АКАДЕМИЯ НАУК СССР
СИБИРСКОЕ ОТДЕЛЕНИЕ
ИНСТИТУТ ФИЗИКИ

В. М. БУСАРКИН, Ю. М. ГОРЧАКОВ

КОНЕЧНЫЕ СЩЕПЛЯЕМЫЕ ГРУППЫ

ИЗДАТЕЛЬСТВО «НАУКА»
МОСКВА 1968

УДК 519.443

Конечные расщепляемые группы. Бусаркин В. М., Горчаков Ю. М. Изд-во «Наука», 1968.

В книге излагаются результаты теории конечных расщепляемых групп, полученные на протяжении примерно 70 лет различными авторами. Интерес представляют не только приведенные в работе данные, но и методы их получения.

Монография предназначена для специалистов в области алгебры, а также для аспирантов, студентов старших курсов вузов.

Библиография — 72 назв.

Ответственный редактор

кандидат физико-математических наук
В. М. КОПЫТОВ

2-2-3
135-68 (II полугодие)

ВВЕДЕНИЕ

Группа *расщепляема*, если она является объединением некоторой совокупности собственных подгрупп, попарно пересекающихся по единичной подгруппе. Эту совокупность подгрупп называют *расщеплением* группы (термин, по-видимому, принадлежит Юнгу [70], а сами подгруппы — *компонентами* расщепления. В явном виде понятие расщепляемой группы встречается уже в работе Миллера [44]. В настоящей работе исследуются конечные расщепляемые группы. Некоторые важные классы расщепляемых групп были рассмотрены в конце прошлого и начале нашего веков. Например, в книге Диксона [18] приведено полное описание проективных линейных групп $PGL(2,q)$ и $PSL(2, q)$ над конечными полями. Особое положение в теории групп занимает следующий результат Фробениуса [26].

Если в транзитивной группе подстановок n символов каждая подстановка перемещает не менее $n-1$ символа, то подстановки, перемещающие все символы, образуют вместе с единицей группы нормальный делитель порядка n.

Группы, удовлетворяющие условиям этой теоремы, называют *группами Фробениуса*. Дальнейшие успехи теории расщепляемых групп связаны с изучением групп Фробениуса. Сразу же возникли две проблемы:

1) проблема классификации групп регулярных автоморфизмов и

2) проблема изучения групп, допускающих такие автоморфизмы.

Первая из них была решена Цассенхаузом [72] в 1936 г. Особенно много исследований связано со второй проблемой, окончательное решение которой не получено. О. Ю. Шмидт (1940 г.) [10] построил первый пример группы Фробениуса с некоммутативным инвариантным множителем и дал критерий коммутативности последнего. Существенный вклад в изучение групп Фробе-

ниуса внес Фейт (см. список литературы). В 1959 г. Томпсон [63, 64] доказал нильпотентность конечной группы, допускающей регулярный автоморфизм простого порядка.

Описание расщепляемых групп было бы невозможным без продвижения в другом направлении теории групп — абстрактной характеризации линейных групп и транзитивных групп подстановок. Здесь следует отметить основополагающую статью Цассенхауза [71]. За последние годы в этой области получено много сильных результатов. Большого успеха добился М. Сузуки. В частности, он открыл в 1960 г. [55] новый класс конечных простых групп (§ 1). Их открытие позволило Сузуки [56] завершить классификацию конечных неразрешимых расщепляемых групп.

Длительное время систематически занимался расщепляемыми группами П. Г. Конторович. Однако зарубежным авторам многие из его работ, по-видимому, остались неизвестными. Например, Бер [11] ввел понятие *нормального расщепления* (расщепления, содержащего вместе с подгруппой все с ней сопряженные подгруппы) и доказал его существование для конечных групп. М. Сузуки [56] (со ссылкой на Бера) снова доказал этот результат. Заметим, что он был доказан П. Г. Конторовичем [5] на 18 лет раньше и без ограничения на мощность группы *. В работе Бера передоказываются также и некоторые другие результаты П. Г. Конторовича (см. РЖМат, 1962, 2А183).

---

* В дальнейшем не представится случая доказать этот результат. Поэтому докажем его сейчас.

Пусть семейство $\{A_\alpha\}$ подгрупп группы G образует расщепление, все компоненты которого не расщепляемы. Для любого $x \in G$ семейство $\{x^{-1}A_\alpha x\}$ также образует расщепление. Так как A_α (а поэтому и $x^{-1}A_\alpha x$) не расщепляемы, то для любых α и β A_α и $x^{-1}A_\beta x$ либо совпадают, либо имеют единичное пересечение. Следовательно, семейства $\{A_\alpha\}$ и $\{x^{-1}A_\alpha x\}$ совпадают, что означает нормальность.

ОБОЗНАЧЕНИЯ И ТЕРМИНЫ

$PGL(2, q)$ — проективная линейная группа над полем из q элементов (см. § 1).

$PSL(2, q)$ — проективная специальная линейная группа (см. § 1).

$GL(2, q)$ — полная линейная группа (см. § 1).

$SL(2, q)$ — специальная линейная группа (см. § 1).

$G(q)$ — простая группа Сузуки (см. § 1).

S_n — симметрическая группа n символов.

A_n — знакопеременная группа n символов.

$S(q, x)$ — 2-группа Сузуки (см. § 1).

$M(q, x)$ — голоморф 2-группы Сузуки (см. § 7).

$GF[q]$ — поле из q элементов.

$N_P(X)$ — нормализатор множества X в подгруппе P группы G.

$N(X)$ — то же при $P = G$.

$C_P(X)$ — централизатор множества X в подгруппе P группы G.

$C(X)$ — то же при $P = G$.

$Z(G)$ — центр группы G.

G' — коммутант группы G.

$\{X, Y\}$ — группа, порожденная множествами элементов X и Y.

$S \times P$ — прямое произведение групп S и P.

$S \leftthreetimes P$ — полупрямое произведение групп S и P.

$X \setminus Y$ — теоретикомножественная разность X и Y.

$|X|$ — порядок группы X.

$|X : Y|$ — индекс группы Y в группе X.

$\{1\}$ — единичная группа.

1 — единица группы.

$[x, y]$ — коммутатор элементов x и y, $x^{-1}y^{-1}xy$.

$|b|$ — порядок элемента b.

(a, b) — наибольший общий делитель чисел a и b.

a/b — число b делит число a.

Расщепляемая группа (см. введение).

Расщепление группы (см. введение).

Компонента расщепления (см. введение).

Нормальное расщепление (см. введение).

Допустимая подгруппа (*относительно данного расщепления*) — это подгруппа, которая либо пересекается по единичной подгруппе с компонентой данного расщепления, либо целиком содержит ее.

Группа Фробениуса (см. введение).

Дополнительный множитель группы Фробениуса — подгруппа, совпадающая со своим нормализатором и взаимно простая с сопряженными подгруппами.

Инвариантный множитель группы Фробениуса — подгруппа, образованная элементами, не принадлежащими дополнительному множителю и сопряженным с ним подгруппам, вместе с единицей группы.

Изолированная подгруппа — подгруппа, содержащая целиком всякую циклическую подгруппу, с которой она имеет неединичное пересечение.

Сильно изолированная подгруппа — это подгруппа, содержащая централизатор каждого своего неединичного элемента.

Изолятор (*подгруппы*) — наименьшая изолированная подгруппа, содержащая данную подгруппу.

HT-группа (см. § 8).

ZT-группа (см. § 11).

Примарная группа — p-группа по некоторому простому числу p.

p'-группа — группа порядка, взаимно простого с p.

Группа диэдра — группа, порожденная элементами a, b, удовлетворяющими соотношениям: $a^n = b^2 = 1$, $bab = a^{-1}$.

Нормальное p-дополнение — инвариантная p'-подгруппа, индекс которой — степень p.

Голоморф пары (B, A) — группа пар (b, a), где $b \in B$, $a \in A$ с умножением $(b, a)\ (b_1, a_1) = (bb_1^{a^{-1}}, aa_1)$, A — группа операторов группы B.

Инволюция — элемент второго порядка.

p-элемент — элемент, порядок которого — степень p.

p'-элемент — элемент порядка, взаимно простого с p.

Элемент составного порядка — неединичный элемент не простого порядка.

Регулярный автоморфизм — автоморфизм φ, удовлетворяющий условию $x^\varphi \neq x$ для любого неединичного элемента x.

Глава I

СВОДКА РЕЗУЛЬТАТОВ

§ 1. Классы расщепляемых групп

Цель книги — доказать следующую теорему.

Теорема 1. *Конечная расщепляемая группа есть группа одного из следующих типов*:

1) *расщепляемая p-группа*;

2) *группа Фробениуса*;

3) *HT-группа*;

4) S_4*-симметрическая группа подстановок четырех символов*;

5) $PGL(2, q)$, $q \geqslant 5$ — *нечетное число*, — *проективная линейная группа над полем из q элементов*;

6) $PSL(2, q)$, $q \geqslant 4$, — *специальная проективная линейная группа*;

7) $G(q)$, $q = 2^{2k+1}$, $k \geqslant 1$, — *простая группа Сузуки*.

Группы типов 1) — 7) — расщепляемы.

Ниже будут описаны эти группы и некоторые их расщепления.

В теореме ничего не сказано о строении расщепляемых p-групп, так как оно неизвестно. Ясно, что любая группа, все неединичные элементы которой имеют один и тот же простой порядок p, расщепляема. Но существуют также расщепляемые p-группы, содержащие элементы порядка более p.

Предположим, что конечная расщепляемая p-группа P содержит элементы составного порядка. Породим ими подгруппу P_0. Так как P расщепляема, то $P_0 \neq P$. Все элементы, лежащие вне P_0, имеют порядок p. Поэтому группа P обладает расщеплением, состоящим из P_0 и циклических подгрупп простого порядка. Неизвестно, совпадает ли $|P : P_0|$ с p (см. Хьюгес и Томпсон [35]). Другая формулировка этого вопроса такова: единственное ли

расщепление имеет конечная расщепляемая p-группа, содержащая элементы составного порядка?

Группы Фробениуса и только они обладают совпадающей со своим нормализатором компонентой нормального расщепления. Все такие компоненты сопряжены и содержатся в любом нормальном расщеплении.

Если A — совпадающая со своим нормализатором компонента нормального расщепления конечной группы G, то $G = B \diagup\!\!\diagdown A$, где B — объединение компонент, не сопряженных с A. Всякий неединичный элемент из A индуцирует в B регулярный автоморфизм. Цассенхауз [72] дал полную классификацию групп регулярных автоморфизмов (см. § 5). Томпсон [64, 65] доказал нильпотентность инвариантного множителя группы Фробениуса. Однако неизвестно, какие нильпотентные группы допускают группу регулярных автоморфизмов. Хигмен [33] рассмотрел важный случай — 2-группы, допускающие циклическую группу автоморфизмов, транзитивную на множестве инволюций. *Если 2-группа Q неабелева и содержит $q - 1 > 1$ инволюций, то*

1) *порядки элементов в Q не превосходят* 4;

2) $|Q| = q^2$ *или* q^3;

3) *если* $|Q| = q^2$, *то Q изоморфна группе $S(q; x)$, которая определена ниже.*

Пусть F — конечное поле из q элементов, где $q = 2^n > 2$, и пусть x — такой автоморфизм поля F, что из $x \neq 1$ и $\alpha^{1+x} = 1$ вытекает, что $\alpha = 1$. Матрицы вида

$$(\alpha, \beta) = \begin{pmatrix} 1 & 0 & 0 \\ \alpha^x & 1 & 0 \\ \beta & \alpha & 1 \end{pmatrix}, \quad \alpha \text{ и } \beta \in F,$$

образуют группу порядка q^2. Следуя Сузуки [58], обозначим ее $S(q; x)$. Свойства группы $S(q; x)$ рассмотрены в § 7.

Если A — группа регулярных автоморфизмов конечной группы B, то голоморф пары (B, A) есть группа Фробениуса.

Так как отличная от своего нормализатора компонента нормального расщепления нильпотентна, то лишь группы Фробениуса могут содержать ненильпотентную компоненту нормального расщепления.

Как p-группы, так и группы Фробениуса всегда имеют нормальное расщепление, относительно которого допустим некоторый нормальный делитель. К классу групп с допустимым нормаль-

ным делителем относятся еще HT-группы, которые имеют следующее строение (см. § 8):

$$G = (S \times P) \leftthreetimes \{a\},$$

где $a^p = 1$, $S \leftthreetimes \{a\}$ — группа Фробениуса, $P \leftthreetimes \{a\}$ — p-группа и P — компонента некоторого расщепления группы $P \leftthreetimes \{a\}$. Группа G имеет центр и поэтому обладает единственным расщеплением, состоящим из допустимого нормального делителя $S \times P$ и подгрупп одного и того же порядка p. Заметим, что в отличие от HT-групп порядок непримарной компоненты расщепления группы Фробениуса взаимно прост с индексом.

Совокупность невырожденных матриц $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ с коэффициентами из $GF[q]$, $q = p^n$, обозначают $GL(2, q)$. Центр группы $GL(2, q)$ состоит из матриц $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ и имеет порядок $q - 1$. Фактор-группа $GL(2, q)$ по центру есть $PG(2, q)$. Порядок последней равен $q(q^2 - 1)$. Множество матриц с определителем 1 образует группу $SL(2, q)$ порядка $q(q^2 - 1)$. Центр группы $SL(2, q)$ состоит из матриц вида $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ с $\lambda^2 = 1$. Поэтому если q — нечетное число, то порядок центра равен 2, а если q — четное число, то порядок равен 1. Соответственно порядок фактор-группы $PSL(2, q)$ группы $SL(2, q)$ по центру равен $q(q^2 - 1)/2$ и $q(q^2 - 1)$. Группа $PSL(2, q)$ проста для $q \geqslant 4$. Подробно о группах $PGL(2, q)$ и $PSL(2, q)$ смотрите в книге Диксона [18].

Всякая циклическая подгруппа группы $PGL(2, q)$ сопряжена некоторой подгруппе одной из трех максимальных абелевых подгрупп A_1, A_2, A_3 порядков q, $q - 1$, $q + 1$ соответственно. A_1 — элементарная абелева подгруппа, A_2 и A_3 — циклические группы. Пересечение двух различных указанных максимальных абелевых подгрупп равно единичной группе.

Группа $PSL(2, q)$ имеет следующие подгруппы:

$q+1$ сопряженных абелевых элементарных подгрупп порядка q;

$1/2\ q\ (q \pm 1)$ сопряженных циклических подгрупп порядка $(q \mp 1)/2$; 1, 2 и 1 берутся в знаменателе согласно $p > 2$ и $p = 2$;

$1/2\ q\ (q \pm 1)$ сопряженных циклических подгрупп порядка $d_\mp$, $d_\mp$ делит $\frac{q-1}{2;\ 1}$;

$M(q)/2d_\mp$ сопряженных групп диэдра порядка $2d_\mp$, где $d_\mp$ — нечетное число и $M(q) = q(q^2 - 1)$ для $p = 2$ и $M(q) = q(q^2 - 1)/2$ для $p > 2$;

две системы, каждая из $M(q)/4d_{\mp}$ сопряженных групп диэдра порядка $2d_{\mp}$, где $d_{\pm}$ — четное число, большее 2;

для $p^n = 8h \pm 3$ одно множество из $M(q)/12$ сопряженных нециклических подгрупп порядка 4;

$\frac{(p^n-1)(p^n-p)\ldots(p^n-p^{m-1})}{(p^m-1)(p^m-p)\ldots(p^m-p^{m-1})}$ множеств каждое из $\frac{p^{2n}-1}{(2,1;1)(p^k-1)}$

сопряженных коммутативных групп порядка p^m, где $(2, 1; 1)$ означает 2, 1 или 1 согласно одному из случаев: $p > 2$ и n/k — четное число, $p > 2$ и n/k — нечетное число; или $p = 2$ и n/k — целое число; k — делитель m, зависящий от свойств группы порядка p^m;

множество из $\frac{(p^{2n}-1)\,p^{n-m}}{(2,1;1)(p^k-1)}$ сопряженных групп Фробениуса порядка $p^m d_-$, где k и d_- зависят от m;

$(2, 1; 1)$ множеств, каждое из $M(q)/(2, 1; 1)\ M(p^k)$ сопряженных подгрупп, изоморфных $PSL(2, p^k)$, k — делитель n;

две системы, каждая из $M(q)/2M(p^k)$ сопряженных подгрупп, изоморфных $PGL(2, p^k)$, $p > 2$, n/k — четное число;

для $q = 8h \pm 1$ два множества, каждое из $M(q)/24$ сопряженных подгрупп S_4;

для $q = 8h \pm 1$ два множества, каждое из $M(q)/24$ сопряженных подгрупп A_4;

для $q = 8h \pm 3$ или $q = 2^n$, n — четное число, $M(q)/12$ сопряженных подгрупп A_4;

для $q = 10l \pm 1$ две системы, каждая из $M(q)/60$ сопряженных подгрупп A_5.

Из этих данных видно, что группы $PGL(2, q)$ и $PSL(2, q)$ имеют расщепление, состоящее из циклических подгрупп.

Группа $PGL(2, q)$, где $q \geqslant 5$ — нечетное число, непроста. Она не имеет допустимых нормальных делителей. В § 9 доказано, что, кроме $PGL(2, q)$, где $q \geqslant 5$ — нечетное число, существует единственная расщепляемая группа, не имеющая допустимых нормальных делителей,— это S_4. Впрочем, $S_4 \cong PGL(2, 3)$.

Группа $PSL(2, q)$, $q \geqslant 4$ проста. К расщепляемым группам относятся и простые группы Сузуки $G(q)$, определенные ниже.

Пусть F — конечное поле из $q = 2^{2k+1}$, $k \geqslant 1$, элементов. Если $r^2 = 2q$, то $\theta : \alpha \to \alpha^r$ — такой автоморфизм поля F, что $\theta^2 = 2$. Пусть α и β — произвольные элементы из F. Обозначим

через (α, β) такую матрицу:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \alpha^{1+\theta}+\beta & \alpha^{\theta} & 1 & 0 \\ \alpha^{2+\theta}+\alpha\beta+\beta & \beta & \alpha & 1 \end{pmatrix}.$$

Нетрудно убедиться, что

$$(\alpha, \beta)\ (\gamma, \delta) = (\alpha + \gamma,\ \alpha\gamma^{\theta} + \beta + \delta).$$

Совокупность $Q\ (q)$ матриц (α, β) образует группу, изоморфную $S\ (q; x)$ (см. § 7). Каждому элементу $k \in F$ сопоставим диагональную матрицу

$$\begin{pmatrix} k^{1+\theta^{-1}} & 0 & 0 & 0 \\ 0 & k^{\theta^{-1}} & 0 & 0 \\ 0 & 0 & k^{-\theta^{-1}} & 0 \\ 0 & 0 & 0 & k^{-1-\theta^{-1}} \end{pmatrix}.$$

Эту матрицу будем обозначать через k. Совокупность $K\ (q)$ матриц k образует циклическую группу порядка $q - 1$. Верна формула

$$k^{-1}\ (\alpha, \beta)k = (\alpha k,\ \beta k^{1+\theta}). \tag{1}$$

Поэтому группа $H\ (q)$, порожденная $Q\ (q)$ и $K\ (q)$, есть группа порядка $q^2\ (q - 1)$, изоморфная $M\ (q; \theta)$ (см. § 7). Положим

$$\tau = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Обозначим через $G\ (q)$ группу, порожденную $H\ (q)$ и τ. Следующая теорема показывает простоту группы $G\ (q)$.

Т е о р е м а 2. *Если* $q > 2$, то $G\ (q)$ *есть ZT-группа порядка* $q^2\ (q - 1)\ (q^2 + 1)$.

Д о к а з а т е л ь с т в о. Вычисления показывают справедливость следующих равенств:

$$H\ (q) \cap \tau\ H\ (q)\tau = K\ (q), \tag{2}$$

$$H\ (q) \cap \tau\ Q\ (q)\tau = \{1\},$$

$$\tau\ k\tau = k^{-1} \text{ для любого } k \in K\ (q). \tag{3}$$

Если $\eta \in H(q)$ и $\pi \in Q(q)$, то $\eta\tau\pi \in G(q)$. Ясно, что $\eta\tau\pi \notin H(q)$. Если $\eta\tau\pi = \eta_1\tau\pi_1$ для $\eta, \eta_1 \in H(q)$, $\pi, \pi_1 \in Q(q)$, то $\eta_1^{-1}\eta = \tau\pi_1\pi^{-1}\tau \in H(q) \cap \tau Q(q)\tau$. В силу (2) $\eta = \eta_1$ и $\pi = \pi_1$. Итак, существует точно $q^4(q-1)$ элементов вида $\eta\tau\pi$.

Покажем, что каждый элемент из $G(q) \setminus H(q)$ имеет вид $\eta\tau\pi$ с $\eta \in H(q)$ и $\pi \in Q(q)$. Так как группа $G(q)$ порождается $H(q)$ и τ, то достаточно показать, что множество элементов вида $\eta\tau\pi$ вместе с $H(q)$ образует группу. Если $\eta_1 \in H(q)$, то $\eta_1\eta \in H(q)$ и $\eta_1(\eta\tau\pi) = (\eta_1\eta)\tau\pi$. Элемент $\pi\eta_1 \in H(q)$, так что $\pi\eta_1 = k\pi'$, где $k \in K(q)$ и $\pi' \in Q(q)$. Использовав (3), получаем:

$$(\eta\tau\pi)\eta_1 = \eta\tau(\pi\eta_1) = \eta\tau(k\pi') = (\eta k^{-1})\tau\pi'.$$

Если $\pi_1 \in Q(q)$, то

$$(\eta\tau\pi)(\eta_1\tau\pi_1) = \eta\tau(\pi\eta_1)\tau\pi_1 = \eta k^{-1}\tau\pi'\tau\pi_1.$$

Поэтому достаточно доказать справедливость равенства

$$\tau\pi\tau = \eta_2\tau\pi_2 \qquad (\eta_2 \in H(q),\ \pi_2 \in Q(q)) \tag{4}$$

для всех $\pi \neq 1$ из $Q(q)$.

Для простоты обозначим $\sigma = (0, 1)$ и $\rho = (1, 0)$. Верно равенство

$$\tau\sigma\tau = \rho^{-1}\tau\rho,\ \tau\rho\tau = \rho\tau\sigma. \tag{5}$$

Если положить $\pi(k) = \rho k^{-1}\rho^{-1}k$ для $k \neq 1$ из $K(q)$, то получаем

$$\tau\pi(k)\tau = \eta_3\tau\pi_3 \qquad (\eta_3 \in H(q),\ \pi_3 \in Q(q)).$$

В самом деле,

$$\tau(\rho k^{-1}\rho^{-1}k)\tau = \tau\rho\tau\tau k^{-1}p^{-1}k\tau = \rho\tau\sigma k\sigma\tau\rho^{-1}k^{-1} = \\ = \rho k^{-2}\tau k^{-1}(k^{-1}\sigma k\sigma) = k\tau k\rho^{-1}k^{-1}.$$

Элемент $k^{-1}(k^{-1}\sigma k\sigma)k$ имеет порядок 2. Поэтому существует такой элемент $\tau \in K(q)$, что

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

Теперь

$$\tau\pi(k)\tau = \rho k^{-2}\lambda\tau\sigma\tau\lambda^{-1}k\rho^{-1}k^{-1} = (\rho k^{-2}\lambda\rho^{-1})\tau\rho(\lambda^{-1}k\rho^{-1}k^{-1}).$$

Получили предыдущий случай, так как $\rho k^{-2}\lambda\rho^{-1}\tau\rho$ имеет вид $\eta\tau\pi$, а $\lambda^{-1}k\rho^{-1}k^{-1} \in H(q)$.

Формула (5) теперь получается из леммы 13 § 7.

Так как каждый элемент из $G(q) \setminus H(q)$ имеет вид $\eta\tau\pi$, то

$$|G(q)| = q^2(q-1)(q^2+1)$$

и

$$G(q) = H(q) + H(q)\tau H(q).$$

Поэтому $G(q)$ имеет дважды транзитивное представление на смежных классах по $H(q)$.

Подгруппа, которая состоит из элементов, оставляющих на месте $H(q)$ и $H(q)\tau$, совпадает с $K(q)$, так как $K(q) = H(q) \cap \cap \tau H(q)\tau$. Предположим, что $H(q)\tau\pi = H(q)\tau\pi k$ для $\pi \in Q(q)$ и $k \in K(q)$. Тогда $\tau\pi k = \eta\tau\pi$ для некоторого $\eta \in H(q)$. Отсюда следует, что $\tau k^{-1}\pi k = k\eta\tau\pi$. Поэтому $k^{-1}\pi k = \pi$. Это означает, что либо $k = 1$, либо $\pi = 1$. Следовательно, лишь 1 оставляет на месте три различных смежных класса. Так как $Q(q)$ имеет более одной инволюции, то $G(q)$ не группа Фробениуса. Этим доказано, что $G(q)$ — ZT-группа.

Сузуки [58] описал подгруппы группы $G(q)$.

Теорема 3. *Группа $G(q)$ имеет следующие максимальные подгруппы*:

1) *$H(q)$-группа Фробениуса порядка $q^2(q-1)$, изоморфна $M(q; \theta)$, где $\theta^2 = 2$;*

2) *группа диэдра порядка $2(q-1)$;*

3) *группа Фробениуса $\{a\} \setminus \{b\}$, где $a^{q+r+1} = b^4 = 1$, $r^2 = 2q$;*

4) *группа Фробениуса $\{a\} \setminus \{b\}$, где $a^{q-r+1} = b^4 = 1$;*

5) *$G(s)$, где $s^t = q$, t — простой делитель числа $2k+1$.*

§ 2. Изолированные подгруппы

Напомним, что подгруппа называется изолированной, если она взаимно проста со всякой не содержащейся в ней циклической подгруппой. Строение изолированных подгрупп описывается следующей теоремой (Бусаркин В. М. [3]).

Собственная изолированная подгруппа M конечной группы G является группой одного из следующих типов:

1) *M — нильпотентная группа*;

2) *M — дополнительный множитель в группе Фробениуса G*;

3) *M — группа Фробениуса*;

4) *M изоморфна $SL(2, 2^n)$, $n > 1$*;

5) *в M существует характеристический ряд*

$$\{1\} \subset N \subset NP \subset M,$$

где N — нильпотентная характеристическая подгруппа из M, P — силовская p-подгруппа M простого порядка, NP — группа Фробениуса, фактор-группа M/N — группа Фробениуса с инвариантным множителем порядка p.

Группы, содержащие собственные изолированные подгруппы, мало изучены. Класс таких групп содержит, например, расщепляемые группы и дважды транзитивные группы подстановок, у которых только тождественная подстановка оставляет на месте три символа. Среди имеющихся в этом направлении результатов отметим следующие:

1) *теорема Фробениуса*;

2) *конечная группа, содержащая собственную сильно изолированную подгруппу четного порядка, является либо группой Фробениуса, либо ZT-группой* (Сузуки [60]);

3) *конечная группа четного порядка, содержащая совпадающую со своим нормализатором изолированную подгруппу нечетного индекса, является либо группой Фробениуса, либо ZT-группой* (Бусаркин В. М. [3]);

4) *конечная группа, покрываемая собственными изолированными подгруппами, расщепляема* (Бусаркин В. М. [3]).

Глава II

ГРУППЫ ФРОБЕНИУСА

§ 3. Теорема Фробениуса

Одним из важнейших результатов теории представлений групп является следующая теорема, полученная Г. Фробениусом в 1901 г. [26].

Теорема 1. *Пусть G—транзитивная группа подстановок n символов, в которой каждая подстановка однозначно определяется образами двух символов. Тогда регулярные подстановки вместе с тождественной подстановкой образуют транзитивный нормальный делитель порядка n.*

Обозначим через H подгруппу тех подстановок, которые не изменяют некоторый символ, скажем a. Так как в G только тождественная подстановка оставляет на месте более одного символа, то, очевидно, $H \cap xHx^{-1} = \{1\}$ для всякого элемента $x \in G \setminus H$. Обратно, если конечная группа G имеет такую подгруппу H индекса n, что $H \cap xHx^{-1} = \{1\}$ для всякого элемента группы, не содержащегося в H, то представление группы G подстановками смежных классов по группе H есть транзитивная группа подстановок n символов, в которой каждая подстановка однозначно определяется образами двух символов. Теореме Фробениуса теперь можно придать следующую формулировку.

Теорема 1′. *Если конечная группа G содержит подгруппу H, совпадающую со своим нормализатором и взаимно простую с каждой из своих сопряженных подгрупп, то совокупность элементов из G, не входящих ни в H, ни в одну из сопряженных с H подгрупп, вместе с единичным элементом образует нормальный делитель F.*

Доказательство теоремы 1. Пусть G—транзитивная группа подстановок, в которой только тождественная подстановка оставляет на месте два различных символа. Очевидно, можно считать, что подгруппа H, образованная элементами, которые оставляют неподвижным некоторый фиксированный символ, не единичная группа.

Рассмотрим группу G как представление самой себя. Так как представление транзитивно, то его характер есть сумма единичного характера и некоторого другого характера, скажем χ_1. $\chi_1(1) = n - 1$, $\chi_1(g) = 0$ для любого неединичного элемента g, сопряженного с некоторым элементом из H, и $\chi_1(g) = -1$ для остальных элементов.

Пусть ψ — неприводимый характер подгруппы H. ψ индуцирует характер χ группы G. Ясно, что $\chi(1) = n\psi(1)$, $\chi(g) = \psi(h)$, если g сопряжен с некоторым неединичным элементом h из H, из $\chi(g) = 0$ для остальных элементов.

Вычислим скалярный квадрат обобщенного характера $\omega = \chi - \psi(1)\chi_1$

$$(\omega, \omega) = \frac{1}{|G|} \sum_{s \in G} (\chi(s) - \psi(1)\chi_1(s))\,\overline{(\chi(s) - \psi(1)\chi_1(s))}.$$

Просуммировав сперва по всем неединичным элементам группы G, сопряженным с элементами из H, получаем

$$\frac{n}{|G|} \sum_{\substack{s \in H \\ s \neq 1}} \psi(s)\overline{\psi(s)} = \frac{n(|H| - \psi^2(1))}{|G|}.$$

Сумма по остальным неединичным элементам равна

$$\frac{\psi^2(1)}{|G|} \sum \chi_1^2(s) = \frac{(n-1)\psi^2(1)}{|G|}.$$

Следовательно,

$$(\omega, \omega) = \frac{1}{|G|}\{\psi^2(1) + n(|H| - \psi^2(1)) + (n-1)\psi^2(1)\} = 1.$$

Это означает, что ω — неприводимый характер группы G.

Положим $\xi = \sum_{\psi} \psi(1)(\chi - \psi(1)\chi_1)$, где суммирование ведется по всем неприводимым характерам ψ группы H и где χ — характер группы G, индуцированный характером ψ. Ограничение ξ на H есть характер регулярного представления группы H. По-

этому $\xi(h) = 0$ для любого неединичного элемента h группы H. Если элемент g не сопряжен ни с одним элементом из H, то $\xi(g) = \xi(1)$. Но это доказывает теорему.

§ 4. Простейшие свойства групп Фробениуса

Из теоремы Фробениуса следует расщепляемость групп Фробениуса. Если H — дополнительный множитель группы Фробениуса, то нормализатор любой подгруппы H_1 из H содержится в последней. В частности, H сильно изолирована. Так как то же самое справедливо для любой подгруппы, сопряженной с H, то сильно изолирован инвариантный множитель группы Фробениуса. Следовательно, любой неединичный элемент, не содержащийся в инвариантном множителе, индуцирует в нем регулярный автоморфизм.

Пусть G — группа порядка hm, где h и m — взаимно простые числа. Тогда G является группой Фробениуса типа (h, m) в том и только в том случае, когда G содержит инвариантную подгруппу M порядка m и когда порядок каждого элемента из G делит либо h, либо m.

Необходимость условия вытекает из теоремы Фробениуса. Докажем достаточность.

Так как M — холловский нормальный делитель, то $G = M \leftthreetimes H$ для некоторой подгруппы H. Если $H \cap r^{-1}Hr \neq \{1\}$, где $r \in M$, то существуют такие элементы s_1 и $s_2 \in H$, что $r^{-1}s_1 r = s_2$. Так как $s_1^{-1}r^{-1}s_1 r = s_1^{-1}s_2 \in M \cap H = \{1\}$, то $s_1 = s_2$. Если $r \neq 1$, то $|s_1 r|$ не взаимно прост ни с h, ни с m, что противоречит условию. Поэтому $r = 1$. Это означает, что G — группа Фробениуса.

Пусть G — группа Фробениуса типа (h, m). Если G_1 — ее подгруппа порядка $h_1 m_1$, где $h_1 \mid h$, $m_1 \mid m$ и $h_1, m_1 \neq 1$, то G_1 — группа Фробениуса типа (h_1, m_1).

Действительно, порядок каждого элемента группы G делит либо h, либо m. Поэтому порядок каждого элемента группы G_1 делит либо h_1, либо m_1. Так как порядок нормального делителя $G_1 \cap M$ равен m_1, то, согласно предыдущему утверждению, G_1 — группа Фробениуса типа (h_1, m_1).

Если $\overline{G}$ — гомоморфный образ группы Фробениуса G типа (h, m) и если $|\overline{G}| = hm_1$, $m_1 > 1$, то $\overline{G}$ — группа Фробениуса типа (h, m_1).

Достаточно доказать, что порядок каждого элемента из $\overline{G}$ делит либо h, либо m_1. Предположим, что $G = M \leftthreetimes H$, где $|M| = m$, $|H| = h$. Если $\overline{G}$ имеет элемент, порядок которого не делит ни h, ни m_1, то существуют такие элементы $s \in M$ и $t \in H$, что

$$t^{-1}st = ss_1, \tag{1}$$

где s_1 принадлежит ядру M_1 гомоморфизма $G \to \overline{G}$.

Отображение $l \to [t, l]$, где $l \in M$, а $t \in H$, взаимно однозначно. Следовательно, для любого $l \in M$ существует такой элемент $l_1 \in M$, что $l = l_1^{-1}t^{-1}l_1t$.

Теперь (1) перепишем так:

$$s^{-1}t^{-1}st = s_2^{-1}t^{-1}s_2t,$$

где $s_2 \in M_1$. Отсюда получаем

$$s_2s^{-1}t^{-1}s\, s_2^{-1} = t^{-1}.$$

Это означает, что $H \cap s_2s^{-1}\, Hss_2^{-1} \neq \{1\}$, что невозможно. Итак, порядок каждого элемента группы $\overline{G}$ делит либо h, либо m_1.

