Оглавление

Глава 1

Абелевы группы

Везде в данной главе под группой, если не оговорено противное, понимается абелева группа. Для записи операции используется аддитивное обозначение.

1.1 Прямые суммы циклических групп

§1 Свободные абелевы группы

Определение 1.1.1.1. [1, стр. 80] Пусть $\mathfrak{L}$ — класс групп. Говорят, что группа $F = \langle x_i | i \in I \rangle$ из $\mathfrak{L}$ есть *свободная группа в классе* $\mathfrak{L}$ *со свободным порождающим множеством* $\{x_i | i \in I\}$, если для любой группы $G \in \mathfrak{L}$ с порождающим множеством $\{a_i | i \in I\}$ отображение $x_i \to a_i$ продолжается до гомоморфизма $F \to G$. Мощность множества I называется *степенью (свободы)* свободной группы F. Само множество $\{x_i | i \in I\}$ будем называть базой группы F.

Теорема 1.1.1.2. *[1, теорема 7.1.1] Прямые суммы бесконечных циклических групп и только они являются свободными в классе абелевых групп.*

Доказательство. Пусть $F = \sum_{i \in I} \langle x_i \rangle$. Очевидно, что группа F является свободной. Обратно, пусть $H = \langle y_i | i \in I \rangle$ — свободная группа. Тогда $\sigma : H \longrightarrow F$ — гомоморфизм групп. По доказанному ранее, $\tau : F \longrightarrow H$ — также гомоморфизм. Здесь σ переводит y_i в x_i, а τ — x_i в y_i. Тогда $(x_i)\tau\sigma = x_i$, следовательно, $\tau\sigma$ — тождественное отображение группы F, следовательно, τ — изоморфизм групп F и H. ⊠

Теорема 1.1.1.3. *[1, теорема 7.1.2] Абелева группа G свободна тогда и только тогда, когда она обладает трансфинитно возрастающей матрешкой, каждая секция которой изоморфна бесконечной циклической группе $\mathbb{Z}$.*

Доказательство. Пусть в абелевой группе G имеется возрастающая матрешка

$$0 = N_0 < N_1 < N_2 < \ldots < N_\alpha < \ldots < N_\gamma = G \tag{1.1}$$

с бесконечными циклическими секциями. Для всякого $\alpha < \gamma$ в разности $N_{\alpha+1} \setminus N_\alpha$ выберем такой элемент $a_{\alpha+1}$, что $N_{\alpha+1} = \langle a_{\alpha+1} + N_\alpha \rangle$, и покажем разложимость группы G в прямую сумму $\sum_{\alpha<\gamma} \langle a_{\alpha+1} \rangle$ бесконечных циклических групп $\langle a_{\alpha+1} \rangle$. Доказательство будем вести индукцией по длине γ матрешки (1.1). При $\gamma = 1$ утверждение очевидно. Сделаем допущение о справедливости этого утверждения для всякого $\alpha < \gamma$.

В группе G выбираем произвольный элемент $g \neq 0$, и считаем, что $g \in N_\beta$, $g \notin \sum_{\sigma<\beta} N_\sigma = N_{\beta-1}$. В силу равенства $N_\beta = \langle a_\beta, N_{\beta-1} \rangle$, элемент g однозначно представляется в виде $g = g_1 + na\beta$, $g_1 \in N_{\beta-1}$. По индуктивному предположению, так как $\beta - 1 < \gamma$, элемент g однозначно записывается через $a_{\beta_i} : g_1 = n_1 a_{\beta_1} + \ldots + n_s a_{\beta_s} + n a_\beta$. Таким образом, доказана разложимость G в прямую сумму бесконечных циклических групп. Обратное очевидно. ⊠

Лемма 1.1.1.4. *[6, лемма 9.4] Если факторгруппа A/B является прямой суммой,*

$$A/b = \sum_i (A_i/B)$$

и подгруппа B служит прямым слагаемым для каждой группы A_i, скажем, $A_i = B \oplus C_i$, то подгруппа B служит прямым слагаемым для группы A,

$$A = B \oplus (\sum_i C_i).$$

Доказательство. Очевидно, подгруппа B и подгруппы C_i вместе порождают группу A. Предположим, что $b + c_1 + \ldots + c_n = 0$ для некоторых элементов $b \in B$ и $c_j \in C_j$ $(j = 1, \ldots, n)$. Переходя к факторгруппе по B, получаем $(c_1 + B) + \ldots + (c_n + B) = B$. Так как $c_j + B \in A_j/B$, то $c_1 + B = \ldots = c_n + B = B$. Следовательно, $c_j \in B$ для каждого j и, таким образом, $c_j \in B \cap C_j = 0$. Но тогда также $b = 0$. Следовательно, подгруппа, порожденная подгруппами B и C_i, является их прямой суммой. ⊠

Теорема 1.1.1.5. *[6, теорема 14.4] Если B — такая подгруппа группы A, что A/B — свободная группа, то B служит для A прямым слагаемым.*

Доказательство. В силу теоремы 1.1.1.2 группа A/B является прямой суммой бесконечных циклических групп. Следовательно, по лемме 1.1.1.4 достаточно проверить утверждение теоремы для случая, когда A/B — бесконечная циклическая группа, скажем $A/B = \langle a^* \rangle$. Выберем в группе A элемент $a \in a^*$. Тогда смежные классы na^* $(n = 0, \pm 1, \pm 2, \ldots)$ по подгруппе B будут иметь в качестве представителей элементы na из циклической подгруппы $\langle a \rangle$. Отсюда $A = B \oplus \langle a \rangle$. Действительно, очевидно, что $A = \langle B, a \rangle$. Кроме того, $B \cap \langle a \rangle = \{0\}$. ⊠

Теорема 1.1.1.6. *[1, теорема 7.1.3] или [6, теорема 14.5] Всякая ненулевая подгруппа свободной абелевой группы является свободной абелевой группой.*

Доказательство. Ввиду важности этой теоремы мы приведем два ее различных доказательства.

1. Пусть G — свободная абелева группа, A — ее нетривиальная подгруппа. В силу теоремы 1.1.1.3 в группе G существует трансфинитная матрешка (1.1) с циклическими бесконечными секциями. Тогда матрешка

$$0 = N_0 \cap A \leqslant N_1 \cap A \leqslant \ldots \leqslant N_\alpha \cap A \leqslant \ldots \leqslant N_\gamma \cap A = A \qquad (1.2)$$

является трансфинитной матрешкой для A, все секции которой либо тривиальны, либо бесконечные циклические. Выбросив все тривиальные секции, получим трансфинитную матрешку для A, все секции которой бесконечные циклические. Таким образом, по той же теореме 1.1.1.3 группа A является свободной абелевой группой.

2. Пусть $F = \sum_{i\in I}\langle a_i\rangle$ — свободная группа. Можно считать, что на множестве I задан некоторый частичный порядок. Пусть, кроме того, I — множество порядковых чисел, меньших некоторого порядкового числа τ. Для $\sigma < \tau$ положим $F_\sigma = \sum_{\rho<\sigma}\langle a_\rho\rangle$. Если G — подгруппа группы F, то положим $G_\sigma = G \cap F_\sigma$. Очевидно, $G_\sigma = G_{\sigma+1} \cap F_\sigma$, так что $G_{\sigma+1}/G_\sigma \cong (G_{\sigma+1} + F_\sigma)/F_\sigma$. Последняя факторгруппа является подгруппой группы $F_{\sigma+1}/F_\sigma \cong \langle a_\sigma\rangle$, поэтому или $G_{\sigma+1} = G_\sigma$, или $G_{\sigma+1}/G_\sigma$ — бесконечная циклическая группа. По теореме 14.4, $G_{\sigma+1} = G_\sigma \oplus \langle b_\sigma\rangle$ для некоторого $b_\sigma \in G_{\sigma+1}$ (если $G_{\sigma+1} = g_\sigma$, то $b_\sigma = 0$). Отсюда следует, что элементы b_σ порождают прямую сумму $\sum\langle b_\sigma\rangle$. Она должна совпадать с группой G, так как G — объединение подгрупп G_σ. ⊠

§2 Линейная независимость и ранг

Существуют два неэквивалентных подхода к линейной независимости в абелевых группах и мы приведем их оба.

Определение 1.1.2.1. [1, стр. 83] Конечное множество элементов $g_1, \dots, g_k$ абелевой группы G называется *линейно зависимым*, если найдутся такие целые числа $n_1, \dots, n_k$, не все равные нулю, что $\sum_{i=1}^{k} n_i g_i = 0$. Произвольная система элементов называется *линейно зависимой*, если линейно зависима ее некоторая конечная подсистема. По лемме Цорна, всякую линейно независимую систему элементов можно расширить до *максимальной*, т. е., не включаемой ни в какую большую.

Теорема 1.1.2.2. *[1, теорема 7.2.1] Для всякой абелевой группы G мощности всех ее максимальных линейно независимых систем одинаковы и либо являются некоторым натуральным числом, либо совпадают с бесконечной мощностью $|G : T(G)|$, где $T(G)$ — периодическая часть группы G.*

Доказательство. Ясно, что система $\overline{a}_1, \dots, \overline{a}_n$ линейно независима в $G/G(T)$ тогда и только тогда, когда система $a_1, \dots, a_n$ линейно независима в G. Следовательно, можно считать, что группа G без кручения.

Покажем, что если G обладает конечной максимальной линейно независимой системой A, то любая другая максимальная линейно независимая система B тоже конечна и $|A| = |B|$. Очевидно,что найдется такая конечная подсистема $B_0 \subseteq B$ и такие целые числа $n \neq 0$, $m \neq 0$; $n_{a,b}$; $m_{b,a}$, что $na = \sum_{b\in B_0} n_{a,b} b$ для всех $a \in A$ и $mb = \sum_{a\in A} m_{b,a} a$ для всех $b \in B_0$. Если $N = (n_{a,b})$, $M = (m_{b,a})$, то очевидно, MN и NM — скалярные матрицы степеней $|A|$ и $|B_0|$ соответственно, с элементами mn по диагонали. Поскольку ранг произведения матриц не превосходит рангов сомножителей, то $|A| = |B_0|$. Но систему B_0 можно заменить на любую бóльшую конечную подсистему системы B. Следовательно, $|A| = |B|$.

Пусть, наконец, группа G не имеет кручения и всякая ее максимальная линейно независимая система элементов A бесконечна; покажем, что тогда $|A| = |G|$. В самом деле, для каждого $g \in G$ существует такое конечное подмножество $\{a_1, \dots, a_k\}$ элементов из A и такие ненулевые целые $n, n_1, \dots, n_k$, что $ng = \sum_{i=1}^{k} n_i a_i$. Так как группа G не имеет кручения, то g полностью определяется набором $\{a_1, \dots, a_k, n, n_1, \dots, n_k\}$. Так как множество A бесконечно, таких наборов существует не более $|A|$, а потому $|G| \leqslant |A|$. ⊠

Теорема 1.1.2.3. *[1, теорема 7.2.2] Ненулевая абелева группа без кручения имеет размерность 1 тогда и только тогда, когда она изоморфна подгруппе аддитивной группы рациональных чисел $\mathbb{Q}$.*

Доказательство. Очевидно, что размерность группы $\mathbb{Q}^+$ равна 1. Следовательно, размерность любой ее подгруппы также не превосходит 1.

Пусть A — абелева группа размерности 1 и g — ее некоторый ненулевой элемент. Тогда для любого элемента $h \in A$ существуют такие целые числа n и m, что $ng = mh$. Тогда отображение $h \longrightarrow \frac{n}{m}$ является искомым изоморфизмом. Нетрудно убедиться, что отображение задано корректно, сохраняет операцию и является биективным. $\boxtimes$

Определение 1.1.2.4. [6, стр. 102] Система $\{a_1, \ldots, a_k\}$ ненулевых элементов группы A называется *независимой*, если из равенства $n_1a_1 + \ldots + n_ka_k = 0$ $(n_i \in \mathbb{Z})$ всегда вытекает, что $n_1a_1 = \ldots = n_ka_k = 0$. Система элементов называется *зависимой*, если она не независима. Бесконечная система $L = \{a_i\}_{i\in I}$ элементов группы A называется *независимой*, если в L всякая конечная подсистема независима.

Лемма 1.1.2.5. *[6, лемма 16.1] Система $L = \{a_i\}_{i\in I}$ независима тогда и только тогда, когда подгруппа, ею порожденная, является прямой суммой циклических групп $\langle a_i\rangle$, $i \in I$.*

Доказательство. Если система L независима, то для любого $i \in I$ пересечение подгруппы $\langle a_i\rangle$ с подгруппой, порожденной всеми элементами a_j из L, где $j \neq i$, обязательно равно нулю. Следовательно, $\langle L\rangle$ — прямая сумма групп $\langle a_i\rangle$, $i \in I$. Обратно, если $\langle L\rangle = \sum_{i\in I}\langle a_i\rangle$, то 0 можно записать в виде $n_1a_{i_1} + \ldots + n_ka_{i_k} = 0$, где $i_1, \ldots, i_k$ — различные элементы из I, лишь тривиальным образом: $n_1a_{i_1} = \ldots = n_ka_{i_k} = 0$. Но это означает, что система L независима. $\boxtimes$

Определение 1.1.2.6. [6, стр. 102] Говорят, что элемент $g \in A$ *зависит* от подмножества L группы A, если существует *отношение зависимости* $0 \neq ng = n_1a_1 + \ldots + n_ka_k$, где $a_i \in L$, n, n_i — целые числа.

Определение 1.1.2.7. [6, стр. 102] Независимая система M элементов группы A называется *максимальной*, если в A не существует независимой системы, строго содержащей M. Таким образом, если $g \in A$, $g \neq 0$, то $\{M, g\}$ — уже не независимая система, и g зависит от M. Если K зависит от L, а L зависит от K, то системы L и K называются *эквивалентными*.

Ясно, что любые две максимальные независимые системы элементов группы A эквивалентны. По лемме Цорна всякую линейно независимую систему элементов группы A можно расширить до максимальной. Кроме того, можно считать, что система M содержит элементы только бесконечного порядка или порядка, равного некоторому простому числу. В самом деле, элемент a порядка $m = \prod_i p_i^{\alpha_i}$ можно заменить элементами $a_1, \ldots, a_k$, где $a_i = \frac{m}{p_i}a$, причем полученные при этом системы будут эквивалентны.

Определение 1.1.2.8. [6, стр. 103] Подгруппа E группы A называется *существенной*, если $E \cap B \neq 0$ для любой ненулевой подгруппы группы A. В этом случае говорят, что группа A есть *существенное расширение* группы E.

Лемма 1.1.2.9. *[6, лемма 16.2] Независимая система M элементов группы A максимальна тогда и только тогда, когда $\langle M\rangle$ — существенная подгруппа группы A. Всякая максимальная независимая система элементов существенной подгруппы группы A является максимальной независимой системой в A.*

Доказательство. Так как элемент $g \in A$ зависит от M тогда и только тогда, когда $\langle M\rangle \cap \langle g\rangle \neq 0$, то первая часть леммы очевидна. Если E — существенная подгруппа группы A и M — максимальная независимая система в E, то возьмем произвольный элемент $g \in A$, $g \neq 0$. Существует ненулевой элемент $h \in E \cap \langle g\rangle$, $h = mg$. Так как h зависит от M, то и g зависит. ⊠

Определение 1.1.2.10. [6, стр. 103] *Рангом* $r(A)$ группы A называется мощность ее максимальной независимой системы, содержащей только элементы бесконечного порядка или порядка, равного степени простого числа. Если мы ограничимся элементами бесконечного порядка группы A, т. е. выберем независимую систему, состоящую только из элементов бесконечного порядка и максимальную по отношению к этому свойству, то мощность такой системы будет называться *рангом без кручения* $r_0(A)$ группы A. Аналогично определяется *p-ранг* $r_p(A)$ группы A: вместо элементов бесконечного порядка используются элементы, порядки которых являются степенями фиксированного простого числа p.

Из этих определений ясно, что для всякой группы A справедливо следующее равенство:

$$r(A) = r_0(A) + \sum_p r_p(A), \tag{1.3}$$

где p пробегает все простые числа. Очевидно, условие $r(A) = 0$ равносильно тому, что $A = 0$.

Теорема 1.1.2.11. *[6, теорема 16.3] Ранги $r(A)$, $r_0(A)$, $r_p(A)$ группы A являются инвариантами этой группы.*

Доказательство. В силу формулы (1.3) достаточно проверить инвариантность $r_0(A)$ и $r_p(A)$. Инвариантность $r_0(A)$ следует из теоремы 1.1.2.2.

Обратимся к рангам $r_p(A)$. Ясно, что $r_p(A) = r(T_p)$, где T_p есть p-компонента группы A. Следовательно, нам нужно только доказать инвариантность ранга $r(A)$ для p-группы A.

Если A есть p-группа и $S(A) = A[p]$ — ее цоколь, то $r(A) = r(S(A))$. В самом деле, система элементов $\{a_1, \dots, a_k\}$ группы A независима тогда и только тогда, когда независима система $\{p^{m_1-1}a_1, \dots, r^{m_k-1}a_k\}$, где $m_i = |a_i|$. Поэтому нужно установить только однозначную определенность $r(S(A))$. Так как $S(A)$ естественным образом является векторным пространством над полем F_p из p элементов и независимость в нашем смысле совпадает с независимостью в векторном пространстве, то получается, что $r(S(A))$ — это в точности размерность векторного пространства $S(A)$, а она определяется однозначно. ⊠

§3 Конечно порожденные абелевы группы

Определение 1.1.3.1. [1, стр. 24] Группа G называется *конечно порожденной*, если существует такой набор $a_1, \dots, a_n$ элементов, что $\langle a_1, \dots, a_n\rangle = G$. Ясно, что любая конечно порожденная абелева группа является конечно мерной.

Теорема 1.1.3.2. *[1, теорема 7.2.4] Пусть G — конечно мерная абелева группа без кручения и φ — ее изоморфизм в себя. Тогда индекс $|G : G\varphi|$ конечен.*

Доказательство. Зафиксируем в G какую-нибудь максимальную линейно независимую систему элементов $a_1, \dots, a_n$. Отображению φ естественным образом можно сопоставить матрицу $(a_{ij}(\varphi))$ над полем $\mathbb{Q}$, полагая $a_i\varphi = \sum_{j=1}^n a_{ij}(\varphi)a_j$. Погрузив G с отмеченной в ней базой $a_1, \ldots, a_n$ в векторное пространство $\mathbb{Q}^n$, мы можем продолжить φ до линейного преобразования этого пространства. Умножим характеристический многочлен этого преобразования на общий знаменатель его коэффициентов, пусть f — получившийся при этом многочлен над $\mathbb{Z}$. По основному свойству характеристического многочлена, $f(\varphi) = 0$; а так как $\det\varphi \neq 0$, то $f(0) = m \neq 0$. Тогда $mG \leqslant G\varphi$. Пусть $m = p_1p_2 \ldots p_s$; где p_i — простые числа (возможно, с повторениями). Так как $G \leqslant \mathbb{Q}^n$, то $\mathrm{rank}G \leqslant n$ (имеется ввиду ранг системы векторов), и, следовательно, $|p_1 \ldots p_{i-1}G : p_1 \ldots p_iG| \leqslant p_i^n$. Действительно, любой вектор $v = \alpha_1a_1 + \ldots + \alpha_na_n$, где $v \in p_1 \ldots p_{i-1}G$ лежит в $p_1 \ldots p_iG$ тогда и только тогда, когда $\alpha_1 \equiv \ldots \equiv \alpha_n \equiv 0(\mathrm{mod}\ p_i)$. Таким образом, $|G : mG| \leqslant |G : G\varphi| \leqslant m^n < \infty$. ⊠

Теорема 1.1.3.3. *[1, теорема 8.1.1] Пусть F_n — свободная абелева группа конечной степени n, A — ее отличная от нуля подгруппа. Тогда группы F_n и A обладают соответственно базисами $f_1, \ldots, f_n$ и $a_1, \ldots, a_k$ такими, что $k \leqslant n$, $a_i = m_if_i$, $1 \leqslant i \leqslant k$ и m_{i+1} делится на m_i, $1 \leqslant i \leqslant k-1$.*

Доказательство. Пусть $F_n = \langle f_1' \rangle \oplus \ldots \oplus \langle f_n' \rangle$, $A = \langle a_1' \rangle \oplus \ldots \oplus \langle a_k \rangle$ и $a_i' = \sum_{j=1}^n m_{ij}f_j'$, $m_{ij} \in \mathbb{Z}$. Возникает матрица $M = (m_{ij})$. Будем называть *элементарными* следующие преобразования строк и солбцов целочисленной матрицы: а) перестановка двух строк (столбцов); б) прибавление к одной строке (столбцу) целочисленного кратного другой строки (столбца); в) умножение строки (столбца) на -1. Тогда элементарными преобразованиями можно привести матрицу M к виду

$$\begin{pmatrix} m_1 \ldots\ 0\ 0 \ldots 0 \\ \ddots \\ 0\ \ldots m_k 0 \ldots 0 \end{pmatrix},$$

где $m_i | m_{i+1}$. Ясно, что элементарные преобразования строк соответствуют переходу к другой базе группы A, а элементарные преобразования столбцов — к другой базе группы F_n. ⊠

Теорема 1.1.3.4. *[1, теорема 8.1.2] Всякая конечно порожденная абелева группа G разлагается в прямую сумму циклических подгрупп. Более точно, G разлагается в прямую сумму бесконечных циклических и примарных циклических групп, причем количество бесконечных циклических слагаемых и набор порядков примарных циклических слагаемых в любом таком разложении одни и те же, т. е. являются инвариантами группы G.*

Доказательство. По условию, группа $G \cong F_n/A$. Согласно теореме 1.1.3.3 в группах F_n и A существуют такие базы $f_1, \ldots, f_n$ и $a_1, \ldots, a_k$, что $a_i = m_if_i$; $1 \leqslant i \leqslant k$ и $m_i | m_{i+1}$. Покажем, что $F_n/A = \sum_{i=1}^n \langle f_i + A \rangle$. Прежде всего ясно, что F_n/A порождается этими подгруппами. Далее, пусть нуль факторгруппы F_n/A имеет запись $A = l_1f_1 + \ldots + l_nf_n + A$, $l_i \in \mathbb{Z}$. Тогда $l_1f_1 + \ldots + l_nf_n = a \in A$. С другой стороны, выражая элемент a через базу $a_1, \ldots, a_k$ подгруппы A и учитывая равенства $a_i = m_if_i$, приходим к соотношению $l_1f_1 + \ldots + l_nf_n = s_1a_1 + \ldots + s_ka_k = s_1m_1f_1 + \ldots + s_km_kf_k$, $s_i \in \mathbb{Z}$. Ввиду однозначности записи элементов через свободные порождающие f_i получаем $l_i = s_im_i$; $1 \leqslant i \leqslant k$, $l_j = 0$, $k < j \leqslant n$. Но это означает, что каждый из элементов l_if_i принадлежит A. Тем самым доказана однозначность представления нуля в виде суммы элементов подгрупп $\langle f_i + A \rangle$ и, значит, разложимость группы G в прямую сумму циклических слагаемых.

Ясно, что количество бесконечных циклических слагаемых совпадает с $r_0(G)$, а количество примарных — с $r_p(G)$. Поэтому в силу теоремы 1.1.2.11 числа, о которых говорится в теореме, являются инвариантами группы G. ⊠

§4 Прямые суммы циклических p-групп

Теорема 1.1.4.1. *[6, теорема 17.1] p-группа A является прямой суммой циклических групп тогда и только тогда, когда A есть объединение возрастающей последовательности подгрупп*

$$A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n \subseteq \ldots, \bigcup_{i=1}^{\infty} A_n = A, \tag{1.4}$$

где высоты отличных от нуля элементов, входящих в A_n, меньше фиксированного числа k_n.

Доказательство. Если A — прямая сумма циклических групп, то для каждого n соберем в ее разложении циклические прямые слагаемые одного и того же порядка p^n и обозначим их прямую сумму через B_n. Очевидно, подгруппы $A_n = B_1 \oplus \ldots \oplus B_n$ будут удовлетворять условию теоремы при $k_n = n$.

Для доказательства достаточности предположим, что подгруппы A_n группы A удовлетворяют нужным условиям. Так как мы можем добавить 0 в начало цепи (1.4) и так как можно повторять одно и то же A_n конечное число раз, то, очевидно, без ограничения общности можно предположить, что $k_n = n$, т. е. что $A_n \cap p^n A = 0$ для каждого n. Рассмотрим все цепи

$$C_1 \subseteq C_2 \subseteq \ \ldots \subseteq C_n \subseteq \ldots$$

подгрупп C_n группы A, для которых

$$1) A_n \subseteq C_n \qquad \text{и} \qquad 2) C_n \cap p^n A = 0$$

при всех n. Будем говорить, что цепь подгрупп C_n меньше или равна цепи подгрупп B_n, если $C_n \subseteq B_n$ для любого n. Тогда множество всех цепей со свойствами 1) и 2) окажется индуктивным. Действительно, если $\mathfrak{C} = \mathcal{C}_1 \leqslant \ldots$ — некоторая цепь в множестве цепей (немного коряво, но что поделать), то сверху эту цепь можно ограничить цепью, элементы которой получаются как $B_n = \bigcup_{\mathcal{C} \in \mathfrak{C}, C_n \in \mathcal{C}} C_n$. Из леммы Цорна следует, что существует цепь $G_1 \subseteq G_2 \subseteq \ldots \subseteq G_n \subseteq \ldots$ со свойствами 1) и 2), максимальная в рассматриваемом смысле. Очевидно, $\bigcup_{n=1}^{\infty} G_n = A$.

Выберем для каждого n максимальную независимую систему L_n элементов подгруппы $G_n[p] \cap p^{n-1}A$ и обозначим через L объединение всех множеств $L_n (n = 1, 2, \ldots)$. Для любого $c_i \in L$ и $m_i = h(c_i)$ выберем такой элемент $a_i \in A$, что $p^{m_i} a_i = c_i$. Мы утверждаем, что подгруппа $A' = \langle \ldots, a_i, \ldots \rangle = \sum_i \langle a_i \rangle$ совпадает с A.

Во-первых, покажем, что $\langle L \rangle = A[p]$. Поскольку в элементарной абелевой p-группе всякая максимальная независимая система служит базисом (см. теорему 1.1.2.11), $\langle L_n \rangle = G_n[p] \cap p^{n-1}A$. Так как все отличные от нуля элементы из $\langle L_n \rangle$ имеют высоту $n-1$, то подгруппы $\langle L_n \rangle$ порождают подгруппу, являющуюся их прямой суммой, т. е. $\langle L \rangle = \sum_n \langle L_n \rangle$. Предположим, что каждый элемент $a \in A[p]$, лежащий в G_r, принадлежит $\langle L \rangle$ [для $r = 1$ это, очевидно, выполнено], и пусть $b \in G_{r+1}[p] \setminus G_r$. Из $b \notin G_r$ следует, что $\langle G_r, b \rangle = \cap p^r A \neq 0$. Пусть $0 \neq g + kb = c \in p^r A$, где $g \in G_r$. Можно считать, что $k = 1$ [так как иначе можем умножить элемент на k', где $kk' \equiv 1 (\mathrm{mod}\ p)$]. Здесь $c \in G_{r+1}$ и $h(c) \geqslant r$; поэтому, в силу условия 2) $|C| = p$ и $h(C) = r$. Отсюда $c \in \langle L_{r+1} \rangle$. Далее из равенства $pg = pc - pb = 0$, включения $g \in G_r$ и индуктивного предположения получаем , что $g \in \langle L \rangle$, откуда $b = c - g \in \langle L \rangle$ и $\langle L \rangle = A[p]$.

