3. (Второй критерий Бернсайда.) *Пусть Δ — произвольное поле, а $\mathfrak{G}$ — подгруппа группы $GL(n, \Delta)$, имеющая лишь конечное число классов сопряженных элементов. Тогда группа $\mathfrak{G}$ конечна.*

Доказательство. Будем трактовать группу $\mathfrak{G}$ как подгруппу в $GL(n, \Omega)$, где Ω — алгебраически замкнутое расширение поля Δ, и запишем матрицы $g \in \mathfrak{G}$ в виде (6). Число классов сопряженных элементов группы $\gamma_\nu(\mathfrak{G}) = \mathfrak{G}_\nu$ конечно, следовательно, множество $\operatorname{tr}(\mathfrak{G}_\nu)$ также конечно и $\mathfrak{G}_\nu$ — конечная группа. Далее воспользуемся индукцией по числу k неприводимых частей группы $\mathfrak{G}$. При $k=1$ критерий уже доказан, будем считать его верным для групп с $k-1$ неприводимыми частями, $k>1$. Рассмотрим представление

$$\varphi(g)=\operatorname{diag}[a_1(g),\ A_2(g)],$$

где $g\in\mathfrak{G}$ — матрицы вида (6). По индуктивному предположению $A_2(g)$ пробегает конечную группу, когда g пробегает группу $\mathfrak{G}$, следовательно, $\varphi(\mathfrak{G})$ — конечная группа. $\operatorname{Ker}\varphi=\mathfrak{N}$ состоит из матриц вида

$$\begin{bmatrix} E_s & b \\ 0 & E_t \end{bmatrix}.$$

Таким образом, $\mathfrak{N}$ — абелев нормальный делитель группы $\mathfrak{G}$ конечного индекса. Легко видеть, что и $\mathfrak{N}$ — конечная группа. В самом деле, пусть n пробегает группу $\mathfrak{N}$, а $\bar{n}$ — класс сопряженных с n элементов группы $\mathfrak{G}$. Так как группа $\mathfrak{N}$ содержится в централизаторе элемента n в $\mathfrak{G}$, то класс $\bar{n}$ конечен. Множество всех $\bar{n}$ также конечно, следовательно, $\mathfrak{N}$ и, значит, $\mathfrak{G}$ — конечные группы. ■

В связи с доказанной выше теоремой 3 отметим для сравнения еще одно утверждение.

Теорема 4. *Подгруппа* Γ *группы* $GL(n,\Delta)$ *над произвольным полем* Δ, *каждый класс сопряженных элементов которой конечен, имеет центр конечного индекса.*

Доказательство. Пусть $g_1, g_2, \ldots, g_m$ — максимальная система линейно независимых над Δ элементов группы Γ, а Z_j — централизатор элемента g_j в Γ. Тогда $m\leqslant n^2$, а $\Gamma:Z_j=r_j$. Центр Z группы Γ есть пересечение всех Z_j. Следовательно, $\Gamma:Z\leqslant r_1r_2\ldots r_m$. ■

Очевидно, обратное утверждение также справедливо.

3. Первая теорема Шура.

Лемма 3. *Пусть* Π — *простое подполе поля* Δ, Φ — *поле всех алгебраических над* Π *элементов из* $K=\Pi(\theta_1,\ldots,\theta_l)$, *где* $\theta_1,\ldots,\theta_l\in\Delta$. *Тогда степень* $\Phi:\Pi$ *конечна.*

Доказательство. Если каждое θ_i — алгебраический элемент относительно поля Π, то лемма очевидна. Пусть среди θ_i есть трансцендентные над полем

Π элементы и $\Sigma = \Pi(\theta_1, \ldots, \theta_r)$ — такое чисто трансцендентное расширение поля Δ, что θ_j при $j > r$ алгебраично над Σ. Тогда, очевидно, $K : \Sigma = m < \infty$. Следовательно, для любой системы

$$\alpha_1, \ldots, \alpha_{m+1} \tag{10}$$

$m+1$ элементов поля K выполняется соотношение вида

$$\sigma_1\alpha_1 + \ldots + \sigma_{m+1}\alpha_{m+1} = 0, \tag{11}$$

где σ_ν, $\nu = 1, \ldots, m+1$, — полином от

$$\theta_1, \ldots, \theta_r \tag{12}$$

с коэффициентами из поля Π, причем не все σ_ν равны нулю. Левую часть равенства (11) представим как полином от (12), коэффициенты k_ρ которого имеют вид

$$k_\rho = a_1^\rho\alpha_1 + \ldots + a_{m+1}^\rho\alpha_{m+1}, \qquad a_j^\rho \in \Pi.$$

Если теперь (10) — элементы поля Φ, то элементы (12) алгебраически независимы над $\Pi(\alpha_1, \ldots, \alpha_n)$, так как они алгебраически независимы над Π. Следовательно, все коэффициенты k_ρ — нули. Но a_j^ρ не все равны нулю, ибо среди σ_ν есть отличные от нуля. Следовательно, элементы (10) линейно зависимы над Π, т. е. $\Phi : \Pi \leqslant m$. ■

В обозначениях леммы 3 справедлива

Лемма 4. *В группе Δ^* имеется лишь конечное множество элементов конечного порядка, являющихся корнями полиномов из $K[x]$ заданной степени n.*

Доказательство. Пусть элемент ε группы Δ^* имеет порядок μ и является корнем неприводимого в $K[x]$ полинома $f(x)$, степень которого не выше n. Тогда $f(x) \in \Phi[x]$ и, в силу леммы 3, $\Pi(\varepsilon) : \Pi \leqslant mn$. С другой стороны, если $\operatorname{char}\Pi = 0$, то $\Pi(\varepsilon) : \Pi = \varphi(\mu)$, где φ — функция Эйлера. Поэтому

$$\varphi(\mu) \leqslant mn. \tag{13}$$

Существует, очевидно, лишь конечное множество чисел μ, удовлетворяющих условию (13). Если же $\operatorname{char}\Pi = p > 0$, то $\mu \leqslant p^{mn} - 1$. ■

Лемма 5. *Пусть $\mathfrak{G}$ — абсолютно неприводимая подгруппа группы $GL(n, \Delta)$ над произвольным полем Δ. Если все корни характеристического полинома каждой матрицы из $\mathfrak{G}$ суть корни из единицы, то группа $\mathfrak{G}$ локально конечна.*

Доказательство. Пусть подгруппа $\mathfrak{H}_1$ группы $\mathfrak{G}$ порождается конечным множеством матриц M_1. Очевидно, M_1 содержится в конечном абсолютно неприводимом множестве M. Множество M порождает абсолютно неприводимую подгруппу $\mathfrak{H}$ группы $\mathfrak{G}$. Докажем, что группа $\mathfrak{H}$ конечна. Обозначим буквой K поле, получающееся присоединением к простому подполю Π поля Δ элементов всех матриц из M. Группа $\mathfrak{H}$ — подгруппа группы $GL(n, K)$. Корни характеристических полиномов матриц из $\mathfrak{H}$ суть элементы конечного порядка, являющиеся корнями полиномов над K степени n. В силу леммы 4 множество корней характеристических полиномов матриц из $\mathfrak{H}$ конечно. Тогда $\operatorname{tr}(\mathfrak{H})$ — конечное множество и, в силу леммы 1, $\mathfrak{H}$ — конечная группа. ■

Теорема 5. (Первая теорема Шура.) *Периодическая подгруппа группы $GL(n, \Delta)$ над произвольным полем Δ локально конечна.*

Доказательство. Пусть $\mathfrak{G}$ — периодическая подгруппа группы $GL(n, \Delta)$. Будем рассматривать ее как подгруппу группы $GL(n, \Omega)$, где Ω — алгебраически замкнутое расширение поля Δ. Пусть, далее, $\mathfrak{H}$ — конечно порожденная подгруппа группы $\mathfrak{G}$. Очевидно, любой ее гомоморфный образ также имеет конечную систему образующих. В частности, $\gamma(\mathfrak{H})$, где γ — гомоморфизм (7), введенный в доказательстве первого критерия конечности, — конечно порожденная группа. Тогда, в силу леммы 5, $\gamma(\mathfrak{H})$ — конечная группа. Если $\operatorname{char} \Delta = 0$, то $\operatorname{Ker} \gamma = (E_n)$ и $\mathfrak{H}$ — конечная группа. Если же $\operatorname{char} \Delta = p > 0$, то $\operatorname{Ker} \gamma$ — нильпотентная p-группа. Нильпотентная p-группа локально конечна (см. Курош [1], стр. 401). $\mathfrak{H}$ — конечное расширение локально конечной группы, т. е. тоже локально конечная группа. Но группа $\mathfrak{H}$ конечно порожденная и, значит, конечна. ■

Для периодической группы G символом $\Pi(G)$ мы обозначили множество всех простых делителей порядков ее элементов.

Из теоремы Шура и следствия 17.1.1 вытекает

Теорема 6. *Пусть G — периодическая подгруппа группы $GL(n, \Delta)$. Если* $\mathrm{char}\,\Delta \notin \Pi(G)$, *то группа G вполне приводима.*

Теорема о локальной конечности сохраняется и для периодических групп, обладающих полной (достаточной) системой линейных представлений ограниченных степеней (Платонов [1]).

В связи с теоремой Шура приведем без доказательства для сравнения один результат Сельберга [1].

Пусть $\mathrm{char}\,\Delta = 0$. *Тогда конечно порожденная подгруппа группы $GL(n, \Delta)$ имеет нормальный делитель без кручения конечного индекса.*

Известно, что теорема о локальной конечности не переносится на произвольные периодические группы. Новиков и Адян [1] установили существование бесконечной группы, порядки элементов которой ограничены, с конечным числом образующих. Голод [1] построил бесконечную p-группу $\mathfrak{G}$ с конечным числом образующих. Порядки элементов группы $\mathfrak{G}$ не ограничены. Она финитно аппроксимируема и потому обладает достаточной системой линейных представлений (степени представлений не ограничены).

Вопрос о локальной конечности периодической группы полностью решается следующей теоремой Процесси [1]:

Периодическая группа тогда и только тогда локально конечна, когда она изоморфна подгруппе мультипликативной группы некоторого кольца R, локально удовлетворяющего полиномиальному тождеству (каждое конечно порожденное подкольцо кольца R удовлетворяет некоторому полиномиальному тождеству).

4. Свойства линейной группы, связанные со свойствами характеристических полиномов ее матриц. Пусть Δ — произвольное поле, а Γ — подгруппа группы $GL(n, \Delta)$. Введем множество $F(\Gamma)$ всех различных характеристических полиномов матриц группы Γ.

Лемма 6. *Пусть поле Δ алгебраически замкнуто, $n > 1$, а множество $F(\Gamma)$ состоит из единственного полинома $(x-1)^n$. Тогда группа Γ приводима.*

Доказательство. Пусть, вопреки лемме, Γ неприводима. Так как для каждого $g \in \Gamma$ $\mathrm{tr}\, g = n$, то в силу леммы 1 порядок Γ равен 1, т. е. $\Gamma = (E_n)$. Последнее противоречит неприводимости Γ. ∎

При произвольном поле Δ верна

Теорема 7 (Супруненко [18]). *Пусть Γ — подгруппа группы $GL(n, \Delta)$, а $F(\Gamma)$ состоит из полиномов вида $(x-\lambda)^n$, где $\lambda \in \Delta$. Тогда в $GL(n, \Delta)$ есть такой элемент t, что матрицы группы $t^{-1}\Gamma t$ имеют вид*

$$\begin{bmatrix} \lambda & \lambda_{12} & \dots & \lambda_{1n} \\ 0 & \lambda & \dots & \lambda_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & \lambda \end{bmatrix}. \tag{14}$$

Доказательство. Сначала заметим, что теорему достаточно доказать для случая, когда поле Δ алгебраически замкнуто. Действительно, пусть в $GL(n, \Omega)$, где Ω — алгебраически замкнутое расширение поля Δ, есть такая матрица t_1, что матрицы группы $t_1^{-1}\Gamma t_1$ имеют вид (14). Тогда, очевидно, все матрицы $g - \lambda(g)E_n$, где $g \in \Gamma$, $\lambda(g)$ — единственное собственное значение матрицы g, принадлежат некоторой нильпотентной подалгебре A алгебры Δ_n, т. е.

$$\Gamma \subset \Delta^* E_n + A, \qquad A^n = 0. \tag{15}$$

Согласно теореме 13.6 в $GL(n, \Delta)$ есть такая матрица t, что матрицы $t^{-1}At$ имеют вид

$$\begin{bmatrix} 0 & \alpha_{12} & \dots & \alpha_{1n} \\ 0 & 0 & \dots & \alpha_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 \end{bmatrix}.$$

В силу (15) матрицы $t^{-1}\Gamma t$ имеют вид (14).

Будем теперь считать, что поле Δ алгебраически замкнуто. Положим $G = \Gamma\Delta^*$. Теорема будет доказана, если мы установим, что степень любой неприводимой части γ группы G равна 1. Пусть $H = \operatorname{Im}\gamma$, m — степень H, а H_0 — ядро гомоморфизма $\det\colon H \to \Delta^*$, $h \mapsto \det h$. Так как $G = \Gamma\Delta^*$, а поле Δ алгебраически замкнуто, то $H = H_0\Delta^*$. Характеристический полином матрицы h_0 из H_0 имеет вид $(x-\varepsilon)^m$, где $\varepsilon^m = \det h_0 = 1$. Следовательно, $\operatorname{tr} h_0$ принимает самое большое m

значений. Следовательно, по лемме 1, группа H_0 конечна. Возможны два случая: 1) $\operatorname{char}\Delta = 0$, 2) $\operatorname{char}\Delta = p > 0$. Так как для любой матрицы $h_0 \in H_0$ характеристический полином имеет вид $(x - \varepsilon)^m$, то из конечности H_0 следует скалярность каждой матрицы из H_0 и равенство $m = 1$. Пусть теперь $\operatorname{char}\Delta = p > 0$. Тогда запишем порядок группы H_0 в виде dp^τ, где $(d, p) = 1$. Если q — простой делитель числа d, то q-подгруппа Силова группы H_0 состоит из скалярных матриц, ибо характеристический полином матрицы h_0 из H_0 имеет вид $(x - \varepsilon)^m$, а $q \neq p$. Следовательно, $H_0 = DP$, где D — подгруппа скалярных матриц из H_0, а P есть p-подгруппа Силова группы H_0. Если $h_0 \in P$, то $\varepsilon = 1$ и характеристический полином матрицы h_0 равен $(x - 1)^m$. Следовательно, согласно лемме 6, P при $m > 1$ приводима. Так как H_0 неприводима, то последнее невозможно. Значит, $m = 1$. ∎

Следствие 1 (Мальцев [3], Колчин [1]). *Любая унипотентная подгруппа группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с некоторой подгруппой группы специальных треугольных матриц. Любые две максимальные унипотентные подгруппы группы $GL(n, \Delta)$ сопряжены в $GL(n, \Delta)$.*

Следствие 2. *Пусть Γ — подгруппа группы $GL(n, \Delta)$, а $F(\Gamma)$ состоит из полиномов вида $(x - \lambda)^n$, $\lambda \in \Delta$. Тогда группа Γ нильпотентна.*

Пусть теперь Δ — алгебраически замкнутое поле, Γ — подгруппа группы $GL(n, \Delta)$, $f \in F(\Gamma)$, $\lambda_1, \ldots, \lambda_r$ — попарно различные корни полинома f,

$$\Sigma_f = \{\lambda_1\lambda_1^{-1}, \lambda_2\lambda_1^{-1}, \ldots, \lambda_r\lambda_1^{-1}\}, \quad \Sigma = \bigcup \Sigma_f, \quad f \in F(\Gamma).$$

Обозначим символом $\Phi(\Gamma)$ подгруппу группы Δ^*, порожденную множеством Σ. Например, для группы Γ из теоремы 6 $\Phi(\Gamma) = (1)$. Ниже рассматриваются такие группы Γ, что $\Phi(\Gamma)$ — периодическая группа.

Лемма 7. *Пусть H — неприводимая подгруппа группы $GL(n, \Delta)$, а C — центр группы H. Если $\Phi(H)$ — периодическая группа, то:*

1) *фактор-группа H/C локально конечна, причем если* $\operatorname{char}\Delta = 0$, *то* $\Pi(H/C) = \Pi(\Phi(H))$, *если* $\operatorname{char}\Delta = p > 0$, *то* $\Pi(\Phi(H)) \subset \Pi(H/C) \subset \Pi(\Phi(H)) \cup \{p\}$;

2) *из конечности группы* $\Phi(H)$ *следует конечность индекса* $H : C$.

Доказательство. Пусть $\mathfrak{H} = H\Delta^* E_n$. Тогда

$$\Phi(\mathfrak{H}) = \Phi(H), \qquad H/C \cong \mathfrak{H}/\Delta^* E_n,$$

где $\Delta^* E_n$ — центр группы $\mathfrak{H}$. Поэтому достаточно доказать утверждение леммы для группы $\mathfrak{H}$. Обозначим символом $\mathfrak{H}_0$ ядро гомоморфизма $\det\colon \mathfrak{H} \to \Delta^*$. Так как поле Δ алгебраически замкнуто и $\Delta^* E_n \subseteq \mathfrak{H}$, то $\mathfrak{H} = \mathfrak{H}_0 \Delta^* E_n$. Пусть $\lambda_1, \lambda_2, \ldots, \lambda_n$ — собственные значения матрицы $h \in \mathfrak{H}_0$. Тогда

$$\lambda_j \lambda_1^{-1} = \varepsilon_j \in \Phi(\mathfrak{H}_0) = \Phi(\mathfrak{H}),$$

$$\det h = \varepsilon_1 \ldots \varepsilon_n \lambda_1^n = 1. \tag{16}$$

В силу равенства (16) все собственные значения матрицы h суть корни из единицы. Согласно лемме 5 группа $\mathfrak{H}_0$ локально конечна. Если же $\Phi(\mathfrak{H})$ — конечная группа, то $\operatorname{tr}(\mathfrak{H}_0)$ — конечное множество и группа $\mathfrak{H}_0$ конечна в силу леммы 1. Группа $\mathfrak{H}/\Delta^* E_n$ также, соответственно, локально конечна или конечна, ибо

$$\mathfrak{H}/\Delta^* E_n \cong \mathfrak{H}_0/\mathfrak{H}_0 \cap \Delta^* E_n.$$

Остается рассмотреть множество $\Pi(\mathfrak{H}/\Delta^* E_n)$. Если $h \in \mathfrak{H}_0$, то, так как $\Phi(\mathfrak{H})$ — периодическая группа, есть такое натуральное k, что $\Pi(k) \subset \Pi\Phi(\mathfrak{H})$, а характеристический полином матрицы h^k имеет вид

$$(x - \eta)^n, \qquad \eta^n = 1.$$

Если $\operatorname{char} \Delta = 0$, то из периодичности группы $\mathfrak{H}_0$ следует $h^k = \eta E_n$. Если же $\operatorname{char} \Delta = p$, h^k — элемент порядка dp^τ, $(d, p) = 1$,

$$h^{dp^\tau} = \eta^{p^\tau} E_n,$$

$$\Pi(\Phi(\mathfrak{H})) \cup \{p\} \supset \Pi(\mathfrak{H}_0/C \cap \mathfrak{H}_0) = \Pi(\mathfrak{H}/C).$$

С другой стороны, очевидно,

$$\Pi(\mathfrak{H}/C) \supset \Pi(\Phi(\mathfrak{H})). \quad \blacksquare$$

Теорема 8. *Если* $\Phi(\Gamma)$ — *периодическая группа, то в* Γ *есть нильпотентный нормальный делитель* N, *обладающий следующими свойствами*:

1) $\Phi(N) = (1)$;

2) *фактор-группа* Γ/N *локально конечна, причем если* $\operatorname{char}\Delta = 0$, *то* $\Pi(\Gamma/N) = \Pi(\Phi(\Gamma))$, *если* $\operatorname{char}\Delta = p > 0$, *то* $\Pi(\Phi(\Gamma)) \cup \{p\} \supset \Pi(\Gamma/N) \supset \Pi(\Phi(\Gamma))$;

3) *если группа* $\Phi(\Gamma)$ *конечна, то конечна и фактор-группа* Γ/N.

Доказательство. Как и при доказательстве предыдущей леммы, можно считать, что $\Delta^* E_n \subset \Gamma$. Пусть γ — гомоморфизм (7), $K = \operatorname{Ker}\gamma$, $N = K\Delta^* E_n$. Очевидно, $N \lhd \Gamma$ и $\Phi(N) = (1)$. Обратимся к группе $\operatorname{Im}\gamma = \overline{\Gamma} \cong \Gamma/K$. Матрицы центра Z группы $\overline{\Gamma}$ имеют вид $\operatorname{diag}[\lambda_1 E_{n_1}, \ldots, \lambda_k E_{n_k}]$. Так как $\Phi(\overline{\Gamma}) = \Phi(\Gamma)$, то $\lambda_j\lambda_1^{-1} \in \Phi(\Gamma)$, $j = 1, 2, \ldots, k$. Следовательно,

$$\Pi(Z/\Delta^* E_n) \subset \Pi(\Phi(\Gamma)). \tag{17}$$

Докажем локальную конечность группы Γ/N. Так как $\gamma^{-1}(\Delta^* E_n) = N$, то

$$\Gamma/N \cong \gamma(\Gamma)/\Delta^* E_n = \overline{\Gamma}/\Delta^* E_n.$$

Если $\overline{\Gamma}_0$ — ядро гомоморфизма $\det\colon \overline{\Gamma} \to \Delta^*$, то

$$\Gamma/N \cong \overline{\Gamma}_0\Delta^* E_n/\Delta^* E_n \cong \overline{\Gamma}_0/\Delta^* E_n \cap \overline{\Gamma}_0.$$

Следовательно, достаточно установить локальную конечность группы $\overline{\Gamma}_0$. Пусть $g \in \overline{\Gamma}_0$, $\lambda_1, \ldots, \lambda_n$ — собственные значения матрицы g. Тогда

$$\lambda_j\lambda_1^{-1} = \varepsilon_j \in \Phi(\Gamma), \qquad \varepsilon_1 \ldots \varepsilon_n\lambda_1^n = 1.$$

Таким образом, все λ_j — корни из единицы. Группа $\overline{\Gamma}_0$ вполне приводима, каждый ее неприводимый блок локально конечен. Поэтому $\overline{\Gamma}_0$ — локально конечная группа. Локальная конечность группы Γ/N установлена.

Если теперь $\Phi(\Gamma)$ — конечная группа, то каждый неприводимый блок группы $\overline{\Gamma}_0$ конечен и, значит, $\overline{\Gamma}_0$ — конечная группа. Тогда конечна и фактор-группа Γ/N.

Рассмотрим

$$\Pi(\Gamma/N) = \Pi(\overline{\Gamma}/\Delta^* E_n).$$

Пусть $\operatorname{char}\Delta = p > 0$. Согласно лемме 7

$$\Pi(\Phi(\Gamma)) \cup \{p\} \supset \Pi(\overline{\Gamma}/Z).$$

Отсюда и из (17) следует

$$\Pi(\Phi(\Gamma)) \cup \{p\} \supset \Pi(\overline{\Gamma}/\Delta^* E_n).$$

С другой стороны, очевидно,

$$\Pi(\Gamma/N) \supset \Pi(\Phi(\Gamma)).$$

Если же $\operatorname{char}\Delta = 0$, то, в силу леммы 7 и (17),

$$\Pi(\Phi(\Gamma)) = \Pi(\overline{\Gamma}/\Delta^* E_n). \blacksquare$$

Следствие 1. *Если Δ — алгебраически замкнутое поле нулевой характеристики, Γ — подгруппа группы $GL(n, \Delta)$, $\Phi(\Gamma)$ — периодическая группа, то множество всех унипотентных матриц группы Γ является в ней нормальным делителем.*

Доказательство. Пусть $u \in \Gamma$ — унипотентная матрица, K — ядро гомоморфизма γ, определяемого формулой (7), $\gamma(u) \in \overline{\Gamma}$. Очевидно, что $\gamma(u)$ — также унипотентная матрица. Следовательно,

$$\det\gamma(u) = 1, \qquad \gamma(u) \in \overline{\Gamma}_0.$$

Так как Γ_0 — периодическая группа, то $\gamma(u) = E_n$, $u \in K$. $\blacksquare$

Следствие 2. *Пусть Δ — алгебраически замкнутое поле нулевой характеристики, Γ — подгруппа в $GL(n, \Delta)$, $\Phi(\Gamma)$ — периодическая группа, причем $2 \notin \Pi(\Phi(\Gamma))$ или $\operatorname{card}\Pi(\Phi(\Gamma)) \leqslant 2$. Тогда группа Γ разрешима.*

Доказательство. Согласно теореме 6

$$\Pi(\Gamma/N) = \Pi(\Phi(\Gamma)),$$

причем фактор-группа Γ/N локально конечна. Если $2 \notin \Pi(\Phi(\Gamma))$, то, в силу теоремы Фейта — Томпсона [1], Γ/N — локально разрешимая группа. Если же $\operatorname{card}\Pi(\Phi(\Gamma)) \leqslant 2$, то группа Γ/N разрешима по известной теореме Бернсайда. С другой стороны,

$$\Gamma/N \cong \overline{\Gamma}_0/\overline{\Gamma}_0 \cap \Delta^* E_n.$$

Следовательно, группа $\overline{\Gamma}_0$ локально разрешима. Согласно теореме 19.7, локально разрешимая группа матриц разрешима. Отсюда вытекает разрешимость группы Γ. $\blacksquare$

§ 24. Существование абелева нормального делителя конечного индекса в периодической линейной группе над полем комплексных чисел

1. Унитарность периодической подгруппы группы $GL(n, C)$. Пусть C — поле комплексных чисел, V_n есть n-мерное векторное пространство над этим полем, $U(n)$ — группа всех унитарных $n \times n$-матриц.

Лемма 1. *Пусть $\mathfrak{G}$ — конечная подгруппа группы $GL(V_n)$. Тогда в V_n можно так задать скалярное произведение $\tau = \tau_{\mathfrak{G}}$, что пространство $\langle V_n, \tau\rangle$ окажется унитарным, а каждый элемент группы $\mathfrak{G}$ — унитарным преобразованием пространства $\langle V_n, \tau\rangle$.*

Доказательство. Пусть $\sigma: V_n \times V_n \to C$ — такое скалярное произведение, что пространство $\langle V_n, \sigma\rangle$ унитарно. Построим еще одно скалярное произведение τ, положив для $x, y \in V_n$

$$\tau(x, y) = \sum_{h \in \mathfrak{G}} \sigma(hx, hy).$$

Очевидно, $\tau: V_n \times V_n \to C$ удовлетворяет всем аксиомам скалярного произведения в унитарном пространстве. Для $g \in \mathfrak{G}$ можно написать

$$\tau(gx, gy) = \sum_{h \in \mathfrak{G}} \sigma(hgx, hgy) = \sum_{h \in \mathfrak{G}} (hx, hy) = \tau(x, y).$$

Следовательно, каждый элемент g группы $\mathfrak{G}$ есть унитарное преобразование унитарного пространства $\langle V_n, \tau\rangle$. ■

Лемма 2. *Пусть $\mathfrak{G}$ — конечная неприводимая подгруппа в $GL(V_n)$. Тогда скалярное произведение $\tau_{\mathfrak{G}}$ леммы 1 определяется группой $\mathfrak{G}$ с точностью до множителя из C^*.*

Доказательство. Пусть $\tau = \tau_{\mathfrak{G}}$. Выберем в унитарном пространстве $\langle V_n, \tau\rangle$ ортонормированный базис B. Тогда в базисе B матрица билинейной формы τ совпадает с E_n, а матрицы группы $\mathfrak{G}$ в базисе B унитарны, т. е. для $g \in \mathfrak{G}$ $g^* = g^{-1}$. Пусть теперь φ — еще одно скалярное произведение такое, что $\langle V_n, \varphi\rangle$ — унитарное пространство, а все элементы группы $\mathfrak{G}$ — унитарные преобразования пространства $\langle V_n, \varphi\rangle$. Если теперь Φ — матрица φ в базисе B, то $g^*\Phi g = \Phi$ для любого элемента g группы $\mathfrak{G}$. Так как $g^{-1} = g^*$, то $\bar{\Phi}g = g\bar{\Phi}$. Отсюда и из неприводимости группы $\mathfrak{G}$ следует, что

$$\Phi = \lambda E_n, \qquad \varphi = \lambda\tau, \qquad \lambda \in C^*. \blacksquare$$

Теорема 1. *Всякая периодическая подгруппа* Γ *группы* $GL(n, C)$ *сопряжена в* $GL(n, C)$ *с некоторой подгруппой группы* $U(n)$.