Теперь легко получить следующие предложения.

Пусть G — группа Фробениуса типа (h, m) и P — ее силовская p-подгруппа порядка p^n, $p|m$. Тогда G содержит подгруппу порядка hp^n, которая есть группа Фробениуса типа (h, p^n).

Если H — группа регулярных автоморфизмов конечной группы, то H — группа регулярных автоморфизмов некоторой элементарной абелевой группы.

Рассмотрим группу Фробениуса G типа (h, m). Если M — подгруппа G порядка m, то для любой инвариантной подгруппы L группы G имеем

1) либо $L \subset M$,

2) либо $L = M$,

3) либо $L \supset M$.

Если предложение не верно, то L, $M \neq LM$. LM — группа Фробениуса типа (h_1, m), где $h_1 \neq 1$. $LM/L \cap M$ — также группа Фробениуса типа (h_1, m_1), где $m_1 = |M : (L \cap M)| \neq 1$. С другой стороны, $LM \,|\, L \cap M$ разлагается в прямое произведение подгрупп $L \,|\, L \cap M$ и $M \,|\, L \cap M$. В группе Фробениуса это невозможно.

Опишем теперь подгруппы группы Фробениуса G типа (h, m). Если A — подгруппа G и $|A| = h_1m_1$ (h_1, $m_1 \neq 1$, $h_1 \mid h$, $m_1 \mid m$),

то A — группа Фробениуса типа (h_1, m_1). Если же $|A| = m_1$, где $m_1 \mid m$, то $A \subseteq M$. И, наконец, если $|A| = h_1$, $h_1 \mid h$, то A содержится в сопряженной с H подгруппе.

Достаточно рассмотреть случай $|A| = h_1$, $h_1 \mid h$. Предположим, что A не содержится ни в одной сопряженной с H подгруппе. Группа A пересекается нетривиально по крайней мере с одной из групп, сопряженных с H, скажем $D = A \cap x^{-1}Hx \neq \{1\}$. Так как A не принадлежит $x^{-1}Hx$, то D — дополнительный множитель группы A. Пусть T — ее инвариантный множитель. Группа T содержит p-подгруппу P, инвариантную относительно D. Можно считать, что P — абелева группа. Ясно, что $P \subseteq y^{-1}Hy$ для $y \notin Hx$. Но тогда для любого $d \in D$

$$y^{-1}Hy \cap d^{-1}y^{-1}Hyd \neq \{1\},$$

что противоречит определению группы Фробениуса.

Из доказанного предложения вытекает сопряженность дополнений для инвариантного множителя.

§ 5. Группы регулярных автоморфизмов

Г. Цассенхауз [72] полностью описал группы регулярных автоморфизмов. Позднее те же результаты получил Винсент [66].

В предыдущем параграфе показано, что группа регулярных автоморфизмов конечной группы изоморфна группе таких же автоморфизмов элементарной абелевой группы. Поэтому конечная группа G тогда и только тогда является группой регулярных автоморфизмов конечной группы, когда G имеет точное представление матрицами с коэффициентами из некоторого поля, все собственные числа которых (матриц) отличны от 1.

Теорема 1 (Бернсайд [14]). *Если подгруппа A группы регулярных автоморфизмов G имеет порядок pq, где p и q (не обязательно различные) простые числа, то A — циклическая группа.*

Доказательство. Считаем, что G — группа регулярных автоморфизмов абелевой группы F и что $|G| = pq$, p и q — простые числа. Группа G порождается элементами a и b, удовлетворяющими соотношениям:

$$a^p = b^q = 1, \qquad b^{-1}ab = a^\alpha.$$

Считаем также, что G — нециклическая группа, т. е. либо $p = q$, либо $\alpha \not\equiv 1 \pmod{p}$.

Пусть $f \in F$ и $f \neq 1$. Рассмотрим таблицу:

$$\begin{array}{llll} f, & f^b, & f^{b^2} & , \ldots, f^{b^{q-1}}, \\ f, & f^{ab}, & f^{(ab)^2} & , \ldots, f^{(ab)^{q-1}}, \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ f, & f^{a^{p-1}b}, & f^{(a^{p-1}b)^2}, & \ldots, f^{(a^{p-1}b)^{q-1}}. \end{array}$$

Из соотношений, связывающих a и b, получаем, что

$$(a^{i-1}b)^q = (b^{-q}a^{i-1}b^q)(b^{-q+1}a^{i-1}b^{q-1}) \ldots (b^{-1}a^{i-1}b) = \\ = a^{(i-1)(\alpha^q+\alpha^{q-1}+\cdots+\alpha)} = 1.$$

Вычислим теперь произведение элементов i-й строки таблицы

$$f \cdot f^{a^{i-1}b} \ldots f^{(a^{i-1}b)^{q-1}} = f^{1+(a^{i-1}b)+\cdots+(a^{i-1}b)^{q-1}} = 1.$$

Отсюда следует, что произведение всех элементов таблицы равно 1.

Перемножим теперь элементы по столбцам. Ясно, что произведение элементов первого столбца равно $f^p \neq 1$. Произведение элементов i-го столбца ($i \geqslant 2$) равно

$$f^{b^{i-1}} \cdot f^{(ab)^{i-1}} \ldots f^{(a^{p-1}b)^{i-1}} = f^{b^{i-1}} \cdot f^{a^{\alpha(i-1)/2}b^{i-1}} \ldots f^{a^{(p-1)\alpha(i-1)i/2}b^{i-1}} = \\ = f^{[1+(a^{\alpha(i-1)i/2})+\cdots+(a^{\alpha(i-1)i/2})^{p-1}]b^{i-1}} = 1.$$

Таким образом, произведение всех элементов таблицы равно $f^p \neq 1$. Противоречие, полученное с предшествующими вычислениями, показывает, что G — циклическая группа.

Теорема 1, в частности, утверждает, что силовские p-подгруппы группы регулярных автоморфизмов либо циклические группы, либо при $p = 2$ группы кватернионов (обобщенная группа кватернионов). Разрешимые группы с такими силовскими подгруппами описаны Цассенхаузом [72], а неразрешимые — Сузуки [49].

В следующем параграфе описаны группы, всякая подгруппа порядка pq которых циклическая. В классе таких групп выделены группы, которые могут служить в качестве группы регулярных автоморфизмов некоторой конечной группы.

Т е о р е м а 2. *Конечная разрешимая группа G тогда и только тогда является группой регулярных автоморфизмов, когда она есть группа одно о из следующих типов* (см. § 6):

1) *циклическая группа*;

2) *группа, определенная следствием 3*;

3) — 9) *группа типа а) — ж)*.

В силу предыдущих результатов осталось лишь доказать, что каждая из перечисленных групп имеет точное представление над некоторым полем, при котором характеристические числа матриц отличны от 1.

Докажем это утверждение индукцией по порядку группы G. Пусть G_0 — подгруппа неразложимой в прямое произведение группы G, порожденная элементами простых порядков. Из строения перечисленных групп следует, что $G_0 = G$ тогда и только тогда, когда либо $|G|$ — простое число, либо $|G| = 24$ и $G \cong SL(2,3)$. В любом из этих случаев G имеет точное представление над полем комплексных чисел, и характеристические корни матриц при этом представлении отличны от 1. Пусть теперь $G_0 \neq G$. Так как $|G_0| < |G|$, то G_0 имеет необходимое представление ρ над полем комплексных чисел. Ввиду инвариантности G_0 в G индуцированное представление ρ^G группы G удовлетворяет всем требованиям. Теорема доказана.

Т е о р е м а 3. *Конечная неразрешимая группа G регулярных автоморфизмов содержит подгруппу G_1 индекса 1 или 2 и типа*

$$G_1 = M \times U,$$

где $M \cong SL(2,5)$ порождается элементами c и d с соотношениями:

$$c^2 = d^3 = (cd)^5, \qquad c^4 = 1,$$

и группа U — либо единичная группа, либо порождается элементами a, b с соотношениями:

$$a^m = 1, \qquad b^n = a^t, \qquad bab^{-1} = a^r,$$

где натуральные числа m, n, t, r удовлетворяют следующим условиям:

$$(m,\ r-1) = r_0 > 0,\ r_0 t = m > 0,\ n > 0,\ r^n \equiv 1 \pmod{m},$$
$$r^v \not\equiv 1 \pmod{m},$$

где $0 < v < n$, $(n,\ t) = 1$, если p — простой делитель n, то p делит r_0, $(nm,\ 30) = 1$.

Если G отлична от G_1, то G еще имеет элемент e, удовлетворяющий следующим соотношениям:

$$e^2 = (ec)^4 = c^2, \qquad eae^{-1} = a^x, \qquad ebe^{-1} = b^x,$$

где $x^2 \equiv 1 \pmod{m}$, $x \equiv 1 \pmod{n}$.

Доказательство. Если группа G отлична от своего коммутанта, то в предположении справедливости теоремы для групп меньшего порядка нетрудно доказать ее и для G. Поэтому считаем, что G совпадает со своим коммутантом. Теорема 5 § 6 в этом случае утверждает, что $G \cong SL(2, q)$, где $q = 2^k + 1$ — простое число. Докажем, что $q = 5$.

Пусть ρ — представление G, при котором все характеристические числа отличны от 1, и пусть χ — характер ρ. Группа G имеет три класса максимальных абелевых подгрупп A_1, A_2, A_3 порядков $2m_1 = 2q$, $2m_2 = q + 1$, $2m_3 = q - 1$. Эти группы циклические. Так как G не имеет элементов порядка qr, где r — нечетный делитель числа $q + 1$, то (Бернсайд [14, § 254]) $\chi(a)$ — рациональное число для любого элемента a нечетного порядка. Следовательно, представление $\rho \mid A_i$ $(i = 1, 2)$ содержит все $\varphi(2\ m_i)$ точные неприводимые представления группы A_i ($\varphi(x)$ — функция Эйлера). Потому $\varphi(2m_i)$ делит $\chi(1)$ для $i = 1, 2$. Значения характера χ образуют поле алгебраических чисел степени d. Характер χ имеет d сопряженных характеров. Их сумму обозначим через ψ. ψ — рациональный характер степени $d\chi(1)$. Ясно, что $d\chi(1)$ делится на $\varphi(2m_i)$, $i = 1,2$. Неприводимое точное представление нормализатора группы A_1 имеет степень $q - 1/2$. Следовательно, $\chi(1)$ делится на $q - 1/2 = 2^{k-1}$.

$$\sum_{x \in A_2} \psi(x)\overline{\psi(x)} = \left(\frac{df}{\varphi(q+1)}\right)^2 (q+1)\varphi(q+1),$$

$$\sum_{\substack{x \in A_2 \\ x^2 \neq 1}} \psi(x)\overline{\psi(x)} = \frac{(df)^2}{\varphi(q+1)}(q+1-2\varphi(q+1)),$$

$$\sum_{y} \sum_{\substack{x \in y^{-1}A_2 y \\ x^2 \neq 1}} \psi(x)\overline{\psi(x)} = \frac{g}{2(q+1)} \frac{(df)^2(q+1-2\varphi(q+1))}{\varphi(q+1)} <$$

$$< \sum_{x \in G} \psi(x)\overline{\psi(x)} = dg,$$

где $g = |G|$ и y — представители различных смежных классов группы G по нормализатору группы A_i. Теперь

$$\varphi(q+1) < \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)(q+1)$$

и

$$q + 1 - 2\varphi(q+1) \geqslant \frac{q+1}{6}.$$

Поэтому

$$\frac{df^2}{6\varphi(q+1)} < 1 \text{ или } \frac{af}{\varphi(q+1)} f < 6.$$

Если $q \neq 5$, то $q \geqslant 17$ и f делится на 8. Следовательно, $q = 5$.

§ 6. Группы, все подгруппы порядка pq которых циклические

Рассмотрим сперва разрешимые группы.

Лемма 1. Конечная (нециклическая) группа с циклическими силовскими p-подгруппами для всех простых делителей p порядка группы является двуциклической (расширением циклической группы при помощи циклической группы).

Доказательство. Утверждение докажем индукцией по числу простых делителей порядка группы G. Пусть P — силовская p-подгруппа, где p — наименьший простой делитель порядка группы G. Ясно, что $P \subseteq Z(N(P))$. По теореме Бернсайда (см., например, М. Холл [9, стр. 227]), в группе G существует такая подгруппа N, что $G = N \leftthreetimes P$. Отсюда вытекает справедливость доказываемого утверждения для случая, когда $|G|$ имеет лишь два различных простых делителя. Предположим, что число различных простых делителей $|G|$ больше двух, и считаем, что утверждение доказано для групп, порядок которых имеет меньше простых делителей, чем их в $|G|$. Тогда N — двуциклическая группа. Коммутант N' группы N — циклическая группа. Так как N' характеристичен в N, то N' инвариантен в G. Ввиду цикличности силовских подгрупп группы G фактор-группа N/N' циклическая. Это означает, что группа G сверхразрешима. По теореме Вендта (см. М. Холл, теорема 10.5.4), коммутант G' группы G нильпотентен. Так как силовские подгруппы группы G циклические, то G/G' и G' — циклические группы.

Уточним строение группы с циклическими силовскими подгруппами.

Теорема 2. *Для того чтобы конечная (нециклическая) группа имела циклические силовские подгруппы, необходимо и достаточно, чтобы она порождалась двумя элементами a и b, удовлетворяющими следующим соотношениям: $a^n = b^m = 1$, где n и m — взаимно простые натуральные числа; $b^{-1}ab = a^s$, где $(n, s) = (n, s-1) = 1$.*

Доказательство. Очевидно, группа G, порожденная элементами a и b с указанными соотношениями, не является циклической и имеет циклические силовские подгруппы.

Докажем необходимость условия теоремы. В силу леммы 1, коммутант G' группы G циклический, скажем $G' = \{a\}$, $n^n = 1$. Так как силовские подгруппы группы G циклические, то G / G' — циклическая группа, $G / G' = \{bG'\}$. Покажем, что $G = \{a\} \leftthreetimes \{b\}$. Ясно, что $a^{-1}b^{-1}ab = a^{s-1}$ для некоторого натурального числа $s - 1$. Так как $\{a^{s-k}\}$ инвариантна в G, то всякий коммутатор группы G лежит в $\{a^{s-1}\}$. Это означает, что $G' = \{a^{s-1}\}$ и $(n, s - 1) = 1$. Так как $\{a\} \cap \{b\} \subseteq Z(G)$, то из цикличности силовских подгрупп следует, что $\{a\} \cap \{b\} = \{1\}$. Отсюда получаем, что $(n, m) = 1$, где $m = |b|$. Так как отображение $a \to a^s$ есть изоморфизм группы $\{a\}$, то $(n, s) = 1$. Теорема доказана.

Следствие 3. *Если всякая подгруппа порядка pq группы с циклическими силовскими подгруппами является циклической, то к соотношениям теоремы 2 необходимо добавить следующее условие: существует такой делитель m_0 числа m, что*

$$s^m/m_0 \equiv 1 \pmod{n},\ s^t \not\equiv 1 \pmod{n}$$

для любого t, где $1 \leqslant t < m \mid m_0$, и каждый простой делитель числа m делит m_0.

Действительно, из соотношения $b^{-x}ab^x = a^{s^x}$ вытекает, что $s^m \equiv 1 \pmod{n}$. Пусть m_0 — такой наибольший делитель m, что $s^{m/m_0} \equiv 1 \pmod{n}$. Тогда $m_0 = |C_{\{b\}}(a)|$. Если p делит m, но не делит m_0, то в группе $\{a\} \leftthreetimes \{c\}$, где c — элемент порядка p из $\{b\}$, существует неабелева подгруппа порядка pq, что противоречит условию.

Далее будем рассматривать разрешимые группы, у которых любая подгруппа порядка pq циклическая и силовская 2-подгруппа — либо группа кватернионов, либо обобщенная группа кватернионов. Коротко такие группы обозначим HZ-группами.

Рассмотрим сперва двуступенно разрешимые HZ-группы. Коммутант G' группы G разлагается в прямое произведение

$$G' = S \times T$$

2-подгруппы S и подгруппы нечетного порядка T. Рассмотрим G / T. Ее коммутант — 2-группа. Потому силовская 2-подгруппа R группы G / T инвариантна в G / T. Так как G двуступенно разрешима, то $|G / T : C_{G/T}(R)|$ — степень 2. Это означает, что G / T

разлагается в прямое произведение своих силовских подгрупп. Но тогда в группе G силовская 2-подгруппа P дополняема нормальным делителем нечетного порядка, скажем $G = N \leftthreetimes P$. Возможны следующие три случая:

1) $|P : C_P(T)| = 1$,

2) $|P : C_P(T)| = 2$,

3) $|P : C_P(T)| = 4$.

В первом случае строение группы определяется сразу;

а) $G = N \times P$, *где* P — *группа кватернионов или обобщенная группа кватернионов, а* N — *группа нечетного порядка.*

Рассмотрим вторую возможность. Если P — обобщенная группа кватернионов, то $C_P(T)$ — либо циклическая группа, либо неабелева группа. Предположим, что $C_P(T)$ — циклическая группа. Известно, что группу P можно задать элементами c и d, удовлетворяющими соотношениям:

$$c^{2^k} = d^4 = cd^{-1}\ cd = 1,\ d^2 = c^{2^{k-1}},\ k > 2.$$

Ясно, что $\{c\} = C_P(T)$. Рассмотрим группу $N \leftthreetimes \{d\}$. Ее силовские подгруппы циклические. Согласно следствию 3 она порождается элементами a и b с соотношениями теоремы 2 и дополнительными условиями следствия 3, причем $m = 4m'$, $(m', 2) = 1$, $(m_0, 4) = 2$. Так как $\{c\}$ инвариантна в G, то $b^{-1}cb = c^{-1}$, $a^{-1}ca = c$.

Если P — просто группа кватернионов, то $C_P(T)$ — циклическая группа и $G = \{a, b, c\}$ с $k = 2$.

б) Итак, если $C_P(T)$ — циклическая группа, то *группа* G *порождается элементами* a, b, c. *Элементы* a *и* b *связаны соотношениями теоремы* 2 *и дополнительными условиями следствия* 3, *причем* $m = 4m'$, $(m', 2) = 1$, $(m_0, 4) = 2$,

$$b^{-1}cb = c^{-1},\quad a^{-1}ca = c,\ c^{2^{k-1}} = b^{2m'},\quad \text{где } k \geqslant 2.$$

Пусть $C_P(T)$ — неабелева группа. $C_P(T)$ порождается двумя элементами c и d, $c^{2^{k-1}} = d^4 = cd^{-1}cd = 1$, $d^2 = c^{2^{k-2}}$, $k > 2$. Пусть r — какой-либо элемент порядка 4 из $P \setminus C_P(T)$. Тогда $P = \{d, r\}$. Рассмотрим группу $N \leftthreetimes \{r\}$. Силовские подгруппы ее циклические. Пусть a и b — порождающие элементы группы $N \leftthreetimes \{r\}$ с соотношениями теоремы 2 и дополнительными условиями следствия 3. Нетрудно убедиться, что

в) *Группа* G *порождается элементами* a, b, d. *Элементы* a *и* b *связаны соотношениями теоремы* 2 *и дополнительными условиями*

следствия 3, *причем* $m = 4m'$, $(m', 2) = 1$, $(m_0, 4) = 2$,

$$(b^{m'}d)^{2^k} = a^{-1}d^{-1}ad = 1, \quad b^{2m'} = d^2, \quad k > 2.$$

Наконец, рассмотрим случай $|P : C_P(T)| = 4$.

Группа P порождается двумя элементами d_1 и d_2, удовлетворяющими соотношениям:

$$d_1^2 = d_2^2 = (d_1d_2)^{2^{k-1}}, \quad d_1^4 = 1, \quad k \geqslant 2.$$

Рассмотрим группы $G_1 = N \leftthreetimes \{d_1\}$ и $G_2 = N \rtimes \{d_2\}$. Их силовские подгруппы циклические. Группы G_i $(i = 1,2)$ порождаются элементами a_i, b_i с соотношениями теоремы 2 и дополнительными условиями следствия 3. Пересечения $\{b_1\} \cap T$, $\{b_2\} \cap T$ дополняемы в $\{b_1\}$ и $\{b_2\}$ соответственно. Пусть $\{b_1\}$ и $\{b_2\}$ — эти дополнения. Можно выбрать b_1 и b_2 так, что коммутант группы $\{b_1, b_2\}$ будет 2-группой. Поэтому справедливо следующее утверждение:

г) *Группа* G *порождается элементами* a_1, a_2, b_1, b_2, *удовлетворяющими соотношениям*:

$$a_i^{n_i} = b_i^{m_i} = 1,$$

где n_i *и* m_i — *взаимно простые натуральные числа, причем*

$m_i = 4\ m_i'$, $(m_i', 2) = 1$, $d = (n_1, n_2) \neq n_1$ *и* n_2, $i = 1, 2$, $b_i^{-1}a_ib_i = a_i^{s_i}$, *где* $(n_i, s_i) = (n_i, s_i - 1) = 1$, *и существует такой делитель* m_{0i} *числа* m_i, *что*

$$s_i^{m_i/m_{0i}} \equiv 1 \pmod{n_i}, \quad s_i^t \not\equiv 1 \pmod{n_i}$$

для любого t, *где* $1 \leqslant t < m_i \mid m_{0i}$, *и каждый простой делитель числа* m_i *делит* m_{0i}, $(m_{0i}, 4) = 2$

$$a_1a_2 = a_2a_1, \quad b_1^{2m_1'} = b_2^{2m_2'}, \quad b_1^4 = b_2^4, \quad a_1^db_2 = b_2a_1^d, \quad a_2^db_1 = b_1a_2^d,$$

$$(b_1^{m_1'}b_2^{m_2'})^{2^k} = 1, \quad (d, n_1/d) = (d, n_2/d) = 1, \quad k \geqslant 2.$$

Предположим, что HZ-группа G трехступенно разрешима;

$$G \supset H \supset Q \supset \{1\} -$$

ряд ее коммутантов. Так как Q — циклическая группа, то $G \mid C(Q)$ — абелева группа. Поэтому $Q \subseteq Z(H)$. Из описания двуступенно разрешимых групп видно, что H — группа типа а). Пусть P — силовская 2-подгруппа H. Силовские подгруппы груп-

ны $C(P)$ — циклические. Поэтому $C(P)P = R \times P$, где R — группа нечетного порядка. $G/R \times P$ изоморфна некоторой подгруппе группы подстановок трех символов. Ясно, что $G|R \times P| \neq 1$. Если $|G/R \times P| = 2$, то $G \subset G/R \times G/P$ — двуступенно разрешимая группа, что невозможно. Если $|G/R \times P| = 6$, то $G/R \cong GL(2,3)$ и, следовательно, четырехступенно разрешима, что также невозможно. Итак, $|G/R \times P| = 3$, $G/R \cong SL(2,3)$, G/P — HZ-группа нечетного порядка. Теперь легко задать G — порождающими элементами и соотношениями.

д) *G порождается элементами a, b, c, d. Элементы a и b удовлетворяют соотношениям теоремы 2 и дополнительным условиям следствия 3, m и n — нечетные числа.*

$$c^4 = 1, \quad c^2 = d^2, \quad c^{-1}dc = d^{-1}, \quad b^{-1}cb = d,$$

$$b^{-1}db = cd, \quad ac = ca, \quad ad = da.$$

е) *G порождается элементами b, c, d с соотношениями предыдущего типа.*

Пусть G — четырехступенно разрешимая HZ-группа. Коммутант G' группы G имеет либо вид д), либо вид е). Так как силовская 2-подгруппа группы G' — группа кватернионов, инвариантная в G', то порядок силовской 2-подгруппы P группы G равен 16. Фактор-группа $G/C(Q)Q$, где Q — группа кватернионов, изоморфна симметрической группе трех символов. Пусть H — подгруппа индекса 2 в группе G. $H = Q \leftthreetimes S$, где S — группа нечетного порядка. Так как обобщенная группа кватернионов порождается двумя элементами порядка 4, то вне H лежит элемент e порядка 4, перестановочный с S. Положим $R = \{S, e\}$. Силовские подгруппы группы R циклические, она неабелева, и потому к ней применимы теорема 2 и следствие 3. Таким образом, получаем следующий тип HZ-групп.

ж) *G порождается элементами a, b, c, d. Элементы a и b удовлетворяют соотношениям теоремы 2 и дополнительным условиям следствиям 3, $m = 4m'$, $(m', 2) = 1$, $(m_0, 4) = 2$, $n = 3^k n'$, $k \geqslant 1$.*

$$b^{m'}a^{n'}b^{m'} = a^{-n'}, \quad c^2 = d^2 = b^{2m'} = (cb^{m'})^2,$$

$$c^4 = 1, \quad c^{-1}dc = d^{-1}, \quad a^{-1}ca = d, \quad a^{-1}da = cd,$$

$$b^{-2}cb^2 = c, \quad b^{-2}db^2 = d.$$

Т е о р е м а 4. *Конечная разрешимая группа, у которой силовская 2-подгруппа неабелева и любая подгруппа порядка pq циклическая, есть группа одного из типов а) — ж).*

Доказательство. Если существует HZ-группа ступени разрешимости $\geqslant 5$, то существует HZ-группа G ступени 5. Так как коммутант G' группы G — группа типа ж), то G имеет инвариантную подгруппу Q кватернионов. $G/C(Q)Q$ изоморфна некоторой подгруппе группы подстановок трех символов. Следовательно, фактор-группа $G/C(Q)Q$ не более чем двуступенно разрешима. Силовские подгруппы группы $C(Q)$ циклические. Поэтому группа $C(Q)Q$ двуступенно разрешима. Итак, группа G не более чем четырехступенно разрешима. Теорема доказана.

Рассмотрим теперь случай неразрешимых групп.

Теорема 5. *Конечная неразрешимая группа, всякая подгруппа порядка pq которой циклическая, содержит подгруппу $H = M \times S$ индекса 1 или 2, где $M \cong SL(2, q)$, $q = 2^k + 1 \geqslant 5$ — простое число, и S—группа нечетного порядка.*

Доказательство. Докажем теорему индукцией по порядку группы. Если группа отлична от своего коммутанта, то простые рассуждения показывают справедливость теоремы. Поэтому считаем, что G совпадает со своим коммутантом.

Пусть τ и σ — две различные инволюции в G. Группа $\{\tau, \sigma\}$ — группа диэдра. Она содержит нециклическую подгруппу порядка $2p$. Это невозможно. Следовательно, G содержит единственную инволюцию τ.

Рассмотрим максимальную подгруппу R группы G. Если $Z(R)$ содержит элемент z нечетного простого порядка p, то $R = C(z) = N(\{z\})$. Поэтому нормализатор силовской p-подгруппы G содержится в R. Группа R имеет фактор-группу, которая является p-группой. Согласно теореме Грюна [30], группа G не совпадает со своим коммутантом. Полученное противоречие показывает, что $Z(R)$ не имеет элементов нечетного порядка. В силу теоремы 4 все подгруппы нечетного порядка группы G циклические. Докажем, что в группе $G/\{\tau\}$ максимальные циклические подгруппы четного порядка либо совпадают, либо пересекаются по единице. Если это утверждение неверно, то оно неверно в некоторой максимальной подгруппе R, которая должна быть группой типов в), г). Предположим, что R имеет тип г). $R = N \leftthreetimes P$, где N—циклическая группа нечетного порядка, а P—силовская 2-подгруппа R. Так как $R/\{\tau\}$ имеет две различные максимальные подгруппы четного порядка, которые имеют неединичное пересечение, то $|P| \geqslant 16$. В противном случае группа R имела бы центральный элемент нечетного порядка, что, как

уже показано, невозможно. Следовательно, в группе R существует характеристическая подгруппа $\{a\}$ порядка 4. $R = N(\{a\})$. Пусть $R \cap x^{-1}Rx = D \neq \{1\}$. Так как $R = N(L)$ для любой подгруппы L из N, то $|R \cap x^{-1}Rx|$ — четное число. Так как $R = N(\{a\})$ и $\{a\}$ содержится в единственной циклической подгруппе, которая имеет индекс 2,— в силовской 2-подгруппе группы R, то $|R \cap x^{-1}Rx| \leqslant 4$. С другой стороны, если Q-подгруппа группы P изоморфна группе кватернионов, то существует элемент x группы G, который индуцирует в Q автоморфизм порядка 3. Поэтому $|R \cap x^{-1}Rx| \geqslant 8$. Полученное противоречие показывает, что если R имеет тип г), то в $R/\{\tau\}$ максимальные циклические подгруппы либо совпадают, либо имеют единичное пересечение. Аналогично рассматривается случай, когда R имеет тип в).

Таким образом, доказано, что в фактор-группе $G/\{\tau\}$ максимальные циклические подгруппы четного порядка либо совпадают, либо пересекаются по единичной подгруппе. Группы с этим условием рассмотрены Брауэром, Сузуки и Воллом [15]. Если централизатор инволюции из $G/\{\tau\}$ имеет порядок более 4, то применимо доказательство теоремы 1 из § 10. В этом случае $G/\{\tau\} \cong PSL(2, q)$. Как известно, тогда $G \cong SL(2, q)$. Осталось рассмотреть случай, когда централизатор любой инволюции σ группы $T = G/\{\tau\}$ имеет порядок 4. Порядок группы $G/\{\tau\}$ равен $4n_1n_2\ldots n_k$, где n_i $(i = 1,2,\ldots, k)$ — порядки максимальных циклических подгрупп нечетного порядка. С другой стороны, порядок группы T равен

$$1 + n_1n_2\ldots n_k + 2n_1n_2\ldots n_k\left\{\sum_{i=1}^{k}\left(1 - \frac{1}{n_i}\right)\right\}.$$

Обозначив $x = n_1n_2\ldots n_k$, получаем

$$4x = x + 2xk - 2x\sum_{i=1}^{k}\frac{1}{n_i},$$

или

$$x = \left(3 - 2k + 2\sum_{i=1}^{k}\frac{1}{n_i}\right)^{-1}.$$

Из неразрешимости G следует, что $k \geqslant 2$. Так как $x > 0$, то

$$3 - 2k + 2\sum_{i=1}^{k}\frac{1}{n_i} > 0.$$

Положив $1/n = \max 1/n_i$, получаем неравенство

$$2k/n > 2k - 3.$$

Так как $n \geqslant 3$, то $k \leqslant 2$. Следовательно, $k = 2$. Теперь верно равенство

$$4n_1n_2 = 1 + n_1n_2 + 2n_1n_2\left(2 - \frac{1}{n_1} - \frac{1}{n_2}\right).$$

Отсюда получаем

$$n_1n_2 - 2(n_1 + n_2) + 1 = 0.$$

Это уравнение имеет единственное решение $n_1 = 3$ и $n_2 = 5$. Итак,

$$|G/\{\tau\}| = 60 \quad \text{и} \quad G \cong SL(2,5).$$

Теорема доказана.

§ 7. Группы, допускающие регулярные автоморфизмы

В этом параграфе будет доказана нильпотентность конечной группы, допускающей регулярный автоморфизм простого порядка. Первоначальное доказательство Томпсона очень сложно (см. [64]). В дальнейшем Томпсон [65] его упростил.

Наименьшее число порождающих элементов группы G обозначим через $m(G)$. Определим $d(G) = \max m(A)$, где A пробегает все абелевы подгруппы G, и пусть $J(G)$ — подгруппа, порожденная всеми абелевыми подгруппами A, которые удовлетворяют равенству $d(G) = m(A)$. Ясно, что $J(G)$ — характеристическая подгруппа любой ее содержащей подгруппы.

Теорема 1 (Томпсон). *Пусть p — нечетное простое число и G_p — силовская p-подгруппа G. Если $C(Z(G_p))$ и $N(J(G_p))$ имеют нормальное p-дополнение, то его имеет группа G.*

Доказательство. Предположим, что G — наименьшая группа, которая удовлетворяет условиям теоремы и не имеет нормального p-дополнения.

Фробениус доказал (см., например, М. Холл [9, стр. 241]), что если в некоторой конечной группе фактор-группа $N(H)/C(H)$ есть p-группа для любой p-подгруппы H, то группа имеет нормальное p-дополнение. Из этой теоремы вытекает, что множество X неединичных p-подгрупп H группы G, нормализатор которых $N(H)$ не имеет нормального p-дополнения, не пусто. В

множестве X введем порядок, считая, что $H \leqslant K$ для H и $K \in X$ тогда и только тогда, когда верно одно из следующих условий:

1) $|N(H)|_p < |N(K)|_p$;

2) $|N(H)|_p = |N(K)|_p$ и $|H| < |K|$;

3) $H = K$;

здесь $|L|_p$ — порядок силовской p-подгруппы группы L. В дальнейших рассуждениях принимаем, что H — максимальный элемент множества X и $N = N(H)$.

Если H — силовская p-подгруппа G, то $N \subseteq N(J(H))$. Но тогда N имеет нормальное p-дополнение, что противоречит выбору H. Пусть P — силовская p-подгруппа N. Считаем, что $P \subseteq G_p$. Из максимальности H вытекает, что в N/H выполняются условия доказываемой теоремы. Так как $|N/H| < |G|$, то N/H имеет нормальное p-дополнение K/H.

Так как P — силовская p-подгруппа N, то $Z(G_p) \subseteq Z(P)$ и $C_N(Z(P))$ имеет нормальное p-дополнение. Если $N_N(J(P))$ не имеет нормального p-дополнения, то из $|N_N(J(P))|_p > |N(H)|_p$ и максимальности H следует, что $P = G_p$. По предположению $N_G(J(G_p))$ имеет нормальное p-дополнение. Итак, $N_N(J(P))$ имеет нормальное p-дополнение.

Если N — собственная подгруппа группы G, то N имеет нормальное p-дополнение. Так как по выбору H группа N нормального p-дополнения не имеет, то $N = G$. Ясно также, что G не имеет инвариантных p'-подгрупп (p'-подгруппа — это подгруппа, порядок которой взаимно прост с p). Так как H максимальна в множестве X, то H есть наибольшая инвариантная p-подгруппа G.

Докажем, что K/H — главный фактор G. Предположим, что $L \subset K$ и L/H — главный фактор G. Тогда LG_p имеет нормальное p-дополнение D. Так как D — характеристическая подгруппа в LG_p, то D инвариантна в G. Поэтому G имеет инвариантную p'-подгруппу D. Как уже отмечалось, это невозможно.

Положим $H_0 = C_{G_p}(K/H)$. Так как G_p и K нормализуют H_0, то H_0 — инвариантная p-подгруппа G. Но тогда $H_0 = H$.