Предположим, что уже доказано, что всякий элемент $a \in A$ порядка $\leqslant p^n$ принадлежит A', и пусть элемент $b \in A$ имеет порядок p^{n+1}, где $n \geqslant 1$. Как показано в предыдущем абзаце, $p^n b \in \langle L \rangle$ и, следовательно, $p^n b = m_1 c_1 + \ldots + m_k c_k$ для некоторых $c_i \in L$. Пусть элементы $c_1, \ldots, c_j$ имеют высоту $\geqslant n$, а элементы $c_{j+1}, \ldots, c_k$ — высоту $\leqslant n-1$. Если записать $m_i c_i = p^n m_i' a_i$ для $i = 1, \ldots, j$, то получится

$$p^n(b - m_1' a_1 - \ldots - m_j' a_j) = m_{j+1} c_{j+1} + \ldots + m_k c_k \in G_{n-1}.$$

Из условия 2) следует, что элемент $b - m_1' a_1 - \ldots - m_j' a_j$ имеет порядок $\leqslant p^n$, т. е. лежит в A', откуда $b \in A'$. ⊠

Из этой теоремы легко получаются следующие два важных следствия.

Теорема 1.1.4.2. *([1, теорема 10.1.5] или [6, теорема 17.2]) Ограниченная группа является прямой суммой циклических групп.*

Доказательство. Если A — ограниченная группа, то ее p-компоненты — тоже ограниченные группы.Если в цепи (1.4) выбрать одну и ту же p-компоненту группы A, то из теоремы 1.1.4.1 получится, что эта p-компонента — прямая сумма циклических групп ⊠

Теорема 1.1.4.3. *([1, теорема 10.1.14] или [6, теорема 17.3]) Счетная p-группа является прямой суммой циклических групп тогда и только тогда, когда она не содержит отличных от нуля элементов бесконечной высоты.*

Доказательство. Необходимость очевидна, проверим достаточность. Пусть A — счетная p-группа без элементов бесконечной высоты и $\{a_1, \ldots, a_n, \ldots\}$ — некоторая ее система образующих. Тогда группа A является объединением возрастающей последовательности своих конечных подгрупп $A_n = \langle a_1, \ldots, a_n \rangle$ $(n = 1, 2, \ldots)$, высоты элементов в которых тривиальным образом ограничены. Остается применить теорему 1.1.4.1. ⊠

1.2 Делимые группы и сервантные подгруппы

§1 Делимость

Мы скажем, что элемент a группы A *делится* на натуральное число n (это обозначается $n|a$), если уравнение

$$nx = a, (a \in A)$$

имеет решение в группе A.

Группа D называется *делимой*, если $n|a$ для всех $a \in D$ и всех натуральных n. Группа D называется *p-делимой*, если $p^k D = d$ для любого натурального числа k

Далее мы объединим несколько свойств делимых групп в одном предложении.

Предложение 1.2.1.1. *[6, стр. 118]*

1. *Группа является делимой тогда и только тогда, когда она p-делима для любого простого p.*

2. *p-группа делима тогда и только тогда, когда она p-делима.*

3. *Если в p-группе D всякий элемент порядка p имеет бесконечную высоту, то D — делимая группа.*

4. *Любой эпиморфный образ делимой группы является делимой группой.*

5. *Прямая сумма и декартова сумма являются делимыми группами тогда и только тогда, когда каждая компонента — делимая группа.*

6. *Если D_i $(i \in I)$ — делимые подгруппы группы A, то и $\langle D_i \rangle$ — делимая подгруппа.*

Доказательство. Данное предложение доказывается непосредственной проверкой с помощью соответствующих определений. ⊠

§2 Инъективные группы

Группа D называется *инъективной*, если для любой диаграммы

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\xi"'] & B \arrow[dl, "\eta"] \\ & D & \end{tikzcd} \tag{1.5}$$

с точной строкой существует гомоморфизм $\eta : B \longrightarrow D$, превращающий эту диаграмму в коммутативную. Если отождествить A и A^α, то инъективность группы D можно интерпретировать как возможность продолжить любой гомоморфизм $\xi : A \longrightarrow D$ до гомоморфизма группы B, содержащей A, в группу D.

Теорема 1.2.2.1. *[6, теорема 21.1] Делимые группы инъективны.*

Доказательство. Пусть D — делимая группа, и пусть дана диаграмма (1.5), где группу A мы будем рассматривать как подгруппу группы B. Рассмотрим все группы G, лежащие между A и B, $A \leqslant G \leqslant B$, для которых существует продолжение $\theta : G \longrightarrow D$ гомоморфизма ξ. Частично упорядочим множество пар (G, θ), полагая $(G, \theta) \leqslant (G', \theta')$, если $G \leqslant G'$ и θ — ограничение морфизма $\theta' : g' \longrightarrow D$ на G. Множество этих пар непусто, так как ему принадлежит пара $(A\xi)$, и индуктивно, так как всякая цепь (G_i, θ_i), $(i \in I)$ имеет верхнюю грань, а именно (G_θ), где $G = \bigcup_i G_i$, а $\theta : G \longrightarrow D$ совпадает с θ_i на G_i. По лемме Цорна в рассматриваемом множестве существует максимальная пара (G_0, θ_0). Если $G_0 \neq B$ и для элемента $b \in B \setminus G_0$ имеет место включение $nb \in G_0$ при некотором $n > 0$, то возьмем минимальное n с этим свойством и предположим, что $nb = g \in G_0$. В силу делимости группы D для некоторого $x \in D$ имеем $nx = \theta_0 g$. Легко проверить, что отображение

$$c + rb \mapsto \theta_0 c + rx (c \in G_0, 0 \leqslant r < n) \tag{1.6}$$

является гомоморфизмом группы $\langle G_0, b \rangle$ в группу D. Если $nb \notin G_0$ при $n \neq 0$, то формула (1.6) дает гомоморфизм группы $\langle G_0, b \rangle$ в группу D при произвольном $x \in D$ [на r ограничений не накладывается]. Следовательно, предположение, что $G_0 \neq B$ противоречит максимальности пары (G_0, θ_0), т. е. $G_0 = B$ и $\theta_0 = \eta$. ⊠

Предложение 1.2.2.2. *[6, предложение 9.2] Для подгруппы B группы A эквивалентны следующие условия [$\rho : B \longrightarrow A$ — вложение]:*

1. *B — прямое слагаемое группы A;*

2. *существует гомоморфизм $\pi : A \longrightarrow B$ такой, что $\rho\pi = 1_D$;*

3. *если*

$$\begin{tikzcd}
0 \arrow[r] & U \arrow[r, "\gamma"] \arrow[d, "\beta"'] & V \arrow[d, "\alpha"] \arrow[dl] \\
0 \arrow[r] & B \arrow[r, "\rho"] & A
\end{tikzcd}$$

— коммутативная диаграмма с точными строками, то существует такой гомоморфизм $\varphi : V \longrightarrow B$, что верхний треугольник коммутативен.

Доказательство. Предполагая выполненным условие 1, докажем сначала, что выполнено 3. Если справедливы предположения пункта 3 и $\pi : A \longrightarrow B$ — проекция, то для $\varphi = \alpha\pi$ имеем $\gamma\varphi = \gamma\alpha\pi = \beta\rho\pi = \beta$. Предположим теперь, что выполнено 3, и возьмем $U = B$, $V = A$, $\gamma = \rho$, $\alpha = 1$ и $\beta = 1_B$. Тогда сразу получаем 2. Наконец, если имеет место 2, то π — проекция группы A на B. Отображение $\theta = 1_A - \pi$ является эндоморфизмом группы A. Кроме того, $\pi + \theta = 1_A$, следовательно, $A = A^{1_A} = A^\pi + A^\theta$. Так как $A^\pi = B$ и $B \cap A^\theta = 0$, то $A = B \oplus A^\theta$. ⊠

Теорема 1.2.2.3. *[6, теорема 21.2] Делимая подгруппа D группы A служит для A прямым слагаемым, т. е. $A = D \oplus C$ для некоторой подгруппы C группы A. Эту подгруппу C можно выбрать так, что она будет содержать заранее заданную подгруппу B группы A, для которой $D \cap B = 0$.*

Доказательство. По теореме 1.6 для естественного вложения $\alpha : D \longrightarrow A$ и тождественного отображения $1_D : D \longrightarrow D$ существует такой гомоморфизм $\eta A \longrightarrow D$, что $\alpha\eta = 1_D$. Предложение 1.2.2.2 показывает, что $A = D \oplus \operatorname{Ker} \eta$.

Если для подгруппы $B \leqslant A$ имеет место равенство $D \cap B = 0$, то $D + B = D \oplus B$ и существует гомоморфизм $\xi : D \oplus B \longrightarrow D$, совпадающий с тождественным на D и нулевой на B. Если в предыдущем абзаце заменить 1_D на ξ, то получится , что $A = D \oplus \operatorname{Ker} \ \eta$, где $B \leqslant \operatorname{Ker} \ \eta$. ⊠

Теорема 1.2.2.4. *[6, теорема 21.3] Всякая группа A является прямой суммой делимой группы D и редуцированной группы C, $A = D \oplus C$. Подгруппа D группы A здесь определена однозначно, подгруппа C — однозначно с точностью до изоморфизма.*

Доказательство. Утверждение очевидно, поскольку сумма двух делимых групп вновь является делимой группой. ⊠

§3 Системы уравнений

Определение 1.2.3.1. [6, стр. 122] *Системой уравнений* над группой A называется совокупность уравнений

$$\sum_{j \in J} n_{ij} x_j = a_i (a_i \in A, i \in I), \tag{1.7}$$

где n_{ij} — целые числа, причем если i фиксированно, то $n_{ij} = 0$ для всех j, кроме, самое большее, конечного числа. Здесь $\{x_j\}_{j \in J}$ — множество неизвестных, а I, J — множества индексов произвольной мощности. Множество $x_j = g_\in A$ $(j \in J)$ называется *решением* системы (1.7), если система (1.7) удовлетворяется при замене x_j элементами g_j. Очевидно, что решение можно рассматривать как элемент $(\ldots, g_j, \ldots)$ декартовой суммы A^J.

Левую часть системы уравнений (1.7) можно рассматривать как элемент свободной группы X, построенной на множестве неизвестных $\{x_j\}_{j\in J}$. Пусть Y — подгруппа группы X, порожденная всеми левыми частями $f_i(x) = \sum_j n_{ij}x_j$ уравнений системы (1.7). Соответствие

$$f_i(x) \longrightarrow a_i(i \in I) \tag{1.8}$$

порождает гомоморфизм $\eta : Y \longrightarrow A$ тогда и только тогда, когда всякая линейная комбинация элементов $f_i(x)$, равная нулю, отображается в 0. В соответствии с этим мы будем называть систему (1.7) *согласованной*, если отображение (1.8) продолжается до гомоморфизма $\eta : Y \longrightarrow A$.

Согласованную систему (1.7) удобно рассматривать как пару (Y, η), где Y — подгруппа свободной группы X, множество свободных образующих которой совпадает с множеством неизвестных, а η — гомоморфизм группы Y в группу A.

Ясно, что $x_j = g_j$ $(j \in J)$ является решением системы (1.7) тогда и только тогда, когда отображение

$$x_j \longrightarrow g_j(j \in J) \tag{1.9}$$

продолжается до гомоморфизма $\chi : X \longrightarrow A$, ограничение которого на Y дает η. Поэтому решение системы (Y, η) можно обозначить через $(X\chi)$.

Теорема 1.2.3.2. *[6, теорема 22.1] Всякая согласованная система уравнений над группой A допускает решение в A тогда и только тогда, когда A — делимая группа.*

Доказательство. Так как одно уравнение $nx = a$, где $n \neq 0$, является согласованной системой, то необходимость очевидна. Переходя к доказательству достаточности, возьмем согласованную систему уравнений (Y, η) над делимой группой A. По теореме 1.2.2.1 гомоморфизм η можно продолжить до гомоморфизма $\chi : X \longrightarrow A$. Следовательно, решение существует. ⊠

Следствие 1.2.3.3. *[6, следствие 22.2] Система уравнений над делимой группой D разрешима в D тогда и только тогда, когда каждая ее конечная подсистема имеет решение в D.*

Предложение 1.2.3.4. *[6, предложение 22.3] Подгруппа B группы A служит для A прямым слагаемым тогда и только тогда, когда всякая система уравнений над B, имеющая решение в группе A, имеет решение и в B.*

Доказательство. Если B — прямое слагаемое группы A, т. е. $A = B \oplus C$, то компоненты в B решения из A, очевидно, удовлетворяют системе уравнений над B.

Обратно, предположим, что всякая система уравнений над B, имеющая решение в группе A, имеет решение и в B. В каждом смежном классе u группы A по подгруппе B выберем по представителю $a(u) \in A$ и рассмотрим систему уравнений

$$x_u + x_v - x_{u+v} = a(u) + a(v) - a(u+v) \in B \text{ для всех } u, v \in A/B.$$

По предположению она имеет решение $x_u = b(u) \in B$. Тогда $a(u) - b(u)$ — представители смежных классов $u \in A/B$, образующие подгруппу в группе A. Следовательно, B служит для A прямым слагаемым. ⊠

§4 Строение делимых групп

Теорема 1.2.4.1. *[6, теорема 23.1] Всякая делимая группа D является прямой суммой квазициклических групп и групп, изоморфных полной рациональной группе. Мощности множеств компонент $\mathbb{Z}(p^\infty)$ (для каждого p) и $\mathbb{Q}$ составляют полную и независимую систему инвариантов группы D.*

Доказательство. Очевидно, что периодическая часть T группы D — делимая группа. Из теоремы 1.2.2.3 следует, что $D = T \oplus E$, где E — группа без кручения, очевидно, снова делимая. Если p-компоненту группы Tобозначить через T_p, то получим

$$D = \sum_p T_p \oplus E,$$

и достаточно показать, что T_p — прямая сумма групп $\mathbb{Z}(P^\infty)$, а E — прямая сумма групп $\mathbb{Q}$.

Выберем в цоколе группы T_p максимальную независимую систему элементов $\{a_i\}_{i\in I}$. В силу делимости в группе T_p для каждого i существует такая бесконечная последовательность элементов $a_{i1}, \ldots, a_{in}, \ldots$, что $a_{i1} = a_i$, $pa_{1,n+1} = a_{in}$, $n = 1, 2, \ldots$. Отсюда мы заключаем, что каждый элемент a_i может быть вложен в подгруппу $A_i \cong \mathbb{Z}(p^\infty)$ группы T_p, именно, $A_i = \langle a_{i1}, \ldots, a_{in}, \ldots \rangle$. Так как $\langle a_1 \rangle$ — цоколь группы A_i и элементы a_i $(i \in I)$ независимы, то подгруппы A_i порождают в группе T_p подгруппу A, являющуюся их прямой суммой: $A = \sum_{i\in I} A_i$. Группа A является делимой подгруппой, т. е. прямым слагаемым группы T_p. Но A содержит цоколь группы T_p, поэтому $A = T_p$, и T_p — прямая сумма групп $\mathbb{Z}(p^\infty)$.

Выберем теперь максимальную независимую систему элементов $\{b_j\}_{j\in J}$ в группе E. Так как E — делимая группа без кручения, то при любом положительном $n \in \mathbb{N}$ существует ровно один элемент $x \in E$, для которого $nx = b_j$. Это означает, что каждый элемент b_j может быть вложен в подгруппу $B_j \cong \mathbb{Q}$ группы E. Так как $\{b_j\}$ — независимая система элементов, то подгруппы B_j порождают в E подгруппу B, являющуюся их прямой суммой:$B = \sum_{j\in J} B_j$. Эта подгруппа —прямое слагаемое группы E, содержащее максимальную независимую систему элементов из E, поэтому $B = E$, и E — прямая сумма групп, изоморфных группе $\mathbb{Q}$.

Число прямых слагаемых, изоморфных $\mathbb{Z}(p^\infty)$ или $\mathbb{Q}$, в разложении группы D в прямую сумму групп $\mathbb{Z}(p^\infty)$ и $\mathbb{Q}$, очевидно, равно соответственно рангу $r_p(D)$ или рангу $r_0(D)$. По теореме 1.1.2.11 эти ранги однозначно определяются группой D. Они образуют полную систему инвариантов, так как если даны $r_p(D)$ и $r_0(D)$, то мы можем по ним однозначно восстановить группу D, взяв прямую сумму $r_p(D)$ групп $\mathbb{Z}(p^\infty)$, для каждого p и $r_0(D)$ групп, изоморфных $\mathbb{Q}$. Независимость этих инвариантов очевидна. ⊠

§5 Делимая оболочка

Теорема 1.2.5.1. *[6, теорема 24.1] Всякую группу можно вложить в качестве подгруппы в делимую группу.*

Доказательство. Бесконечную циклическую группу $\mathbb{Z}$, очевидно, можно вложить в делимую группу, именно в группу $\mathbb{Q}$. Следовательно, всякая свободная группа F вложима в прямую сумму групп, изоморфных $\mathbb{Q}$, т. е. в делимую группу. Если A — произвольная группа, то можно написать $A \cong F/N$, где F — соответствующая свободная группа. Если вложить группу F в делимую группу D, то группа A окажется изоморфной подгруппе F/N делимой группы D/N. ⊠

Далее мы улучшим эту теорему, установив существование минимальной делимой группы, содержащей заданную группу.

Лемма 1.2.5.2. *[6, лемма 24.2] Подгруппа B группы A является существенной тогда и только тогда, когда гомоморфизм $\alpha : A \longrightarrow G$ в произвольную группу G обязательно является мономорфизмом, если $\alpha|_B : B \longrightarrow G$ — мономорфизм.*

Доказательство. Если B — существенная подгруппа группы A и $\alpha|_B$ — мономорфизм, то $\mathrm{Ker}\ \alpha \cap B = \mathrm{Ker}\ (\alpha|_B) = 0$, откуда $\mathrm{Ker}\ \alpha = 0$. Обратно, если B — не существенная подгруппа и подгруппа $C \neq 0$ группы A такова, что $C \cap B = 0$, то канонический эпиморфизм $\alpha : A \longrightarrow A/C$ не является мономорфизмом, хотя $\alpha|_B$ — мономорфизм. ⊠

Определение 1.2.5.3. [6, стр. 127] Для заданной группы A делимая группа E, содержащая A называется *минимальной делимой группой*, если в E нет собственных делимых подгрупп, содержащих A.

Лемма 1.2.5.4. *[6, лемма 24.3] Делимая группа E, содержащая группу A, является минимальной делимой группой тогда и только тогда, когда A — существенная подгруппа группы E.*

Доказательство. Если E — не минимальная делимая группа и D — собственная делимая подгруппа группы E, содержащая A, то можно написать $E = D \oplus C$, где $C \neq 0$. Так как $A \cap C \subseteq D \cap C = 0$, то группа A не является существенной подгруппой группы E. Обратно, если A — не существенная подгруппа группы E, то в E существует такая циклическая подгруппа $C = \langle c \rangle \neq 0$, что $A \cap C = 0$. Без ограничения общности можно предположить, что $|c| = \infty$, или $|c| = p^k$. Тогда подгруппу C можно вложить в такую подгруппу B группы E, что $B \cong \mathbb{Q}$ или $B \cong \mathbb{Z}(p^\infty)$. По теореме 1.2.2.3 $E = D \oplus B$ для некоторой подгруппы D, содержащей A. Следовательно, группа E не минимальная. ⊠

Теорема 1.2.5.5. *[6, теорема 24.4] Всякая делимая группа, подгруппой которой является группа A, содержит минимальную делимую группу, содержащую A. Любые две минимальные делимые группы, содержащие A, изоморфны над A.*

Доказательство. Пусть D — делимая группа, содержащая группу A. Делимые подгруппы группы D, имеющие с A нулевое пересечение, образуют индуктивное множество, поэтому в этом множестве существует максимальный член M. По теореме 1.2.2.3 имеем $D = M \oplus E$, где $A \subseteq E$. Очевидно, E — делимая группа, а из максимальности подгруппы M следует, что E не может содержать собственных прямых слагаемых и, таким образом, собственных делимых подгрупп, все еще содержащих A. Следовательно, E – минимальная делимая подгруппа, содержащая A.

Если E_1 и E_2 — две минимальные делимые группы, содержащие группу A, то в силу теоремы 1.2.2.1 тождественный автоморфизм 1_A группы A можно продолжить до гомоморфизма $\eta : E_1 \longrightarrow E_2$. Так как ηE_1 — делимая группа, содержащая A, то η — эпиморфизм. По лемме 1.2.5.4 группа A — существенная подгруппа группы E_1, а так как $\eta|_A = 1_A$, то из леммы 1.2.5.2 следует, что η — мономорфизм. Следовательно, η является изоморфизмом между группами E_1 и E_2, оставляющим каждый элемент группы A на месте. ⊠

Определение 1.2.5.6. [6, стр. 128] Минимальную делимую группу E, содержащую группу A, мы вправе называть *делимой оболочкой* (или *инъективной оболочкой*) группы A. Очевидно, из леммы 1.2.5.4 следует, что $r_0(A) = r_0(E)$ и $r_p(A) = r_p(E)$ для любого простого числа p.

Результаты данного раздела можно обобщить в одной теореме.

Теорема 1.2.5.7. *[6, теорема 24.5] Для группы D эквивалентны следующие условия:*

1) D — делимая группа;

2) D — инъективная группа;

3) D служит прямым слагаемым для всякой содержащей ее группы.

Доказательство. Нужно проверить лишь 3) $\Rightarrow$ 1). Вложим группу D в делимую группу E. Из условия 3) вытекает, что D служит для E прямым слагаемым. Следовательно, имеет место условие 1). $\boxtimes$

§6 Сервантность

Определение 1.2.6.1. [6, стр. 135] Подгруппа G группы A называется *сервантной*, если уравнение $nx = g \in G$, имеющее решение во всей группе A, имеет решение и в G. Иными словами, G сервантна в A, если

$$nG = G \cap nA \text{ для любого } n \in \mathbb{Z}. \tag{1.10}$$

Подгруппа G группы A называется *p-сервантной* (p — простое число), если

$$p^n G = G \cap p^n A \text{ для любого } n \in \mathbb{Z}. \tag{1.11}$$

Приведем некоторые основные факты, касающиеся сервантных подгрупп.

а) Всякое прямое слагаемое является сервантной подгруппой, 0 и A — (тривиальные) сервантные подгруппы.

б) Периодическая часть смешанной группы и ее p-компоненты являются сервантными подгруппами (но не обязательно прямыми слагаемыми).

в) Подгруппы групп $\mathbb{Q}$ и $\mathbb{Z}(p^\infty)$ не имеют нетривиальных сервантных подгрупп.

г) Если A/G — группа без кручения, то G — сервантная подгруппа группы A. В самом деле, из $na = g \in G$ ($n \neq 0$) для $a \in A$ вытекает $a \in G$.

д) В группах без кручения пересечения сервантных подгрупп снова сервантны.

Действительно, уравнение $nx = g$ в группе без кручения имеет единственное решение. Поэтому, если все подгруппы сервантны, то каждая из них содержит это единственное решение x.

В группе без кручения A для всякого подмножества S существует минимальная сервантная подгруппа, содержащая S. Эта подгруппа называется *сервантной подгруппой, порожденной множеством S*, $\langle S \rangle_*$.

е) Сервантность является индуктивным свойством.

Пусть $G_1 \subseteq G_2 \subseteq \ldots$ — цепочка сервантных подгрупп, тогда их объединение, очевидно, является сервантной подгруппой.

ж) p-сервантная p-подгруппа всегда сервантна.

з) Если A есть p-группа и элементы порядка p ее подгруппы G имеют одинаковую высоту в G и в A, то G — сервантная подгруппа группы A.

Чтобы доказать, что любой элемент $g \in G$ имеет в G и в A одинаковую высоту, применим индукцию по $\exp(g) = n$. Для $\exp(g) = 1$ это выполнено по условию. Индукционный шаг проводится очевидным образом.

и) Если A есть p-группа, G — ее сервантная подгруппа и $G[p] = A[p]$, то $G = A$.

Лемма 1.2.6.2. *[6, лемма 26.1] Пусть B, C — такие подгруппы группы A, что $C \leqslant B \leqslant A$. Тогда*

1) если подгруппа C сервантна в B, а подгруппа B сервантна в A, то C сервантна в A;

2) если подгруппа B сервантна в A, то подгруппа B/C сервантна в A/C;

3) если подгруппа C сервантна в A и подгруппа B/C сервантна в A/C, то подгруппа B сервантна в A.

Доказательство. При предположения п. 1) имеем

$$nC = C \cap nB = C \cap (B \cap nA) = (C \cap B) \cap na = C \cap nA$$

для любого $n \in \mathbb{N}$, что доказывает сервантность подгруппы C в A. Утверждение 2) вытекает из равенств

$$n(B/C) = (nB + C)/C = ((B \cap nA) + C)/C = (B \cap (nA + c))/C = (B/C) \cap n(A/C).$$

Предположим, что выполнены условия п. 3), и пусть $na = b \in B$ для некоторого $a \in A$ и некоторого $n > 0$. Тогда $n(a + C) = b + C$, и по предположению для некоторого $b' \in B$ имеет место равенство $n(b' + C) = b + C$. Из $nb' = b + c$ $(c \in C)$ получаем $n(b' - a) = c$. Следовательно, $nc' = c$ для некоторого $c' \in C$. Наконец, $n(b' - c') = b$, где $b' - c' \in B$, что завершает доказательство. ⊠

Предложение 1.2.6.3. *[6, предложение 26.2] Всякую бесконечную подгруппу можно вложить в сервантную подгруппу той же мощности, а всякую конечную подгруппу — в счетную сервантную подгруппу.*

Доказательство. Пусть B — подгруппа группы A, и пусть $|B| = \mathfrak{m}$. Рассмотрим все уравнения $nx = b \in B$, имеющие решение в группе A. Для всякого такого уравнения добавим к B решение $a_{n,b} \in A$ и получим подгруппу B_1 группы A, в которой все такие уравнения над B имеют решение (т. е. подгруппа B_1 порождается подгруппой B и всеми этими элементами $a_{n,b}$). Затем повторим этот процесс, заменив B на B_1, и получим подгруппу B_2, в которой имеют решение все уравнения с правой частью из B_1, имеющие решения в группе A. Объединение G подгрупп B_i $(i = 1, 2, \ldots)$ является сервантной подгруппой группы A. Очевидно, $|G| \leqslant \mathfrak{m}|\mathbb{N}|$. ⊠

§7 Ограниченные сервантные подгруппы

Докажем сначала две леммы технического характера.

Лемма 1.2.7.1. *[6, лемма 9.8] Если B — подгруппа группы A и C является B-высокой подгруппой в A, то из включений $a \in A$, $pa \in C$ (p — простое число) следует, что $a \in B \oplus C \leqslant A$.*

Доказательство. Если $a \in C$, то доказывать нечего. Если $a \notin C$, то согласно выбору C, группа $\langle C, a\rangle$ содержит некоторый элемент $b \in B$. Следовательно, $b = c + ka$ для некоторого $k \in \mathbb{Z}$ такого, что $(k, p) = 1$. Следовательно, $rk + sp = 1$ для некоторых целых чмсел r, s, и, таким образом, $a = r(ka) + s(pa) = r(b - c) + s(pa) \in B \oplus C$. ⊠

Лемма 1.2.7.2. *[6, лемма 9.9] Пусть группы A, B, C — такие же, как в лемме 1.2.7.1. Тогда $A = B \oplus C$ в том и только в том случае, когда из равенства $pa = b + c$ ($a \in A, b \in B, c \in C$) непременно следует $pb' = b$ для некоторого $b' \in B$.*

Доказательство. Если $A = B \oplus C$ и $a = b' + c'$, то $pa = pb' + pc' = b + c$ дает $pb' = b$. Обратно, если из равенства $pa = b + c$ всегда следует $pb' = b$ для некоторого $b' \in B$, то $a - b'$ удовлетворяет условиям предыдущей леммы и, следовательно, $a - b' \in B \oplus C$, $a \in B \oplus C$. Это означает, что факторгруппа $A/(B \oplus C)$ не содержит элементов простого порядка, т. е. является группой без кручения. Но если x — произвольный элемент группы A, не лежащий в $B \oplus C$, то пересечение $\langle C, x\rangle \cap B$ содержит ненулевой элемент $c'' + lx = b''$ для некоторого $c'' \in C$ и целого числа l. Тогда $l \neq 0$, так как $B \cap C = 0$, поэтому из включения $lx = b'' - c'' \in B \oplus C$ следует, что $A/(B \oplus C)$ — периодическая группа. Таким образом $A = B \oplus C$. ⊠

Определение 1.2.7.3. Система L элементов группы A называется *системой кообразующих*, если для любой группы B всякий гомоморфизм $\varphi : A \longrightarrow B$ для которого $L \cap \operatorname{Ker} \varphi = \emptyset$ или $= 0$, является мономорфизмом. Это, очевидно, эквивалентно тому, что каждая ненулевая подгруппа из A содержит ненулевой элемент из L. Ясно, что подгруппа $\langle L\rangle$ должна быть существенной в A, и существенная подгруппа всегда является системой кообразующих. Если существует система кообразующих L такая, что $|L| = 1$, то группа называется *коциклической*.