Доказательство. Согласно теореме 23.6 периодические подгруппы группы $GL(n, C)$ вполне приводимы. Следовательно, мы можем доказывать теорему для случая, когда группа Γ неприводима. Итак, пусть Γ — неприводимая периодическая подгруппа группы $GL(n, C)$. Будем трактовать Γ как подгруппу в $GL(V_n)$. Теорема будет доказана, если мы зададим на V_n такое скалярное произведение τ, что $\langle V_n, \tau\rangle$ окажется унитарным пространством, а операторы группы Γ — его унитарными преобразованиями. Из неприводимости и локальной конечности группы Γ следует, что она содержит неприводимую конечную подгруппу $\mathfrak{G}$. Согласно лемме 1 в V_n есть такое скалярное произведение τ, что операторы группы $\mathfrak{G}$ суть унитарные преобразования унитарного пространства $\langle V_n, \tau\rangle$. Если $\Gamma = \mathfrak{G}$, то теорема доказана.

Пусть теперь $\Gamma \neq \mathfrak{G}$ и $h_1 \in \Gamma \setminus \mathfrak{G}$. Тогда для конечной группы $\mathfrak{H}$, порождаемой h_1 и $\mathfrak{G}$, существует такое скалярное произведение $\tau_1(x, y)$, что для $h \in \mathfrak{H}$

$$\tau_1(hx, hy) = \tau_1(x, y).$$

В частности, это равенство верно, если h — произвольная матрица группы $\mathfrak{G}$. В силу леммы 2 $\tau = \lambda\tau_1$. Следовательно,

$$\tau(h_1x, h_1y) = \tau(x, y),$$

элементы группы Γ суть унитарные операторы пространства $\langle V_n, \tau\rangle$. $\blacksquare$

2. Пространство матриц C_n. В n^2-мерном пространстве матриц C_n введем скалярное произведение

$$(a, b) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij}\bar{\beta}_{ij} = \operatorname{tr}(ab^*), \quad \|\alpha_{ij}\| = a, \quad \|\beta_{ij}\| = b \qquad (1)$$

и положим
$$v(a) = \operatorname{tr}(aa^*) = (a, a).$$
Для $a \in C_n$ и $u \in U(n)$
$$v(ua) = v(au) = v(a). \tag{2}$$
Действительно,
$$v(au) = \operatorname{tr}(au(au)^*) = \operatorname{tr}(a(uu^*)a^*) = v(a)$$
и, аналогично, $v(ua) = v(a)$. В силу (2) для $u \in U(n)$
$$v(u) = v(uu^{-1}) = v(E_n) = \operatorname{tr}(E_n) = n.$$
Следовательно, если $\|a\| = \sqrt{(a, a)}$ — длина вектора $a \in C_n$, то
$$\|u\| = \sqrt{n}. \tag{3}$$

Лемма 3. *Если a и b — унитарные матрицы, то*
$$v(E_n - aba^{-1}b^{-1}) \leqslant 2v(E_n - a)\,v(E_n - b). \tag{4}$$

Доказательство. В силу (2) и унитарности матрицы a можно считать, что
$$a = \operatorname{diag}[\alpha_{11}, \ldots, \alpha_{nn}].$$
Далее,
$$v(E_n - aba^{-1}b^{-1}) = v(ba - ab) =$$
$$= v((b - E_n)a + a(E_n - b)) =$$
$$= \sum_{i=j}^{n} \sum_{j=1}^{n} |(\beta_{ij} - \delta_i^j)\alpha_{jj} + \alpha_{ii}(\delta_i^j - \beta_{ij})|^2 =$$
$$= \sum_{i=1}^{n} \sum_{j=1}^{n} |\alpha_{ii} - \alpha_{jj}|^2 |\delta_i^j - \beta_{ij}|^2;$$
$$|\alpha_{ii} - \alpha_{jj}|^2 = |(1 - \alpha_{ii}) - (1 - \alpha_{jj})|^2 \leqslant$$
$$\leqslant (|1 - \alpha_{ii}|^2 + |1 - \alpha_{jj}|^2) \leqslant 2(|1 - \alpha_{ii}|^2 + |1 - \alpha_{jj}|^2) \leqslant$$
$$\leqslant 2v(E_n - a).$$
Отсюда и из предыдущего равенства вытекает (4). ■

Лемма 4. *Пусть*
$$a, b \in U(n), \quad c = aba^{-1}b^{-1}, \quad ac = ca, \quad v(E_n - b) < 4.$$
Тогда $ab = ba$.

Доказательство. Из условия леммы вытекает перестановочность матриц a и bab^{-1}, следовательно, можно считать обе эти матрицы диагональными. Пусть

$$a = \operatorname{diag}[\lambda_1 E_{n_1}, \ldots, \lambda_r E_{n_r}], \ \lambda_i \neq \lambda_j \quad \text{при} \quad i \neq j.$$

Матрицы bab^{-1} и a различаются лишь расположением диагональных элементов, следовательно, $bab^{-1} = pap^{-1}$, где p — подстановка степени n, записанная в виде матрицы. Матрица $q = pb$ перестановочна с матрицей a и имеет, следовательно, вид $q = \operatorname{diag}[q_1, \ldots, q_r]$. Матрицу p запишем в виде

$$p = \begin{bmatrix} l_{11} & \ldots & l_{1r} \\ \cdot & \cdot & \cdot & \cdot \\ l_{r1} & \ldots & l_{rr} \end{bmatrix},$$

где l_{ij} есть $n_i \times n_j$-матрица. Пусть теперь матрицы b и a неперестановочны. Тогда для каких-либо μ и ν, $\mu \neq \nu$, $l_{\mu\nu} \neq 0$, ибо $b = p^{-1}q$. Так как p — мономиальная матрица, то $\det l_{\mu\mu} = 0$. Следовательно, найдется еще такая пара i, j, $i \neq j$, что $l_{ij} \neq 0$. Ясно, что одна из строк матрицы $l_{\mu\mu}$ и один из столбцов матрицы $l_{\nu\nu}$ нулевые. Отсюда следует, что

$$v(p - q) \geqslant 1 + 1 + (u_1, u_1) + (u_2, u_2) = 4,$$

где u_1 — некоторая строка матрицы q_μ, u_2 — столбец матрицы q_ν, (u_i, u_i) — скалярный квадрат. Но

$$v(p - q) = v(p^{-1}(p - q)) = v(E_n - b).$$

Следовательно, $v(E_n - b) \geqslant 4$, что противоречит условию леммы. ■

Лемма 5. *Пусть a и b — такие унитарные матрицы, принадлежащие некоторой периодической подгруппе группы $GL(n, C)$, что $v(E_n - a) < \frac{1}{2}$, $v(E_n - b) < 4$. Тогда $ab = ba$.*

Доказательство. Матрицы a и b, в силу локальной конечности периодической линейной группы, порождают конечную группу $\mathfrak{G}$. Рассмотрим последовательность матриц из $\mathfrak{G}$:

$$b_0, b_1, \ldots, b_k, \ldots, \tag{5}$$

где $b_0=b$, $b_k=ab_{k-1}a^{-1}b_{k-1}^{-1}$, $k>0$. Положим $\alpha=$ $=v(E_n-a)$. Тогда с помощью леммы 3 получим

$$v(E_n-b_k)\leqslant 2v(E_n-a)\,v(E_n-b_{k-1})=2\alpha v(E_n-b_{k-1}).$$

Отсюда

$$v(E_n-b_k)\leqslant(2\alpha)^k v(E_n-b),\qquad k>0. \tag{6}$$

Так как число различных матриц последовательности (5) не больше порядка группы $\mathfrak{G}$, а в силу (6) для любого $\varepsilon>0$ можно найти такое $k=k(\varepsilon)$, что $v(E_n-b_k)<$ $<\varepsilon$, то для некоторого натурального l

$$v(E_n-b_l)=0,\qquad b_l=E_n. \tag{7}$$

С другой стороны, из (6) получим

$$v(E_n-b_k)<4\quad\text{при}\quad k>0.$$

Отсюда и из (7), применяя лемму 4, найдем

$$b_{l-1}=b_{l-2}=\ldots=b=E_n. \blacksquare$$

3. Основная теорема.

Теорема 2. (Вторая теорема Шура.) *Периодическая подгруппа* Γ *группы* $GL(n, C)$ *имеет абелев нормальный делитель* A, *индекс которого не больше некоторого числа* $\rho(n)$, *зависящего лишь от* n.

Доказательство. Согласно теореме 1 можно считать, что $\Gamma\subset U(n)$. Положим теперь

$$D=\left\{d\mid d\in\Gamma,\ v(E_n-d)<\frac{1}{2}\right\}.$$

По лемме 5 элементы множества D попарно перестановочны. Следовательно, оно порождает абелеву подгруппу A группы Γ. Если $d\in D$, то, согласно формуле (2), $gdg^{-1}\in D$ для $g\in\Gamma$. Следовательно, A — абелев нормальный делитель группы Γ. Пусть b и c — представители двух различных смежных классов группы Γ по A. Тогда

$$v(b-c)\geqslant\frac{1}{2}. \tag{8}$$

Действительно, пусть $v(b-c)<\frac{1}{2}$. Тогда

$$v\left(E_n-b^{-1}c\right)=v\left(b\left(E_n-b^{-1}c\right)\right)=v(b-c)<\frac{1}{2},$$

$b^{-1}c \in D$, $b^{-1}c \in A$. Последнее включение противоречит выбору матриц b и c. Неравенство (8) доказано.

Будем теперь трактовать пространство матриц C_n как $2n^2$-мерное евклидово пространство R^{2n^2}. Если $a, b \in C_n$,

$$a = \| \alpha_{\mu\nu} \|, \quad b = \| \beta_{\mu\nu} \|, \quad \alpha_{\mu\nu} = \lambda_{\mu\nu} + i\rho_{\mu\nu}, \quad \beta_{\mu\nu} = \sigma_{\mu\nu} + i\tau_{\mu\nu},$$

то будем рассматривать матрицу a как вектор пространства R^{2n^2} с координатами

$$\lambda_{11}, \rho_{11}, \ldots, \lambda_{\mu\nu}, \rho_{\mu\nu}, \ldots, \lambda_{nn}, \rho_{nn},$$

а скалярное произведение векторов a и b зададим формулой

$$\sum_{\mu=1}^{n} \sum_{\nu=1}^{n} (\lambda_{\mu\nu}\sigma_{\mu\nu} + \rho_{\mu\nu}\tau_{\mu\nu}). \tag{9}$$

Из (9) следует, что скалярный квадрат матрицы a в пространстве C_n совпадает с ее скалярным квадратом в пространстве R^{2n^2} и равен $v(a)$.

Пусть теперь B — полная система представителей смежных классов группы Γ по A. Так как $\Gamma \subset U_n$, то, в силу формулы (3), все точки множества B лежат на сфере S радиуса $\sqrt{n}$ в пространстве R^{2n^2}. В силу неравенства (8) для двух различных точек $b, c \in B$ $\| b - c \| \geqslant \frac{1}{2}$. Отсюда вытекает, что $\operatorname{card} B < \rho(n)$, где $\rho(n)$ — число, зависящее лишь от n, и значит,

$$\Gamma : A < \rho(n). \ \blacksquare$$

Из теоремы Шура вытекает следующая

Теорема 3. (Теорема Жордана.) *Конечная подгруппа группы $GL(n, C)$ обладает абелевым нормальным делителем, индекс которого меньше некоторого числа $\rho(n)$, зависящего лишь от n.*

Отметим еще очевидное следствие теоремы Шура: *Периодическая простая подгруппа группы $GL(n, C)$ конечна, ее порядок меньше числа $\rho(n)$.*

Теорема Шура остается верной для периодических линейных групп над произвольным полем нулевой характеристики. Но на случай полей простой характеристики теорема Шура не распространяется. Существуют даже простые бесконечные периодические линейные группы. Например, пусть Δ — бесконечное поле характеристики 2, алгебраическое над $GF(2)$. Тогда $G = SL(2, \Delta)$ — периодическая бесконечная простая группа. Действительно, группа G — периодическая, ибо Δ^* — периодическая группа. Группа G проста, так как $Z(G) = (E_2)$,

$$G/Z(G) = PSL(2, \Delta).$$

Можно привести столь же простой пример разрешимой периодической группы матриц, у которой нет инвариантной абелевой подгруппы конечного индекса. Пусть Δ — бесконечное поле, алгебраическое над своим простым подполем $GF(p)$, а G — группа всех матриц вида

$$\begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix},$$

где $\alpha, \gamma \in \Delta^*$, $\beta \in \Delta$. Тогда, очевидно, G — разрешимая периодическая подгруппа группы $GL(2, \Delta)$. Однако, как легко проверить, в G нет абелева нормального делителя конечного индекса.

Для полей простой характеристики Брауэр и Фейт [1] доказали следующий аналог теоремы Жордана:

Пусть p — простое число. Тогда существует целозначная функция $f_p(m, n)$ такая, что если Δ — поле характеристики p, а G — конечная подгруппа в $GL(n, \Delta)$, p-подгруппа Силова которой имеет порядок не больше p^m, то G обладает абелевым нормальным делителем A с индексом

$$G : A < f_p(m, n).$$

В дальнейшем нам понадобится следующая

Теорема 4. *Пусть G — неприводимая конечная подгруппа группы $GL(n, C)$, где C — поле комплексных чисел, а A — абелев нормальный делитель группы G. Тогда индекс $G : A$ делится на n.*

Доказательство см., например, в книге Серра [1], стр. 62.

§ 25. Подгруппы Силова полной линейной группы

1. Общие замечания. p-подгруппы Силова группы $GL(n, \Delta)$ при $p = \mathrm{char}\,\Delta$. Пусть Δ — произвольное поле, Π — непустое множество простых чисел, а G — какая-либо Π-подгруппа Силова группы $GL(n, \Delta)$. В частности, когда Π — множество всех простых чисел, тогда, очевидно, G — максимальная периодическая подгруппа группы $GL(n, \Delta)$. В подходящем базисе пространства Δ^n матрицы g группы G имеют вид

$$g = \begin{bmatrix} a_1(g) & a_{12}(g) & \dots & a_{1k}(g) \\ 0 & a_2(g) & \dots & a_{2k}(g) \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_k(g) \end{bmatrix}, \tag{1}$$

где

$$\gamma_j\colon G \to GL(n_j, \Delta), \qquad g \mapsto a_j(g), \qquad j = 1, \dots, k,$$

— неприводимые части группы G. Ясно, что $\mathrm{Im}(\gamma_j)$ суть Π-группы. Если $\mathrm{char}\,\Delta = 0$ или $\mathrm{char}\,\Delta = p > 0$, но $p \notin \Pi$, то группа G вполне приводима (теорема 23.6), и можно считать, что $a_{ij}(g) = 0$ при $i \neq j$.

Введем еще представление γ, положив

$$\gamma\colon G \to GL(n, \Delta), \qquad g \mapsto \mathrm{diag}\,[a_1(g), \dots, a_k(g)]. \tag{2}$$

Если $\mathrm{char}\,\Delta \notin \Pi$, то γ — точное представление, $\mathrm{Im}(\gamma_j)$ есть Π-подгруппа Силова группы $GL(n_j, \Delta)$, а G — прямое произведение групп $\mathrm{Im}(\gamma_1), \dots, \mathrm{Im}(\gamma_k)$.

Лемма 1. *Пусть* $\mathrm{char}\,\Delta \in \Pi$. *Тогда*

$$G = FN, \qquad F = \mathrm{Im}\,\gamma, \qquad N = \mathrm{Ker}\,\gamma, \qquad F \cap N = (E_N),$$

подгруппа F *— прямое произведение групп* $\mathrm{Im}(\gamma_1), \dots, \mathrm{Im}(\gamma_k)$, *группа* $\mathrm{Im}(\gamma_j)$ *есть* Π-*подгруппа Силова группы* $GL(n_j, \Delta)$, *а нормальный делитель* N *есть множество всех матриц* c *вида*

$$c = \begin{bmatrix} E_{n_1} & x_{12} & \dots & x_{1k} \\ 0 & E_{n_2} & \dots & x_{2k} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & E_{n_k} \end{bmatrix}, \tag{3}$$

$x_{\alpha\beta}$ *— произвольная* $n_\alpha \times n_\beta$-*матрица над* Δ.

Доказательство. Из (1), (2) и (3) вытекает равенство

$$g = \gamma(g)\,c, \qquad \gamma(g) \in F, \qquad c \in N.$$

Следовательно, $b \in FN$. С другой стороны, FN есть П-группа. Отсюда $G = FN$. ■

С самого начала выделим простой частный случай П-подгрупп Силова группы $GL(n, \Delta)$, когда $\Pi = \{p\}$, где $p = \operatorname{char} \Delta$.

Теорема 1. *Пусть простое число p совпадает с $\operatorname{char} \Delta$. Тогда p-подгруппы Силова группы $GL(n, \Delta)$ попарно сопряжены в ней. Каждая p-подгруппа Силова группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с группой всех специальных треугольных матриц.*

Доказательство. Множество всех унипотентных элементов группы $GL(n, \Delta)$ совпадает с множеством всех ее p-элементов. Действительно, пусть $a \in GL(n, \Delta)$ и $a^{p^\alpha} = 1$. Тогда

$$a^{p^\alpha} - 1 = (a-1)^{p^\alpha} = 0.$$

Следовательно, a — унипотентный элемент. Пусть теперь u — унипотентный элемент группы $GL(n, \Delta)$. Тогда $(u-1)^n = 0$. Если число ν таково, что

$$p^{\nu-1} < n \leqslant p^\nu, \tag{4}$$

то

$$u^{p^\nu} = 1,$$

т. е. u есть p-элемент. Отсюда вытекает, что класс всех p-подгрупп Силова группы $GL(n, \Delta)$ и класс всех ее максимальных унипотентных подгрупп совпадают. Но максимальная унипотентная подгруппа группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с группой всех специальных треугольных матриц. Отсюда и следует теорема. ■

Заметим, что p^ν, *где ν определяется неравенствами* (4), *есть наибольшее число среди порядков p-элементов группы $GL(n, \Delta)$, когда $p = \operatorname{char} \Delta$.*

Отметим некоторые свойства неприводимых и вполне приводимых П-подгрупп Силова группы $GL(n, \Delta)$.

Лемма 2. *Пусть G — неприводимая* П-*подгруппа Силова группы $GL(n, \Delta)$. Тогда G — либо примитивна, либо представима в виде сплетения $\mathfrak{G} \wr \Gamma$, где $\mathfrak{G}$ — примитивная* П-*подгруппа Силова в $GL(m, \Delta)$, а Γ — транзитивная* П-*подгруппа Силова симметрической группы S_k, $mk = n$.*

Лемма является частным случаем теоремы 15.4.

Заметим, что утверждение, обратное лемме 2, не верно, т. е. сплетение примитивной П-подгруппы Силова группы $GL(m, \Delta)$ и транзитивной П-подгруппы группы S_k не обязательно является П-подгруппой Силова в $GL(mk, \Delta)$. Например, пусть

$$\Pi = \{2\}, \quad \Delta = GF(q), \quad q = 4t + 1, \quad \mathfrak{G} = \{\pm 1\} \subset \Delta^*.$$

Тогда сплетение $\mathfrak{G} \wr S_2$ — подгруппа группы $GL(2, \Delta)$; $\mathrm{card}(\mathfrak{G} \wr S_2) = 8$. Но

$$32 \mid \mathrm{card}\, GL(2, \Delta) = (q^2 - 1)(q^2 - q).$$

Следовательно, $\mathfrak{G} \wr S_2$ не есть 2-подгруппа Силова группы $GL(2, \Delta)$.

Из леммы 2 и общих замечаний, сделанных в начале параграфа, вытекает, что *в случае, когда* $\mathrm{char}\,\Delta \notin \Pi$, *П-подгруппа Силова группы* $GL(n, \Delta)$ *сопряжена в* $GL(n, \Delta)$ *с группой* G *матриц* g *вида*

$$g = \mathrm{diag}\,[g_1, \ldots, g_t], \tag{5}$$

где $g_1, \ldots, g_t$ *независимо друг от друга пробегают, соответственно, группы* $G_1, \ldots, G_t$, $G_j = \mathfrak{G}_j \wr \Gamma_j$, $\mathfrak{G}_j$ — *примитивная П-подгруппа Силова в* $GL(m_j, \Delta)$, Γ_j — *транзитивная П-подгруппа Силова в* S_{k_j}, $j = 1, \ldots, t$, $\sum\limits_{j=1}^{t} m_j k_j = n$.

Группу G матриц g вида (5) будем иногда записывать еще так:

$$G = \mathrm{diag}\,[\mathfrak{G}_1 \wr \Gamma_1, \ldots, \mathfrak{G}_t \wr \Gamma_t]. \tag{6}$$

Лемма 3. *Пусть группа* G *вида* (6) *является П-подгруппой Силова в* $GL(n, \Delta)$. *Тогда справедливы два утверждения.*

(i) *Если* П — *множество всех простых чисел, то никакие две группы* $\mathfrak{G}_\mu$ *и* $\mathfrak{G}_\nu$, $\mu \neq \nu$, *не сопряжены.*

(ii) *Если* $\Pi = \{p\}$, *то любая группа* $\mathfrak{G}_j \wr \Gamma_j$, $1 \leqslant j \leqslant t$, *повторяется на диагонали* (6) *меньше чем* p *раз.*

Доказательство. (i) Пусть П — множество всех простых чисел. Тогда G — максимальная периодическая подгруппа группы $GL(n, \Delta)$. Если $\mathfrak{G}_1 = \mathfrak{G}_2$, то группа

$$\mathrm{diag}\,[\mathfrak{G}_1 \wr S_{k_1}, \mathfrak{G}_2 \wr S_{k_2}]$$

— истинная подгруппа периодической группы $\mathfrak{G}_1 \wr S_{k_1+k_2}$. Отсюда следует (i).

(ii) Пусть $\Pi = \{p\}$. Тогда $k_j = p^{\alpha_j}$. Если

$$\mathfrak{G}_1 \wr \Gamma_1 = \ldots = \mathfrak{G}_p \wr \Gamma_p,$$

то группа

$$\operatorname{diag}[\mathfrak{G}_1 \wr \Gamma_1, \ldots, \mathfrak{G}_p \wr \Gamma_p]$$

является истинной подгруппой в $\mathfrak{G}_1 \wr \Gamma$, где Γ есть p-подгруппа Силова группы $S_{p^{\alpha_1}+1}$. ∎

2. p-подгруппы Силова группы $GL(n, \Delta)$ при $p \neq \operatorname{char} \Delta$ для случая алгебраически замкнутого поля Δ.

Лемма 4. *Пусть Δ — алгебраически замкнутое поле, p — простое число, отличное от $\operatorname{char}\Delta$, а $n > 1$. Тогда в группе $GL(n, \Delta)$ нет примитивных p-подгрупп.*

Доказательство. Пусть Φ — примитивная p-подгруппа группы $GL(n, \Delta)$. По теореме 23.5 группа Φ локально конечна. Так как конечная p-группа нильпотентна, то Φ локально нильпотентна и, следовательно, согласно теореме 19.9, разрешима. По теореме 19.5 группа Φ имеет абелев нормальный делитель H конечного индекса k. В силу примитивности группы Φ и теоремы 16.2 $H \subset \Delta^* E_n$. Очевидно, группа $G = \Phi\Delta^*$ также примитивна;

$$G/\Delta^*E_n = \Phi\Delta^*/\Delta^*E_n \cong \Phi/\Delta^*E_n \cap \Phi = \Phi/H.$$

Следовательно,

$$G : \Delta^*E_n = k.$$

Рассмотрим отображение $\det\colon G \to \Delta^*$;

$$\operatorname{Ker}(\det) = G \cap SL(n, \Delta) = G_0.$$

Пусть $g \in G$, $\det g = \lambda \in \Delta^*$. Так как поле Δ алгебраически замкнуто, то в группе Δ^* есть такой элемент ρ, что $\rho^n = \lambda$. Очевидно,

$$\rho^{-1}g \in G_0, \qquad g = \rho g_0, \qquad g_0 \in G_0;$$
$$G = G_0\Delta^*, \qquad G/\Delta^*E_n \cong G_0/\Delta^*E_n \cap G_0.$$

Следовательно, G_0 — конечная группа. Так как группа Φ локально нильпотентна, то G_0 нильпотентна. Следовательно, группа G нильпотентна. Пусть Z_1 — центр группы G, Z_2/Z_1 — центр в G/Z_1, а $c \in Z_2 \setminus Z_1$. Тогда $(c)Z_1$ — абелев нормальный делитель в G, причем $(c)Z_1 \not\subset \Delta^* E_n$. Так как группа G примитивна, то последнее противоречит теореме Клиффорда. ■

Из леммы 4 следует

Лемма 5. *Пусть Δ — алгебраически замкнутое поле, а p — простое число, отличное от* $\operatorname{char} \Delta$. *Тогда любая p-подгруппа группы $GL(n, \Delta)$ мономиальна.*

Из лемм 2 и 4 вытекает

Лемма 6. *Пусть Δ и p удовлетворяют условиям леммы 4 и в группе $GL(m, \Delta)$ есть неприводимые p-подгруппы. Тогда $m = p^\alpha$, неприводимые p-подгруппы Силова группы $GL(p^\alpha, \Delta)$ сопряжены в ней с группой*

$$G_{p^\alpha} = P \wr N_{p^\alpha},$$

где P есть p-подгруппа Силова группы Δ^*, а N_{p^α} есть p-подгруппа Силова симметрической группы S_{p^α}.

Теорема 2. *Пусть Δ — алгебраически замкнутое поле, а p — простое число, отличное от* $\operatorname{char} \Delta$. *Тогда p-подгруппы Силова группы $GL(n, \Delta)$ попарно сопряжены в ней. Пусть, далее,*

$$n = a_0 + a_1 p + \ldots + a_\mu p^\mu,$$
$$0 \leqslant a_\nu < p, \quad \nu = 0, \ldots, \mu, \quad a_\mu \neq 0.$$

Тогда всякая p-подгруппа Силова группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с группой

$$\operatorname{diag}[\ldots, G_{p^\nu}, \ldots], \tag{7}$$

где $G_{p^\nu} = P \wr N_{p^\nu}$, P есть p-подгруппа Силова группы Δ^*, N_{p^ν} есть p-подгруппа Силова симметрической группы S_{p^ν}, причем группа G_{p^ν} повторяется в (7) a_ν раз.

Доказательство. Из полной приводимости p-подгруппы Силова в $GL(n, \Delta)$ и из леммы 6 вытекает, что p-подгруппа Силова группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с группой вида (7), надо лишь показать, что группа G_{p^ν} входит в (7) a_ν раз. Пусть она фигурирует в (7) b_ν раз. Тогда

$$n = b_0 + b_1 p + \ldots + b_\lambda p^\lambda.$$

Теорема будет доказана, если установить, что $b_\nu < p$ для $\nu = 0, 1, \ldots, \lambda$. Пусть, напротив, для некоторого ν $b_\nu \geqslant p$. Тогда группа G содержит прямой множитель

$$U = \operatorname{diag}[G_{p^\nu}, \ldots, G_{p^\nu}],$$

где G_{p^ν} повторяется p раз. Очевидно, что

$$N_{p^{\nu+1}} = N_{p^\nu} \wr N_{p^\nu}.$$

Отсюда легко заключить, что U есть истинная подгруппа группы

$$G_{p^{\nu+1}} = P \wr N_{p^{\nu+1}}.$$

Следовательно, группа, задаваемая формулой (7), не есть p-подгруппа Силова в $GL(n, \Delta)$. Отсюда $b_\nu = a_\nu$. ∎

Очевидно, что *для p и Δ, удовлетворяющих условиям теоремы, p-подгруппа Силова P группы Δ^* есть группа типа p^∞*. Отсюда и из теоремы 2 вытекает, что *p-подгруппа Силова группы $GL(n, \Delta)$ с точностью до изоморфизма задается только двумя числами n и p, т. е. если Δ_1 — другое алгебраически замкнутое поле и $\operatorname{char}\Delta_1 \neq p$, то p-подгруппы Силова групп $GL(n, \Delta_1)$ и $GL(n, \Delta)$ изоморфны.*

3. p-подгруппы Силова группы $GL(n, \Delta)$ при произвольном поле Δ. Такие группы изучены Вольвачевым [1]. Здесь мы приведем результаты Р. Т. Вольвачева без доказательств.