Положим $C = C_K(H)$. Ясно, что C инвариантна в G. Если $C \notin H$, то $K = HC$, так как K/H — главный фактор. Но $C \cap H = Z(H)$ — силовская p-подгруппа C, и по упоминавшейся выше теореме Фробениуса C имеет нормальное p-дополнение, которое инвариантно в G. Так как это невозможно, то $C(H)$ есть p-группа и $C(H) = Z(H)$. В частности, $Z(H)$ содержит центр группы G_p.

Пусть q — простой делитель $|K:H|$ и пусть Q/H — силовская q-подгруппа K/H. Можно считать, что G_p/H нормализует Q/H. Ясно, что QG_p не имеет нормального p-дополнения, так как $C(H) = Z(H)$. Следовательно, $Q = K$ и K/H — элементарная абелева q-группа, а G_p — максимальная подгруппа G.

Так как $N(J(G_p))$ имеет нормальное p-дополнение, то отсюда следует, что $J(G_p) \not\subseteq H$. Пусть $d = d(G_p)$, и возьмем абелеву подгруппу A из G_p, которая удовлетворяет условию $m(A) = d$ и $A \not\subseteq H$. Положим $A_0 = A \cap H$.

Пусть $P_0 = HA$. Воспользуемся теперь следующим очевидным предложением (Фиттинг).

Если G имеет порядок g и A — правый G-модуль, такой, что отображение $a \to ag$ $(a \in E)$ есть автоморфизм A, то $A = A_0 \oplus \oplus A_1$, где $A_0 = A\sigma$, $A_1 = A(1-\sigma)$, $\sigma = \sigma(G) = g^{-1}\sum_{x\in G} x$.

Применив это предложение к A-модулю K/H, получаем

$$K_1/H = (K/H)(1-\sigma),\ \sigma = \sigma(A).$$

Так как $C_{Gp}(K/H) = H$, то H — собственная подгруппа K_1. Поэтому K_1 не имеет нормального p-дополнения. Положим $G_0 = K_1P_0$. Ясно, что $A \subseteq J(P_0)$ и что $N_{G_0}(J(P_0)) = P_0$ имеет нормальное p-дополнение. Так как $Z(G_p) \subseteq Z(P_0)$, то $C_{G_0}(Z(P_0)$ имеет нормальное p-дополнение. Следовательно, $G_0 = G$.

Так как $G_p = HA$ — максимальная подгруппа G, то из $C_{G_p}(K/H) = Z(H)$ получаем, что A/A_0 — циклическая группа. В частности, $m(A_0) \geqslant d - 1$. Так как G_p — максимальная подгруппа G, то $C(Z(G_p)) = G_p$. Пусть W — наименьший нормальный делитель, содержащий $Z(G_p)$. Тогда $W \subseteq Z(H)$. Рассмотрим W как K/H-модуль. Применив теорему Фиттинга, получаем $W_1 = W(1-\sigma)$, $\sigma = \sigma(K/H)$. Так как K не содержит в своем центре $Z(G_p)$, то $W_1 \neq \{1\}$. Пусть

$$V = \{w \mid w \in W_1,\ w^p = 1\},$$

так что $V = V(1-\sigma)$.

Пусть $V_0 = V \cap A_0 = V \cap A$ и пусть $m(V/V_0) = r$. Так как $\{A_0, V\}$ — абелева группа и V элементарна, то $m(\{A_0, V\}) = m(A_0) + r$. Следовательно, $r \leqslant 1$ по определению $d(G_p)$.

Выберем a в A так, что aA_0 — порождающий элемент A/A_0, и выберем g в $K - H$. Если $m(V) \geqslant 3$, то a и $g^{-1}ag$ перестановочны с одним и тем же элементом v из $V - \{1\}$. Но так как K/H не

содержится в центре G/H, то

$$\{H, a, g^{-1}ag\} = G.$$

Это противоречит тому, что $V = V(1 - \sigma)$. Следовательно, $m(V) \leqslant 2$ и потому $m(V) = 2$. G/H порождается p-элементами. Это означает, что G/H — подгруппа группы $SL(2, p)$. В $SL(2, p)$ нет p'-подгрупп нечетного порядка, которые бы были инвариантны относительно элементов порядка p. Полученное противоречие доказывает теорему.

Замечание 2. Как видно из доказательства теоремы, для $p = 2$ получается следующее утверждение.

Если G_2 — силовская 2-подгруппа G и $C(Z(G_2))$ и $N(J(G_2))$ имеют нормальное 2-дополнение, то при условии, что группа G не имеет подгруппы, некоторый гомоморфный образ которой изоморфен S_4, группа G имеет нормальное 2-дополнение.

Следствие 3. *Конечная группа G, допускающая регулярный автоморфизм φ простого порядка p, нильпотентна.*

Следствие вытекает из теоремы 1 и замечания 2.

Не всякая нильпотентная группа допускает регулярный автоморфизм. В § 1 сформулирована теорема Хигмена о 2-группах, допускающих транзитивную на инволюциях циклическую группу автоморфизмов. Если $q - 1$ — число инволюций 2-группы P, то $|P|$ равен либо q^2, либо q^3 (если P — неабелева). В случае, когда $|P| = q^2$, строение группы P полностью определено, $P \cong S(q; x)$ (см. § 1). Изучим некоторые свойства группы $S(q, x)$. Свойства групп $S(q; x)$ необходимо знать хотя бы потому, что $S(q; x)$ с $x^2 = 2$ содержится в качестве силовской 2-подгруппы в простой группе Сузуки (см. § 1). Если (α, β) и (γ, δ) принадлежат $S(q; x)$, то

$$(\alpha, \beta)(\gamma, \delta) = (\alpha + \gamma, \alpha\gamma^x + \beta + \delta).$$

Если есть необходимость отметить автоморфизм x, то вместо (α, β) будем писать $(\alpha, \beta; x)$. Простые вычисления показывают справедливость следующих предложений.

Лемма 3. $|S(q; x)| = q^2$. Центр $S(q; x)$ состоит из матриц вида $(0, \beta)$ и имеет порядок q. Порядки элементов в $S(q; x)$ не превышают 4. Элемент из $S(q; x)$ является инволюцией тогда и только тогда, когда он имеет вид $(0, \beta)$.

Лемма 4. Централизатор элемента $(1, 0)$ в $S(q; x)$ состоит из элементов вида (α, β) с $\alpha^x = \alpha$.

Л е м м а 5. Группа $S(q; x)$ не содержит группы кватернионов.

Л е м м а 6. Если $x^{-1} = y$, то $S(q; x) \cong S(q; y)$.

Автоморфизм можно задать так: $(\alpha, \beta; x) \to (\alpha^x, \beta + \alpha^{1+x}; y)$.

Л е м м а 7. Для любого $\zeta \in GF(q)$ отображение $\varphi(\zeta)$: $:(\alpha, \beta) \to (\zeta\alpha, \zeta^{1+x}\beta)$ есть автоморфизм $S(q; x)$. Элемент (α, β) остается неподвижным при $\varphi(\zeta)$ тогда и только тогда, когда $\alpha = \beta = 0$ или совокупность автоморфизмов $\varphi(\zeta)$ образует циклическую группу Z, изоморфную с мультипликативной группой поля $GF[q]$.

Л е м м а 8. Пусть Z' — циклическая группа регулярных автоморфизмов группы $S(q; x)$. И пусть $|Z'| = q - 1$. Тогда существует такой автоморфизм θ группы $S(q; x)$, что $Z' = \theta^{-1} Z \theta$.

Д о к а з а т е л ь с т в о. Пусть C — центр группы $S(q; x)$. Каждый элемент из Z' можно записать в виде $\psi(\zeta)$ с $\zeta \in GF[q]$, $\zeta \neq 0$, так что $\psi(\zeta)$ совпадает на C с $\varphi(\zeta)$. Тогда $\psi(\zeta)$ отображает $(1,0)$ на $(\zeta, f(\zeta))$, где $f(\zeta) \in GF[q]$. Пусть ξ — порождающий элемент мультипликативной группы поля $GF[q]$. Элементы $(1, 0)$, $(\xi, 0)$,..., $(\xi^{n-1}, 0)$ порождают группу $S(q; x)$ и независимы в фактор-группе $S(q; x)/C$. Элемент $(\xi^n, 0)$ можно записать так:

$$\Pi'(\xi^i, 0)(0, \alpha),$$

где произведение рассматривается лишь для тех $i < n$, для которых коэффициент a_i минимального полинома $p(t) = \Sigma a_i t^i$ для ξ не равен нулю. Возьмем $(1, \gamma)$ с подходящим γ и применим $\psi(\xi)$ последовательно несколько раз:

$$\psi(\xi)^k (1, \gamma) = \psi(\xi^k)(1, \gamma) = (\xi^k, f(\xi^k) + \eta^k\gamma), \quad (k \leqslant n),$$

где $\eta = \xi^{1+x}$. Для $k = n$ получаем

$$(\xi^n, f(\xi^n) + \eta^n\gamma) = \Pi'(\xi^i, f(\xi^i) + \eta^i\gamma)(0, \alpha'),$$

где

$$\alpha' = \alpha + \Sigma' f(\xi^i) + f(\xi^n) + \gamma(\Sigma'\eta^i + \eta^n),$$

умножение и суммирование производится по тем же i, что и прежде. В частности, коэффициент при γ есть $p(\eta)$. Так как $p(t)$ — минимальный полином для ξ и $\eta = \xi^{1+x}$, то $p(\eta)$ — не нуль. Следовательно, для подходящего выбора γ $\alpha = \alpha'$.

Отображение

$$(\xi^i, 0) \to (\xi^i, f(\xi^i) + \eta^i\gamma) \qquad (0 \leqslant i < n)$$

можно распространить до автоморфизма θ^{-1} группы $S(q; x)$

$$(\xi^n, 0) = \theta(\xi^n, f(\xi^n) + \eta^n\gamma).$$

Теперь легко доказать, что $\theta^{-1}\varphi(\xi)\theta = \psi(\xi)$.

Пусть $M = M(q; x)$ — голоморф $S(q; x)$ посредством группы автоморфизмов Z. Группа M есть группа Фробениуса с неабелевым ядром.

Лемма 9. Пусть $H = Q \leftthreetimes K$, где $Q \cong S(q; x)$ и K — циклическая группа порядка $q - 1$, индуцирующая в Q группу регулярных автоморфизмов. Тогда $H \cong M$.

Доказательство. Рассмотрим M и H как подгруппы голоморфа $S(q; x)$ посредством полной группы автоморфизмов. Согласно лемме 8 M и H сопряжены в голоморфе.

Лемма 10. Группа внешних автоморфизмов группы M изоморфна с группой автоморфизмов поля $GF[q] = F$.

Доказательство. Пусть A — группа автоморфизмов M, и пусть A_0 — группа внутренних автоморфизмов. Пусть C — центр $S(q; x)$. Возьмем инволюцию $\sigma \in C$ и рассмотрим совокупность B автоморфизмов M, оставляющих K и σ на месте. Для каждого автоморфизма θ существует такой элемент $\rho \in M$, что $\theta(K) = \rho^{-1}K\rho$ и $\theta(\sigma) = \rho^{-1}\sigma\rho$. Следовательно, $A = BA_0$. Каждый элемент из B индуцирует автоморфизм поля F. Если $\pi \in B$ индуцирует тривиальный автоморфизм F, то π оставляет каждый элемент из CK на месте. Предположим, что π отображает $(1, 0)$ на $(1, \gamma)$. Это определяет действие π однозначно:

$$\pi(\alpha, \beta) = (\alpha, \beta + \alpha^{1+x}\gamma).$$

Так как π — автоморфизм M, то

$$(\alpha + \beta)^{1+x}\gamma = \alpha^{1+x}\gamma + \beta^{1+x}\gamma$$

для каждой пары элементов α и β. Так как $x \neq 1$, то существует такая пара элементов α и β, что $\alpha^x\beta \neq \alpha\beta^x$. Следовательно, $\gamma = 0$ и $\pi = 1$. Следовательно, B — группа автоморфизмов F. С другой стороны, группа A/A_0 — не более чем группа автоморфизмов F. Так как A/A_0 гомоморфна B, то утверждение доказано.

Лемма 11. $M(q; x) \cong M(q, y)$, если $y = x^{-1}$.

Действительно, отображение

$$(\alpha, \beta; x) \to (\alpha^x, \beta + \alpha^{1+x}; y), \varphi_x(\zeta) \to \varphi_y(\zeta^x)$$

дает нужный изоморфизм.

Л е м м а 12. Пусть $x:\alpha \to \alpha^r$ — автоморфизм $GF[q]$. $S(q; x)$ распределяется в $M(q; x)$ точно по четырем классам сопряженных элементов тогда и только тогда, когда $(r-1, q-1) = 1$.

Д о к а з а т е л ь с т в о. Пусть $s = (\alpha, \beta) \in S(q; x)$, $\alpha \neq 0$. Найдем $C(s)$. Так как $(\alpha\beta)(\gamma\delta) = (\gamma\delta)(\alpha\beta)$, то для $\gamma \neq 0$

$$(\gamma/\alpha)^{r-1} = 1. \tag{1}$$

Если γ удовлетворяет этому уравнению, то $(\gamma, \delta) \in C(s)$. Так же $C(s) \ni (0, \delta)$ для любого δ. Так как в $M(q; x)$ s и s^{-1} не сопряжены, то $|C(s)| \leqslant 2q$. Поэтому $|C(s)| = 2q$ тогда и только тогда, когда уравнение (1) имеет единственное решение, т. е. когда $(r-1, q-1) = 1$.

Для удобства отождествим Z с мультипликативной группой поля $GF[q]$ следующим образом:

$$\varphi(\zeta)(\alpha, \beta) = (\zeta^{-1}(\alpha, \beta)\zeta$$

для любого $\zeta \in F$, $\zeta \neq 0$.

Будем писать, что $M(q; x) = S(q; x) \diagup Z$, и вместо $\varphi(\zeta) \in Z$ будем писать $\zeta \in Z$.

Л е м м а 13. Любой неединичный элемент из $S(q; x)$ сопряжен с помощью элементов из Z к одному и только одному из следующих элементов:

$$\sigma = (0, 1), \quad \rho = (1, 0), \quad \rho^{-1} = (1, 1)$$

и

$$\pi(k) = \rho k^{-1}\rho^{-1}k \text{ для } k \in Z, \ k \neq 1.$$

Д о к а з а т е л ь с т в о. Пусть

$$\pi(k') = \zeta^{-1}\pi(k)\zeta, \ k, k', \zeta \in Z.$$

Тогда

$$(1 + k', (1 + k')k'^{x}) = (\zeta(1 + k), \zeta^{1+x}(1 + k)k^{x}).$$

Отсюда получаем

$$\zeta(1 + k) = 1 + k',$$

$$\zeta^{1+x}(1 + k)k^{x} = (1 + k')k'^{x}; \tag{2}$$

так как $k, k' \neq 1$, то из этих равенств вытекает

$$(\zeta k)^{x} = k'^{x}.$$

Из первого равенства (2) получаем теперь

$$k'^x = (1 + \zeta + k')^x.$$

Поэтому $\zeta = 1$.

Итак, ясно, что элементы, указанные в формулировке леммы, не сопряжены элементами из Z.

Так как каждый из перечисленных элементов сопряжен с помощью элементов из Z точно с $q - 1$ элементом, то все $q^2 - 1$ неединичных элемента группы $S(q; x)$ в этих классах уже содержатся.

Глава III

КЛАССИФИКАЦИЯ КОНЕЧНЫХ РАСЩЕПЛЯЕМЫХ ГРУПП

§ 8. Группы с допустимым нормальным делителем

Если расщепляемая группа является p-группой или группой Фробениуса, то она имеет расщепление, относительно которого допустим некоторый нормальный делитель.

Пусть P — p-группа. Если все неединичные элементы из P имеют равные порядки, то относительно (нормального) расщепления группы P, составленного из всех ее циклических подгрупп, допустим любой ее нормальный делитель. Если P имеет элементы составного порядка, то подгруппа P_0, ими порожденная, вместе с подгруппами простых порядков, не лежащими в P_0, дает нормальное расщепление, относительно которого P_0 допустима.

Предположим, что P — группа Фробениуса. Тогда инвариантный множитель группы P и совокупность дополнительных множителей образуют нормальное расщепление группы P, относительно которого допустим инвариантный множитель.

Расщепляемые группы с допустимыми нормальными делителями не исчерпываются p-группами и группами Фробениуса. К ним относятся также группы, рассмотренные Хьюгесом и Томпсоном [35]. Поэтому их и называют HT-группами.

Непримарная нильпотентная конечная группа G называется HT-группой, если существует такой простой делитель p числа $|G|$, что подгруппа H, порожденная элементами G, порядки которых не равны p, отлична от G и $|H|$ делится на p.

Как следует из доказанной ниже теоремы 6, такое число p существует только одно. В дальнейшем нам будут нужны следующие вспомогательные предложения.

Лемма 1. Пусть φ — автоморфизм группы G, действующий так:

$$g^{\varphi} = g^{-1}$$

для любого $g \in G$. Тогда G — абелева группа.

В самом деле, для любых g и h из G верны равенства:

$$gh = (h^{-1}g^{-1})^{\varphi} = (h^{-1})^{\varphi}(g^{-1})^{\varphi} = hg.$$

Лемма 2. При обозначениях определения HT-группы положим $p = 2$. Тогда H — абелева группа.

Доказательство. Вне H лежат лишь элементы второго порядка. Пусть $a \notin H$. Тогда для любого $h \in H$ имеем $(ha)^2 = 1$ или $a^{-1}ha = h^{-1}$. По предыдущей лемме, H — абелева группа.

Лемма 3. Пусть P — расщепляемая некоммутативная 2-группа. Тогда

$$P = P_0 \leftthreetimes \{a\},$$

где $a^2 = 1$, P_0 — абелева группа, содержащая элемент порядка 4, и для любого $b \in P_0$ $aba = b^{-1}$.

Доказательство. Пусть a и b не принадлежат подгруппе P_0, порожденной элементами составных порядков. Так как для любого $h \in P_0$ $aha = h^{-1}$ и $bhb = h^{-1}$, то $ahabh^{-1}b = 1$. Это означает, что ab перестановочен с любым элементом из P_0. Так как P_0 содержит все элементы составных порядков, то $ab \in P_0$. Поэтому $P = P_0 \leftthreetimes \{a\}$.

Лемма 4. Если конечная p-группа P расщепляема, имеет элемент порядка p^2 и инвариантную элементарную абелеву подгруппу N простого индекса, то она есть прямое произведение группы диэдра порядка 8 и элементарной 2-группы.

Доказательство. Предположим, что P — не 2-группа. Так как любая фактор-группа группы P имеет элементарную абелеву подгруппу индекса p и так как центр группы P находится целиком в компоненте расщепления, порожденной элементами составного порядка, то можно считать, что центр группы P циклический. В этом случае группа P совпадает со сплетением двух циклических групп простого порядка, которое нерасщепляемо при $p \neq 2$. Итак, P — 2-группа, и утверждение леммы вытекает из леммы 3.

Лемма 5. Пусть N — элементарный абелев нормальный делитель простого индекса конечной p-группы G ($p \neq 2$). Тогда

если N — компонента некоторого расщепления G, то наименьшая степень уравнения $(x-1)^k = 0$, которому удовлетворяет элемент $a \notin N$ (рассматриваемый как автоморфизм N) меньше p.

В самом деле, a приводится к нормальной форме

$$\begin{pmatrix} S_1 & 0 & \dots & 0 \\ 0 & S_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & S_\lambda \end{pmatrix}$$

где S_i — клетки вида

$$\begin{pmatrix} 1 & 1 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Так как N — компонента расщепления, то порядки элементов в G, согласно предыдущей лемме, простые числа. В этом случае степени клеток S_i меньше p.

Т е о р е м а 6. *Конечная HT-группа G имеет следующее строение*:

$$G = (S \times P) \leftthreetimes \{a\},$$

где $a^p = 1$, $S \leftthreetimes \{a\}$ — *группа Фробениуса*, $P \leftthreetimes \{a\}$ — *p-группа и* P — *компонента некоторого расщепления группы* $P \leftthreetimes \{a\}$.

Д о к а з а т е л ь с т в о. Обозначим через H подгруппу группы G, о которой идет речь в определении HT-группы. Группа G имеет расщепление, состоящее из H и подгрупп простого порядка, не лежащих в H.

В предположении нильпотентности H докажем, что $|G:H| = p$. Ясно, что G/H — p-группа. Пусть $H = N \times P$, где P — силовская p-подгруппа H. Каждый элемент, лежащей вне H, индуцирует в N регулярный автоморфизм. Поэтому G/H — циклическая группа (см. § 5). Так как вне H лежат элементы простого порядка p, то $|G:H| = p$.

Итак, если H — нильпотентная группа, то теорема доказана. Докажем теперь нильпотентность H. На основании леммы 2 считаем, что $p \neq 2$.

Предположим, что H не всегда нильпотентна. И пусть G — минимальная группа, у которой H не нильпотентна. Тогда $G = H \leftthreetimes \{a\}$, где $a^p = 1$.

Если K — нормальный делитель группы G, содержащийся в H, то K и H/K нильпотентны. Возможны два случая:

1) K — p-группа, H/K — p'-группа;

2) K — p'-группа, H/K — p-группа.

Рассмотрим первый случай. В силу теоремы 12.2.2 М. Холла [9] и минимальности G подгруппа Фраттини группы K равна $\{1\}$. Рассмотрим группу $K \leftthreetimes \{a\}$. Это расщепляемая p-группа. В силу леммы 5 наименьшая степень уравнения $(x - 1)^m = 0$, которому удовлетворяет a (если рассматривать a как автоморфизм K), меньше p. По теореме В Холла — Хигмена [31] силовская p-подгруппа группы G инвариантна. Но тогда $a \in H$ и $H = G$, что противоречит определению HT-группы. Следовательно, первый случай невозможен.

Рассмотрим второй случай. Ввиду минимальности G, в K содержится лишь один минимальный нормальный делитель группы G. Это означает, что K — q-группа для некоторого $q \neq p$. Как и в предыдущем случае, устанавливается, что K — элементарная абелева группа. $H = K \leftthreetimes P$, где P — силовская p-подгруппа H. Пусть $z \in Z(P \leftthreetimes \{a\}) \cap P$.

Ввиду минимальности G, H имеет единственный минимальный нормальный делитель группы G. Поэтому $C_K(z) \neq K$. Согласно § 5, $C = C_k(z) \neq \{1\}$. Итак, $G = (K \leftthreetimes \{z\}) \leftthreetimes \{a\}$. Покажем, что $a^{-1} Ca = C$. Так как $a^{-1}ca = a^{-1}z^{-1}cza = z^{-1}(a^{-1}ca)z$, то $a^{-1}ca \in C$, где $c \in C$. По теореме Машке (см., например, М. Холл [9, стр. 278]), $K = C \times T$, где T — инвариантная подгруппа группы G. Но это противоречит минимальности G. Таким образом, и второй случай невозможен.

Так как непростота H вытекает из теоремы Томпсона [65] (см. § 7), то теорема доказана.

Л е м м а 7. *Отличная от своего нормализатора компонента расщепления конечной группы нильпотентна.*

Действительно, если Σ — нормальное расщепление G, $U \in \Sigma$ и $N(U) \neq U$, то вне U в $N(U)$ содержится элемент a простого порядка p. Если $|U|$ не делится на p, то $U \leftthreetimes \{a\}$ — группа Фробениуса. Поэтому (см. § 7) U нильпотентна. Если $|U|$ делится на p, то либо U — p-группа, либо подгруппа из $U \leftthreetimes \{a\}$, порожденная элементами, порядки которых не равны p, отлична

от $U \leftthreetimes \{a\}$ (она не содержит a). В этом случае U также нильпотентна по теореме 6. Лемма доказана.

Т е о р е м а 8. *Если G — конечная расщепляемая группа с допустимым нормальным делителем, то она*

1) *либо p-группа,*

2) *либо группа Фробениуса,*

3) *либо HT-группа.*

Д о к а з а т е л ь с т в о. Предположим, что G не является группой типов 1) и 2). Покажем, что она HT-группа. Доказательство проведем индукцией по порядку группы G. Возьмем в G максимальный допустимый нормальный делитель G_1. Докажем, что G_1 имеет простой индекс в G. Сперва докажем, что в G/G_1 нет циклических подгрупп составного порядка. Допустим противное и рассмотрим подгруппу $G_1 \leftthreetimes \{a\}$, где $\{a\}$ — циклическая подгруппа составного порядка, не содержащаяся в G_1, $N_G(\{a\}) \cap \cap G_1$ есть компонента расщепления в группе $N_G(\{a\}) = \{a\} \times \times (N_G(\{a\}) \cap G_1)$, которая, очевидно, нерасщепляема. Следовательно, $G \neq G_1 \leftthreetimes \{a\}$ и, по индуктивному предположению, $G_1 \leftthreetimes \{a\}$ является группой типов 1) — 3). Из свойств последних и непростоты циклической подгруппы $\{a\}$ следует, что $G_1 \leftthreetimes \{a\}$ — группа Фробениуса. Пусть A — компонента расщепления группы G, содержащая $\{a\}$. По предположению, A отлична от своего нормализатора. Выберем в $N_G(A)$ собственную подгруппу $\{c\} \leftthreetimes \leftthreetimes \{b\}$, где $\{c\}$ — характеристическая подгруппа простого порядка из A, а $\{b\}$ — циклическая подгруппа простого порядка из $N_G(A)$, не лежащая в A. Ясно, что $\{c\} \leftthreetimes \{b\}$ — не циклическая группа. Рассмотрим подгруппу $H = G_1 \leftthreetimes (\{c\} \leftthreetimes \{b\})$. Это собственная подгруппа G. Очевидно, $G_1 \leftthreetimes \{c\}$, и все циклические подгруппы из H, не содержащиеся в $G_1 \leftthreetimes \{c\}$, составляют расщепление H. Значит, $G_1 \leftthreetimes \{c\}$ как отличная от своего нормализатора компонента расщепления нильпотентна. Это противоречит тому, что $G_1 \leftthreetimes \{c\}$ — группа Фробениуса. Следовательно, все циклические подгруппы из G/G_1 имеют простой порядок.

В фактор-группе G/G_1 возьмем циклическую подгруппу $\{d\}G_1/G_1$ порядка, взаимно простого хотя бы с одним из делителей $|G_1|$. Если $\{d\}G_1/G_1$ совпадает со своим нормализатором в G/G_1, то $G/G_1 = F/G_1 \leftthreetimes \{d\}G_1/G_1$ — группа Фробениуса и F — допустимый при некотором расщеплении нормальный делитель группы G, что противоречит максимальности G_1. Если $\{d\}G_1/G_1$ отлична от своего нормализатора, то $\{d\}G_1$ — допустимый нормальный

делитель в $N_G\{d\}\ G_1)$ и поэтому $\{d\}\ G_1$ является непримарной нильпотентной группой, что противоречит расщепляемости $\{d\}\ G_1$. Значит, $|\ G : G_1\ | = p$ — простое число. Так как G — не p-группа и не группа Фробениуса, то G_1 — непримарная подгруппа и p делит $|\ G_1\ |$. Очевидно, G_1 порождается всеми элементами группы G, порядки которых отличны от p. Поэтому G — HT-группа.

§ 9. Непростые группы без допустимого нормального делителя

Симметрическая группа четырех символов S_4 имеет расщепление, состоящее из циклических подгрупп. Это единственное расщепление S_4. S_4 не имеет допустимых нормальных делителей. Следующее предложение выделяет группу S_4 в классе конечных расщепляемых групп.

Теорема 1. *Пусть G — конечная расщепляемая группа без допустимых нормальных делителей. Тогда если G имеет коммутативный нормальный делитель, то G изоморфна S_4.*

Доказательство. Пусть N — максимальный абелевый нормальный делитель G. Ясно, что N не содержится ни в какой компоненте расщепления, и поэтому N расщепляем. Это означает, что N — элементарная абелева p-группа. Ввиду того что p-группа всегда содержит допустимый нормальный делитель, G — не p-группа, и вне N имеется элемент b простого порядка $q \neq p$. Для любого элемента b порядка $q \neq p$ группа $N \leftthreetimes \{b\}$ расщепляема, так как N не лежит ни в какой компоненте расщепления. Из расщепляемости $N \leftthreetimes \{b\}$ вытекает, что b действует регулярно на N. Компонента расщепления, пересекающаяся с N, есть p-группа (так как иначе она нильпотентна и непримарна, что противоречит тому, что все p'-элементы действуют регулярно на N). В одной из компонент, пересекающихся с N, есть элемент a порядка p^2. Рассмотрим подгруппу $H = \{N, a\}$. $|\ H : N\ | = p$. В силу леммы 4 из § 8 $p = 2$ и H — прямое произведение группы диэдра порядка 8 и элементарной абелевой группы. Если пересечение N с некоторой компонентой — нециклическая группа, то существует по крайней мере еще одна компонента, с которой N имеет нециклическое пересечение. Если $|\ H\ | > 8$, то нециклическое пересечение возможно лишь одно. Итак, пересечения циклические, $|\ N\ | = 4$ и $|\ G/N\ | = 6$. Пусть R — нормализатор силовской 3-подгруппы группы G. Тогда $G = N \leftthreetimes R$. G имеет точное представление

подстановками на смежных классах по R. Так как $|G| = 24$, то $G \cong S_4$.

Теперь легко получается следующая

Лемма 2. *Конечная расщепляемая группа G либо p-нормальна, либо (при $p = 2$) нормализатор некоторого максимального пересечения ее силовских 2-подгрупп есть S_4, а силовские p-подгруппы — группы диэдра.*

Доказательство. Пусть G — не p-нормальна для некоторого p. Тогда центр Z силовской p-подгруппы P содержится в другой силовской подгруппе $x^{-1}Px$ и не является центром последней. Более того, Z не инвариантен в $x^{-1}Px$ (см., например, М. Холл [9, стр. 228]). Положим $D = P \cap x^{-1}Px$. На основании теоремы Бернсайда [9, стр. 57] можно считать, что D — максимальное пересечение силовских p-подгрупп. $N(D)$ не нильпотентен, не группа Фробениуса и не HT-группа. Из результатов § 8 следует, что $N(D)$ изоморфен S_4. Это означает, что P содержит нециклическую подгруппу порядка 4, совпадающую со своим централизатором. Поэтому P — группа диэдра порядка $\geqslant 8$. Если $D = P \cap g^{-1}Pg$ — любое максимальное нециклическое пересечение силовских подгрупп (не особо выбранное), то из результатов § 8 вытекает, что $N(D) \cong S_4$.

Предположим, что непростая расщепляемая группа G не содержит разрешимых нормальных делителей. Обозначим через C минимальный нормальный делитель группы G. Так как группа C неразрешима, то она не содержится в компоненте никакого расщепления группы G; следовательно, C — простая группа.

Теорема 3. $|G : C| = 2$ *и* $G \cong PGL(2, q)$, *где* $q \geqslant 5$ — *нечетное число.*

Доказательство проведем индукцией по порядку группы G. Предположим, что для всех групп, порядок которых меньше $|G|$, утверждение справедливо. Отсюда следует, что (если утверждение для G неверно): 1) либо $|G : C| = 4$; 2) либо $|G : C| = p$, p — простое число.

Рассмотрим первый случай: $|G : C| = 4$. Обозначим через H подгруппу из G, содержащую C. По индуктивному предположению, $H \cong PGL(2, r)$, где r — нечетное число. Рассмотрим нормализатор силовской подгруппы Q порядка r в группе G. Так как $N_H(Q)$ — группа Фробениуса, то $N_G(Q)$, как разрешимая ненильпотентная расщепляемая группа, является либо группой Фробениуса, либо HT-группой. Если $N_G(Q)$ — HT-группа, то

порядок дополнительного множителя в $N_H(Q)$ есть простое число. С другой стороны, его порядок равен $r-1$. Поэтому $r=3$, а это противоречит предположению о неразрешимости C. Если же $N_G(Q)$ — группа Фробениуса, то ее инвариантный множитель совпадает с инвариантным множителем группы $N_H(Q)$. Но тогда порядок дополнительного множителя группы $N_G(Q)$ равен $2(r-1)>r$, что невозможно. Значит, $|G:C| \neq 4$.