Предложение 1.2.7.4. *[6, предложение 27.1] Предположим, что подгруппа B группы A является прямой суммой циклических групп одного и того же порядка p^k. Тогда эквивалентны следующие утверждения:*
- *а) B — сервантная (p-сервантная) подгруппа группы A;*
- *б) для B выполнено равенство $B \cap p^k A = 0$;*
- *в) B — прямое слагаемой группы A.*

Доказательство. Если B есть p-сервантная подгруппа группы A, то $B \cap p^m A = p^m B$ для любого целого числа $m > 0$, в частности для $m = k$, когда $p^k B = 0$. Следовательно, из п. а) вытекает б). Пусть выполнено условие б), и пусть C — такая B-высокая подгруппа группы A, что $p^k A \leqslant C$. Если для некоторого $a \in A$ имеет место равенство $pa = b + c$ ($b \in B, c \in C$), то $p^k a = p^{k-1}b + p^{k-1}c$, откуда $p^{k-1}b = 0$, так как $p^k a \in C$. Из предположения относительно строения группы B следует, что существует такой элемент $b' \in B$, что $pb' = b$. Теперь простое использование леммы 1.2.7.2 и того факта, что $qB = B$ для всех простых чисел $q \neq p$, показывает, что $A = B \oplus C$, т. е. выполнено в). Тот факт, что из в) следует а) очевиден. ⊠

Следствие 1.2.7.5. *[6, следствие 27.2] Всякий элемент порядка p и конечной высоты можно вложить в конечное циклическое прямое слагаемое группы.*

Доказательство. Пусть элемент $a \in A$ имеет порядок p и высоту $k < \infty$, и пусть $p^k b = a$. Тогда $\langle b\rangle$ — сервантная подгруппа конечного порядка, и можно применить предложение 1.2.7.4. ⊠

Следствие 1.2.7.6. *[6, следствие 27.3] Если группа содержит элемент конечного порядка, то она обладает коциклическим прямым слагаемым.*

Доказательство. Если для некоторого p группа содержит подгруппу $\mathbb{Z}(p^\infty)$, то эта подгруппа выделяется прямым слагаемым. Если группа не содержит подгрупп вида $\mathbb{Z}(p^\infty)$, но содержит элементы порядка p, то она содержит и элемент порядка p конечной высоты. Остается применить следствие 1.2.7.5. $\boxtimes$

Следствие 1.2.7.7. *[6, следствие 27.4] Прямо неразложимые группы являются или группами без кручения, или коциклическими группами.*

Теорема 1.2.7.8. *[6, теорема 27.5] Всякая ограниченная сервантная подгруппа является прямым слагаемым.*

Доказательство. Если B — ограниченная группа, то в силу теоремы 1.1.4.2 можно написать $B = B_1 \oplus C$, где B_1 — прямая сумма циклических групп одного и того же порядка p^k, а в C наименьшая верхняя грань порядков элементов меньше соответствующей грани для группы B. Если B — сервантная подгруппа группы A, то и подгруппа B_1 сервантна в A_1, и из предложения 1.2.7.4 следует, что $A = B_1 \oplus A_1$. Отсюда $B = B_1 \oplus C_1$. Здесь C_1 — сервантная подгруппа группы A_1, и по индуктивному предположению C_1 — прямое слагаемое группы A_1. Следовательно, B — прямое слагаемое группы A. $\boxtimes$

Следствие 1.2.7.9. *Всякая конечная копорожденная сервантная подгруппа выделяется прямым слагаемым.*

Теорема 1.2.7.10. *[6, теорема 27.7] Для любого простого числа p и натурального числа n всякая p^nA-высокая подгруппа группы A служит для A прямым слагаемым.*

Доказательство. Пусть B есть p^nA-высокая подгруппа группы A. Тогда $p^nB \subseteq B \cap p^nA = 0$, т. е. B — ограниченная p-группа. Проверим, что B — сервантная подгруппа группы A. Для этого покажем, что $B \cap p^kA \subseteq p^kB$ при любом целом $k \geqslant 0$. Для $k = 0$ это выполняется тривиальным образом. Применим индукцию по k. Если $b = p^{k+1}a \neq 0$ $(b \in B, a \in A)$, то по лемме 1.2.7.1 $p^ka \in p^nA \oplus B$, т. е. $p^ka = p^nc + d$ для некоторых $c \in A, d \in B$. Так как $p^na \in p^nA$, то $k \leqslant n-1$. Поэтому $d = p^ka - p^kc$ принадлежит подгруппе $B \cap p^kA$, которая равна p^kB в силу индуктивного предположения. Следовательно, $b = p^{k+1}a = p^{n+1}c + pd$ дает $b = pd \in p^{k+1}B$. Таким образом, B — ограниченная сервантная подгруппа группы A. Остается применить теорему 1.2.7.8. $\boxtimes$

Следствие 1.2.7.11. *[6, следствие 27.8] p-подгруппу B группы A можно вложить в ограниченное прямое слагаемое группы A тогда и только тогда, когда высоты отличных от нуля элементов группы B, взятые в группе A, ограничены.*

Доказательство. Так как необходимость очевидна, предположим, что m — верхняя грань высот элементов в B. Выберем $p^{m+1}A$-высокую подгруппу C группы A, для которой $B \leqslant C$, и применим предыдущую теорему. Тогда получится, что C — ограниченное прямое слагаемое, содержащее подгруппу B. $\boxtimes$

Следствие 1.2.7.12. *[6, следствие 27.9] Элемент a, порядок которого — степень простого числа, принадлежит конечному прямому слагаемому группы тогда и только тогда, когда подгруппа $\langle a \rangle$ не содержит отличных от нуля элементов бесконечной высоты.*

Теорема 1.2.7.13. *[6, теорема 25.1] Для группы A эквивалентны следующие условия:*

1. *A — конечно копорожденная группа;*

2. A — существенное расширение конечной группы;

3. A — прямая сумма конечного числа коциклических групп;

4. подгруппы группы A удовлетворяют условию минимальности.

Доказательство. Пусть выполнено условие 1, и пусть L — конечная система кообразующих группы A. В группе A нет элементов бесконечного порядка, так как иначе в циклической группе, порожденной элементом бесконечного порядка, можно было бы выбрать ненулевую подгруппу, не содержащую ни одного отличного от нуля элемента из L. Следовательно, L — конечная система элементов конечного порядка, откуда $\langle L\rangle$ — конечная подгруппа. Так как A — существенное расширение подгруппы $\langle L\rangle$, то отсюда вытекает 2.

Пусть теперь выполнено условие 2, т. е. A — существенное расширение конечной подгруппы B. Очевидно, A является периодической группой с конечным числом p-компонент, и, чтобы доказать 3, мы можем предположить, что A и B — это p-группы. Так как $A[p] = B[p]$ — конечная группа, то для фиксированного элемента $a \in A$ уравнение $px = a$ может иметь не более конечного числа решений в группе A. Если $h(a) = \infty$, то решения $x_1, \ldots, x_k$ не могут иметь конечную высоту. Следовательно, начав с элемента $a \in A[p]$ бесконечной высоты, мы можем построить квазициклическую подгруппу группы A. Объединение D всех квазициклических подгрупп группы A является делимой подгруппой, поэтому $A = D \oplus C$. Так как $C[p]$ — конечная группа, то существует максимум mвысот ее элементов, и, таким образом, $p^{m+1}C = 0$. Следовательно, A — прямая сумма коциклических групп, где число слагаемых конечно в силу конечности цоколя группы A.

Покажем теперь, что из 3 следует 4. Если $r(A) = 1$, т. е. $A = \mathbb{Z}(p^k)$, где $1 \leqslant k \leqslant \infty$, то утверждение очевидно. Для $r(A) = n > 1$ доказательство проведем по индукции. Предположим, что в группах ранга $\leqslant n-1$ условие минимальности выполнено. Пусть $A = \mathbb{Z}(p^k) \oplus B$, где $r(B) = n-1$, и пусть $G_1 \leqslant G_2 \leqslant \ldots$ — убывающая последовательность подгрупп группы A. Тогда $B \cap G_1 \leqslant B \cap G_2 \leqslant \ldots$ и, начиная с некоторого номера m, имеем $B \cap G_m = B \cap G_{m+1} = \ldots$. Из соотношений

$$G_i/(B \cap G_m) = G_i/(B \cap G_i) \cong (B + G_i)/B \leqslant A/B = \mathbb{Z}(p^k) \ (i \geqslant m)$$

следует, что группы $G_i/(B \cap G_m)$, а тогда и группы G_i, начиная с некоторого индекса совпадают. Этим условие 4 доказано.

Наконец, предположим, что выполнено условие 4. Группа A не содержит элементов бесконечного порядка. Так как цоколь группы A не может быть бесконечной прямой суммой, то $S(A)$ — конечная подгруппа. Следовательно, группа A обладает конечной системой кообразующих. ⊠

Предложение 1.2.7.14. *[6, предложение 25.2] Пусть $a_1, \ldots, a_n$ — конечное множество ненулевых элементов группы A и M — подгруппа группы A, максимальная относительно того свойства, что она не содержит ни одного из элементов $a_1, \ldots, a_n$. Тогда в фактор-группе A/M выполнено условие минимальности для подгрупп. Если $n = 1$, то A/M — коциклическая группа.*

Доказательство. Всякая подгруппа группы A, строго содержащая M, содержит хотя бы один из элементов $a_1, \ldots, a_n$. Другими словами, всякая ненулевая подгруппа группы A/M содержит один из элементов $a_1 + M, \ldots, a_n + M$, т. е. $a_1 + M, \ldots, a_n + M$ — система кообразующих группы A/M. Остается применить предыдущую теорему. ⊠

Теорема 1.2.7.15. *[6, теорема 27.10] Для подгруппы B группы A эквивалентны следующие условия:*

1. *подгруппа B сервантна в A;*

2. *B/nB — прямое слагаемое группы A/nB для любого $n > 0$;*

3. *если $C \leqslant B$ и B/C — конечно копорожденная группа, то B/C — прямое слагаемое группы A/C.*

Доказательство. Если выполнено 1, то из леммы 1.2.6.2 получается, что B/nB — сервантная подгруппа группы A/nB, так что 2 сразу следует из теоремы 1.2.7.8. Предположим, что выполнено условие 2, и пусть C — подгруппа со свойством, указанным в 3. Очевидно, можно ограничиться случаем, когда группа B/C редуцированная, что равносильно конечности B/C (см. теорему 1.2.7.13). Тогда существует целое число $n > 0$, для которого $nB \leqslant C$, и по предположению B/nB — прямое слагаемое группы A/nB. Здесь C/nB содержится в B/nB. Переходя к факторгруппе по C, получаем, что B/C — прямое слагаемое для A/C. Пусть, наконец, выполнено условие 3. Если уравнение $nx = b \in B$ имеет решение в группе A, но не имеет решения в B, то $b \notin nB$. Пусть C — подгруппа группы B, содержащая nB и максимальная среди подгрупп, не содержащих b. Тогда по предложению 1.2.7.14 B/C — коциклическая группа. По предположению B/C — прямое слагаемое группы A/C. Так как $b + C (\neq C)$ делится на n, а $n(B/C) = 0$, получаем противоречие. ⊠

§8 Факторгруппы по сервантным подгруппам

Теорема 1.2.8.1. *[6, теорема 28.1] Подгруппа B группы A сервантна тогда и только тогда, когда каждый смежный класс группы A по подгруппе B содержит элемент того же порядка, что и этот смежный класс.*

Доказательство. Пусть B — сервантная подгруппа группы A, и пусть $a^* \in A/B$. Если $|a| = \infty$, то любой представитель смежного класса a^* имеет бесконечный порядок. Если $|a^*| = n < \infty$, то для любого представителя $g \in a^*$ имеем $ng \in B$. Из сервантности получаем, что $nb = ng$ для некоторого $b \in B$. Элемент $a = g - b \in a^*$ имеет порядок $\leqslant n$, т. е. порядок n. Обратно, если выполнено сформулированное в теореме условие и $ng \in B$ для некоторого $g \in A$, то выберем в смежном классе $g + B$ представитель a, имеющий порядок, равный порядку этого смежного класса. Тогда $na = 0$ и для элемента $g - a \in B$ выполнено равенство $n(g - a) = b$. ⊠

Теорема 1.2.8.2. *[6, теорема 28.2] Если B — сервантная подгруппа группы A и A/B — прямая сумма циклических групп, то B служит для A прямым слагаемым.*

Доказательство. В силу леммы 1.1.1.4 можно ограничиться случаем, когда A/B — циклическая группа, скажем, порожденная элементом a^*. Ввиду теоремы 1.2.8.1 можно выбрать представитель $a \in a^*$ того же порядка, что и a^*. Тогда элементы подгруппы $\langle a \rangle$ составят полную систему представителей смежных классов группы A по подгруппе B. Отсюда $A = B \oplus \langle a \rangle$. ⊠

Следствие 1.2.8.3. *[6, следствие 28.3] Если B сервантна в A и A/B — конечно порожденная группа, то B — прямое слагаемое группы A.*

Теорема 1.2.8.4. *[6, теорема 28.3] Для подгруппы B группы A эквивалентны условия:*

1) подгруппа B сервантна в A;

2) подгруппа B служит прямым слагаемым для $n^{-1}B$ при любом $n > 0$;

3) если C — группа, лежащая между B и A, и C/B — конечно порожденная группа, то B служит для C прямым слагаемым.

Доказательство. Если подгруппа B сервантна в A, то по теоремам 1.1.4.2 и 1.2.8.2 условие 2) вытекает из ограниченности группы $(n^{-1}B)/B$. Чтобы доказать, что из 2) следует 3), мы можем в силу теоремы 1.1.1.5 ограничиться случаем, когда C/B — конечная группа. Тогда $C \leqslant n^{-1}B$ для некоторого n, и 3) непосредственно получается из 2). Так как из 3) следует, что каждый смежный класс группы A по подгруппе B содержит элемент того же порядка, что и этот смежный класс, то условие 1) непосредственно вытекает из теоремы 1.2.8.1 ⊠

Теорема 1.2.8.5. *[6, теорема 28.5] Если система уравнений*

$$\sum_{j=1}^{m} n_{ij}x_j = b_i \quad (b_i \in B, i \in I)$$

над сервантной подгруппой B группы A, содержащая конечное число m неизвестных, имеет решение в группе A, то она имеет решение и в B. (В бесконечном случае утверждение теоремы неверно.)

Доказательство. Пусть $x_j = a_j$ $(j = 1, \ldots, m)$ — решение данной системы уравнений в группе A. В силу теоремы 1.2.8.4, п. 3), подгруппа B служит прямым слагаемым для подгруппы $\langle Ba_1, \ldots, a_m\rangle = C$, т. е. $C = B \oplus B_1$. Компоненты элементов a_j в прямом слагаемом B дают решение, лежащее в B. ⊠

§9 Сервантно точные последовательности

Лемма 1.2.9.1. *[6, лемма 2.4] (3×3-лемма) Предположим, что диаграмма*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_1 & \xrightarrow{\alpha_1} & B_1 & \xrightarrow{\beta_1} & C_1 & \longrightarrow & 0 \\
 & & \lambda_1 \downarrow & & \mu_1 \downarrow & & \downarrow \nu_1 & & \\
0 & \longrightarrow & A_2 & \xrightarrow{\alpha_2} & B_2 & \xrightarrow{\beta_2} & C_2 & \longrightarrow & 0 \\
 & & \lambda_2 \downarrow & & \mu_2 \downarrow & & \downarrow \nu_2 & & \\
0 & \longrightarrow & A_3 & \xrightarrow{\alpha_3} & B_3 & \xrightarrow{\beta_3} & C_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

коммутативна, а все три ее столбца точны. Тогда если первые две или последние две строки точны, то оставшаяся строка тоже точна.

Доказательство. Мы докажем только, что из точности двух первых строк вытекает точность последней строки.

Пусть $a_3 \in \operatorname{Ker} \alpha_3$. Так как λ_2 — эпиморфизм, то $a_2\lambda_2 = a_3$ для некоторого $a_2 \in A_2$. Из $a_2\alpha_2\mu_2 = a_2\lambda_2\alpha_3 = 0$ и точности среднего столбца вытекает существование такого $b_1 \in B_1$, что $b_1\mu_1 = a_2\alpha_2$. Из соотношения $b_1\beta_1\nu_1 = b_1\mu_1\beta_2 = 0$ мы получаем $b_1\beta_1 = 0$, так как ν_1 — мономорфизм. Отсюда и из точности первой строки получается, что $a_1\alpha_1 = b_1$ для некоторого $a_1 \in A_1$. Следовательно, $a_2\alpha_2 = b_1\mu_1 = a_1\alpha_1\mu_1 = a_1\lambda_1\alpha_2$. Таким образом, так как α_2 — мономорфизм, $a_2 = a_1\lambda_1$, откуда $a_3 = a_2\lambda_2 = a_1\lambda_1\lambda_2 = 0$, т. е. α_3 — мономорфизм.

Так как $\lambda_2\alpha_3\beta_3 = \alpha_2\mu_2\beta_3 = \alpha_2\beta_2\nu_2 = 0$ и λ_2 — эпиморфизм, то имеет место $\alpha_3\beta_3 = 0$. Чтобы показать, что $\operatorname{Ker}\beta_3 \leqslant \operatorname{Im}\alpha_3$, возьмем $b_3 \in \operatorname{Ker}\beta_3$. Мы знаем, что для некоторого $b_2 \in B_2$ справедливо равенство $b_2\mu_2 = b_3$. Отсюда $b_2\beta_2\nu_2 = b_2\mu_2\beta_3 = 0$. В силу точности третьего столбца существует вытекает такой элемент $c_1 \in C_1$, что $c_1\nu_1 = b_2\beta_2$. Из точности первой строки вытекает, что $b_1\beta_1 = c_1$ для некоторого $b_1 \in B_1$, откуда получаем, что существует $a_2 \in A_2$, для которого $a_2\alpha_2 = b_2 - b_1\mu_1$, откуда $a_2\lambda_2\alpha_3 = a_2\alpha_2\mu_2 = b_2\mu_2 = b_3$, т. е. $b_3 \in Im\alpha_3$.

Наконец, из соотношения $Im\beta_3 \leqslant Im\mu_2\beta_3 = Im\beta_2\nu_2 = C_3$ вытекает, что β_3 — эпиморфизм. ⊠

Определение 1.2.9.2. [6, стр. 145] Короткая точная последовательность

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \qquad (1.12)$$

называется *сервантно точной*, если $Im\alpha$ — Сервантная подгруппа группы B. Данная точная последовательность называется *p-сервантно точной*, если $Im\alpha$ есть p-сервантная подгруппа группы B.

Для простоты в следующей теореме мы будем обозначать одной и той же буквой заданный гомоморфизм и все гомоморфизмы, им индуцированные.

Теорема 1.2.9.3. *[6, теорема 29.1] Для точной последовательности* (1.12) *каждое из следующих условий эквивалентно тому, что последовательность* (1.12) *сервантно точна:*

а) последовательность $0 \longrightarrow nA \xrightarrow{\alpha} nB \xrightarrow{\beta} nC \longrightarrow 0$ *точна при любом* n*;*

б) последовательность $0 \longrightarrow A[n] \xrightarrow{\alpha} B[n] \xrightarrow{\beta} C[n] \longrightarrow 0$ *точна при любом* n*;*

в) последовательность $0 \longrightarrow A/nA \xrightarrow{\alpha} B/nB \xrightarrow{\beta} C/nC \longrightarrow 0$ *точна при любом* n*;*

г) последовательность $0 \longrightarrow A/A[n] \xrightarrow{\alpha} B/B[n] \xrightarrow{\beta} C/C[n] \longrightarrow 0$ *точна при любом* n*;*

Доказательство. Если последовательность (1.12) точна, то в п. а) отображение α — мономорфизм, β — эпиморфизм. Ядром отображения β из а) является подгруппа $\alpha A \cap nB$, которая равна $\alpha(nA)$ тогда и только тогда, когда (1.12) — сервантно точная последовательность.

В п. б) отображение α всегда является мономорфизмом, а β — эпиморфизм при любом n в точности тогда, когда каждый элемент группы C, имеющий порядок n, является образом элемента порядка n из B; это по теореме 1.2.8.1 эквивалентно сервантности. Так как α — мономорфизм, $\operatorname{Ker}\beta = \alpha A \cap B[n] = \alpha A[n]$.

Остальное следует из уже доказанного и из 3×3-леммы. ⊠

Теорема 1.2.9.4. *[6, теорема 29.2] Точная последовательность* (1.12) *сервантно точна тогда и только тогда, когда каждая коциклическая группа G инъективна относительно последовательности* (1.12)*, т. е. для всякой коциклической группы G диаграмма*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[r, "\beta"] \arrow[dl, "\psi"] & C \arrow[r] & 0 \\ & G & & & \end{tikzcd}$$

может быть вложена в коммутативную диаграмму при соответствующем выборе гомоморфизма $\psi : B \longrightarrow G$.

Доказательство. Легко показать, что конечная прямая сумма $G_1 \oplus \ldots \oplus G_m$ инъективна относительно последовательности (1.12) тогда и только тогда, когда каждая группа G_i инъективна относительно этой последовательности. Поэтому группу G можно считать конечно копорожденной. Далее, ясно, что достаточно рассмотреть случай, когда φ — эпиморфизм. Тогда существование гомоморфизма ψ эквивалентно возможности продолжить изоморфизм $A/\mathrm{Ker}\ \varphi \cong G$ до гомоморфизма $B/(\mathrm{Ker}\ \varphi)\alpha \longrightarrow G$, т. е. эквивалентно тому, что $(A/\mathrm{Ker}\ \varphi)\alpha$ — прямое слагаемое группы $B/(\mathrm{Ker}\ \varphi)\alpha$. Теперь остается применить теорему 1.2.7.15. ☒

Теорема 1.2.9.5. *[6, теорема 29.3] Необходимым и достаточным условием для того, чтобы точная последовательность* (1.12) *была сервантно точной, является проективность относительно последовательности* (1.12) *любой циклической группы G и любого гомоморфизма $\varphi : G \longrightarrow C$ существует гомоморфизм $\psi : G \longrightarrow B$, при котором становится коммутативной диаграмма*

$$\begin{array}{c} G \\ \psi \swarrow \ \downarrow \varphi \\ 0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \end{array}$$

Доказательство. Легко получается рассуждениями, двойственными к предыдущему доказательству, после применения теоремы 1.2.8.4. ☒

§10 Сервантная проективность и сервантная инъективность

Определение 1.2.10.1. [6, стр. 149] Группа X называется *сервантно проективной*, если она проективна относительно класса сервантно точных последовательностей, т. е. если каждая диаграмма

$$\begin{array}{c} X \\ \psi \swarrow \ \downarrow \varphi \\ 0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \end{array} \tag{1.13}$$

с сервантно точной строкой может быть пополнена соответствующим гомоморфизмом $\psi : X \longrightarrow B$ так, что получится коммутативная диаграмма.

Лемма 1.2.10.2. *[6, лемма 30.1] Для любой группы A существуют такая прямая сумма циклических групп $X = \sum_{i \in I} \langle x_i \rangle$ и такой гомоморфизм $\eta : X \longrightarrow A$, что* $\mathrm{Ker}\ \eta$ *— сервантная подгруппа группы X.*

Доказательство. Пусть $\{a_i\}_{i \in I}$ — множество всех элементов группы A, и пусть $A_i = \langle a_i \rangle$. Для каждого элемента a_i возьмем группу $\langle x_i \rangle$, изоморфную группе $A_i = \langle a_i \rangle$, и положим $X = \sum_{i \in I} \langle x_i \rangle$. Вложения $\eta_i : \langle x_i \rangle \longrightarrow A$, где $x_i \eta_i = a_i$, порождают эпиморфизм $\eta : X \longrightarrow A$, ядро которого обозначим через K. Нужно проверить, что K — сервантная подгруппа группы X. Пусть $nx = b \in K$ для некоторого $x \in X$. Если $x\eta = a_i \in A$, то из $x_i \eta = a_i$ имеем $x - x_i \in K$. Так как $na_i = (nx)\eta = b\eta = 0$ и $|x_i = |a_i|$, то $nx_i = 0$, откуда $n(x - x_i) = b$. ☒

Теорема 1.2.10.3. *[6, теорема 30.2] Группа сервантно проективна тогда и только тогда, когда она — прямая сумма циклических групп.*

Доказательство. Пусть X — прямая сумма циклических групп, т. е. $X = \sum_{i \in I} \langle x_i \rangle$, и пусть в диаграмме (1) строка сервантно точна. Из теоремы 1.2.9.5 следует, что для каждого i существует такой элемент $b_i \in B$, что $b_i\beta = x_i\varphi$ и $|b_i| = |x_i\varphi|$. Определим гомоморфизм $\psi : X \longrightarrow B$ так, чтобы он продолжал соответствие $x_i \longmapsto b_i$; учитывая условия на порядки элементов и строение группы X, получаем, что это возможно. Очевидно, что гомоморфизм ψ превращает диаграмму 1.13 в коммутативную.

Обратно, пусть группа X сервантно проективна. По лемме 1.2.10.2 существует диаграмма

$$\begin{array}{ccccccccc} & & & & & & X & & \\ & & & & \psi & \swarrow & \| & & \\ 0 & \longrightarrow & K & \xrightarrow{\xi} & G & \xrightarrow{\eta} & X & \longrightarrow & 0 \end{array}$$

с сервантно точной строкой, где G — прямая сумма циклических групп. По предположению можно найти такой гомоморфизм $\psi : X \longrightarrow G$, что $\psi\eta = 1_X$. Следовательно, ψ — инъекция на прямое слагаемое группы G. Поскольку подгруппы прямых сумм циклических групп сами являются прямыми суммами циклических групп, X — также прямая сумма циклических групп. ⊠

Определение 1.2.10.4. [6, стр.150] Назовем группу Y *сервантно инъективной*, если всякая диаграмма

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & \varphi\downarrow & & \swarrow & \psi & & & & \\ & & Y & & & & & & \end{array} \tag{1.14}$$

может быть вложена в коммутативную диаграмму при соответствующем выборе гомоморфизма $\psi : B \longrightarrow Y$.

Лемма 1.2.10.5. *[6, лемма 30.3] Всякую группу можно вложить в качестве сервантной подгруппы в декартову сумму коциклических групп.*

Доказательство. Пусть B_i $(i \in I)$ — семейство всех факторгрупп данной группы A, и пусть $B = \overline{\sum}_{i \in I} B_i$. Эпиморфизмы $\eta_i : A \longrightarrow B_i$ индуцируют гомоморфизм

$$\eta =: A \longrightarrow B.$$

Так как для каждого элемента $a \in A$, $a \neq 0$, существует такой гомоморфизм η_i, что a не лежит в его ядре (см. предложение 1.2.7.14, то η является мономорфизмом. Чтобы доказать сервантность подгруппы $\operatorname{Im} \eta$ в B, предположим, что $a \in A$, $a \notin p^n A$, и выберем в A подгруппу M, максимальную относительно свойств $p^n A \leqslant M$ и $a \notin M$. Тогда по предложению 1.2.7.14 A/M будет коциклической группой, и из включения $p^n A \leqslant M$ мы получим, что $A/M = \mathbb{Z}(p^k)$, где $k \leqslant n$. Так как $A/M = B_i$ для некоторого i и элемент $a + M$ имеет в группе A/M высоту $\leqslant k - 1$, то включение $a\eta \in p^k B$ невозможно. ⊠

Теорема 1.2.10.6. *[6, теорема 30.4] Группа сервантно инъективна тогда и только тогда, когда она — прямое слагаемое декартовой суммы коциклических групп.*

Доказательство. Пусть Y — прямое слагаемое декартовой суммы $G = \overline{\sum} G_i$, где все G_i — коциклические группы. Пусть π_i, ρ_i — координатные проекции и инъекции, связанные с этим декартовой суммой, и пусть $\pi : G \longrightarrow Y$, $\rho : Y \longrightarrow G$ таковы, что $\pi\rho = 1_Y$. Если в диаграмме 1.14 строка сервантно точна, то по теореме 1.2.9.4 для каждого i существует такое отображение $\psi_i : B \longrightarrow G_i$, что $\varphi\rho\pi_i = \alpha\psi_i$. Отображения ψ_i порождают отображение $\psi : B \longrightarrow G$, где $\psi\pi_i = \psi_i$. Отсюда $\varphi\rho\pi_i = \alpha\psi\pi_i$ для каждого i, т. е. $\varphi\rho = \alpha\psi$. Следовательно, $\varphi = \varphi\rho\pi = \alpha\psi\pi$ и $\psi\pi : B \longrightarrow Y$ — искомый гомоморфизм.