Теорема 3. *p-подгруппы Силова группы $GL(n, \Delta)$, где Δ — произвольное поле, почти всегда попарно сопряжены в $GL(n, \Delta)$. Исключение составляет случай, когда одновременно $p = 2$, поле Δ подчинено трем следующим условиям: 1) в Δ^* нет элемента 4-го порядка, 2) -1 есть сумма двух квадратов в Δ, 3) всякий 2-элемент $\alpha + \beta i$ из $\Delta(i)$, где $\alpha, \beta \in \Delta$, $i^2 = -1$, удовлетворяет соотношению $(\alpha + \beta i)(\alpha - \beta i) = 1$. В этом исключительном случае множество всех 2-подгрупп Силова группы $GL(n, \Delta)$ разбивается на $[n/2] + 1$ классов сопряженных подгрупп.*

Строение p-подгрупп Силова группы $GL(n, \Delta)$ зависит от определенных свойств пары $\langle \Delta, p \rangle$. Пару $\langle \Delta, 2 \rangle$, где Δ удовлетворяет условиям 1), 2), 3), назовем *исключительной*. Примером исключительной пары является пара $\langle\Delta, 2\rangle$ при $\Delta = Q(\sqrt{-5})$, где Q — поле рациональных чисел.

Обозначим символом P_p p-подгруппу Силова группы Δ^*. Множество всех пар $\langle\Delta, p\rangle$, где Δ — произвольное поле, а p — простое число, отличное от $\operatorname{char}\Delta$, разобьем следующим образом на классы $\mathfrak{M}_1, \ldots, \mathfrak{M}_5$:

1) Если P_p — группа типа p^∞, то положим $\langle\Delta, p\rangle \in \mathfrak{M}_1$.

2) Если порядок группы P_p равен $p^l > 2$, то положим $\langle\Delta, p\rangle \in \mathfrak{M}_2$.

3) Если $p=2$, P_2 — группа порядка 2, но $\langle\Delta, 2\rangle$ не является исключительной парой, то положим $\langle\Delta, 2\rangle \in \mathfrak{M}_3$.

4) Если $\langle\Delta, 2\rangle$ — исключительная пара, то положим $\langle\Delta, 2\rangle \in \mathfrak{M}_4$.

5) Если $p > 2$, $P_p = (1)$, то положим $\langle\Delta, p\rangle \in \mathfrak{M}_5$.

Пусть $\langle\Delta, p\rangle$ принадлежит либо $\mathfrak{M}_1$, либо $\mathfrak{M}_2$, а $n = a_0 + a_1 p + \ldots + a_\mu p^\mu$, $a_\mu \neq 0$, $0 \leqslant a_\nu < p$, $\nu = 0, \ldots, \mu$. Тогда любая p-подгруппа Силова группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с группой

$$G = \operatorname{diag}[\ldots, G_{p^\nu}, \ldots],$$

где прямой множитель $G_{p^\nu} = P_p \wr N_{p^\nu}$ повторяется a_ν раз. Различие между первым случаем и вторым состоит в том, что при $\langle\Delta, p\rangle \in \mathfrak{M}_1$ p-подгруппа Силова в $GL(n, \Delta)$ бесконечна, а при $\langle\Delta, p\rangle \in \mathfrak{M}_2$ — конечна.

Пусть $\langle\Delta, 2\rangle \in \mathfrak{M}_3$, а $n = a_0 + a_1 2 + \ldots + a_\mu 2^\mu$, $a_\mu = 1$, $a_\nu = 0, 1$, $\nu = 1, \ldots, \mu$. Тогда любая 2-подгруппа Силова группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с группой

$$G = \operatorname{diag}[\ldots, G_{2^\nu}, \ldots],$$

где $G_{2^0} = \{\pm 1\}$, $G_{2^\nu} = \mathfrak{G} \wr N_{2^{\nu-1}}$ при $\nu > 0$; группа $\mathfrak{G}$ является 2-подгруппой Силова группы $GL(2, \Delta)$, причем прямой множитель G_{2^ν} повторяется a_ν раз.

Пусть $\langle\Delta, 2\rangle \in \mathfrak{M}_4$. Тогда любая 2-подгруппа Силова группы $GL(2, \Delta)$ сопряжена в $GL(2, \Delta)$ с одной из двух не сопряженных между собой подгрупп $\mathfrak{G}_1$ и $\mathfrak{G}_2$. Представим теперь $[n/2]$ в виде

$$\left[\frac{n}{2}\right] = m + l, \tag{8}$$

где m и l — целые неотрицательные числа. Очевидно, $n=a_0+2(m+l)$, $a_0=0$, 1. Запишем m и l в двоичной системе счисления

$$m=b_0+b_1 2+\ldots+b_\lambda 2^\lambda, \qquad l=c_0+c_1 2+\ldots+c_\mu 2^\mu.$$

Каждому представлению числа $[n/2]$ в виде (8) поставим в соответствие группу

$$G_{m,l}=\mathrm{diag}\left[\ldots, G^1_{2^\alpha}, \ldots, G^2_{2^\beta}, \ldots\right], \tag{9}$$

где прямые множители $G^1_{2^\alpha}=\mathfrak{G}_1 \wr N_{2^{\alpha-1}}$ и $G^2_{2^\beta}=\mathfrak{G}_2 \wr N_{2^{\beta-1}}$ повторяются, соответственно, b_α и c_β раз, а при $a_0=1$ группа $G_{m,l}$ содержит еще прямой множитель $\{\pm 1\}$. Тогда любая из $[n/2]+1$ групп $G_{m,l}$ вида (9) является 2-подгруппой Силова в $GL(n, \Delta)$ и каждая 2-подгруппа Силова группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с одной и только одной группой вида $G_{m,l}$.

Пусть, наконец, $\langle\Delta, p\rangle \in \mathfrak{M}_5$, а $\Sigma=\Delta(\varepsilon)$, где ε — первообразный корень степени p из 1. Положим $m=\Sigma:\Delta$ и запишем число n в виде

$$n=c+mn_0, \qquad 0 \leqslant c < m.$$

В свою очередь, число n_0 запишем в виде

$$n_0=b_0+b_1 p+\ldots+b_\mu p^\mu, \quad b_\mu \neq 0, \quad 0 \leqslant b_j < p,$$
$$j=0, \ldots, \mu.$$

Тогда любая p-подгруппа Силова группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с группой

$$G=\mathrm{diag}\left[1, \ldots, 1, \ldots, G_{mp^\alpha}, \ldots\right],$$

где 1 входит c раз, $G_{mp^\alpha}=P'_p \wr N_{p^\alpha}$, P'_p есть p-подгруппа Силова в Σ^*, Σ^* трактуется как подгруппа в $GL(m, \Delta)$, группа G_{mp^α} повторяется b_α раз.

4. О p-подгруппах Силова группы $GL(n, T)$ над телом T. Приведем без доказательств один результат из статьи Залесского [3].

Теорема 4. *Пусть T — тело, C — его центр, $T:C=p^{2\alpha}m^2$, $(m, p)=1$. Пусть, кроме того, при $p=2$ в группе C^* есть элемент 4-го порядка. Тогда множество всех p-подгрупп Силова группы $GL(n, T)$ разбивается, самое* *большое, на $\alpha+1$ классов сопряженных подгрупп. В частности, если $((T:C),\ p)=1$, то p-подгруппы Силова группы $GL(n,\ T)$ попарно сопряжены в ней.*

5. П-подгруппы Силова группы $GL(n, C)$ над полем C комплексных чисел.

Лемма 7. *В группе $GL(n,\ C)$ тогда и только тогда есть неприводимые* П*-подгруппы, когда* $\Pi(n)\subset\Pi$.

Доказательство. Пусть G — неприводимая П-подгруппа в $GL(n,\ C)$. По теореме 23.5 группа G локально конечна и, следовательно, содержит конечную неприводимую группу $\mathfrak{G}$. По теореме 24.4 $n|\operatorname{card}\mathfrak{G}$, следовательно, $\Pi(n)\subset\Pi(\mathfrak{G})\subset\Pi$. Обратно, пусть $\Pi(n)\subset\subset\Pi$. Рассмотрим группу G, порожденную двумя матрицами a и b:

$$a=\operatorname{diag}[1,\ \varepsilon,\ \ldots,\ \varepsilon^{n-1}],$$

$$b=e_{21}+e_{32}+\ldots+e_{n,\,n-1}+e_{1n},$$

где ε — элемент порядка n, принадлежащий группе C^*. Как легко проверить, $ab=\varepsilon ba$; $\operatorname{card} G=n^3$, т. е. G есть П-группа. Очевидно, G — неприводимая группа. ■

Лемма 8. *Пусть G — примитивная* П*-подгруппа Силова группы $GL(n,\ C)$. Тогда порядок пересечения $G_0=G\cap SL(n,\ C)$ меньше некоторого числа $\mu(n)$, зависящего лишь от n, а группа G представима в виде*

$$G=G_0PE_n, \tag{10}$$

где P есть П*-подгруппа Силова группы C^*, а PE_n — единственный максимальный абелев нормальный делитель группы G.*

Доказательство. Очевидно, $G\supset PE_n$. С другой стороны, по теореме 16.2, любой абелев нормальный делитель группы G содержит только скалярные матрицы. Следовательно, PE_n — единственный максимальный абелев нормальный делитель группы G. По теореме 24.2

$$G:PE_n<\rho(n).$$

Докажем (10). Так как G является П-группой, то для $a\in G$ $\det a=\alpha\in P$. Пусть γ — корень уравнения $x^n=\alpha$. Тогда $\gamma\in P$, ибо $\Pi(n)\subset\Pi$. Очевидно, что

$$\det(\gamma^{-1}a)=1,\qquad \gamma^{-1}a\in G_0.$$

Отсюда следует (10). Остается оценить $\operatorname{card} G_0$. Ясно, что

$$G_0 \cap PE_n = SL(n, C) \cap PE_n.$$

Следовательно,

$$\operatorname{card}(G_0 \cap PE_n) = n.$$

Далее,

$$G : PE_n < \rho(n), \qquad G/PE_n = G_0 PE_n/PE_n \cong G_0/PE_n \cap G_0.$$

Отсюда вытекает

$$\operatorname{card} G_0 < \mu(n) = n\rho(n). \ \blacksquare$$

Лемма 9. *Пусть G — неприводимая* П-*подгруппа Силова группы $GL(n, C)$. Тогда либо группа G примитивна, либо имеется только одно непродолжаемое разложение пространства C^n на ее системы импримитивности.*

Доказательство. Пусть пространство C^n допускает два непродолжаемых разложения

$$C^n = Q_1 \dotplus \ldots \dotplus Q_\nu \quad \text{и} \quad C^n = L_1 \dotplus \ldots \dotplus L_\mu \tag{11}$$

на системы импримитивности группы G. Тогда, согласно лемме 15.5, группа G допускает два представления вида

$$G = \mathfrak{G} \wr \Gamma \quad \text{и} \quad G = \mathfrak{G}_1 \wr \Gamma_1,$$

где Γ и Γ_1 — транзитивные П-подгруппы Силова групп S_ν и S_μ соответственно, $\mathfrak{G}$ — примитивная П-подгруппа Силова в $GL(n\nu^{-1}, C)$, а $\mathfrak{G}_1$ — примитивная П-подгруппа Силова в $GL(n\mu^{-1}, C)$. Из равенства $G = \mathfrak{G} \wr \Gamma$ следует, что G обладает абелевым нормальным делителем A, матрицы которого a в базисе, отнесенном к первому разложению (11), имеют вид

$$a = \operatorname{diag}[\lambda_1 E_m, \ldots, \lambda_\nu E_m], \qquad m = n\nu^{-1},$$

где λ_j независимо друг от друга пробегают группу P;

$$G : A \leqslant \nu!\,(\mathfrak{G} : PE_n) < \nu!\,\rho(m).$$

В свою очередь, из второго разложения (11) вытекает, что G имеет другой абелев нормальный делитель B конечного индекса. Представим группу A в виде $A = A_1 \ldots A_\nu$, где A_j состоит из матриц вида

$$\operatorname{diag}[E_m, \ldots, E_m, \lambda_j E_m, E_m, \ldots, E_m].$$

Так как

$$A_jB/B \cong A_j/A_j \cap B,$$

то для $D_j = A_j \cap B$ $A_j : D_j < \infty$. Следовательно, $D_j \neq \neq (E_n)$. Произведение $D_1 \dots D_\nu = D$ является прямым и содержится в группе B. Отсюда вытекает, что каждое подпространство Q_j инвариантно относительно группы B. Далее, ограничение $B|Q_j$ является нормальным делителем группы $\mathfrak{G}$. Так как $\mathfrak{G}$ — примитивная группа, а группа $B|Q_j$ абелева, то каждая матрица из группы $B|Q_j$ скалярна. С другой стороны, если пространство C^n трактовать как аддитивную операторную группу с областью операторов $C \cup B$, то одномерные подпространства из Q_i и Q_j при $i \neq j$ не изоморфны операторно. Следовательно, оба разложения (11) получаются из разложения пространства C^n в прямую сумму операторно простых групп объединением всех операторно изоморфных друг другу слагаемых. Согласно предложению 13.3 такое разложение единственно. Следовательно, $\nu = \mu$ и при подходящей нумерации $L_j = Q_j$, $j = 1, \dots, \nu$. ∎

Теорема 5. *П-подгруппа Силова группы $GL(n, C)$ обладает единственным максимальным абелевым нормальным делителем.*

Доказательство. Пусть G есть П-подгруппа Силова группы $GL(n, C)$. Легко видеть, что достаточно рассмотреть тот случай, когда группа G неприводима. Для примитивных групп теорема уже доказана (см. лемму 8). Будем теперь считать, что G — импримитивная группа, а

$$C^n = Q_1 \dotplus \dots \dotplus Q_k \tag{12}$$

— непродолжаемое разложение пространства C^n на ее системы импримитивности. Разложение (12) определяет абелев нормальный делитель A группы G, матрицы a которого в базисе, отнесенном к этому разложению, имеют вид

$$a = \operatorname{diag}[\lambda_1 E_m, \dots, \lambda_k E_m], \qquad \lambda_j \in P, \qquad m = nk^{-1}.$$

Группа A — прямое произведение k экземпляров группы P. Пусть теперь B — максимальный абелев нормальный делитель в G. Тогда B содержит группу PE_n в качестве истинной подгруппы. По теореме 16.2 существует такое разложение

$$C^n = R_1 \dotplus \ldots \dotplus R_t$$

пространства C^n на системы импримитивности группы G, что

$$B \mid R_j = PE_{nt^{-1}}.$$

Это разложение можно продлить до непродолжаемого разложения на системы импримитивности группы G, которое, в силу леммы 9, совпадает с (12). Отсюда вытекает, что $B \subset A$. Так как B — максимальный абелев нормальный делитель группы G, то $B = A$. ∎

Лемма 10. *Пусть $n = km$, $\mathfrak{G}$ — примитивная* П-*подгруппа Силова группы* $GL(m, C)$, *а* Γ — *транзитивная* П-*подгруппа Силова симметрической группы* S_k. *Тогда сплетение*

$$H = \mathfrak{G} \wr \Gamma \tag{13}$$

является неприводимой П-*подгруппой Силова группы* $GL(n, C)$.

Доказательство. Согласно лемме 15.4 группа H неприводима. Остается, следовательно, доказать, что группа H не содержится в другой П-подгруппе в $GL(n, C)$. Пусть G есть П-подгруппа Силова в $GL(n, C)$, содержащая группу H. Группа H имеет абелев нормальный делитель A, являющийся множеством всех матриц a вида

$$a = \operatorname{diag}[a_1, \ldots, a_k], \qquad a_j \in PE_m.$$

Представим группу A в виде прямого произведения $A = A_1 \times \ldots \times A_k$, где A_j состоит из элементов $\operatorname{diag}[E_m, \ldots, a_j, \ldots, E_m]$, $A_j \cong P$. Пусть B — максимальный абелев нормальный делитель группы G. Тогда $G : B < \infty$, $A_j : (A_j \cap B) < \infty$. Следовательно, $A_j \cap B = D_j \neq (E_n)$. Произведение $D_1 \ldots D_k = D$ является прямым и содержится в группе B. Если теперь

$$C^n = Q_1 \dotplus \ldots \dotplus Q_k \tag{14}$$

— непродолжаемое разложение пространства C^n на системы импримитивности группы H, определяемое равенством (13), то, в силу включения $D \subset B$, каждое подпространство Q_j инвариантно относительно группы B.

Отсюда же следует, что одномерные подпространства из Q_i операторно не изоморфны одномерным подпространствам пространства Q_j при $i \neq j$ (область операторов $C \cup B$). Следовательно, непродолжаемое разложение пространства C^n на системы импримитивности группы G есть продолжение разложения (14). В силу включения $G \supset H$ оно совпадает с (14). Отсюда вытекает равенство $G = H$. ∎

Теорема 6. *Для любого фиксированного множества простых чисел* Π *число классов сопряженных* Π-*подгрупп Силова не превышает некоторой границы* $\tau(n)$, *зависящей только от* n.

Доказательство. Очевидно, что достаточно доказать теорему для неприводимых Π-подгрупп Силова. Для примитивных Π-подгрупп теорема следует из леммы 8, ибо примитивная Π-подгруппа Силова группы $GL(n, C)$ задается однозначно конечной группой, порядок которой меньше $\mu(n)$ (см. (10)). Импримитивная Π-подгруппа Силова G группы $GL(n, C)$, в силу леммы 2, сопряжена с группой вида $G = \mathfrak{G} \wr \Gamma$, где $\mathfrak{G}$ — примитивная Π-подгруппа Силова в $GL(m, C)$, а Γ — транзитивная Π-подгруппа Силова группы S_k, $km = n$. Отсюда следует теорема. ∎

6. О максимальных периодических подгруппах группы $GL(n, C)$. Взяв в теоремах 5 и 6 в качестве Π множество всех простых чисел, получим следующие две теоремы 5а и 6а.

Теорема 5а. *Максимальная периодическая подгруппа группы $GL(n, C)$ обладает единственным максимальным абелевым нормальным делителем.*

Теорема 6а. *Множество всех максимальных периодических подгрупп группы $GL(n, C)$ разбивается на конечное число классов сопряженных подгрупп. Число этих классов ограничено некоторым $\tau(n)$, зависящим только от n.*

Из леммы 10 следует

Лемма 10а. *Пусть $n = km$, $\mathfrak{G}$ — максимальная периодическая примитивная подгруппа в $GL(m, C)$. Тогда сплетение $\mathfrak{G} \wr S_k$ является максимальной периодической подгруппой группы $GL(n, C)$.*

Следствие 1. *Пусть P — периодическая часть группы C^*. Тогда группа всех мономиальных матриц,* *отличные от нуля элементы которых принадлежат группе P, является максимальной периодической подгруппой в $GL(n, C)$.*

Теорема 7. (i) *Всякая максимальная периодическая подгруппа группы $GL(n, C)$ сопряжена в $GL(n, C)$ с группой вида*

$$G = \operatorname{diag}[G_1, \ldots, G_t], \qquad G_j = \mathfrak{G}_j \wr S_{k_j}, \tag{15}$$

где $\mathfrak{G}_j$ — примитивная максимальная периодическая подгруппа в $GL(m_j, C)$, $\sum_{j=1}^{t} k_j m_j = n$, причем в системе групп $\mathfrak{G}_1, \ldots, \mathfrak{G}_t$ нет пары сопряженных.

(ii) *Любая группа вида* (15) *является максимальной периодической подгруппой группы $GL(n, C)$.*

Доказательство. (i) следует из лемм 2 и 3. Докажем (ii). Пусть группа G задается формулой (15) и является истинной подгруппой максимальной периодической подгруппы F из $GL(n, C)$. Пусть, далее,

$$C^n = R_1 \dotplus \ldots \dotplus R_t \tag{16}$$

— разложение пространства C^n на инвариантные и неприводимые относительно G подпространства R_j, а

$$C^n = U_1 \dotplus \ldots \dotplus U_s \tag{17}$$

— разложение его на инвариантные и неприводимые относительно F подпространства U_j. Подпространства $R_1, \ldots, R_t$ — единственные инвариантные неприводимые относительно группы G подпространства в C^n. Следовательно, каждое подпространство U_j из (17) есть прямая сумма некоторых слагаемых из (16). Так как $F \neq G$, то, в силу леммы 10а, некоторое U_j содержит более одного слагаемого из (16); пусть

$$U_1 = R_1 \dotplus \ldots \dotplus R_\gamma, \qquad \gamma > 1.$$

Рассмотрим теперь две группы:

$$\Phi = F \mid U_1 \quad \text{и} \quad \Psi = G \mid U_1.$$

Так как

$$\Psi = \operatorname{diag}[G_1, \ldots, G_\gamma], \quad G_\alpha = \mathfrak{G}_\alpha \wr S_{k_\alpha}, \qquad \alpha = 1, \ldots, \gamma,$$

то группа Ψ имеет абелев нормальный делитель A конечного индекса, который является прямым произведением k групп $A_1, \ldots, A_k$, $k=k_1+\ldots+k_\gamma$, $A_j\cong P$, где P — периодическая часть группы C^*. Если

$$R_\alpha=Q_{\alpha 1}\dotplus \ldots \dotplus Q_{\alpha k_\alpha}$$

— непродолжаемое разложение пространства R_α на системы импримитивности группы G_α, то $A\,|\,Q_{\alpha\beta}\cong P$. Группа Φ обладает абелевым нормальным делителем B конечного индекса. Подгруппа $D_j=A_j\cap B$ имеет конечный индекс в A_j. Так как группа A_j бесконечна, то $D_j\neq(E)$. Произведение $D=D_1\ldots D_k$ является прямым и содержится в группе B. Следовательно, подпространства $Q_{\alpha\beta}$ инвариантны относительно группы B.

$$U_1=\dot{\sum} Q_{\alpha\beta} \tag{18}$$

— непродолжаемое разложение на системы импримитивности группы Φ. Действительно, $B\supset D$, следовательно, в двух различных подпространствах вида $Q_{\alpha\beta}$ нет операторно изоморфных одномерных подпространств. Значит, непродолжаемое разложение пространства U_1 на системы импримитивности группы Φ является продолжением разложения (18). Так как $\Phi\supset\Psi$, то отсюда следует, что (18) — непродолжаемое разложение пространства U_1 на системы импримитивности группы Φ. Так как Φ — максимальная периодическая линейная группа, то $\Phi=\mathfrak{G}\wr S_k$, где $\mathfrak{G}$ — примитивная группа. Так как $\Phi\supset\Psi$, то для $j=1, \ldots, \gamma$ группа $\mathfrak{G}_j$ сопряжена с некоторой подгруппой группы $\mathfrak{G}$. Но $\mathfrak{G}_j$ — максимальная периодическая подгруппа в $GL(m_j, C)$. Следовательно, $\mathfrak{G}_j$ сопряжена с $\mathfrak{G}$, т. е. группы $\mathfrak{G}_1, \ldots, \mathfrak{G}_\gamma$ попарно сопряжены. Последнее противоречит построению групп вида (15). ■

Доказанные в этом пункте теоремы о максимальных периодических подгруппах группы $GL(n, C)$ остаются справедливыми для любого алгебраически замкнутого поля нулевой характеристики. Если Δ — алгебраически замкнутое поле, характеристика которого не принадлежит множеству Π, то леммы 7, 9, теорема 5 и лемма 10 переносятся без изменений на Π-подгруппы Силова группы $GL(n, \Delta)$. Теорема 6 при переходе от C к полю Δ претерпевает некоторое изменение: границу $\tau(n)$ надо заменить на $\tau(n, p)$, где $p=\operatorname{char}\Delta$.

§ 26. Структурные теоремы о периодических матричных группах над полем

Периодичность и точная линейная представимость над полем, взятые вместе, являются настолько сильным ограничением для группы, что группы, подчиненные одновременно этим двум условиям, обладают многими свойствами конечных групп. Здесь мы приведем без доказательства теоремы о периодических матричных группах, принадлежащие Платонову [11], которые можно рассматривать как широкое обобщение некоторых классических теорем теории конечных групп.

Теорема 1. *Пусть G — периодическая группа матриц над полем, а N — такой ее нормальный делитель, что*

$$\Pi(N)\cap\Pi(G/N)=\varnothing.$$

Тогда группа G представима в виде произведения

$$G=DN;\qquad D\cap N=E.$$

Если еще

$$G=D_1N,\qquad D_1\cap N=E,$$

то подгруппы D и D_1 сопряжены в группе G.

Теорема 2. *В периодической группе матриц над полем p-подгруппы Силова сопряжены.*

Π-подгруппа H периодической группы G называется *холловской*, если для любого $p\in\Pi$ подгруппа H содержит p-подгруппу Силова группы G.

В следующей теореме $\Pi'=\Pi\setminus\Pi(G)$.

Теорема 3. *Пусть G — периодическая группа матриц над полем.*

(i) *Если G — разрешимая группа, H и H' — ее, соответственно, Π- и Π'-подгруппы Силова, то $G=HH'$.*

(ii) *Если для каждого $p\in\Pi(G)$ в группе G есть p-подгруппа Силова, имеющая холловское дополнение, то G — разрешимая группа.*

Пусть G — периодическая группа. Система $\{P_k\}$ p-подгрупп Силова P_k группы G, взятых точно по одной для каждого $p_k\in\Pi(G)$, называется *полной силовской базой* группы G, если G есть произведение групп P_k, а для любой конечной подсистемы

$$P_{k_1},\ \ldots,\ P_{k_m} \tag{1}$$

$\Pi(H) = \{p_{k_1}, \ldots, p_{k_m}\}$, где H — группа порождаемая системой (1).

Теорема 4. (i) *Разрешимая периодическая группа G матриц над полем обладает полными силовскими базами; любые две из них сопряжены в группе G.*

(ii) *Если периодическая группа матриц над полем обладает полной силовской базой, то она разрешима.*

Приведем еще две теоремы из статьи Платонова [11] об алгебраических матричных группах.

Теорема 5. *p-подгруппы Силова алгебраической группы матриц над алгебраически замкнутым полем сопряжены в ней.*

Теорема 6. *Пусть Π — произвольное множество простых чисел. Π-подгруппы Силова разрешимой алгебраической группы матриц над алгебраически замкнутым полем сопряжены в ней.*

ГЛАВА VII

НИЛЬПОТЕНТНЫЕ И ЛОКАЛЬНО НИЛЬПОТЕНТНЫЕ ГРУППЫ МАТРИЦ

§ 27. Неприводимые нильпотентные группы матриц

1. Конечность индекса центра. Пусть G — произвольная группа. *Верхний центральный ряд*

$$Z_0=(e)\subset Z_1(G)\subset Z_2(G)\subset \ldots \subset Z_n(G)\subset \ldots$$

группы G определяется индуктивно:

$$Z_{j+1}(G)/Z_j(G)$$

— центр фактор-группы $G/Z_j(G)$. Группа $Z_j(G)$ называется j-м *гиперцентром* группы G. Группа G называется *нильпотентной*, если для некоторого натурального l $G=Z_l(G)$. Если l — наименьшее число, для которого $G=Z_l(G)$, то l называется *классом нильпотентности группы* G.

В частности, абелева неединичная группа является нильпотентной группой класса 1, а единичная группа есть нильпотентная группа класса 0.

Если G и H — поэлементно перестановочные подгруппы некоторой группы, группа H абелева, а G — нильпотентная класса $l>0$, то GH — тоже нильпотентная группа класса l.

Нижний центральный ряд

$$G_0=G\supset G_1\supset G_2\supset \ldots \supset G_j\supset \ldots$$

группы G также определяется индуктивно: $G_{j+1}=(G_0,\ G_j)$, где $j=0,\ 1,\ \ldots,$ а $(G_0,\ G_j)$ — взаимный коммутант групп G_0 и G_j.

Группа G тогда и только тогда нильпотентна класса l, когда l — наименьшее число, для которого G_l совпадает с единичной группой.

Таким образом, *для нильпотентной группы верхний и нижний центральные ряды имеют одну и ту же длину* (Курош [1], стр. 388).

Пусть теперь Δ — произвольное поле, G — нильпотентная неприводимая подгруппа группы $GL(n, \Delta)$ класса l, а

$$Z_0 = (E) \subset Z_1 \subset Z_2 \subset \ldots \subset Z_l = G$$

— верхний центральный ряд группы G. Тогда справедлива

Лемма 1. *Группа G содержится в такой нильпотентной подгруппе $\mathfrak{G}$ группы $GL(n, \Delta)$, что*

(i) *класс нильпотентности группы $\mathfrak{G}$ совпадает с числом l — классом нильпотентности группы G;*

(ii) *$\mathfrak{G}$ — абсолютно неприводимая подгруппа группы $GL(r, \Sigma)$, где Σ — расширение поля Δ, $\Sigma : \Delta = nr^{-1}$;*

(iii) $Z_1(\mathfrak{G}) = \Sigma^* E_r \supset Z_1 = Z_1(G)$.