Покажем, что во втором случае: $|G:C|=p$ индекс C равен 2. Если G — p-нормальна, то нормализатор центра силовской p-подгруппы P группы G имеет инвариантную подгруппу индекса p. Поэтому $N(Z(P))$ — либо HT-группа, либо нильпотентная группа. В любом случае $N(Z(P))$ имеет нормальное p-дополнение. Это означает, что $|P|$ — простое число, и $N(P)$-нильпотентная группа. Следовательно, $N(P)$ содержится в некоторой компоненте нормального расщепления. Так как G не группа Фробениуса, то нормализатор группы $N(P)$ в G отличен от $N(P)$, что невозможно. Итак, G не p-нормальна и $p=2$ (см. лемму 2). В силу леммы 2 силовская 2-подгруппа группы G есть группа диэдра. Поэтому группа G имеет точно 2 класса сопряженных инволюций. Так как G не 2-нормальна, то она имеет точно 2 класса сопряженных компонент четного порядка. Пусть A_1 и A_2 — несопряженные компоненты четного порядка, и допустим, для определенности, что $|A_1|<|A_2|$. Так как $N(A_i)$ имеет инвариантную подгруппу индекса 2, то $N(A_i)=A_j \leftthreetimes \{a_i\}$, $a_i^2=1$ (N_{A_i},— HT-группа и A_i— компонента расщепления $N(A_i)$). Группа G имеет $\gamma/2\alpha_i$ инволюций, лежащих в подгруппах, сопряженных с A_i'; здесь $\gamma=|G|$, $\alpha_i=|A_i|$. Из них можно составить $\gamma/2\alpha_i \times (\gamma/2\alpha_i-1)$ отличных от единицы попарных произведений, из которых $\gamma/8(\alpha_1+\alpha_2-\gamma/2)$. содержатся в компонентах, сопряженных либо A_1, либо A_2. Очевидно,

$$\gamma/2(\gamma/2\alpha_1-1)>\gamma/8(\alpha_1+\alpha_2-\gamma/2).$$

Поэтому G содержит две инволюции, сопряженные инволюции из A_1, произведение которых принадлежит компоненте A_3, не сопряженной ни A_1, ни A_2. Так как упомянутые выше инволюции принадлежат $N(A_3)$ и $|A_3|$ — нечетное число, то $N(A_3)$ — группа Фробениуса. Некоторый дополнительный множитель C_3 группы $N(A_3)$ имеет с A_1 неединичное пересечение. Поэтому $C_3 \subseteq A_1$. Можно считать расщепление таким, что A_3 — инвариантный множитель группы $N(A_3)$. В этом случае покажем, что G содержит

точно три класса сопряженных компонент. Допустим, что C имеет n классов сопряженных компонент и пусть A_i — их представители. Положим $\alpha_i = |A_i|$, $v_i = |N(A_i)|$, $i = 1, 2, \ldots, n$. Тогда

$$\gamma - 1 = \sum_{i=1}^{n} \gamma/v_i(\alpha_i - 1).$$

Учитывая значения v_i для $i = 1,2$, получаем

$$\gamma - 1 = \gamma/2\alpha_1(\alpha_1 - 1) + \gamma/2\alpha_2(\alpha_2 - 1) + \sum_{i=3}^{n} \gamma\alpha_i/v_i\left(\frac{\alpha_i - 1}{\alpha_i}\right).$$

Так как при $i > 2$ $\alpha_j \geqslant 3$, то

$$\gamma/2\left(\frac{1}{\alpha_1} + \frac{1}{\alpha_2}\right) > \frac{3}{4}\sum_{i=3}^{n} \gamma\alpha_i/v_i.$$

Из $\alpha_1 < \alpha_2$ вытекает, что

$$1/\alpha_1 > \frac{3}{4}\sum_{i=1}^{n} \alpha_i/v_i.$$

Но тогда $1/\alpha_1 > {}^3/_4\,\alpha_3/v_3$. Это означает, что $\alpha_1 = v_3/\alpha_3$ и что существует лишь один класс сопряженных компонент, нормализаторы которых содержат инволюции из сопряженных с A_1 подгрупп. Таким образом,

$$\gamma/2\alpha_1(\gamma/2\alpha_1 - 1) = \gamma/8(\alpha_1 + \alpha_2 - \gamma/2 + \gamma/\alpha_1(\alpha_3 - 1)).$$

Отсюда

$$\gamma/4\alpha_1{}^2 < (\alpha_1 + \alpha_2)/8 + (\alpha_3 - 1)/\alpha_1,$$

или

$$\gamma/4\alpha_1{}^2 < \alpha_2/4 + \alpha_3/\alpha_1.$$

Так как α_1, α_2 и α_3 не имеют общих нечетных делителей, то $\gamma = \alpha_1\alpha_2\alpha_3\delta$, где δ — целое число. Но тогда

$$\alpha_2\alpha_3\delta/4\alpha_1 < (\alpha_1\alpha_2 + 4\alpha_3)/4\alpha_1,$$

Так как $\alpha_2 \geqslant 4$, то

$$\delta < \frac{\alpha_1\alpha_2 + \alpha_2\alpha_3}{\alpha_2\alpha_3}$$

или

$$\delta < (\alpha_1 + \alpha_2)/a_3 < 2.$$

Поэтому $\delta = 1$ и $\gamma = \alpha_1\alpha_2\alpha_3$. Подгруппы A_1, A_2, A_3 абелевы (см. лемму § 8), и, следовательно, любая компонента расщепления группы G сопряжена с одной из подгрупп A_i $(i = 1, 2, 3)$.

Докажем, что $\alpha_1 = \alpha_3 - 1$, $\alpha_2 = \alpha_3 + 1$. Из равенств

$$\gamma - 1 = \gamma(\alpha_1 - 1)/2\alpha_1 + \gamma\,(\alpha_2 - 1)/2\alpha_2 + \gamma\,(\alpha_3 - 1)/\alpha_1\alpha_3$$

и

$$\gamma = \alpha_1\alpha_2\alpha_3$$

получаем

$$\alpha_3\,(\alpha_2 - \alpha_1) = 2\,(\alpha_2 - 1).$$

Так как $\alpha_3 \geqslant 5$, то

$$3\alpha_2 < 5\alpha_1.$$

Теперь

$$\alpha_2 - \alpha_1 < 2\,(\alpha_2 - 1)/\alpha_3 < {}^{10}/_3 \cdot \alpha_1/\alpha_3 < 4.$$

Так как $\alpha_2 - \alpha_1$ — четное число, то

$$\alpha_2 - \alpha_1 = 2.$$

равенство $\alpha_2\,(\alpha_2 - \alpha_1) = 2\,(\alpha_2 - 1)$ можно преобразовать к виду

$$\alpha_2 = \alpha_3 + 1.$$

Но тогда $\alpha_1 - \alpha_3 = 1$.

Так как $N\,(A_3)$ — группа Фробениуса порядка $\alpha_3\,(\alpha_3 - 1)$, то $\alpha_3 = p^k$ для некоторого нечетного простого числа p. Обозначим $\alpha_3 = q$.

Рассмотрим группу G как группу подстановок, сопряженных с A_3 подгрупп. Нетрудно убедиться, что G — дважды транзитивная группа подстановок $q + 1$ символа. Так как нормализаторы силовских p-подгрупп (групп, сопряженных с A_3) группы G пересекаются по компонентам порядка α_1 и так как $|N\,(A_1) : A_1| = 2$, то пересечение нормализаторов трех любых попарно различных силовских p-подгрупп равно $\{1\}$. Это означает, что каждая подстановка в G однозначно определена образами своих трех символов. Подстановки, лежащие в компонентах, сопряженных A_2, регулярны; лежащие в компонентах, сопряженных A_3, оставляют на месте точно один символ; лежащие в компонентах, сопряженных A_1, оставляют на месте точно два символа.

Обозначим переставляемые символы через $0, 1, 2, \ldots, q-1, \infty$. Пусть H — подгруппа, состоящая из всех элементов группы G, оставляющих на месте символ ∞. Очевидно, порядок H равен

q $(q-1)$, и она совпадает с нормализатором некоторой силовской p-подгруппы. Можно считать, что $H = A_3 \leftthreetimes A_1$. На символах $0, 1, \ldots, q-1$ H — дважды транзитивная группа Фробениуса, и все нетождественные подстановки из A_3 регулярны. Без ограничения общности можно считать, что элементы из A_1 не изменяют символ 0. В A_3 существует единственная подстановка π_b, переводящая 0 в символ $b \neq \infty$. В A_1 существует также единственная подстановка m_a, переводящая 1 в символ $a \neq 0, \infty$. Определим сумму двух (не равных ∞) символов a и b следующим образом: $a + b = \pi_b(a)$, а произведение двух (не равных 0 и ∞) символов a и b следующим образом: $ab = m_a(b)$. Дополнительно положим $0b = b0$. Легко проверить, что относительно определенных операций символы $0, 1, \ldots, q-1$ образуют поле, аддитивная группа которого изоморфна A_3, а мультипликативная — A_1. Элементами H являются подстановки вида $az + b$ $(a \neq 0)$.

Обозначим через $\sigma(z)$ подстановку, переставляющую 0 и ∞: $\sigma(0) = \infty$, $\sigma(\infty) = 0$. Группа $\sigma^{-1}H\sigma = H_1$ состоит из подстановок, оставляющих на месте символ 0. Так как $H \cap H_1 = A_1$, то σ содержится в нормализаторе A_1; поэтому $\sigma^2 = 1$, и для любой подстановки $az \in A_1$ имеем $\sigma(a\sigma(x)) = a^{-1}x$. В частности, при $x = a$ получаем $\sigma(a\sigma(a)) = 1$. Значит, $\sigma(a) = a^{-1}\sigma(1)$. Ясно, что группа, порожденная H и σ, имеет порядок $q(q^2-1)$ и совпадает с $PGL(2, q)$.

§ 10. Простые расщепляемые группы

Теорема 1. *Конечная простая расщепляемая группа есть группа одного из типов:*

а) $PSL(2, q)$, $q \geqslant 4$;

б) $G(q)$, $q = 2^{2k+1}$, $k \geqslant 1$, — *простая группа Сузуки.*

Предположим, что теорема неверна. Тогда существует группа G наименьшего порядка, простая, все подгруппы которой таковы:

1) $PGL(2, q)$;
2) $PSL(2, q)$;
3) $G(q)$;
4) S_4;
5) нильпотентные группы;
6) группы Фробениуса;
7) HT-группы.

Сразу же считаем, что порядок группы G — четное число (см. В. Фейт, М. Холл и Д. Томпсон [24] и М. Сузуки [56]).

Рассмотрим сначала случай, когда все силовские 2-подгруппы имеют единичное пересечение. Обозначим через M максимальную нильпотентную подгруппу группы G, содержащую силовскую 2-подгруппу. Нетрудно убедиться, что M имеет единичное пересечение с любой сопряженной с ней подгруппой. $N(M)$ — либо группа Фробениуса, либо HT-группа. В любом случае она представима в виде полупрямого произведения $N(M) = M \leftthreetimes H$. Пусть $n_1x, n_2x, \ldots, n_kx$ — все инволюции смежного класса $N(M)x$, $x \notin N(M)$. Так как $n_1xx^{-1}n_i^{-1} = n_1n_i^{-1}$ и $x^{-1}n_i^{-1} \cdot n_1x$ — обратные элементы, то $N(M)$ и $x^{-1}N(M)x$ имеют не менее $k-1$ общих неединичных элементов. Порядок пересечения $N(M)$ и $x^{-1}N(M)x$, очевидно, не превосходит $|H|$. Поэтому $k \leqslant |H|$. Так как инволюций в G точно $t\,|\,G : N(M)\,|$, где t — число инволюций в M, то из $t \geqslant |H|$ следует, что $k \geqslant |H|$. Следовательно, любой смежный класс группы G по $N(M)$ содержит точно $|H|$ инволюций. Отсюда следует, что $N(M)$ нетривиально пересекается с любой сопряженной с ней подгруппой. Так как $N(M)$ сопряжена с последней инволюцией, то H содержится точно в одной отличной от $N(M)$ и сопряженной с ней подгруппе. Значит, представление группы G подстановками смежных классов по подгруппе $N(M)$ есть дважды транзитивная группа подстановок, в которой только тождественная подстановка оставляет неизменными три различных символа. Поэтому G — ZT-группа. Из результатов следующего параграфа вытекает, что в этом случае теорема доказана.

Допустим, что некоторые две силовские 2-подгруппы группы G имеют неединичное пересечение. Обозначим через $N(D)$ нормализатор максимального пересечения силовских 2-подгрупп. Если G — не 2-нормальна, то $N(D) \cong S_4$. В этом случае силовские 2-подгруппы группы G есть группы диэдра (см. лемму 2 § 9). Поэтому из простоты группы G вытекает сопряженность всех инволюций. Если G 2-нормальна, то $N(D)$ — HT-группа, $N(D) = (S \times P) \leftthreetimes \{a\}$, где $S \leftthreetimes \{a\}$ — группа Фробениуса, а $P \leftthreetimes \{a\}$ — расщепляемая 2-группа. Если $P \leftthreetimes \{a\}$ не элементарная абелева группа, то нормализатор подгруппы Фраттини группы $P \leftthreetimes \{a\}$ есть HT-группа, которая, очевидно, совпадает с $N(D)$. Но тогда $P \leftthreetimes \{a\}$ — силовская 2-подгруппа G, а $N(D)$ — нормализатор ее центра.

По теореме Грюна [30] группа G не проста. Полученное противоречие показывает, что $P \leftthreetimes \{a\}$ — элементарная абелева группа. Нетрудно доказать, что $|P| = 2$. Это означает, что силовская 2-подгруппа группы G есть группа диэдра. Если она неабелева, то она выделяется прямым множителем в нормализаторе центра. По теореме Грюна [30] группа G не проста. Итак, если группа G 2-нормальна, то порядок силовской 2-подгруппы равен 4.

Дальнейшее доказательство проведем, как в статье Брауэра, Сузуки и Волла [16]. Зафиксируем обозначения. P — силовская 2-подгруппа, G, τ — инволюция из ее центра, $C = C(\tau) = H \leftthreetimes \leftthreetimes \{\sigma\}$, где $\sigma^2 = 1$, $\sigma h \sigma = h^{-1}$ для любого $h \in H$. Группа C совпадает с нормализатором любой подгруппы из H. Если $h \in H$ и $h \neq \tau$, то $C(h) = H$. C — холловская подгруппа группы G. Пусть h_1 и h_2 сопряжены: $h_1 = x^{-1}h_2x$, h_1 и $h_2 \in H$. Тогда $D = H \cap x^{-1}Hx \neq \neq \{1\}$. Так как $C = N(D), N(D) \supset H$ и $x^{-1}Hx$, то $H = x^{-1}Hx$. Это означает, что $x \in C$. Следовательно, если элементы из H сопряжены в G, то они сопряжены уже в C.

Рассмотрим ограничения неприводимых характеров группы G на подгруппу H. Обозначим $|H| = s$. Группа H имеет s неприводимых характеров:

$$\xi_{-r}, \xi_{-r+1}, \ldots, \xi_0, \xi_1, \ldots, \xi_r, \xi_{r+1},$$

где $r = s/2 - 1$ и $\xi_{-j}(t) = \overline{\xi_j(t)}$.

Пусть $\chi^{(1)}$, $\chi^{(2)}$, ..., $\chi^{(k)}$ — все неприводимые характеры группы G. Положим

$$\chi^{(\mu)}|H = \sum_{j=-r}^{r+1} a_{\mu j}\xi_j \quad (\mu = 1, 2, \ldots, k), \tag{1}$$

где $a_{\mu j}$ — целые неотрицательные числа. Так как $\chi^{(m)}(t) = \chi^{(\mu)}(t^{-1})$ для $t \in H$, то $a_{\mu j} = a_{\mu -j}$.

Из (1) следует, что

$$a_{\mu j} = \frac{1}{s} \sum_{x \in H} \chi^{(\mu)}(x)\,\overline{\xi_j(x)}. \tag{2}$$

Обозначим через a_i столбец из чисел $a_{1i}, a_{2i}, \ldots, a_{ki}$. Докажем, что

$$\begin{aligned} a_i a_j &= u && \text{для } i \neq j,\ 0 \leqslant i, j \leqslant r+1, \\ a_i^2 &= u+1 && \text{для } i = 1, 2, \ldots, r, \\ a_i^2 &= u+2 && \text{для } i = 0 \text{ и } i = r+1; \end{aligned} \tag{3}$$

здесь $u = (n - 2s)/s^2$, $n = |G|$, $a_i a_j$ — обычное скалярное произведение. В силу (2) имеем

$$\sum_{\mu=1}^{k} a_{\mu i} a_{\mu j} = \sum_{\mu=1}^{k} a_{\mu i} \overline{a}_{\mu j} = \frac{1}{s^2} \sum_{x, y \in H}^{k} \overline{\xi_i(x)}\, \xi_j(y) \sum_{\mu=1}^{k} \chi^{(\mu)}(x)\, \overline{\chi^{(\mu)}(y)}.$$

Если x и y не сопряжены, то

$$\sum_{\mu=1}^{k} \chi^{(\mu)}(x)\, \overline{\chi^{(\mu)}(y)} = 0;$$

если они сопряжены, то

$$\sum_{\mu=1}^{k} \chi^{(\mu)}(x)\, \overline{\chi^{(\mu)}(y)} = |C(x)|.$$

Поэтому

$$\sum_{\mu=1}^{k} a_{\mu i} a_{\mu j} = \frac{n}{s^2} + \frac{2s}{s^2} \overline{\xi_i(\tau)}\, \xi_j(\tau) + \frac{s}{s^2} \sum_{x \in H,\, x \neq 1,\, \tau} \overline{\xi_i(x)} \left(\xi_j(x) + \xi_j(x^{-1})\right).$$

Из соотношений ортогональности получаем

$$\frac{1}{s} \sum_{x \in H} \overline{\xi_i(x)} \left(\xi_j(x) + \overline{\xi_j(x)}\right) = \begin{cases} 0 \text{ для } i \neq j; \\ 1 \text{ для } i = j,\ i \neq 0,\ r+1; \\ 2 \text{ для } i = j,\ i = 0 \text{ или } r+1, \end{cases}$$

где $0 \leqslant i, j \leqslant r + 1$. Так как

$$2\overline{\xi_j(\tau)}\xi_j(\tau) = \overline{\xi_i(\tau)}\left(\xi_j(\tau) + \overline{\xi_j(\tau)}\right),$$

то

$$\sum_{\mu=1}^{k} a_{\mu i} a_{\mu j} = \begin{cases} 0 \\ 1 = \dfrac{n}{s^2} - \dfrac{2}{s}. \\ 2 \end{cases}$$

Это доказывает (3).

Из (2) вытекает, что

$$a_{\mu j} - a_{\mu 1} = \frac{1}{s} \sum_{\substack{x \in H \\ x \neq 1}} \chi^{(\mu)}(x) \left(\overline{\xi_j(x)} - \overline{\xi_1(x)}\right).$$

Пусть y не сопряжен с неединичными элементами из H. Домножим предыдущее равенство на $\overline{\chi^{(\mu)}(y)}$ и просуммируем

по $\mu = 1,2,\ldots,k$

$$\sum_{\mu=1}^{k} (a_{\mu j} - a_{\mu 1}) \overline{\chi^{(\mu)}(y)} = \frac{1}{s} \sum_{\substack{x \in H \\ x \neq 1}} \overline{(\xi_j(x) - \xi_1(x))} \sum_{\mu=1}^{k} \chi^{(\mu)}(x) \overline{\chi^{(\mu)}(y)}.$$

Согласно соотношениям ортогональности

$$\sum_{\mu=1}^{k} \chi^{(\mu)}(x) \overline{\chi^{(\mu)}(y)} = 0.$$

Обозначим через $\chi(y)$ столбец $\chi^{(1)}(y), \chi^{(2)}(y),\ldots, \chi^{(x)}(y)$. Для y, не сопряженного с неединичным элементом из H, получаем

$$(a_j - a_1)\,\chi(y) = 0 \qquad (j = 0,1,\ldots,\ r+1). \tag{4}$$

Покажем существование исключительных характеров группы G. Предположим, что $r > 1$. Будем говорить, что характер $\chi^{(\mu)}$ исключительный, если не все числа $a_{\mu_2} - a_{\mu_1}$, $a_{\mu_3} - a_{\mu_1},\ldots, a_{\mu r} - a_{\mu_1}$ равны 0. Так как доказательство очень длинное, то для удобства будем нумеровать некоторые промежуточные результаты.

а) Пусть $r \geqslant 2$. Тогда существует точно r исключительных характеров группы G. Их можно взять в качестве $\chi^{(1)}, \chi^{(2)},\ldots, \chi^{(r)}$ в таком порядке, что

$$a_{ij} = a + \varepsilon\delta_{ij} \qquad (\text{для } i,\ j = 1,2,\ldots,r), \tag{5}$$

где a — фиксированное целое число, а $\varepsilon = \pm 1$.

Доказательство. Пусть $j = 2, 3,\ldots, r$. Тогда равенства (3) показывают, что

$$(a_j - a_1)^2 = 2.$$

Так как коэффициенты столбца $(a_j - a_1)$ — целые числа, то лишь два из них отличны от нуля и равны ± 1. В силу соотношений (4) один из коэффициентов равен $+1$, а другой -1, так как $\chi^{(\mu)}(1)$ — целое положительное число. Предположим, что $r \geqslant 3$. Если $j' = 2, 3,\ldots, r$, то из равенств (3) получаем, что

$$(a_j - a_1)(a_{j'} - a_1) = 1 \qquad \text{для } j \neq j'.$$

Следовательно, $a_j - a_1$ и $a_{j'} - a_1$ имеют равные ненулевые коэффициенты точно в одной строке. В других строках, если в одном из столбцов стоит ненулевой коэффициент, то в другом стоит нуль. Выберем $\chi^{(1)}$ так, чтобы $a_2 - a_1$ и $a_3 - a_1$ имели равные ненуле-

вые коэффициенты в первой строке, и обозначим этот коэффициент через $-\varepsilon$. Характеры $\chi^{(1)}$, $\chi^{(2)}$,..., χ^{k} можно перенумеровать так, что таблица M, составленная из столбцов $a_2 - a_1$, $a_3 - a_1$,..., $a_r - a_1$, приобретает вид

$$M = \begin{pmatrix} -\varepsilon & -\varepsilon & -\varepsilon & \dots & -\varepsilon \\ \varepsilon & 0 & 0 & \dots & 0 \\ 0 & \varepsilon & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \varepsilon \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{6}$$

Из таблицы видно, что существует точно r исключительных характеров, которыми можно считать $\chi^{(1)}$, $\chi^{(2)}$,..., $\chi^{(r)}$. Формулы (3) показывают, что $a_1 (a_i - a_1) = -1$ для $i = 2, 3,..., r$. Таблица (6) теперь приводит к равенству $a_{11}(-\varepsilon) + a_{i1}\varepsilon = -1$. Следовательно, $a_{i1} = a_{11} - \varepsilon$ для $i = 2, 3,..., r$. Прибавив столбец a_1 к $a_j - a_1$, видим, что $a_{ii} = a_{11}$, $a_{ij} = a_{11} - \varepsilon$ для $i \neq j$. Обозначим через $a = a_{11} - \varepsilon$. Утверждение а) доказано.

$$\chi^{(1)}(y) = \chi^{(2)}(y) = \dots = \chi^{(r)}(y) \tag{7}$$

для y, не сопряженного с неединичными элементами из H.

Утверждение (7) вытекает из равенств (4) и таблицы (6).

Определим значения характеров группы G на неединичных элементах из H. Сначала найдем $a_0 - a_1$ и $a_{r+1} - a_1$. Из равенств (3) получаем

$$(a_0 - a_1)^2 = 3, \qquad (a_{r+1} - a_1)^2 = 3, \qquad (a_0 - a_1)(a_{r+1} - a_1) = 1, \tag{8}$$

$$a_0 (a_j - a_1) = 0, \quad a_{r+1}(a_j - a_1) = 0 \qquad \text{для } j = 2, 3,..., r. \tag{9}$$

Формулы (8) показывают, что $a_0 - a_1$ и $a_{r+1} - a_1$ имеют три ненулевых коэффициента, которые равны ± 1. Точно в одной строке $a_0 - a_1$ и $a_{r+1} - a_1$ имеют равный ненулевой коэффициент. Если бы существовала еще одна строка, в которой $a_0 - a_1$ и $a_{r+1} - a_1$ имели одновременно ненулевой коэффициент, то $a_0 - a_1$ и $a_{r+1} - a_1$ имели бы равные ненулевые коэффициенты (согласно (8)) точно в двух строках и в одной противоположные. Тогда столбец $(a_0 - a_1) - (a_{r+1} - a_1)$ имеет точно один ненулевой коэффициент, равный ± 2. Так как $\chi^{(\mu)}(1)$ — целое положительное число, то равенство (4) приводит к противоречию. Итак,

точно в одной строке $a_0 - a_1$ и $a_{r+1} - a_1$ имеют одновременно ненулевые коэффициенты, последние равны. Из формулы (4) следует, что не все коэффициенты в $a_0 - a_1$ и $a_{r+1} - a_1$ имеют один знак. Соотношения (9) и таблица (6) показывают, что первые r коэффициентов столбца $a_0 - a_1$ равны следующим числам:

$$a_{10} - a - \varepsilon,\ a_{10} - a, \ldots,\ a_{10} - a. \tag{10}$$

Так как эти коэффициенты равны 0, 1 или -1, то $a_{10} = a$ или $a_{10} = a + \varepsilon$. Так же первые r коэффициентов столбца $a_{r+1} - a_1$ равны

$$a_{1r+1} - a - \varepsilon,\ a_{1r+1} - a, \ldots,\ a_{1r+1} - a. \tag{11}$$

Поэтому $a_{1r+1} = a$ или $a_{1r+1} = a + \varepsilon$. Покажем, что $a_{10} = a_{1r+1} = a$. Это ясно для $r \geqslant 4$, так как в противном случае столбцы $a_0 - a_1$ и $a_{r+1} - a_1$ имели бы более трех ненулевых коэффициентов. Следовательно, необходимо рассмотреть случаи $r = 3$ и 2. Если $\chi^{(j)}$ — главный характер, то равенства (1) показывают, что $a_{j0} = 1$, $a_{jv} = 0$ для $v \neq 0$. Поэтому $\chi^{(j)}$ не исключительный. Можно считать, что $j = r + 1$.

Предположим, что $r = 3$. Если $a_{10} = a_{1r+1} = a + \varepsilon$, то согласно (10) и (11) столбцы $a_0 - a_1$ и $a_{r+1} - a_1$ имеют во второй и третьей строках ненулевые коэффициенты, что невозможно. Если одно из чисел a_{10}, a_{r+1}, 0 равно a, а другое $a + \varepsilon$, то первые три коэффициента в $a_0 - a_{r+1}$ равны. Их значения есть ± 1. Более того, коэффициент в четвертой строке ± 1. Так как $(a_0 - a_{r+1})^2 = 4$, то все другие коэффициенты равны нулю. Согласно равенству (7) характеры $\chi^{(1)}$, $\chi^{(2)}$, $\chi^{(3)}$ имеют одну и ту же степень f. Главный характер $\chi^{(4)}$ имеет степень 1. В силу (4)

$$(a_0 - a_{r+1})\chi(1) = (a_0 - a_1)\chi(1) - (a_{r+1} - a_1)\chi(1) = 0.$$

Следовательно, $\pm 3f \pm 1 = 0$. Это невозможно. Итак, для $r = 3$ $a_{10} = a_{r+10} = a$.

Рассмотрим случай $r = 2$. Пусть $a_{10} = a_{1r+1} = a + \varepsilon$. Заменим $a + \varepsilon$ на a, ε на $-\varepsilon$ и $\chi^{(1)}$ на $\chi^{(2)}$. Если $a_{10} = a + \varepsilon$, $a_{1r+1} = a$, то из равенств (1) и (2) следует, что

$$\chi^{(1)} | H = \varepsilon(\xi_0 + \xi_1 + \xi_1^{-1}) + a \sum_{i=-r}^{r+1} \xi_i.$$

Так как $r = 2$, то H — циклическая группа. Если $H = \{h\}$, то

$$\chi^{(1)}(h) = 2\varepsilon, \qquad \chi^{(1)}(h^2) = 0.$$

Поскольку h^2 имеет порядок 3, то степень f характера $\chi^{(1)}$ делится на 3. Ввиду того что $n\,\chi^{(1)}(h)$ делится на sf (см., например, М. Холл [9, стр. 313]), $n\chi^{(1)}(h) = 2\varepsilon n$ делится на $3s$. Но тогда n делится на 9. Это противоречит тому, что C — холловская подгруппа G. Аналогично, если $a_{10} = a$, $a_{1r+1} = a + \varepsilon$, противоречие получится при рассмотрении $\chi^{(2)}$. Таким образом, в случае $r = 2$ $a_{10} = a_{1r+1} = a$.

Рассматривая коэффициенты (10) и (11) столбцов $a_0 - a_1$ и $a_{r+1} - a_1$, можно заметить, что первый коэффициент есть $-\varepsilon$, а далее $r - 1$ коэффициент равен 0. Строка с номером $r + 1$ принадлежит главному характеру, так что коэффициенты в ней 1 и 0 соответственно. Ранее доказано, что можно так выбрать $\chi^{(r+2)}$, $\chi^{(r+3)}$, $\chi^{(r+4)}$, что $a_0 - a_1$ имеет в строке с номером $r + 2$ коэффициент ± 1, а $a_{r+1} - a_1$ имеет такие коэффициенты в строках с номерами $r + 3$ и $r + 4$. Все остальные коэффициенты в этих столбцах — нули. Собирая полученные результаты (см. равенство (1) и утверждение а)), находим ограничения характеров на H:

$$\chi^{(i)} \mid H = \varepsilon(\xi_i + \xi_{-i}) + a \sum_{j=-r}^{r+1} \xi_j, \qquad i = 1, 2, \ldots, r,$$

$$\chi^{(r+1)} \mid H = \xi_0,$$

$$\chi^{(r+2)} \mid H = \delta_2 \xi_0 + a_{r+21} \sum_{j=-r}^{r+1} \xi_j, \tag{12}$$

$$\chi^{(r+3)} \mid H = \delta_3 \xi_{r+1} + a_{r+31} \sum_{j=-r}^{r+1} \xi_j,$$

$$\chi^{(r+4)} \mid H = \delta_4 \xi_{r+1} + a_{r+41} \sum_{j=-r}^{r+1} \xi_j,$$

$$\chi^{(r+\mu)} \mid H = a_{r+\mu 1} \sum_{j=-r}^{r+1} \xi_j,$$

где $\delta_2, \delta_3, \delta_4 = \pm 1$.

Заметим, что этот результат верен и для $r = 1$. Действительно, в этом случае столбцы таковы: a_0, a_2, $a_1 = a_{-1}$. Как и прежде, столбцы $a_0 - a_1$ и $a_2 - a_1$ имеют одновременно ненулевые коэффициенты точно в одной строке. Эти коэффициенты равны,

скажем, ε. Соответствующий этой строке характер обозначим $\chi^{(1)}$. Характер $\chi^{(2)}$ можно взять главным. Характер $\chi^{(3)}$ выберем так, чтобы коэффициент ± 1 столбца $a_0 - a_1$ был в третьей строке, а характеры $\chi^{(4)}$ и $\chi^{(5)}$ — так, чтобы ± 1 стояли в 4-й и 5-й строках. Итак, результат (12) верен для $r = 1$.

Обозначим через χ_μ характер $\chi^{(r+\mu)}$ для $\mu > 0$. Тогда получаем следующее утверждение.

б) Неприводимые характеры группы G можно обозначить следующим образом: $\chi^{(1)}, \ldots, \chi^{(r)}, \chi_1, \chi_2, \ldots, \chi_m, m \geqslant 4$, так что для любого $x \neq 1$ из H справедливы равенства:

$$
\begin{aligned}
&\chi^{(i)}(x) = \varepsilon(\xi_i(x) + \xi_{-i}(x)), && i = 1,2,\ldots,r,\\
&\chi_j(x) = \delta_j, && j = 1, 2,\\
&\chi_j(x) = \delta_j \xi_{r+1}(x), && j = 3, 4,\\
&\chi_j(x) = 0, && j \geqslant 5;
\end{aligned} \tag{13}
$$

здесь $\delta_1 = 1$.

Выведем соотношения между степенями неприводимых характеров группы G. Если ψ — характер C, то из соотношений ортогональности получаем

$$
\psi(1) + \frac{s}{2}\psi(\sigma) + \frac{s}{2}\psi(\sigma\tau) + \sum_{\substack{x \in H \\ x \neq 1}} \psi(x) \equiv 0 \pmod{2s}.
$$

Если ψ — ограничение характера группы G, то $\psi(\sigma) = \psi(\sigma\tau) = \psi(\tau)$, так как инволюции в группе G сопряжены. Комбинируя это с равенствами (13), получаем утверждение:

в) Если f — степень исключительных характеров $\chi^{(i)}$ и если f_j — степень χ_j, $j = 1,2,\ldots,m$, то

$$
\begin{aligned}
&f \equiv 2\varepsilon \pmod{2s},\\
&f_j \equiv \delta_j \pmod{2s}, && j = 1, 2,\\
&f_j \equiv s + \delta_j \pmod{2s}, && j = 3, 4,\\
&f_j \equiv 0 \pmod{2s}, && j \geqslant 5.
\end{aligned} \tag{14}
$$

Доказательство. Для $\psi = \chi^{(i)} \mid C$ сравнение, написанное выше, приобретает вид

$$
f + s\varepsilon(\xi_i(\tau) + \xi_{-i}(\tau)) + \varepsilon \sum_{\substack{x \in H \\ x \neq 1}} (\xi_i(x) + \xi_{-i}(x)) \equiv 0 \pmod{2s}.
$$

Так как

$$2+\sum_{\substack{x\in H\\ x\neq 1}}(\xi_i(x)+\xi_{-i}(x))=0,$$

то $f\equiv 2\varepsilon \pmod{2s}$. Подобно для $j=1,2$ имеем уравнение

$$f_j+\delta_j s+\delta_j\sum_{\substack{x\in H\\ x\neq 1}}1\equiv 0 \pmod{2s}.$$

Отсюда $f_j=\delta_j \pmod{2s}$. Остальные сравнения доказываются так же.

$$1+\delta_2\chi_2(x)=\varepsilon\chi^{(j)}(x),$$

$$\delta_3\chi_3(x)+\delta_4\chi_4(x)=\varepsilon\chi^{(j)}(x) \tag{15}$$

для x, не сопряженного с неединичным элементом из H. В частности,

$$1+\delta_2 f_2=\varepsilon f,\quad \delta_3 f_3+\delta_4 f_4=\varepsilon f. \tag{16}$$

Равенства (15) вытекают из

$$(a_0-a_1)\chi(x)=0,\ (a_{r+1}-a_1)\chi(x)=0$$

и значений коэффициентов столбцов a_0-a_1 и $a_{r+1}-a_1$.

Пусть $K_1,\ldots,K_k$ — классы сопряженных элементов группы G; считаем, что $1\in K_1$, $\tau\in K_2$; если $x\neq 1$, τ и $x\in H$, то $x\in K_{2+j}$, $j=1,2,\ldots,r$. K_1, $K_2,\ldots,K_t$, $t\geqslant 2+r$,— все классы, содержащие вещественные элементы (элемент вещественный, если он сопряжен с обратным). Рассмотрим групповую алгебру A группы G над полем рациональных чисел. Пусть Z — центр A. Если обозначить k_i сумму элементов из K_i, то $k_1,\ldots,k_k$ образуют базис Z. В частности,

$$k_2^2=\sum_{j=1}^{k}c_j k_j. \tag{17}$$

Здесь c_j означает число упорядоченных пар (x, y) элементов из K_2, таких, что xy равняется фиксированному элементу g_j из K_j Так как $x^2=y^2=1$, то из $xy=g_j$ вытекает $g_j^{-1}=yx=y^{-1}g_j x$. Обратно, если x имеет порядок 2 и $xg_jx^{-1}=g_j^{-1}$, то, обозначив $y=xg_j$, получаем $xy=g_j$ и $y^2=xg_jxg_j=g_j^{-1}g_j=1$. Итак, y имеет порядок 2, если $y\neq 1$. Но $y=1$ возможно, лишь, если $g_j^2=1$, т. е. если $j=2$. Следовательно:

г) Если g_j — представитель K_j, то для $j \neq 2$ число c_j означает число элементов x порядка 2, которые удовлетворяют уравнению

$$x^{-1}g_jx = g_j^{-1}.$$

Для $j = 2$ c_j меньше, чем число таких решений.