Предположим теперь, что группа Y сервантно инъективна. По лемме 1.2.10.5 существует сервантно точная последовательность $0 \longrightarrow Y \longrightarrow G \longrightarrow H \longrightarrow)$, где G — декартова сумма коциклических групп. В силу сервантной инъективности, тождественное отображение $Y \longrightarrow Y$ можно продолжить до отображения $G \longrightarrow Y$, откуда следует, что группа Y изоморфна прямому слагаемому группы G. ⊠

1.3 Алгебраически компактные группы

§1 Алгебраическая компактность

Определение 1.3.1.1. [6, стр. 187] Группа A называется *алгебраически компактной*, если она выделяется прямым слагаемым из всякой группы G, содержащей ее в качестве сервантной подгруппы.

Теорема 1.3.1.2. *[6, теорема 38.1] Следующие условия для группы A эквивалентны:*

а) группа A сервантно инъективна;

б) группа A алгебраически компактна;

в) группа A — прямое слагаемое декартовой суммы коциклических групп;

г) группа A в алгебраическом смысле является прямым слагаемым группы, допускающей компактную топологию;

д) если всякая конечная подсистема системы уравнений над A имеет решение в группе A, то и вся система уравнений разрешима в A.

Доказательство. Доказательство будем вести по циклу. Предположим сначала, что выполнено условие а), и пусть A — сервантная подгруппа группы G. Из наличия сервантно точной последовательности $0 \longrightarrow A \longrightarrow G \longrightarrow G/A \longrightarrow 0$ и из условия а) мы получаем, что тождественное отображение $1_A : A \longrightarrow A$ можно продолжить до гомоморфизма $G \longrightarrow A$. Следовательно, A — прямое слагаемое группы G, что доказывает б).

Предположим теперь, что выполнено условие б). По лемме 1.2.10.5 группу A можно вложить в качестве сервантной подгруппы в декартову сумму коциклических групп. Следовательно, из п. б) вытекает в).

Предположим, что выполнено в). Так как декартова сумма компактных групп сама компактна в топологии произведения и так как свойство быть прямым слагаемым транзитивно, то свойство г) будет доказано, если мы покажем, что им обладают коциклические группы. Но это очевидно, так как группа $\mathbb{Z}(p^k)$ $(k < \infty)$ компактна в дискретной топологии, а группа $\mathbb{Z}(p^\infty)$ — прямое слагаемое аддитивной группы действительных чисел, которая, как хорошо известно, является компактной группой.

Чтобы вывести д) из г), возьмем систему уравнений

$$\sum_{j \in J} n_{ij} x_j = a_i \quad (a_i \in A, i \in I), \tag{1.15}$$

где $n_i j$ —целые числа, которые при фиксированном i почти все равны нулю, и предположим, что всякая ее конечная подсистема имеет в группе A решение. По условию г) существует такая группа B, что группа $A \oplus B = C$ допускает компактную топологию. Систему уравнений (1.15) мы можем рассматривать как систему уравнений над группой C. Решение i-ого уравнения системы (1.15) можно рассматривать как элемент $(\ldots, c_j, \ldots)$ группы $C^J = \overline{C}$, где элементы $x_j = c_j$ $(j \in J)$ удовлетворяют i-ому уравнению. Таким образом, множество всех решений i-ого является подмножеством X_i компактного пространства $\overline{C}$. Кроме того, подмножество X_i замкнуто, так как оно определяется уравнением. Предположение, что всякое конечное подмножество множества всех X_i имеет непустое пересечение. В силу компактности пространства $\overline{C}$ пересечение $\cap X_i$ всех подмножеств X_i не пусто, поэтому всякая система уравнений (1.15) допускает решение в C. Компоненты этого решения в прямом слагаемом A группы C дают решение в группе A.

Наконец предположим, что выполнено условие д). Пусть $0 \longrightarrow B \longrightarrow C \longrightarrow C/B \longrightarrow 0$ — сервантно точная последовательность и $\eta : B \longrightarrow A$ — гомоморфизм. Пусть $c_j (j \in J)$ — система образующих группы C по модулю B и

$$\sum_{j \in J} = n_{ij} c_j = b_i \in B \quad (i \in I)$$

все соотношения между элементами c_j и элементами группы B. Рассмотрим систему уравнений

$$\sum_{j \in J} n_{ij} x_j = b_i \eta (\in A) \quad (i \in I). \tag{1.16}$$

Конечная подсистема системы (1.16) содержит явно лишь конечное число неизвестных $x_{j_1}, \ldots, x_{j_k}$. В силу сервантности подгруппа B выделяется прямым слагаемым из подгруппы $B' = \langle B, c_{j_1}, \ldots, c_{j_k} \rangle$, т. е. $B' = B \oplus C'$ (см. теорему 1.2.8.4), и образы компонент в B элементов $c_{j_1}, \ldots, c_{j_k}$ при гомоморфизме η дают решение в группе A. Следовательно, система (1.16) удовлетворяет предположениям п. д). Мы заключаем, что в группе A существует решение $x_j = a_j$ всей системы (1.16). Соответствие $c_j \longmapsto a_j$ порождает продолжение гомоморфизма η до гомоморфизма $C \longrightarrow A$. Следовательно, выполнено условие а). $\boxtimes$

Следствие 1.3.1.3. *[6, следствие 38.2] Редуцированная алгебраически компактная группа является прямым слагаемым декартовой суммы циклических p-групп.*

Доказательство. Если A — редуцированная алгебраически компактная группа, то для некоторой группы B имеем $A \oplus B = C = C_1 \oplus C_2$, где C_1 — декартова сумма циклических групп $\mathbb{Z}(p^k)$, а C_2 — декартова сумма квазициклических групп. Очевидно, C_2 является максимальной делимой подгруппой группы C. В силу того, что, C_2 — вполне характеристическая подгруппа, следовательно, $C_2 = (A \cap C_2) \oplus (B \cap C_2)$. Первое слагаемое здесь должно быть нулевым (в силу редуцированности). Поэтому $C_2 \leqslant B$ и $A \oplus (B/C_2) \cong C_1$. $\boxtimes$

Следствие 1.3.1.4. *[6, следствие 38.3] Декартова сумма групп алгебраически компактно тогда и только тогда, когда каждая компонента алгебраически компактна.*

Объединяя лемму 1.2.10.5 с этой теоремой, получаем

Следствие 1.3.1.5. *[6, следствие 38.4] Всякую группу можно вложить в качестве сервантной подгруппы в алгебраически компактную группу.*

Предложение 1.3.1.6. *[6, предложение 38.5] Группа A алгебраически компактна тогда и только тогда, когда A служит прямым слагаемым для всякой такой группы G, что A — сервантная подгруппа группы G, а факторгруппа G/A изоморфна группе $\mathbb{Q}$ или некоторой группе $\mathbb{Z}(p^\infty)$.*

Доказательство. Нужно проверить только достаточность условия. Предположим, что группа A обладает указанным свойством. Тогда группа A должна выделяться прямым слагаемым из всякой группы G, где она — сервантная подгруппа и G/A — делимая группа. В самом деле, это вытекает из наших предположений, леммы 1.1.1.4 и теоремы 1.2.2.1. Рассмотрим, далее, случай, когда A —сервантная подгруппа группы G и G/A — периодическая группа. Если B/A — базисная подгруппа группы G/A, то из теоремы 1.2.8.2 имеем $B = A \oplus B'$ для некоторой подгруппы $B' \leqslant B$. Теперь $G/B \cong (G/A)/(B/A)$ — делимая группа, поэтому G/B' содержит $B/B' \cong A$ в качестве сервантной подгруппы, факторгруппа по которой делима. Следовательно, $G/B' = B/B' \oplus G'/B'$ для некоторой подгруппы $G' \leqslant G$. Так как $G = B + G' = A + B' + G' = A + G'$ и $A \cap G' = (A \cap B) \cap G' = A \cap (B \cap G') = A \cap B' = 0$, то $G = A \oplus G'$.

Если G/A — группа без кручения, то из теоремы 1.2.5.7 легко следует, что существует такая группа H, что $G \leqslant H$ и H/A — делимая группа без кручения. По первой части настоящего доказательства группа A служит прямым слагаемым для группы H, а тогда и для группы G. Наконец, если G/A — произвольная группа и T/A — ее периодическая часть, то A служит прямым слагаемым для группы T, т. е. $T = A \oplus T'$, а так как $T/T' \cong A$ — прямое слагаемое группы G/T', то $G = A \oplus G'$ для некоторой подгруппы $G' \leqslant G$. ⊠

§2 Полные группы

Определение 1.3.2.1. [6, стр. 42] *$\mathbb{Z}$-адическая топология* — это такая топология, в которой базу окрестностей нуля образуют подгруппы nA $(n \in \mathbb{Z})$. Аналогично, *p-адическая топология* — это такая топология, в которой базу окрестностей нуля образуют подгруппы $p^n A$.

Определение 1.3.2.2. [6, стр. 82] Последовательность $\{a_i\}_{i \in I}$ называется *последовательностью Коши*, если для любого заданного индекса $i \in I$ существует такой индекс $j \in I$, что

$$a_k - a_{k'} \in U_i, \text{ если } k, k' \geqslant j.$$

Определение 1.3.2.3. [6, стр. 82] Группа A называется *полной* в заданной топологии, если она хаусдорфова и если всякая последовательность Коши в группе A имеет в A предел.

Теорема 1.3.2.4. *[6, теорема 39.1] Группа полна в $\mathbb{Z}$-адической топологии тогда и только тогда, когда она — редуцированная алгебраически компактная группа.*

Доказательство. Предположим сначала, что A — редуцированная алгебраически компактная группа. Из следствия 1.3.1.3 мы знаем, что она служит прямым слагаемым для декартовой суммы циклических групп $\mathbb{Z}(p^k)$. Так как каждая группа $\mathbb{Z}(p^k)$ полна в своей $\mathbb{Z}$-адической топологии и декартова сумма полных групп вновь является полной группой, группа A полна в своей $\mathbb{Z}$-адической топологии.

Предположим теперь, что группа A полна в своей $\mathbb{Z}$-адической топологии. Тогда группа A хаусдорфова. Следовательно, она редуцированная. Действительно, в противном случае группа A содержит нетривиальную делимую подгруппу, которая выделяется прямым слагаемым и, следовательно, полна. Но делимая группа, очевидно, неполна в $\mathbb{Z}$-адической топологии. Пусть группа G содержит группу A в качестве сервантной подгруппы, причем можно считать, что G/A — делимая группа. Для завершения доказательства нам нужно только показать, что A служит для G прямым слагаемым (см. предложение 1.3.1.6).

Заметим, что группа A плотна в G. Действительно, подгруппа A плотна в $\mathbb{Z}$-адической топологии, если для любой подгруппы H конечного индекса $A+H=G$. Ясно, что ее образ в группе G/A также является подгруппой конечного индекса. Но так как G/A — делимая группа, она не содержит подгрупп конечного индекса. Если группа G хаусдорфова в своей $\mathbb{Z}$-адической топологии, то в силу плотности подгруппы A в G каждый элемент $g \in G$ является пределом некоторой последовательности элементов из A. Так как индуцированная топология группы A совпадает с $\mathbb{Z}$-адической топологией группы A, то эта последовательность является последовательностью Коши в группе A, откуда $g \in A$ и $A = G$.

Пусть $\mathfrak{X}$ — класс всех конечных циклических групп. Положим $U(G) = G^1 = \cap_\varphi \mathrm{Ker}\ \varphi$, где $\varphi : A \longrightarrow X \in \mathfrak{X}$. Если группа G не хаусдорфова, то группа G/G^1 хаусдорфова. Действительно, предел хаусдорфовой последовательности определен с точностью до $\cap U_i$, где U_i — подгруппы конечного индекса. Но очевидно, что $G^1 \leqslant \cap U_i$. В силу предложения 1.3.1.3, справедливо $A \cap G^1 = 0$, поэтому $A_1 \cong (A + G^1)/G^1$ является сервантной подгруппой группы G/G^1. В силу доказанного выше, $A \cong G/G^1$, следовательно, $G = A \oplus G^1$. ⊠

Предложение 1.3.2.5. *[6, предложение 13.1] Пусть группа A полна в некоторой топологии. Подгруппа группы A замкнута тогда и только тогда, когда она полна в индуцированной топологии.*

Доказательство. Это обычная топологическая лемма. ⊠

Предложение 1.3.2.6. *[6, предложение 13.2] Если B — замкнутая подгруппа полной группы A, и B содержит счетную базу окрестностей нуля, то факторгруппа A/B полна в индуцированной топологии.*

Доказательство. По предположению существует такая база $\{U_m\}_m$ окрестностей нуля в A, что $U_1 \supseteq U_2 \supseteq \ldots$ и $\cap_m U_m = 0$. Группы $\overline{U}_m = (U_m + B)/B$ $(m = 1, 2, \ldots)$ образуют базу окрестностей нуля в A/B. Пусть $a_1 + B, \ldots, a_m + B, \ldots$ — последовательность Коши в группе A/B, которую без ограничения общности можно считать чистой, т. е. такой, что $a_{m+1} - a_m + B \subseteq U_m + B$ для любого m. Положим $c_1 = a_1$ и предположим, что элементы $c_1, \ldots, c_m \in A$ уже выбраны так, что $c_i \in a_i + B$ и $c_i - c_{i-1} \in U_{i-1}$, $i = 2, \ldots, m$. Тогда $a_{m+1} - c_m = u_m + b_m \in a_{m+1} + B$ для некоторых $u_m \in U_m$, $b_m \in B$. Положим $c_{m+1} = a_{m+1} - b_m \in a_{m+1} + B$ и получим $c_{m+1} - c_m \in U_m$. Таким образом, существует последовательность $\{c_m\}_m$ со свойствами $c_m \in a_m + B$ и $c_{m+1} - c_m \in U_m$ при любом m. Другими словами, с помощью заданной последовательности Коши $\{a_m + B\}$ группы A/B можно получить последовательность Коши $\{c_m\}$ в группе A. Если $a \in A$ — предел последовательности $\{c_m\}$, то $\overline{a} = a + B$ — предел последовательности $\{a_m + B\}$. Так как B — замкнутая подгруппа группы A, то группа A/B хаусдорфова. ⊠

Замечание. Часть теоремы 1.3.2.4, касающуюся необходимости, можно немного усилить, заметив, что *группа A полна в $\mathbb{Z}$-адической топологии, если она полна в некоторой [хаусдорфовой] топологии, более грубой, чем $\mathbb{Z}$-адическая топология.* В самом деле, пусть

$a_1, \dots, a_n \dots$ — последовательность Коши в $\mathbb{Z}$-адической топологии, где, как можно предполагать, для любого n имеет место равенство $a_n - a_{n+1} = n! g_n$ [при некотором $g_n \in A$]. (В случае необходимости можно проредить последовательность.) Положим

$$b_{nk} = g_n + (n+1)g_{n+1} + \dots + (n+1)\dots(n+k)g_{n+k}.$$

Тогда последовательность $b_{n0}, \dots, b_{nk}, \dots$ будет снова последовательностью Коши в $\mathbb{Z}$-адической топологии, так как $k! | (n+1)\dots(n+k)$, и мы будем иметь $a_n = n! b_{nk} + a_{n+k+1}$ для любых n и k. Всякая последовательность Коши в $\mathbb{Z}$-адической топологии является последовательностью Коши в более грубой топологии, поэтому при $k \longrightarrow \infty$ получим $a_n = n! b_n + a$, где a и b_n — пределы соответственно последовательностей $\{a_n\}$ и $\{b_{nk}\}$. Следовательно, $a - a_n \in n! A$ и элемент a служит пределом последовательности $\{a_n\}$ также в $\mathbb{Z}$-адической топологии.

Так как $\mathbb{Z}$-адическая топология группы A индуцирует топологию на подгруппе B, более грубую, чем $\mathbb{Z}$-адическая топология группы B (группа B не обязана быть сервантной), то из теоремы 1.3.2.4, нашего замечания, предложения 1.3.2.5 и предложения 1.3.2.6 получаем

Следствие 1.3.2.7. *[6, следствие 39.2] Если A — редуцированная алгебраически компактная группа и B — такая ее подгруппа, что $(A/B)^1 = 0$, то B и A/B — редуцированные алгебраически компактные группы.*

Следствие 1.3.2.8. *[6, следствие 39.3] Если θ — эндоморфизм полной группы A, то* $\mathrm{Ker}\,\theta$ *и* $\mathrm{Im}\,\theta$ *— полные группы.*

Доказательство. Положим $B = \mathrm{Ker}\,\theta$, применим следствие 1.3.2.7 и заметим, что $A/\mathrm{Ker}\,\theta$ — полная группа в силу предложения 1.3.2.6. ⊠

Предложение 1.3.2.9. *[6, предложение 39.4] Обратный предел редуцированных алгебраически компактных групп является редуцированной алгебраически компактной группой. В частности, J_p (группа целых p-адических чисел) — алгебраически компактная группа.*

Доказательство. Из общей теории проконечных групп следует, что обратный предел является замкнутой подгруппой декартовой суммы в топологии произведения. В силу предположений и следствия 1.3.1.4 декартова сумма является алгебраически компактной группой. Остается применить следствие 1.3.2.7. ⊠

Теорема 1.3.2.10. *[6, теорема 39.5] Для любой группы A группа*

$$\widehat{A} = \varprojlim_n A/nA$$

является полной. Каноническое отображение $\mu : a \mapsto (\dots, a + nA, \dots) \in \widehat{A}$ имеет ядро A^1, $A\mu$ — сервантная подгруппа группы $\widehat{A}$ и $\widehat{A}/A\mu$ — делимая группа.

Доказательство. Так как группы A/nA ограниченные и, следовательно, алгебраически компактные, то первая часть теоремы вытекает из предложения 1.3.2.9. Очевидно, $A\mu = 0$ дает $a \in nA$ для любого n, откуда $\mathrm{Ker}\,\mu = A^1$. Если для элемента $\widehat{a} = (\dots, a_n + nA, \dots)$ $(a_n \in A)$ выполнено равенство $m\widehat{a} = A\mu$ при некотором $a \in A$, то $ma_n - a \in nA$ для каждого n, в частности для $n = m$, откуда $a \in mA$, что дает сервантность подгруппы $A\mu$ в группе $\widehat{A}$. Чтобы доказать делимость группы $\widehat{A}/A\mu$, достаточно показать, что индуцированная топология в группе $\widehat{A}$ совпадает с $\mathbb{Z}$-адической топологией, так как тогда из плотности подгруппы $A\mu$ в группе $\widehat{A}$ сразу будет следовать делимость $\widehat{A}/A\mu$. (Плотность группы A вытекает из [6, теорема 13.6] и это доказательство мы приводить не будем.)

Поскольку группы A/nA ограниченные и, следовательно, дискретные, то окрестностями нуля в группе $\widehat{A}$ служат $U_n = \pi_n^{-1}0$, где π_n есть n-ая координатная проекция $\widehat{A} \longrightarrow A/nA$. Покажем, что $U_n = n\widehat{A}$. Так как включение $n\widehat{A} \subseteq U_n$ очевидно, предположим, что $\widehat{a} \in U_n$, т. е. $\widehat{a} = (\ldots, a_m + mA, \ldots)$, где $a_n = 0$. Для любого m существует такой элемент $c_m \in A$, что $a_{(m+1)!n} - a_{m!n} = m!nc_m$. Положим $b_1 = 0$ и $b_{m+1} = b_m + m!c_m$ при $m > 1$. Тогда по индукции получится $a_{m!n} = nb_m$ для каждого $m \geqslant 1$, и $\widehat{b} = (\ldots, b_m + m!A, \ldots) \in \widehat{A}$. Для этого элемента $\widehat{b}$ выполнено равенство $n\widehat{b} = \widehat{a}$, откуда $U_n \subseteq n\widehat{A}$. ⊠

Предложение 1.3.2.11. *[6, предложение 39.7] Гомоморфизм $\alpha : A \longrightarrow B$ индуцирует единственный гомоморфизм $\widehat{\alpha} : \widehat{A} \longrightarrow \widehat{B}$, для которого диаграмма*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \mu\downarrow & & \downarrow\nu \\ \widehat{A} & \xrightarrow{\widehat{\alpha}} & \widehat{B} \end{array} \tag{1.17}$$

коммутативна (вертикальные отображения — канонические).

Определение 1.3.2.12. [6, стр. 194] Группа $\widehat{A}$ называется $\mathbb{Z}$-*адическим пополнением* группы A. В силу предложения 1.3.2.11 соответствие $A \mapsto \widehat{A}$, $\alpha \mapsto \widehat{\alpha}$ является функтором из категории $\mathcal{A}$ в категорию полных групп.

Теорема 1.3.2.13. *[6, теорема 12.3] Пусть*

$$\mathbf{A} = \{A_i(i \in I); \pi_i^j\},\ \mathbf{B} = \{B_i(i \in I); \rho_i^j\},\ \mathbf{C} = \{C_i(i \in I); \sigma_i^j\}$$

— обратные спектры с одним и тем же множеством индексов I и $\varphi : \mathbf{A} \longrightarrow \mathbf{B}$, $\psi : \mathbf{B} \longrightarrow \mathbf{C}$ — такие гомоморфизмы, что последовательность

$$0 \longrightarrow \mathbf{A} \xrightarrow{\varphi} \mathbf{B} \xrightarrow{\psi} \mathbf{C}$$

точна (т. е. для каждого i точна последовательность

$$0 \longrightarrow A_i \xrightarrow{\varphi_i} B_i \xrightarrow{\psi_i} C_i).$$

Тогда для обратных пределов имеет место точная последовательность

$$0 \longrightarrow A^* \xrightarrow{\varphi^*} B^* \xrightarrow{\psi^*} C^*,$$

где $A^* = \varprojlim_I A_i$ (и аналогично B^* и C^*), а φ^* и ψ^* — канонические продолжения гомоморфизмов φ и ψ.

Доказательство. Если каждый гомоморфизм φ_i — мономорфизм и $a\varphi^* = 0$ для некоторого $a \in A^*$, то $a\pi_i\varphi_i = a\varphi^*\rho_i = 0$, откуда $a\pi_i = 0$ для любого $i \in I$, т. е. $a = 0$. Если π_i, ρ_i, σ_i — канонические отображения, то диаграмма

$$\begin{array}{ccccccc} 0 \longrightarrow & A^* & \xrightarrow{\varphi^*} & B^* & \xrightarrow{\psi^*} & C^* & \\ & \downarrow \pi_i & & \downarrow \rho_i & & \downarrow \sigma_i & \quad (i \in I) \\ 0 \longrightarrow & A_i & \xrightarrow{\varphi_i} & B_i & \xrightarrow{\psi_i} & C_i & \end{array}$$

коммутативна. Пусть $b \in \mathrm{Ker}\ \psi^*$. В силу того, что $b\rho_i\psi_i = b\psi^*\sigma_i = 0$, и точности нижней строки при каждом $i \in I$ существует $a_i \in A_i$, для которого $a_i\varphi_i = b\rho_i$. При $j > i$ имеем $a_j\pi_i^j\varphi_i = a_j\varphi_j\rho_i^j = b\rho_j\rho_i^j = b\rho_i = a_i\varphi_i$, откуда $a_j\pi_i^j = a_i$, так как φ_i — мономорфизм. Мы заключаем, что $a = (\ldots, a_i, \ldots, a_j, \ldots) \in A^*$. Для этого элемента a имеем $a\varphi^*\rho_i = a\pi_i\varphi_i = a_i\varphi_i = b\rho_i$ при каждом i, откуда $a\varphi^* = b$. ⊠

Теорема 1.3.2.14. *[6, теорема 39.8] Пусть $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ — сервантно точная последовательность. Тогда последовательность*

$$0 \longrightarrow \widehat{A} \xrightarrow{\widehat{\alpha}} \widehat{B} \xrightarrow{\widehat{\beta}} \widehat{C} \longrightarrow 0 \tag{1.18}$$

точна и расщепляема.

Доказательство. Если заданная последовательность сервантно точна, то в силу теоремы 1.2.9.3 индуцированные последовательности $0 \longrightarrow A/nA \longrightarrow B/nB \longrightarrow C/nC \longrightarrow 0$ точны для всех n. Из теоремы 1.3.2.10 и теоремы 1.3.2.13 следует, что последовательность

$$0 \longrightarrow \widehat{A} \xrightarrow{\widehat{\alpha}} \widehat{B} \xrightarrow{\widehat{\beta}} \widehat{C}$$

точна. Таким образом, для доказательства точности последовательность 1.18 достаточно проверить, что $\widehat{\beta}$ — эпиморфизм. Здесь $\mathrm{Im}\ \widehat{\beta} \leqslant \widehat{C}$, и из следствия 1.3.2.7 вытекает полнота группы $\mathrm{Im}\ \widehat{\beta}$. Так как $\mathrm{Im}\ \widehat{\beta}$ содержит образ группы C при каноническом отображении, плотный в группе $\widehat{C}$, то обязательно $\mathrm{Im}\ \widehat{\beta} = \widehat{C}$. Плотность следует из того, что $\widehat{C}$ является пополнением группы C. Остается доказать сервантность подгруппы $\mathrm{Im}\ \widehat{\alpha} \cong \widehat{A}$ в группе $\widehat{B}$. Отображение $a + A^1 \mapsto a\alpha + B^1$ переводит A/A^1 в сервантную подгруппу группы B/B^1. Отсюда и из того, что подгруппа $B\nu$ сервантна в $\widehat{B}$ следует, что $A\alpha\nu$ — сервантная подгруппа группы $\widehat{B}$. Так как $\alpha\nu = \mu\widehat{\alpha}$ (см. 1.17) и $\widehat{A}\widehat{\alpha}/A\mu\widehat{\alpha}$ — делимая группа, то подгруппа $\widehat{A}\widehat{\alpha}$ сервантна в $\widehat{B}$. ⊠

Теорема 1.3.2.15. *[6, теорема 39.9] Предположим, что полная группа A содержится в прямой сумме $\sum_{i \in I} C_i$ таких групп C_i, что $C_i^1 = 0$ для каждого i. Тогда существует такое целое число $n > 0$, что подгруппа nA содержится в прямой сумме конечного числа групп C_i.*

Доказательство. Если это не так, то существует строго возрастающая последовательность натуральных чисел $n_1, \ldots, n_j, \ldots$, где $n_j | n_{j+1}$, и существуют такие группы B_j, каждая из которых есть прямая сумма конечного числа групп C_i, что эти B_j порождают в $\sum C_i$ подгруппу, являющуюся их прямой суммой, и

$$n_jA \cap \sum_{k=1}^{j-1} B_k \leqslant n_jA \cap \sum_{k=1}^{j} B_k \quad (j = 1, 2, \ldots).$$

Пусть a_j — элемент, входящий в правую часть, но не лежащий в левой части; тогда элемент a_{j-1} имеет нулевую компоненту в B_j, а элемент a_j — ненулевую. Поэтому последовательность Коши $a_1, \ldots, a_j \ldots \in A$ не может иметь предела в $\sum_i C_i$. ⊠

Следствие 1.3.2.16. *[6, следствие 39.10] Если $A = \sum_{i \in I} C_i$ — прямое разложение полной группы A, то все C_i — полные группы и существует такое целое число $n > 0$, что $nC_i = 0$ для почти всех $i \in I$.*

§3 Строение алгебраически компактных групп

Лемма 1.3.3.1. *[6, лемма 9.3] Если $A = B \oplus C$ и G — вполне характеристическая подгруппа группы A, то $G = (G \cap B) \oplus (G \cap C)$.*

Доказательство. Пусть π, θ — проекции, связанные в прямым разложением $A = B \oplus C$. Так как G — вполне характеристическая подгруппа, $G\pi$ и $G\theta$ — подгруппы группы G. Далее, из включений $G\pi \leqslant B$ и $G\theta \leqslant C$ следует, что $G\pi \cap G\theta = 0$, а $g = g\pi + g\theta$ $(g \in G)$ дает $G = G\pi + G\theta$, так что $G = G\pi \oplus G\theta$. Очевидно, $G\pi \leqslant G \cap B$ и $G\theta \leqslant G \cap C$, откуда обязательно $G\pi = G \cap B$ и $G\theta = G \cap C$. ⊠

Предложение 1.3.3.2. *[6, предложение 40.1] Редуцированная группа A алгебраически компактна тогда и только тогда, когда она имеет вид*

$$A = \overline{\sum_p} A_p, \tag{1.19}$$

где каждая группа A_p полна в своей p-адической топологии (произведение берется по всем различным простым числам p). Группы A_p однозначно определяются группой A.