Доказательство. Пусть $[G]$ — линейная Δ-оболочка группы G. Так как группа G неприводима, то, по теореме 14.4, $[G] = T_\rho$, где T — тело, $T : \Delta = n\rho^{-1}$. Возможны два случая: 1) T — поле, 2) T — некоммутативное тело. В первом случае, полагая $\Sigma = T$, $r = \rho$, $\mathfrak{G} = GT^*$, находим, что группа $\mathfrak{G}$ удовлетворяет условиям (i), (ii) и (iii). Во втором случае группа G содержится в другой нильпотентной подгруппе G_1 класса l группы $GL(n, \Delta)$ такой, что $[G_1] : \Delta > [G] : \Delta$. Действительно, если тело T некоммутативно, то в $GL(n, \Delta) \setminus T_\rho$ есть матрица h, перестановочная с каждым элементом алгебры T_ρ. Группа $G_1 = (h) G$ является нильпотентной подгруппой $GL(n, \Delta)$ класса l. Так как $h \in GL(n, \Delta) \setminus T_\rho$, то $[G_1] \neq [G]$. Следовательно, $[G_1] : \Delta > [G] : \Delta$. Отсюда и вытекает лемма 1. ∎

Лемма 2. *Порядок каждого элемента фактор-группы Z_2/Z_1 является делителем числа n.*

Доказательство. Согласно лемме 1 $G \subset \mathfrak{G} \subset GL(r, \Sigma)$, $Z_1 \subset \Sigma^* E_r$, $r \mid n$. Для $a \in Z_2$, $g \in G$ имеем $ag = \sigma g a$, $\sigma \in \Sigma^*$. Отсюда

$$\det(ag) = \sigma^r \det(ga), \qquad \sigma^r = 1.$$

Следовательно,

$$a^r g = \sigma^r g a^r = g a^r, \qquad a^r \in Z_1, \qquad (aZ_1)^r = Z_1. \ ∎$$

Лемма 3. *Пусть ν — порядок элемента aZ_1 фактор-группы Z_2/Z_1. Тогда в группе G есть такой элемент g, что порядок элемента $(a, g) = aga^{-1}g^{-1}$ также равен ν.*

Доказательство. Согласно лемме 1

$$G \subset GL(r, \Sigma), \qquad Z_1 \subset \Sigma^* E_r.$$

Для любого элемента g группы G

$$(a, g) \in \Sigma^* E_r, \qquad (a, g)^r = 1.$$

Если $h \in G$, то

$$(a, g)(a, h) = (a, gh).$$

Следовательно, все коммутаторы вида (a, g), где $g \in G$, образуют конечную циклическую группу. Пусть τ — её порядок. Тогда для $g \in G$

$$(a^\tau, g) = (a, g)^\tau = 1, \quad (aZ_1)^\tau = Z_1, \qquad \nu \mid \tau.$$

Далее,

$$(a, g)^\nu = (a^\nu, g) = 1, \qquad \tau \mid \nu, \qquad \tau = \nu. \ \blacksquare$$

Следствие 1. $\operatorname{char} \Delta$ *не может делить порядок элемента фактор-группы Z_2/Z_1.*

Лемма 4. *Пусть $Z_1 = \Delta^* E_n$. Тогда $Z_2 : Z_1 = [Z_2] : \Delta$, где $[Z_2]$ — линейная Δ-оболочка группы Z_2.*

Доказательство. Пусть

$$d_1, \ldots, d_t \tag{1}$$

— представители t различных смежных классов группы Z_2 по Z_1. Покажем, что система (1) линейно независима над полем Δ. Пусть

$$\lambda_1 \alpha_1 + \lambda_2 \alpha_2 + \ldots + \lambda_t \alpha_t = 0, \qquad \lambda_j \in \Delta, \tag{2}$$

— нетривиальное линейное соотношение, содержащее наименьшее число ненулевых слагаемых. Мы можем считать, что $\lambda_1 \neq 0$, $\lambda_2 \neq 0$. Для $g \in G$

$$g d_j g^{-1} = \gamma_j d_j, \qquad \gamma_j \in \Delta^*,$$

причем для $i \neq j$ в группе G есть такой элемент g, что

$$\gamma_i \neq \gamma_j, \tag{3}$$

ибо d_i и d_j входят в разные классы по Z_1. Пусть элемент g группы G удовлетворяет условию (3). Тогда из (2) следует

$$\begin{aligned}\gamma_1(\lambda_1 d_1 + \lambda_2 d_2 + \ldots + \lambda_t d_t) - \\ - g(\lambda_1 d_1 + \lambda_2 d_2 + \ldots + \lambda_t d_t) g^{-1} = \\ = \lambda_2(\gamma_1 - \gamma_2) d_2 + \ldots + \lambda_t(\gamma_1 - \gamma_t) d_t = 0.\end{aligned}$$

Последнее равенство противоречит выбору соотношения (2). Следовательно, (1) — линейно независимая система и

$$Z_2 : Z_1 \leqslant [Z_2] : \Delta.$$

Пусть теперь элементы $u_1, \ldots, u_\tau$ группы Z_2 составляют Δ-базис алгебры $[Z_2]$. Тогда они принадлежат τ различным классам группы Z_2 по Z_1 т. е.

$$Z_2 : Z_1 \geqslant [Z_2] : \Delta.$$

Отсюда следует лемма. ■

Лемма 5. *Пусть k — экспонента фактор-группы Z_2/Z_1. Тогда экспонента группы Z_{j+1}/Z_j, $j = 1, \ldots, l-1$, является делителем числа k.*

Доказательство. Для $j = 1$ лемма тривиальна. Предположим, что $j > 1$ и что лемма уже доказана для Z_j/Z_{j-1}. Если $a \in Z_{j+1}$, $g \in G$, то $ga = bag$, где $b \in Z_j$. Следовательно,

$$gZ_{j-1}aZ_{j-1} = bZ_{j-1}aZ_{j-1}gZ_{j-1}.$$

Так как $bZ_{j-1}gZ_{j-1} = gZ_{j-1}bZ_{j-1}$, то

$$gZ_{j-1}(aZ_{j-1})^k = (bZ_{j-1})^k (aZ_{j-1})^k gZ_{j-1}.$$

По индуктивному предположению $(bZ_{j-1})^k = Z_{j-1}$. Следовательно, $(aZ_{j-1})^k \subset Z_j$, $(aZ_j)^k = Z_j$. ■

Следствие 1. *Порядок каждого элемента фактор-группы G/Z_1 является делителем числа k^{l-1}, где k — экспонента группы Z_2/Z_1.*

Лемма 6. *Пусть Δ — алгебраически замкнутое поле. Тогда группа G мономиальна, т. е. существует такой базис $u_1, \ldots, u_n$ пространства Δ^n, что для каждого $g \in G$*

$$g(u_1) = \lambda_1 u_{i_1}, \ \ldots, \ g(u_n) = \lambda_n u_{i_n},$$

где $\lambda_j \in \Delta^*$, а $i_1, \ldots, i_n$ — перестановка чисел $1, \ldots, n$.

Доказательство. Покажем, что нильпотентная неприводимая подгруппа группы $GL(n, \Delta)$ при $n > 1$ импримитивна, если поле Δ алгебраически замкнутое. Пусть $a \in Z_2 \setminus Z_1$. Тогда $(a)Z_1$ — абелев нормальный делитель группы G и $(a)Z_1 \not\subset \Delta^* E_n$. По теореме 16.2 группа G импримитивна. Пусть теперь $\Delta^n = V_1 \dotplus \ldots \dotplus V_t$ — непродолжаемое разложение пространства Δ^n на ее системы импримитивности, а

$$H_j = \{h_j \mid h_j \in G,\ h_j(V_j) = V_j\}.$$

Тогда ограничение $H_j | V_j = G_j$ — нильпотентная примитивная группа степени $nt^{-1} = n_1$. Следовательно, $n_1 = 1$, $t = n$. Отсюда вытекает мономиальность группы G. ■

Теорема 1. *Пусть Δ — произвольное поле, а G — неприводимая нильпотентная подгруппа группы $GL(n, \Delta)$ класса нильпотентности l. Тогда*

$$G : Z_1(G) \leqslant n!\, n^{(l-1)(n-1)} = \nu(n, l),$$

причем $\operatorname{char} \Delta \nmid (G : Z_1(G))$.

Доказательство. Согласно лемме 1 $G \subset \mathfrak{G}$, где $\mathfrak{G}$ — абсолютно неприводимая нильпотентная подгруппа класса l группы $GL(r, \Sigma)$, $Z_1(\mathfrak{G}) = \Sigma^* E_r \supset Z_1(G)$, $r | n$. Если теперь Ω — алгебраически замкнутое поле, содержащее поле Σ, то $\mathfrak{G}$ — неприводимая подгруппа группы $GL(r, \Omega)$, $Z_1(\mathfrak{G}) \subset \Omega^* E_r$. В силу леммы 6 $\mathfrak{G}$ является мономиальной подгруппой группы $GL(r, \Omega)$. Следовательно, существует такой гомоморфизм γ: $\mathfrak{G} \twoheadrightarrow S_r$, где S_r — симметрическая группа степени r, что $\operatorname{Ker} \gamma = \mathfrak{H}$ — подгруппа всех диагональных матриц группы $\mathfrak{G} \subset GL(r, \Omega)$. Очевидно, что $\mathfrak{H} \supset Z_1(\mathfrak{G}) = \Sigma^* E_r$. Пусть, далее, $h = \operatorname{diag}[\omega_1, \ldots, \omega_r]$, $\omega_j \in \Omega^*$, — произвольная матрица из $\mathfrak{H}$. Тогда, согласно лемме 5, $h^{k^{l-1}} \in Z_1(\mathfrak{G})$. Матрицу h можно записать в виде

$$h = \omega_1 \operatorname{diag}[1, \alpha_2, \ldots, \alpha_r].$$

Так как

$$\omega_1^{k^{l-1}} = \omega_2^{k^{l-1}} = \ldots = \omega_r^{k^{l-1}},$$

то

$$\alpha_j^{k^{l-1}} = 1, \quad j = 2, \ldots, r.$$

Если теперь $h_1 \in \mathfrak{H}$ и $h_1 = \omega_1^1 \operatorname{diag}[1, \alpha_2, \ldots, \alpha_r]$, то

$$h_1 h^{-1} \in Z_1(\mathfrak{G}).$$

Следовательно,

$$\mathfrak{H} : Z_1(\mathfrak{G}) \leqslant \left(k^{l-1}\right)^{r-1} = k^{(l-1)(r-1)}.$$

Так как $\mathfrak{G} : \mathfrak{H} \leqslant r!$, то

$$\mathfrak{G} : Z_1(\mathfrak{G}) \leqslant r!\, k^{(l-1)(r-1)} \leqslant n!\, n^{(l-1)(n-1)} = \nu(n, l).$$

Так как $G : Z_1(G) = GZ_1(\mathfrak{G}) \leqslant \nu(n, l)$, то

$$G : Z_1(G) \leqslant \nu(n, l). \blacksquare$$

Из теоремы 1 с использованием леммы 17.5 получаем

Следствие 1. *Если поле Δ совершенно, то неприводимая нильпотентная подгруппа группы $GL(n, \Delta)$ является d-группой.*

2. Неприводимые нильпотентные группы матриц над алгебраически замкнутым полем.

Теорема 2. *Пусть G — неприводимая нильпотентная подгруппа группы $GL(n, \Omega)$, где Ω — алгебраически замкнутое поле. Тогда $\Pi(G/Z_1(G)) = \Pi(n)$.*

Доказательство. Согласно лемме 6 группа G мономиальна. Следовательно, существует такой гомоморфизм γ: $G \to S_n$, что $\operatorname{Ker}\gamma \supset Z_1(G)$. Так как группа G неприводима, то $\operatorname{Im}\gamma$ — транзитивная группа. Следовательно, $n \mid \operatorname{card}(\operatorname{Im}\gamma)$. Очевидно, что

$$G : Z_1(G) = (G : \operatorname{Ker}\gamma)(\operatorname{Ker}\gamma : Z_1(G)), \quad n \mid G : Z_1(G),$$

$$\Pi(n) \subset \Pi(G/Z_1(G)).$$

С другой стороны, в силу леммы 5, порядок каждого элемента фактор-группы $G/Z_1(G)$ делит число k^{l-1}, где $k \mid n$. Следовательно, $\Pi(G/Z_1(G)) \subset \Pi(n)$.

Следствие 1. *Если основное поле алгебраически замкнуто, то $\Pi(k) = \Pi(n)$, где k — экспонента фактор-группы $Z_2(G)/Z_1(G)$.*

Следствие 2. *Если Ω — алгебраически замкнутое поле, а $\operatorname{char}\Omega \mid n$, то в группе $GL(n, \Omega)$ нет неприводимых нильпотентных подгрупп.*

Следствие 3. *Пусть Δ — произвольное поле, а G — абсолютно неприводимая нильпотентная подгруппа группы $GL(n, \Delta)$.*

Тогда $\Pi(G/Z_1(G)) = \Pi(n)$.

Теорема 3. ***Пусть Ω — алгебраически замкнутое поле, а G — неприводимая нильпотентная подгруппа*** *в* $GL(n,\Omega)$ *такая, что* $Z_1(G)=\Omega^*E_n$. *Тогда* $G_0 = G\cap SL(n,\Omega)$ *является конечной группой,* $\Pi(G_0) = \Pi(n)$.

Доказательство. Пусть $g\in G$. Так как поле Ω алгебраически замкнуто, то в Ω^* есть такой элемент ω, что $\det g=\omega^n$. Следовательно,

$$\omega^{-1}E_n g\in G_0,\qquad G=G_0Z_1(G).$$

Далее,

$$G:Z_1(G)=G_0Z_1(G):Z_1(G)=G_0:(G_0\cap Z_1(G)),$$
$$\mathrm{card}\,(G_0\cap Z_1(G))=n.$$

Отсюда

$$G_0:(E_n)=n(G:Z_1(G)).$$

Следовательно, G_0 — конечная группа, $\Pi(G_0)=\Pi(n)$. ∎

Следствие 1. *Пусть* H — *неприводимая нильпотентная подгруппа группы* $SL(n,\Omega)$, *где* Ω — *алгебраически замкнутое поле. Тогда группа* H *конечна и* $\Pi(H) = \Pi(n)$.

Доказательство. Пусть $G = H\Omega^*$, $G_0 = G\cap SL(n,\Omega)$. Тогда, по теореме 3, G_0 — конечная группа и $\Pi(G_0) = \Pi(n)$. Очевидно, $H\subset G_0$, следовательно, $\Pi(H)\subset\Pi(n)$, а H конечна. Далее,

$$G/\Omega^*E_n\cong H/H\cap\Omega^*E_n.$$

Следовательно,

$$\Pi(H/H\cap\Omega^*E_n)=\Pi(G/\Omega^*E_n)=\Pi(n),\qquad \Pi(H)\supset\Pi(n).$$

Отсюда $\Pi(H) = \Pi(n)$. ∎

Пусть Ω — алгебраически замкнутое поле, а $\mathfrak{M}_l$ — система всех таких подгрупп группы $GL(n,\Omega)$, что:

(i) каждая группа из $\mathfrak{M}_l$ есть неприводимая нильпотентная группа класса l;

(ii) группа из $\mathfrak{M}_l$ не содержится в другой нильпотентной подгруппе группы $GL(n,\Omega)$ класса l.

Тогда справедлива

Теорема 4. *Система* $\mathfrak{M}_l$ *разбивается на конечное число классов сопряженных в* $GL(n,\Omega)$ *подгрупп.*

Доказательство. Пусть $G\in\mathfrak{M}_l$. Тогда $Z_1 = Z_1(G) = \Omega^*E_n$. В силу теоремы 3 $G = G_0\Omega^*$. Следовательно, группа G однозначно определяется конечной группой G_0, порядок которой не превосходит $n\nu(n, l)$.

Существует лишь конечное число неизоморфных групп, порядки которых не превосходят числа $n\nu(n, l)$. Каждая конечная группа имеет лишь конечное число неэквивалентных неприводимых линейных представлений степени n над полем Ω. Отсюда и вытекает теорема. ∎

Нильпотентную группу класса нильпотентности 2 будем называть *метабелевой*. Ниже в качестве примера опишем все максимальные неприводимые метабелевы подгруппы группы $GL(n, \Omega)$, где Ω — алгебраически замкнутое поле.

Теорема 5. *Пусть Ω — алгебраически замкнутое поле, а G — неприводимая нильпотентная подгруппа в $GL(n, \Omega)$. Если группа $Z_2 = Z_2(G)$ неприводима, то $G = Z_2$, т. е. G — метабелева группа.*

Доказательство. Абелеву группу Z_2/Z_1, где $Z_1 = Z_1(G)$, запишем в виде произведения ρ циклических групп порядков $l_1, \ldots, l_\rho$:

$$Z_2/Z_1 = (c_1 Z_1) \ldots (c_\rho Z_1);$$
$$Z_2 = (c_1)(c_2) \ldots (c_\rho) Z_1, \quad Z_2 : Z_1 = l_1 l_2 \ldots l_\rho.$$

Согласно лемме 3 в группе G есть такой элемент g_j, что $(c_j, g_j) = \varepsilon_j E_n$, где ε_j — элемент порядка l_j из Ω^*. С другой стороны, для $g \in G$ $(c_j, g) = \varepsilon_j^\alpha E_n$. Следовательно, $G = (g_j) F_j$, где F_j — централизатор c_j в G. Как легко видеть, $G : F_j = l_j$. Если теперь F — централизатор Z_2 в G, то $G : F \leqslant l_1 \ldots l_\rho$, так как F — пересечение групп $F_1, \ldots, F_\rho$. В силу неприводимости группы Z_2 $F = Z_1$. Следовательно, $G : Z_1 \leqslant l_1 \ldots l_\rho = Z_2 : Z_1$. Отсюда $G = Z_2$. ∎

Теорема 6. *Пусть G — неприводимая метабелева подгруппа группы $GL(n, \Omega)$ над алгебраически замкнутым полем Ω, а $Z_1(G) = \Omega^* E_n$. Тогда группа G максимальна среди метабелевых подгрупп в $GL(n, \Omega)$.*

Доказательство. Согласно лемме 4 $G : Z_1(G) = n^2$. Если $\mathfrak{G}$ — метабелева подгруппа группы $GL(n, \Omega)$ и $\mathfrak{G} \supset G$, то $Z_1(\mathfrak{G}) = Z_1(G)$ и $\mathfrak{G} : Z_1(G) = n^2$. Отсюда $\mathfrak{G} = G$. ∎

Теорема 7. *Пусть Ω — такое алгебраически замкнутое поле, что $\operatorname{char} \Omega \nmid n$. Запишем число n в виде*

$$n = k_1 k_2 \ldots k_t, \tag{4}$$

где $k_i > 1$, $i = 1, \ldots, t$, $k_j | k_i$ при $i < j$. Тогда:

(i). *Каждое разложение* (4) *числа* n *определяет максимальную неприводимую метабелеву подгруппу* $\Gamma_{k_1k_2\dots k_t}$ *группы* $GL(n,\Omega)$, *матрицы* g *которой имеют вид*

$$g=\lambda a_1^{\alpha_1}b_1^{\beta_1}\dots a_t^{\alpha_t}b_t^{\beta_t},\qquad \lambda\in\Omega^*, \tag{5}$$

где

$$a_j=E_{k_1\dots k_{j-1}}\dot{\times}\operatorname{diag}\left[1,\varepsilon_j,\dots,\varepsilon_j^{k_j-1}\right]\dot{\times}E_{k_{j+1}\dots k_t},$$

$$b_j=E_{k_1\dots k_{j-1}}\dot{\times}\begin{bmatrix}0 & 1\\ E_{k_j-1} & 0\end{bmatrix}\dot{\times}E_{k_{j+1}\dots k_t},$$

ε_j — *элемент порядка* k_j *из* Ω^*.

(ii). *Два различных разложения числа* n *вида* (4) *определяют две неизоморфные группы* $\Gamma_{k_1k_2\dots k_t}$.

(iii). *Каждая максимальная неприводимая метабелева подгруппа группы* $GL(n,\Omega)$ *сопряжена с одной и только с одной подгруппой* $\Gamma_{k_1\dots k_t}$, *определяемой некоторым разложением числа* n *вида* (4).

Доказательство. Рассмотрим $\Gamma_{k_1\dots k_t}=(a_1)(b_1)\dots$ $\dots(a_t)(b_t)\Omega^*$. Очевидно, $\Gamma_{k_1\dots k_t}\supset\Omega^*E_n$. Из (5) следует, что $(a_j,b_j)=\varepsilon_jE_n$, $(a_i,b_j)=(a_i,a_j)=(b_i,b_j)=E_n$ при $i\neq j$. Отсюда вытекает метабелевость группы $\Gamma_{k_1\dots k_t}$. Из этих же соотношений следует линейная независимость n^2 элементов

$$a_1^{\alpha_1}b_1^{\beta_1}\dots a_t^{\alpha_t}b_t^{\beta_t},\qquad 0\leqslant\alpha_j<k_j,\qquad 0\leqslant\beta_j<k_j.$$

Таким образом, $\Gamma_{k_1\dots k_t}$ — неприводимая метабелева подгруппа группы $GL(n,P)$ и $Z_1(\Gamma_{k_1\dots k_t})=\Omega^*E_n$. Отсюда и из теоремы 6 следует (i).

Далее,

$$\overline{\Gamma}=\Gamma_{k_1\dots k_t}/Z_1=(a_1Z_1)(b_1Z_1)\dots(a_kZ_1)(b_kZ_1),$$
$$Z_1=Z_1(\Gamma_{k_1\dots k_t}),$$

т. е. $\overline{\Gamma}$ — прямое произведение $2t$ циклических групп порядков $k_1,k_1,\dots,k_t,k_t$. (ii) доказано.

Пусть G — произвольная максимальная неприводимая метабелева подгруппа группы $GL(n,\Omega)$. Тогда, как при доказательстве теоремы 19.2, можно установить, что

$$G=(c_1)(d_1)\ \ldots\ (c_t)(d_t)\,\Omega^*,\qquad (c_\nu,\ d_\nu)=\varepsilon_\nu E_n,$$

где ε_ν — элемент порядка k_ν из Ω^*, элементы разных пар перестановочны, $k_1\ \ldots\ k_t=n$, $k_{j+1}|k_j$, $j=1,\ \ldots$ $\ldots,\ t-1$. Ясно, что $c_\nu^{k_\nu}$, $d_\nu^{k_\nu}\in\Omega^*E_n$. Так как поле Ω алгебраически замкнуто, то можно считать, что

$$c_\nu^{k_\nu}=d_\nu^{k_\nu}=E_n.$$

Следовательно, $G\cong\Gamma_{k_1\ldots k_t}$ и изоморфизм

$$\lambda c_1^{\alpha_1}d_1^{\beta_1}\ \ldots\ c_t^{\alpha_t}d_t^{\beta_t}\longmapsto\lambda a_1^{\alpha_1}b_1^{\beta_1}\ \ldots\ a_t^{\alpha_t}b_t^{\beta_t},\qquad \lambda\in\Omega^*,$$

можно продолжить до автоморфизма

$$\sum\lambda_{\alpha_1\ldots\beta_t}c_1^{\alpha_1}d_1^{\beta_1}\ \ldots\ c_t^{\alpha_t}d_t^{\beta_t}\longmapsto\sum\lambda_{\alpha_1\ldots\beta_t}a_1^{\alpha_1}b_1^{\beta_1}\ \ldots\ a_t^{\alpha_t}b_t^{\beta_t}$$

алгебры $\Omega_n=[G]=[\Gamma_{k_1\ldots k_t}]$. Отсюда вытекает, что группы G и $\Gamma_{k_1\ldots k_t}$ сопряжены в $GL(n,\ \Omega)$. ∎

Следствие 1. *Группа $GL(n,\Omega)$, где $\operatorname{char}\Omega\nmid n$, имеет столько несопряженных максимальных неприводимых метабелевых подгрупп, сколько существует неизоморфных абелевых групп порядка n.*

Следствие 2. *Две максимальные неприводимые метабелевы подгруппы группы $GL(n,\Omega)$ тогда и только тогда сопряжены в $GL(n,\Omega)$, когда изоморфны их фактор-группы по центру.*

3. Одна бесконечная цепь неприводимых нильпотентных подгрупп в $GL(n,\Omega)$. Следующая лемма справедлива при любом основном поле Δ.

Лемма 7. *Пусть*

$$h=\begin{bmatrix}0 & 1\\ E_{n-1} & 0\end{bmatrix}\in GL(n,\ \Delta),\tag{6}$$

а d — произвольная диагональная матрица из $SL(n,\Delta)$. Тогда в группе $GL(n,\Delta)$ есть диагональная матрица c такая, что

$$(c,\ h)=chc^{-1}h^{-1}=d.\tag{7}$$

Если c и f — диагональные матрицы из $GL(n,\Delta)$ и *$(c,h)=(f,h)$, то $f=\lambda c$, $\lambda\in\Delta^*$.*

Доказательство. Пусть

$$d = \operatorname{diag}[\delta_0, \delta_1, \ldots, \delta_{n-1}] \in SL(n, \Delta).$$

Как легко проверить, матрица

$$c = \operatorname{diag}[1, \gamma_1, \ldots, \gamma_{n-1}],$$

$$\gamma_j = \delta_1, \ldots, \delta_j, \quad j = 1, \ldots, n-1,$$

удовлетворяет условию (7).

Пусть теперь c и f — диагональные матрицы из $GL(n, \Delta)$ такие, что $(c, h) = (f, h)$. Тогда $(c^{-1}f, h) = E_n$. Однако простой подсчет показывает, что диагональная матрица, перестановочная с h, скалярна. Следовательно,

$$c^{-1}f = \lambda E_n, \qquad \lambda \in \Delta^*, \qquad f = \lambda c. \ ■$$

Пусть теперь Ω — алгебраически замкнутое поле, а $\operatorname{char}\Omega \nmid n$. С помощью леммы 7 мы построим возрастающую цепь неприводимых нильпотентных подгрупп $GL(n, \Omega)$, содержащую группы любого класса нильпотентности $l > 1$.

Сперва построим бесконечную цепь подгрупп группы диагональных невырожденных $n \times n$-матриц над Ω:

$$A_1, A_2, \ldots, A_j, \ldots,$$

где $A_1 = \Omega^* E_n$, а A_j при $j > 1$ есть множество всех таких диагональных матриц f из $GL(n, \Omega)$, что $(f, h) = fhf^{-1}h^{-1} \in A_{j-1}$, h — матрица вида (6) из $GL(n, \Omega)$.

Лемма 8. *Для любого $j \geqslant 1$ фактор-группа A_{j+1}/A_j является циклической группой порядка n.*

Доказательство. Рассмотрим сперва A_2. Пусть $c_2 = \operatorname{diag}[1, \varepsilon, \ldots, \varepsilon^{n-1}]$, где ε — элемент порядка n из Ω^*. Легко проверяется, что

$$c_2 h c_2^{-1} h^{-1} = \varepsilon E_n.$$

Если теперь

$$u h u^{-1} h^{-1} = \lambda E_n \in A_1 = \Omega^* E_n,$$

то $\lambda^n = 1$. Следовательно, $\lambda = \varepsilon^\alpha$, $0 \leqslant \alpha < n$. Отсюда, в силу леммы 7, находим

$$A_2 = (c_2)\, \Omega^* E_n = (c_2)\, A_1.$$

Таким образом, для $j = 1$ лемма доказана.