Если $j = 1$, то c_1 есть число элементов в K_2, т. е. $c_1 = n/2s$. Если $j = 2$, то в качестве g_j можно взять элемент τ. $c_2 + 1$ есть число элементов порядка 2, перестановочных с τ. Поэтому $c_2 + 1 = s + 1$ и $c_2 = s$. Так как для любого $x \neq 1$, τ из H равенство $y^{-1}xy = x^{-1}$ означает, что $y \in C$, то $c_j = s$ для $3 \leqslant j \leqslant 2 + r$. Если $2 + r < j \leqslant t$, то g_j и g_j^{-1} сопряжены. Поэтому существует точно $|C(g_j)|$ элементов x в G, таких, что $x^{-1}g_jx = g_j^{-1}$ и $[x^2, g_j] = 1$. Если $|x^2|$ делится на простой делитель числа $2s$, то $x^2 \in C$. Так как $j > 2+r$, то $x^2=1$. Таким образом, $c_j = |C(g_j)|$ для $2 + r < j \leqslant t$. Наконец, для $j > t$ элементы g_j и g_j^{-1} не сопряжены и $c_j = 0$.

Подсчитаем число слагаемых (элементов группы G) в обеих частях равенства (17)

$$(n/2s)^2 = \sum_{j=1}^{k} c_j n/|C(g_j)|.$$

Подставив значения c_j, получим

$$\frac{n^2}{4s^2} = \frac{n}{2s} + \frac{n}{2s}s + \sum_{j=3}^{r+2}\frac{n}{s}s + \sum_{j=r+3}^{t}\frac{n}{|C(g_j)|}|C(g_j)|.$$

Упрощаем

$$\frac{n^2}{4s^2} = \frac{n}{2s} + \frac{n}{2} + n(t-2).$$

Отсюда

$$t - 2 = (n - 2s - 2s^2)/4s^2. \tag{18}$$

Определим степени неприводимых представлений группы G. Рассмотрим сперва случай $\varepsilon = 1$. Согласно равенствам (16) $\delta_2 = 1$. Таблица (13) показывает теперь, что $\bar{\chi}_2 = \chi_2$. Если $f_2 = 1$, то G имеет линейный характер $\chi_2 \neq \chi_1$, $\chi_2^2 = \chi_1$ (см. (13)). Но тогда G/G' (G' — коммутант G) имеет четный порядок, что невозможно. Следовательно, $f_2 \neq 1$ и, ввиду сравнений (14), $f_2 \geqslant 2s + 1$. Из равенств (15) получаем $f \geqslant 2s + 2$. Нумерацией χ_3 и χ_4, если

необходимо, выводим из равенств (15), что $\delta_3 = 1$. В силу сравнений (14), $f_3 \geqslant s + 1$, $f_4 \geqslant s + \delta_4$, $f_j \geqslant 2s$ для $j \geqslant 5$. Итак,

$$f \geqslant 2s + 2,\ f_1 = 1,\ f_2 \geqslant 2s + 1,\ f_3 \geqslant s + 1,$$

(19) $$f_4 \geqslant s + \delta_4,\ f_j \geqslant 2s \text{ для } j \geqslant 5.$$

Группа G имеет r характеров $\chi^{(i)}$. Поэтому она имеет $k - r - 4 = k - s/2 - 3$ характеров χ_j с $j \geqslant 5$. Так как n есть сумма квадратов степеней неприводимых характеров, то

(20) $$n \geqslant (s/2 - 1)\ (2s + 2)^2 + 1 + (2s + 1)^2 + (s + 1)^2 + (s + \delta_4)^2 + (k - s/2 - 3)\ 4s^2.$$

В соответствии с равенством (18) n можно записать так:

$$n = 4s^2\ (t - 2) + 2s + 2s^2.$$

Подставляя это значение n в неравенство (20), получаем

(21) $$4s^2t \geqslant 4ks^2 + 2\delta_4 s - 2s.$$

Если $\delta_4 = 1$, то $t \geqslant k$. Так как $k \geqslant t$, то $k = t$. Поэтому в неравенствах (19) везде должен быть знак равенства. Если $\delta_4 = -1$, то также $k = t$. Но в этом случае левая часть неравенства (20) на $4s$ превосходит правую часть. Следовательно, хотя бы в одном случае в неравенствах (19) выполняется строгое неравенство. Если это неравенство записать в виде $f_j > f_j^*$, то сравнения (14) показывают, что $f_j \geqslant f_j^* + 2s$. Так как $f_j^2 \geqslant f_j^{*2} + 4sf_j^* + 4s^2$, то к правой части неравенства (20) можно добавить не менее $4sf_j^* + 4s^2$, что больше $4s$. Полученное противоречие показывает, что $\delta_4 = 1$. Итак, если $\varepsilon = 1$, то

$$n = 4s^2k - 6s^2 + 2s,\quad \delta_2 = \delta_3 = \delta_4 = 1,\quad f = 2s + 2,$$

(22) $$f_1 = 1,\quad f_2 = 2s + 1,\quad f_3 = f_4 = s + 1,\ f_j = 2s \text{ для } j \geqslant 5.$$

Рассмотрим случай $\varepsilon = -1$. В силу равенств (16) $\delta_2 = -1$. Поэтому

(16*) $$f_2 - 1 = f,\ f_3 - \delta_4 f_4 = f.$$

Пусть $\delta_4 = 1$. Из сравнений (14) вытекает, что $f \geqslant 2s - 2$ и $f_2 \geqslant 2s - 1$. Более того, $f_4 \geqslant s + 1$, и, применив равенства (16*), получаем $f_3 \geqslant 3s - 1$. Так же $f_j \geqslant 2s$ для $j \geqslant 5$. Итак,

(20*) $$n \geqslant (s/2 - 1)(2s - 2)^2 + 1 + (2s - 1)^2 + (3s - 1)^2 + (s + 1)^2 + (k - s/2 - 3)4s^2.$$

Подставляя сюда n из равенства (18), получаем

(21*) $$4s^2t \geqslant 4s^2k.$$

Отсюда $t = k$. Поэтому

$$f = 2s - 2, \quad f_1 = 1, \quad f_2 = 2s - 1, \quad f_3 = 3s - 1,$$
$$f_4 = s + 1, \quad f_j = 2s \quad \text{для } j \geqslant 5.$$

Предположим, что $\delta_4 = -1$. Тогда

$$f \geqslant 2s - 2, \quad f_2 \geqslant 2s - 1, \quad f_3 \geqslant s - 1,$$
$$f_4 \geqslant s - 1, \quad f_j \geqslant 2s \quad \text{для } j \geqslant 5.$$
$$n \geqslant (s/2 - 1)(2s - 2)^2 + 1 + (2s - 1)^2 + (s - 1)^2 +$$
$$+ (s - 1)^2 + (k - s/2 - 3)4s^2.$$

Отсюда получаем

(21**) $$4ts^2 \geqslant 4ks^2 - 8s^2.$$

Если одна из степеней f_i больше правой части f_i^* неравенства, в которое входит f_i, то $f_i \geqslant f_i^* + 2s$. Поэтому к правой части неравенства (21**) можно добавить не менее чем $4sf_i^* + 4s^2$. Если $i \geqslant 5$, то этот добавочный член равен $12s^2$, что невозможно. Если $1 \leqslant j \leqslant 4$, то строгое неравенство выполняется для двух значений j и опять получается противоречие. Наконец, если $f > f^*$, то добавочный член не меньше $(s/2 - 1)(4s(2s - 2) + 4s^2)$, что невозможно. Итак, в (21**) должно быть равенство. Поэтому $t = k - 2$. Применяя полученные результаты для $\varepsilon = -1$, приходим к следующему утверждению:

если $\varepsilon = -1$, то $\delta_2 = \delta_3 = -1$, $f = 2s - 2$,
$f_1 = 1$, $f_2 = 2s - 1$, $f_j = 2s$ для $j \geqslant 5$;

(23) 1) в случае $\delta_4 = 1$ $f_3 = 3s - 1$, $f_4 = s + 1$,
$k = t$ и $n = 4ks^2 - 6s^2 + 2s$;

2) в случае $\delta_4 = -1$ $f_3 = f_4 = s - 1$, $t = k - 1$,
$n = 4ks^2 - 14s^2 + 2s$.

Найдем порядок группы G. Как известно,

(24) $$c_j = \frac{n}{|C(\tau)|^2} \sum_{\mu=1}^{k} \frac{\varkappa^{(\mu)}(\tau)^2 \varkappa^{(\mu)}(g_j)}{\chi^{(\mu)}(1)},$$

где $g_j \in K_j$. Значения многих величин, входящих в равенство, известны: $|C(\tau)| = 2s$; если $g_j \in H$ и $g_j \neq 1$, τ, то $c_j = s$. Из таблицы (13) значений характеров находим $\chi^{(\mu)}(\tau) = \pm 2$ для $\mu = 1,2,\ldots,r$; $\chi_i(\tau) = \pm 1$ для $i = 1, 2, 3, 4$ и $\chi_j(\tau) = 0$ для $j \geqslant 5$. Пусть $\varepsilon = 1$ или $\varepsilon = -1$ и $\delta_4 = -1$. Тогда

$$s = \frac{n}{(2s)^2}\left[\sum_{\mu=1}^{r} \frac{4s\,(\xi_\mu(g_j) + \xi_{-\mu}(g_j))}{2s+2\varepsilon} + 1 + \frac{\varepsilon}{2s+\varepsilon} + 2\,\frac{-s}{s+\varepsilon}\right],$$

где элемент g_j таков, что группа $\{g_j\}$ содержит силовскую 2-подгруппу H. Так как $\sum_{i=-r}^{r+1} \xi_i(x) = 0$ для $x \neq 1$, то

$$\sum_{i=1}^{r} (\xi_i(x) + \xi_{-i}(x)) = -\xi_0(x) - \xi_{r+1}(x) = -1 + 1 = 0.$$

Поэтому из написанного выше равенства получаем

$$n = 2s\,(2s+\varepsilon)(s+\varepsilon). \tag{25}$$

Если $\varepsilon = -1$ и $\delta_4 = 1$, то

$$s = \frac{n}{(2s)^2}\left[\sum_{\mu=1}^{r} \frac{4\varepsilon\,(\xi_\mu(g_j) + \xi_{-\mu}(g_j))}{2s+2\varepsilon} + 1 + \frac{-1}{2s-1} + \frac{1}{3s-1} + \frac{-1}{s+1}\right].$$

Отсюда получаем

$$4s^2 = n\left(1 - \frac{1}{2s-1} + \frac{1}{3s-1} - \frac{1}{s+1}\right).$$

Поэтому

$$4 \equiv n\left(1 - 1 + \frac{1}{2} - \frac{1}{2}\right) \equiv 0 \pmod{s-1}.$$

Это невозможно, так как s — четное число и $s > 2$. Таким образом,

$$\delta_2 = \varepsilon, \quad \delta_3 = \varepsilon, \quad \delta_4 = \varepsilon. \tag{26}$$

Обозначим через d произвольный элемент, порядок которого делится на простой делитель числа $s + \varepsilon$, и через e — элемент, порядок которого делится на простой делитель числа $2s + \varepsilon$. Так как числа $2s$, $2s + \varepsilon$, $s + \varepsilon$ попарно взаимно просты, то из формулы (25) следует, что f_2 делится на порядок силовской p-подгруппы группы G, где p — простой делитель числа $2s + \varepsilon$. Следовательно,

$$\chi_2(e) = 0. \tag{27}$$

Аналогично получаем, что

$$\chi_3(d) = \chi_4(d) = 0. \tag{28}$$

Из равенств (15) вытекает, что $\chi^{(j)}(e) = \varepsilon$, $\chi^{(j)}(d) = 0$, $\chi_2(d) = -\varepsilon$. Ясно, что $d \neq e$. Итак, справедливо следующее предложение:

д) $|C(d)|$ делит $s + \varepsilon$, $|C(e)|$ делит $2s + \varepsilon$.

Применим формулу (24) для $g_j = d$:

$$c_j = \frac{n}{4s^2}\left(1 - \frac{\varepsilon}{2s+\varepsilon}\right) = \frac{s+\varepsilon}{2s} 2s = s + \varepsilon.$$

Так как $c_j \neq 0$, то класс K_j вещественный и

$$|C(d)| = s + \varepsilon. \tag{29}$$

Взяв $g_j = e$, получим

$$c_j = \frac{n}{4s^2}\left[\frac{4r}{2s+2\varepsilon}\chi^{(1)}(e) + \frac{1}{s+\varepsilon}(\chi_3(e) + \chi_4(e)) + 1\right].$$

Но

$$\chi_3(e) + \chi_4(e) = \chi^{(1)}(e).$$

Поэтому

$$c_j = \frac{n}{4s^2}\left(\frac{(s-2)\varepsilon + \varepsilon}{s+\varepsilon} + 1\right) = \frac{2s+\varepsilon}{2s} s(1+\varepsilon).$$

Следовательно, если $\varepsilon = 1$, то K_j — вещественный класс и

$$|C(e)| = 2s + 1.$$

Если $\varepsilon = -1$, то K_j — не вещественный класс. Так как существует лишь два невещественных класса ($k = t + 2$), то существует точно два класса, содержащих элементы типа e. Это означает, что $2s - 1$ есть степень простого числа. Последнее верно и в случае $\varepsilon = 1$. Действительно, из формул (22) и (25) для $\varepsilon = 1$ получаем

$$2sk - 3s + 1 = 2s^2 + 3s + s.$$

Следовательно, $k = s + 3$. Так как $r = 2 = s/2 + 1$ классов содержат элементы 1τ и h ($h \in H$), то $s/2 + 2$ классов содержат элементы d и e.

Соотношения ортогональности для χ_2 и χ_3 дают равенство

$$(2s + 1) + n/2s + r(n/s) - \sum_d 1 = 0.$$

Поэтому число элементов d равно

$$2s + 1 + (2s + 1)(s + 1)(1 + 2r) = (2s + 1)(1 + (s + 1)(s - 1)) = (2s + 1)s^2.$$

Из равенства (29) следует, что каждый класс K_j, содержащий элемент d, имеет $n \mid (s+1) = (2s+1)(2s)$ элементов. Поэтому существует $s/2$ классов, содержащих элементы d. Следовательно, существует точно два класса, содержащих элементы e. Как уже было отмечено, это возможно, когда $2s + \varepsilon$ есть степень простого числа,

$$2s + \varepsilon = p^m. \tag{30}$$

Для $\varepsilon = 1$ $| C(e) | = 2s + \varepsilon$. Покажем, что это верно для $\varepsilon = -1$. Так как $k = t + 2$, то существует два невещественных класса. Они содержат элементы типа e. Если e содержится в центре силовской p-подгруппы, то $| C(e) | = p^m = 2s + \varepsilon = 2s - 1$. Так как другой класс содержит e^{-1}, то $| C(e^{-1}) | = 2s - 1$. Следовательно, для любого ε

$$| C(e) | = 2s + \varepsilon. \tag{31}$$

е) Группа G имеет абелеву подгруппу D порядка $s + \varepsilon$. $C(d)$ каждого элемента d равен D.

Доказательство. Для каждого d $| C(d) | = s + \varepsilon$. Элементы из $C(d)$ снова имеют тип d. Каждый элемент из $C(d)$ вещественный. Если инволюция x действует на d так:

$$xdx = d^{-1},$$

то в силу $xcxd^{-1} = d^{-1}xcx$ и $C(d) = C(d^{-1})$ получаем, что

$$xC(d)x = C(d).$$

Но тогда x действует на $C(d)$ регулярно. Поэтому $C(d)$ — абелева группа. Обозначим $D = C(d)$. Ясно, что $D \cap y^{-1}Dy = \{1\}$ для любого $y \notin N(D)$. Положим $| N(D) | = w(s + \varepsilon)$, w делит $s + \varepsilon - 1$. Тогда

$$n = w(s + \varepsilon)(1 + N(s + \varepsilon)),$$

где N — целое число. Отсюда

$$2s(2s + \varepsilon) = w(1 + N(s + \varepsilon)).$$

Следовательно,

$$w \equiv 2s(2s + \varepsilon) \pmod{s + \varepsilon},$$

или

$$w \equiv -2\varepsilon(-\varepsilon) \equiv 2 \pmod{s + \varepsilon}.$$

Так как $w \leqslant s + \varepsilon - 1$, то $w = 2$. Итак,

$$|N(D)| = 2(s + \varepsilon). \tag{32}$$

ж) В частности, если d сопряжен с d^{μ}, то $d^{\mu} = d^{\pm 1}$.

Если $\varepsilon = 1$, то элемент e вещественный и можно так же показать, что $C(e) = E$ — абелева группа. Это же будет доказано и для $\varepsilon = -1$.

Пусть p — такое же простое число, как в равенстве (30), и пусть B — силовская p-подгруппа группы G. $|C(e)| = 2s + \varepsilon$. Следовательно, каждый элемент из B лежит в центре некоторой силовской p-подгруппы. Если B неабелева, то $R = B \cap x^{-1}Bx$ — наибольшее пересечение силовских p-подгрупп — отлично от $\{1\}$. Так как $C(e)$ — p-подгруппа, то силовские q-подгруппы из $N(R)$ при $q \neq p$ — циклические. Так как для любой подгруппы L из H или D ее нормализатор не имеет элементов типа e, то $N(R) = T \leftthreetimes U$, где T — силовская p-подгруппа $N(R)$. Это невозможно, так как R — максимальное пересечение силовских подгрупп. Следовательно,

з) Силовская p-подгруппа B порядка $2s + \varepsilon = p^m$ есть элементарная абелева группа.

Два элемента из B сопряжены в G тогда и только тогда, когда они сопряжены в $N(B)$. Так как $|C(e)| = 2s + \varepsilon$ для любого $e \in B$ и $e \neq 1$ и так как B содержит точно два класса сопряженных элементов, то

$$2\,|N(B) : B| = p^m - 1.$$

Следовательно,

$$|N(B)| = \frac{1}{p}\,p^m(p^m - 1) = \begin{cases} (2s+1)\,s & \text{для } \varepsilon = 1, \\ (2s-1)(s-1) & \text{для } \varepsilon = -1 \end{cases}$$

Завершим доказательство теоремы. Так как G имеет подгруппу $N(B)$ порядка $(2s + 1)s$ для $\varepsilon = 1$ и порядка $(2s - 1)(s - 1)$ для $\varepsilon = -1$, то G имеет транзитивное представление ρ подстановками на $2(s + 1)$ или $2s$ буквах соответственно. Пусть $\varepsilon = 1$. Вычитая из характера представления ρ главный характер, получаем характер степени $2s + 1$, не содержащий более единичного характера. Из равенств (22) следует, что этот характер неприводим и равен χ_2. Следовательно, характер представления ρ равен $\chi_1 + \chi_2$. Это означает, что группа $\rho(G)$ дважды транзитивна. Если $g \in G$, то $\chi_1(g) + \chi_2(g)$ означает число символов, которые ос-

таются неподвижными под действием $\rho(g)$. Как видно из таблицы (13), $\chi_1(g) + \chi_2(g) \leqslant 2$. Следовательно, ни один элемент группы $\rho(G)$ не оставляет на месте более двух символов.

Пусть $\varepsilon = -1$. Здесь характер представления ρ равен $\chi_1 + \chi$, где χ — характер степени $2s - 1$. Ввиду равенств (22*), $\chi = \chi_2$. Опять $\rho(G)$ дважды транзитивна, и ни один неединичный элемент $\rho(G)$ не оставляет на месте три различных символа.

Применяя метод Цассенхауза [72] (см. конец § 9), получаем, что

$$G \cong PSL(2,\ 2s + \varepsilon) \qquad (\varepsilon = \pm 1).$$

Теорема доказана.

§ 11. *ZT*-группы

Напомним, что *ZT-группой* называется отличная от группы Фробениуса дважды транзитивная группа подстановок нечетного числа символов, лишь тождественная подстановка которой оставляет на месте три различных символа. Цель настоящего параграфа — доказать, что *ZT*-группа изоморфна либо $PSL(2, q)$, где $q = 2^n$, либо $G(g)$ (см. § 1).

Пусть G — *ZT*-группа подстановок $1 + N$ символов. Фейт [21] доказал, что N есть степень 2. Обозначим через H подгруппу группы G, оставляющую на месте некоторый символ a. H есть группа Фробениуса. По теореме Фробениуса (см. § 3) $H = Q \leftthreetimes K$, где Q — инвариантный множитель порядка N и K — дополнительный множитель. K состоит из подстановок, которые оставляют на месте два символа a и еще b. Следующая лемма очевидна.

Лемма 1. 1) *Q — сильно изолирована в G*; 2) *Q — силовская 2-группа G*; 3) *K — циклическая группа и $N(K)$—группа диэдра, порожденная K и некоторой инволюцией τ.*

Доказательство. Так как G дважды транзитивна, то существует элемент τ, переводящий символ a в символ b и b в a. Поэтому некоторая степень τ есть инволюция π. Согласно 1) централизатор $C(\pi)$ инволюции π содержится в силовской 2-подгруппе группы G. Так как $\tau \in C(\pi)$, то τ содержится в силовской 2-подгруппе и оставляет на месте лишь один символ, скажем c. Элемент τ^2 оставляет на месте уже три символа a, b, c. Следовательно, $\tau^2 = 1$.

Пусть k — неединичный элемент K. Тогда

$$\tau k \tau(a) = \tau k(b) = \tau(b) = a$$

и подобно $\tau k\tau\,(b) = b$. Эти равенства означают, что $\tau \in N\,(K)$. Так как $C\,(\tau)$ — 2-группа, то для любого $k \in K$ $\tau k\tau = k^{-1}$. Поэтому K — циклическая группа. Если $\pi \in N\,(K)$, то $\pi^{-1}k\pi\,(a) = a$ или $k\pi\,(a) = \pi\,(a)$ и подобно $k\pi\,(b) = \pi\,(b)$. Но тогда либо $\pi \in K$, либо π содержит цикл (ab) и потому содержится в $\{K, \tau\}$.
Это означает справедливость равенства

$$\{K,\ \tau\} = N\,(K).$$

Лемма доказана.

Так как Q сильно изолирована в G, то

$$H \cap \tau H\tau = K \text{ и } Q \cap \tau H\,\tau = \{1\}. \tag{1}$$

Л е м м а 2. *Каждый элемент вне H можно однозначно записать в виде* $\eta\tau\pi$, *где* $\eta \in H$ и $\pi \in Q$.

Д о к а з а т е л ь с т в о. Предположим, что запись неоднозначна, т. е. $\eta\tau\pi = \eta'\tau\pi'$, где $\eta, \eta' \in H$ и $\pi, \pi' \in Q$. Тогда $\tau^{-1}\eta'^{-1}\,\eta\tau = \pi'\pi^{-1}$. Так как $Q \cap \tau H\tau = \{1\}$, то $\pi'\pi^{-1} = 1$ и $\pi = \pi'$, $\eta = \eta'$. Этим доказана единственность записи каждого элемента.

Существует точно hN элементов вида $\eta\tau\pi$, где $\eta \in H$, $\pi \in Q$ и $h = |\,H\,|$. Все эти элементы лежат вне H. Так как порядок G равен $h\,(1 + N)$, то существует точно hN различных элементов вне H. Следовательно, любой элемент вне H может быть однозначно записан в виде $\eta\tau\pi$.

Если $\sigma \in Q$, $\sigma \neq 1$, то $\tau\sigma\tau$ есть элемент из $\tau Q\tau$, лежащий вне H. Существуют поэтому такие $\eta \in H$ и $\pi \in Q$, что

$$\tau\sigma\tau = \eta\tau\pi. \tag{2}$$

Элемент $\pi \in Q$ есть функция от σ. Обозначим ее так:

$$\pi = f\,(\sigma). \tag{3}$$

Функция f определена на $Q \setminus \{1\}$ и принимает значения в $Q \setminus \setminus \{1\}$. Так как $H = Q \diagdown K$, то в силу равенств (2) и (3) можно записать η следующим образом:

$$\eta = g\,(\sigma)h\,(\sigma), \tag{4}$$

где $g\,(\sigma) \in Q$, $h\,(\sigma) \in K$.

Л е м м а 3. *Функции f, g и h удовлетворяют следующим условиям*:

$$f\,(f\,(\sigma)) = \sigma; \tag{5}$$

$$g\,(\sigma) = f\,(\sigma^{-1})^{-1}; \tag{6}$$

(7) $$f(k^{-1}\sigma k) = kf(\sigma)x^{-1};$$

(8) $$h(k^{-1}\sigma k) = k^2 h(\sigma);$$

(9) $$f(g(\sigma)) = h(\sigma)^{-1} f(\sigma)^{-1} h(\sigma);$$

(10) $$f(\sigma\rho) = h(\rho) f(\pi) h(\rho)^{-1} f(\rho),$$

где $\sigma, \rho \in Q, \sigma\rho \neq 1, k \in K, \pi = f(\sigma)\, g(\rho)$.

Доказательство. Из равенств (2), (3) и (4) получаем

(11) $$\tau\sigma\tau = g(\sigma)\ h(\sigma)\tau f(\sigma).$$

Отсюда

$$\tau f(\sigma)\tau = h(\sigma)^{-1} g(\sigma)^{-1}\tau\sigma.$$

Элемент $h(\sigma)^{-1}g(\sigma)^{-1}$ принадлежит H. Согласно определению (3) $f(f(\sigma)) = \sigma$.

$$\tau\sigma^{-1}\tau = f(\sigma)^{-1}\tau h(\sigma)^{-1} g(\sigma)^{-1} = f(\sigma)^{-1} h(\sigma)\tau g(\sigma)^{-1}.$$

Итак, $g(\sigma)^{-1} = f(\sigma^{-1})$ или $g(\sigma) = f(\sigma^{-1})^{-1}$.

$$\tau^{-1}(k^{-1}\sigma k)\tau = k\tau\sigma\tau k^{-1} = kg(\sigma)h(\sigma)\tau f(\sigma)k^{-1} =$$

$$= kg(\sigma)k^{-1}k^2 h(\sigma)\tau kf(\sigma)k^{-1}.$$

Так как $kf(\sigma)k^{-1}$ и $kg(\sigma)k^{-1} \in Q$, $k^2 h(\sigma) \in K$, то условия (7) и (8) доказаны.

$$\tau g(\sigma)\tau = \sigma\tau f(\sigma)^{-1} h(\sigma) = \sigma h(\sigma)^{-1}\tau h(\sigma)^{-1} f(\sigma)^{-1} h(\sigma).$$

Поэтому свойство (9) доказано. Если $\sigma\rho \neq 1$, то

$\tau(\sigma\rho)\tau = \tau\sigma\tau\tau\rho\tau =$

$$= g(\sigma)h(\sigma)\tau f(\sigma)g(\rho)h(\rho)\tau f(\rho) = g(\sigma)h(\sigma)\tau\pi\tau h(\rho)^{-1} f(\rho) =$$

$$= g(\sigma)h(\sigma)g(\pi)h(\pi)\tau f(\pi)h(\rho)^{-1} f(\rho) = \eta\tau h(\rho) f(\pi) h(\rho)^{-1} f(\rho),$$

где $\eta \in H$ и $\pi = f(\sigma)g(\rho)$. Лемма доказана.

Рассмотрим некоторые свойства инволюций группы G.

Лемма 4. *Элемент* $\eta\tau\pi$ *есть инволюция тогда и только тогда, когда* $\pi\eta \in K$.

Доказательство. Если $\eta\tau\pi$ — инволюция, то $\eta\tau\pi\eta\tau\pi = 1$ или $\tau\pi\eta\tau = \eta^{-1}\pi^{-1}$.

Так как $H \cap \tau H \tau = K$, то $\pi\eta \in K$. С другой стороны, если $\pi\eta \in K$, то $\pi\eta = k^{-2}$ для некоторого $k \in K$. Тогда

$$\eta\tau\pi = \pi^{-1}k^{-2}\tau\pi = \pi^{-1}k^{-1}\tau k\pi.$$

Лемма доказана.

Как только что доказано, любая инволюция вне H сопряжена с τ.

Л е м м а 5. *Каждая инволюция из G сопряжена с τ. Если σ — инволюция из Q, то σ лежит в $Z(Q)$ и любая другая инволюция из Q имеет вид $k^{-1}\sigma k$, где $k \in K$. Порядок K совпадает с числом инволюций Q.*

Д о к а з а т е л ь с т в о. $C(\sigma) = Q$. Если $\sigma' \in Q$ и $\sigma'^2 = 1$, то из равенства $Q \cap x^{-1}Qx = \{1\}$ и сопряженности инволюций следует, что $\sigma' \in Z(Q)$ и σ' сопряжена с σ в $N(Q)$. Поэтому существует $k \in K$, такое, что $\sigma' = k^{-1}\sigma k$. Так как $H = Q \leftthreetimes K$ — группа Фробениуса, то $|K|$ совпадает с числом инволюций Q.

Л е м м а 6. *Q содержит два элемента σ и ρ таких, что $\sigma^2 = 1$ и $\tau\sigma\tau = \rho^{-1}\tau\rho$.*

Д о к а з а т е л ь с т в о. Для любого элемента $\pi \neq 1$ из Q справедливо равенство

$$\tau\pi\tau = g(\pi)\,h(\pi)\tau\,f(\pi).$$

Если π — инволюция, то согласно лемме 4 $f(\pi)g(\pi)h(\pi) \in K$. Это означает, что $f(\pi) = g(\pi)^{-1}$. Так как $h(\pi) \in K$, то $h(\pi) = k^{-2}$ для некоторого k из K. Применяя свойство (8), получаем

$$\tau k^{-1}\pi k\tau = f(k^{-1}\pi k)^{-1}h(k^{-1}\pi k)\tau f(k^{-1}\pi k) = f(\sigma)^{-1}h(\pi)k^2\tau\, f(\sigma),$$

где $\sigma = k^{-1}\pi k$. Так как $h(\pi)k^2 = 1$, то σ и $\rho = f(\sigma)$ удовлетворяют всем требованиям.

В дальнейшем предполагается, что σ и ρ удовлетворяют требованиям леммы 6.

Л е м м а 7. *Элементы σ и ρ однозначно определены выбором H, K и τ.*

Д о к а з а т е л ь с т в о. Если σ' — инволюция из Q, то $\sigma' = k^{-1}\sigma k$, где $k \in K$ (см. лемму 5). Поэтому

$$\tau\sigma'\tau = \tau k^{-1}\sigma k\tau = k\rho^{-1}k^{-1}k^2\tau k\rho k^{-1}.$$

Если существует такой элемент ρ' из Q, что $\tau\sigma'\tau = \rho'^{-1}\tau\rho'$, то $k^2 = 1$. Следовательно, $\sigma' = \sigma$ и $\rho = \rho'$.

Л е м м а 8. *Если $\pi = \sigma\tau$, то $\rho^{-1}\pi\,\rho = \pi^2$.*

Действительно, из $\sigma\tau\sigma\tau = \sigma\rho^{-1}\tau\rho$ (см. лемму 6) и $\sigma \in Z(Q)$ (лемма 5) следует, что $\sigma\tau\sigma\tau = \rho^{-1}\sigma\tau\rho$.

Лемма 9. *Инволюция* σ *есть степень* ρ.

Доказательство. Положим $U = \{\pi\}$, $\pi = \sigma\tau$. Так как $\sigma\pi\sigma = \pi^{-1}$, то $\sigma \in N(U)$. В силу предыдущей леммы $\rho^{-1}\pi\rho = \pi^2$. Так как $\pi \notin Q$, то $C(U) \cap Q = \{1\}$. Поэтому $N(U) \cap Q$ изоморфна некоторой подгруппе группы $N(U) / C(U)$, которая из-за цикличности U абелева. С другой стороны, ни один неединичный элемент из $N(U) \cap Q$ не перестановочен с неединичным элементом из U. Следовательно, $N(U) \cap Q$ — циклическая группа. Но тогда σ — единственная инволюция в $N(U) \cap Q$. Она является степенью любого неединичного элемента из $N(U) \cap Q$.

Замечание 10. Теорема Хигмена, сформулированная в § 1, утверждает, что если группа Q неабелева, то $\rho^2 = \sigma$, так как все элементы из Q имеют порядок не более 4.

Рассмотрим теперь свойства строго вещественных элементов группы G. Напомним, что элемент строго вещественный, если он есть произведение двух инволюций.

Лемма 11. *Каждый неединичный строго вещественный элемент — либо инволюция, либо сопряжен с* $\pi\tau$, *где* π — *некоторая инволюция из* Q. *Если* π, π' — *инволюции из* Q, *то* $\pi\tau$ *и* $\pi'\tau$ *сопряжены тогда и только тогда, когда* $\pi = \pi'$.

Доказательство. Пусть α — строго вещественный элемент. По определению, α — произведение двух инволюций τ' и τ''. Предположим, что H' и H'' — подгруппы, сопряженные с H и содержащие τ' и τ'' соответственно. Если $H' = H''$, то $\tau'\tau'' \in H'$. В этом случае α — инволюция. Предположим, что $H' \neq H''$. Инволюция τ содержится в некоторой подгруппе H_1, сопряженной с H. Пересечение $H \cap H_1$ сопряжено с K и переставляет транзитивно инволюции из H_1. Так как G дважды транзитивна, то существует элемент, который переводит H' в H и H'' в H_1. Следовательно, α сопряжен произведению двух инволюций, одна из которых содержится в H, а другая — в H_1. Полученный элемент можно трансформировать элементами из $H \cap H_1$ в элемент вида $\pi\tau$, где π — инволюция из Q.

Пусть π и π' — инволюции из Q. Если $x^{-1}\pi\tau x = \pi'\tau$, то группы диэдра $\{x^{-1}\pi x,\ x^{-1}\tau x\}$ и $\{\pi',\ \tau\}$ совпадают и имеют порядок $2l$, где l — нечетное число (см. лемму 1). Элементы $x^{-1}\tau x$ и τ сопряжены некоторой степенью элемента $\pi'\tau$. Поэтому $x^{-1}\pi\tau x = \pi'\tau = y^{-1}\pi'\tau y$ или $\pi'\tau = yx^{-1}\pi\tau xy^{-1}$. Так как $xy^{-1} \in C(\tau)$, то $yx^{-1}\pi xy^{-1}\tau =$

$= \pi'\tau$. В силу леммы 1 $xy^{-1} \in H$. Так как H и $C(\tau)$ имеют единичное пересечение, то $xy^{-1} = 1$. Отсюда следует, что $\pi = \pi'$.