Доказательство. Предположим сначала, что группа A алгебраически компактна, и пусть $A \oplus B = C$ — декартова сумма циклических p-групп (см. следствие 1.3.1.3). Соберем слагаемые $\mathbb{Z}(p^k)$, относящиеся к одному и тому же простому числу p, и образуем их декартову сумму C_p. Это подгруппа группы C, причем, очевидно, $C = \overline{\sum}_p C_p$. Подгруппы C_p являются вполне характеристическими в C, поэтому в силу леммы 1.3.3.1 имеем $C_p = A_p \oplus B_p$, где $A_p = A \cap C_p$, $B_p = B \cap C_p$. Таким образом, $C = \overline{\sum}_p A_p \oplus \overline{\sum} B_p$. Очевидно, подгруппы A_p при переменном p порождают в группе A подгруппу A_0, являющуюся их прямой суммой. Если рассматривать группу C как топологическую группу с $\mathbb{Z}$-адической топологией, то ясно, что замыкание в C подгруппы A_0 должно содержать $\overline{\sum}_p A_p$, так как $\overline{\sum}_p A_p / A_0$ — делимая группа. Действительно, пусть $\overline{a} \in \overline{\sum}_p A_p / A_0$, рассмотрим уравнение $nx = a$. Пусть $p_1, \ldots, p_k$ — все простые делители числа n. Тогда элемент $\overline{a}$ можно представить в виде $\overline{a} = a + A_0$, причем p_1-ая, …, p_k-ая координаты элемента a нулевые. Тогда для каждой из оставшихся координат уравнение $nx = a_p$ имеет решение в группе A_p, объединяя эти решения получим искомое решение для элемента $\overline{a}$. Так как $B^1 = 0$ (поскольку $C^1 = 0$), то подгруппа A замкнута в C, откуда получаем включение $\overline{\sum}_p A_p \leqslant A$. Аналогично получаем, что $\overline{\sum}_p B_p \leqslant B$. Следовательно, $A = \overline{\sum}_p A_p$, $B = \overline{\sum}_p B_p$. Как прямое слагаемое полной группы группа A_p должна быть полной в своей $\mathbb{Z}$-адической топологии, которая здесь совпадает с p-адической, так как $\mathbb{Z}$-адическая и p-адическая топологии на группе $\mathbb{Z}(p^k)$ совпадают.

Обратно, пусть A_p — группа, полная в своей p-адической топологии. Тогда группу A_p можно следующим естественным образом превратить в модуль над кольцом $\mathbb{Q}_p^*$ целых p-адических чисел. Пусть $a \in A_p$ и $\pi = s_0 + s_1 p + \ldots + s_n p^n \ldots \in \mathbb{Q}_p^*$. Последовательность

$$s_0 a, (s_0 + s_1 p)a, \ldots, (s_0 + s_1 p + \ldots + s_n p^n)a, \ldots$$

является последовательностью Коши в группе A_p, следовательно, она сходится в A_p к пределу, и мы определяем $a\pi$ как этот предел. Легко проверить, что таким путем группа A_p действительно превращается в унитарный $\mathbb{Q}_p^*$-модуль. Отсюда получается, что $qA_p = A_p$ для всех простых чисел $q \neq p$, т. е. что $\mathbb{Z}$-адическая топология в группе A_p совпадает с

p-адической. По теореме 1.3.2.4 группа A_p алгебраически компактна, а из следствия 1.3.1.4 вытекает, что декартова сумма групп A_p алгебраически компактна.

Наконец, единственность компонент A_p в разложении (1.19) сразу следует из соотношения

$$A_p = \bigcap_{q \neq p} q^k A \quad (k = 1, 2, \ldots),$$

где q опять обозначает простые числа. Это — следствие соотношений $qA_p = A_p$ $(q \neq p)$ и $\cap_k p^k A_p = 0$. $\boxtimes$

Глава 2

Нильпотентные группы

2.1 Общие свойства и примеры

§1 Определение

Определение 2.1.1.1. [6, стр. 148] Пусть G — группа. Нормальная матрешка

$$1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_s = G \tag{2.1}$$

называется *центральной*, если все ее секции центральны, т. е.

$$G_{i+1}/G_i \leqslant Z(G/G_i) \text{ для всех } i \tag{2.2}$$

или, что равносильно,

$$[G_{i+1}, G] \leqslant G_i \text{ для всех } i. \tag{2.3}$$

Группа, обладающая центральными матрешками, называется *нильпотентной*, а минимальное число секций таких матрешек — ее *ступенью нильпотентности.*

Пусть G — произвольная группа. Пусть

$$\zeta_0 G = 1, \zeta_{i+1}G/\zeta_i G = Z(G/\zeta_i G),\ i = 0, 1, 2, \ldots,$$
$$\gamma_1 G = G, \gamma_{j+1}G = [\gamma_j G, G],\ j = 1, 2, \ldots$$

Подгруппы $\zeta_i G$ называются *гиперцентрами* группы G, а подгруппы $\gamma_i G$ — это *централы* группы G. Ясно, что если некоторый централ совпадает с единицей или некоторый гиперцентр совпадает со всей группой, то группа нильпотентна.

Обратно, пусть группа G нильпотентна и 2.1 — произвольная центральная матрешка в ней. Положим для краткости $Z_i = \zeta_i G$, $\Gamma_j = \gamma_j G$. Определения и легкая индукция дают следующие включения:

$$\begin{array}{ccccccccccc}
1= & Z_0 & \leqslant & Z_1 & \leqslant & \ldots, & & & & & \\
 & \vee & & \vee & & & & & & & \\
1= & G_0 & \leqslant & G_1 & \leqslant & \ldots & \leqslant & G_{s-1} & \leqslant & G_s & =G, \\
 & & & & & & & \vee & & \vee & \\
 & & & & & \ldots & \leqslant & \Gamma_2 & \leqslant & \Gamma_1 & =G.
\end{array} \tag{2.4}$$

Отсюда видно, что в нильпотентной группе ряды гиперцентров и централов являются матрешками, т. е. содержат 1 и G, и число секций в каждой из них равно ступени нильпотентности группы. Эти ряды называются *верхним центральным* и *нижним центральным.*

§2 Общие свойства

Лемма 2.1.2.1. *[1, лемма 16.2.1] Пусть G — нильпотентная группа ступени $s \geqslant 2$. Любая ее подгруппа, порожденная коммутантом и одним элементом, имеет ступень нильпотентности меньше s.*

Доказательство. Пусть $a \in G$, $H = \langle a, [G, G]\rangle$. Так как

$$[G, G] \leqslant (\zeta_{s-1}G) \cap H \leqslant \zeta_{s-1}H,$$

то группа $H/\zeta_{s-1}H$ циклическая. Поскольку факторгруппа по центру не может быть циклической, отличной от 1, то $\zeta_{s-1}H = H$, что и требовалось. Действительно, если $G/Z(G)$ — циклическая группа, то пусть $a \in G$ — элемент, образ которого совпадает с порождающим элементом группы $G/Z(G)$. Тогда группа $\langle a, Z(G)\rangle$ абелева и совпадает с G. ⊠

Теорема 2.1.2.2. *[1, теорема 16.2.2] Любая подгруппа нильпотентной группы субнормальна. Более точно, если G — нильпотентная группа ступени s, то для любой ее подгруппы H ряд последовательных нормализаторов достигает G не позже чем через s шагов.*

Доказательство. Введем обозначения

$$Z_i = \zeta_i G, H_0 = H, H_{j+1} = N_G(H_j).$$

Достаточно проверить, что $Z_i \leqslant H_i$. Для $i = 0$ это очевидно. Перейдем от i к $i + 1$. Так как

$$[G, Z_{i+1}] \leqslant Z_i \leqslant H_i,$$

то

$$H_i^{Z_{i+1}} \leqslant H_i[H_i, Z_{i+1}] \leqslant H_i.$$

Это означает, что Z_{i+1} нормализует H_i, т. е. $Z_{i+1} \leqslant H_{i+1}$. ⊠

Теорема 2.1.2.3. *[1, теорема 16.2.3] В нильпотентной группе любая нетривиальная нормальная подгруппа имеет нетривиальное пересечение с центром.*

Доказательство. Проводится индукцией по ступени нильпотентности. Пусть G — нильпотентная группа, $H \trianglelefteq G$, $H \neq 1$, $Z_i = \zeta_i G$. Если $H \leqslant Z_1$, то утверждение тривиально. Пусть $H \nleqslant Z_1$. Тогда по индуктивному предположению, примененному к G/Z_1, пересечение $HZ_1 \cap Z_2$ содержит некоторый элемент $a \notin Z_1$. Так как

$$a = hz, h \in H, z \in Z_1,$$

то $h \in H \cap Z_2$, $h \notin Z_1$. Пусть элемент $g \in G$ таков, что $[h, g] \neq e$. Тогда

$$[h, g] \in H \cap [Z_2, G] \leqslant H \cap Z_1,$$

т. е. пересечение $H \cap Z_1$ нетривиально. ⊠

Теорема 2.1.2.4. *[1, теорема 16.2.5] Пусть G — нильпотентная группа. Если A — ее подгруппа с условием $A[G, G] = G$, то $A = G$. В частности, $[G, G] \leqslant \Phi(G)$.*

Доказательство. Пусть, напротив, $A \neq G$. Положим $A_i = A\zeta_i G$, $i = 0, 1, 2, \ldots$. Очевидно, $A_i \trianglelefteq A_{i+1}$. Пусть $A_m < G$, $A_{m+1} = G$. Так как секция A_{m+1}/A_m абелева, то $[G, G] \leqslant A_m$, откуда

$$A[G, G] \leqslant A_m < G.$$

Противоречие. ⊠

Теорема 2.1.2.5. *[1, теорема 16.2.6] В любой нильпотентной группе G любая максимальная абелева нормальная подгруппа A совпадает со своим централизатором. В частности, A — максимальная абелева подгруппа и G/A изоморфно вкладывается в* $\mathrm{Aut}\ A$.

Доказательство. Обозначим $H = C_G(A)$, $Z_i = \zeta_i G$. Пусть уже доказано, что $H \cap Z_i \leqslant A$, и пусть $x \in H \cap Z_{i+1}$. Для всякого $g \in G$ имеем $[x, g] \in H \cap Z_i \leqslant A$, поэтому $\langle x, A\rangle$ — абелева нормальная подгруппа из G, содержащая A. Ввиду максимальности A имеем $x \in A$, т. е. $H \cap Z_{i+1} \leqslant A$. Так как $Z_n = G$ при некотором n, то $H = A$. ⊠

Теорема 2.1.2.6. *[1, теорема 16.2.7] В любой нильпотентной группе G совокупность τG периодических элементов есть подгруппа (периодическая часть группы G).*

Доказательство. Вновь используем индукцию по ступени нильпотентности при помощи леммы 2.1.2.1. Пусть a, b — периодические элементы группы G. Положим

$$A = \langle a[G, G]\rangle,\ B = \langle b, [G, G]\rangle.$$

По индуктивному предположению τA, τB — подгруппы в A, B соответственно. Так как τA эндоморфно допустима в A, а A нормальна в G, то τA нормальна в G. По той же причине τB нормальна в G. Так как любой элемент из $\tau A \cdot \tau B$ при возведении в подходящую степень попадает сначала в τB, а затем в 1, то группа $\tau A \cdot \tau B$ периодическая. В частности, элементы $ab\ a^{-1}$ периодические. ⊠

Теорема 2.1.2.7. *[1, теорема 16.2.8] В любой нильпотентной группе G без кручения извлечение корней — однозначная операция (хотя и не обязательно всюду определенная), т. е. из $a^n = b^n$, $n =\neq 0$ следует $a = b$.*

Доказательство. Индукция по ступени нильпотентности. Так как для абелевых групп теорема очевидна, то будем считать, что G неабелева. Рассмотрим подгруппу $\langle a, [G, G]\rangle$. Она нормальна в G и имеет меньшую ступень нильпотентности (лемма 2.1.2.1). Так как $a, a^b \in \langle a, [G, G]\rangle$ и, очевидно, $(a^b)^n = a^n (= b^n)$, то по индуктивному предположению $a^b = a$. Значит элементы a и b перестановочны, откуда $(ab^{-1})^n = e$. Так как G без кручения, то $a = b$. ⊠

Предложение 2.1.2.8. *[1, упражнение 16.2.9] В любой нильпотентной группе без кручения $x^m y^n = y^n x^m$ $(m, n \neq 0) \Longrightarrow xy = yx$.*

Доказательство. Имеем $(y^{-n} x y^n)^m = x^m$, поэтому, в силу теоремы 2.1.2.7, $y^{-n} x y^n = x$. Далее, $(x^{-1} y x)^n = y^n$, поэтому в силу той же теоремы, $x^{-1} y x = y$. ⊠

Предложение 2.1.2.9. *[1, упражнение 16.2.10] В нильпотентной группе без кручения все секции верхней центральной матрешки тоже без кручения.*

Доказательство. Индукция по ступени нильпотентности. При $i = 1$ утверждение очевидно. Докажем переход от i к $i+1$. Ясно, что достаточно доказать следующее утверждение. Если G — нильпотентная группа без кручения, то $G/Z(G)$ — также без кручения. Предположим, что $x^m \in Z(G)$, но $x \notin Z(G)$ для некоторых $x \in G$, $m \in \mathbb{N}$. Тогда x^m перестановочен с любым элементом из G, следовательно, по предложению 2.1.2.8, элемент x перестановочен с любым элементом из G, поэтому $x \in Z(G)$, противоречие. $\boxtimes$

Лемма 2.1.2.10. *[1, лемма 3.2.3] (лемма о трех коммутантах) Пусть A, B, C — подгруппы некоторой группы, H — ее нормальная подгруппа. Если два из коммутантов*

$$[A, B, C], [B, C, A], [C, A, B]$$

лежат в H, то и третий лежит в H.

Доказательство. Доказательство вытекает из следующего соотношения, проверяемого непосредственно (тождества Ф. Холла):

$$[a, b^{-1}, c]^b [b, c^{-1}, a]^c [c, a^{-1}, b]^a = 1.\boxtimes$$

Предложение 2.1.2.11. *[1, упражнение 3.2.6] Если A, B и C нормальные подгруппы группы G, то $[AB, C] \leqslant [A, C][B, C]$ и*

$$[A, B, \underbrace{G, \ldots, G}_{n}] \leqslant \prod_{i+j=n} \left[[A, \underbrace{G, \ldots, G}_{i}], [B, \underbrace{G, \ldots, G}_{j}] \right].$$

Доказательство. Легко проверить, что для трех нормальных подгрупп A, B и C справедливо соотношение $[AB, C] = [A, C][B, C]$. Отсюда получаем следующую цепочку равенств.

$$[A, B, \underbrace{G, \ldots, G}_{n+1}] = \left[\prod_{i+j=n} \left[[A, \underbrace{G, \ldots, G}_{i}], [B, \underbrace{G, \ldots, G}_{j}] \right], G \right] =$$

$$= \prod_{i+j=n} \left[\left[[A \underbrace{G, \ldots, G}_{i}], [B, \underbrace{G, \ldots, G}_{j}] \right], G \right]$$

Далее, коммутанты

$$\left[\left[[B, \underbrace{G, \ldots, G}_{j}], G \right], [A \underbrace{G, \ldots, G}_{i}] \right]$$

и

$$\left[\left[G, [A, \underbrace{G, \ldots, G}_{i}] \right], [B \underbrace{G, \ldots, G}_{j}] \right],$$

очевидно, лежат в

$$\prod_{i+j=n+1} \left[[A, \underbrace{G, \ldots, G}_{i}], [B, \underbrace{G, \ldots, G}_{j}] \right],$$

следовательно, по лемме о трех коммутантах, каждый коммутант

$$\left[\left[[A\underbrace{G,\ldots,G}_{i}],[B,\underbrace{G,\ldots,G}_{j}]\right],G\right]$$

также лежит в

$$\prod_{i+j=n+1}\left[[A,\underbrace{G,\ldots,G}_{i}],[B,\underbrace{G,\ldots,G}_{j}]\right].$$

⊠

Теорема 2.1.2.12. *[1, теорема 16.2.12] Во всякой группе произведение двух нормальных нильпотентных подгрупп ступеней s, t есть нормальная нильпотентная подгруппа ступени $\leqslant s+t$.*

Доказательство. Пусть $A \trianglelefteq G$, $B \trianglelefteq G$, $\gamma_{s+1}A = 1$, $\gamma_{t+1}B = 1$. Тогда

$$\gamma_n(AB) = [\underbrace{AB,\ldots,AB}_{n}] = \prod [H_1,\ldots,H_n], \tag{2.5}$$

где каждое H_i совпадает либо с A, либо с B (см. предложение 2.1.2.11). Так как $\gamma_i A \overset{e}{\leqslant} A \trianglelefteq G$, то $\gamma_i A \trianglelefteq G$ и, значит,

$$[\gamma_i A, B] \leqslant \gamma_i A \text{ для всех } i.$$

Таким образом, если i членов из $H_1,\ldots,H_n$ совпадают с A, а остальные $n-i$ совпадают с B, то

$$[H_1,\ldots,H_n] \leqslant \gamma_i A \cap \gamma_{n-i} B. \tag{2.6}$$

Возьмем $n = s+t+1$. Тогда либо $i \geqslant s+1$, либо $n-i \geqslant t+1$, откуда ввиду (2.5), (2.6) $\gamma_n(AB) = 1$. ⊠

Предложение 2.1.2.13. *[1, упражнение 14.4.2] Для любой группы G имеем*

$$[\gamma_i G, \gamma_j G] \leqslant \gamma_{i+j} G, \quad i,j = 1,2,\ldots.$$

Доказательство. Проводится индукцией, с помощью леммы о трех коммутантах. ⊠

Теорема 2.1.2.14. *[1, теорема 16.2.14] Если группа G содержит нильпотентную нормальную подгруппу N ступени r, факторгруппа по коммутанту которой G/N' нильпотентна ступени s, то сама G нильпотентна ступени $< \binom{r+1}{2}s - \binom{r}{2}$.*

Доказательство. Покажем сначала, что для каждого $i = 1,2,\ldots$ найдется такое число $m(i,s)$, что

$$[\gamma_i N, \underbrace{G,\ldots,G}_{m(i,s)}] \leqslant \gamma_{i+1} N. \tag{2.7}$$

Действительно, по условию можно взять $m(1,s) = s$, а если $m(i-1,s)$ уже найдено, то предложения 2.1.2.11 и 2.1.2.13 показывают, что можно взять $m(i,s) = m(i-1,s)+s-1$. Из этой рекуррентной формулы легко получается явная: $m(i,s) = i(s-1)+1$. Наконец, последовательное применение формулы (2.7) при $i = 1,\ldots,r$ показвает, что $\gamma_m G = 1$, где $m = \sum_{i=1}^{s} = \binom{r+1}{2}s - \binom{r}{2}$. ⊠

§3 Нильпотентные группы автоморфизмов

Лемма 2.1.3.1. *[1, лемма 16.3.1] Пусть в группе G задана $(r+1)$-членная матрешка*

$$G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_r = 1 \tag{2.8}$$

и Φ — группа всех автоморфизмов группы G, оставляющих члены матрешки (2.8) инвариантными и действующих тождественно в секциях G_i/G_{i+1} (стабилизатор матрешки (2.8)). Будем рассматривать G, Φ как подгруппы голоморфа $\mathrm{Hol}\, G$.

Тогда группы Φ и $[G, \Phi]$ нильпотентны ступени $< r$.

Доказательство. а) Группа Φ нильпотентна ступени $< r$. Действительно, по условию

$$G_i^{\Phi} = G_i, \ [G_i, \Phi] \leqslant G_{i+1} \text{ для всех } i. \tag{2.9}$$

Пусть Φ_j — централизатор в Φ секций G_i/G_{i+j}, $i = 0, 1, 2, \ldots$. Очевидно, $\Phi = \Phi_1 \geqslant \Phi_2 \geqslant \ldots \geqslant \Phi_r = 1$, (здесь полагается, что $C_\Phi(G) = 1$) и нам достаточно доказать, что это центральная матрешка в Φ, т. е. $[\Phi_j, \Phi] \leqslant \Phi_{j+1}$ для всех j или $[G_i, [\Phi_j, \Phi]] \leqslant G_{i+j+1}$ для всех i, j. Но это следует из соотношений

$$[\Phi_j, [\Phi, G_i]] \leqslant [\Phi_j, G_{i+1}] \leqslant G_{i+j+1},$$

$$[\Phi, [G_i, \Phi_j]] \leqslant [\Phi, G_{i+j}] \leqslant G_{i+j+1}$$

ввиду леммы о трех коммутантах 2.1.2.10.

б) Группа $[G, \Phi]$ нильпотентна ступени $< r$. Действительно,

$$[G, [\Phi, G_i]] \leqslant [G, G_{i+1}] \leqslant G_{i+1},$$

$$[\phi, [G_i, G]] \leqslant [\Phi, G_i] \leqslant G_{i+1},$$

поэтому, снова ввиду леммы о трех коммутантах, $[G_i, [G, \Phi]] \leqslant G_{i+1}$ для всех i. Это означает, что сопряжения элементами из $[G, \Phi]$ действуют тождественно в секциях матрешки $G_1 \geqslant G_2 \geqslant \ldots \geqslant G_r = 1$. По уже доказанному утверждению а) группа этих сопряжений, т. е. $[G, \Phi]/C_{[G,\Phi]}(G_1)$, нильпотентна ступени $< r - 1$. Но $[G, \Phi] \leqslant G_1$, поэтому $C_{[G,\Phi]}(G_1)$ лежит в центре $[G, \Phi]$. Отсюда и следует б). ⊠

Теорема 2.1.3.2. *[1, теорема 16.3.2] Стабилизатор любой (не обязательно нормальной) $(r+1)$-членной матрешки подгрупп есть нильпотентная группа ступени $\leqslant \binom{r}{2}$.*

Доказательство. Индукция по r. Пусть Φ — стабилизатор матрешки (2.8). Пусть еще $\Psi = C_\Phi(G_1)$. Так как Φ стабилизирует r-членную матрешку $G_1 \geqslant G_2 \geqslant \ldots$, то по индуктивному предположению группа Φ/Ψ нильпотентна ступени $\leqslant \binom{r-1}{2}$, т. е. $\gamma_{1+\binom{r-1}{2}}\Phi \leqslant \Psi$. Обозначим $\Psi_1 = \Psi$, $\Psi_{i+1} = [\Psi_i, \Phi]$. Так как $\Psi \trianglelefteq \Phi$, то $\Psi = \Psi_1 \geqslant \Psi_2 \geqslant \ldots$. Нам достаточно доказать, что $[G, \Psi_r] = 1$. Для этого мы проверим, что $[G, \Psi_i] \leqslant G_i$ для всех i. Для $i = 1$ это очевидно. Перейдем от i к $i+1$. Пусть $g \in G$, $\psi_{i+1} \in \Psi_{i+1}$. Надо показать, что $[\psi_{i+1}, g] \in G_{i+1}$. Но ψ_{i+1} — слово от коммутаторов вида $[\psi_i, \varphi^{-1}]$, $\psi_i \in \Psi_i$, $\varphi \in \Phi$. Элемент ψ_{i+1}^g — то же самое слово от произведений

$$[\psi_i, \varphi^{-1}]^g = [\psi_i, \varphi^{-1}][\psi_i, \varphi^{-1}, g]. \tag{2.10}$$

(Здесь мы используем равенство $a^g = a[a, g]$.) Заметим, что $[\psi_i, \varphi, g] \in G_{i+1}$ ввиду тождества Ф. Холла (см. 2.1.2.10) и соотношений $[\varphi, g^{-1}, \psi_i] \in [\Phi, G, \Psi_i] \leqslant [G_1, \Psi] = 1$, $[g, \psi_i^{-1}, \varphi] \in [G, \Psi_i, \Phi] \leqslant [G_i, \Phi] \leqslant G_{i+1}$. Таким образом, в произведении (2.10) левый множитель принадлежит Ψ, а правый — G_{i+1}. Но Ψ централизует $G_1 \geqslant G_{i+1}$, поэтому $\psi_{i+1}^g \in \psi_{i+1} G_{i+1} = G_{i+1}$. Отсюда $[\psi_{i+1}, g] \in G_{i+1}$. ⊠

§4 Корни из подгрупп

Определение 2.1.4.1. [1, стр. 159] Если G — группа, H — ее подгруппа, то пусть $\sqrt{H}$ обозначает совокупность всех элементов из G, которые в некоторой степени попадают в H (*корень* из H в G; более точное обозначение: $\sqrt{H}|_G$).

Предложение 2.1.4.2. *[1, упражнение 14.4.1] Пусть G — произвольная группа. Если G порождается множеством M, то централ $\gamma_i G$ порождается следующим централом $\gamma_{i+1}G$ и простыми коммутаторами веса i от элементов из M.*

Доказательство. Для $i = 1$ очевидно. Перейдем от i к $i+1$. По определению $\gamma_{i+1}G$ порождается элементами $[x, y]$, $x \in \gamma_i G$, $y \in G$. По индуктивному предположению $x = x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} z$, где каждое x_i — простой коммутатор веса i от элементов из M, $z \in \gamma_{i+1}G$, $\varepsilon_j = \pm 1$. Далее, y — слово от элементов из $M \cup M^{-1}$. Используя коммутаторные соотношения (предложение 2.1.4.4), мы видим, что $[x, y]$ — слово от элементов вида

$$[x_j, a]^g = [x_j, a][x_j, a, g],\ \ [z, a]^g,\ \ a \in M,\ \ g \in G.$$

Так как $[x_j, a, g]$, $[z, a]$ принадлежат $\gamma_{i+2}G$, то все доказано. ⊠

Предложение 2.1.4.3. *[1, упражнение 16.1.6] Любая конечно порожденная нильпотентная группа является полициклической.*

Доказательство. Легко доказывается с помощью индукции из предыдущего предложения. ⊠

Непосредственной проверкой доказывается следующее предложение.