Пусть $j>1$, и пусть доказано, что $A_j=(c_j)A_{j-1}$, а $1, c_j, \ldots, c_j^{n-1}$ — полная система представителей смежных классов группы A_j по A_{j-1}. Покажем, что A_{j+1}/A_j — циклическая группа порядка n. Две матрицы u и v из A_{j+1} тогда и только тогда принадлежат одному и тому же смежному классу по A_j, когда матрицы (u, h) и (v, h) находятся в одном и том же смежном классе A_j по A_{j-1}. Действительно, пусть

$$uhu^{-1}h^{-1}=d_{j-1}vhv^{-1}h^{-1}, \qquad d_{j-1}\in A_{j-1}.$$

Тогда $v^{-1}uh=d_{j-1}hv^{-1}u$, откуда

$$(v^{-1}u, h)=d_{j-1}\in A_{j-1}, \quad v^{-1}u\in A_j, \quad u\in vA_j.$$

Обратно, пусть $u=d_jv$, $d_j\in A_j$. Тогда

$$(u, h)=d_jvhv^{-1}d_j^{-1}h^{-1}=d_j\left(vhv^{-1}h^{-1}\right)hd_j^{-1}h^{-1}=$$
$$=(v, h)(d_j, h)=d_{j-1}(v, h),$$
$$(u, h)\in(v, h)A_{j-1}.$$

В силу леммы 7 в A_{j+1} есть такая матрица c_{j+1}, что $(c_{j+1}, h)=\lambda c_j$, где $\det(\lambda c_j)=1$, $\lambda\in\Omega^*$. Очевидно, что $(c_{j+1}^\alpha, h)=\lambda^\alpha c_j^\alpha$. Отсюда и из предыдущего замечания следует, что $1, c_{j+1}, \ldots, c_{j+1}^{n-1}$ есть полная система представителей смежных классов A_{j+1} по A_j. ■

Введем теперь группы Γ_n^l, положив

$$\Gamma_n^l=(h)A_l, \qquad l>1.$$

Теорема 8. (i) Γ_n^l — *неприводимая нильпотентная подгруппа группы* $GL(n, \Omega)$ *класса* l.

(ii) *При* $j<l$ A_j *есть* j-*й гиперцентр группы* Γ_n^l, *т. е.* $A_j=Z_j(\Gamma_n^l)$.

(iii) Γ_n^l *максимальна среди нильпотентных подгрупп группы* $GL(n, \Omega)$ *класса* l.

(iv) $\Gamma_n^l : Z_1(\Gamma_n^l)=n^l$.

Доказательство. Группа Γ_n^l неприводима, ибо она содержит n^2 линейно независимых матриц $c_2^\alpha h^\beta$, $0\leqslant\alpha<n$, $0\leqslant\beta<n$. Из неприводимости Γ_n^l и включения $A_1=\Omega^*E_n\subset\Gamma_n^l$ следует, что A_1 есть центр группы Γ_n^l.

Пусть $1<j<l$ и доказано, что

$$A_{j-1}=Z_{j-1}(\Gamma_n^l).$$

Докажем равенство

$$A_j=Z_j(\Gamma_n^l). \tag{8}$$

С этой целью рассмотрим взаимный коммутант $(A_j,\ \Gamma_n^l)$:

$$(A_j,\ \Gamma_n^l)=(A_j,\ (h)\,A_l)=(A_j,\ (h))\subset A_{j-1},\qquad A_j\subset Z_j(\Gamma_n^l).$$

С другой стороны, каждая диагональная матрица группы $Z_j(\Gamma_n^l)$ принадлежит A_j. Если же $w\in\Gamma_n^l$ и w — недиагональная матрица, то $w\notin Z_j(\Gamma_n^l)$. Действительно,

$$w=h^\alpha c,\qquad 0<\alpha<n,\qquad c\in A_l,$$

$$(c_l,\ w)=(c_l,\ h^\alpha)=(c_l,\ h)^\alpha=\lambda c_{l-1}^\alpha,\qquad \lambda\in\Delta^*.$$

Так как $j-1<l-1$, то

$$\lambda c_{l-1}^\alpha\notin A_{j-1},\qquad w\notin Z_j(\Gamma_n^l).$$

Следовательно, (8) верно при $j<l$. Так как $\Gamma_n^l:A_l=n$, $A_l:Z_{l-1}(\Gamma_n^l)=n$, то

$$\Gamma_n^l:Z_{l-1}(\Gamma_n^l)=n^2.$$

Далее, $\Gamma_n^l=(h)\,(c_l)\,A_{l-1}$. Фактор-группа

$$\Gamma_n^l/A_{l-1}=(h)\,A_{l-1}/A_{l-1}\cdot(c_l)\,A_{l-1}/A_{l-1}$$

абелева, ибо $(h,\ c_l)\in A_{l-1}$. Значит,

$$Z_l(\Gamma_n^l)=\Gamma_n^l,$$

т. е. Γ_n^l — нильпотентная группа класса l. Очевидно, что $A_{l-1}:A_1=n^{l-2}$. Следовательно,

$$\Gamma_n^l:Z_1(\Gamma_n^l)=n^l.$$

(iv) доказано.

Остается доказать (iii). Пусть $\Gamma_n^l\subset\Gamma$, где Γ — нильпотентная подгруппа группы $GL(n,\ \Omega)$ класса нильпотентности l. Тогда $Z_1(\Gamma)=A_1$. Пусть $j<l$ и для всех i, меньших j, $Z_i(\Gamma)\subset A_i$. Покажем, что

$$Z_j(\Gamma)\subset A_j. \tag{9}$$

Для $g_j \in Z_j(\Gamma)$ имеем

$$d_{j-1} = (g_j, h) \in Z_{j-1}(\Gamma) \subset A_{j-1}, \qquad \det d_{j-1} = 1.$$

Следовательно, в группе A_j есть такой элемент d_j, что

$$(d_j, h) = (g_j, h) = d_{j-1}.$$

Отсюда $g_j = d_j v$, $(v, h) = 1$. Рассмотрим (c_2, g_j):

$$(c_2, g_j) = (c_2, d_j v) = d'_{j-1} \in Z_{j-1}(\Gamma) \subset A_{j-1}.$$

Следовательно, матрица $c_2 d_j v c_2^{-1} v^{-1} d_j^{-1}$, а с ней и матрица $v c_2^{-1} v^{-1}$ диагональны, $(c_2, g_j) = (c_2, v)$. Далее,

$$(h, d'_{j-1}) = (h, c_2 v c_2^{-1} v^{-1}) = h c_2 v c_2^{-1} v^{-1} h^{-1} v c_2 v^{-1} c_2^{-1} = \\ = h c_2 v c_2^{-1} h^{-1} c_2 v^{-1} c_2^{-1}.$$

Так как $c_2 h = \varepsilon h c_2$, то $h^{-1} c_2 = \varepsilon c_2 h^{-1}$. Следовательно,

$$(h, d'_{j-1}) = h c_2 v c_2^{-1} \varepsilon c_2 h^{-1} v^{-1} c_2^{-1} = \varepsilon h c_2 h^{-1} c_2^{-1} = \varepsilon \varepsilon^{-1} E_n = E_n.$$

Таким образом, $c_2 v c_2^{-1} v^{-1}$ — диагональная матрица, перестановочная с h. Так как $\det(c_2, v) = 1$, то $(c_2, v) = \varepsilon^{\alpha} E_n$, $v = \lambda h^{\alpha}$, $\lambda \in \Omega^*$, $g_j = \lambda d_j h^{\alpha}$. Рассмотрим

$$(c_{j+1}, g_j) = (c_{j+1}, \lambda d_j h^{\alpha}) = c_{j+1} d_j h^{\alpha} c_{j+1}^{-1} h^{-\alpha} d_j^{-1} = \\ = c_{j+1} d_j d_j^{-1} h^{\alpha} c_{j+1}^{-1} h^{-\alpha} = (c_{j+1}, h^{\alpha}) = \mu c_j^{\alpha} \in A_{j-1}, \quad \mu \in \Omega^*.$$

Отсюда получим $\alpha = 0$, $g_j = \lambda d_j$, т. е. (9) верно для $j < l$. В частности, $Z_{l-1}(\Gamma) \subset A_{l-1}$. Пусть теперь g — произвольный элемент группы Γ. Тогда

$$(g, h) = d_{l-1} \in Z_{l-1}(\Gamma) \subset A_{l-1}, \qquad \det d_{l-1} = 1.$$

Следовательно, в группе A_l есть такая матрица d_l, что $(d_l, h) = d_{l-1}$. Отсюда $g = d_l v$, $(v, h) = E_n$, $v = \lambda h^{\alpha}$, $g = \lambda d_l h^{\alpha} \in \Gamma_n^l$, $\Gamma = \Gamma_n^l$. ■

Следствие 1. *Для любого $l > 1$ в группе $GL(n, \Omega)$ есть конечная неприводимая нильпотентная класса l подгруппа $\mathfrak{G}$ порядка n^{l+1}.*

Доказательство. Положим $\mathfrak{G} = \Gamma_n^l \cap SL(n, \Omega)$. Очевидно, $\Gamma_n^l = \mathfrak{G}\Omega^* E_n$. Отсюда следует, что $\mathfrak{G}$ — неприводимая нильпотентная подгруппа группы $GL(n, \Omega)$ класса l. Далее,

$$\Gamma_n^l/\Omega^* E_n \cong \mathfrak{G}/\Omega^* E_n \cap \mathfrak{G}.$$

Согласно теореме 8

$$\Gamma_n^l : \Omega^* E_n = n^l.$$

Очевидно, что $\operatorname{card}(\Omega^* E_n \cap \mathfrak{G}) = n$. Следовательно,

$$\operatorname{card} \mathfrak{G} = n^{l+1}. \blacksquare$$

Лемма 9. *Пусть Γ — такая нильпотентная класса l неприводимая подгруппа группы $GL(n, \Omega)$, что фактор-группа $Z_2(\Gamma)/Z_1(\Gamma)$ содержит элемент порядка n. Тогда Γ сопряжена в $GL(n, \Omega)$ с некоторой подгруппой группы Γ_n^l.*

Доказательство. Очевидно, что $Z_1(\Gamma) \subset \Omega^* E_n$. Следовательно, можно считать, что $Z_1(\Gamma) = \Omega^* E_n$. Пусть $aZ_1(\Gamma)$ — элемент порядка n фактор-группы $Z_2(\Gamma)/Z_1(\Gamma)$. Тогда, согласно лемме 3, в группе Γ есть элемент b такой, что

$$(a, b) = \varepsilon E_n, \tag{10}$$

где ε — элемент порядка n из Ω^*. Так как $\Gamma \supset \Omega^* E_n$, а поле Ω алгебраически замкнуто, то a и b можно выбрать так, что

$$a^n = b^n = E_n. \tag{11}$$

Из равенств (10) и (11) следует, что в подходящем базисе пространства Ω^n матрицы a и b имеют вид

$$a = c_2 = \operatorname{diag}[1, \varepsilon, \ldots, \varepsilon^{n-1}], \quad b = h,$$

где h определяется формулой (6). Следовательно, заменяя Γ группой, сопряженной с ней, мы можем считать, что $c_2 \in Z_2(\Gamma)$, $h \in \Gamma$. Пусть теперь g — произвольный элемент группы Γ. Тогда

$$(c_2, g) = \varepsilon^\alpha E_n = (c_2, h^\alpha), \quad (c_2, h^{-\alpha} g) = E_n.$$

Следовательно, $h^{-\alpha} g$ — диагональная матрица, $\Gamma = (h)\Phi$, где Φ — централизатор c_2 в Γ, т. е. совокупность всех диагональных матриц группы Г. Так как $\Gamma_n^l = (h) A_l$, то для доказательства леммы достаточно установить справедливость включения $\Phi \subset A_l$. Положим $\Phi_j = \Phi \cap Z_j(\Gamma)$, $j = 1, \ldots, l$. Тогда $\Phi_1 = \Phi \cap Z_1(\Gamma) = A_1$. Пусть $j > 1$ и $\Phi_{j-1} \subset A_{j-1}$. Покажем, что $\Phi_j \subset A_j$. Для $\varphi \in \Phi_j$ имеем $(\varphi, h) \in \Phi$, $(\varphi, h) \in A_{j-1}$, $(\varphi, h) \in \Phi_{j-1}$. Группа A_j содержит φ по построению. Следовательно, $\Phi_j \subset A_j$;

$$\Phi = \Phi_l = \Phi \cap Z_l(\Gamma) = \Phi \cap \Gamma \subset A_l. \blacksquare$$

Теорема 9. *Пусть в разложении числа n все простые множители различны. Тогда каждая неприводимая нильпотентная подгруппа группы $GL(n, \Omega)$ класса l сопряжена в $GL(n, \Omega)$ с некоторой подгруппой группы Γ_n^l. Любые две неприводимые подгруппы группы $GL(n, \Omega)$, максимальные среди ее нильпотентных подгрупп заданного класса нильпотентности, сопряжены в ней.*

Доказательство. Пусть Г — неприводимая нильпотентная подгруппа группы $GL(n, \Omega)$ класса l. Так как число n не имеет квадратных делителей, то, в силу следствия 2.1, экспонента фактор-группы $Z_2(\Gamma)/Z_1(\Gamma)$ равна n. Следовательно, по лемме 9, Г сопряжена в $GL(n, \Omega)$ с некоторой подгруппой группы Γ_n^l. Если же Г максимальна среди нильпотентных класса l подгрупп группы $GL(n, \Omega)$, то Г сопряжена с Γ_n^l. $\blacksquare$

Нильпотентные неприводимые линейные группы над конечным полем изучались в статьях Супруненко, Апатенок [1], [2]. Полностью описаны максимальные нильпотентные неприводимые подгруппы группы $GL(n, \Delta)$ для конечного Δ. В частности, установлено, что в случае конечного Δ две максимальные нильпотентные неприводимые подгруппы $GL(n, \Delta)$ сопряжены, если сопряжены их центры.

§ 28. Неприводимые локально нильпотентные группы матриц

1. Редукция к абсолютно неприводимым группам. Фактор-группа по центру. Группа называется *локально нильпотентной*, если каждое конечное множество ее элементов порождает нильпотентную группу.

Всюду в этом пункте Δ — произвольное поле.

Теорема 1. *Пусть G — абсолютно неприводимая локально нильпотентная подгруппа группы $GL(n, \Delta)$. Тогда фактор-группа $G/Z_1(G)$ является периодической группой и* $\Pi(G/Z_1(G)) = \Pi(n)$.

Доказательство. Так как группа G абсолютно неприводима, то $Z_1(G) \subset \Delta^* E_n$. Каждый элемент g группы G содержится в некоторой абсолютно неприводимой нильпотентной подгруппе $\mathfrak{H}$ группы G. Действительно, если $g, g_2, \ldots, g_{n^2}$ — линейно независимые матрицы из G, то порождаемая ими группа $\mathfrak{H}$ нильпотентна, абсолютно неприводима и содержится в группе G. Согласно следствию 27.2.3

$$\Pi(\mathfrak{H}/Z_1(\mathfrak{H})) = \Pi(n).$$

С другой стороны,

$$Z_1(\mathfrak{H}) \subset Z_1(G) \subset \Delta^* E_n.$$

Следовательно, для любого $h \in \mathfrak{H}$ порядок элемента $hZ_1(\mathfrak{H})$ фактор-группы $\mathfrak{H}/Z_1(\mathfrak{H})$ совпадает с порядком элемента $hZ_1(G)$ фактор-группы $G/Z_1(G)$. Отсюда и вытекает теорема. ■

Теорема 2. *Пусть G — неприводимая локально нильпотентная подгруппа группы $GL(n, \Delta)$. Тогда $G/Z_1(G)$ — периодическая группа, причем* $\Pi(G/Z_1(G)) \subset \Pi(n)$.

Доказательство. Как и при доказательстве леммы 27.1, можно установить, что группа G содержится в локально нильпотентной подгруппе $\mathfrak{G}$ группы $GL(n, \Delta)$, обладающей следующими свойствами:

(i) $\mathfrak{G}$ — абсолютно неприводимая подгруппа группы $GL(r, \Sigma)$, $\Sigma : \Delta = m$, $mr = n$.

(ii) $$Z_1(\mathfrak{G}) = \Sigma^* E_r \supset Z_1(G).$$

По теореме 1

$$\Pi(\mathfrak{G}/Z_1(\mathfrak{G})) = \Pi(r).$$

Далее,

$$G/Z_1(G) = G/G \cap Z_1(\mathfrak{G}) \cong GZ_1(\mathfrak{G})/Z_1(\mathfrak{G}).$$

Следовательно,

$$\Pi(G/Z_1(G)) \subset \Pi(r) \subset \Pi(n). \blacksquare$$

Теорема 3. *Пусть G — неприводимая локально нильпотентная подгруппа группы $GL(n, \Delta)$, $[G]$ — линейная Δ-оболочка группы G, а $[Z_1(G)]$ — линейная Δ-оболочка группы $Z_1(G)$. Пусть центр алгебры $[G]$ совпадает с $[Z_1(G)]$. Тогда $\Pi(G/Z_1(G)) = \Pi(n\mu^{-1})$, где $\mu = [Z_1(G)] : \Delta$.*

Доказательство. Положим $[Z_1(G)] = FE_{n\mu^{-1}}$, где поле F есть образ неприводимой части $[Z_1(G)]$, $n_1 = n\mu^{-1}$. Тогда $G \subset GL(n_1, F)$, а центр алгебры $[G]$ совпадает с FE_{n_1}. С другой стороны, $[G] = T_l$, где T — тело, центр которого совпадает с $FE_{n_1 l^{-1}}$, $n_1 = l(T : E)$. Централизатор алгебры T_l в полной матричной алгебре E_{n_1} совпадает с DE_l, где D — тело, инверсно изоморфное телу T. Очевидно, $D \cap T = FE_{n_1 l^{-1}}$. Пусть теперь Σ — максимальное коммутативное подтело тела D. Тогда

$$(\Sigma : F)^2 = T : F = D : F = n_1 l^{-1} = m^2.$$

Группа $\mathfrak{G} = \Sigma^* G$ локально нильпотентна. Рассмотрим линейную F-оболочку $[\mathfrak{G}]$ группы $\mathfrak{G}$. Очевидно, что $[\mathfrak{G}] = \Sigma T_l$. Далее, ΣT_l — алгебра над Σ, $\Sigma T_l : \Sigma = m^2 l^2$. С другой стороны, элементы алгебры ΣT_l — матрицы порядка ml над Σ. Следовательно, $[\mathfrak{G}] = \Sigma_{ml}$, т. е. $\mathfrak{G}$ — абсолютно неприводимая подгруппа группы $GL(ml, \Sigma)$. По теореме 1

$$\Pi(\mathfrak{G}/\Sigma^* E_{ml}) = \Pi(ml) = \Pi(m^2 l) = \Pi(n_1).$$

Далее,

$$G/Z_1(G) \cong GZ_1(\mathfrak{G})/Z_1(\mathfrak{G}) = \mathfrak{G}/\Sigma^* E_{ml}.$$

Следовательно,

$$\Pi(G/Z_1(G)) = \Pi(n_1) = \Pi(n\mu^{-1}). \blacksquare$$

Теорема 4. *Пусть G — максимальная неприводимая локально нильпотентная подгруппа группы $GL(n, \Delta)$, а Σ — линейная Δ-оболочка группы $Z_1(G)$. Тогда G — максимальная абсолютно неприводимая локально нильпотентная подгруппа группы $GL(r, \Sigma)$, где $r = n(\Sigma : \Delta)^{-1}$.*

Эта теорема следует из теоремы 14.7.

Теорема 5. *Пусть G — максимальная неприводимая локально нильпотентная подгруппа группы $GL(n, \Delta)$, а Σ — линейная Δ-оболочка группы $Z_1(G)$. Тогда $\Pi(G/Z_1(G)) = \Pi(r)$, где $r = n(\Sigma : \Delta)^{-1}$.*

Доказательство. По теореме 4 G — абсолютно неприводимая подгруппа группы $GL(r, \Sigma)$. Отсюда и из теоремы 1 находим $\Pi(G/Z_1(G)) = \Pi(r)$. ∎

Теорема 6. *Группа $GL(n, \Delta)$ тогда и только тогда обладает абсолютно неприводимыми локально нильпотентными подгруппами, когда для любого $q \in \Pi(n)$ в Δ^* найдется элемент порядка q.*

Доказательство. Пусть в группе $GL(n, \Delta)$ есть абсолютно неприводимая локально нильпотентная подгруппа. Тогда, очевидно, в $GL(n, \Delta)$ есть абсолютно неприводимая нильпотентная подгруппа G. Согласно следствию 27.2.3

$$\Pi(G/Z_1(G)) = \Pi(n).$$

В силу леммы 27.5

$$\Pi(G/Z_1(G)) = \Pi(k),$$

где k — экспонента фактор-группы $Z_2(G)/Z_1(G)$. Следовательно,

$$\Pi(n) = \Pi(k). \tag{1}$$

Так как G — абсолютно неприводимая группа, то $Z_1(G) \subset \Delta^* E_n$. В силу леммы 3 в группе Δ^* есть элемент порядка k. Отсюда и из равенства (1) следует, что для любого числа q из $\Pi(n)$ в группе Δ^* найдется элемент порядка q.

Обратно, пусть для любого простого делителя q числа n в группе Δ^* есть элемент порядка q. Покажем, что группа $GL(n, \Delta)$ обладает абсолютно неприводимыми локально нильпотентными подгруппами. Пусть сперва $n = q^l$, где q — простое число. Рассмотрим группу $G = Q \wr N_{q^l}$, где Q — подгруппа порядка q группы Δ^*, а N_{q^l} — подгруппа Силова симметрической группы S_{q^l}. Если Ω — любое поле, содержащее поле Δ, то в силу леммы 15.4 G — неприводимая подгруппа в $GL(q^l, \Omega)$. Следовательно, G — абсолютно неприводимая подгруппа группы $GL(q^l, \Delta)$. Очевидно, G является конечной q-группой. Следовательно, группа G нильпотентна. Таким образом, для $n = q^l$ утверждение доказано. Пусть теперь

$$n = q_1^{l_1} \ldots q_k^{l_k}$$

— каноническое разложение числа n, а G_j, $j = 1, \ldots, k$, — абсолютно неприводимая локально нильпотентная подгруппа группы $GL\left(q_j^{l_j}, \Delta\right)$. Тогда кронекерово произведение $G_1 \dot{\times} \ldots \dot{\times} G_k$ является локально нильпотентной абсолютно неприводимой подгруппой в $GL(n, \Delta)$. ■

Теорема 6а. *В группе $GL(n, \Delta)$ тогда и только тогда имеются неприводимые локально нильпотентные подгруппы, когда поле Δ обладает таким расширением Σ, что $\Sigma : \Delta$ делит число n, а для каждого $p \in \Pi\left(\frac{n}{\Sigma : \Delta}\right)$ в Σ^* есть элемент порядка p.*

Доказательство. Пусть в группе $GL(n, \Delta)$ есть неприводимые локально нильпотентные подгруппы. Тогда в ней есть неприводимые нильпотентные подгруппы. Следовательно, в силу леммы 27.1, в $GL(r, \Sigma)$, где Σ — такое расширение поля Δ, что $\Sigma : \Delta | n$, а $r = \frac{n}{\Sigma : \Delta}$, есть абсолютно неприводимая нильпотентная подгруппа $\mathfrak{G}$. По теореме 6 для любого $p \in \Pi(r)$ в группе Σ^* есть элемент порядка p. Следовательно, необходимость доказана.

Докажем достаточность. Пусть поле Δ обладает таким расширением Σ, что для каждого $p \in \Pi\left(\frac{n}{\Sigma : \Delta}\right)$ в Σ^* есть элемент порядка p. Тогда, по теореме 6, в группе $GL(r, \Sigma)$, где $r = \frac{n}{\Sigma : \Delta}$, существует абсолютно неприводимая локальная нильпотентная подгруппа G такая, что $Z_1(G) = \Sigma^* E_r$. Изображая элементы σ поля Σ матрицами степени $\Sigma : \Delta$ над полем Δ, мы можем трактовать G как подгруппу группы $GL(n, \Delta)$. В силу леммы 14.4 G — неприводимая подгруппа группы $GL(n, \Delta)$. ■

2. Неприводимые локально нильпотентные подгруппы группы $GL(n, \Omega)$ над алгебраически замкнутым полем Ω. Пусть Ω — *алгебраически замкнутое поле.* Из теоремы 6 следует, что в группе $GL(n, \Omega)$ тогда и только тогда имеются неприводимые локально нильпотентные подгруппы, когда $\operatorname{char} \Omega \notin \Pi(n)$.

Лемма 1. *Пусть G — неприводимая локально нильпотентная подгруппа группы $GL(n, \Omega)$ такая, что $Z_1(G) = \Omega^* E_n$. Тогда $G_0 = G \cap SL(n, \Omega)$ является локально конечной группой, $\Pi(G_0) = \Pi(n)$,*

$$G = G_0\Omega^*. \qquad (2)$$

Доказательство. Равенство (2) очевидно. Из (2) следует, что G_0 — неприводимая локально нильпотентная подгруппа группы $GL(n, \Omega)$. Любое конечное множество элементов группы G_0 содержится в неприводимой нильпотентной подгруппе $H \subset SL(n, \Omega)$. По следствию 27.3.1 H — конечная группа и $\Pi(H) = \Pi(n)$. Отсюда и вытекает лемма. ∎

Лемма 2. *Локально нильпотентная неприводимая подгруппа G группы $GL(n, \Omega)$ мономиальна.*

Доказательство. Из свойств непродолжаемых разложений пространства на системы импримитивности группы следует, что достаточно установить импримитивность группы G при $n > 1$. Пусть группа G примитивна. Мы можем считать, что $Z_1(G) = \Omega^* E_n$. Из примитивности группы G следует, что $\Omega^* E_n$ — ее максимальный абелев нормальный делитель. Так как группа G разрешима, то $G : \Omega^* E_n < \infty$, $G_0 = G \cap SL(n, \Omega)$ — конечная группа. Отсюда следует, что G_0 — нильпотентная примитивная подгруппа в $GL(n, \Omega)$. В силу леммы 27.6 $n = 1$. ∎

Опишем теперь максимальные локально нильпотентные неприводимые подгруппы группы $GL(n, \Omega)$. Как уже отмечено выше, если $\operatorname{char} \Omega \in \Pi(n)$, то в группе $GL(n, \Omega)$ нет неприводимых локально нильпотентных подгрупп. Пусть $\operatorname{char} \Omega \notin \Pi(n)$. Сперва рассмотрим случай, когда $n = p^\nu$, где p — простое число. Введем одну неприводимую локально нильпотентную подгруппу Γ_{p^ν} группы $GL(p^\nu, \Omega)$, положив

$$\Gamma_{p^\nu} = (P \wr N_{p^\nu})\,\Omega^* E_n,$$

где $n = p^\nu$, P есть p-подгруппа Силова группы Ω^*, а N_{p^ν} есть p-подгруппа Силова симметрической группы S_{p^ν}. Как известно, группа N_{p^ν} транзитивна, а группа

$P \wr N_{p^\nu}$ является p-подгруппой Силова P_{p^ν} группы $GL(p^\nu, \Omega)$. В силу леммы 15.4 группа P_{p^ν} неприводима. Так как P_{p^ν} — локально конечная p-группа, то $\Gamma_{p^\nu} = P_{p^\nu}\Omega^* E_n$ является неприводимой локально нильпотентной подгруппой группы $GL(p^\nu, \Omega)$. ■

Лемма 3. *Всякая неприводимая локально нильпотентная подгруппа группы $GL(p^\nu, \Omega)$ сопряжена в $GL(p^\nu, \Omega)$ с некоторой подгруппой группы Γ_{p^ν}.*

Доказательство. Пусть G — неприводимая локально нильпотентная подгруппа группы $GL(p^\nu, \Omega)$. Мы можем считать, что $G \supset \Omega^* E_{p^\nu}$. Согласно лемме 1 $G = G_0\Omega^*$, где $G_0 = G \cap SL(p^\nu, \Omega)$, $\Pi(G_0) = \Pi(p^\nu) = \{p\}$. Таким образом, G_0 есть p-группа. G_0 содержится в некоторой p-подгруппе Силова Q группы $GL(p^\nu, \Omega)$. Согласно лемме 25.6 $tQt^{-1} = P_{p^\nu}$, где $t \in GL(p^\nu, \Pi)$. Отсюда

$$tGt^{-1} = tG_0t^{-1}\Omega^* E_{p^\nu} \subset P_{p^\nu}\Omega^* E_{p^\nu} = \Gamma_{p^\nu}. \blacksquare$$

Следствие 1. *Γ_{p^ν} — максимальная неприводимая локально нильпотентная подгруппа группы $GL(p^\nu, \Omega)$. Любые две максимальные неприводимые локально нильпотентные подгруппы группы $GL(p^\nu, \Omega)$ сопряжены в ней.*

Построим теперь одну неприводимую локально нильпотентную подгруппу Γ_n группы $GL(n, \Omega)$. Пусть

$$n = p_1^{\nu_1} \ldots p_k^{\nu_k}$$

— каноническое разложение числа n. Положим

$$\mathfrak{H}_n = P_{p_1^{\nu_1}} \dot{\times} \ldots \dot{\times} P_{p_k^{\nu_k}}, \qquad \Gamma_n = \mathfrak{H}_n \Omega^* E_n.$$

Так как группы $P_{p_i^{\nu_i}}$ неприводимы и локально нильпотентны, то Γ_n — неприводимая локально нильпотентная подгруппа группы $GL(n, \Omega)$.