Лемма 12. *Пусть* π — *строго вещественный элемент, такой, что* $\pi^2 \neq 1$. *Тогда* $A = C(\pi)$ — *абелева группа. Если* π' — *неединичный элемент из* A, *то* π' — *строго вещественный элемент и* $C(\pi^1) = A$. *Группа* $N(A)/A$ — 2-*группа.*

Доказательство. Так как π — строго вещественный элемент, то $\pi = \alpha\beta$, где α и β — инволюции. Ясно, что $\alpha\pi\alpha = \pi^{-1}$. Поэтому $\alpha \in N(A)$. В силу леммы 1 $C(\alpha)$ — 2-группа. По условию $\pi^2 \neq 1$. Так как $|K|$ — нечетное число, то из леммы 1 следует, что элемент из Q является вещественным тогда и только тогда, когда его порядок равен 2. Поэтому порядок π — нечетное число. $|C(\pi)|$ — также нечетное число. Так как $A = C(\pi)$ инвариантна относительно α, то $\alpha\omega\alpha = \omega^{-1}$ для любого $\omega \in A$. Но тогда A — абелева группа. Ясно, что A совпадает с централизатором любого своего неединичного элемента. Группа $N(A)/A$ имеет четный порядок. Каждый элемент из $N(A) \diagup A$ индуцирует в A регулярный автоморфизм. Так как $C(\alpha)$ — 2-группа, то из $Q \cap x^{-1}Qx = \{1\}$ следует, что $N(A)/A$ — 2-группа. Лемма доказана.

В группе $PSL(2,2^n)$ элемент $\pi = \sigma\tau$ имеет порядок 3 и поэтому $\sigma = \rho$. Докажем обратное утверждение.

Теорема 13. *Если* $\sigma = \rho$, *то* $G \cong PSL(2,2^n)$.

Доказательство. По предположению верно равенство $\tau\sigma\tau = \sigma\tau\sigma$. Если σ' — произвольная инволюция из Q, то существует такой элемент $k \in K$, что $\sigma' = k^{-1}\sigma k$ (см. лемму 5). Положим $\sigma'' = k\sigma k^{-1}$. Тогда σ'' — инволюция, отличная от σ', и

$$\tau\sigma'\tau = \tau k^{-1}\sigma k\tau = k\tau\sigma\tau k^{-1} = \sigma'' k^2 \tau\sigma''. \tag{12}$$

Обозначим через G_0 совокупность элементов вида $\sigma' k$ или $\sigma' k\tau\sigma''$, где σ', σ'' — либо 1, либо инволюции из Q и $k \in K$. Покажем, что G_0 — группа. Действительно,

$$(\sigma' k)(\sigma'' k') = (\sigma' k\sigma'' k^{-1})(kk');$$

здесь $\sigma' k\sigma'' k^{-1}$ — инволюция из Q (см. 1) и $kk' \in K$. Пусть теперь оба элемента имеют вид $\sigma' k\tau\sigma''$. Рассмотрим $\pi = \sigma_1 k_1 \tau\sigma_2\sigma_3 k_2\tau\sigma_4$; здесь σ_i может быть 1. Если $\sigma_2\sigma_3 = 1$, то выражение для π можно сократить, $\pi = \sigma_1 k_1 k_2^{-1}\sigma_4$. В этом случае π можно записать в виде $\sigma' k$ или k. Если $\sigma_2\sigma_3 = \sigma'$ — инволюция, то согласно равенству (12)

$$\pi = \sigma_1 k_1 \tau\sigma'\tau k_2^{-1}\sigma_4 = \sigma_1 k_1\sigma'' k'\tau\sigma'' k_2^{-1}\sigma_4.$$

Используя формулу $\tau k\tau = k^{-1}$, последнее выражение преобразуем к виду $\sigma_5 k\tau\sigma_6$ с $\sigma_i \in Q$, $\sigma_i^2 = 1$.

Точно так же показывается, что произведение элементов вида $\sigma' k$ и $\sigma'' k\tau\sigma'''$ имеет такой же вид. Итак, G_0 — группа.

Если $q - 1$ — число инволюций в Q, то G_0 содержит точно $q(q^2 - 1)$ элементов. Совокупность элементов вида σk есть подгруппа H_0 группы G_0. $|G_0 : H_0| = 1 + q$. H_0 содержит K, и инволюции из H_0 порождают абелеву подгруппу порядка q. Группу G_0 можно транзитивно представить подстановками смежных классов по H_0. Это представление трижды транзитивно. Цассенхауз [71] показал, что $G_0 \cong PSL(2, q)$ (см. конец § 9). Группа $PSL(2, q)$ содержит для четного q циклическую подгруппу порядка $1 + q$. Обозначим через V циклическую подгруппу этого порядка из группы G_0. $N_{G_0}(V)$ — группа диэдра порядка $2(1 + q)$. Согласно лемме 11 каждый строго вещественный элемент из G сопряжен с некоторым элементом из G_0. Следовательно, порядок строго вещественного элемента π делит числа 2, $q - 1$ или $q + 1$. Если порядок π делит $q - 1$, то π сопряжен с элементом из K. Если порядок делит $q + 1$, то π сопряжен с элементом из V. В силу леммы 1 неединичные элементы из K распадаются на $(q-2)/2$ классов. Так как существует точно q классов неединичных вещественных элементов (см. лемму 11), то V содержит точно $q/2$ классов. Следовательно, элементы v и v' из V сопряжены в G тогда и только тогда, когда $v' = v^{\pm 1}$. Положим $W = C_G(V)$. Так как V — циклическая группа, состоящая из строго вещественных элементов, то из леммы 12 следует абелевость W. Из этой же леммы вытекает, что каждый неединичный элемент $\omega \in W$ строго вещественный и что $C_G(\omega) = W$. Если порядок ω делит $q - 1$, то ω сопряжен с элементом из K. Но тогда $|C_G(\omega)| = q - 1$. Это невозможно. Следовательно, $|\omega|$ делит $q + 1$ и ω сопряжен с некоторым элементом из V.

Предположим, что $D = V \cap V' \neq \{1\}$ для $V' = \alpha^{-1} V \alpha$. Группа $\alpha^{-1} D \alpha$ есть подгруппа V' и $|\alpha^{-1} D_\alpha| = |D|$. Так как V' — циклическая группа, то $\alpha^{-1} D \alpha = D$. Если $D = \{\beta\}$, то $\alpha^{-1}\beta\alpha = \beta^{\pm 1}$. Так как силовская 2-подгруппа сильно изолирована, то $\alpha^{-1}\beta\alpha = \beta^{-1}$. В силу леммы 12 $N_G(W)/W$ — 2-группа. В этом случае $N_G(W)$ — группа Фробениуса и $\alpha^2 = 1$. Но тогда $V = V'$. Предположим, что $W \neq V$. Так как каждый элемент из W сопряжен с некоторым элементом из V, то существует сопряженная подгруппа $V' \neq V$, содержащаяся в W. $V \cap V' = \{1\}$.

Предположим, что $q+1$ — не простое число. Пусть p — простой делитель $q+1$. Возьмем в V' элемент δ простого порядка p. Положим $V=\{\varepsilon\}$. Так как V и V' содержатся в абелевой подгруппе W, то $\delta\varepsilon=\varepsilon\delta$. Равенство $(\delta\varepsilon)^p=\varepsilon^p$ означает, что $V''=\{\delta\varepsilon\}$ имеет порядок $q+1$ и $V''\cap V\neq\{1\}$, $V''\neq V$. Это невозможно. Итак, $q+1$ — простое число p. Поэтому $|W|$ — степень p. Положим $w=|W|$, $l=|N(W):W|$. Элементы из W распределяются на $w-1/l$ классов. С другой стороны, существует точно $q/2$ классов порядка p. Следовательно,

$$w-1=lq/2.$$

Так как $w-1$ есть p^n-1, а $lq/2$ — степень 2, то

$$(p^n-1)/(p-1)=1+p+\ldots+p^{n-1}$$

есть степень 2, $n=2m$ — четное число. Тогда $p^n-1=(p^m-1)\cdot(p^m+1)$ — степень 2. Так как $(p^m-1, p^m+1)=2$, то $p^m-1=2$. Следовательно, $p=3$ и $q=2$. В этом случае G — группа Фробениуса, что противоречит определению ZT-группы. Следовательно, $W=C(V)=V$.

Сосчитаем число элементов в группе G. Подгруппы, сопряженные с Q, содержат N^2 элементов $N=qt$, где t — целое число. Подгруппы, сопряженные с K, содержат $N(N+1)(q-2)/2$ неединичных элементов. Так как $|N(V):V|=2$, то существует $N(N+1)(q-1)/2(q+1)$ подгрупп, сопряженных с V. Если $g=|G|$, то

$$g\geqslant N^2+N(N+1)(q-2)/2+N(N+1)(q^2-q)/2(q+1).$$

Разделим на g и используем равенство

$$g=N(N+1)(q-1).$$

Получаем

$$q+1>N=tq,$$

что означает $t=1$ и $N=q$. Итак, $|G_0|=|G|$ и $G_0=G$. Теорема доказана.

Теорема 14. *Если число $q-1$ инволюций в силовской 2-подгруппе Q ZT-группы G делится на 3, то $G\cong PSL(2, q)$.*

Доказательство. Группа K — циклическая группа порядка $q-1$. По предположению K содержит элемент α порядка 3. В силу леммы 1 α — строго вещественный элемент. Поэтому существует такая инволюция $\pi\in Q$, что $(\pi\tau)^3=1$. Нетрудно

видеть, что

$$\tau\pi\tau = \pi\tau\pi.$$

Так как π удовлетворяет уравнению из леммы 6, то в силу леммы 7 $\pi = \sigma = \rho$. Из предыдущей теоремы вытекает, что $G \cong PSL(2, q)$.

Теорема 15. *Если $q - 1$ — число инволюций силовской 2-подгруппы, то порядок группы G есть либо $q(q^2 - 1)$, либо $q^2(q - 1)(q^2 + 1)$.*

Доказательство. Если силовская 2-подгруппа Q абелева, то G изоморфна $PSL(2, q)$ (см. В. Фейт [21]). В этом случае $|G| = q(q^2 - 1)$. Это утверждение можно доказать аналогично теореме 13 и теореме 1 из § 10.

Предположим, что Q — неабелева группа. В силу леммы 5 Q допускает циклическую группу автоморфизмов, транзитивную на множестве инволюций. По теореме Хигмена (см. § 1), $|Q| = q^2$ или q^3. Докажем, что $|Q| = q^2$. Согласно лемме 6

$$\tau\sigma\tau = \rho^{-1}\tau\rho.$$

По теореме Хигмена (§ 1), $\rho^4 = 1$. Так как σ есть степень ρ и Q неабелева, то $\rho^2 = \sigma$. Положим $\pi = \sigma\tau$. Применив лемму 8, получим

$$\pi^{-1} = \sigma^{-1}\pi\sigma = \rho^{-2}\pi\rho^2 = \pi^4 \text{ или } \pi^5 = 1.$$

Поэтому $|G|$ делится на 5.

$$|G| = q^n(q - 1)(q^n + 1),$$

где $n = 2$ или 3. По теореме 14 $q - 1$ не делится на 3. Следовательно, q не является квадратом. Это означает, что $q - 1$ не делится на 5. Поэтому на 5 делится $q^n + 1$. Теперь нетрудно установить, что q^n — квадрат. Теорема доказана.

Следствие 16. *Силовская 2-подгруппа Q группы G — либо элементарная абелева группа, либо изоморфна группе $S(q; x)$, где q — нечетная степень 2.*

Следствие 17. *Если π — такой строго вещественный элемент, что $\pi^2 \neq 1$, то $A = C(\pi)$ — абелева группа, все неединичные элементы которой строго вещественные. $N(A)/A$ — циклическая группа порядка $\leqslant 4$.*

Следствие 17 вытекает из следствия 16, леммы 12 и леммы 3 из § 7.

Напомним, что элемент π называется вещественным, если π сопряжен с π^{-1}. Строго вещественный элемент является вещественным. В ZT-группе всякий вещественный элемент — строго вещественный. В самом деле, пусть π — вещественный элемент. Если π — инволюция, то π является строго вещественным, так как силовская 2-подгруппа Q группы G имеет более одной инволюции. Предположим, что $\pi^2 \neq 1$. Если $|\pi|$ — четное число, то $\pi^4 = 1$, и в силу леммы 1 π — невещественный элемент. Поэтому $|\pi|$ — нечетное число. По предположению существует такой элемент α из G, что $\alpha^{-1}\pi\alpha = \pi^{-1}$. Так как $[\alpha^2, \pi] = 1$, то в силу леммы 1 $\alpha^2 = 1$. Это означает, что π — строго вещественный элемент.

Найдем абелевы подгруппы группы G. Для этого опишем классы вещественных элементов группы G. Выберем из каждого класса централизаторов вещественных элементов, не являющихся инволюциями, по одному централизатору. Пусть они следующие: $A_0 = K$, $A_1, \ldots, A_s$. Положим $n_i = |A_i|$ и $l_i = |N(A_i) : A_i|$. Согласно лемме 12 все A_i — холловские подгруппы G. Группа A_i содержит точно $(n_i - 1)/l_i$ классов вещественных элементов. В силу леммы 11 существует точно $q - 1$ класс вещественных элементов, не являющихся инволюциями. Поэтому

$$q - 1 = \sum_{i=0}^{s} (n_i - 1)/l_i. \tag{13}$$

Если π — неединичный и невещественный элемент нечетного порядка, то $C(\pi)$ не содержит вещественных элементов (см. лемму 12). Следовательно, $C(\pi)$ и $2n_0n_1\ldots n_s$ взаимно просты. Подсчитаем число g элементов группы G

$$g = 1 + (q^2 - 1)(q^2 + 1) + \sum_{i=0}^{s} (n_i - 1)\, g/n_i l_i + d, \tag{14}$$

где d — число невещественных неединичных элементов группы G. Число d делится на $q^2 n_0 \ldots n_s$. Числа l_i равны либо 2, либо 4. Предположим, что u чисел из l_i равны 2, и положим $v = s - u + 1$. Так как $l_0 = 2$, то $u \neq 0$. Если $i > 0$, то n_i делит $q^2 + 1$. Следовательно, при $i > 0$ n_i не делится на 3. Поэтому для всех i верно неравенство

$$(n_i - 1)/n_i \geqslant 4/5.$$

Разделив обе части равенства (14) на g и использовав это неравенство, получим $4 \geqslant 2u + v$. Так как $u \geqslant 1$ и $v \geqslant 0$, то возможны следующие 4 случая: $u = 2$ и $v = 0$; $u = 1$ и $v = 0,1,2$.

Предположим, что $u = 2$ и $v = 0$. Тогда $s = 1$ и равенство (13) принимает вид

$$q - 1 = (q - 2)/2 + (n_1 - 1)/2.$$

Отсюда $q = n_1 - 1$. По теореме 14 $q \not\equiv 1 \pmod 3$. Но тогда $n_1 = q + 1 \equiv 0 \pmod 3$, что невозможно. Следовательно, $u = 1$. Если $v = 0$, то из равенства (14) получаем $q = 0$, что невозможно. Если $v = 1$, то $s = 1$ и из равенства (13) следует, что $n_1 = 2q + 1$. Так как n_1 делит $q^2 + 1$, то $q^2 + 1 = k(2q + 1)$ для целого k. Отсюда $k \equiv 1 \pmod q$. Если $k > 1$, то $k \geqslant q + 1$ и

$$q^2 + 1 = k(2q + 1) \geqslant (q + 1)(2q + 1) > q^2 + 1.$$

Это невозможно. Если же $k = 1$, то $q = 2$, что также невозможно. Поэтому $v = 2$. Перепишем уравнение (13) следующим образом:

$$n_1 + n_2 = 2(q + 1). \tag{15}$$

Упростим равенство (14)

$$(q + 1)/2n_1/n_2 = (q + 1)/2(q^2 + 1) + cn_1n_2/(q^2 + 1), \tag{16}$$

где $d = cq^2(q - 1)n_1n_2$. Из этого равенства получаем, что c делится на $q + 1$. Из него же следует, что

$$(q + 1)/2 > c\,(n_1n_2)^2/(q^2 + 1).$$

Если $c > 0$, то $c \geqslant q + 1$. В силу равенства (15) $n_1n_2 \geqslant q + 1$. Теперь видим, что

$$(q + 1)/2 > (q + 1)^2n_1n_2/(q^2 + 1) > n_1n_2 \geqslant q + 1.$$

Это невозможно. Поэтому $c = 0$. Из равенства (16) следует, что

$$n_1n_2 = q^2 + 1. \tag{17}$$

Система уравнений (15) и (17) имеет единственное решение $n_1 = q + r + 1$ и $n_2 = q - r + 1$, где $2q = r^2$. Равенство $c = 0$ означает, что все элементы нечетного порядка вещественны. Таким образом, доказано следующее предложение.

Т е о р е м а 18. *Если порядок ZT-группы G равен $q^2(q - 1) \times (q^2 + 1)$, то G содержит абелевы подгруппы $A_0 = K, A_1, A_2$ порядков $q - 1$, $q + r + 1$, $q - r + 1$ $(r^2 = 2q)$ соответственно.*

Если π — *неединичный элемент из* A_i, *то* $C(\pi) = A_i$. *Более того,*

$$|N(A_1) : A_i| = |N(A_2) : A_2| = 4.$$

Следствие 19. *ZT-группа G расщепляема.*

Следствие получается применением к теореме 18 леммы 1 и теоремы 15.

М. Сузуки [58] из теоремы 18 с использованием результатов статьи Брауэра и Фаулера [17] получил следующую

Лемму 20. *ZT-группа G порядка* $q^2(q-1)(q^2+1)$ *имеет точно два класса сопряженных элементов порядка* 4.

Для доказательства леммы достаточно знать число неприводимых характеров группы G. Нетрудно убедиться, что если неприводимый характер группы G не является исключительным ни для одной из подгрупп A_0, A_1, A_2, то он единичный характер. Степени и число неединичных неприводимых характеров теперь можно получить, используя метод предыдущего параграфа.

Теорема 21. *Если силовская 2-подгруппа Q ZT-группы G неабелева, то Q изоморфна* $S(q, \theta)$, *где* θ — *автоморфизм поля из q элементов, удовлетворяющий условию* $\theta^2 = 2$.

Следствие 16 утверждает, что $Q \cong S(q; \theta)$ для некоторого θ. Осталось показать, что $\theta^2 = 2$. Согласно лемме 20 и лемме 12 из § 7 отображение $\alpha \to \alpha^{\theta-1}$ есть эпиморфизм поля из q элементов.

В лемме 7 говорится, что заданием H, K и τ элементы σ и ρ, удовлетворяющие соотношению $\tau\sigma\tau = \rho^{-1}\tau\rho$, определены однозначно. Так как все инволюции из H сопряжены с помощью элементов из K, то можно считать, что при изоморфизме $Q \to S(q;\theta)$ элементу σ соответствует пара (0,1), которую будем обозначать снова σ.

Лемма 22. *В качестве элемента* ρ *можно выбрать* (1,0).

Доказательство. Так как $\rho^2 = \sigma$, то $\rho = (1,\gamma)$ для некоторого γ. Вычислим $\pi(k)$ для $k \neq 1$ (см. § 7)

$$\pi(k) = (1+k,\ k^\theta + \gamma + k^{1+\theta}(1+\gamma)).$$

Так как $\pi(k)$ не сопряжен с $\rho^{-1} = (1,1+\gamma)$ с помощью элементов из K (см. § 7, лемму 13), то

$$(1+k)^{1+\theta}(1+\gamma) \neq k^\theta + \gamma + k^{1+\theta}(1+\gamma)$$

Предположим, что $\gamma \neq 0$. Тогда неравенство упрощается так

$$\gamma^{-1} + 1 \neq (1 + k)^{\theta-1}.$$

Так как $\alpha \to \alpha^{\theta-1}$ — эпиморфизм, то $(1 + k)^{\theta-1}$ не равняется лишь 0 и 1. Следовательно,

$$1 + \gamma^{-1} = 0 \text{ или } 1.$$

Так как $\gamma^{-1} \neq 0$, то $\gamma = 1$. Поэтому ρ — либо (1,0), либо (1,1). Так как $M(q; \theta) \cong M(q; \theta^{-1})$ (см. лемму 11, § 7), то, выбрав вместо θ автоморфизм θ^{-1} (если необходимо), получим, что $\rho = (1,0)$. Лемма доказана.

Если $\pi = (\alpha, \beta) \neq 1$ — элемент из Q, то $f(\pi)$ можно вычислить, пользуясь формулой (3) и леммой 3. Пусть $f(\pi) = (\alpha', \beta')$. Тогда α' и β' — функции от α и β. Найдем вид этих функций. Для простоты вместо $f(\pi)$ будем писать $f(\alpha, \beta)$.

Л е м м а 23. *Функция f определена следующим образом*:

$$\begin{aligned} f(0, \alpha^{1+\theta}) &= (\alpha^{-1}, 0), \\ f(\alpha, 0) &= (0, \alpha^{-(1+\theta)}), \\ f(\alpha, \alpha^{1+\theta}) &= (\alpha^{-1}, \alpha^{-(1+\theta)}). \end{aligned} \tag{18}$$

Если α и $\beta \neq 0$, $\beta \neq \alpha^{1+\theta}$, то

$$f(\alpha, \beta) = (c(k)/\alpha, \ c(k)/\beta), \tag{19}$$

где $k^\theta = \beta/(\beta + \alpha^{1+\theta})$, $c(k) = (1 + k)(k^{-1} + \lambda^{-1})$ и λ определяется из равенства

$$k^{1+\theta} + k^{2(1+\theta)} = \lambda^{1+\theta}. \tag{20}$$

Д о к а з а т е л ь с т в о. Формулы (18) получаются из леммы 6 и равенства (7). Пусть $(\alpha, \beta) \in Q$ и $\alpha \neq 0$, $\beta \neq 0$, $\beta \neq \alpha^{1+\theta}$. Тогда (α, β) сопряжен с $\pi(k)$ для $k \in K$ (см. лемму 13, § 7). Так как

$$\pi(k) = (1 + k, \ k^\theta + k^{1+\theta}),$$

то

$$(\alpha, \ \beta) = (\eta(1 + k), \ \eta^{1+\theta}(k^\theta + k^{1+\theta}))$$

для некоторого η. Положим $\omega = \theta^{-1}$. Тогда

$$\eta = \alpha + (\beta/\alpha)^\omega, \ k = \beta^\omega/(\alpha^{1+\omega} + \beta^\omega).$$

Заметим, что $\alpha^{1+\theta} + \beta^\omega \neq 0$, так как $\beta \neq \alpha^{1+\theta}$. Аналогично $\eta \neq 0$ и $k \neq 0,1$. Из определения f (см. равенство (3)) получаем

$$f(\pi(k)) = \lambda\rho\lambda^{-1}k\rho^{-1}k^{-1},$$

где λ определяется из равенства (20).

$$f(\pi(k)) = (\lambda^{-1} + k^{-1},\ (\lambda^{-1} + k^{-1})k^{-\theta}).$$

Так как $(\alpha,\ \beta) = \eta^{-1}\pi(k)\eta$, то

$$f(\alpha,\ \beta) = \eta f(\pi(k))\eta^{-1} =$$

$$= (\eta^{-1}(\lambda^{-1} + k^{-1}),\ \eta^{-1-\theta}(\lambda^{-1} + k^{-1})k^{-\theta}) = (c(k)/\alpha,\ c(k)/\beta),$$

где

$$c(k) = (1 + k)(\lambda^{-1} + k^{-1}).$$

Лемма доказана.

Функция f леммой 23 вполне определена. Но в нашем случае эта функция должна удовлетворять еще условию (10). Так как $(\alpha^{-1},\ 0)\ (0,\ 1) = (\alpha^{-1},\ 1)$, то из равенства (10) получаем (21)

$$f(\alpha^{-1},\ 1) = f(1{,}1 + \alpha^{1+\theta})\ (1,\ 0)$$

для любых $\alpha \neq 0$. Здесь использованы равенства

$$h(0,\ 1) = 1,\ g(0{,}1) = (1{,}1).$$

Если $\alpha = 1$, то

$$f(\alpha^{-1},\ 1) = (1{,}1) \text{ и } f(1,\ 1 + \alpha^{1+\theta}) = (0,\ 1).$$

Эти равенства не дают ничего. Предположим, что $\alpha \neq 0{,}1$. Вычислим левую часть равенства (21). Значение k известно:

$$k = 1/(1 + \alpha^{-(1+\omega)}) = \alpha^{1+\omega}/(1 + \alpha^{1+\omega}), \tag{22}$$

где $\omega = \theta^{-1}$. Пусть λ определяется из уравнения

$$\lambda^{1+\theta} = k^{1+\theta} + k^{2(1+\theta)}.$$

Так как $c(k) = (1 + k^{-1})(1 + \lambda^{-1}k)$, то

$$f(\alpha^{-1},\ 1) = (\alpha^{-\omega}(1 + \lambda^{-1}k),\ \alpha^{-1-\omega}(1 + \lambda^{-1}k)). \tag{23}$$

Применим формулы (19) к $(1{,}1 + \alpha^{1+\theta})$. Этот элемент сопряжен элементами из K с $\pi(k^{-1})$, где k дан равенством (22).

$$f(1{,}1 + \alpha^{1+\theta}) = (c(k^{-1}),\ c(k^{-1})/(1 + \alpha^{1+\theta})).$$

Справа в равенстве (21) стоит величина $\left(1 + c(k^{-1}),\ \frac{c(k^{-1})\,\alpha^{1+\theta}}{1 + \alpha^{1+\theta}}\right)$.

Поэтому получаем два уравнения:

$$\alpha^{-\omega}(1 + \lambda^{-1}k) = 1 + c(k^{-1}), \tag{24}$$

$$\alpha^{-1-\omega}(1 + \lambda^{-1}k) = c(k^{-1})\alpha^{1+\theta}/(1 + \alpha^{1+\theta}).$$

Если v определить из уравнения

$$v^{1+\theta} = k^{-(1+\theta)} + k^{-2(1+\theta)},$$

то $c\,(k^{-1})$ равен

$$(1 + k^{-1})(k + v^{-1}) = (1 + k)(1 + k^{-1}v^{-1}) = (1 + k^{-1}v^{-1}) \times \\ \times (1 + \alpha^{1+\omega}).$$

По определению λ и v получаем, что $\lambda k^{-1} = k^2 v$.

Положим $\xi = \lambda k^{-1}$. Тогда

$$\xi^{1+\theta} = 1 + k^{1+\theta}. \tag{25}$$

Второе из уравнений (24) запишется теперь так:

$$1 + \xi^{-1} = (1 + k\xi^{-1})\, k^{1+\theta}$$

или

$$\xi = (1 + k^{2+\theta})/(1 + k^{1+\theta}).$$

Подставим значение ξ в формулу (25). Получим

$$(1 + k^{2+\theta})(1 + k^{2^{1}+\theta^2})/(1 + k^{1+\theta})(1 + k^{0+\theta^2}) = 1 + k^{1+\theta}.$$

Упростив, получаем

$$k^{\theta}\,(1 + k^{\theta})(k^2 + k^{\theta^2}) = 0. \tag{26}$$

Считаем $\alpha \neq 0, 1$. Из (22) видно, что $k \neq 0,1$. Поэтому равенство (26) дает

$$k^2 = k^{\theta^2}. \tag{27}$$

Итак, $\theta^2 = 2$ и теорема 21 доказана.

Как уже доказано, порядок ZT-группы G есть либо $q\,(q^2 - 1)$, либо $q^2(q - 1)\,(q^2 + 1)$, где $q > 2$ — степень 2. Во втором случае q — нечетная степень 2. Если $|\,G\,| = q\,(q^2 - 1)$, то силовская 2-подгруппа абелева и $G \cong PSL\,(2, q)$. Рассмотрим другой случай, когда $|\,G\,| = q^2\,(q - 1)\,(q^2 + 1)$.

Т е о р е м а 24. *Если порядок ZT-группы G равен* $q^2\,(q - 1) \times (q^2 + 1)$, *то* $G \cong (G\,(q))$.

Д о к а з а т е л ь с т в о. По теореме 21 силовская 2-подгруппа Q группы G изоморфна $Q\,(q)$. Следовательно, по лемме 9 из § 7 $H \cong H\,(q)$ из $G\,(q)$.

Пусть σ, ρ и τ — элементы, определенные леммой 6. В силу леммы 22 и леммы 9 из § 7 существует изоморфизм $\mu : H \to H\,(q)$, удовлетворяющий условиям

$$\mu\,(\sigma) = (0,\ 1),\ \mu\,(\rho) = (1,0),\ \mu\,(K) = K\,(q). \tag{28}$$

Напомним, что одни и те же буквы (как и ранее) будут использоваться для обозначения элементов группы G и $G\,(q)$. В частности,

k будет обозначать элемент из K и элемент $\mu(k)$ из $K(q)$, τ — элемент из G и из $G(q)$. Расширим μ с H на G. Новое отображение будем обозначать той же буквой. Если $\zeta \in G \setminus H$, то ζ однозначно записывается в виде $\eta\tau\pi$ с $\eta \in H$, $\pi \in Q$. Определим

$$\mu(\zeta) = \mu(\eta)\tau\mu(\pi). \tag{29}$$

Нужно показать, что это отображение определяет изоморфизм G в $G(q)$. Пусть ζ_1, ζ_2 — два элемента из G. Докажем, что

$$\mu(\zeta_1\zeta_2) = \mu(\zeta_1)\mu(\zeta_2). \tag{30}$$

Если $\zeta_1 \in H$ и $\zeta_2 \in H$, то формула (30) верна по определению μ. Если $\zeta_1 \in H$ и $\zeta_2 \notin H$, то $\zeta_2 = \eta_2\tau\pi_2$.

$$\zeta_1\zeta_2 = (\zeta_1\eta_2)\tau\pi_2.$$

Следовательно,

$$\mu(\zeta_1\zeta_2) = \mu(\zeta_1\eta_2)\tau\mu(\pi_2) = \mu(\zeta_1)\mu(\eta_2)\tau\mu(\pi_2) = \mu(\zeta_1)\mu(\zeta_2).$$

Если $\zeta_1 \notin H$, $\zeta_1 = \eta_1\tau\pi_1$ и $\zeta_2 \in H$, то $\pi_1\zeta_2 \in H$ и $\pi_1\zeta_2 = k\pi$. Поэтому

$$\zeta_1\zeta_2 = \eta_1\tau\pi_1\zeta_2 = \eta_1\tau k\pi = \eta_1 k^{-1}\tau\pi,$$

$$\mu(\zeta_1\zeta_2) = \mu(\eta_1 k^{-1})\tau\mu(\pi).$$

С другой стороны,

$$\mu(\zeta_1)\mu(\zeta_2) = \mu(\eta_1)\tau\mu(\pi_1)\mu(\zeta_2) = \mu(\eta_1)\tau\mu(\pi_1\zeta_2) = \mu(\eta_1)\tau\mu(k\pi) = \mu(\eta_1)\tau\mu(\pi).$$

Пусть $\zeta_i \notin H$, $\zeta_2 \notin H$, $\zeta_i = \eta_i\tau\pi_i$ и $\pi_1\eta_2 = k\pi$. Если $\pi \notin 1$, то

$$\zeta_1\zeta_2 = \eta_1\tau\pi_1\eta_2\tau\pi_2 = \eta_1\tau k\pi\tau\pi_2 = \eta_1 k^{-1}\tau\pi\tau\pi_2 = \eta_1 k^{-1}g(\pi)h(\pi)\tau f(\pi)\pi_2,$$

где f, g, h — функции, определенные равенствами (3) и (4). Поэтому

$$\mu(\zeta_1\zeta_2) = \mu(\eta_1 k^{-1}g(\pi)h(\pi))\tau\mu(f(\pi)\pi_2).$$

Подобно

$$\mu(\zeta_1)\mu(\zeta_2) = \mu(\eta_1)k^{-1}g^*h^*\tau f^*\mu(\pi_2),$$

где $\tau\mu(\pi)\tau = g^*h^*\tau f^*$ с f^*, $g^* \in Q(q)$ и $h^* \in K(q)$. Согласно лемме 22 элемент f^* однозначно определяется равенством леммы 6 и строением силовской 2-подгруппы. Поэтому $f^* = \rho$, $g^* = \rho^{-1}$,

$h^* = 1$, если $\pi = \sigma$. Вообще говоря,

$$f^* = \mu(f(\pi)),\ g^* = \mu(g(\pi)),\ h^* = \mu(h(\pi)).$$

Равенство (30) доказано. Это означает, что теорема доказана.

Опишем, наконец, подгруппы ZT-группы.

Т е о р е м а 25. *Любая максимальная подгруппа группы* $G(q)$ *изоморфна одной из следующих подгрупп*:

1) $H(q)$-*группе Фробениуса порядка* $q^2(q-1)$, *изоморфной* $M(q; \theta)$, *где* $\theta^2 = 2$;

2) *группе диэдра порядка* $2(q-1)$;

3) *группе Фробениуса порядка* $4(q \pm r + 1)$ *с циклическим инвариантным множителем порядка* $q \pm r + 1$, где $r^2 = 2q$;

4) *группе* $G(s)$, *где* $s^t = q$, t — *простое число*.

Д о к а з а т е л ь с т в о. В теореме утверждается, что группа $G(q)$ содержит три абелевых подгруппы $A_0 = K$, A_1, A_2, порядков $q-1$, $q+r+1$, $q-r+1$, где $r^2 = 2q$. Эти подгруппы холловские. Нормализатор любой подгруппы из A_i совпадает с $N(A_i)$. Поэтому если некоторая подгруппа имеет нормальный делитель нечетного порядка, то она сопряжена какой-либо подгруппе одной из групп $N(A_i)$ $(i = 0, 1, 2)$. Покажем, что A_i — циклическая группа. По определению $G(q)$ есть подгруппа группы $GL(4, q)$, порядок которой равен $q^6(q^4-1)(q^3-1)(q^2-1)(q-1)$. $GL(4, q)$ содержит циклическую холловскую подгруппу Z порядка q^2+1. Следовательно, группы A_1 и A_2 сопряжены некоторым подгруппам из Z (см. Виланд [68]). Итак, если максимальная подгруппа имеет нормальный делитель нечетного порядка, то она сопряжена одной из групп 2) или 3).

Если подгруппа M имеет нормальный делитель, являющийся 2-группой, то в силу леммы 1 M содержится в подгруппе, сопряженной с $H(q)$.