Предложение 2.1.4.4. *[1, стр. 38] Справедливы следующие коммутаторные тождества*

$$[a, b]^{-1} = [b, a],\ \ [ab, c] = [a, c]^b [b, c], [a^{-1}, b] = [b, a]^{a^{-1}}.$$

Теорема 2.1.4.5. *[1, теорема 16.4.1] Для всякой подгруппы H нильпотентной группы G корень $\sqrt{H}$ из подгруппы H в G — тоже подгруппа.*

Доказательство. Пусть $x, y \in \sqrt{H}$; надо убедиться, что $xy \in \sqrt{H}$. Положим $A = \langle x, y \rangle$, $B = A \cap H$, $A_i = \gamma_i A$. Достаточно проверить, что все $|BA_i : BA_{i+1}| < \infty$, так как тогда будет $|A : B| < \infty$. Ряд $BA_1 \geqslant BA_2 \geqslant \dots$ субнормальный с абелевыми секциями, так как справедлива следующая цепь включений

$$[BA_i, BA_i] \leqslant [B, B]^{A_i} [A_i, B]^{A_i} [A_i, A_i] \leqslant BA_{i+1}.$$

Пусть $x^m, y^m \in B$ и уже доказано, что секция BA_{i-1}/BA_i конечна и имеет период m^{i-1}. Докажем, что секция BA_i/BA_{i+1} конечно порождена и имеет период m^i. Первое вытекает из полицикличности A (см. предложение 2.1.4.3). Далее, $[A_{i-1}, A, A] \equiv 1 (\mathrm{mod}\ A_{i+1})$, поэтому функция $[u, v] (\mathrm{mod}\ A_{i+1})$, $u \in A_{i-1}$, $v \in A$, гомоморфна по обоим аргументам (т. е. отображение, задаваемое этой функцией по обоим аргументам является гомоморфизмом). Действительно, $[u_1, v] \cdot [u_2, v] \overset{1}{\equiv} [u_1, v]^{u_1} [u_2, v] = [u_1 u_2, v]$ (1 — поскольку BA_i/BA_{i+1} абелева) и $[u, v_1 v_2] = ([v_1 v_2, u])^{-1} = ([u, v_1]^{v_1} [u, v_2])^{-1} \overset{2}{\equiv} ([u, v_1][u, v_2])^{-1} \overset{3}{\equiv} ([u, v_1])^{-1} ([u, v_2])^{-1} = [u, v_1][u, v_2]$, (2 — поскольку $A_i/A_{i+1} \leqslant Z(A/A_{i+1})$, 3 — поскольку A_i/A_{i+1} абелева). Отсюда

$$A_i^{m^i} = [A_{i-1}, A]^{m^i} \leqslant [A_{i-1}^{m^{i-1}}, A^m] A_{i+1}.$$

Так как
$$A_{i-1}^{m^{i-1}} \leqslant (B \cap A_{i-1})A_i,\ \ A^m \leqslant BA_2,$$
то, применяя коммутаторные тождества (предложение 2.1.4.4), получаем $A_i^{m^i} \leqslant BA_{i+1}$. ⊠

Отметим, что нами попутно доказана следующая лемма.

Лемма 2.1.4.6. *[1, лемма 16.4.2] Если A, B — подгруппы нильпотентной группы и индекс $|A : AB'|$ конечен, то индекс $|A : B|$ также конечен.*

Теорема 2.1.4.7. *[1, теорема 16.4.3] Пусть H — подгруппа нильпотентной группы G без кручения. Гиперцентры подгрупп H и $\sqrt{H}$ (корень из H в G) связаны следующим образом:*
$$\zeta_i\sqrt{H} = \sqrt{\zeta_i H},\ \ \zeta_i H = H \cap \sqrt{\zeta_i H}.$$
Доказательство. Обозначим $H_i = \zeta_i H$ и перейдем от i к $i+1$. Прежде всего, $\zeta_{i+1}\sqrt{H} \leqslant \sqrt{H_{i+1}}$, так как для любого x из $\zeta_{i+1}\sqrt{H}$ имеем $x^m \in H$ при подходящем m и $[x^m, H] \leqslant H \cap \sqrt{H_i} = H_i$, откуда $x^m \in H_{i+1}$, $x \in \sqrt{H_{i+1}}$. Обратно, $\sqrt{H_{i+1}} \leqslant \zeta_{i+1}\sqrt{H}$, т. е. подгруппы $\sqrt{H}$, $\sqrt{H_i}$ поэлементно перестановочны по модулю $\sqrt{H_i}$. Действительно, пусть $x \in \sqrt{H}$, $y \in \sqrt{H_{i+1}}$, т. е. $x^m \in H$, $y^n \in H_{i+1}$ при подходящих m, n. Так как $[H, H_{i+1}] \leqslant H_i \leqslant \sqrt{H_i}$, то $x^m y^n \equiv y^n x^m (\mathrm{mod}\ \sqrt{H_i})$. Так как $\sqrt{H}/\sqrt{H_i}$ — группа без кручения, то $xy \equiv yx (\mathrm{mod}\ \sqrt{H_i})$ (предложение 2.1.2.8).

Наконец, $H \cap \sqrt{H_{i+1}} = H_{i+1}$. Докажем только нетривиальное включение $H \cap \sqrt{H_{i+1}} \leqslant H_{i+1}$. Пусть $x \in H \cap \sqrt{H_{i+1}}$, $x^m \in H_{i+1}$. Тогда x^m перестановочно с любым элементом из H по модулю H_i, а, значит, таково и x (предложения 2.1.2.8 и 2.1.2.9). Отсюда $x \in H_{i+1}$. ⊠

Предложение 2.1.4.8. *[1, упражнение 16.4.4] Пусть G — конечно порожденная нильпотентная группа, H — ее подгруппа. Тогда*

а) Индекс $|\sqrt{H} : H|$ всегда конечен.

б) Если $|G : H|$ конечен, то и $|G' : H'|$ конечен.

Доказательство. а) Применить лемму 2.1.4.6 для $A = \sqrt{H}$, $B = H$.

б) Ясно, что если H — подгруппа группы G конечного индекса, то $\cap_{g\in G} H^g$ — нормальная подгруппа группы G конечного индекса. Действительно, нормальность подгруппы $\cap_{g\in G} H^g$ очевидно. Кроме того, ясно, что это — максимальная подгруппа группы H, которая нормальна в G. Далее подстановочное представление группы G на смежных классах по подгруппе H — конечная группа, следовательно, H содержит нормальную подгруппу группы G конечного индекса. Так как она лежит в $\cap_{g\in G} H^g$, получаем, что $\cap_{g\in G} H^g$ — также подгруппа конечного индекса. Таким образом, можно считать, что группа H нормальна. Пусть φ — факторизация G по $\sqrt{H'}$. Ясно, что группа H^φ абелева и индекс $|G^\varphi : H^\varphi|$ конечен. Следовательно, $G^\varphi = \sqrt{H^\varphi}$, а потому G^φ тоже абелева (см. теорему 2.1.4.7). Значит, $G' \leqslant \sqrt{H'}$, и остается учесть а). ⊠

Теорема 2.1.4.9. *[1, теорема 16.4.5] Для любых двух подгрупп H и K любой нильпотентной группы G справедливо включение $[\sqrt{H}, \sqrt{K}] \leqslant \sqrt{[H, K]}$.*

Доказательство. Пусть $x \in \sqrt{H}$, $y \in \sqrt{K}$, покажем, что $[x, y] \in \sqrt{[H, K]}$. Пусть m, n — такие показатели, что $x^m \in H$, $y^n \in K$, и $A = \langle x, y\rangle$, $B = \langle x^m, y^n\rangle$. Так как индекс $|A : BA'|$ конечен (любой элемент из A представим в виде $x^k y^l z$, где $z \in A'$, кроме того, $x^m, y^n \in B$, откуда получаем, что индекс конечен), то $|A : B|$ также конечен (лемма 2.1.4.6), а потому и $|A' : B'|$ конечен (предложение 2.1.4.8). Следовательно, $[x, y] \in \sqrt{B'}$. Далее $[\langle x^m\rangle, \langle y^n\rangle] \lhd B$. Ясно, что $B' \leqslant [H, K]$, откуда $[x, y] \in \sqrt{[H, K]}$. ⊠

2.2 Важнейшие подклассы

§1 Конечные нильпотентные группы

Теорема 2.2.1.1. (Бернсайд–Виланд). *[1, теорема 17.1.4] Пусть G — конечная группа. Следующие условия равносильны:*

а) G нильпотентна,

б) любая подгруппа из G субнормальна,

в) G — прямое произведение своих силовских p-подгрупп,

г) $[G, G] \leqslant \Phi(G)$

Доказательство. Доказательство проведем по следующей схеме:

$$\begin{array}{ccc} & \text{а)} & \\ \swarrow & \uparrow & \searrow \\ \text{б)} & | & \text{г)} \\ \searrow & | & \swarrow \\ & \text{в)} & \end{array}$$

а) $\Longrightarrow$ б) см. теорему 2.1.2.2.

б) $\Longrightarrow$ в). Пусть P — силовская p-подгруппа из G. Заметим, что $N_G(P) = N_G(N_G(P))$. Действительно, поскольку P — нормальная силовская p-подгруппа группы $N_G(P)$, она является характеристической. Поэтому если некоторый элемент x нормализует $N_G(P)$, то он нормализует P, следовательно, лежит в P. Поскольку ввиду б) нормализатор любой собственной подгруппы больше ее самой, получаем $N_G(P) = G$. Следовательно, любая силовская подгруппа нормальна в G, откуда уже легко вытекает в).

в) $\Longrightarrow$ а) очевидно.

а) $\Longrightarrow$ г) см. теорему 2.1.2.4.

г) $\Longrightarrow$ в). Опять достаточно проверить, что любая силовская p-подгруппа P нормальна в G. Пусть, напротив, $N_G(P)$ — собственная подгруппа в G и H — содержащая ее максимальная подгруппа из G. Так как $[G, G] \leqslant \Phi(G) \leqslant H$, то H нормальна в G. с другой стороны, H содержит $N_G(P)$, а потому должна совпадать со своим нормализатором в G. Действительно, пусть $H^x = H$. Тогда $P^x = P_1$ — силовская p-подгруппа группы H. В силу сопряженности силовских подгрупп, существует $h \in H$ такой, что $P^h = P_1$. Тогда $xh^{-1} \in N_G(P) \leqslant H$, откуда $x \in H$. Противоречие. ⊠

Теорема 2.2.1.2. (Фраттини) *[1, теорема 17.1.7] Подгруппа Фраттини конечной группы нильпотентна.*

Доказательство. Пусть G — конечная группа, A — ее подгруппа Фраттини. Ввиду теоремы 2.2.1.1 достаточно проверить, что любая силовская p-подгруппа P группы A нормальна в A или, что равносильно, в G, т. е. $N_G(P) = G$. Но это равносильно соотношению $G = A \cdot N_G(P)$, так как множество A конечно и состоит из непорождающих элементов группы G. Последнее соотношение мы и докажем.

Пусть g — произвольный элемент из G. Сопряжение G отображает A в себя, поэтому P^g — снова силовская p-подгруппа из A. Группы P и P^g сопряжены в A некоторым элементом $a \in A$, т. е. $P^g = P^a$. Отсюда $ga^{-1} \in N_G(P)$, $g \in A \cdot N_G(P)$. ⊠

Отметим, что нами доказана

Лемма 2.2.1.3. (лемма Фраттини) *[1, лемма 17.1.8] Пусть A — нормальная подгруппа конечной группы G, P — ее силовская p-подгруппа. Тогда $G = A \cdot N_G(P)$.*

§2 Конечно порожденные нильпотентные группы

Определение 2.2.2.1. [1, стр. 166] Будем говорить, что *группа почти* или *почти вся обладает некоторым свойством*, если она содержит нормальную подгруппу конечного индекса, обладающую этим свойством.

Теорема 2.2.2.2. *[1, теорема 17.2.1] Любая конечно порожденная нильпотентная группа G обладает центральной матрешкой с циклическими секциями и почти вся без кручения. Если G вся без кручения, то она обладает центральной матрешкой с бесконечными циклическими секциями.*

Доказательство. а) Пусть G конечно порождена и нильпотентна. Каждая секция ее нижней центральной матрешки — конечно порожденная абелева группа (см. предложение 2.1.4.2) и, значит, группа G обладает матрешкой с циклическими секциями. Поскольку уплотнение центральной матрешки — снова центральная матрешка, то G обладает центральной матрешкой с циклическими секциями. Индукцией по числу членов матрешки докажем, что G почти вся без кручения. Пусть H — максимальный член матрешки, отличный от G, a — элемент, порождающий $G \pmod H$. По индуктивному предположению H почти без кручения, поэтому при некотором m подгруппа $H^m = \langle h^m | h \in H\rangle$ без кручения. Поскольку H — конечно порожденная нильпотентная группа, как уже отмечалось, она является полициклической. Поэтому $|H : H^m| < \infty$. Если $|G : H| < \infty$, то H^m — искомая подгруппа без кручения в G. Пусть $|G : H|$ бесконечен. Тогда $\langle a, H^m\rangle$ содержит искомую подгруппу, так как она без кручения и $|G : \langle a, H^m| = |H : H \cap \langle a, H^m| \trianglelefteq |H : H^m| < \infty$.

б) Пусть G — нильпотентная группа без кручения. По доказанному она полициклическая, поэтому секции ее верхней центральной матрешки — тоже полициклические и являются группами без кручения (предложение 2.1.2.9). Поэтому верхняя центральная матрешка уплотняется до матрешки с бесконечными циклическими секциями. ⊠

Определение 2.2.2.3. [1, стр. 167] Пусть G — множество. Набор функций $f_i : G \longrightarrow \mathbb{Z}$, $i = 1, \ldots, s$ называется *координатным*, если отображение $x \mapsto (f_1(x), \ldots, f_s(x))$ является взаимно однозначным отображением множества G в множество $\mathbb{Z}^s$ всех целочисленных s-ок. Пусть $G \subseteq \mathbb{Z}^s$. Отображение $\varphi : G \longrightarrow \mathbb{Z}^r$ называется *полиномиальным*, если существуют такие многочлены $f_1, \ldots, f_r$ от s переменных с коэффициентами из поля $\mathbb{Q}$, что $x^\varphi = (f_1(x), \ldots, f_r(x))$ для $x \in G$. Если $f_1, \ldots, f_r$ — многочлены первой степени, то φ называется *линейным*.

Определение 2.2.2.4. [1, стр. 167] Пусть G — конечно порожденная нильпотентная группа без кручения. Рассмотрим в ней центральную матрешку

$$G = G_1 > G_2 > \ldots > G_{s+1} = 1$$

с бесконечными циклическими секциями и возьмем элементы $a_1, \ldots, a_s$ с условием $G_i = \langle a_i, G_{i+1}\rangle$. Очевидно, каждый элемент x из G однозначно записывается в виде $x = a_1^{t_1(x)} \ldots a_s^{t_s(x)}$, $t_i(x) \in \mathbb{Z}$, так что набор функций $t_1, \ldots, t_s$ является координатным. Упорядоченную систему $a_1, \ldots, a_s$ назовем *мальцевской базой* группы G, а числа $t_1(x), \ldots, t_s(x)$ — *координатами* элемента x в этой базе.

Теорема 2.2.2.5. *[1, теорема 17.2.4] Пусть G — конечно порожденная нильпотентная группа без кручения с отмеченными на ней мальцевскими координатами $t_1, \ldots, t_s$. Существуют натуральное число $n = n(G)$ и такое изоморфное вложение $\varphi : G \longrightarrow UT_n(\mathbb{Z})$, что отображение φ полиномиально на G, а обратное к нему отображение φ^{-1} линейно на G^φ (в матричных координатах, имеющихся на $UT_n(\mathbb{Z})$). В частности, умножение и возведение в степень в группе G записываются многочленами в мальцевских координатах. Более точно, если $x, y \in G$, $m \in \mathbb{Z}$, $1 \leqslant i \leqslant s$, то $t_i(xy)$ = многочлен над $\mathbb{Q}$ от*

$$\{t_\alpha(x), t_\alpha(y) | \alpha < i\} + t_i(x) + t_i(y), \tag{2.11}$$

$t_i(x^m)$ = многочлен над $\mathbb{Q}$ от m и

$$\{t_\alpha(x) | \alpha < i\} + mt_i(x). \tag{2.12}$$

Доказательство. а) Выведем сначала утверждение «в частности». Для любой матрицы a из $UT_n(\mathbb{Z})$ и любого m из $\mathbb{Z}$ мы имеем

$$a^m = \sum_{i=0}^{n-1} \binom{m}{i} (a - e)^i, \tag{2.13}$$

т. е. коэффициенты матрицы a^m являются многочленами от m и коэффициенты матрицы a. В силу основного утверждения теоремы координаты $t_i(xy)$, $t_i(x^m)$ линейно выражаются через коэффициенты матриц $(xy)^\varphi$, $(x^m)^\varphi$, которые полиномиально выражаются через коэффициенты матриц x^φ, y^φ и число m. Снова по основному утверждению теоремы коэффициенты матриц x^φ, y^φ полиномиально выражаются через координаты $t_\alpha(x)$, $t_\alpha(y)$, поэтому мальцевские координаты произведения xy и степени x^m являются многочленами от мальцевских координат элементов x, y и числа m. То, что эти многочлены имеют вид (2.11), (2.12), сразу вытекает из определения центральной матрешки.

б) Теперь заметим, что вместо вложения φ достаточно указать полиномиальное вложение $\psi : G \longrightarrow GL_n(\mathbb{Z})$, обратное к которому ψ^{-1} линейно на G^ψ, причем G^ψ состоит из унипотентных матриц. Действительно, группу $H = G^\psi$ путем сопряжения в $GL_n(\mathbb{Q})$ можно отобразить в $UT_n(\mathbb{Z})$. Покажем это. Мы докажем сначала, что H сопряжена с подгруппой из $UT_n(\mathbb{Q})$. Будем рассматривать $GL_n(\mathbb{Q})$ как группу автоморфизмов n-мерного векторного пространства V над полем $\mathbb{Q}$ и возьмем неуплотняемую матрешку $V = V_1 > V_2 > \ldots > V_{m+1} = 0$ подпространств, инвариантных относительно H. В базе, согласованной с этой матрешкой, автоморфизмы из H записываются клеточно-треугольными матрицами, диагональные клетки которых изображают действие H в секциях V_i/V_{i+1}, поэтому достаточно доказать, что каждая такая секция имеет размерность 1. Так как коммутант $[H, H]$ имеет меньшую ступень нильпотентности, можно считать, что $[H, H]$ приводится в унитреугольному виду (применить индукцию по ступени нильпотентности). Тогда существует ненулевой вектор $u \in U$, неподвижный относительно $[H, H]$. Пусть U' — подпространство всех таких векторов. Оно инвариантно относительно H, так как для $h \in H$, $h' \in [H, H]$ имеем $(uh)h' = u(hh'h^{-1})h = uh$. Так как секция U не содержит собственных подпространств, инвариантных относительно H, то $U' = U$. Отсюда $[H, H] = 1$ на U, т. е. H индуцирует абелеву группу автоморфизмов секции U. Но любое конечное множество перестановочных линейных преобразований имеет общий собственный вектор над расширением основного поля с помощью характеристических корней этих преобразований. Так как группа H унипотентна, то она имеет общий собственный вектор в U. Так как подпространство, натянутое на этот вектор, инвариантно относительно H и U не содержит собственных инвариантных подпространств, то U одномерно. Этим доказано, что $H^a \leqslant UT_n(\mathbb{Q})$ при подходящем $a \in GL_n(\mathbb{Q})$. Возьмем теперь в H^a конечное число порождающих матриц, возьмем общий знаменатель N их коэффициентов и рассмотрим матрицу $b = \mathrm{diag}(1, N, N^2, \dots, N^{n-1})$. Легко видеть, что $H^{ab} \leqslant UT_n(\mathbb{Z})$.

в) Остается доказать существование ψ. Мы сделаем это индукцией по длине мальцевской базы. Пусть для групп с мальцевской базой длины $< s$ требуемое матричное представление уже найдено, а вместе с ним доказана и вся теорема (см. а) и б)). Пусть группа G имеет мальцевскую базу $a_1, \dots, a_s$ длины s. В качестве подготовки к построению ψ мы установим в этом пункте формулу (2.11) для группы G. Обозначим для краткости $t_i(x) = \xi_i$, $t_i(y) = \eta_i$. Очевидно,

$$xy = a_1^{\xi_1+\eta_1}(a_1^{-\eta_1}a_2^{-1}a_1^{\eta_1})^{xi_2} \dots (a_1^{-}\eta_1 a_s^{-1}a_1^{\eta_1})^{-\xi_s}a_2^{\eta_2} \dots a_s^{\eta_s}$$

и

$$a_1^{-\eta}a_i^{-1}a_1^{\eta} = [a_1^{\eta}, a_i]a_i^{-1}.$$

По индуктивному предположению и ввиду а), б) формулы (2.11), (2.12) справедливы для групп с мальцевской базой длины $< s$, поэтому достаточно проверить, что координаты элементов $[a_1^{\eta}, a_i]$ в мальцевской базе $a_2, \dots, a_s$ — многочлены от η. Очевидно, $[a_1^{\eta}, a_i] = a_1^{-\eta}(a_i^{-1}a_1a_i)^{\eta}$ и $a_i^{-1}a_1a_i = a_1a_{i+1}^{c_{i,i+1}} \dots a_s^{c_{is}}$, $c_{ij} \in \mathbb{Z}$. Применяя к $\langle a_1, a_{i+1}, \dots, a_s\rangle$ индуктивное предположение, мы заключаем, что $(a_i^{-1}a_1a_i)^{\eta} = a_1a_{i+1}^{\zeta_{i,i+1}} \dots a_s^{\zeta_{is}}$, где ζ_{ij} — многочлены от η. Отсюда $[a_1^{\eta}, a_i] = a_{i+1}^{\zeta_{i,i+1}} \dots a_s^{\zeta_{is}}$ и формула (2.11) доказана для группы G.

г) Построение ψ. Пусть $\mathbb{Q}(t)$ — кольцо многочленов над $\mathbb{Q}$ от функций $t_1, \dots, t_s$. Определим на нем действие группы G, полагая для a из G $f^a(x) = f(ax)$, $f \in \mathbb{Q}[t]$, $x \in G$ («левый сдвиг аргумента»). Непосредственно проверяется, что оператор $\mathrm{op}(a)$, задаваемый этой формулой, является автоморфизмом кольца $\mathbb{Q}[t]$, а правило $a \mapsto \mathrm{op}(a)$ определяет изоморфизм $G \longrightarrow \mathrm{Aut}\ (\mathbb{Q}[t])$. Произведение вида $M(t) = t_1^{m_1} \dots t_s^{m_s}$ назовем *одночленом* от $t_1, \dots, t_s$. Ввиду (2.11)

$$t_i^a = t_i + \sum_j c_{ij}(a)M_j(t), \tag{2.14}$$

где $c_{ij}(a)$ — многочлен над $\mathbb{Q}$ от мальцевских координат элемента a, а одночлены $M_j(t)$, входящие с ненулевыми коэффициентами в выражение для t_i^a, не содержат переменных $t_i, \dots, t_s$ (и не зависят от a). Отсюда видно, что $\mathrm{op}(a) - \mathrm{op}(e)$ отображает произвольный одночлен $M(t)$ либо в 0, либо в либо в линейную комбинацию меньших одночленов, если считать одночлены упорядоченными по последним различным показателям. Значит, при подходящем $m = m(a, M)$ преобразование $(\mathrm{op}(a) - \mathrm{op}(e))^m$ аннулирует $M(T)$.

Пусть H — аддитивная подгруппа, порожденная орбитой множества координатных функций $\{t_1, \dots, t_s\}$ относительно операторов $\mathrm{op}(x)$, $x \in G$. Ввиду (2.14) H лежит в подгруппе, порожденной функциями $\{t_i, \frac{1}{N}M_j(t)\}$ при некотором натуральном N, а потому конечно порождена. Пусть $h_1, \dots, h_n$ — база свободной абелевой группы H. Пусть еще

$$h_k^x = \sum_l \psi_{kl}(x)h_l, \tag{2.15}$$

т. е. $(\psi_{kl}(x))$ — матрица сужения $\mathrm{op}(x)$ на H в базе $h_1, \dots, h_n$. Так как H содержит координатные функции $t_1, \dots, t_s$, то правило $x \mapsto (\psi_{kl}(x))$ определяет изоморфизм $\psi : G \longrightarrow GL_n(\mathbb{Z})$, причем G^{ψ} состоит из унипотентных матриц. Отображение ψ^{-1} линейно на G^{ψ}, так как множество $\{t_i\}$ линейно выражается через $\{h_k\}$, а вычисляя функции (2.15) в точке e, мы видим, что $\{h_k\}$ линейно выражается через $\{\psi_{kl}\}$. Само ψ полиномиально, т. е. функции ψ_{kl} являются сужениями на G некоторых многочленов над $\mathbb{Q}$. Действительно, пусть $x \in G$. Так как каждое h_k — линейная комбинация над $\mathbb{Z}$ от некоторых t_i^g, $g \in G$, то ввиду (2.13) h_l^x — такая же комбинация от $t_i^{gx} = t_i + \sum_j c_{ij}(gx)M_j(t)$. Отсюда

$$h_k^x = \sum_j P_{kj}(x)M_j(t), \tag{2.16}$$

где P_{kj} — многочлен над $\mathbb{Q}$; в частности,

$$h_k = \sum_j P_{kj}(e)M_j(t). \tag{2.17}$$

Так как множество $\{h_k\}$ линейно независимо над $\mathbb{Q}$, то таковы и строки матрицы $(P_{kj}(e))$. Подставляя (2.16), (2.17) в (2.15) и пользуясь линейной независимостью $\{M_j(t)\}$, получим для $\psi_{kl}(x)$ систему уравнений $P_{kj}(x) = \sum_l \psi_{kl}(x)P_{lj}(e)$, откуда и видно, что функции ψ_{kl} полиномиальны над $\mathbb{Q}$. ⊠

Пусть H — подгруппа конечного индекса m в произвольной группе G. Пусть $a_1, \dots, a_m$ — правые представители G по H. Если σ — точное представление группы H матрицами степени n, то формула $g \mapsto ||(a_i g a_j^{-1})^\sigma||$ задает точное представление группы G матрицами степени mn (здесь считается $x^\sigma = 0$ при $x \notin H$).

§3 Нильпотентные группы без кручения

Определение 2.2.3.1. [1, стр. 172] Произвольная группа G называется *полной*, если для любого ее элемента g и любого натурального m в G существует решение уравнения $x^m = g$. Примером полной группы является группа $UT_n(K)$ над полем K произвольной характеристики.

Определение 2.2.3.2. [1, стр. 173] Полная нильпотентная группа $\sqrt{G}$ без кручения называется *(нильпотентным) пополнением* группы G, если она содержит G и не содержит собственных полных подгрупп, содержащих G.

Теорема 2.2.3.3. А. И. Мальцев *[1, теорема 17.3.1] Любая нильпотентная группа G без кручения обладает нильпотентным пополнением той же ступени нильпотентности. Любые два нильпотентных пополнения группы G изоморфны; более того, для любого автоморфизма φ группы G существует изоморфизм между ними, продолжающий φ.*

Доказательство. а) Единственность. Пусть G_1, G_2 — группы, изоморфные G, φ — изоморфизм G_1 на G_2, $\sqrt{G_i}$ — нильпотентное пополнение группы G_i. Возьмем прямое произведение $P = \sqrt{G_1} \times \sqrt{G_2}$, в нем подгруппу $D = \{xx^\varphi | x \in G_1\}$ и рассмотрим ее корень $\sqrt{D}$ в этом произведении. Проверим, что

$$P = \sqrt{D} \cdot \sqrt{G_i}, \sqrt{D} \cap \sqrt{G_i} = 1 \text{ при } i = 1, 2. \tag{2.18}$$

Действительно, если $x \in \sqrt{D} \cap \sqrt{G_i}$, то $x^m \in D \cap G_i$ при подходящем m. Отсюда $x = 1$ и вторая из формул (2.18) доказана. Из нее следует, что сужение проектирования $\pi : P \longrightarrow \sqrt{G_1}$ на группу $\sqrt{D}$ есть изоморфизм, следовательно, $\sqrt{D^\pi} = \sqrt{D}^\pi$. Далее, сужение π на

$\sqrt{G_1}$ — тоже изоморфизм, поэтому $\sqrt{G_1}^\pi = \sqrt{G_1^\pi}$. Но $D^\pi = G_1^\pi$, поэтому $\sqrt{D}^\pi = \sqrt{G_1}^\pi$. Возвращаясь к полным прообразам относительно π, получаем первую из формул (2.18) для $i = 2$. По симметрии она верна и для $i = 1$.