Теорема 7. *Всякая неприводимая локально нильпотентная подгруппа группы $GL(n, \Omega)$ сопряжена в $GL(n, \Omega)$ с некоторой подгруппой группы Γ_n. Любая максимальная неприводимая локально нильпотентная подгруппа группы $GL(n, \Omega)$ сопряжена в $GL(n, \Omega)$ с группой Γ_n.*

Доказательство. Пусть G — неприводимая локально нильпотентная подгруппа группы $GL(n, \Omega)$. Мы можем считать, что $\Omega^* E_n \subset G$. Тогда $G = G_0 \Omega^* E_n$, $G_0 = G \cap SL(n, \Omega)$. Согласно лемме 1, G_0 — периодическая группа и $\Pi(G_0) = \Pi(n)$. Следовательно, G_0 — прямое произведение $G_0 = \mathfrak{P}_1 \times \ldots \times \mathfrak{P}_k$, где $\mathfrak{P}_j$ есть p_j-подгруппа Силова группы G_0, $j = 1, 2, \ldots, k$. В силу леммы 16.4, неприводимые части группы $\mathfrak{P}_j$ попарно эквивалентны. По теореме 2 степень неприводимой части группы $\mathfrak{P}_j$ делит число $p_j^{\nu_j}$, $j = 1, 2, \ldots, k$. Отсюда, применив теорему 16.3, получим: $G_0 = \overline{\mathfrak{P}}_1 \dot{\times} \ldots \dot{\times} \overline{\mathfrak{P}}_k$, где $\overline{\mathfrak{P}}_j$ — неприводимая подгруппа группы $GL\left(p_j^{\nu_j}, \Omega\right)$, изоморфная $\mathfrak{P}_j$, $j = 1, 2, \ldots, k$, а $\dot{\times}$ есть знак кронекерова произведения групп. Подгруппа $\overline{\mathfrak{P}}_j$ сопряжена в $GL\left(p_j^{\nu_j}, \Omega\right)$ с некоторой подгруппой группы $\mathfrak{P}_{p_j}^{\nu_j}$. Следовательно, G_0 сопряжена в $GL(n, \Omega)$ с подгруппой группы $\mathfrak{H}$, а G — с подгруппой группы Γ_n. ■

3. Максимальные неприводимые локально нильпотентные группы матриц над произвольным полем Δ. В силу теоремы 4 *при изучении максимальных неприводимых локально нильпотентных матричных групп можно ограничиться случаем абсолютно неприводимых групп.*

Теорема 8. *Пусть $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ — каноническое разложение числа n, G — максимальная абсолютно неприводимая локально нильпотентная подгруппа группы $GL(n, \Delta)$. Тогда $G = G_1 \dot{\times} \ldots \dot{\times} G_k$, где G_j — максимальная локально нильпотентная абсолютно неприводимая подгруппа группы $GL\left(p_j^{\alpha_j}, \Delta\right)$, $j = 1, \ldots, k$.*

Доказательство. Так как группа G абсолютно неприводима и максимальна среди локально нильпотентных подгрупп в $GL(n, \Omega)$, то $Z_1(G) = \Delta^* E_n$. По теореме 1

$$\Pi(G/\Delta^* E_n) = \Pi(n) = \{p_1, \ldots, p_k\}.$$

Следовательно,

$$G/\Delta^* E_n = H_1/\Delta^* E_n \times \ldots \times H_k/\Delta^* E_n, \tag{3}$$

где $H_j/\Delta^* E_n$ есть p_j-подгруппа Силова группы $G/\Delta^* E_n$. Для $i \neq j$ группы H_i и H_j перестановочны поэлементно.

Действительно, пусть $a \in H_i$, $b \in H_j$, $i \neq j$. Тогда $ab = \lambda ba$, $\lambda \in \Delta^*$, $a^{p_i^\gamma} \in \Delta^* E_n$, $b^{p_i^\delta} \in \Delta^* E_n$. Отсюда

$$\lambda^{p_i^\gamma} = \lambda^{p_i^\delta} = 1, \quad \lambda = 1, \quad ab = ba.$$

Пусть теперь $\mathfrak{B}_i$ — линейная Δ-оболочка группы H_i. Докажем, что центр C алгебры $\mathfrak{B}_i$ совпадает с ΔE_n. Очевидно, $C \supset \Delta E_n$. С другой стороны, элементы центра C перестановочны с каждым элементом группы G. Следовательно, $C \subset \Delta E_n$, $C = \Delta E_n$. Из (3) находим

$$G = H_1 U, \tag{4}$$

где $U = H_2 \ldots H_k$, а взаимный коммутант $(H_1, U) = (E_n)$. Неприводимые части групп H_1 попарно эквивалентны (лемма 16.4). Следовательно, в подходящем базисе пространства Δ^n матрицы $h_1 \in H_1$ можно записать в виде

$$h_1 = g_1 \dot{\times} E_{nn_1^{-1}}$$

где g_1 пробегает неприводимую локально нильпотентную подгруппу G_1 группы $GL(n_1, \Delta)$, когда h_1 пробегает H_1. Так как центр алгебры $\mathfrak{B}_1$ совпадает с ΔE_n, то центр линейной Δ-оболочки $[G_1]$ группы G_1 равен ΔE_{n_1}, а центр группы G_1 равен $\Delta^* E_{n_1}$. Следовательно, к группе G_1 применима теорема 3, т. е.

$$\Pi(G_1/Z_1(G_1)) = \Pi(n_1).$$

Очевидно, что $G_1/Z_1(G_1) \cong H_1/\Delta^* E_n$. Так как $H_1/\Delta^* E_n$ есть p_1-подгруппа Силова группы $G/\Delta^* E_n$, то

$$n_1 = p_1^{\beta_1}, \quad 0 < \beta_1 \leqslant \alpha_1.$$

Рассмотрим теперь группу U (см. формулу (4)). Центр ее линейной Δ-оболочки $[U]$ совпадает с ΔE_n, неприводимые ее части попарно эквивалентны. Пусть n_2 — степень неприводимой части алгебры $[U]$. Тогда, применяя предыдущие рассуждения, находим

$$n_2 = p_2^{\beta_2} \ldots p_k^{\beta_k}, \quad 0 < \beta_j \leqslant \alpha_j, \quad j = 2, \ldots, k.$$

Очевидно, $n_1 n_2 \leqslant n$. К группам G_1, H_1, U применима теорема 16.3, следовательно,

$$G = G_1 \dot{\times} U_1, \tag{5}$$

где G_1 — абсолютно неприводимая локально нильпотентная подгруппа в $GL(p_1^{\alpha_1}, \Delta)$, а $U_1 \cong U$ — абсолютно неприводимая локально нильпотентная подгруппа в $GL(np_1^{-\alpha_1}, \Delta)$,

$$Z_1(G_1) = \Delta^* E_{p_1^{\alpha_1}}, \qquad Z_1(U_1) = \Delta^* E_{np_1^{-\alpha_1}}.$$

Так как G максимальна среди локально нильпотентных подгрупп группы $GL(n, \Delta)$, то G_1 максимальна среди локально нильпотентных подгрупп группы $GL(np_1^{-\alpha_1}, \Delta)$, а U_1 — среди локально нильпотентных подгрупп группы $GL(np_1^{-\alpha_1}, \Delta)$. Применяя предыдущие рассуждения к группе U_1, с помощью формулы (5) получим требуемое. ■

Доказанная теорема сводит описание максимальных абсолютно неприводимых локально нильпотентных матричных групп степени n к случаю, когда n есть степень простого числа.

Рассмотрим теперь максимальные абсолютно неприводимые локально нильпотентные подгруппы группы $GL(p^\alpha, \Delta)$, где p — простое число.

Теорема 9. (i). *Пусть G — максимальная абсолютно неприводимая локально нильпотентная подгруппа группы $GL(p^\alpha, \Delta)$. Тогда фактор-группа $G/\Delta^* E_{p^\alpha}$ является p-подгруппой Силова проективной группы $PGL(p^\alpha, \Delta) = GL(p^\alpha, \Delta)/\Delta^* E_{p^\alpha}$.*

(ii) *Пусть $H/\Delta^* E_{p^\alpha}$ есть p-подгруппа Силова группы $PGL(p^\alpha, \Delta)$, а H — абсолютно неприводимая подгруппа группы $GL(p^\alpha, \Delta)$. Тогда H — максимальная локально нильпотентная подгруппа группы $GL(p^\alpha, \Delta)$.*

Доказательство. (ii) Пусть Ω — алгебраически замкнутое поле, содержащее поле Δ. Очевидно, что

$$GL(p^\alpha, \Delta)/\Delta^* E_{p^\alpha} \cong GL(p^\alpha, \Delta)\, \Omega^* E_{p^\alpha}/\Omega^* E_{p^\alpha} \subset$$
$$\subset GL(p^\alpha, \Omega)/\Omega^* E_{p^\alpha}.$$

Следовательно, группа $H/\Delta^* E_{p^\alpha}$ изоморфна некоторой p-подгруппе группы $GL(p^\alpha, \Omega)/\Omega^* E_{p^\alpha}$. Любая p-подгруппа группы $GL(p^\alpha, \Omega)/\Omega^* E_{p^\alpha}$ содержится в некоторой

p-подгруппе Силова $\mathscr{P}/\Omega^* E_{p^\alpha}$ группы $GL(p^\alpha, \Omega)/\Omega^* E_{p^\alpha}$. Группу $\mathscr{P}$ можно записать в виде

$$\mathscr{P} = \mathscr{P}_0 \Omega^* E_{p^\alpha}, \qquad \mathscr{P}_0 = SL(p^\alpha, \Omega) \cap \mathscr{P}.$$

Так как

$$\mathscr{P}/\Omega^* E_{p^\alpha} \cong \mathscr{P}_0/(\eta E_{p^\alpha}),$$

где η — элемент порядка p^α из Ω^*, то $\mathscr{P}_0$ является p-подгруппой в $GL(p^\alpha, \Omega)$. Отсюда следует локальная конечность группы $\mathscr{P}_0$ и локальная нильпотентность групп $\mathscr{P}$ и H. Пусть теперь $H \subset H_1$, где H_1 — локально нильпотентная подгруппа группы $GL(p^\alpha, \Delta)$. Тогда

$$Z_1(H_1) = Z_1(H) = \Delta^* E_{p^\alpha}, \qquad \Pi(H_1/\Delta^* E_{p^\alpha}) = \{p\}.$$

Следовательно, $H_1/\Delta^* E_{p^\alpha}$ есть p-подгруппа группы $GL(p^\alpha, \Delta)/\Delta^* E_{p^\alpha}$ и

$$H_1/\Delta^* E_{p^\alpha} \supset H/\Delta^* E_{p^\alpha}.$$

Отсюда $H_1 = H$. (ii) доказано.

Докажем (i). Из условий теоремы вытекает

$$\Pi(G/\Delta^* E_{p^\alpha}) = \{p\}.$$

Следовательно, $G/\Delta^* E_{p^\alpha}$ — подгруппа некоторой p-подгруппы Силова $H/\Delta^* E_{p^\alpha}$ группы $PGL(p^\alpha, \Delta)$. В силу (ii) группа H локально нильпотентна. Следовательно, $G = H$. ■

Максимальные неприводимые локально нильпотентные подгруппы группы $GL(n, R)$ над полем вещественных чисел R описаны Супруненко в статье [9], где установлены следующие теоремы:

1. *Если нечетное число $n > 1$, то в $GL(n, R)$ нет неприводимых локально нильпотентных подгрупп.*

2. *Если n — четное число, не являющееся степенью двойки, то в $GL(n, R)$ с точностью до сопряженности имеется только одна максимальная неприводимая локально нильпотентная подгруппа.*

3. *Если $n = 2^\alpha$ ($\alpha \geqslant 1$), то множество всех максимальных неприводимых локально нильпотентных подгрупп группы $GL(n, R)$ разбивается на два класса сопряженных подгрупп.*

4. *Любая неприводимая локально нильпотентная подгруппа в $GL(n, R)$ при $n > 2$ импримитивна.*

§ 29. Приводимые локально нильпотентные группы

1. Группа $\Gamma_k(F)$. Пусть Δ — произвольное поле, F — неприводимая подгруппа группы $GL(m, \Delta)$, тело D — централизатор группы F в алгебре Δ_m, $k > 1$ — целое число, а $n = km$. Введем подгруппу $\Gamma_k(F)$ группы $GL(n, \Delta)$, положив

$$\Gamma_k(F) = (F \dot{\times} E_k)\, T_k(D), \tag{1}$$

где $F \dot{\times} E_k$ состоит из всех матриц вида

$$f \dot{\times} E_k = \operatorname{diag}[f, \ldots, f], \qquad f \in F,$$

а $T_k(D)$ — группа всех матриц вида

$$\begin{bmatrix} E_m & d_{12} & \ldots & d_{1k} \\ 0 & E_m & \ldots & d_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & E_m \end{bmatrix}, \qquad d_{ij} \in D \subset \Delta_m. \tag{2}$$

Очевидно, что $\Gamma_k(F)$ — прямое произведение своих подгрупп $F \dot{\times} E_k$ и $T_k(D)$.

Теорема 1. *Группа $\Gamma_k(F)$ неразложима* *).

Доказательство. Как легко видеть, подмножество M из Δ_n тогда и только тогда разложимо, когда централизатор M в Δ_n содержит элемент, минимальный полином которого равен $x(x-1)$. Покажем, что каждая матрица c из централизатора C группы $\Gamma_k(F)$ в алгебре Δ_n либо нильпотентна, либо обратима, и теорема будет доказана. Пусть

$$c = \begin{bmatrix} c_{11} & \ldots & c_{1k} \\ \cdot & \cdot & \cdot \\ c_{k1} & \ldots & c_{kk} \end{bmatrix}, \qquad c_{ij} \in \Delta_m.$$

*) То есть Δ^n нельзя представить в виде прямой суммы двух нетривиальных инвариантных относительно $\Gamma_k(F)$ подпространств.

Так как матрица c перестановочна с каждой матрицей группы $F \times E_k$, то $c_{ij} \in D$. Покажем сперва, что $c_{ij} = 0$ при $i > j$. Очевидно, достаточно установить, что $c_{i1} = 0$ при $i = 2, \ldots, k$. Пусть

$$u = \begin{bmatrix} E_m & 0 & \ldots & d_{1\nu} & 0 \\ 0 & E_m & \ldots & 0 & 0 \\ . & . & . & . & . \\ 0 & 0 & \ldots & 0 & E_m \end{bmatrix}, \quad d_{1\nu} \in D^*, \quad \nu = 2, \ldots k.$$

Тогда из равенства $cu = uc$ получаем $c_{11} = c_{11} + d_{1\nu}c_{\nu 1}$. Отсюда $c_{\nu 1} = 0$. Следовательно,

$$c = \begin{bmatrix} c_1 & c_{12} & \ldots & c_{1k} \\ 0 & c_2 & \ldots & c_{2k} \\ . & . & . & . \\ 0 & 0 & \ldots & c_k \end{bmatrix}, \quad c_i \in D.$$

Очевидно, что

$$\begin{bmatrix} c_i & c_{i,i+1} \\ 0 & c_{i+1} \end{bmatrix}\begin{bmatrix} E_m & E_m \\ 0 & E_m \end{bmatrix} = \begin{bmatrix} E_m & E_m \\ 0 & E_m \end{bmatrix}\begin{bmatrix} c_i & c_{i,i+1} \\ 0 & c_{i+1} \end{bmatrix}.$$

Отсюда

$$c_i = c_{i+1}, \qquad c_1 = c_2 = \ldots = c_k = d \in D.$$

Следовательно, матрица c либо обратима, либо нильпотентна. ∎

По теореме 13.5 $T_k(D)$ — нильпотентная группа класса нильпотентности $k - 1$. Следовательно, $\Gamma_k(F)$ тогда и только тогда нильпотентна (локально нильпотентна), когда нильпотентна (локально нильпотентна) группа F. В дальнейшем мы докажем, что любая неразложимая максимальная локально нильпотентная подгруппа группы $GL(n, \Delta)$, где Δ — совершенное поле, сопряжена в $GL(n, \Delta)$ с группой $\Gamma_k(F)$ при подходящих F и k.

2. Эквивалентность неприводимых частей неразложимой локально нильпотентной группы. Здесь будет доказана

Теорема 2. *Неприводимые части локально нильпотентной неразложимой подгруппы группы $GL(n, \Delta)$, где Δ — произвольное поле, попарно эквивалентны.*

Доказательству теоремы предпошлем ряд лемм. Пусть Δ — произвольное поле, а $G_{m,l}$ — нильпотентная подгруппа группы $GL(m+l, \Delta)$, матрицы g которой имеют вид

$$g=\begin{bmatrix} a_g & b_g \\ 0 & c_g \end{bmatrix}, \qquad (3)$$

где

$$\gamma_1\colon\ g\mapsto a_g, \qquad \gamma_2\colon\ g\mapsto c_g$$

— неприводимые неэквивалентные части группы $G_{m,l}$ степени m и l соответственно.

Лемма 1. *Пусть $h\in G_{m,l}$, $\gamma_1(h)=E_m$, $\gamma_2(h)=E_l$, тогда $h=E_{m+l}$.*

Доказательство. Пусть

$$h=\begin{bmatrix} E_m & b \\ 0 & E_l \end{bmatrix}\in G_{m,l}, \qquad b\neq 0. \qquad (4)$$

Для g из $G_{m,l}$ коммутатор (g, h) либо равен E_{m+l}, либо имеет вид (4). Отсюда и из нильпотентности группы $G_{m,l}$ следует, что в $G_{m,l}$ имеется такая матрица $h_1\neq E_{m+1}$ вида (4), что

$$(g, h_1)=E_{m+l}$$

для всех g из $G_{m,l}$. Пусть

$$h_1=\begin{bmatrix} E_m & b_1 \\ 0 & E_l \end{bmatrix}, \qquad b_1\neq 0.$$

Тогда из (3) находим

$$(g, h_1)=\begin{bmatrix} E_m & a_g b_1 c_g^{-1}-b_1 \\ 0 & E_l \end{bmatrix}=E_{m+l}.$$

Отсюда

$$a_g b_1 c_g^{-1}-b_1=0, \qquad a_g b_1=b_1 c_g.$$

В силу леммы Шура (лемма 13.1) $b_1=0$. Это противоречие и доказывает лемму. ∎

Из леммы 1 вытекает

Лемма 2. *Если $h\in G_{m,l}$, $\gamma_1(h)\in Z_1(\operatorname{Im}\gamma_1)$, $\gamma_2(h)\in Z_1(\operatorname{Im}\gamma_2)$, то $h\in Z_1(G_{m,l})$.*

Лемма 3. *Индекс $Z_1(G_{m,l})$ в $G_{m,l}$ конечен и не делится на* $\operatorname{char}\Delta$.

Доказательство. Положим

$$\Gamma_1 = \operatorname{Im}\gamma_1, \qquad \Gamma_2 = \operatorname{Im}\gamma_2.$$

По теореме 27.1 индекс $Z_1(\Gamma_i)$ в Γ_i конечен и не делится на $\operatorname{char}\Delta$ ($i = 1, 2$). Введем две подгруппы группы $G_{m,l}$:

$$H_1 = \gamma_1^{-1}(Z_1(\Gamma_1)), \qquad H_2 = \gamma_2^{-1}(Z_1(\Gamma_2)).$$

В силу леммы 2

$$Z_1(G_{m,l}) = H_1 \cap H_2.$$

Так как H_1 и H_2 — подгруппы конечного индекса, то и $Z_1(G_{m,l})$ — подгруппа конечного индекса в $G_{m,l}$. Далее,

$$\operatorname{char}\Delta \notin \Pi(G_{m,l}/Z_1(G_{m,l})),$$

ибо

$$\operatorname{char}\Delta \notin \Pi(G_{m,l}/H_i), \qquad i = 1, 2. \blacksquare$$

Лемма 4. *Группа $G_{m,l}$ вполне приводима.*

Доказательство. Рассмотрим линейную Δ-оболочку C группы $Z_1(G_{m,l})$. Элементы c из C имеют вид

$$c = \begin{bmatrix} c_1 & c_3 \\ 0 & c_2 \end{bmatrix},$$

где $c_1 \in \Sigma_1$, $c_2 \in \Sigma_2$, а Σ_1 и Σ_2 — конечные расширения поля Δ. Следовательно, если c — нильпотентный элемент, то

$$c_1 = 0, \qquad c_2 = 0.$$

Но тогда для любого g из $G_{m,l}$

$$a_g c_3 = c_3 c_g.$$

Отсюда и из леммы Шура вытекает, что

$$c_3 = 0, \qquad c = 0.$$

Таким образом, C — вполне приводимая алгебра, $Z_1(G)$ — вполне приводимая группа. В силу леммы 3 и теоремы 17.1 группа $G_{m,l}$ вполне приводима. $\blacksquare$

Лемма 5. *Лемма 4 остается верной, если вместо нильпотентности группы $G_{m,l}$ предположить локальную нильпотентность.*

Доказательство. Локально нильпотентная подгруппа группы $GL(m+l, \Delta)$ содержится в линейной Δ-оболочке некоторой нильпотентной подгруппы. ■

Отметим еще, что матрицу t из $GL(m+l, \Delta)$, трансформирующую матрицы группы $G_{m,l}$ одновременно к виду $\operatorname{diag}[a_g, c_g]$, можно выбрать такой:

$$t = \begin{bmatrix} E_m & b \\ 0 & E_l \end{bmatrix}. \tag{5}$$

Действительно, пусть

$$u_1, \ldots, u_{m+l} \tag{6}$$

— базис пространства Δ^{m+l}, в котором матрицы группы $G_{m,l}$ имеют вид (3). Тогда подпространство Q_1, натянутое на векторы

$$u_1, \ldots, u_m,$$

инвариантно относительно $G_{m,l}$. Так как группа $G_{m,l}$ вполне приводима, то

$$\Delta^n = Q_1 \dotplus Q_2,$$

где Q_2 — тоже инвариантное относительно $G_{m,l}$ подпространство. Матрица t_1, выражающая базис

$$u_1, \ldots, u_m, g_1, \ldots, g_l,$$

где $g_1, \ldots, g_l$ — базис подпространства Q_2, через базис (6), имеет вид

$$t_1 = \begin{bmatrix} E_m & b_1 \\ 0 & d \end{bmatrix}.$$

Следовательно,

$$t_1^{-1} g t_1 = \operatorname{diag}[a_g, d^{-1} c_g d].$$

Если теперь $t_2 = \operatorname{diag}[E_m, d^{-1}]$, $t = t_1 t_2$, то t имеет вид (5), а

$$t^{-1} g t = \operatorname{diag}[a_g, c_g]$$

для любого g из $G_{m,l}$.

Доказательство теоремы 2. Пусть G — локально нильпотентная подгруппа группы $GL(n, \Delta)$. Подходящим выбором базиса пространства Δ^n матрицы g

группы G можно одновременно трансформировать к виду

$$g=\begin{bmatrix} a_1(g) & a_{12}(g) & \dots & a_{1k}(g) \\ 0 & a_2(g) & \dots & a_{2k}(g) \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & a_k(g) \end{bmatrix}, \tag{7}$$

где

$$\gamma_j\colon\ g\mapsto a_j(g)$$

— неприводимая часть группы G степени n_j, $j=1, \dots, k$,

$$n_1+\dots+n_k=n.$$

Докажем следующее утверждение, равносильное теореме 2:

($*$) *Пусть среди неприводимых частей γ_j есть две неэквивалентные. Тогда группа G разложима.*

Ясно, что есть такое i, $1\leqslant i<k$, что γ_i и γ_{i+1} неэквивалентны. Когда g пробегает группу G, матрица

$$\begin{bmatrix} a_i(g) & a_{i,\,i+1}(g) \\ 0 & a_{i+1}(g) \end{bmatrix}$$

пробегает локально нильпотентную подгруппу группы $GL(n_i+n_{i+1}, \Delta)$. В силу леммы 5 мы можем считать, что

$$a_{i,\,i+1}(g)=0$$

при любом g из G. Следовательно, перейдя к другому базису пространства Δ^n, можно γ_i и γ_{i+1} поменять местами. Таким образом, мы вправе считать, что в (7) эквивалентные неприводимые части γ_j расположены рядом, т. е. если γ_i и γ_j, где $i<j$, эквивалентны, а $i<\nu<j$, то γ_ν и γ_i эквивалентны. Будем доказывать утверждение ($*$) индукцией по числу k. Для $k=2$ оно верно в силу леммы 5. Пусть $k>2$ и для случая $k-1$ неприводимых частей утверждение ($*$) верно. Так как среди неприводимых частей γ_j есть неэквивалентные, то, по индуктивному предположению, либо группа G_{k-1} матриц

$$g_{k-1}=\begin{bmatrix} a_1(g) & \dots & a_{1,\,k-1}(g) \\ \cdot & \cdot & \cdot \\ 0 & \dots & a_{k-1}(g) \end{bmatrix},$$

либо группа $\bar{G}_{k-1}$ матриц

$$\bar{g}_{k-1} = \begin{bmatrix} a_2(g) & \dots & a_{2k}(g) \\ \cdot & \cdot \cdot \cdot \cdot & \cdot \\ 0 & \dots & a_k(g) \end{bmatrix}$$

разложима. Пусть разложима группа G_{k-1}. Тогда матрицам g из группы G можно придать вид

$$g = \begin{bmatrix} & a_{1k}(g) \\ g_{k-1}(g) & \vdots \\ & a_{k-1,\,k}(g) \\ 0 & a_k(g) \end{bmatrix} = \begin{bmatrix} & & a_{1k}(g) \\ A_1(g) & 0 & \vdots \\ & & a_{\tau k}(g) \\ 0 & A_2(g) & B(g) \\ 0 & 0 & a_k(g) \end{bmatrix}, \tag{8}$$

где

$$A_1(g) = \begin{bmatrix} a_1(g) & \dots & a_{1\tau}(g) \\ 0 & \dots & a_{2\tau}(g) \\ \cdot & \cdot \cdot \cdot \cdot & \cdot \\ 0 & \dots & a_\tau(g) \end{bmatrix}, \tag{9}$$

причем неприводимые части γ_i, $1 \leqslant i \leqslant \tau$, неэквивалентны с γ_k. Введем отображение f_τ (см. (8) и (9)):

$$f_\tau\colon\ g \mapsto \begin{bmatrix} a_\tau(g) & a_{\tau k}(g) \\ 0 & a_k(g) \end{bmatrix}. \tag{10}$$

В силу (8) и (9) для

$$x,\ y \in G \qquad f_\tau(xy) = f_\tau(x) f_\tau(y),$$

т. е. f_τ — гомоморфизм. Следовательно, $\operatorname{Im} f_\tau$ — локально нильпотентная группа. В силу леммы 5 и формулы (5) существует такая матрица

$$t = \begin{bmatrix} E_{n_\tau} & b \\ 0 & E_{n_k} \end{bmatrix},$$

что

$$t^{-1} \begin{bmatrix} a_\tau(g) & a_{\tau k}(g) \\ 0 & a_k(g) \end{bmatrix} t = \operatorname{diag}[a_\tau(g),\ a_k(g)] \tag{11}$$

для любого $g \in G$. Положим теперь

$$t_\tau = \begin{bmatrix} E_{n_1 \dots n_\tau} & \begin{matrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ b \end{matrix} \\ 0 & E_{n_{\tau+1} \dots n_k} \end{bmatrix}.$$

Тогда, в силу (8) и (11), матрица $t_\tau^{-1} g t_\tau$ будет иметь вид (8), но такой, что

$$a_{\tau k}(g) = 0$$

при любом $g \in G$. После этого введем подобное (10) отображение

$$f_{\tau-1}\colon\ g \mapsto \begin{bmatrix} a_{\tau-1}(g) & a_{\tau-1,\,k}(g) \\ 0 & a_k(g) \end{bmatrix}$$

и устраним в (8) $a_{\tau-1,\,k}(g)$. Поступая так τ раз, мы докажем разложимость группы G. Случай, когда разложима группа $\overline{G}_{k-1}$, рассматривается аналогично. ■

3. Неразложимые локально нильпотентные группы. Пусть G — локально нильпотентная неразложимая подгруппа группы $GL(n, \Delta)$. Тогда, согласно теореме 2, в некотором базисе пространства Δ^n матрицы g группы G имеют вид

$$g = \begin{bmatrix} a(g) & a_{12}(g) & \dots & a_{1k}(g) \\ 0 & a(g) & \dots & a_{2k}(g) \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & a(g) \end{bmatrix}, \tag{12}$$

где $\gamma\colon\ g \to a(g)$ — неприводимое представление степени m группы G, $km = n$. Положим $\operatorname{Im}\gamma = A$, а централизатор группы A в алгебре Δ_m обозначим буквой D. Справедлива

Теорема 3. *Пусть A является d-группой. Тогда группа G сопряжена в $GL(n, \Delta)$ с некоторой подгруппой группы*

$$\Gamma_k(A) = (A \dot{\times} E_k)\, T_k(D). \tag{13}$$

В частности, если G максимальна среди локально нильпотентных подгрупп группы $GL(n, \Delta)$, то G сопряжена в $GL(n, \Delta)$ с группой $\Gamma_k(A)$.