Если подгруппа M не имеет абелевых нормальных делителей, то из леммы 1 и теоремы 18 можно получить, что она проста. Обозначим через $N(T)$ нормализатор силовской 2-подгруппы T подгруппы M. Очевидно, $N(T)$ — группа Фробениуса. Пусть $s-1$ — число инволюций в T и $l = |M : N(T)|$. Тогда M содержит точно $l(s-1)$ инволюций. Так как порядок дополнительного множителя в группе Фробениуса $N(T)$ не превосходит $s-1$ и пересечение $N(T)$ с сопряженными с ней подгруппами содержится в некотором дополнительном множителе $N(T)$, то в каждом смежном классе M по $N(T)$ имеется не более $s-1$ инволюции.

Следовательно, каждый смежный класс M по $N(T)$ содержит точно $s-1$ инволюцию. Но тогда подгруппа $N(T)$ имеет неединичное пересечение с любой из своих сопряженных подгрупп, в точности совпадающее с некоторым дополнительным множителем. Так как дополнительный множитель группы $N(T)$ имеет индекс 2 в своем нормализаторе в группе M, то M — ZT-группа. Так как $|M|$ не делится на 3, то $M \cong G(s)$. Число $s-1$ как порядок дополнительного множителя группы $N(T)$ делит число $q-1$. Поэтому q — степень числа s.

Глава IV

ИЗОЛИРОВАННЫЕ ПОДГРУППЫ

§ 12. Строение изолированных подгрупп в конечных группах

Теорема 1. *Собственная изолированная подгруппа M конечной группы G является группой одного из следующих типов:*

1) *M — нильпотентная подгруппа;*

2) *M — дополнительный множитель в группе Фробениуса G;*

3) *M — группа Фробениуса;*

4) *M изоморфна $SL(2, 2^n)$, $n > 1$;*

5) *в M существует характеристический ряд $\{1\} \subset N \subset NP \subset M$, где N — нильпотентная характеристическая подгруппа из M, P — силовская p-подгруппа из M и порядок подгруппы P прост, NP — группа Фробениуса, фактор-группа M/N — группа Фробениуса с инвариантным множителем, изоморфным P.*

Доказательство. Пусть M — изолированная подгруппа. Если подгруппа M отлична от своего нормализатора, то она нильпотентна (см. лемму 7 из § 8). Если же она совпадает со своим нормализатором и взаимно проста со своими сопряженными подгруппами, то группа G является группой Фробениуса и M — ее дополнительный множитель. Поэтому в дальнейшем будем считать, что рассматриваемая изолированная подгруппа совпадает со своим нормализатором и имеет неединичное пересечение хотя бы с одной сопряженной подгруппой. При доказательстве теоремы мы будем часто использовать следующее замечание.

Если нормализатор подгруппы H, принадлежащей изолированной подгруппе M, не содержится в M, то подгруппа H нильпотентна.

Действительно, подгруппа H инвариантна и изолирована в группе $\{H, g\}$ для любого элемента g из $N(H) \setminus M$. Поэтому H нильпотентна.

С л у ч а й I. Изолированная подгруппа имеет четный порядок.

А. Пусть M — совпадающая со своим нормализатором изолированная подгруппа нечетного индекса.

1) Покажем, что подгруппа M изолирована относительно силовских 2-подгрупп, т. е. из $M \cap T \neq \{1\}$ следует, что $T \subset M$ (T — силовская 2-подгруппа группы G). Предположим противное. Тогда существует такая силовская 2-подгруппа T группы G, не содержащаяся в M, пересечение которой с подгруппой M имеет максимальный порядок, $T \cap M = D \neq \{1\}$. Подгруппа D как пересечение подгруппы T с изолированной подгруппой M изолирована в T, а поэтому подгруппа K из T, содержащая подгруппу D в качестве максимальной подгруппы, расщепляема. Подгруппа D абелева и любая ее инволюция лежит в центре группы K (см. лемму 3 из § 8).

Так как подгруппа M имеет нечетный индекс в группе G, то в M найдется силовская 2-подгруппа T_1, содержащая подгруппу D. Рассмотрим $C(d)$, где d — инволюция, лежащая в пересечении подгрупп $Z(T_1)$ и D. Если это пересечение не содержит инволюций, то d — произвольная инволюция из D. Очевидно, $C(d) \supseteq K$ и $C(d) \cap T_1 \neq D$. В силу выбора подгруппы D силовская 2-подгруппа из $C(d)$, содержащая $C(d) \cap T_1$, принадлежит M. Из изолированности подгруппы M следует, что все силовские подгруппы нечетного порядка из $C(d)$ содержатся в M. Поэтому $C(d) \subset M$ и $K \subset M$, что противоречит выбору подгруппы D.

2) Покажем, что подгруппа M пересекается с сопряженными подгруппами по подгруппам нечетного порядка.

Допустим, что подгруппа M пересекается с некоторой сопряженной подгруппой $x^{-1}Mx$ по подгруппе четного порядка. Подгруппа $D = M \cap x^{-1}Mx$ содержит некоторую силовскую 2-подгруппу T из G (см. пункт 1)). Нетрудно убедиться, что подгруппа $N_G(T)$ не содержится в M и, значит, $N_M(T)$ — собственная изолированная подгруппа в $N_G(T)$. Покажем, что подгруппа $N_M(T)$ нильпотентна и инвариантна в $N_G(T)$. Действительно, пусть K — наибольшая инвариантная подгруппа из $N_G(T)$, содержащаяся в $N_M(T)$, и пусть $K \neq N_M(T)$.

Так как изолятор инвариантной подгруппы — инвариантная подгруппа, то K — изолированная подгруппа $N_G(T)$. Рассмотрим $N_G(T)/K$. Фактор-группа $N_M(T)/K$ — истинная изолированная подгруппа в $N_G(T)/K$. Пусть R/K — минимальная изо-

лированная подгруппа из $N_M(T)/K$. Если R/K совпадает со своим нормализатором в $N_G(T)/K$, то $N_G(T)/K$ — группа Фробениуса. Прообраз F ее инвариантного множителя является непримарной изолированной инвариантной подгруппой в $N_G(T)$. Непримарная нильпотентная подгруппа F содержит собственную изолированную подгруппу K, что невозможно. Если же R/K отлична от своего нормализатора, то R как отличная от своего нормализатора изолированная подгруппа нильпотентна, что снова противоречит, в силу непримарности подгруппы R, существованию в ней собственной изолированной подгруппы.

Этим доказано, что подгруппа $N_M(T)$ нильпотентна и инвариантна в $N_G(T)$.

Пусть теперь в T есть элемент $a \neq 1$, перестановочный с некоторым элементом нечетного порядка группы G. Тогда $C(a)$ непримарен. Обозначим через L подгруппу из $C(a)$, порожденную элементами нечетного порядка. Очевидно, $\{L, a\} \subset M$. Рассмотрим подгруппу H, порожденную всеми подгруппами, сопряженными подгруппе $\{L, a\}$ с помощью элементов из $N_G(T)$. Из изолированности подгруппы M и из того, что $M \cap g^{-1}\{L, a\}g \neq \{1\}$ для любого $g \in N_G(T)$, следует, что подгруппа H содержится в G. Подгруппа $\{N_M(T), H\}$ нильпотентна, так как она инвариантна относительно элементов из $N_G(T)$ и так как она целиком содержится в изолированной подгруппе M. Поэтому $\{N_M(T), H\} = N_M(T)$.

Таким образом, если в T существует элемент, перестановочный с элементами нечетного порядка, то $N_M(T)$ — непримарная нильпотентная группа.

Покажем, что в этом случае группа $N_M(T)$ взаимно проста со своими сопряженными в M подгруппами. Предположим обратное. И пусть $N_M(T) \cap N_M(x^{-1}Tx) = D_1 \neq \{1\}$. Возьмем в D_1 произвольный элемент d простого порядка p и рассмотрим его централизатор. Централизатор элемента d содержит все силовские подгруппы из $N_M(T)$ и $N_M(x^{-1}Tx)$, порядки которых взаимно просты с p. Подгруппа, ими порожденная, целиком содержится в изолированной подгруппе M. Обозначим эту подгруппу через A. Рассмотрим подгруппу A_1, порожденную всеми подгруппами, сопряженными с подгруппой A элементами из $N_G(T)$. Очевидно, подгруппа $\{N_M(T), A_1\}$ содержится в M и нильпотентна. Поэтому $A_1 \subseteq N_M(T)$ и подгруппа $N_M(x^{-1}Tx)$ должна совпадать с подгруппой $N_M(T)$. Этим показано, что подгруппа $N_M(T)$

взаимно проста со своими сопряженными подгруппами, а так как она совпадает со своим нормализатором в M, то M—группа Фробениуса, дополнительным множителем которой является подгруппа $N_M(T)$. Отсюда следует, что в $N_M(T)$ должна содержаться характеристическая подгруппа второго порядка, а это невозможно, так как все элементы из $N_G(T) - N_M(T)$ индуцируют в каждой характеристической подгруппе из $N_M(T)$ регулярные автоморфизмы.

Полученное противоречие показывает, что в T нет элементов, перестановочных с элементами нечетного порядка из G. Следовательно, $N_M(T) = T$. Если группа T взаимно проста со своими сопряженными в M подгруппами, то M является группой Фробениуса с дополнительным множителем T и T, в силу этого, имеет характеристическую подгруппу порядка 2, что невозможно.

Значит, силовская 2-подгруппа T группы M имеет нетривиальное пересечение хотя бы с одной из своих сопряженных подгрупп. Пусть $D_2 = T \cap x^{-1}Tx$ — максимальное пересечение силовских 2-подгрупп из M. Рассмотрим $N_M(D_2)$. В фактор-группе $N_M(D_2)/D_2$ силовские 2-подгруппы взаимно просты и совпадают со своими нормализаторами, так как в противном случае получилось бы противоречие либо с предположением, что силовская 2-подгруппа группы M совпадает со своим нормализатором, либо с предположением, что D_2 — максимальное пересечение силовских 2-подгрупп из M. Поэтому $N_M(D_2)/D_2$ — группа Фробениуса, силовская 2-подгруппа которой является дополнительным множителем. Инвариантный множитель обозначим через K/D_2.

Подгруппа K не изолирована в $N(D_2)$, потому что в противном случае она была бы непримарной нильпотентной группой и содержала бы элементы второго порядка, перестановочные с элементами нечетного порядка. Отсюда следует, что в D_2, а поэтому и в T существует неединичный элемент, который есть степень элемента c, не содержащегося в T, но принадлежащего некоторой сопряженной с T подгруппе.

Рассмотрим подгруппу C, порожденную всеми элементами группы G, сопряженными с элементом c элементами из $N_G(T)$. Подгруппа C содержится в M и инвариантна относительно $N_G(T)$. Подгруппа $\{C, T\}$ также инвариантна относительно $N_G(T)$, поэтому она нильпотентна. Но так как $N_M(T) = T$, то $\{C, T\} = T$ и $c \in T$, что противоречит выбору элемента c. Этим завершено

доказательство того, что подгруппа M пересекается с сопряженными подгруппами по подгруппам нечетного порядка.

3) Введем обозначения: $|M| = m$, $|G : M| = t$, l — число инволюций в M.

В случае, если $l = 1$, в M имеется единственная инволюция и, следовательно, она лежит в центре подгруппы M. Отсюда нетрудно получить, что подгруппа M плотна (не содержит собственных изолированных подгрупп и поэтому взаимно проста с сопряженными подгруппами, что противоречит нашему предположению. Следовательно, $l > 1$.

Так как в пересечениях подгруппы M со своими сопряженными инволюции не содержатся, то в группе G имеется точно lt инволюций. Покажем, что во всяком смежном классе Mg имеется точно l инволюций. Предположим противное. Тогда в некотором смежном классе Ma инволюций будет больше l. Пусть их будет $r > l$. Обозначим через a, x_2a,..., x_ra инволюции из смежного класса Ma. Очевидно, $ax_ia = x_i^{-1}$ $(2 \leqslant i \leqslant r)$.

Рассмотрим подгруппу $R\{a\}$, где R — подгруппа, порожденная элементами $x_2, x_3,..., x_r$. Так как $R \subset M \cap a^{-1}Ma$, то порядок подгруппы R нечетен. Следовательно, $R\{a\}$ — группа Фробениуса и элемент a индуцирует в R регулярный автоморфизм, переводящий все элементы в обратные. Отсюда следует, в частности, что подгруппа R абелева, а так как в смежном классе $Ra \subset Ma$ число инволюций равно порядку подгруппы R, то $|R| = r$. Пусть X — подгруппа, составленная из элементов группы p, либо перестановочных с элементом $g \in R$ простого порядка p, либо трансформирующих его в обратный. Очевидно, $|X : C(g)| = 2$ и подгруппа $C(g)$ инвариантна в подгруппе X.

Предположим сначала, что $C(g)$ не p-группа. В этом случае все элементы из $C(g)$ порядка взаимно простого с порядком элемента g лежат в M. Подгруппа K, ими порожденная, инвариантна в X. Рассмотрим фактор-группу $X/I(K)$, где $I(K)$ — изолятор подгруппы K в X. Порядок этой фактор-группы делится не более чем на два различных простых числа и она сверхразрешима. Подгруппа $X \cap M/I(K)$ изолирована в $X/I(K)$. Рассуждениями, аналогичными рассуждениям пункта 2), можно показать, что $X \cap M$ — нильпотентная группа. Отсюда следует, что если некоторая инволюция из M перестановочна хотя бы с одной циклической подгруппой из R, то она принадлежит ее централизатору. Но тогда $C(g)$ имеет четный порядок и в G найдется

силовская 2-подгруппа, не лежащая в M, но имеющая с M нетривиальное пересечение. Это невозможно. Значит, никакая циклическая подгруппа из R не перестановочна с инволюцией из M.

Пусть теперь $C(g)$ — p-группа. Тогда $X = P\{a\}$, где $P = C(g)$. Предположим, что в M есть инволюция b, перестановочная с подгруппой $\{g\}$. Легко видеть, что в этом случае элемент b индуцирует в R регулярный автоморфизм. Подгруппа $R\{b\}$ из M содержит точно r инволюций, что невозможно, так как в M имеется только $l < r$ инволюций.

В обоих случаях ни одна циклическая подгруппа из R не перестановочна с инволюцией из M. Следовательно, в каждом смежном классе подгруппы M по R имеется не более одной инволюции и не более одного элемента из централизатора инволюции.

Итак, $m/r \geqslant k$, где k — порядок централизатора некоторой инволюции, $lk \geqslant m$. Из этих неравенств просто выводится неравенство $l \geqslant r$, противоречащее нашему предположению $r > l$. Отсюда следует, что в каждом смежном классе группы G по M имеется точно l инволюций.

Таким образом, подгруппа M может быть сопряжена со своей сопряженной подгруппой при помощи инволюции и порядок пересечения подгруппы M с любой своей сопряженной подгруппой равен l.

4) Пусть $D = M \cap a^{-1}Ma$. Если D нормализуется инволюцией из M, то в каждой 2-подгруппе из M есть не более одной инволюции, и из [15] получаем, что M и G — группы Фробениуса. Поэтому, далее всюду считаем, что $(|N_M(D)|, 2) = 1$. Докажем, что D взаимно проста с сопряженными в M. Пусть существует отличная от D подгруппа $D = M \cap a^{-1}Ma$ и $D \cap D_1 \neq D_0 \neq 1$. Породим подгруппу X всеми элементами, перестановочными либо трансформирующими d ($d \in D_0$) в обратный. Очевидно, $X \supset \{D, D_1, a, a_1\}$ (a и a_1 — инволюции из G). Подгруппа $\{D, D_1\}$ содержится в подгруппе M.

Пусть сначала $C(d)$ не примарен. Тогда множество элементов Y из X порядка, взаимно простого с порядком элемента d, содержится в M и перестановочно с элементами a и a_1. Элемент a перестановочен с подгруппой $\{D, Y\} \subset M$ и поэтому $\{D, Y\} \subset M \cap a^{-1}Ma$, что невозможно.

Значит, можно считать, что $C(d)$ — примарная подгруппа и $X = P\{a\}$, где $P = C(d)$. Пусть $X \cap M = B$. Подгруппа B не содержит инволюций, так как ни одна инволюция из M не перестановочна с циклической подгруппой из D. Следовательно, B — p-группа, и поэтому она отлична от своего нормализатора в X. Отсюда следует, что подгруппа B содержится в пересечении подгруппы M с некоторой сопряженной подгруппой, а это невозможно, так как порядок подгруппы B больше l.

Теперь докажем, что D совпадает со своим нормализатором в M. Допустим, что $N_M(D) \neq D$ и рассмотрим $N_G(D)$. Подгруппа $N_M(D)$ изолирована в $N_G(D)$.

Возможны два случая. Рассмотрим сначала первый: подгруппа D не примарная.

Пусть K — наибольший нормальный делитель подгруппы $N_G(D)$, содержащийся в M. Так как фактор-подгруппа $N_M(D)/K$ изолирована в $N_G(D)/K$, то она содержит минимальную изолированную подгруппу R/K. Если R/K совпадает со своим нормализатором в $N_G(D)/K$, то $N_G(D)/K$ является группой Фробениуса. Прообраз F ее инвариантного множителя — нильпотентная непримарная группа и имеет с изолированной подгруппой M нетривиальное пересечение, содержащее D, поэтому $F \subset M$. Отсюда следует, что $N_G(D) = \{F, R\} \subset M$, что невозможно. Поэтому можно считать, что фактор-подгруппа R/K отлична от своего нормализатора в $N_G(D)/K$ и подгруппа R как отличная от своего нормализатора изолированная подгруппа в $N_G(D)$ нильпотентна. Это противоречит существованию в R собственной изолированной подгруппы D.

Рассмотрим теперь второй случай: D — примарная подгруппа.

Если подгруппа D — силовская подгруппа в M и отлична от своего нормализатора, то противоречие получается, как и в первом случае. Если же D — не силовская подгруппа M, то рассмотрим подгруппу X, состоящую из всех элементов группы G, либо перестановочных с некоторым элементом d из D, либо трансформирующих его в обратный. Так как подгруппа D изолирована в G, то $C(d)$ — примарная подгруппа. Следовательно, $X = P\{a\}$, где $P = C(d)$. Подгруппа $R = X \cap M$ содержит D и отлична от своего нормализатора в X. Значит, R содержится в пересечении подгруппы M с некоторой сопряженной подгруппой. Это невозможно, потому что элемент d можно выбрать таким, что $|R| > l$.

Таким образом, доказано, что подгруппа D совпадает со своим нормализатором в M и взаимно проста со своими сопряженными. Это означает, что M — группа Фробениуса и D — ее дополнительный множитель. Из коммутативности подгруппы D и из того, что силовские подгруппы в D циклические, следует, что D — циклическая подгруппа.

Б. M — совпадающая со своим нормализатором подгруппа четного порядка и силовская 2-подгруппа из M не является силовской в группе G.

Пусть T — произвольная силовская 2-подгруппа из M. Так как T не силовская в G, то она отлична от своего нормализатора в G и $N_G(T)$ не содержится в M. Обозначим через K — наибольший нормальный делитель подгруппы $N_G(T)$, содержащийся в M, и предположим сначала, что $K \neq N_M(T)$. Очевидно, подгруппа K абелева и изолирована в $N_G(T)$. Рассмотрим $N_G(T)/K$. Подгруппа $N_M(T)/K$ изолирована в $N_G(T)/K$. Пусть R/K — ее минимальная изолированная подгруппа. Подгруппа R/K должна совпадать со своими нормализатором, так как в противном случае непримарная подгруппа R была бы нильпотентной, что противоречит существованию в ней собственной изолированной подгруппы K. Если же R/K совпадает со своим нормализатором в $N_G(T)/K$, то $N_G(T)/K$ — группа Фробениуса и прообраз ее инвариантного множителя как подгруппа, не содержащаяся целиком в изолированной подгруппе M, но имеющая с M нетривиальное пересечение, должен быть 2-группой.

Отсюда следует, что $N_G(T)$ также является группой Фробениуса и $N_G(T) = F \cdot H$, где F — инвариантный, а H — дополнительный множитель и $H \subset M$. Подгруппа $N_M(T)$ — также группа Фробениуса с дополнительным множителем H и абелевым инвариантным множителем T. Нетрудно проверить, что централизатор любого неединичного элемента из T в подгруппе M абелев и силовские 2-подгруппы в M взаимно просты. Далее, так как силовская 2-подгруппа в M не циклическая, то либо T инвариантна в M и тогда M — группа Фробениуса с инвариантным множителем T, либо T не инвариантна в M и тогда подгруппа M изоморфна $SL(2,2^n)$ для некоторого $n > 1$ (Фейт [23, теорема 4]).

Если же $N_M(T)$ инвариантна в $N_G(T)$, то в этом случае подгруппа $M_M(T)$ абелева и совпадает со своим нормализатором в M. Докажем, что подгруппа $N_M(T)$ взаимно проста с сопряжен-

ными в M подгруппами. Предположим противное. Пусть $N_M(T) \cap \cap x^{-1}N_M(T)x = D \neq \{1\}$. Обозначим через R подгруппу, образованную либо элементами группы G, либо перестановочными с элементами из D, либо трансформирующими их в обратные. Ясно, что $R \cap M$ — абелева группа. Отсюда следует, что $R \cap M = N_M(T)$, и поэтому $N_M(T) = x^{-1}N_M(T)x$. Противоречие. Значит, подгруппа $N_M(T)$ взаимно проста с сопряженными в M подгруппами и M — группа Фробениуса.

Случай II. Изолированная подгруппа M имеет нечетный порядок.

Согласно теореме Фейта и Томпсона [25], подгруппа M разрешима.

А. Подгруппа M холловская.

1) Пусть в G существует силовская p-подгруппа P, не лежащая в M, но имеющая с M неединичное пересечение. Обозначим через D максимальное пересечение силовской p-подгруппы P из M с силовской подгруппой P_1 из G, не содержащейся в M.

Рассмотрим подгруппу $N_G(D)$. Пусть R — наибольший изолированный нормальный делитель подгруппы $N_G(D)$, содержащийся в $N_M(D)$. Если подгруппа R непримарная, то нетрудно показать, что $R = N_M(D)$. Так как в этом случае подгруппа R взаимно проста с сопряженными подгруппами и совпадает со своим нормализатором в подгруппе M, то M является группой Фробениуса. Покажем, что R не может быть примарной подгруппой. Предположим обратное. Ясно, что в этом случае минимальная изолированная подгруппа из $N_G(D)/R$, содержащаяся в $N_M(D)/R$, является p-группой. Так как подгруппа R изолирована, то все силовские q-подгруппы ($q \neq p$) из $N_G(D)$ либо циклические, либо обобщенные группы кватернионов.

Допустим, что в M имеется инвариантная p'-подгруппа. Тогда подгруппа R циклическая и ее нормализатор разрешим. Отсюда легко получить, что R — силовская p-подгруппа в $N_G(R)$, что невозможно. Значит, M не имеет инвариантных p'-подгрупп.

Выясним строение подгруппы $N_G(R)$. Покажем сначала, что если фактор-группа $N_G(R)/R$ имеет четный порядок, то в ней имеется точно одна инволюция. Действительно, если $\bar{a}$ и $\bar{b}$ — две различные инволюции из $N_G(R)/R$, то произведение инволюций a и b подгруппы $N_G(R)$, взятых из смежных классов $\bar{a}$ и $\bar{b}$ соответственно, содержится в централизаторе подгруппы R, но не

содержится в R. Если абелева p-группа $\{R, ab\}$ содержится в подгруппе M, то можно выбрать в R такой элемент x, что его централизатор в подгруппе P_1 не принадлежит R. Так как элемент x содержится в изолированной p-группе R, то его централизатор также является p-группой. Силовская p-группа группы G, содержащая централизатор элемента x, не принадлежит M, но имеет с ней большее, чем D, пересечение. Получаем противоречие. Если же $\{R, ab\}$ не содержится в M, то противоречие получается аналогично, только вместо $x \in R$ нужно взять элемент, централизатор которого в подгруппе P не содержится в R.

Итак, фактор-группа $N_G(R)/R$ имеет единственную инволюцию. Поэтому $N_G(R)/R$ плотна и, следовательно, $N_G(R) \cap M = R$. Это невозможно.

Если же подгруппа $N_G(R)$ имеет нечетный порядок, то она разрешима. Тогда $N_G(R) = P_0X$, где P_0 — силовская p-подгруппа из $N_G(R)$, X — ее дополнение. Так как подгруппа X плотная, то $N_G(R) \cap M = P_0$. Из изолированности подгруппы P_0 в $N_G(R)$ получаем, что в фактор-группе $N_G(R)/R$ все силовские подгруппы — циклические и $N_G(R)/R = RX/R \cdot P_0/R$ — группа Фробениуса. Подгруппа $R \cdot X$ инвариантна и изолирована в нормализаторе подгруппы R. Поэтому $R \cdot X$ нильпотентна, что противоречит существованию в ней собственной изолированной подгруппы.

2) Пусть в G нет силовских p-подгрупп, не содержащихся в M, но имеющих с M нетривиальное пересечение. Это значит, что M пересекается с сопряженными подгруппами по холловским подгруппам; в частности, если пересечение $D = M \cap x_1^{-1}Mx_1 \cap \ldots \ldots \cap x_n^{-1}Mx_n$ нетривиально, то D — холловская подгруппа.

Пусть D — минимальное нетривиальное пересечение некоторого множества сопряженных с M подгрупп. Если $N_M(D) \neq D$, то нетрудно показать, что подгруппа $N_M(D)$ инвариантна в $N_G(D)$ и $N_M(D)$ — непримарная нильпотентная подгруппа. Это противоречит существованию в $N_M(D)$ собственной изолированной подгруппы D.

Пусть подгруппа D совпадает со своим нормализатором в подгруппе M. Так как она взаимно проста с ней сопряженными подгруппами, то подгруппа M является группой Фробениуса.

Б. M — не холловская подгруппа группы G.

Обозначим через P силовскую p-подгруппу группы M, не являющуюся силовской в G. Рассмотрим $N_G(P)$.

1) Предположим, что подгруппа $N_M(P)$ не инвариантна в $N_G(P)$. Пусть K/R — минимальная изолированная подгруппа в $N_M(P)/R$, где R — наибольший изолированный нормальный делитель подгруппы $N_G(P)$, содержащийся в $N_M(P)$. Подгруппа K/R совпадает со своим нормализатором, так как в противном случае подгруппа K оказалась бы нильпотентной и, в силу ее непримарности, плотной, что противоречит существованию в ней собственной изолированной подгруппы R. Так как подгруппа K/R взаимно проста с ней сопряженными подгруппами, то факторгруппа $N_G(P)/R$ является группой Фробениуса. Обозначим ее инвариантный множитель через L/R. Из изолированности подгруппы R в $N_G(P)$ и изолированности L/R в $N_G(P)/R$ следует, что L изолирована в $N_G(P)$. Так как подгруппа L инвариантна в $N_G(P)$, то она нильпотентна.

Из существования в L собственной изолированной подгруппы R следует, что L — p-группа. Так как порядки подгрупп K/R и L/R взаимно просты, то L — силовская p-группа. Следовательно, подгруппа $N_G(P)$ является группой Фробениуса с инвариантным множителем L и дополнительным множителем, изоморфным K/R.

Пусть A — элементарный абелев нормальный делитель подгруппы M. Предположим, что A — p-группа. Из разрешимости подгруппы M следует, что $M = P \cdot F$, где F — холловская p'-подгруппа из M. Так как элементы из F индуцируют в A регулярные автоморфизмы, то все силовские подгруппы из F циклические и строение подгруппы F в этом случае хорошо известно. Обозначим через B максимальную инвариантную p-подгруппу группы M. Если $B \neq P$, то из теоремы 5.9 П. Г. Конторовича и В. М. Бусаркина [6] следует, что в M имеется характеристический ряд $\{1\} \subset B \subset BF \subset M$, где BF — группа Фробениуса с инвариантным множителем B, а факторгруппа M/B — группа Фробениуса с инвариантным множителем BF/B. В силу этого в группе Фробениуса $N_M(P)$ имеется характеристический ряд $\{1\} \subset B \subset BF \subset N_M(P) \subset N_M(P)$ с такими же свойствами. Отсюда следует существование в $N_M(P)$ инвариантной подгруппы $BF \cap N_M(P)$, не содержащей P и не содержащейся в ней, что невозможно. Поэтому $B = F$ и подгруппа $M = P \cdot F$ является группой Фробениуса с инвариантным множителем P и дополнительным множителем F.

Пусть A — не p-группа. Подгруппа P как изолированная

подгруппа группы G индуцирует в A регулярные автоморфизмы и, следовательно, циклическая. Покажем, что порядок подгруппы P прост. Действительно, так как P изолирована в L и L примарная, то в ней имеется подгруппа L_0, содержащая подгруппу P как максимальную. Из изолированности подгруппы P в L_0 следует, что порядок любого элемента подгруппы L_0, не содержащегося в P, прост и поэтому подгруппа L_0 расщепляема. С другой стороны, легко установить, что p-группа нечетного порядка, содержащая циклическую максимальную подгруппу непростого порядка, не расщепляема. Следовательно, порядок подгруппы P прост.

Применяя теорему 5.9 П. Г. Конторовича и В. М. Бусаркина [6], получаем, что в M имеется характеристический ряд $\{1\} \subset \subset N \subset NP \subset M$, где N — нильпотентная характеристическая подгруппа, NP — группа Фробениуса, M/N — группа Фробениуса с инвариантным множителем NP/N.

Докажем, что не существуют конечные разрешимые группы, содержащие такую подгруппу в качестве изолированной. Предположим противное. Пусть также подгруппа M максимальна и изолирована в некоторой конечной разрешимой группе G. Обозначим через D элементарный абелев нормальный делитель группы G. Если $D \cap M = \{1\}$, то $G = DM$. Так как P — не силовская p-подгруппа в G, то подгруппа D является p-группой. Все силовские q-подгруппы ($q \neq p$) из M индуцируют в D регулярные автоморфизмы и поэтому они циклические. Отсюда легко следует, что подгруппа M сверхразрешима, а это противоречит ненильпотентности ее коммутанта. Пусть $D \cap M \neq \{1\}$. Если $D \subset M$, то подгруппа D содержится в N и силовская p-подгруппа группы G индуцирует в D регулярные автоморфизмы. Следовательно, силовская p-подгруппа из G циклическая, что противоречит существованию в ней собственной изолированной подгруппы P. Если же D не содержится в M, то D является p-группой и можно считать, что $D \cap M = P$. Отсюда получается инвариантность подгруппы P в M. Противоречие.

2) Пусть $N_M(P)$ инвариантна в $N_G(P)$. В этом случае подгруппа $N_M(P)$ нильпотентна. Покажем, что она взаимно проста с сопряженными подгруппами. Допустим противное. Предварительно докажем, что подгруппа $N_M(P)$ изолирована в M.

Действительно, если в M имеется циклическая подгруппа $\{a\}$, не содержащаяся в подгруппе $N_M(P)$, и имеющая с ней не-

тривиальное пересечение, то можно образовать подгруппу $B = \{N_M(P), a\}$. Подгруппа B и все подгруппы, сопряженные с ней элементами из $N_C(P)$, содержатся в M. Тогда подгруппа A, ими порожденная, содержится в изолированной подгруппе и инвариантна относительно $N_G(P)$. Подгруппа $N_M(P)$ содержится в нильпотентной подгруппе A и совпадает со своим нормализатором, поэтому $N_M(P) = A$. Противоречие.

Из изолированности подгруппы $N_M(P)$ в M следует, что она может иметь неединичные пересечения с сопряженными подгруппами только в том случае, если $N_M(P) = P$. Пусть $N_M(P) = P$. Очевидно, максимальные пересечения силовских p-подгрупп из M изолированы в M. Обозначим через $D = P \cap P_1$ одно из таких пересечений. Рассмотрим $N_M(D)$. В фактор-группе $N_M(D)/D$ подгруппа $N_P(D)/D$ взаимно проста с сопряженными подгруппами и совпадает со своим нормализатором. Поэтому $N_M(D)/D$ — группа Фробениуса, и полный прообраз ее инвариантного множителя является непримарной нильпотентной подгруппой, а это противоречит существованию в ней собственной изолированной подгруппы D.

Таким образом, подгруппа $N_M(P)$ совпадает со своим нормализатором и взаимно проста с ней сопряженными подгруппами. Поэтому подгруппа M — группа Фробениуса.

Теорема доказана.

§ 13. Группы, содержащие собственные изолированные группы

Т е о р е м а 1. *Если в конечной группе G четного порядка существует собственная совпадающая со своим нормализатором изолированная подгруппа M нечетного индекса, то G является группой одного из следующих типов*:

1) *G — группа Фробениуса и M — ее дополнительный множитель*;

2) *G — ZT-группа и M содержит нормализатор ее силовской 2-подгруппы.*

Д о к а з а т е л ь с т в о. Если M взаимно проста с сопряженными подгруппами, то, очевидно, G — группа первого типа. Если же подгруппа M не взаимно проста с сопряженными подгруппами, то по теореме 1 § 12 M является группой Фробениуса и ее инвариантный множитель имеет четный порядок.

Так как подгруппа M пересекается с каждой из сопряженных подгрупп по дополнительным множителям и пересечение любых трех различных сопряженных с M подгрупп — единичная группа, то G — дважды транзитивная группа подстановок множества силовских 2-подгрупп, причем каждая подстановка однозначно определяется образами трех символов. Значит, G — ZT-группа. Теорема доказана.

Т е о р е м а 2 (Сузуки [60]). *Пусть H — сильно изолированная подгруппа четного порядка конечной группы G. Тогда G является группой одного из следующих типов:*

1) *G — группа Фробениуса и H — либо инвариантный, либо дополнительный множитель;*

2) *G — ZT-группа и H — либо силовская 2-подгруппа, либо ее нормализатор.*

Д о к а з а т е л ь с т в о. Если H совпадает со своим нормализатором, то утверждение следует из предыдущей теоремы. Если H инвариантна в G, то G — группа Фробениуса и H — ее инвариантный множитель.

Пусть H — не инвариантная, отличная от своего нормализатора, сильно изолированная подгруппа. Нормализатор подгруппы H — группа Фробениуса. Обозначим через t порядок дополнительного множителя группы Фробениуса $N(H)$, а через m — индекс подгруппы $N(H)$ в группе G. Пусть r — число инволюций в подгруппе H. Группа G содержит точно rm инволюций. Так как подгруппа $N(H)$ пересекается с сопряженными подгруппами по подгруппам, содержащимся в дополнительных множителях группы Фробениуса $N(H)$, то каждый смежный класс группы G по $N(H)$ содержит не более t инволюций. Поэтому $rm \leqslant r + t(m-1)$ и $r \leqslant t$. С другой стороны, число инволюций в инвариантном множителе группы Фробениуса $N(H)$ не меньше порядка дополнительного множителя. Поэтому $r = t$. Кроме того, отсюда получается, что подгруппа $N(H)$ имеет неединичное пересечение с любой сопряженной подгруппой и каждое пересечение совпадает с одним из дополнительных множителей. Отсюда, как и в предыдущей теореме, получаем, что G — ZT-группа и H — ее силовская 2-подгруппа. Теорема доказана.