Формулы (2.18) показывают, что любой элемент x_1 из $\sqrt{G_1}$ является проекцией точно одного элемента x из $\sqrt{D}$ на множитель $\sqrt{G_1}$. Сопоставляя элементу x_1 проекцию элемента x на множитель $\sqrt{G_2}$, мы получим изоморфизм $\sqrt{G_1}$ на $\sqrt{G_2}$, продолжающий φ.

б) Существование. Если группа G конечно порождена, то она вкладывается в полную нильпотентную группу $UT_n(\mathbb{Q})$ при некотором n (теорема 2.2.2.5). Корень $\sqrt{G}$ из подгруппы G в группе $UT_n(\mathbb{Q})$ будет нильпотентным пополнением группы G. Для g из G и натурального m обозначим $\sqrt[m]{g}$ решение уравнения $x^m = g$ в группе $\sqrt{G}$. Очевидно,

$$\sqrt[m]{g} = \sqrt[m']{g'} \Longleftrightarrow g^{m'} = g'^m, \tag{2.19}$$

причем ввиду а) таблица умножения в $\sqrt{G}$ полностью определяется таблицей умножения в G. Отбросим теперь предположение, что G конечно порождена, и рассмотрим множество формальных символов $\sqrt[m]{g}$, $g \in G$, $m = 1, 2, \ldots$. Определим на этом множестве формулой (2.19) отношение равенства и обозначим через $\sqrt{G}$ получившееся множество классов равных элементов. Условимся умножать $\sqrt[m]{g}$, $\sqrt[m']{g'}$ как элементы нильпотентного пополнения группы $\langle g, g'\rangle$. Тогда $\sqrt{G}$ становится группой, содержащей подгруппу G. Если группа G нильпотентна ступени s, то пополнения ее конечно порожденных подгрупп имеют ступени $\leqslant s$ (теорема 2.1.4.7), поэтому $\sqrt{G}$ удовлетворяет тождеству $[x_1, \ldots x_{s+1}] = 1$. Значит, $\sqrt{G}$ — нильпотентное пополнение группы G с той же самой ступенью нильпотентности. ⊠

Нильпотентная группа, содержащая периодические элементы, уже не всегда вкладывается в полную нильпотентную группу, так как периодическая часть полной нильпотентной группы G обязана лежать в центре. Действительно, по индуктивным соображениям можно считать, что любой периодический элемент g из G лежит во втором гиперцентре. Если $g^m = 1$, $m \neq 0$, то $[g, x^m] = [g, x]^m = [g^m, x] = 1$ для произвольного $x \in G$. Ввиду полноты G элемент x^m пробегает всю группу, поэтому элемент g центральный.

2.3 Обобщения нильпотентности

§1 Локальная нильпотентность

Определение 2.3.1.1. [1, стр. 175] Говорят, что группа *локально нильпотентна*, если все ее конечно порожденные подгруппы нильпотентны. При этом сама группа может не быть нильпотентной. Более общо, если σ — свойство групп, которое переносится на подгруппы, то говорят, что группа G *локально* обладает свойством σ, если все конечно порожденные подгруппы из G обладают свойством σ.

Предложение 2.3.1.2. *[1, упражнение 18.1.1] Подгруппы факторгруппы локально нильпотентных групп сами локально нильпотентны. Всякая локально нильпотентная группа является локально полициклической.*

Доказательство. Первая часть следует из того, что гомоморфные образы и подгруппы нильпотентной группы нильпотентны. Вторая вытекает из того, что конечно порожденные нильпотентные группы являются полициклическими. ⊠

Лемма 2.3.1.3. *[1, лемма 3.2.2] Пусть G — произвольная группа, A, B — ее подгруппы, $H = \langle A, B\rangle$. Тогда $[A,B]$, $A[A,B]$, $B[A,B]$ нормальны в H, $A[A,B]\cdot B[A,B] = H$, $[A,B] = \langle\langle C^A\rangle^B\rangle$, где $C = \{[a_i,b_j] | i \in I, j \in J\}$, если $A = \langle a_i | i \in I\rangle$, $B = \langle b_j | j \in J\rangle$.*

Доказательство. Легко доказывается с помощью предложения 2.1.4.4. ⊠

Теорема 2.3.1.4. *[1, теорема 18.1.2] 1) Во всякой группе произведение двух нормальных локально полициклических подгрупп есть локально полициклическая подгруппа.*

2) (Б. И. Плоткин). *Во всякой группе произведение двух нормальных локально нильпотентных подгрупп есть локально нильпотентная подгруппа.*

Доказательство. 1) Пусть K, L — нормальные локально полициклические подгруппы произвольной группы G. Надо показать, что любая конечно порожденная подгруппа из KL полициклическая. Возьмем в KL такую подгруппу и запишем ее порождающие в виде произведений ab, $a \in K$, $b \in L$. Пусть A — подгруппа, порожденная левыми множителями, B — правыми. По условию группы A, B полициклические. Очевидно, достаточно убедиться, что их порождение $H = \langle A, B\rangle$ — полициклическая группа. Воспользуемся леммой 2.3.1.3, описывающей строение H. Поскольку группа $[A,B]$ содержится в $A[A,B]$, $H = A[A,B] \cdot B[A,B]$ и произведение двух нормальных полициклических подгрупп — вновь полициклическая подгруппа, то достаточно доказать, что $A[A,B]$ — полициклическая группа.

Так как K, L нормальны в G, то $[K,L] \leqslant K \cap L$. Так как A, $\langle C\rangle$ конечно порождены и лежат в локально полициклической группе K, то группа $\langle A, C\rangle$ полициклическая. Значит, лежащая в ней подгруппа $\langle C^A\rangle$ также полициклическая. С другой стороны, она лежит в L, поэтому $\langle\langle C^A\rangle^B\rangle$ — конечно порожденная подгруппа из L и, значит, тоже полициклическая. По лемме 2.3.1.3 в ней содержится $[A,B]$, поэтому $[A,B]$ — полициклическая группа. Так как A и $[A,B]$ обе лежат в K и конечно порождены, то их произведение — полициклическая группа.

2) Доказывается по той же схеме. ⊠

Теорема 2.3.1.5. (Маклейн). *[1, теорема 18.1.3] Любая максимальная подгруппа H локально нильпотентной группы G нормальна.*

Доказательство. Пусть, напротив, H не нормальна в G. Тогда существует $x \in [G,G]$, $s \notin H$. Ввиду максимальности H $\langle H, x\rangle = G$. Пусть $x = [y_1,z_1]\ldots[y_n,z_n]$, $y_i, z_i \in G$. Пусть y_i, z_i выражаются как слова от x и $h1,\ldots,h_m$ из H, и $H^* = \langle h_1,\ldots,h_m\rangle$, $G^* = \langle h_1,\ldots,h_m,x\rangle$. По условию группа G^* нильпотентна. Очевидно, $x \in [G^*,G^*]$, $x \notin H^*$, поэтому H^* — собственная подгруппа в G^*. По теорема 2.1.2.2 можно включить H^* в субнормальную матрешку группы G^*, которая по теореме 2.2.2.2 уплотняется до полициклической матрешки

$$1 < \ldots < H^* < H_1 < \ldots < H_s < G^*. \tag{2.20}$$

Так как секция G^*/H_s коммутативна, то $[G^*,G^*] \leqslant H$, и, значит, $x \in H_s$. Но тогда $G^* \leqslant H_s$, что противоречит строгим включениям (2.20). ⊠

Предложение 2.3.1.6. *[1, упражнение] Во всякой локально нильпотентной группе G периодические элементы составляют подгруппу (называемую* периодической частью *группы G).*

Доказательство. Очевидно, поскольку произведение двух элементов конечного порядка лежит в нильпотентной подгруппе, а потому — также элемент конечного порядка. ⊠

Предложение 2.3.1.7. *[1, упражнение 18.1.5] Всякая периодическая локально нильпотентная группа разлагается в прямое произведение силовских подгрупп.*

Доказательство. Вновь любые два p-элемента порождают нильпотентную и, следовательно, конечную подгруппу. Поэтому произведение любых двух p-элементов — вновь p-элемент. Таким образом, группа G содержит единственную (и, значит, нормальную) силовскую p-подгруппу для любого p. ⊠

§2 Нормализаторное условие

Определение 2.3.2.1. [1, стр. 177] Следующее условие называется *нормализаторным*: каждая собственная подгруппа отлична от своего нормализатора.

Теорема 2.3.2.2. (Б. И. Плоткин). *[1, теорема 18.2.1] Всякая группа G с нормализаторным условием локально нильпотентна.*

Доказательство. По лемме Цорна всякий элемент из G лежит в некоторой максимальной локально нильпотентной подгруппе H. Достаточно показать, что H нормальна в G (тогда G будет покрываться локально нильпотентными нормальными подгруппами, а потому по теореме 2.3.1.4 сама будет локально нильпотентной). Обозначим $N = N_G(H)$. Если $N^g = N$, то H^g, H нормальны в N. По теореме 2.3.1.4 их произведение H^gH локально нильпотентно. Ввиду максимальности H имеем $H^gH = H$, откуда $H^g = H$, $g \in N$. Таким образом, N совпадает со своим нормализатором. Ввиду нормализаторного условия $N = G$. ⊠

Пример. (М. И. Каргаполов). Определим для каждого трансфинитного числа α группу G_α, полагая

$$G_0 = \mathbb{C}_p, G_\alpha = \begin{cases} \mathbb{C}_p \wr G_{\alpha-1} \text{ при непредельном } \alpha, \\ \bigcup_{\beta<\alpha} G_\beta \text{ при предельном } \alpha. \end{cases}$$

(Здесь $\mathbb{C}_p$ — группа корней из единицы p-ой степени в $\mathbb{C}$.)

Из построения видно, что каждое G_α является p-группой, причем все ее конечно порожденные подгруппы конечны и $|G_\alpha| \geqslant \alpha$. (Конечность здесь получается из-за того, что сплетение прямое.) В частности, все группы G_α локально нильпотентны.

Пусть γ — первое несчетное трансфинитное число. Ясно, что все G_α при $\alpha < \gamma$ счетны, а группа G_γ несчетна. Покажем, что G_γ не удовлетворяет нормализаторному условию. Действительно, в противном случае в G_γ существовала бы последовательность подгрупп H_λ, занумерованных трансфинитными числами $\lambda \leqslant \nu$, с условиями:

а) $H_0 = 1$, $H_\mu \lhd H_{\mu+1}$, $H_\lambda = \cap_{\mu<\lambda} H_\mu$ при предельном λ, $H_\nu = G_\gamma$,

б) все секции H_{m+1}/H_μ коммутативны.

(Такую последовательность можно было бы построить, например, беря первую и третью формулы из а) за определение H_λ, а в качестве $H_{\mu+1}$ беря порождение H_μ и любого элемента из $N_{G_\gamma}(H_\mu)$, лежащего вне H_μ.) Мы покажем сейчас, что группа G_γ в действительности не содержит подгрупп с условиями а) и б).

Пусть, напротив, такие H_λ существуют. Уплотнив, если нужно, последовательность этих подгрупп, можно считать, что все секции $H_{\mu+1}/H_\mu$ циклические. Тогда все H_n с натуральными номерами n счетны, а потому и их объединение H_ω счетно. Занумеруем элементы из H_ω: $h_1, h_2, \ldots$. Очевидно, $h_m \in G_{\beta_m}$ при некотором $\beta_m < \gamma$. Объединение всех G_{β_m} есть некоторое G_β, причем $\beta < \gamma$, поскольку G_β счетно, а группа G_γ несчетна. Мы получим противоречие, если установим, что G_β содержит все H_λ при $\omega < \lambda \leqslant \nu$. Сделаем это индукцией по λ. Для предельных λ утверждение очевидно, поэтому пусть λ — непредельное число. Пусть уже доказано, что $H_{\lambda-1} \leqslant G_\beta$, но существует $h \in H_\lambda$, $h \notin G_\beta$. Пусть α таково, что $h \in G_\alpha$, но $h \notin G_{\alpha-1}$. Очевидно, что $\beta \leqslant \alpha - 1$, поэтому $H_{\lambda-1} \leqslant G_{\alpha-1}$. По определению сплетения, $h = bf$, $b \in G_{\alpha-1}$, $f \in \operatorname{fun}(G_{\alpha-1}, \mathbb{C}_p)$, причем $f \neq 1$. Для всех $x \in H_{\lambda-1}$ имеем $[x^b, f] = (x^b)^{-1} x^{bf} \in G_{\alpha-1} \cap \operatorname{fun}(G_{\alpha-1}, \mathbb{C}_p) = 1$, т. е. $H^b_{\lambda-1}$ централизует f. (Действительно, поскольку H_λ нормализует $H_{\lambda-1}$ имеем $x^{bf} \in H_{\lambda-1} \leqslant G_{\alpha-1}$ и $x^b \in H_{\lambda-1}$. С другой стороны, группа $\operatorname{fun}(G_{\alpha-1}, \mathbb{C}_p)$ нормальна в G_α, поэтому $f^{x^b} \in \operatorname{fun}(G_{\alpha-1}, \mathbb{C}_p)$, откуда вытекает требуемое включение.) Таким образом, элемент $f' = bfb^{-1} \neq 1$ имеет в $G_{\alpha-1}$ имеет в $G_{\alpha-1}$ бесконечный централизатор. С другой стороны, этот централизатор, действуя на $G_{\alpha-1}$ правыми сдвигами, должен переводить $\operatorname{supp}(f')$ (носитель) в себя. С другой стороны, этот централизатор должен переводить $\operatorname{supp}(f')$ в себя. Значит, он изоморфен группе подстановок конечного множества $\operatorname{supp}(f')$ и потому не может быть бесконечным.

§3 Энгелевость

Определение 2.3.3.1. [1, стр. 179] Коммутаторное тождество

$$[x_0, x_1, \ldots, x_n] = 1, \tag{2.21}$$

определяющее, как мы знаем, нильпотентные группы ступени $\leqslant n$ служит источником этого обобщения нильпотентности. Стремление иметь возможно меньшее количество переменных приводит нас к тождеству

$$[x, \underbrace{y, \ldots, y}_{n}] = 1 \tag{2.22}$$

(отсутствие внутренних скобок означает «правильную» их расстановку: $[\ldots[[x, y], y], \ldots, y])$. Группа с тождеством (2.22) называется *ограниченно энгелевой группой* ступени $\leqslant n$ — в честь Энгеля, заложившего вместе с Ли основы теории групп и алгебр Ли.

Предложение 2.3.3.2. *[1, упражнение 6.2.3] Пусть группа A нетривиальна. Тогда $Z(A\bar{\wr}B) = \operatorname{Diag}(B, Z(A))$, $Z(A \wr B) = 1$, если B бесконечна.*

Доказательство. Пусть $z \in Z(A\bar{\wr}B)$. Тогда $z = bf$, где $b \in B$ и $f \in \operatorname{Fun}(B, A)$. Предположим сначала, что $b \neq e$. Тогда для любого $g \in \operatorname{Fun}(B, A)$ имеем $g^{z^{-1}} = f^{b^{-1}} g^{b^{-1}} (f^b)^{-1}$. Поскольку $z \in Z(A\bar{\wr}B)$ получаем $g^{z^{-1}} = g$. Это означает, что для любого $b_1 \in B$ справедливо $f^{b^{-1}} g^{b^{-1}} (f^b)^{-1}(b_1) = g(b_1)$. Возьмем $b_1 = e$, получим, $f(b^{-1}) g(b^{-1}) f^{-1}(b) = g(e)$ для всех $g \in \operatorname{Fun}(B, A)$. Но если $g(e) = e$, а $g(b) \neq (f(b^{-1})^{-1} f(b)$, то равенство невозможно. Таким образом, $z = f$. Далее, для любого $bg \in (B\bar{\wr}A)$ имеем $(bg)^f = b(f^{-1})^b gf = bg$, откуда $(f^{-1})^b gf = g$. Следовательно, для любого $b_1 \in B$ справедливо $f^{-1}(bb_1) g(b_1) f(b_1) = g(b_1)$. Если $f(bb_1) \neq f(b_1)$ для некоторого b, то тогда взяв в качестве g функцию, которая все элементы из B посылает в e получим противоречие. Таким образом, $f \in \operatorname{Diag}(B, A)$. Кроме того, если $f(b_1) \notin Z(A)$, то выбрав такой элемент a из A, что $a^{f(b_1)} \neq a$ и положив $g(x) = a$ для всех $x \in A$ получим противоречие с выбором f. Таким образом, $f \in \operatorname{Diag}(B, Z(A))$.

Для доказательства второго равенства достаточно заметить, что когда B бесконечна в $\mathrm{Diag}(B, Z(A))$ нет функций с конечным носителем. $\boxtimes$

П р и м е р. Если A, B — группы периода 2, то прямое сплетение $G = A \wr B$ удовлетворяет тождеству $[x, y, y, y] = 1$. В самом деле, пусть $x, y \in G$. Очевидно, $[x, y] = f \in \mathrm{fun}(B, A)$ и

$$[f, y, y] = (f^{-1}f^y)^{-1}(f^{-1}f^y)^y = f(f^{-1})^y(f^{-1})^y f^{y^2} = 1,$$

поскольку $y^2 \in \mathrm{fun}(B, A)$ и $f^2 = 1$. С другой стороны, при $A \neq 1$ и бесконечной B сплетение $G = A \wr B$ ненильпотентно (см. предложение 2.3.3.2).

2.4 Коммутаторное исчисление

§1 Собирательный процесс

Рассмотрим формальные *слова*, или *цепочки* $b_1 b_2 \dots b_n$, где каждый символ b_i представляет одну из букв $x_1, x_2, \dots, x_r$. Определим также *формальные коммутаторы* c_j и их веса́ $\omega(c_j)$ следующим образом:

1) $c_i = x_i$, $i = 1, \dots, r$ — коммутаторы веса 1, т. е. $\omega(x_i) = 1$

2) если c_i и c_j — коммутаторы то и $c_k = [c_i, c_j]$ — коммутатор и $\omega(c_k) = \omega(c_i) + \omega(c_j)$.

Будем говорить, что слово $c_{i_1}, \dots, c_{i_m}$, составленное из коммутаторов, собрано, если $i_1 \leqslant i_2 \leqslant \dots \leqslant i_m$, т. е. если коммутаторы расположены в порядке возрастания индексов слева на право. Произвольное слово из коммутаторов

$$c_{i_1} \dots c_{i_m} c_{i_{m+1}} \dots c_{i_n} \tag{2.23}$$

содержит, вообще говоря, *собранную часть* $c_{i_1}, \dots, c_{i_m}$, где $i_1 \leqslant \dots \leqslant i_m$ и $i_m \leqslant i_j$, $j = m+1, \dots, n$, и *несобранную часть* $c_{i_{m+1}}, \dots, c_{i_n}$, где i_{m+1} уже не наименьший из индексов i_j, $j = m+1, \dots, n$. Собранная часть слова $c_{i_1} \dots c_{i+n}$ пуста, если только i_1 — не наименьший из индексов.

Определим *собирательный процесс* для слов из коммутаторов. Пусть c_u — коммутатор с наименьшим индексом в несобранной части слова, и пусть $c_{i_j} = c_u$ — первое вхождение c_u в несобранную часть. Заменим тогда слово $c_{i_1} \dots c_{i_m} \dots c_{i_{j-1}} c_{i_j} \dots c_{i_n}$ словом $c_{i_1} \dots c_{i_m} \dots c_{i_j} c_{i_{j-1}} [c_{i_{j-1}}, c_{i_j}] \dots c_{i_n}$. При этом коммутатор c_{i_j} сдвинется на одно место влево и появится новый коммутатор $[c_{i_{j-1}}, c_{i_j}]$, который по весу больше, чем c_{i_j}.

Таким образом, и после указанного преобразования c_{i_j} останется коммутатором с наименьшим индексом в несобранной части. После конечного числа таких шагов коммутатор c_{i_j} займет $(m+1)$-место и станет элементом собранной части. Так определенный собирательный процесс, вообще говоря, не будет обрываться, так как на каждом шаге вводится новый коммутатор.

Пусть $x_1, \dots, x_r$ — образующие элементы группы F (мы будем в основном рассматривать случай, когда группа F — свободная группа с образующими $x_1, x_2, \dots, x_r$), и пусть $[u, v] = u^{-1}v^{-1}uv$, тогда

$$c_{i_{j-1}} c_{i_j} = c_{i_j} c_{i_{j-1}} [c_{i_{j-1}}, c_{i_j}], \tag{2.24}$$

и мы видим, что собирательный процесс не изменяет элемент группы, представленный словом. При нашем определении собирательный процесс применим не ко всем словам, а только к так называемым *положительным словам*, т. е. к словам, составленным из букв x_j и не содержащим букв вида x_j^{-1}. Ниже мы освободимся от этого ограничения.

В ходе собирательного процесса, примененного к положительным словам, возникают не любые коммутаторы. Так, например, коммутатор $[x_2, x_1]$ может возникнуть, а коммутатор $[x_1, x_2]$ возникнуть не может, так как буква x_1 собирается до x_2. Коммутаторы, которые действительно могут возникнуть в собирательном процессе, называются *базисными*. Дадим формальное определение базисных коммутаторов группы F с образующими $x_1, x_2, \ldots, x_r$.

Определение 2.4.1.1. [7, стр. 187] 1) $c_i = x_i$, $i = 1, \ldots, r$ — базисные коммутаторы веса один, $\omega(x_i) = 1$.

2) Пусть базисные коммутаторы весов, меньших n, уже определены. Тогда базисными коммутаторами веса n являются коммутаторы $c_k = [c_i, c_j]$, где

а) c_i и c_j — базисные коммутаторы и $\omega(c_i) + \omega(c_j) = n$;

б) $c_i > c_j$, а если $c_j = [c_s, c_t]$, то $c_j \geqslant c_t$.

3) Коммутаторы веса n следуют за коммутаторами весов, меньших n, и между собой они упорядочены произвольным образом. Базисные коммутаторы считаем пронумерованными так, что они упорядочены по индексам.

Заметим, что если коммутаторы упорядочены по весам, а в остальном — произвольным образом, то собирательный процесс, примененный к положительным словам, дает только базисные коммутаторы.

Мы покажем сейчас, что по модулю $\gamma_{k+1}F$, где $\gamma_{k+1}F$ — $(k+1)$-й член нижнего центрального ряда группы F, обозначаемый также F_{k+1} (k — любое число), произвольный элемент может быть представлен в виде

$$f = c_1^{e_1} c_2^{e_2} \ldots c_t^{e_t} \pmod{F_{k+1}}, \tag{2.25}$$

где $c_1, \ldots, c_t$ — базисные коммутаторы весов $1, 2, \ldots, k$.

В ходе собирательного процесса имеем

$$vu = uv[v, u], \tag{2.26}$$

где u, v и $[v, u]$ — базисные коммутаторы. Мы должны также рассмотреть выражения vu^{-1}, $v^{-1}u^{-1}$ и $v^{-1}u$. При этом $vu^{-1} = u^{-1}v[vu^{-1}]$, а из соотношения $[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z]$ имеем

$$1 - [v, uu^{-1}] = [v, u^{-1}][v, u][v, u, u^{-1}], \tag{2.27}$$

откуда $[vu^{-1}] = [v, u, u^{-1}]^{-1}[v, u]^{-1}$. Аналогично $[v, u, u^{-1}] = [v, u, u, u^{-1}]^{-1}[v, u, u]^{-1}$. Положив $v_0 = v$ и $v_{t+1} = [v_t, u]$, получим

$$[v, u^{-1}] = [v_1, u^{-1}]v_1^{-1} = v_2[v_2, u^{-1}]v_1^{-1} \equiv v_2 v_4 \ldots v_5^{-1} v_3^{-1} v_1^{-1} \pmod{F_{k+1}}. \tag{2.28}$$

Если здесь коммутатор $v_1 = [v, u]$ базисный, то и $v_2, v_3, \ldots$ — также базисные коммутаторы. По модулю F_{k+1} мы можем пренебречь коммутатором $[v_s, u^{-1}]$, если индекс s настолько велик, что вес этого коммутатора не меньше $k+1$. Следовательно, в качестве элементарного этапа собирательного процесса мы допускаем следующую замену:

$$vu^{-1} \equiv u^{-1} v v_2 v_4 \ldots v_5^{-1} v_3^{-1} v_1^{-1} \pmod{F_{k+1}}. \tag{2.29}$$

Аналогично, $v^{-1}u = uv^{-1}[v^{-1}, u]$, и из равенства $[xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z]$ получаем $1 = [vv^{-1}, u] = [v, u][v, u, v^{-1}][v^{-1}, u]$, откуда, полагая $w_1 = [v, u]$, $w_{t+1} = [w_t, v]$, имеем

$$v^{-1}u \equiv uv^{-1} w_2 w_4 \ldots w_3^{-1} w_1^{-1} \pmod{F_{k+1}}. \tag{2.30}$$

Имеет место тождество $v^{-1}u^{-1} = u^{-1}(uvu^{-1})^{-1}$, а из (2.29) получаем

$$uvu^{-1} \equiv v \cdot v_2 v_4 \ldots v_5^{-1} v_3^{-1} v_1^{-1} \pmod{F_{k+1}}, \tag{2.31}$$

откуда

$$v^{-1}u^{-1} \equiv u^{-1} v_1 v_3 v_5 \ldots v_4^{-1} v_2^{-1} v^{-1} \pmod{F_{k+1}}. \tag{2.32}$$

Повторное применение замен (2.26), (2.29), (2.30) и (2.32) приводит к записи (2.25) произвольного элемента f группы F в виде слова из базисных коммутаторов.

§2 Формула Витта. Теорема о базисе

Предположим, нам дана последовательность базисных коммутаторов $c_1, c_2, \ldots$, состоящих из образующих $x_1, x_2, \ldots, x_r$. Назовем произведение базисных коммутаторов

$$c_{i_1} c_{i_2} \ldots c_{i_s} \tag{2.33}$$

базисным, если слово (2.33) собрано, т. е. если $i_1 \leqslant i_2 \leqslant \ldots \leqslant i_s$. Для произведения коммутаторов $p = a_1 a_2 \ldots a_n$ произвольного вида мы определим понятие веса $\omega(p) : \omega(p) = \omega(a_1) + \ldots + \omega(a_n)$. Собирательный процесс изменяет вес произведения. Мы определим сейчас аналогичный процесс — *процесс заключения в скобки*, не меняющий веса произведения. Если u, v и $[u, v]$ — базисные коммутаторы, то слово $\ldots uv \ldots$ заменяется на $\ldots [u, v] \ldots$ в отличие от собирательного процесса, где слово $\ldots uv \ldots$ заменяется произведением $\ldots v, u[u, v] \ldots$.

Теорема 2.4.2.1. *[7, теорема 11.2.1] Число базисных произведений веса n, составленных из образующих $x_1, \ldots, x_r$, равно r^n.*

Доказательство. Для всех $k = 1, 2, \ldots$ определим семейство $P_k = P_k^{(n)}$ всех произведений $a_1 a_2 \ldots a_t$ веса n (где a_i — базисные коммутаторы) вида

$$c_1^{e_1} c_2^{e_2} \ldots c_k^{e_k} c_{i_1} \ldots c_{i_s}, \tag{2.34}$$

где $e_i \geqslant 0$, $i_1 > k$, $i_2, \ldots, i_s \geqslant k$, и для каждого коммутатора $c_{i_j} = [c_u, c_v]$ коммутатор c_v предшествует c_k. Таким образом, P_k можно рассматривать как семейство слов, в которых коммутаторы $c_1, \ldots, c_{k-1}$ собраны, а c_k еще не собраны. Ясно, что P_1 — семейство всех произведений n образующих x_i, откуда $|P_1| = r^n$. Действительно, если бы у нас был хоть один множитель вида $[c_i, c_j]$, то это бы означало, что коммутатор c_j уже собран, что противоречит нашему выбору.