Иными словами, *если A является d-группой, то в подходящем базисе пространства Δ^n матрицы g группы G принимают вид*

$$g = \begin{bmatrix} a(g) & c_{12}(g)\,a(g) & \dots & c_{1k}(g)\,a(g) \\ 0 & a(g) & \dots & c_{2k}(g)\,a(g) \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a(g) \end{bmatrix}, \tag{14}$$

где $c_{ij}(g) \in D$.

Согласно следствию 27.1.1 неприводимая локально нильпотентная линейная группа над совершенным полем является d-группой. Следовательно, из теоремы 3 вытекает

Теорема 3а. *Пусть поле Δ совершенно. Тогда неразложимая локально нильпотентная подгруппа G группы $GL(n, \Delta)$ сопряжена в $GL(n, \Delta)$ с некоторой подгруппой группы $\Gamma_k(A)$.*

Доказательству теоремы 3 предпошлем длинный ряд лемм.

Лемма 6. *Пусть матрица c является d-матрицей из $GL(m, \Delta)$, а*

$$u = \begin{bmatrix} c & b \\ 0 & c \end{bmatrix}.$$

Тогда существует в $\Delta[x]$ такой полином $f(x)$, что

$$f(u) = \begin{bmatrix} c & b_1 \\ 0 & c \end{bmatrix} = u_1,$$

а минимальный полином матрицы u_1 совпадает с минимальным полиномом $\varphi(x)$ матрицы c.

Доказательство. Так как c есть d-матрица, то полиномы $\varphi(x)$ и $\varphi'(x)$ взаимно просты. Следовательно, в $\Delta[x]$ есть такие полиномы $f_1(x)$ и $f_2(x)$, что

$$\varphi(x)\,f_1(x) - \varphi'(x)\,f_2(x) = 1. \tag{15}$$

Положим

$$f(x) = x + \varphi(x)\,f_2(x).$$

Тогда

$$\varphi(x+\varphi(x)f_2(x))=\varphi(x)+\varphi'(x)f_2(x)+(\varphi(x))^2 q(x).$$

В силу (15)

$$\varphi'(x)f_2(x)=\varphi(x)f_1(x)-1.$$

Следовательно,

$$\varphi(f(x))=\varphi(x)^2 f_2(x)+(\varphi(x))^2 q(x)\equiv 0 \pmod{(\varphi(x))^2}.$$

Отсюда

$$\varphi(f(u))=\varphi(u_1)=0. \blacksquare$$

Лемма 7. *Пусть* $a,\ b\in\Delta_n,\quad c=ab-ba,\quad ca=ac$, *матрица* a *является* d-*матрицей. Тогда матрица* c *нильпотентна.*

Доказательство. Так как $ca=ac$, то для некоторого расширения Σ поля Δ в $GL(n,\ \Sigma)$ существует такая матрица q, что

$$a_1=q^{-1}aq=\operatorname{diag}[\alpha_1,\ \ldots,\ \alpha_n],$$

$$c_1=q^{-1}cq=\begin{bmatrix}\gamma_1 & * & \ldots & * \\ 0 & \gamma_2 & \ldots & * \\ . & . & . & . \\ 0 & 0 & \ldots & \gamma_n\end{bmatrix}.$$

Положим

$$b_1=\|\beta_{ij}\|=q^{-1}bq.$$

Тогда $c_1=a_1b_1-b_1a_1$. Отсюда

$$\gamma_i=\alpha_i\beta_{ii}=\beta_{ii}\alpha_i=0,\qquad i=1,\ \ldots,\ n,$$

т. е. матрица c нильпотентна. $\blacksquare$

Будем сперва рассматривать нильпотентную группу $\Gamma\subset GL(2m,\ \Delta)$, матрицы g которой имеют вид

$$g=\begin{bmatrix}a(g) & b(g)\\ 0 & a(g)\end{bmatrix}, \tag{16}$$

где $\gamma\colon g\mapsto a(g)$ — неприводимое представление группы Γ степени m. Пусть $A=\operatorname{Im}\gamma$, а D — централизатор группы A в алгебре Δ_m. Будем предполагать, что A является d-группой. Как легко проверить, справедлива

Лемма 8. *Матрица*

$$h=\begin{bmatrix} E_m & b \\ 0 & E_m \end{bmatrix} \tag{17}$$

тогда и только тогда принадлежит централизатору группы Γ *в* $GL(2m, \Delta)$, *когда* $b \in D$.

Ниже мы предполагаем, что матрица h вида (17), где $b \in D$, принадлежит $Z_1(\Gamma)$.

Лемма 9. *Пусть* h — *матрица вида* (17), *и пусть* $(g, h) \in Z_1(\Gamma)$ *при любом* g *из* Γ. *Тогда* $(g, h) \in E_{2m}$ *для любого* g *из* Γ.

Доказательство. Из (16) и (17) имеем

$$(g, h)=\begin{bmatrix} E_m & a(g)\,b\,(a(g))^{-1}-b \\ 0 & E_m \end{bmatrix}.$$

В силу леммы 8 для любого $g \in \Gamma$ имеем

$$a(g)\,b\,(a(g))^{-1}-b=b_1 \in D.$$

Отсюда

$$a(g)\,b-ba(g)=b_1a(g)=c. \tag{18}$$

Очевидно, матрица c перестановочна с $a(g)$. Так как A является d-группой, то $a(g)$ есть d-матрица. В силу леммы 7 c — нильпотентная матрица. Так как матрица $a(g)$ не вырождена, то вырождена $b_1 \in D$. Но D — тело, следовательно,

$$b_1=0, \qquad (g, h)=E_{2m}. \ \blacksquare$$

Лемма 10. *Пусть матрица* h *вида* (16) *принадлежит* Γ. *Тогда*

$$h \in Z_1(\Gamma). \tag{19}$$

Доказательство. Пусть

$$h \in \Gamma \setminus Z_1(\Gamma). \tag{20}$$

Очевидно, что (g, h), где $g \in \Gamma$, тоже имеет вид (16). Так как группа Γ нильпотентна, то существуют такое целое $k>1$, что

$$(x_k, (x_{k-1}, \ldots, (x_1, h)\ldots))=E_{2m} \tag{21}$$

при любых $x_1, \ldots, x_k \in \Gamma$, и такие $g_1, \ldots, g_{k-1} \in \Gamma$, что

$$(g_{k-1}, (g_{k-2}, \ldots, (g_1, h)\ldots)) \neq E_{2m}. \tag{22}$$

Пусть

$$h_1 = (g_{k-2}, \ldots, (g_1, h) \ldots),$$

если $k > 2$, и $h_1 = h$ при $k = 2$. Тогда в силу (21) и леммы 9,

$$h_1 \in Z_1(\Gamma),$$

что противоречит неравенству (22). ■

Лемма 11. *Пусть*

$$v = \begin{bmatrix} c & b \\ 0 & c \end{bmatrix}, \qquad v_1 = \begin{bmatrix} c_1 & b_1 \\ 0 & c_1 \end{bmatrix} \tag{23}$$

— такие матрицы из $GL(2m, \Delta)$, что

$$c, \ c_1 \in Z_1(A), \tag{24}$$

а

$$(g, v), \quad (g, v_1) \in Z_1(\Gamma) \tag{25}$$

для каждого g из Γ. Пусть, далее, $\alpha, \beta \in \Delta$, а матрица $u = \alpha v + \beta v_1$ не вырождена. Тогда

$$(g, u) \in Z_1(\Gamma)$$

при любом g из Γ.

Доказательство. Из (23) и (25) получаем

$$(g, vv_1) = (g, v)(g, v_1) \in Z_1(\Gamma), \qquad (g, vv_1^{-1}) \in Z_1(\Gamma).$$

Следовательно, достаточно рассмотреть случай, когда $v_1 = E_{2m}$. Положим

$$(g, u) = \begin{bmatrix} E_m & x_{\alpha\beta} \\ 0 & E_m \end{bmatrix}.$$

Из равенства

$$\begin{bmatrix} a(g) & b(g) \\ 0 & a(g) \end{bmatrix} \begin{bmatrix} \alpha c + \beta E_m & \alpha b \\ 0 & \alpha c + \beta E_m \end{bmatrix} = \\ = \begin{bmatrix} E_m & x_{\alpha\beta} \\ 0 & E_m \end{bmatrix} \begin{bmatrix} \alpha c + \beta E_m & \alpha b \\ 0 & \alpha c + \beta E_m \end{bmatrix} \begin{bmatrix} a(g) & b(g) \\ 0 & a(g) \end{bmatrix}$$

находим

$$\alpha a(g) b + \alpha b(g) c + \beta b(g) = \\ = (\alpha c + \beta E_m) b(g) + [\alpha b + x_{\alpha\beta}(\alpha c + \beta E_m)] a(g).$$

Отсюда

$$x_{\alpha\beta}(\alpha c+\beta E_m)=\alpha[a(g)b-ba(g)+b(g)c-cb(g)]a(g)^{-1}. \tag{26}$$

В частности, при $\alpha=1$, $\beta=0$ получаем

$$x_{10}c=[a(g)b-ba(g)+b(g)c-cb(g)]a(g^{-1}). \tag{27}$$

По условию $x_{10}\in D$. Из (26) и (27)

$$x_{\alpha\beta}(\alpha c+\beta E_m)=\alpha x_{10}c.$$

Следовательно,

$$x_{\alpha\beta}\in D,\qquad (g,\ u)\in Z_1(\Gamma). \ \blacksquare$$

Лемма 12. *Пусть v и v_1 — матрицы вида* (23), *а матрица*

$$u=\alpha v+\beta v_1$$

вырождена. Тогда u перестановочна с каждой матрицей $g\in\Gamma$.

Доказательство. Так как матрица u вырождена, то

$$\alpha vv_1^{-1}+\beta E_n=\begin{bmatrix}0 & b\\ 0 & 0\end{bmatrix}.$$

Для любого $\gamma\neq\beta$ ($\gamma\in\Delta$), в силу лемм 11 и 9, матрица $\alpha vv_1^{-1}+\gamma E_{2m}$ перестановочна с каждой матрицей g из Γ. Очевидно, что

$$\alpha vv_1^{-1}+\gamma E_{2m}=\begin{bmatrix}(\gamma-\beta)E_m & b\\ 0 & (\gamma-\beta)E_m\end{bmatrix}.$$

Следовательно, $b\in D$. Так как

$$u=\begin{bmatrix}0 & bc_1\\ 0 & 0\end{bmatrix},\qquad bc_1\in D,$$

то лемма доказана. $\blacksquare$

Положим теперь

$$V=\gamma^{-1}(Z_1(A)).$$

Лемма 13. *Пусть u — невырожденная матрица из линейной Δ-оболочки $[V]$ группы V. Тогда*

$$(g,\ u)\in Z_1(\Gamma)$$

для любого g из Γ.

Доказательство. Для любого $v \in V$, в силу леммы 10, $(g, v) \in Z_1(\Gamma)$ при каждом $g \in \Gamma$. Для u можно написать

$$u_1 = \alpha_1 v_1 + \ldots + \alpha_r v_r,$$

где $\alpha_j \in \Delta$, $\alpha_j \neq 0$, $v_j \in V$, $j = 1, \ldots, r$. Введем r матриц:

$$u_1 = \alpha_1 v, \quad u_2 = u_1 + \alpha_2 v_2, \ \ldots, \quad u = u_r = u_{r-1} + \alpha_r v_r.$$

Если $u_1, \ldots, u_{r-1}$ — невырожденные матрицы, то лемма 13 следует из леммы 11.

Пусть матрицы $u_1, \ldots, u_{k-1}$ не вырождены, а u_k — вырожденная матрица. Так как u_{k-1} — невырожденная матрица, в силу леммы 12,

$$u_k = \begin{bmatrix} 0 & t \\ 0 & 0 \end{bmatrix}, \qquad t \in D.$$

Для u_{k+1} имеем

$$u_{k+1} = u_k + \alpha_{k+1} v_{k+1}.$$

Если

$$v_{k+1} = \begin{bmatrix} \lambda E_m & b \\ 0 & \lambda E_m \end{bmatrix}, \qquad \lambda \in \Delta^*,$$

то, в силу леммы 10, матрица u_{k+1} перестановочна с каждой матрицей $g \in \Gamma$. Если же

$$v_{k+1} = \begin{bmatrix} c & b \\ 0 & c \end{bmatrix}, \qquad c \in Z_1(A), \qquad c \notin \Delta^* E_m,$$

то

$$u_{k+1} = u_k + E_{2m} + \alpha_{k+1}\left(v_{k+1} - \alpha_{k+1}^{-1} E_{2m}\right).$$

Очевидно, что для $g \in \Gamma$

$$(g, u_k + E_{2m}) = E_{2m}, \qquad (g, v_{k+1} - \alpha_{k+1}^{-1} E_{2m}) \in Z_1(\Gamma).$$

Следовательно, $v_{k+1} - \alpha_{k+1}^{-1} E_{2m}$ и $u_k + E_{2m}$ суть матрицы вида (23). В силу леммы 11

$$(g, u_{k+1}) \in Z_1(\Gamma). \ ■$$

Продолжим рассмотрение алгебры $[V]$. Пусть поле P — линейная Δ-оболочка группы $Z_1(A)$. Так как A есть d-группа, то $Z_1(A)$ состоит из d-матриц. Следовательно, элементы группы $Z_1(A) \subset P$ сепарабельны над Δ_m и P

является сепарабельным расширением поля Δ. Введем сюръективный гомоморфизм

$$\psi\colon [V] \longrightarrow P, \qquad \begin{bmatrix} d & b \\ 0 & d \end{bmatrix} \mapsto d \in P.$$

Так как P — сепарабельное расширение поля Δ, то $P = \Delta[c]$, где c — примитивный элемент поля P. Пусть $u \in \psi^{-1}(c)$, а U — мультипликативная группа коммутативного кольца $\Delta[u] \subset [V]$. В силу леммы 13 каждый элемент группы U перестановочен с каждой матрицей группы Γ с точностью до множителя из $Z_1(\Gamma)$. Очевидно, что группы $Z_1(\Gamma)$ и U перестановочны поэлементно. Следовательно, $\Gamma U = U\Gamma$ — тоже нильпотентная подгруппа группы $GL(2m, \Delta)$. Таким образом, мы вправе считать, что

$$U \subset \Gamma, \qquad U \subset Z_2(\Gamma).$$

В силу леммы 6 в группе U есть такая матрица u_1, минимальный полином которой совпадает с минимальным полиномом примитивного элемента c. Будем считать, что

$$u_1 = \operatorname{diag}[c, c],$$

так как u_1 можно трансформировать к такому виду с помощью матрицы

$$\begin{bmatrix} E_m & S \\ 0 & E_m \end{bmatrix}.$$

Лемма 14. $u_1 \in Z_1(\Gamma)$.

Доказательство. Так как $u \in U \subset Z_2(\Gamma)$, то

$$(g, u_1) = \begin{bmatrix} E_m & t \\ 0 & E_m \end{bmatrix}, \qquad t \in D.$$

С другой стороны, $tca(g) = b(g)c - cb(g)$ и d-матрица c перестановочна с $b(g)c - cb(g)$. В силу леммы 7 матрица $tca(g)$ нильпотентна. Следовательно, $t = 0$, $u_1 \in Z_1(\Gamma)$. ■

Лемма 15. *Пусть*

$$h = \begin{bmatrix} z & b \\ 0 & z \end{bmatrix} \in \gamma^{-1}(Z_1(A)).$$

Тогда $h \in Z_1(\Gamma)$.

Доказательство. Очевидно, для g из Γ имеем

$$(g,\ h)=\begin{bmatrix} E_m & x \\ 0 & E_m \end{bmatrix}.$$

В силу леммы 10 $(g,\ h)\in Z_1(\Gamma)$, $x\in D$. Из равенства $gh=(g,h)hg$ находим

$$xza(g)=a(g)\,b-ba(g)+b(g)\,z-zb(g).$$

В силу леммы 14 $b(g)z=zb(g)$. Следовательно,

$$xza(g)=a(g)\,b-ba(g).$$

В силу леммы 7 $xza(g)$ — нильпотентная матрица. Следовательно,

$$x=0,\qquad h\in Z_1(\Gamma). \ ■$$

Итак, мы можем считать, что $Z_1(\Gamma)$ состоит из всех матриц вида

$$\begin{bmatrix} z & t \\ 0 & z \end{bmatrix},\qquad t\in D,\qquad z\in Z_1(A)=P^*,\qquad P=\Delta[c]. \tag{28}$$

Из леммы 15 и теоремы 27.1 следует

Лемма 16. *Индекс $Z_1(\Gamma)$ в Γ конечен:*

$$\Gamma:Z_1(\Gamma)=A:Z_1(A). \tag{29}$$

Пусть теперь

$$M=P^*E_2,\qquad \bar\Gamma=\Gamma/M.$$

Рассмотрим смежные классы группы $\bar\Gamma$ по нормальному делителю

$$\bar Z_1=Z_1(\Gamma)/M.$$

Лемма 17. *В каждом смежном классе группы $\bar\Gamma$ по $\bar Z_1$ имеется один и только один элемент $\bar g_1\in\bar\Gamma$, порядок которого конечен и делится на* char Δ.

Доказательство. Пусть

$$g=\begin{bmatrix} a(g) & b(g) \\ 0 & a(g) \end{bmatrix}\in\Gamma,$$

а класс $a(g)Z_1(A)$ из $A/Z_1(A)$ имеет порядок l. По теореме 27.1 $\operatorname{char}\Delta \nmid l$. В силу леммы 15

$$g^l = \begin{bmatrix} z & b \\ 0 & z \end{bmatrix} \in Z_1(\Gamma), \qquad z \in Z_1(A), \quad b \in D.$$

Далее,

$$h = \begin{bmatrix} E_m & -l^{-1}z^{-1}b \\ 0 & E_m \end{bmatrix} \in Z_1(\Gamma)$$

и

$$(gh)^l = \begin{bmatrix} z & b \\ 0 & z \end{bmatrix} \begin{bmatrix} E_m & -z^{-1}b \\ 0 & E_m \end{bmatrix} = \operatorname{diag}[z,\ z] \in M.$$

Положим $g_1 = gh$, $\bar{g}_1 = g_1M$. Тогда $\bar{g}_1 \in \bar{\Gamma}$, $g_1M \in \bar{g}_1\bar{Z}_1$. Очевидно, что порядок элемента $\bar{g}_1$ равен l. Так как группа $\bar{Z}_1$ изоморфна группе H всех матриц вида

$$h = \begin{bmatrix} E_m & t \\ 0 & E_m \end{bmatrix}, \qquad t \in D, \tag{30}$$

то $\bar{Z}_1$ — группа без кручения, когда $\operatorname{char}\Delta = 0$, и p-группа, когда $\operatorname{char}\Delta = p$. Следовательно, порядок любого элемента из $\bar{g}_1\bar{Z}_1$, отличного от $\bar{g}_1$, либо бесконечен, либо делится на $\operatorname{char}\Delta$. ■

Лемма 18. *В $GL(2m, \Delta)$ есть такой элемент*

$$q = \begin{bmatrix} E_m & b \\ 0 & E_m \end{bmatrix},$$

что матрицы g группы $q^{-1}\Gamma q$ имеют вид

$$g = \begin{bmatrix} a(g) & t(g)\,a(g) \\ 0 & a(g) \end{bmatrix},$$

где $t(g) \in D$.

Доказательство. Совокупность $\bar{N}$ всех элементов группы $\bar{\Gamma}$, порядки которых конечны и не делятся на $\operatorname{char}\Delta$, является нормальным делителем группы $\bar{\Gamma}$. В силу леммы 17

$$\bar{\Gamma} = \bar{N}\bar{Z}_1.$$

Следовательно, если $\bar{N} = N/M$, то

$$\Gamma = NZ_1(\Gamma) = NH. \tag{31}$$

где H — группа всех матриц вида (30). Группа M вполне приводима, а индекс $N:M$ конечен и не делится на $\operatorname{char}\Delta$, следовательно, по теореме 17.1, группа N вполне приводима. Таким образом, матрицы g_0 группы N можно с помощью матрицы q трансформировать к виду

$$g_0 = \operatorname{diag}[a(g_0),\ a(g_0)].$$

Матрица q перестановочна с каждой матрицей из H. Отсюда и из (31) вытекает лемма. ■

Напомним, что в леммах 8—18 Γ — нильпотентная группа матриц вида (16).

Основная лемма. *Лемма* 18 *остается верной, если вместо нильпотентности группы* Γ *предположить локальную нильпотентность.*

Доказательство. Пусть $a_1, \ldots, a_\rho$ — максимальная система линейно независимых над Δ матриц группы A, а

$$g_j = \begin{bmatrix} a_j & b_j \\ 0 & a_j \end{bmatrix}, \quad j = 1, \ldots, p, \tag{32}$$

— элементы из Γ. Группа B, порожденная матрицами (32), нильпотентна и имеет две неэквивалентные неприводимые части. В силу леммы 18 мы можем считать, что B состоит из матриц вида

$$b = \begin{bmatrix} a(b) & t(b)\,a(b) \\ 0 & a(b) \end{bmatrix}, \tag{33}$$

где $t(b) \in D$, т. е.

$$B \subset \Gamma_2(A).$$

Покажем, что

$$\Gamma \subset \Gamma_2(A),$$

и лемма будет доказана. Пусть g — произвольный элемент группы Γ, а U — подгруппа группы Γ, порождаемая B и g. Тогда, согласно лемме 18, в $GL(2m, \Delta)$ есть такая матрица

$$q = \begin{bmatrix} E_m & W \\ 0 & E_m \end{bmatrix},$$

что для любого $u \in U$

$$q^{-1}uq = \begin{bmatrix} a(u) & f(u)\,a(u) \\ 0 & a(u) \end{bmatrix}, \quad f(u) \in D. \tag{34}$$

В частности, это верно и для $b \in B$:

$$\begin{bmatrix} a(b) & t(b)a(b) \\ 0 & a(b) \end{bmatrix} \begin{bmatrix} E_m & W \\ 0 & E_m \end{bmatrix} = \begin{bmatrix} E_m & W \\ 0 & E_m \end{bmatrix} \begin{bmatrix} a(b) & f(b)a(b) \\ 0 & a(b) \end{bmatrix}.$$

Отсюда $a(b)W - Wa(b) = (f(b) - t(b))a(b)$. В силу леммы 7 $f(b) - t(b) = 0$, $W \in D$. Следовательно,

$$qg = gq, \quad g \in \Gamma_2(A), \quad \Gamma \subset \Gamma_2(A). \ \blacksquare$$

Лемма 19. *Пусть матрицы g локально нильпотентной подгруппы G_1 группы $GL(ms, \Delta)$ имеют вид*

$$g = \begin{bmatrix} a(g) & c_{12}(g)a(g) & \dots & c_{1,s-1}(g)a(g) & a_{1s}(g) \\ 0 & a(g) & \dots & c_{2,s-1}(g)a(g) & c_{2s}(g)a(g) \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & a(g) & c_{s-1,s}(g)a(g) \\ 0 & 0 & \dots & 0 & a(g) \end{bmatrix}, \tag{35}$$

где $a(g)$ пробегает неприводимую локально нильпотентную подгруппу A группы $GL(m, \Delta)$, $c_{ij}(g) \in D$, а D — централизатор группы A в алгебре Δ_m. Тогда группа $G_1T_s(D)$ локально нильпотентна.

Доказательство. Достаточно показать, что группа $\mathfrak{G} = T_s(D)\mathfrak{H}$, где $\mathfrak{H}$ — любая нильпотентная подгруппа группы G_1, нильпотентна. Как показывают прямые вычисления, матрицы из $T_s(D)$ вида

$$\begin{bmatrix} E_m & 0 & \dots & 0 & d_{1s} \\ 0 & E_m & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & E_m \end{bmatrix}, \quad d_{1s} \in D, \tag{36}$$

перестановочны с каждой матрицей группы G_1 и, следовательно, содержатся в $Z_1(\mathfrak{G})$. Далее, коммутатор матрицы

$$\begin{bmatrix} E_m & 0 & \dots & d_{1,s-1} & d_{1s} \\ 0 & E_m & \dots & 0 & d_{2s} \\ 0 & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & E_m \end{bmatrix}, \quad d_{ij} \in D, \tag{37}$$

и любой матрицы из группы $\mathfrak{G}$ имеет вид (36), следовательно, все матрицы вида (37) входят в $Z_2(\mathfrak{G})$. Аналогично,

$$T_s(D) \subset Z_{s-1}(\mathfrak{G}).$$

Отсюда и следует лемма. ■

Лемма 20. *Пусть локально нильпотентная подгруппа G_1 группы $GL(ms, \Delta)$ состоит из матриц вида* (35). *Тогда матрицы g группы G_1 можно одновременно трансформировать к виду*

$$\begin{bmatrix} a(g) & c_{12}(g)a(g) & \dots & c_{1,s-1}(g)a(g) & c_{1s}(g)a(g) \\ 0 & a(g) & \dots & c_{2,s-1}(g)a(g) & c_{2s}(g)a(g) \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & a(g) \end{bmatrix} \tag{38}$$

с помощью матрицы

$$\begin{bmatrix} E_m & 0 & \dots & 0 & k \\ 0 & E_m & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & E_m \end{bmatrix}, \qquad k \in \Delta_m.$$

Доказательство. В силу леммы 19 можно считать, что $T_s(D) \subset G_1$. Следовательно, в группе G_1 вместе с матрицей g вида (35) содержится матрица

$$g_2 = g \begin{bmatrix} E_m & c_{12}(g) & \dots & c_{1s}(g) \\ 0 & E_m & \dots & c_{2s}(g) \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & E_m \end{bmatrix}^{-1} = \begin{bmatrix} a(g) & 0 & \dots & 0 & b(g) \\ 0 & a(g) & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & a(g) \end{bmatrix}.$$

Из (38) вытекает равенство

$$G_1 = T_s(D)\,\mathfrak{H}_1, \tag{39}$$

где матрицы g_2 группы $\mathfrak{H}_1$ имеют вид

$$g_2 = \begin{bmatrix} a(g) & 0 & \dots & 0 & b(g) \\ 0 & a(g) & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & a(g) \end{bmatrix}.$$

Группа $\mathfrak{H}_1 \subset G_1$ локально нильпотентна. Так как отображение

$$\gamma_2\colon g_2 \mapsto \begin{bmatrix} a(g) & b(g) \\ 0 & a(g) \end{bmatrix}$$

является изоморфизмом, то группа $\operatorname{Im}\gamma_2$ тоже локально нильпотентна. Следовательно, в силу основной леммы, матрицы группы $\operatorname{Im}\gamma_2$ одновременно трансформируются к виду

$$\begin{bmatrix} a(g) & c(g)a(g) \\ 0 & a(g) \end{bmatrix}, \quad c(g) \in D,$$

с помощью матрицы

$$\begin{bmatrix} E_m & W \\ 0 & E_m \end{bmatrix}.$$

Положим теперь

$$t = \begin{bmatrix} E_m & 0 & \dots & 0 & W \\ 0 & E_m & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & E_m \end{bmatrix} \in GL(ms, \Delta).$$

Тогда

$$t^{-1}g_2t = \begin{bmatrix} a(g) & 0 & \dots & 0 & c(g)a(g) \\ 0 & a(g) & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & a(g) \end{bmatrix},$$

Очевидно, что матрица t перестановочна с каждой матрицей группы $T_s(D)$. Следовательно, в силу (39), матрица t трансформирует матрицы группы G_1 к виду (38). ■

Доказательство теоремы 3. По условию матрицы g локально нильпотентной группы G имеют вид (12). В силу основной леммы существуют в $GL(2m, \Delta)$ такие матрицы

$$t_j = \begin{bmatrix} E_m & W_{j,j+1} \\ 0 & E_m \end{bmatrix}, \quad j = 1, \dots, k-1,$$

что

$$t_j^{-1}\begin{bmatrix} a(g) & a_{jj}(g) \\ 0 & a(g) \end{bmatrix} t_j = \begin{bmatrix} a(g) & c_{j,\,j+1}(g)\,a(g) \\ 0 & a(g) \end{bmatrix},$$

где

$$c_{j,\,j+1}(g) \in D$$

при любом $g \in G$. Положим

$$q_1 = \begin{bmatrix} E_m & W_{12} & 0 & \ldots & 0 \\ 0 & E_m & W_{23} & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & W_{k-1,\,k} \\ 0 & 0 & 0 & \ldots & E_m \end{bmatrix}.$$

Тогда в матрице $q_1^{-1}gq_1$ на позиции $(j,\ j+1)$ расположена субматрица

$$c_{j,\,j+1}(g)\,a(g), \qquad j = 1, \ldots, k-1,$$

где $c_{j,\,j+1}(g) \in D$ при любом g из G. В силу леммы 20 существует матрица q_2 вида

$$q_2 = \begin{bmatrix} E_m & 0 & W_{13} & 0 & \ldots & 0 & 0 \\ 0 & E_m & 0 & W_{24} & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \ldots & 0 & W_{k-2,\,k} \\ 0 & 0 & 0 & 0 & \ldots & E_m & 0 \\ 0 & 0 & 0 & 0 & \ldots & 0 & E_m \end{bmatrix}$$

такая, что на позиции $(i,\ j)$, где $0 < j - i \leqslant 2$, в матрице

$$q_2^{-1}q_1^{-1}gq_1q_2$$

расположена субматрица $c_{ij}(g)\,a(g)$, $c_{ij}(g) \in D$. Применяя еще несколько раз лемму 20, приведем матрицы g группы G к виду (14). ■

В частности, из теоремы 3 вытекает, что *максимальная неразложимая локально нильпотентная подгруппа G группы $GL(n, \Delta)$ с точностью до сопряженности в $GL(n, \Delta)$ определяется группой $\operatorname{Im}\gamma = A$, где γ — неприводимая часть группы G, если A является d-группой.*

Теорему 3, как и приведенное выше утверждение, нельзя распространить на тот случай, когда $A = \operatorname{Im}\gamma$ не является d-группой. Приведем пример коммутативной неразложимой группы, матрицы которой нельзя одновременно трансформировать к виду (14). Пусть $\Sigma : \Delta = m$, Σ — простое несепарабельное расширение поля Δ, $\Sigma = \Delta(\omega)$, $\Sigma \subset \Delta_m$. Пусть $R \subset \Delta_{2m}$ состоит из матриц

$$r = \begin{bmatrix} 0 & \sigma \\ 0 & 0 \end{bmatrix},$$

где $\sigma \in \Sigma \subset \Delta_m$. Положим

$$u = \begin{bmatrix} \sigma & d \\ 0 & \sigma \end{bmatrix},$$

где

$$d = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ . & . & . & . \\ 0 & 0 & \dots & 0 \end{bmatrix} \in \Delta_m, \qquad \mathfrak{A} = \Delta[u] + R,\ \mathfrak{A}^* = G.$$

Тогда G — коммутативная неразложимая подгруппа группы $GL(2m, \Delta)$. В силу теоремы 1 статьи Супруненко [21] матрицы группы G нельзя привести к виду (14).