Т е о р е м а 3. *Конечная группа, покрываемая собственными изолированными подгруппами, расщепляема.*

Д о к а з а т е л ь с т в о. а) Пусть группа G разрешима. Доказательство проведем индукцией по порядку группы G. Предпо-

ложим, что для всех групп, порядок которых меньше порядка группы G, теорема доказана. Обозначим через M максимальную инвариантную подгруппу группы G. Пусть $|G : M| = p$ (p — простое число). Будем считать, что подгруппа M не изолирована в группе G, так как в противном случае утверждение теоремы тривиально выполняется.

Так как подгруппа M не изолирована в G, то она покрывается изолированными подгруппами и, по индуктивному предположению, расщепляема. Из описания разрешимых расщепляемых групп следует, что M является группой одного из четырех типов:

1) M — расщепляемая q-группа;
2) $M = (A \times P) \leftthreetimes \{b\}$ — HT-группа;
3) $M = F \leftthreetimes H$ — группа Фробениуса;
4) $M \cong S_4$.

Рассмотрим все возможные случаи.

1) Пусть M — q-группа. Если G—не p-группа, то $G=M \leftthreetimes \{b\}$, где M — инвариантная q-подгруппа ($q \neq p$) и $\{b\}$ — циклическая подгруппа простого порядка p. Подгруппа $\{b\}$ совпадает со своим нормализатором. Действительно, если $\{b\} \neq N(\{b\})$, то $N(\{b\}) = \{b\} \times K$, где $K = N(\{b\}) \cap M$. Так как $N(\{b\})$ — нильпотентная и непримарная подгруппа, то она плотна (не содержит собственных изолированных подгрупп). Поэтому в G найдется изолированная подгруппа, целиком содержащая $N(\{b\})$.

Пусть L — изолятор подгруппы $N(\{b\})$. Очевидно, $L = A \leftthreetimes \{b\}$, где $A = L \cap M$. Так как подгруппа A содержит подгруппу K и так как L — изолятор подгруппы K, то изолятор подгруппы A совпадает с L. Так как $N(A) \subset N(L)$, то подгруппа L отлична от своего нормализатора, что невозможно, ибо L как подгруппа, содержащая нормализатор силовской подгруппы $\{b\}$, должна совпадать со своим нормализатором. Противоречие. Следовательно, подгруппа $\{b\}$ совпадает со своим нормализатором. Поэтому G — группа Фробениуса.

Всякая изолированная подгруппа с элементами составного порядка содержит центр группы. Если G — p-группа, то факторгруппа группы G по изолятору центра покрывается собственными изолированными подгруппами и, по предположению индукции, расщепляема. Так как множество элементов составного порядка расщепляемой p-группы порождает собственную подгруппу и

полный прообраз этой подгруппы содержит все элементы составного порядка, то группа G расщепляема.

2) M — HT-группа. В этом случае $M = (A \times P) \leftthreetimes \{b\}$, где $A \leftthreetimes \{b\}$ — группа Фробениуса, а $P \leftthreetimes \{b\}$ — расщепляемая q-группа и $b^q = 1$.

Пусть подгруппа $A \times P$ не изолирована в группе G. Так как подгруппа $A \times P$ плотная, то она содержится в некоторой изолированной подгруппе. Обозначим через L изолятор подгруппы $A \times P$. Очевидно, индекс подгруппы L в группе G прост (равен q), и, следовательно, группа G расщепляема.

Пусть $A \times P$ изолирована в G. Так как подгруппа M не изолирована в G, то по крайней мере одна циклическая подгруппа порядка q группы M, не лежащая в подгруппе $A \times P$, не изолирована в G. Без ограничения общности можно считать, что подгруппа $\{b\}$ не изолирована в G. Пусть L — изолятор подгруппы $\{b\}$. Так как $A \times P$ не имеет изолированных подгрупп, то $L \cap (A \times P) = \{1\}$ и $G = (A \times P) \leftthreetimes L$. Ясно, что L — циклическая группа порядка pq.

Группа P содержит элемент c простого порядка q, перестановочный с b. Так как $L \cap c^{-1}Lc \supset \{b\}$ и L изолирована, то $L = c^{-1}Lc$. Но в группе $L \times \{c\}$ подгруппа L, очевидно, не изолирована. Поэтому $A \times P$ не изолирована в G.

3) M — группа Фробениуса. Подгруппу M можно представить в виде $F \leftthreetimes H$, где F — инвариантный множитель группы Фробениуса M. Так как подгруппа F характеристична в M, то F инвариантна в G.

Пусть H не изолирована в группе G. Тогда найдется такой элемент c, что $c \notin H$, но $\{c\} \cap H \neq \{1\}$. Заметим, что $g^p \in M$ для любого элемента g из G, так как M — инвариантная подгруппа группы G и $|G : M| = p$. Следовательно, если $\{g\} \cap X \neq \{1\}$, где X — произвольная компонента расщепления подгруппы M, то $g^p \in X$. Рассмотрим подгруппу $K = F \leftthreetimes \{c\}$. В силу предыдущего замечания $F \cap \{c\} = \{1\}$.

Предположим, что K — собственная подгруппа группы G. В этом случае порядок подгруппы H не прост. Изолятор подгруппы K содержит подгруппу H и поэтому он совпадает с группой G. Следовательно, подгруппа K покрывается собственными изолированными подгруппами и, по предположению индукции, расщепляема. Так как порядок циклической подгруппы $\{c\}$ не прост и $\{c\}$ содержит подгруппу, индуцирующую группу регулярных автомор-

физмов группы F, то из описания расщепляемых групп нетрудно получить, что подгруппа K является группой Фробениуса с инвариантным множителем F и дополнительным множителем $\{c\}$. Отсюда следует, что F — холловская подгруппа группы G.

Если подгруппа F изолирована в группе G, то в этом случае G — группа Фробениуса, и, следовательно, она расщепляема. Пусть теперь подгруппа F не изолирована в G. Это значит, что в G найдется элемент b простого порядка, не принадлежащий подгруппе F и перестановочный с некоторым отличным от единицы элементом подгруппы F.

Как и в случае 1), можно показать, что подгруппа $F \leftthreetimes \{b\}$ не расщепляема, и, следовательно, не покрывается собственными изолированными подгруппами. Это возможно только в том случае, если подгруппа $F \leftthreetimes \{b\}$ содержится в некоторой изолированной подгруппе.

Изолятор подгруппы $F \leftthreetimes \{b\}$ нормален в G, так как он содержит инвариантную подгруппу F, изолятор которой содержит подгруппу $F \leftthreetimes \{b\}$. Пусть M_1 — максимальный нормальный делитель группы G, содержащий подгруппу $F \leftthreetimes \{b\}$. Так как порядок подгруппы H не прост, то $M_1 \cap H \neq \{1\}$. Подгруппа $F \leftthreetimes \leftthreetimes \{b\}$ как нерасщепляемая подгруппа группы M_1 принадлежит некоторой компоненте расщепления группы M_1.

Докажем, что подгруппа $F \leftthreetimes \{b\}$ нильпотентна. Действительно, если $F \leftthreetimes \{b\}$ — не нильпотентная подгруппа, то $F \leftthreetimes \{b\}$ лежит в дополнительном множителе группы Фробениуса M_1. Но это невозможно, потому что в этом случае в дополнительном множителе группы Фробениуса M_1 содержалась бы инвариантная подгруппа (подгруппа F инвариантна в G). Значит, подгруппа $F \leftthreetimes \{b\}$ нильпотентна.

Теперь из равенства $G = (F \leftthreetimes \{b\})H$ и плотности подгрупп $F \leftthreetimes \{b\}$ и H следует, что подгруппа H совпадает со своим изолятором. Это противоречит нашему предположению.

Пусть теперь подгруппа K совпадает с группой G. В этом случае подгруппа H содержится в подгруппе $\{c\}$. Действительно, с одной стороны, $|G| = |F| \cdot |H| \cdot p$; с другой стороны, из $G = F \leftthreetimes \{c\}$ и $c^p \in H$ следует, что $|G| = |F| \cdot |H \cap \{c\}| \cdot p$. Значит, $|H| = |\{c\} \cap H|$ и $H = \{c\} \cap H \subset \{c\}$. Можно считать, что $\{c\} = H \times \{c_1\}$, где $c_1^p = 1$, так как в противном случае все неединичные элементы группы $\{c\}$ индуцировали бы в группе F

регулярные автоморфизмы и группа G была бы группой Фробениуса.

Рассмотрим максимальную инвариантную подгруппу M_2 группы G, содержащую подгруппу $F \leftthreetimes \{c_1\}$. По индуктивному предположению группа M_2 расщепляема и не может быть симметрической группой подстановок четырех символов, так как она является расширением нильпотентной группы с помощью циклической группы. Случаи, когда максимальная инвариантная подгруппа — примарная группа или HT-группа, уже рассмотрены. Поэтому можно считать, что M_2 является группой Фробениуса и ее инвариантная подгруппа $F \leftthreetimes \{c_1\}$ (так как $\{c\}$ индуцирует в F нерегулярные автоморфизмы) лежит в инвариантном множителе.

Из того, что подгруппа $F \leftthreetimes \{c_1\}$ является холловской в G, следует, что подгруппа H должна содержать элемент, индуцирующий регулярный автоморфизм в инвариантном множителе группы Фробениуса M_2, что невозможно, так как любой элемент из H перестановочен с элементом c_1.

Если подгруппа H изолирована в группе G, то подгруппа F не изолирована в группе G. Подгруппа H отлична от своего нормализатора. Положим $N(H) = H \leftthreetimes K$. Очевидно, порядок подгруппы K равен p и $G = (F \leftthreetimes H) \leftthreetimes K$. Так как подгруппа F не изолирована, то в G найдется такой элемент b, что $b \notin F$ и $\{b\} \cap F \neq \{1\}$. Рассмотрим подгруппу $\{F, b\}$. Ее пересечение K_1 с подгруппой $H \leftthreetimes F$ отлично от $\{1\}$. Так как $\{F, b\} \cap H = \{1\}$, то его порядок равен p. Без ограничения общности можно считать, что $K_1 = K$. Значит, $\{F, b\} = F \leftthreetimes K$.

Если подгруппа $F \leftthreetimes K$ не покрывается собственными изолированными подгруппами, то она целиком лежит в некоторой изолированной подгруппе. Пусть L — ее изолятор. Так как подгруппа F не изолирована в $F \leftthreetimes K$, то, как и выше, $I(F \leftthreetimes K) = I(F)$ и подгруппа L инвариантна в G. Группа L нильпотентна. Подгруппа H плотна. Поэтому $L \cap H = \{1\}$ и $L = F \leftthreetimes K$. Отсюда следует, что подгруппы H и K поэлементно перестановочны. Так как подгруппа H изолирована, то все ее неединичные элементы имеют порядок p. Подгруппа H не содержит нециклических подгрупп порядка p^2. Поэтому она — циклическая группа простого порядка. Отсюда получаем, что индекс инвариантной изолированной подгруппы L в группе G равен простому числу и что группа G расщепляема.

Если подгруппа $F \leftthreetimes K$ покрывается собственными изолированными подгруппами, то по предположению индукции она расщепляема. Группа $F \leftthreetimes K$ как расширение нильпотентной группы F с помощью циклической группы не может быть симметрической группой подстановок четырех символов. Если $F \leftthreetimes K$ — группа Фробениуса, то подгруппа F как максимальная нильпотентная инвариантная подгруппа группы $F \leftthreetimes K$ должна быть инвариантным множителем группы Фробениуса $F \leftthreetimes K$. Поэтому она изолирована в $F \leftthreetimes K$. Это противоречит выбору подгруппы $F \leftthreetimes K$.

Если $F \leftthreetimes K$ группа типа $(A \times P) \leftthreetimes \{b\}$, то и в этом случае подгруппа F как максимальная инвариантная подгруппа группы $F \leftthreetimes K$ совпадает с $A \times P$ и изолирована в $F \leftthreetimes K$, что снова противоречит выбору подгруппы $F \leftthreetimes K$.

Пусть, наконец, $F \leftthreetimes K$ — примарная группа. Тогда она силовская p-подгруппа группы G. Обозначим ее через P. Так как группа P расщепляема, то ее подгруппа P_0, порожденная всеми элементами составного порядка, отлична от P. Если $P = \{1\}$, то все p-элементы группы G имеют простой порядок. В этом случае группа G расщепляема. Расщепление группы G состоит из подгрупп, сопряженных с H, и из циклических подгрупп группы G простого порядка p.

Покажем, что при $p \neq 2$ подгруппа F — элементарная абелева группа. Предположим, что F_0 — собственная характеристическая подгруппа группы F. Если F_0HK — собственная подгруппа группы G, то в случае ее расщепляемости $F_0HK \cong S_4$. Но тогда $p = 2$, что противоречит нашему предположению. Если подгруппа F_0HK не расщепляема, то она лежит в некоторой изолированной подгруппе. Значит, изолятор подгруппы F_0 — собственная изолированная подгруппа группы G. Так как $I(F_0)$ — инвариантная подгруппа, а все не содержащиеся в F инвариантные подгруппы не изолированы в G, то $I(F_0) \subset F$. Подгруппа F не изолирована в G. Поэтому $I(F_0)$ — собственная подгруппа группы F.

Рассмотрим подгруппу $I(F_0)\,HK$. Ясно, что $I(F_0)$—подгруппы, сопряженные с H, и все циклические подгруппы порядка p из $I(F_0)\,HK$, не принадлежащие $I(F_0)$, составляют расщепление группы $I(F_0)HK$. Но тогда подгруппа $I(F_0)H$ и все циклические подгруппы порядка p из $I(F_0)HK$, не принадлежащие $I(F_0)H$, также составляют расщепление группы $I(F_0)HK$. Подгруппа $I(F_0)H$ как инвариантная компонента расщепления этой группы

должна быть нильпотентной, что невозможно. Следовательно, при нечетном p группа F не имеет неединичных характеристических подгрупп.

Таким образом, о строении группы P нам известно следующее: она расщепляема, все ее неединичные элементы имеют нечетный порядок p и ее максимальная подгруппа F — элементарная абелева группа. Покажем, что этот случай невозможен. Действительно, из расщепляемости группы P следует, что все ее элементы составного порядка лежат в некоторой максимальной подгруппе P_0 группы P. Следовательно, в P найдется элемент b простого порядка, не принадлежащий ни подгруппе P_0, ни подгруппе F.

Легко видеть, что $P = F\{b\}$. Без ограничения общности можно считать, что хотя бы один элемент составного порядка подгруппы P имеет вид ba, где $a \in F$. Из очевидного равенства $(ba)^p = bab^{-1}b^2ab^{-2}\ldots b^pab^{-p}$ и перестановочности (ввиду коммутативности подгруппы F) всех сопряженных с a элементов следует, что при $p \neq 2$ $(b^2a)^p = (ba)^p$ и, значит, элемент b^2a так же, как и элемент ba, содержится в подгруппе P_1. Таким образом, мы получаем, что $b = b^2a\,(ba)^{-1} \in P_1$, а это противоречит выбору элемента b. Значит, P — 2-группа.

Отсюда следует, что изоляторы циклических подгрупп порядка 4 группы G абелевы и совпадают с соответствующими компонентами расщепления силовской 2-подгруппы P и сопряженных с ней подгрупп.

Группа G может быть нерасщепляемой только в том случае, когда по крайней мере изоляторы двух циклических подгрупп четвертого порядка, принадлежащие различным силовским 2-подгруппам, имеют пересечение, отличное от единицы. Предположим, что существуют два таких изолятора. Обозначим их через A и B, а их пересечение — через D. Очевидно, $D \subset F$. Рассмотрим централизатор C подгруппы D. Так как $C \supset \{A, B\}$ и $\{A, B\}$ не лежит ни в какой силовской 2-подгруппе из G_1, то C содержит элементы нечетного порядка. Но элементы нечетного порядка содержатся только в подгруппах, сопряженных с подгруппой H, и ни один из них не может лежать в централизаторе никакого отличного от единицы элемента подгруппы F, так как все они индуцируют в подгруппе F регулярные автоморфизмы. Противоречие. Значит, группа G расщепляема.

4) $M \cong S_4$, $|G : M| = p$. Группа M содержит характерис-

тическую подгруппу индекса 2. Поэтому если $p \neq 2$, то группа G содержит максимальную инвариантную подгруппу индекса 2, которая не изоморфна симметрической группе подстановок четырех символов. Этот случай рассмотрен ранее. Поэтому считаем, что $p = 2$. Следовательно, порядок группы равен 48.

Обозначим через P силовскую 2-подгруппу группы G. Так как силовская 2-подгруппа подгруппы M не изолирована в M, то и подгруппа P не изолирована в G. Но тогда она расщепляема и $P = A \leftthreetimes \{b\}$, где A — абелева подгруппа из P, порожденная элементами составного порядка, $b^2 = 1$. Пересечение подгруппы A с подгруппой M не инвариантно в M. Поэтому подгруппа A не инвариантна в группе G. Индекс подгруппы A в группе G меньше ее порядка. Значит, подгруппа A нетривиально пересекается с любой сопряженной подгруппой. Ясно, что все такие пересечения содержатся в центре группы G. Так как центр подгруппы M — единичная группа, то $Z(G) \cap M = \{1\}$ и $G = M \times Z(G)$. Очевидно, подгруппа $Z(G)$ не может быть включена в собственную изолированную подгруппу группы G. Противоречие. Случай 4) невозможен.

б) Группа G неразрешима.

Допустим, что существуют неразрешимые группы, каждый неединичный элемент которых содержится в собственной изолированной подгруппе. Обозначим через G группу наименьшего порядка с таким свойством. Согласно теореме Фейта и Томпсона [25], эта группа имеет четный порядок.

Предположим, что силовская 2-подгруппа содержится в некоторой собственной изолированной подгруппе группы G. Пусть K — максимальная изолированная подгруппа, содержащая силовскую 2-подгруппу. Если подгруппа K совпадает со своим нормализатором, то расщепляемость группы G следует из теоремы 1.

Пусть подгруппа K отлична от своего нормализатора. Так как индекс подгруппы K в своем нормализаторе нечетен и подгруппа K нильпотентна, то подгруппа $N(K)$ разрешима и, следовательно, отлична от G. Подгруппа $N(K)$ не содержится ни в какой собственной изолированной подгруппе группы G и поэтому покрывается собственными изолированными подгруппами. Тогда в силу выбора группы G подгруппа $N(K)$ расщепляема.

Покажем, что K взаимно проста с сопряженными подгруппами. Допустим противное. Так как пересечение изолированных под-

групп является изолированной подгруппой, а непримарная нильпотентная подгруппа не содержит собственных изолированных подгрупп, то можно считать, что K — 2-группа.

Пусть D — максимальное пересечение подгруппы K с некоторой сопряженной подгруппой. Если нормализатор подгруппы D отличен от G, то $N(D)$ — расщепляемая группа. Она изоморфна симметрической группе подстановок четырех символов. Но это противоречит изолированности подгруппы D, так как в S_4 инвариантная 2-подгруппа не изолирована.

Если же подгруппа D нормальна в G, то в фактор-группе G/D силовская 2-подгруппа сильно изолирована (содержит централизатор любого своего неединичного элемента). Из теоремы 2 следует, что G/D — ZT-группа. Для получения противоречия теперь достаточно рассмотреть полный прообраз подгруппы Фробениуса с инвариантным множителем нечетного порядка.

Значит, подгруппа K взаимно проста с сопряженными подгруппами и централизатор любого неединичного элемента подгруппы K содержится в $N(K)$. Можно считать, что K не сильно изолирована в группе G, так как в противном случае из теоремы 2 следовала бы расщепляемость группы G.

Подгруппа $N(K)$ как расщепляемая группа имеет следующее строение:

$$N(K) = (A \times P) \leftthreetimes \{a\},$$

где $a^p = 1$, подгруппа $A \times P = K$ порождается всеми элементами из $N(K)$, порядок которых отличен от p, $P \leftthreetimes \{a\}$ — силовская p-подгруппа из $N(K)$.

Обозначим через n число инволюций в K, а через m — индекс подгруппы $N(K)$ в G. Группа G содержит точно nm инволюций. Так как $n > 1$, то найдется смежный класс $gN(K)$ $(g \notin N(K))$, содержащий по крайней мере две инволюции. Обозначим их через a и ab, $b \in N(K)$. Тогда $N(K) \cap aN(K)a = D \supseteq \{b\} \neq \{1\}$ и $aba = b^{-1}$. $N(D)$ — собственная подгруппа в G и имеет четный порядок. Поэтому $N(D)$ расщепляема. Из описания расщепляемых групп нетрудно получить, что элемент a индуцирует в силовской p-подгруппе из $N(D)$ регулярный автоморфизм. Так как подгруппы K и $N(D)$ имеют неединичное пересечение, в котором инволюция a также индуцирует регулярный автоморфизм, то, в противоречие доказанному выше, мы получаем, что подгруппа K имеет неединичное пересечение с подгруппой aKa.

Пусть силовская 2-подгруппа не содержится ни в какой изолированной подгруппе из G. В этом случае силовская 2-подгруппа T из G расщепляема.

Пусть T — элементарная абелева группа. Так как подгруппа T не изолирована в G, то централизатор H некоторой инволюции из T не содержится в T. Предположим, что подгруппа H выбрана так, что ее порядок — максимальный из всех возможных. Подгруппа H содержит силовскую 2-подгруппу T и расщепляема, а подгруппа T не содержится ни в какой непримарной нильпотентной подгруппе. Поэтому

$$H = (A \times T_0) \leftthreetimes \{a\},$$

$$T_0\{a\} = T \text{ и } a^2 = 1.$$

Пусть g — произвольный элемент из $N(T)$, не содержащийся в T. Индекс подгруппы $T_0 \cap gTg^{-1}$ в подгруппе T равен 4. Так как вследствие выбора подгруппы H подгруппа $A \times T_0$ взаимно проста с сопряженными подгруппами, то порядок силовской 2-подгруппы из G равен 4. Применяя теорему Горенштейна и Уолтера [28, теорема 2], нетрудно получить, что G изоморфна $PSL(2, q)$ и поэтому расщепляема.

Если подгруппа T не элементарна, то $T = A \leftthreetimes \{a\}$, где A — абелева 2-подгруппа группы T, порожденная всеми элементами составного порядка, $a^2 = 1$ и $aa_1a = a_1^{-1}$ для всех a_1 из A.

Центр подгруппы T состоит из всех инволюций подгруппы A. Легко видеть, что силовская 2-подгруппа T совпадает со своим нормализатором и $N(Z(T)) = T$. Следовательно, группа G не 2-нормальна. Пусть T и T_1 — такие две силовские 2-подгруппы из G, что

$$D = T \cap T_1 \supset \{Z(T), Z(T_1)\}.$$

Если порядок центра силовской 2-подгруппы больше 2, то, очевидно, центры силовских 2-подгрупп T и T_1 имеют неединичное пересечение. Централизатор этого пересечения содержит подгруппы T и T_1 и является не 2-нормальной расщепляемой HT-группой. Это невозможно, так как HT-группы p-нормальны для любого простого делителя их порядка. Если же порядок центра

подгруппы T равен 2, то T — группа диэдра. Силовская 2-подгруппа нормализатора максимального пересечения силовских 2-подгрупп T и T_1 группы G также группа диэдра. Отсюда следует, что подгруппа $N(D)$ не 2-нормальна и поэтому изоморфна S_4.

Это означает, что $D = T \cap T_1$ — совпадающая со своим централизатором нециклическая группа четвертого порядка. Из теоремы Горенштейна и Уолтера [28, теорема 2] получаем, что G изоморфна либо $PSL(2, q)$, либо $PG(2, q)$ и, следовательно, расщепляема. Теорема доказана.

ЛИТЕРАТУРА

1. Бусаркин В. М. О группах Фробениуса. Матем. зап. Уральск. ун-та, 1961, **3**, 51—53.
2. Бусаркин В. М. Изолированные покрытия конечных разрешимых групп. Матем. зап. Уральск. ун-та, 1963, **4**.
3. Бусаркин В. М. Строение изолированных подгрупп в конечных группах. Алгебра и логика. Семинар, 1965, **4**, вып. 2.
4. Конторович П. Г. О разложении группы в прямую сумму подгрупп. I, II. Матем. сб., 1959, **5**, 289—296; 1940, **7**, 27—33.
5. Конторович П. Г. Группы с базисом расщепления. I, II, III, IV. Матем. сб., 1943, **12**, 56—70; 1946, **19**, 287—308; 1948, **22**, 79—100; 1950, **26**, 311—320.
6. Конторович П. Г. и Бусаркин В. М. θ-изолированные комплексы в группах. Алгебра и логика. Семинар, 1962, **3**,
7. Конторович П. Г., Пекелис А. С., Старостин А. И. Структурные вопросы теории групп. Матем. зап. Уральск. ун-та, 1961, **3**, 3—50.
8. Трофимов П. И. Транзитивно-коммутативные группы. Томск, Учен. зап. ун-та, 1947, **6**, 110—116.
9. Холл М. Теория групп. М., ИЛ, 1962.
10. Шмидт О. Ю. О группах Фробениуса. Докл. АН СССР, 1940, **26**, 3—5.
11. Baer R. Partitionen endlicher Gruppen. Math. Z., 1961, **75**, N 4, 333—372.
12. Baer R. Einfache Partitionen nicht-einfacher Gruppen. Math. Z., 1961, **77**, 1—37.
13. Baer R. Einfache Partitionen endlicher Gruppen mit nicht-trivialer Fittingscher Untergruppen.— Arch. Math., 1961, **12**, 81—89.
14. Bransde W. Theory of groups of finite Order. Cambridge, 1911.
15. Brauer R. and Suzuki M. On finite groups of even order whose 2-Sylow groups is a quaternion group. Proc. Nat. Acad. U. S. A., 1959, **45**, 1757—1759.
16. Brauer R., Suzuki M. and Wall G. E. A characterization of the one-dimensional unimodular projektive groups over finite fields. Illinois J. Math., 1958, **2**, 718—745.
17. Brauer R. and Fowler K. A. On groups of even order. Ann. Math., 1955, **62**, 565—583.
18. Dickson L. Linear groups. Leipzig, 1901.
19. Feit W. On a conjecture of Frobenius. Proc. Amer. Math. Soc., 1956, **7**, 177—187.

20. Feit W. On the structure of Frobenius groups. Canad. J. Math., 1957, 9, 587—596.
21. Feit W. On a class of double transitive permutation groups. Illinois J. Math., 1960, 4, 170—186.
22. Feit W. A characterisation of the simple groups SL$^{\cdot}$(2,2^{Q}). Amer. J. Math. 1960, 82, 281—300.
23. Feit W. On groups which contain Frobenius groups. Proc. Sympos. Pure Mathematics Amer. Math. Soc., 1959, 1, 22—27.
24. Feit W., Hall M. and Thompson J. G. Finite groups in which the centralizer of any non-identity element is nilpotent. Math. Z., 1960, 74, 1—17.
25. Feit W. and Thompson J. G. Solvability of groups of odd order.— Pacif. J. Math., 1963, 13, 771—1029.
26. Frobenius G. Ueber auflöshare Grouppen. IV. Sitzungsberichte, Berlin, 1901, 1223—1220.
27. Gorenstein D. A class of Frobenius groups. Canad. J. Math , 1959, 11, 39—47.
28. Gorenstein D. and Walter J. On finite groups with dihedral Sylow 2-subgroups. Illinois J. Math., 1962, 6, 553—593.
29. Gorenstein D. and Walter J. The characterizations of finite groups. I, II, III. J. Algebra, 1965, 2, 85—151, 218—270, 354—393.
30. Grün O. Beiträge zur Gruppentheorie. I. J. reine und angew. Math., 1936, 174, 1—14.
31. Hall Ph. and Higman G. The p-length of a p-soluble group and reduc, tion theorems for Burnsides problem. Proc. London Math. Soc., 1956, 7, 1—42.
32. Higman G. Finite groups in which every element has prime power order J. London Math. Soc., 1957, 32, 335—342.
33. Higman G. Suzuki 2-groups. Illinois J. Math., 1963, 7, 79—96.
34. Hoffman F. Nilpotent height of finite groups admitting fixed point-free automorphisms.— Math. L., 1964, 85, 260—267.
35. Hugher D. R. and Thompson J. G. The H_p-problem and the structure of H_p-groups. Pacif. J. Math., 1959, 9, 1097—1102.
36. Ito N. On a class of doubly transitive permutation groups. Illinois J. Math., 1962, 6, 341—352.
37. Iwahori N. On a property of a finite group.— J. Fac. Sci. Univ. Tokyo, 1964, 11, 47—64.
38. Iwahori N. and Kondo T. A criterian for the existence o a non-trivial partition of a finite group with applications to finite reflection groups. J. Math. Soc. Japan, 1965, 17, 207—215.
39. Iwahori N. and Kondo T. On a finite group admitting a permutation representation P such that TrP (σ)-3 for all $\sigma \neq 1$. J. Fac. Sci. Univ. Tokyo, 1965, 11, 113—114.
40. Kegell O. H. Die Nilpotenz der H_p-Gruppen. Math. Z., 1961, 75, 373 — 376.
41. Kegell O. H. Nicht-einfache Partitionen endlicher Gruppen. Arch. Math., 1961, 12. 170—175.

42. Kegell O. H. Aufzählung der Partitionen endlicher Gruppen mit trivialer Fittingscher Untergruppen. Arch. Math., 1961, 12, 409—412.
43. Kegell O. H. Zur Struktur endlicher Gruppen mit nicht-trivialer Partition. Arch. Math., 1961, 12, 251—261.
44. Miller G. A. Groups in which all the operators are contained in a series of subgroups such that any two have only the identity in common. Bull. Amer. Math. Soc., 1906, 446.
45. Shaw R. H. Remark on a theorem of Frobenius groups. Canad. J. Math., 1956, 7, 177—187.
46. Straus E. and Szekeres G. On a problem of D. R. Hughes. Proc. Amer. Math. Soc., 1957, 9, 157—158.
47. Suzuki M. On the finite group with a complete partition. J. Math. Soc. Japan, 1950, 5, 165—185.
48. Suzuki M. A characterization of simple groups LF (2, p). J. Fac. Sci. Univ. Tokyo, Sect. I, 1951, 6, 259—293.
49. Suzuki M. On finite groups with cyclic Sylow subgroups for all odd primes. Amer. Z. Math., 1955, 77, 657—691.
50. Suzuki M. The nonexistence of a certain type of simple groups of odd order. Proc. Amer. Math. Soc., 1957, 8, 686—695.
51. Suzuki M. On finite groups containing an element of order four which commutes only with its powers. Illinois J. Math., 1959, 3, 255—271.
52. Suzuki M. On characterizations of linear groups. I, II, III. Trans. Amer. Math. Soc., 1959, 92, 191—204, 205—219; Nagoya Math. J., 1962, 21, 159—183.
53. Suzuki M. Applications of group characters. Proc. Sympos. Pure Mathematics Amer. Math. Soc., 1959, 1, 88—99.
54. Suzuki M. Investigations on finite groups. Proc. Nat. Acad. Sci. U. S. A., 1960, 46, 1611—1614.
55. Suzuki M. A new type of simple groups of finite order. Proc. Nat. Acad. Sci. U. S. A., 1960, 46, 868—870.
56. Suzuki M. On a finite group with a partition. Arch. Math., 1961, 12, 241—254.
57. Suzuki M. Finite groups which nilpotent centalizers. Trans. Amer. Math. Soc., 1961, 99, 425—470.
58. Suzuki M. On a class of doubly transitive groups. I, II. Ann. Math., 1962, 75, 105—145; 1964, 79, 514—589.
59. Suzuki M. On generalized ZT-groups. Arch. Math., 1962, 13, 199—202.
60. Suzuki M. Two characteristic properties of ZT-groups. Osaka Math. J., 1963, 15, 143—150.
61. Suzuki M. Finite groups of even order in which Sylow 2-groups are independent. Ann. Math., 1964, 80, 58—77.
62. Suzuki M. A characterization of the 3-dimensional projective unitary group over a finite field of odd characteristic. J. Algebra, 1965, 2, 1—14.
63. Thompson J. G. Finite groups with fixed point-free automorphisms of prime order. Proc. Nat. Amer. Sci. U. S. A., 1959, 45, 578—581.
64. Thompson J. G. Normal p-complements for finite groups. Math. Z., 1960, 72, 332—354.

65. Thompson J. G. Normal p-complements for finite groups. J. Algebra 1964, 1, 43—46.
66. Vincent G. Les groupes lineaires finis sans points fixes. Comment. math. helv., 1947, 20, 117—171.
67. Walter J. H. On the characterizations of linear and projektive linear groups. I, II. Trans. Amer. Math. Soc., 1961, 100, 481—529; 1961, 101,107—123.
68. Wielandt H. Zum Satz von Sylow.— Math Z., 1954, 60, 407—408.
69. Wiesner L. Groups in which the normalizer of every element exept identity is abelian. Bull. Amer. Math. Soc., 1925, 31, 413—416.
70. Yonng J. M. On the partition of group and the resulting classification. Bull. Amer. Math. Soc., 1927, 33, 453—461.
71. Zassenhaus H. Kennzeichnung endlicher linearer Gruppen als Permutations gruppen. Abhandl. math. Semin. Univ. Hamburg, 1936, 11, 17—40.
72. Zassenhaus H. Über endliche Fastkörper. Abhandl. math. Semin. Univ. Hamburg, 1936, 11, 187—220.

ОГЛАВЛЕНИЕ

Бусаркин Виктор Михайлович,
Горчаков Юрий Михайлович

Конечные расщепляемые группы

Утверждено к печати
Институтом физики Сибирского отделения
Академии наук СССР

Редактор издательства *Э. Н. Терентьева*
Технический редактор *И. Н. Жмуркина*

Сдано в набор 24/V 1968 г. Подписано к печати 23/X-1968 г.
Формат 60×90¹/₁₆. Бумага типогр. № 2. Усл. печ. л. 7
Уч.-изд. л. 5,3. Тираж 2600. Т-13293. Тип. зак. 734.

Цена 32 к.

Издательство «Наука»
Москва, К-62, Подсосенский пер., 21

2-я типография издательства «Наука»
Москва, Г-99, Шубинский пер., 10