Теорема 4 (Цассенхауз [1]). *Локально нильпотентная подгруппа G группы $GL(n, \Delta)$ тогда и только тогда нильпотентна, когда $\operatorname{Im}\gamma$ — нильпотентная подгруппа для любой неприводимой части γ группы G.*

Доказательство. Необходимость очевидна. Докажем достаточность. Пусть для любой неприводимой части γ группы G группа $\operatorname{Im}\gamma$ нильпотентна. Ясно, что это свойство группы G сохранится, если мы заменим поле Δ алгебраически замкнутым полем Ω, содержащим поле Δ. Следовательно, можно считать, что $\operatorname{Im}\gamma$ является d группой. Таким образом, к неразложимым частям группы G применима теорема 3. Так как группа $\Gamma_k(A)$ нильпотентна, когда нильпотентна группа A, то отсюда вытекает нильпотентность группы G ■

4. Другие результаты о локально нильпотентных группах. Локально нильпотентная подгруппа $GL(n, \Delta)$, где Δ — произвольное поле, разрешима, следовательно, в силу теоремы 22.5, локально нильпотентная d-группа из $GL(n, \Delta)$ всегда вполне приводима. В силу следствия 27.1.1 для совершенного основного поля Δ справедливо обратное утверждение: локально нильпотентная вполне приводимая группа матриц над Δ является d-группой. В случае несовершенного основного поля, как легко видеть, существуют даже абелевы неприводимые группы матриц, не являющиеся d-группами.

Теорема 5. *Пусть G — вполне приводимая локально нильпотентная подгруппа группы $GL(n, \Delta)$, где Δ — произвольное поле. Тогда любая подгруппа группы G вполне приводима.*

Доказательство. Пусть H — произвольная подгруппа группы G, $h_1, h_2, \ldots, h_r$ — максимальная система линейно независимых над Δ элементов группы H, а H_1 — группа, порождаемая элементами $h_1, \ldots, h_r$. Теорема будет доказана, если мы докажем полную приводимость группы H_1. Дополним систему $h_1, h_2, \ldots, h_r$ до максимальной линейно независимой системы элементов группы G:

$$h_1, h_2, \ldots, h_r, g_{r+1}, \ldots, g_s. \tag{40}$$

Так как группа G вполне приводима, то группа G_1, порожденная системой (40), тоже вполне приводима. Группа G_1 нильпотентна и содержит H_1, следовательно, существует (см. Курош [1], стр. 389) нормальный ряд вида

$$G_1 \supset H_t \supset H_{t-1} \supset \ldots \supset H_1 \supset (E_n). \tag{41}$$

Очевидно, что из полной неприводимости группы G_1 и теоремы 16.2 вытекает полная приводимость каждой группы ряда (41). ∎

Следствие 1. *Пусть G — вполне приводимая локально нильпотентная группа матриц над произвольным полем. Тогда каждый элемент g из G является полупростой матрицей.*

Возвратимся снова к группам типа $\Gamma_k(F)$ п. 1.

Лемма 21. *Пусть неприводимая подгруппа F группы $GL(m, \Delta)$ является d-группой. Тогда $F \dot{\times} E_k$ совпадает с совокупностью всех d-матриц группы $\Gamma_k(F)$, а $T_k(D)$ — с совокупностью всех унипотентных матриц группы $\Gamma_k(F)$.*

Доказательство. Пусть $a = (f \dot{\times} E_k) u \in \Gamma_k(F)$, $f \in F$, $u \in T_k(D)$. Очевидно, что

$$\det(xE_n - a) = (\det(xE_m - f))^k.$$

Следовательно, если a унипотентна, то $\det(xE_m - f) = (x-1)^m$. Так как F является d-группой, то для унипотентной матрицы a имеем $f = E_m$, $a = u \in T_k(D)$. Таким образом, $T_k(D)$ совпадает с множеством всех унипотентных матриц группы $\Gamma_k(F)$. Пусть теперь $a = (f \dot{\times} E_k) u$ и является d-матрицей. d-матрица $b = f^{-1} \dot{\times} E_k$ перестановочна с a. Следовательно, в силу леммы 17.1, $u = ab$ — тоже d-матрица. Отсюда $u = E_n$, $a = b \dot{\times} E_k \in F \dot{\times} E_k$.

Теорема 6. *Пусть Δ — произвольное поле, G — локально нильпотентная подгруппа группы $GL(n, \Delta)$, $d(G)$ — множество всех d-матриц группы G, а $u(G)$ — множество всех унипотентных матриц группы G. Тогда $d(G)$ и $u(G)$ — нормальные делители группы G.*

Доказательство. Достаточно доказать, что $d(G)$ и $u(G)$ — подгруппы группы G. Так как свойство быть d-матрицей и унипотентность матрицы сохраняются при расширении основного поля, то мы можем рассматривать G как подгруппу $GL(n, P)$, где P — алгебраически замкнутое поле, содержащее поле Δ.

Очевидно, мы можем считать, что G состоит из матриц вида

$$g = \operatorname{diag}[g_1, g_2, \ldots, g_t], \tag{42}$$

где g_j пробегает некоторую локально нильпотентную неразложимую подгруппу G_j группы $GL(n_j, P)$, $j = 1, 2, \ldots, t$, $n_1 + n_2 + \ldots + n_t = n$. Так как алгебраически замкнутое поле совершенно, то к группе G_j применима теорема 3а. Следовательно, мы можем считать, что $G_j \subset \Gamma_{k_j}(F_j)$, где F_j — неприводимая локально нильпотентная подгруппа группы $GL(m_j, P)$, $m_j k_j = n_j$.

В силу леммы 21 теорема верна для группы $G_j \subset \Gamma_{k_j}(F_j)$. Отсюда и из формулы (42) вытекает справедливость теоремы для группы G. ■

Лемма 22. *Пусть F и H — такие неприводимые подгруппы группы $GL(m, \Delta)$, что $[F] = [H]$. Тогда из* *строгого включения $F \subset H$ вытекает строгое включение $\Gamma_k(F) \subset \Gamma_k(H)$.*

Доказательство. Из равенства $[F] = [H]$ вытекает, что централизатор группы H в Δ_m совпадает с централизатором D группы F в Δ_m. Следовательно,

$$\Gamma_k(H) = (H \dot{\times} E_k)\, T_k(D) \supset (F \dot{\times} E_k)\, T_k(D) = \Gamma_k(F). \blacksquare$$

Следствие 1. *Пусть F — абсолютно неприводимая локально нильпотентная подгруппа группы $GL(m, \Delta)$. Если группа $\Gamma_k(F)$ максимальна среди локально нильпотентных подгрупп в $GL(n, \Delta)$, то F — максимальная локально нильпотентная подгруппа группы $GL(m, \Delta)$.*

Отметим без доказательства следующее свойство группы $\Gamma_k(F)$. *Пусть Δ — совершенное поле, F — неприводимая локально нильпотентная подгруппа группы $GL(m, \Delta)$, M — мультипликативная группа кольца $[F]$, $k > 1$, $mk = n$. Группа $\Gamma_k(F)$ тогда и только тогда максимальна среди локально нильпотентных подгрупп группы $GL(n, \Delta)$, когда F максимальна среди локально нильпотентных подгрупп группы M* (Супруненко [20]).

Теорема 7. *Пусть Δ — алгебраически замкнутое поле, а $\mathfrak{M}$ — совокупность всех максимальных локально нильпотентных подгрупп группы $GL(n, \Delta)$. Тогда число классов сопряженных в $GL(n, \Delta)$ подгрупп, на которые разбивается $\mathfrak{M}$, меньше некоторого числа $k(n)$, зависящего только от n.*

Доказательство. Пусть $G \in \mathfrak{M}$. Тогда согласно теореме 3а группа G сопряжена в $GL(n, \Delta)$ с группой всех матриц g вида

$$g = \operatorname{diag}[g_1, g_2, \ldots, g_\nu],$$

где $g_j \in \Gamma_{k_j}(F_j)$, F_j — неприводимая локально нильпотентная подгруппа группы $GL(m_j, \Delta)$, $m_j k_j = n_j$, $n_1 + n_2 + \ldots + n_\nu = n$. В силу леммы 22 F_j — максимальная локально нильпотентная подгруппа в $GL(m_j, \Delta)$. Согласно теореме 28.7 F_j с точностью до сопряженности в $GL(m_j, \Delta)$ определяется числом m_j. Таким образом, группа G с точностью до сопряженности в $GL(n, \Delta)$ задается представлением числа n в виде

$$n = k_1 m_1 + k_2 m_2 + \ldots + k_\nu m_\nu, \qquad (43)$$

где $k_j > 0$, $m_j > 0$ *). Следовательно, искомое число классов не превышает числа представлений n в виде (43). ■

В заключение приведем одну теорему без доказательства.

Теорема 8. *Пусть группа G допускает точное линейное представление над некоторым полем. Тогда следующие четыре утверждения эквивалентны:*

1. *G — локально нильпотентная группа;*
2. *G удовлетворяет нормализаторному условию;*
3. *G — нильгруппа;*
4. *G является ZA-группой.*

Доказательство см. в статьях Гаращук [1], Гаращук и Супруненко [1].

---

*) Можно добавить еще, что, в силу теоремы 28.6, char $\Delta \notin \Pi(m_j)$.

ЛИТЕРАТУРА

Артин Э.
1. Геометрическая алгебра, «Наука», 1969.

Ауслендер Л. (Auslander L.)
1. On a problem of Philip Hall, Ann. Math. **86**, № 1 (1967), 112—116.

Басс Х. (Bass H.)
1. K-theory and stable algebra, Publ. Math. **22** (1964), 5—60.

Басс Х., Лазар М., Серр Ж.-П. (Bass H., Lazard M., Serre J.-P.)
1. Sons-groupes d'indice fini dans $SL(n, Z)$, Bull. Amer. Math. Soc. **70**, № 3 (1964), 385—392.

Басс Х., Милнор Дж., Серр Ж.-П.
1. Решение конгруэнцпроблемы для SL_n $(n \geqslant 3)$ и Sp_{2n} $(n \geqslant 2)$, сб. перев. «Математика» **14**, № 6 (1970), 64—128.

Бернсайд В. (Burnside W.)
1. On an unsettled question in the theory of discontinuous groups, Quart. J. Pure and Appl. Math. **33** (1902), 230—238.
2. On criteria for the finiteness of the order of a group of linear substitutions, Proc. London Math. Soc. **3** (1905), 345—440.
3. On the arithmetical nature of the coefficients in a group of linear substitutions, Proc. London Math. Soc. 7 (1908), 8—13.

Борель А. (Borel A.)
1. Groupes lineaires algébriques, Ann. Math. **64**, № 1 (1956), 20—82.

Брауэр Р., Фейт В. (Brauer R., Feit W.)
1. An analogue of Jordan's theorem in characteristic p, Ann. Math. **84**, № 1 (1966), 119—131.

Бреннер Дж. (Brenner J. L.)
1. The linear homogeneous group, III, Ann. Math. **71**, № 2 (1960), 210—223.

Бурбаки Н.
1. Алгебра (алгебраические структуры, линейная и полинейная алгебра), Физматгиз, 1962.

Бэр Р.
1. Линейная алгебра и проективная геометрия, ИЛ, 1955.

Ван-дер-Варден Б. Л. (Van der Waerden B. L.)
1. Современная алгебра, часть первая, Гостехиздат, 1947.
2. Современная алгебра, часть вторая, Гостехиздат, 1948.
3. Gruppen von linearen Transformationen, Berlin, 1935.

Верфриц Б. (Wehrfritz B. A. F.)
1. Sylow theorem for periodic linear groups, Proc. London Math. Soc. **18**, № 1 (1968), 125—140.
2. Soluble periodic linear groups, Proc. London Math. Soc. **18**, № 1 (1968), 141—157.

Вольвачев Р. Т.
1. p-подгруппы Силова полной линейной группы, Изв. АН СССР, сер. матем. **27** (1963), 1031—1054.
2. Периодические нильпотентные линейные группы над полем рациональных чисел, ДАН СССР **167** (1966), 499—502.

Гаращук М. С.
1. К теории обобщенных нильпотентных линейных групп, ДАН БССР **4** (1960), 276—277.

Гаращук М. С., Супруненко Д. А.
1. Линейные нильгруппы, ДАН БССР **4** (1960), 407—408.

Голод Е. С.
1. О ниль-алгебрах и финитно-аппроксимируемых p-группах, Изв. АН СССР, сер. матем. **28** (1964), 273—276.

Грюн О. (Grün O.)
1. Über eine Faktorgruppe freier Gruppen I, Deutsche Math. **1** (1936), 772—782.

Диксон Дж. (Dixon J. D.)
1. Complete reducibility of infinite groups, Canadian J. Math. **16**, № 2 (1964), 267—274.
2. The Solvable lehgth of Solvable linear group, Math. Zeitschr. **107** (1968), 151—158.

Диксон Л. Е. (Dickson L. E.)
1. Linear groups, Leipzig, 1901.

Дирихле Л.
1. Лекции по теории чисел, ОНТИ, 1936.

Дьедонне Ж. (Diedonné J.)
1. Les determinants sur un corps non commutatif, Bull. Soc. Math. France **71** (1943), 27—45.
2. La geometrie des groupes classiques, Ergebnisse der Mathematik und ihrer Crenzgebiete (N. F.), Heft 5, Springer Verlag, Berlin — Göttingen — Heidelberg, 1955.
3. Sur les groupes classiques (Actual. scient. et industr. № 1040, publish. Inst. math. Univ. Strasbourg, 6), Paris. Hermann, 1958.

Жаврид Г. П.
1. К теории разрешимых матричных групп, ДАН БССР **11** (1967), 873—877.

Жордан К. (Jordan C)
1. Sur la résolution algébrique des équations primitives de degré p^2, J. Math. pures et appl. **12** (1868).
2. Traité des substitutions et équations algébriques, Paris, 1870.
3. Mémoire sur les équations différentielles linéaires á intégral algebrique, J. für die reine und angew. Math. **84** (1878), 89—215.

З а л е с с к и й А. Е.
1. Разрешимые подгруппы мультипликативной группы локально конечной алгебры, Матем. сб. **61** (1963), 408—417.
2. Разрешимые подгруппы мультипликативной группы простой алгебры, ДАН БССР **7** (1963), 80—82.
3. Силовские p-подгруппы полной линейной группы над телом, Изв. АН СССР, серия матем. **31** (1967), 1149—1158.

И в а н ю т а И. Д.
1. Силовские p-подгруппы счетной симметрической группы, Укр. матем. ж. **15**, № 3 (1963), 240—249.
2. О полных множествах силовских подгрупп счетной симметрической группы, Укр. матем. ж. **18**, № 3 (1966), 112—115.

К а л у ж н и н Л. А. (Kaloujnine L.)
1. Sur les p-groupes de Sylow du groupe symétrique de degré p^m, C. R., Paris **221** (1945), 222—224.
2. Sur les p-groupes de Sylow du groupe symétrique de degré p^m (Suite centrale ascendante et descendante), C. R., Paris **223** (1946), 703—705.
3. La structure des p-groupes de Sylow des groupes sumétriques finis, Annales de L'Ecole Normale **65** (1948), 239—276.

К а п л а н с к и й И.
1. Введение в дифференциальную алгебру, ИЛ, 1959.

К а р г а п о л о в М. И.
1. О периодических группах матриц. Сиб. матем. ж. **3**, № 6 (1962), 834—836.
2. О конечнопорожденных линейных группах, Алгебра и логика (семинар) **6**, № 5 (1967), 17—20.

К е г е л ь О. (Kegel O. H.)
1. Lecture on locally finite groups, Mathematical institute, Oxford, 1969.

К л и н г е н б е р г В. (K l i n g e n b e r g W.)
1. Die struktur der linearen Gruppen üer einem nichtkommutativen lokalen Ring, Arch. Math. **13**, № 1—2 (1962), 73—81.

К л и ф ф о р д А. (C l i f f o r d A. H.)
1. Representations induced in an invariant subgroup, Ann. of Math. **38** (1937), 533—550.

К о л ч и н Е. Р. (Kolchin E. R.)
1. On certain concepts in the theory of algebraic matric groups, Ann. of Math. **49**, № 4 (1948), 774—789.

К у р о ш А. Г.
1. Теория групп, «Наука», 1967.
2. Лекции по общей алгебре, Физматгиз, 1962.

К э р т и с Ч., Р а й н е р И.
1. Теория представлений конечных групп и ассоциативных алгебр, «Наука», 1969.

Л е н г С.
1. Алгебра, «Мир», 1968.

Максвелл Г. (Maxwell G.)
1. Infinite general linear groups over rings, Trans. Amer. Math. Soc. **151**, № 2 (1970), 371—375.

Мальцев А. И.
1. Об изоморфном представлении бесконечных групп матрицами, Матем. сб. 8 (1940), 405—432.
2. Об одном общем методе получения локальных теорем теории групп, Ученые записки Ивановск. пед. инстит. **1**, № 1 (1941), 3—9.
3. О некоторых классах бесконечных разрешимых групп, Матем. сб. **28** (1951), 567—588.
4. Основы линейной алгебры, «Наука», 1970.
5. Алгебраические системы, «Наука», 1970.

Менникe И. (Mennice I.)
1. Finite factor groups of the unimodular group, Annals of Math. **81**, № 1 (1965), 31—37.

Мерзляков Ю. И.
1. Центральные ряды и ряды коммутантов матричных групп, Алгебра и логика **3**, № 4 (1964), 49—59.
2. О линейных группах с ограниченными циклическими подгруппами, Сиб. матем. ж. **7**, № 2 (1966), 318—321.
3. Целочисленное представление голоморфов полициклических групп, Алгебра и логика **9**, № 5 (1970), 539—558.

Милнор Дж.
1. Кручение Уайтхеда, сб. перев. «Математика» **11**, № 1 (1967), 3—42.

Нисневич В. Л.
1. О группах, изоморфно представимых матрицами над коммутативным полем, Матем. сб. 8 (1940), 395—404.

Новиков П. С., Адян С. И.
1. О бесконечных периодических группах I, II, III, Изв. АН СССР, сер. матем. **32** (1968), 212—244, 251—524, 709—731.

Платонов В. П.
1. К теории алгебраических линейных групп, ДАН СССР **146** (1962), 1025—1026.
2. Разрешимые алгебраические группы, ДАН СССР **151** (1963), 48—51.
3. Расщепляемые линейные группы, ДАН СССР **151** (1963), 286—289.
4. Периодические подгруппы алгебраических групп, ДАН СССР **153** (1963), 270—272.
5. Разрешимые алгебраические группы, ДАН БССР **7** (1963), 298—300.
6. О разрешимых алгебраических линейных группах, ДАН БССР **7** (1963), 439—442.
7. О полной приводимости линейных групп, Изв. АН БССР, сер. физ.-техн. н., № 3 (1964), 126—128.
8. Строение периодических линейных групп и алгебраические группы, ДАН СССР **160** (1965), 541—544.

9. Алгебраические d-группы, ДАН БССР **7** (1963), 729—731.
10. Автоморфизмы алгебраических групп, ДАН СССР **168** (1966), 1257—1260.
11. Теория алгебраических линейных групп и периодические группы, Изв. АН СССР, сер. матем. **30** (1966), 573—620.
12. Подгруппа Фраттини линейных групп и финитная аппроксиммируемость, ДАН БССР **171** (1966), 798—801.
13. Линейные группы с тождественными соотношениями, ДАН БССР **11** (1967), 581—582.
14. Доказательство гипотезы конечности для разрешимых подгрупп алгебраических групп, Сиб. матем. ж. **10**, № 5, 1969, 1084—1090.

Платонов В. П., Залесский А. Е.
1. Задача Ауэрбаха, ДАН БССР **10** (1966), 5—6.

Плоткин Б. И.
1. О некоторых признаках локально нильпотентных групп, УМН **9**, № 3 (1954), 181—186.
2. О нильгруппах, ДАН СССР **94** (1954), 999—1001.
3. О бесконечномерных линейных группах, ДАН СССР **153** (1963), 42—45.
4. Группы автоморфизмов алгебраических систем, «Наука», 1966.

Просесси К. (Procesi C.)
1. The Burnside problem, J. Algebra **4**, № 3 (1966), 421—425.

Райнер И. (Reiner I.)
1. Normal subgroups of the unimodular group, Illinois J. Math. **2**, № 1 (1958), 142—144.

Розенберг А. (Rosenberg A.)
1. The structure of the infinite general linear group, Ann. Math. **68**, № 2 (1958), 278—294.

Сельберг А.
1. О дискретных группах в многомерных симметрических пространствах, сб. перев. «Математика» **6**, № 3 (1962), 3—15.

Серр Ж.-П.
1. Линейные представления конечных групп, «Мир», 1970.

Суон Р. Г. (Swan R. G.)
1. Representation of polycyclic groups, Proc. Amer. Math. Soc. **18**, № 3 (1967), 573—574.

Супруненко Д. А.
1. Примитивные разрешимые группы подстановок, Матем. сб. **20** (1947), 331—350.
2. Разрешимые группы матриц, Ученые записки БГУ, вып. **12** (1951), 74—112.
3. Неприводимые нильпотентные матричные группы простой степени, Матем. сб. **31** (1952), 353—358.
4. О матричных нильпотентных группах, Ученые записки БГУ, вып. **15** (1953), 3—6.
5. О нильпотентных транзитивных подгруппах симметрической группы, ДАН СССР **99** (1954), 23—25.

6. О неприводимых нильпотентных матричных группах, Матем. сб. **35** (1954), 501—512.
7. Локально нильпотентные неприводимые подгруппы полной линейной группы, ДАН СССР **102** (1955), 41—44.
8. Разрешимые и нильпотентные линейные группы, Минск, 1958.
9. Вещественные линейные локально нильпотентные группы, Матем. сб. **50** (1960), 59—66.
10. О периодических линейных группах, Сиб. матем. ж. **3**, № 1 (1962), 87—94.
11. О периодических подгруппах разрешимых матричных групп, ДАН СССР **147** (1962), 310—312.
12. О гомоморфизме Минковского, Сб. памяти Н. Г. Чеботарева, Казань, 1964, 89—92.
13. Ядро одного гомоморфизма, Сиб. матем. ж. **6**, № 1 (1965), 199—206.
14. Локально нильпотентные матричные группы над произвольным полем, Матем. сб. **68** (1965), 614—622.
15. О локально нильпотентных подгруппах бесконечной симметрической группы, ДАН СССР **167** (1966), 302—304.
16. Одно условие полной приводимости матричной группы, Изв. АН СССР, сер. матем. **27** (1963), 435—438.
17. О разрешимых подгруппа мультипликативной группы тела, Изв. АН СССР, сер. матем **26** (1962), 631—638.
18. Две теоремы о матричных группах, ДАН БССР **8** (1964), 491—494.
19. О максимальных нильпотентных подгруппах полной линейной группы над фактор-кольцом $Z/(p^m)$, Матем. сб. **66** (1965), 598—607.
20. Неприводимые части приводимой максимальной локально нильпотентной матричной группы, Изв. АН СССР, сер. матем. **32** (1968), 527—532.
21. К теории коммутативных матричных алгебр над несовершенным полем, Изв. АН БССР, сер. физ.-матем. н., № 3 (1967), 9—19.
22. К теории разрешимых линейных групп, Сиб. матем. ж. **10**, № 5 (1969), 1161—1172.
23. Подгруппы полной линейной группы над телом D, содержащие группу всех специальных треугольных матриц $U(n, D)$, ДАН БССР **14** (1970), 305—308.

Супруненко Д. А., Апатенок Р. Ф.
1. О нильпотентных неприводимых линейных группах над конечным полем, ДАН БССР **3** (1959), 475—478.
2. Нильпотентные неприводимые группы матриц над конечным полем, ДАН БССР **5** (1961), 535—537.

Супруненко Д. А., Station Гаращук М. С.
1. Линейные группы с категорией, ДАН БССР **6** (1962), 411—414.
2. Линейные группы с условием Энгеля, ДАН БССР **6** (1962), 277—280.

Супруненко Д. А., Жаврид Г. П.
1. Интранзитивные нильпотентные подгруппы симметрической группы, ДАН БССР **2** (195[illegible]), 320—322.

С у п р у н е н к о Д. А., П л а т о н о в В П.
1. Об одной теореме Шура, ДАН БССР 7 (1963), 510—512.

С у п р у н е н к о Д. А., Т ы ш к е в и ч Р И.
1. Перестановочные матрицы, «Наука и техника», Минск, 1966.
2. Приводимые локально нильпотентные линейные группы, Изв. АН СССР, сер. матем. **24** (1960), 787—806.

У и р А. И. (Weir A. I.)
1. Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p, Proc. Amer. Math. Soc. **6**, № 4 (1955), 529—533.

Ф е й т В., Т о м п с о н Дж. (Feit W., Thompson J.)
1. Solvability of groups of odd order, Pacific J. Math. **13**, № 3 (1963), 775—1024.

Х о л л М.
1. Теория групп, ИЛ, 1962.

Х о л л Ф.
1. Нильпотентные группы, сб. перев. «Математика» **12**, № 1 (1968), 3—36.

Х у п п е р т Б. (Huppert B.)
1. Lineare auflösbare Gruppen, Math. Z. **67** (1957), 479—518.

Ц а с с е н х а у з Х. (Zassenhaus H.)
1. Beweis eines Satzes über diskrete Gruppen, Abhandl. Math. Sem. Hansische Univ. **12** (1938), 289—312.

Ш м и д т О. Ю.
1. Избранные труды, Математика, Изд-во АН СССР, 1959.

Ш у р И. (Schur I.)
1. Über Gruppen periodischer linearer Substitutionen, S—B, Preuss Akad. der Wiss., 1911, 619—627.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