Далее можно установить взаимно однозначное соответствие между элементами семейств P_k и P_{k+1}. Действительно, если $c_1^{e_1} \ldots c_k^{e_k} c_{i_1} \ldots c_{i_s}$ — произведение из семейства P_k, то коммутатор c_{i_1} следует за c_k и, хотя в произведении могут встречаться цепочки коммутаторов c_k в несобранной части, каждой такой цепочке непосредственно предшествует коммутатор c_y, где $y > k$. Ко всем подобным цепочкам $c_y c_k \ldots c_k c_w$, $y > k$, $w > k$ применим операции заключения в скобки, заменив их выражениями $[\ldots [[c_y, c_k], c_k], \ldots, c_k], c_w$, и так как при условии $c_y = [c_u, c_v]$, $k > v$, то вновь возникающий коммутатор будет опять базисным и будет следовать за c_k. Указанное преобразование дает однозначно определенное произведение из семейства P_{k+1}. Обратно, если в произведении семейства P_{k+1} убрать все скобки, заключающие коммутатор c_k, то мы получим однозначно определенное произведение из семейства P_k. Следовательно, $|P_{k+1}| = |P_k| = |P_1| = r^k$. Но при достаточно большом k семейство P_k состоит из всех базисных произведений веса n. ⊠

С помощью теоремы 2.4.2.1 можно найти число базисных коммутаторов веса n, и, даже более того, можно найти число базисных коммутаторов с заданными весами относительно каждого образующего.

Определение 2.4.2.2. [7, стр. 191] Слово $a_1 \dots a_n$ будем называть *циклическим*, если считать, что a_1 следует за a_n, а $a_1 a_2 \dots a_n$, $a_2 \dots a_n a_1$, ..., $a_n a_1 \dots a_{n-1}$ — записи одного и того же слова. Циклическое слово C длины n может быть получено в результате повторения подслова из d букв n/d раз, где d — некоторый делитель числа n. Каждому циклическому слову соответствует единственный наименьший период, который в свою очередь однозначно определяет некоторое циклическое слово длины d.

Лемма 2.4.2.3. *[7, лемма 11.2.1] Между базисными коммутаторами веса n и циклическими словами длины и периода n имеет место взаимно однозначное соответствие. Оно осуществляется подходящей расстановкой скобок в циклическом слове.*

Доказательство. Пусть $a_1 a_2 \dots a_n$ — циклическое слово длины n. Циклические слова веса n образуют семейство $C_k^n = C_k$, если они вида $c_{i_1} c_{i_2} \dots c_{i_s}$, где c_{i_j} — базисные коммутаторы, и для любого $c_{i_j} = c_w$, если $c_w = [c_u, c_v]$, то $v < k$, причем или (1) $i_1 = i_2 = \ldots = i_s$ (включая случай $s = 1$), или (2) $i_1, \dots, i_s \geqslant k$ и некоторый индекс $i_j > k$. Если имеет место случай (1), то слово принадлежит, по определению, также семейству C_{k+1}. Если же налицо случай (2), то мы берем каждую циклическую подпоследовательность (если таковые существуют) вида $c_w, c_k, \dots, c_k, c_t$, $w > k$, $t > k$, и расставляем скобки следующим образом: $[\dots[c_w, c_k], \dots, c_k]$. Получается циклическое слово из семейства C_{k+1}. Обратно, удалив из какого-либо слова семейства C_{k+1} все скобки, заключающие c_k, получаем слово из семейства C_k. Таким образом, установлено существование однозначного соответствия между словами семейства C_k и семейства C_{k+1} для произвольного k. Если же k достаточно велико, то коммутатор c_k имеет вес, бóльший n, и случай (2) невозможен. Следовательно, в итоге процесс расстановки скобок прекращается и получается циклическое слово, для которого имеет место случай (1). Это слово будет или базисным коммутатором веса n, или последовательностью $s = n/d$ тождественных базисных коммутаторов веса d. Расстановка скобок, при помощи которой осуществляется переход от семейства C_k к семейству C_{k+1}, охватывает один коммутатор c_w и некоторое число коммутаторов c_k. Следовательно, каждая такая расстановка скобок осуществляется только внутри одного периода и в точности повторяется во всех остальных процессах. При всем этом число периодов в слове остается неизменным. Следовательно, расстановка скобок во всех циклических словах длины n дает все базисные коммутаторы веса n, а в случае $d|n$ дает все базисные коммутаторы веса d, повторенные n/d раз каждый, так как все они являются членами семейства C_k при достаточно большом k. ⊠

Определение 2.4.2.4. [7, стр. 190] Определим вес $\omega_i(x_i) = 1$, $\omega_i(x_j) = 0$, $i \neq j$, а далее по правилу $\omega_i([c_u, c_v]) = \omega_i(c_u) + \omega_j(c_v)$. Пусть $M_r(n)$ — число базисных коммутаторов веса n от r образующих $x_1, x_2, \dots, x_r$, и пусть $M(n_1.n_2, \dots, n_r)$ — число таких коммутаторов c, что $\omega_i(c) = n_i$, $i = 1, 2, \dots, r$, причем $n = n_1 + n_2 + \ldots + n_r$.

Теорема 2.4.2.5. (Теорема Витта). *[7, теорема 11.2.2]*

$$M_r(n) = \frac{1}{n} \sum_{d|n} \mu(d) r^{n/d}, \tag{2.35}$$

$$M(n_1, n_2, \ldots, n_r) = \frac{1}{n} \sum_{d|n_i} \mu(d) \left(\frac{n}{d}\right)!| \left(\frac{n_1}{d_1}\right)! \ldots \left(\frac{n_r}{d}\right)! \tag{2.36}$$

Здесь $\mu(m)$ — функция Мебиуса, определенная на множестве натуральных чисел следующим образом: $\mu(1) = 1$; для $n = p_1^{e_1} \ldots p_s^{e_s}$, где $p_1, \ldots, p_s$ — различные простые числа, $\mu(n) = 0$, если хоть один показатель степени $e_i > 1$, а $\mu(p_1 p_2 \ldots p_s) = (-1)^s$.

Доказательство. Согласно теореме 2.4.2.1, число базисных произведений равно r^n. Это приводит к следующему формальному тождеству для степенных рядов от переменной z: $\frac{1}{1-rz} = \prod_{n=1}^{\infty}(1-z^n)^{-M_r(n)}$. Процесс расстановки скобок оставляет веса $\omega_i (i = 1, \ldots, r)$ неизменными. Число слов W то образующих $x_1, \ldots, x_r$ с весом $\omega_i(W) = n_i$ (для всех i) равно, очевидно, $\frac{n!}{n_1! \ldots n_r!}$. Отсюда вытекает формальное тождество для рядов от переменных $z_1, \ldots, z_r$:

$$\frac{1}{1 - z_1 - \ldots - z_r} = \prod_{n_1, \ldots, n_r = 1}^{\infty} (1 - z_1^{n_1} \ldots z_r^{n_r})^{-M(n_1, \ldots, n_r)}. \tag{2.37}$$

В силу леммы 2.4.2.3 нам достаточно изучать слова длины и периода n. Сколько существует слов длины n и периода n? Циклическое слово длины n и периода d, где $d|n$, дает точно d обыкновенных (не обязательно циклических) слов длины n:

$$\begin{gathered} a_1 \ldots a_d a_1 \ldots a_d \ldots a_1 \ldots a_d \\ a_2 \ldots a_d a1 \ldots a_1 \ldots a_d a_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_d a_1 \ldots a_d \ldots a_1 \ldots a_{d-1}. \end{gathered}$$

Таким образом, $r^n = \sum_{d|n} dM_r(d)$, так как число циклических слов длины и периода d равно $M_r(d)$ и каждому из r^n обыкновенных слов соответствует вполне определенный период d. Из тождества

$$r^n = \sum_{d|n} dM_r(d) \tag{2.38}$$

можно найти $M_r(d)$, пользуясь формулой обращения Мебиуса: если

$$f(n) = \sum_{d|n} g(d), \tag{2.39}$$

то

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d). \tag{2.40}$$

Отсюда $nM_r(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) r^d$ или

$$M_r(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) r^d, \tag{2.41}$$

т. е. получим формулу Витта.

Число обыкновенных слов W, таких, что $\omega_i(W) = n_i$, где $n_1 + \ldots + n_r = n$, равно $\frac{n!}{n_1! \ldots n_r!}$. Это приводит к формуле

$$\frac{n!}{n_1! \ldots n_r!} - \sum_{d|n_1, \ldots, n_r} dM\left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_r}{d}\right). \tag{2.42}$$

Здесь d пробегает все делители числа $n_0 = (n_1, \ldots, n_r)$. Вновь применяя формулу обращения Мебиуса (2.40) мы получаем вторую формулу Витта (2.36). ⊠

Рассмотрим свободное ассоциативное кольцо R с целочисленными коэффициентами и с r образующими $x_1, x_2, \ldots, x_r$. Элементы степени m образуют свободную абелеву группу R_m с базисом, состоящим из r^m произведений вида $x_{i_1} \ldots x_{i_m}$. В этом кольце R мы следующим образом определяем коммутатор $[u, v]$:

$$[u, v] = uv - vu. \tag{2.43}$$

Формальные свойства расстановки скобок для коммутаторов кольца те же, что и для коммутаторов групп. Мы покажем, что в действительности существует очень тесная связь между групповыми и кольцевыми коммутаторами, которая впервые была установлена Магнусом.

Теорема 2.4.2.6. *[7, теорема 11.2.3] Базисные произведения степени m образуют аддитивный базис группы R_m.*

Доказательство. Так как, согласно теореме 2.4.2.1, число базисных произведений степени m равно r^m, т. е. числу базисных элементов группы R_m, то достаточно показать, что любой элемент из R_m может быть представлен как линейная комбинация базисных произведений с целыми коэффициентами. Так как семейство $P_1^{(m)} = P_1$ образует базис, состоящий из r^m произведений $x_{i_1}, \ldots, x_{i_m}$, и так как для достаточно большого k семейство P_k состоит из базисных произведений, то достаточно выразить элементы из P_k в виде линейных комбинаций с целыми коэффициентами элементов из P_{k+1}. Для этого нам понадобится одно тождество. Для упрощения записи введем обозначения: $[[\ldots[[u, v], v], \ldots], v] = [u, \overbrace{v, \ldots, v}^{s}] = [^s u, v^s]$, если число букв v равно s. Необходимое нам тождество выглядит так:

$$uv^s = v^s u + \sum_{j=1}^{s} \binom{s}{j} v^{s-j} [^j u, v^j]. \tag{2.44}$$

При $s = 1$ оно сводится к $uv = vu + [u, v]$. Предположив выполнимость (2.44) для s, при помощи тождества

$$[^j u, v^j] v = [^{j+1} u, v, v^{j+1}] + v[^j u, v^j] \tag{2.45}$$

легко показать справедливость равенства (2.44) для $s + 1$.

Если элемент из P_k содержит подпоследовательность вида $\ldots uc_k \ldots c_k w \ldots$, $w \neq c_k$, где коммутатор u больше коммутатора c_k, который встречается здесь s раз, то мы применяем тождество (2.44), полагая $u = u$, $v = c_k$. При этом получаются произведения или принадлежащие семейству P_{k+1}, или семейству P_k с меньшим числом коммутаторов c_k, или содержащие коммутаторы c_k ближе к началу слова. В результате многократного применения тождества (2.44) произведение из P_k представится в виде линейной комбинации с целыми коэффициентами элементов из P_{k+1}. ⊠

Следствие 2.4.2.7. *[7, следствие 11.2.1] Базисные коммутаторы степени m линейно независимы.*

Определение 2.4.2.8. [7, стр. 195] Присоединим теперь к кольцу R единицу 1 и будем рассматривать целые рациональные числа как элементы степени нуль. Их совокупность обозначим через R_0. Образуем в R факторкольцо $\overline{R}$ по двустороннему идеалу, порожденному всеми членами, степени которых не меньше $n + 1$. Тогда

$$\overline{R} = R_0 + R_1 + \ldots + R_n. \tag{2.46}$$

В $\overline{R}$ элементы вида $1+z$, где $z \in R_1+\ldots)R_n$, образуют группу G, так как в силу равенства $z^{n+1}=0$ имеем

$$(1+z)^{-1} = 1 - z + z^2 - \ldots + (-1)^n z^n. \tag{2.47}$$

Если $1+z = 1+u_m+u_{m+1}+\ldots+u_n$, где $u_j \in R_j$ для $j=m,\ldots,n$ и $u_m \neq 0$, то мы говорим, что u_m — *старший член* элемента $1+z$.

Лемма 2.4.2.9. *[7, лемма 11.2.2] Пусть $u, v \neq 1$ — элементы группы G со старшими членами u_s и v_t степеней s и t соответственно. Старшими членами элементов u^{-1} и v^{-1} являются элементы $-u_s$ и $-v_t$. Если $s < t$, то старший член элемента uv есть u_x. Если кольцевой коммутатор $[u_s, v_t]$ не равен нулю, то он является старшим членом группового коммутатора $[u,v]$.*

Доказательство. Пусть $u=1+a$, $v=1+b$, $u^{-1}=1+a'$, $v^{-1}=1+b'$. Тогда $a+a'+aa'=0$, $aa'=a'a$, $b+b'+bb'=0$, $a=u_s+\ldots+u_n$, $b=v_t+\ldots+v_n$, $uv=1+a+b+ba$. Из этих соотношений сразу получаются утверждения леммы о старших членах элементов u^{-1}, v^{-1} и vu. Используя эти же соотношения, получаем $[u,v]=u^{-1}v^{-1}uv=(1+a')(1+b')(1+a)(1+b) = 1+ab-ba+aa'b-bb'a+b'ab+a'b'a+a'b'ab$, откуда

$$[u,v] = 1 + [u_s, v_t] + \text{слагаемые более высокой степени.} \tag{2.48}$$

⊠

Пусть $c_1, c_2, \ldots$ — последовательность базисных коммутаторов свободной группы F, порожденной элементами $y_1,\ldots,y_r$, и пусть $d_1, d_2, \ldots$ — кольцевые коммутаторы в кольце R, получающиеся заменой $y_1,\ldots,y_r$ на $x_1,\ldots,x_r$. Кроме того, пусть c_t — последний коммутатор веса n. Тогда существует соответствие между коммутаторами c_i и d_i в кольце $\overline{R}$, устанавлимое следующей леммой.

Лемма 2.4.2.10. *[7, лемма 11.2.3] При соответствии $y_i \longrightarrow 1+x_i$, $i=1,2,\ldots,r$, определяющем отображение группы F на группу G, пусть $c_i \longrightarrow g_i \in G$. Тогда старший член элемента g_i равен d_i $(i=1,\ldots,t)$.*

Доказательство. Так как $y_i \longrightarrow 1+x_i$, $i=1,\ldots,r$, то старший член элемента $g_i = 1+x_i$ есть x_i при $i=1,\ldots,r$. Доказательство проведем индукцией. Если $c_w=[c_u,c_v]$, $w \leqslant t$ то по предположению индукции, старший член элемента g_u равен d_u, а элемента g_v равен d_v. Следовательно, по лемме 2.4.2.9 старший член коммутатора $[g_u,g_v]$ равен $d_u, d_v]$, если последний коммутатор не равен нулю. Будучи базисным коммутатором, он на самом деле не равен нулю, как показывает следствие 2.4.2.7. Итак, старший член коммутатора $g_w=[g_u,g_v]$ равен $[d_u,d_v]=d_w$. ⊠

Теорема 2.4.2.11. (Теорема о базисе). *[7, теорема 11.2.4] Если F — свободная группа со свободными образующими $y_1,\ldots,y_r$ и если в некоторой последовательности базисных коммутаторов $c_1,c_2,\ldots,c_t$ — все базисные коммутаторы весов $1,2,\ldots,n$, то произвольный элемент f группы F однозначно представим в виде*

$$f \equiv c_1^{e_1} c_2^{e_2} \ldots c_t^{e_t} \pmod{F_{n+1}}. \tag{2.49}$$

Базисные коммутаторы веса n образуют базис свободной абелевой группы F_n/F_{n+1}.

Доказательство. Сначала докажем второе утверждение. Пусть $c_s, \dots, c_t$ — базисные коммутаторы веса n. Согласно лемме 2.4.2.10, при отображении, определенном соответствиями

$$y_i \longrightarrow 1 + x_i = g_i,\ i = 1, \dots, r, \tag{2.50}$$

группы F на кольцо R, старшие члены коммутаторов $c_s, \dots, c_t$ будут соответствующими кольцевыми коммутаторами $d_s, \dots, d_t$, являющимися кольцевыми базисными коммутаторами степени n. В силу следствия 2.4.2.7 коммутаторы $d_s, \dots, d_t$ линейно независимы, а по лемме 2.4.2.9 старший член произведения $c_s^{e_s} \dots c_t^{e_t}$ равен $e_s d_s + \dots + e_t d_t$. Он не равен нулю, если только не все числа $e_s, \dots, e_t$ равны нулю. Следовательно, коммутаторы $c_s, \dots, c_t$ являются независимыми элементами факторгруппы F_n/F_{n+1} и, следовательно, образуют базис, так как мы уже знаем из равенства (2.25), что любой элемент факторгруппы можно представить как произведение $c_s, \dots, c_t$. Существование по меньшей мере одного представления для элемента f в виде (2.49) установлено соотношением (2.25). Покажем единственность этого представления. Действительно, если бы имело место равенство

$$c_1^{e_1} \dots c_t^{e_t} \equiv c_1^{h_1} \dots c_t^{h_t} \pmod{F_{n+1}}, \tag{2.51}$$

где $h_i = e_i$, $i = 1, \dots, j-1$, но $h_j \neq e_j$ и если бы вес c_j был равен k, то это привело бы к зависимости между базисными коммутаторами веса k по модулю F_{k+1}. Но этого не может быть, следовательно, представление (2.49) однозначно. ⊠

§3 Теорема Бернсайда о базисе. Автоморфизмы p-групп

Теорема 2.4.3.1. (Теорема Бернсайда о базисе). *[7, теорема 12.2.1] Факторгруппа $P/\Phi(P) = A$ — элементарная абелева группа. Если порядок группы A равен p^r, то любое множество образующих элементов $z_1, \dots, z_s$ группы P содержит подмножество из r элементов $x_1, \dots, x_r$, также порождающих группу P. При отображении $P \longrightarrow A$ элементы $x_1, \dots, x_r$ отображаются в базис $a_1, \dots, a_r$ группы A. Обратно, любое множество r элементов группы P, отображаемое при $P \longrightarrow A$ на базис группы A, является системой образующих группы P.*

Доказательство. Из теоремы 2.2.1.1 следует, что группа $G/\Phi(P) = A$ — абелева группа, откуда уже нетрудно получить, что A является элементарной абелевой. Остальные утверждения очевидны. ⊠

С помощью этой теоремы мы можем получить некоторые сведения о группе автоморфизмов Aut (P) группы P. Базис $a_1, \dots, a_r$ группы $P/\Phi(P)$ можно выбрать $\theta(p^r) = (p^r-1)(p^r-p)\dots(p^r-p^{r-1})$ различными способами. Действительно, это — порядок группы $GL_r(p)$, а поскольку $P/\Phi(P)$ — это векторное пространство над полем $GF(p)$ размерности r, то группа ее автоморфизмов совпадает с $GL_r(p)$.

Существует точно $p^{r(n-r)}\theta(p^r)$ последовательностей $X = (x_1, \dots, x_r)$, порождающих группу P. Действительно, при отображении $x_i \longrightarrow a_i$, $i = 1, \dots, r$, последовательность X переходит в базис группы A, последний может быть выбран $\theta(p^r)$ различными способами, а для каждого элемента a_i любой из p^{n-r} элементов смежного класса по $\Phi(P)$, отображаемого в a_i, может быть выбран в качестве x_i. Любой автоморфизм группы P отображает последовательности X друг в друга. Следовательно, группу Aut (P) можно рассматривать как группу подстановок на множестве последовательностей X. Но Aut (P) действует регулярно на множестве последовательностей X, так как автоморфизм, отображающий некоторое множество X на себя определяет тождественное отображение на множестве элементов x_i, а, следовательно, и на всей группе P, т. е. является тождественным автоморфизмом. Таким образом, множество последовательностей X распадается на орбиты в каждой из которых k множеств, где k — порядок группы Aut (P). Итак, $p^{r(n-r)}\theta(p^r) = kt$.

Определение 2.4.3.2. [7, стр. 200] Будем говорить, что два семейства $X = (x_1, \ldots, x_r$ и $Y = (y_1, \ldots, y_r)$ порождают группу P *одинаковым образом*, если из любого отношения $w(x_1, \ldots, x_r) = 1$ следует отношение $w(y_1, \ldots, y_r) = 1$ и обратно.

Пусть $A_1(P)$ — инвариантная подгруппа группы Aut (P), индуцирующая тождественный автоморфизм в факторгруппе $P/\Phi(P)$. Эти автоморфизмы переставляют регулярно $p^{r(n-r)}$ порождающих семейств $X = (x_1, \ldots, x_r)$, которые отображаются в один и тот же базис $a_1, \ldots, a_r$ группы A при гомоморфизме $P \longrightarrow P/\Phi(P) = A$. Таким образом, порядок подгруппы $A_1(P)$ делит $p^{r(n-r)}$. Сформулируем эти результаты Ф. Холла в виде теоремы.

Теорема 2.4.3.3. *[7, теорема 12.2.2] Пусть P — группа порядка p^n, и пусть $|P : \Phi(P)| = p^r$. Тогда порядок группы* Aut (P) *автоморфизмов группы P делит $p^{r(n-r)}\theta(p^r)$. Порядок группы $A_1(P)$ автоморфизмов, индуцирующих тождественный автоморфизм в группе $P/\Phi(P)$, делит $p^{r(n-r)}$.*

§4 Собирательная формула

Пусть G — группа, порожденная элементами $a_1, a_2, \ldots, a_r$. Мы выведем формулу для выражения $(a_1 a_2 \ldots a_r)^n$ через базисные коммутаторы элементов $a_1, a_2, \ldots, a_r$. Можно считать, что G — свободная группа, порожденная элементами $a_1, \ldots, a_r$, тогда искомая формула тем более будет справедлива в любой группе, порожденной r элементами. Уточним определение 2.4.1.1.

1) $a_1, \ldots, a_r$ — коммутаторы веса один, просто упорядоченные следующим образом: $a_1 < a_2 < \ldots < a_r$;

2) если базисные коммутаторы весов меньших n, уже определены и просто упорядочены, то $[x, y]$ — базисный коммутатор веса n тогда и только тогда, когда

а) x и y — базисные коммутаторы, причем $\omega(x) + \omega(y) = n$,

б) $x > y$,

в) если $x = [u, v]$, то $y \geqslant v$;

3) коммутаторы веса n следуют за всеми коммутаторами весов, меньших n; для коммутаторов одинакового веса $[x_1, y_1] < [x_2, y_2]$, если $y_1 < y_2$ или если $y_1 = y_2$, но $x_1 < x_2$.

Рассмотрим тождество

$$(a_1 a_2 \ldots a_r)^n = a_1(1) a_2(1) \ldots a_r(1) a_1(2) a_2(2) \ldots a_r(2) \ldots a_r(n), \tag{2.52}$$

где мы пронумеровали образующие a_i слева направо числами в скобках от 1 до n, чтобы различать все различные вхождения буквы a_i. Так как по определению коммутатора $SR = RS[S, R]$, мы можем правую часть равенства (2.52) заменить другим равным ему выражением, в котором вместо некоторой пары SR последовательных элементов стоит произведение $RS[S, R]$. Эта замена сдвигает элемент R ближе к началу слова, причем появляется коммутатор $[S, R]$. Последовательным выполнением таких замен мы можем сдвинуть любую букву как угодно близко к началу слова. Мы будем преобразовывать (2.52) в следующем порядке. Сдвигаем $a_1(2)$ влево до тех пор, пока эта буква не займет место сразу после $a_1(1)$, затем сдвигаем $a_1(3)$ влево до тех пор, пока эта буква не окажется непосредственно за $a_1(2)$, и т. д. до тех пор, пока в начале слова не будут собраны все буквы $a_1(i)$, $i = 1, \ldots, n$. Этим заканчивается первый этап собирательного процесса. После этого мы таким же образом собираем буквы $a_2(i)$, $i = 1, \ldots, n$, справа за буквами $a_1(i))$, $i = 1, \ldots, n$.

Опишем собирательный процесс более точно. После i-ого этапа имеем выражение

$$(a_1 a_2 \ldots a_r)^n = c_1^{e_1} c_2^{e_2} \ldots c_i^{e_i} R_1 R_2 \ldots R_t, \tag{2.53}$$

где $c_1, c_2, \ldots, c_i$ — первые i базисных коммутаторов, а $R_1, \ldots, R_t$ — базисные коммутаторы, следующие за c_i. Если $R_{j_1}, R_{j_2}, \ldots, R_{j_s}$ — те из коммутаторов $R_1, \ldots, R_t$ (выписанные по порядку их следования), которые равны c_{i+1}, то мы сначала сдвигаем R_{j_1} на место, непосредственно следующие за элементом $c_i^{e_i}$, затем $R_{j_2}, R_{j_3}, \ldots$, и, наконец, R_{j_s}, так что $e_{i+1} = s$ и тождество (2.53) принимает вид

$$(a_1 a_2 \ldots a_r)^n = c_1^{e_1} c_2^{e_2} \ldots c_{i+1}^{e_{i+1}} R_1^* \ldots R_k^*. \tag{2.54}$$

Это был $(i+1)$-й этап собирательного процесса. В слове (2.53) назовем $c_1^{e_1} \ldots c_i^{e_i}$ собранной частью, а $R_1, \ldots, R_t$ — несобранной. Но для оправдания приведенного выше описания мы дожны показать, что при таком процессе в каждой формуле могут возникнуть только базисные коммутаторы. Исходная формула (2.52) представляет собой нулевой этап и содержит только образующие a_i, являющиеся базисными коммутаторами веса один. Предположим по индукции, что на i-ом этапе преобразований несобранная часть $R_1, \ldots, R_t$ содержит только базисные коммутаторы, следующие за c_i. В процессе собирания коммутаторов $R_{j_1}, \ldots, R_{j_s}$, равных c_{i+1}, мы вводим только коммутаторы вида $[c_j, c_{i+1}, \ldots, c_{i+1}]$, где $j \geqslant i+2$. Такие коммутаторы являются базисными, так как если $c_j = [c_r, c_s]$, то коммутатор c_j возник на s-ом этапе, когда собирались коммутаторы c_s, откуда $s < i+1$, и поэтому $c_s < c_{i+1}$. Таким образом, коммутатор $[c_j, c_{i+1}]$ базисный, и, следовательно, $[c_j, c_{i+1}, \ldots, c_{i+1}]$ — также базисный коммутатор.

Мы уже пометили в формуле (2.52) вхождения образующих a_i метками j: $a_i(j)$, $j = 1, \ldots, n$. Пусть коммутатор R веса w_1 имеет уже метку $(\lambda_1, \ldots, \lambda_{w_1})$, а коммутатор S веса w_2 — метку $(\mu_1, \ldots, \mu_{w_2})$; сопоставим тогда коммутатору $[R, S]$ метку $(\lambda_1, \ldots, \lambda_{w_1}, \mu_1, \ldots, \mu_{w_2})$. Вычисление показателей $e_1, \ldots, s_i, e_{i+1}$ в формуле (2.54) может быть осуществлено с помощью определенных нами меток. При этом $e_{i+1} = s$ есть число несобранных коммутаторов, равных c_{i+1}, на i-ом этапе, т. е. это число вхождений коммутатора c_{i+1} на i-ом этапе. Пусть $c_{i+1} = [c_r, c_s]$, тогда коммутатор c_{i+1} возникал всякий раз, когда собирались коммутаторы, равные c_s, причем c_{i+1} появлялся, когда вхождение коммутатора c_r предшествовало вхождению c_s в несобранной части слова. Следовательно, мы должны также учитывать условия предшествования вхождения коммутатора c_r вхождению c_s, когда оба они встречаются в несобранной части.

На нулевом этапе присутствуют только коммутаторы веса один, и для любого индекса $\lambda = 1, \ldots, n$ существует элемент $a_k(\lambda)$. При этом элемент $a_k(\lambda)$ предшествует элементу $a_s(\mu)$ на нулевом этапе при $k > s$, если $\lambda < \mu$, а при $k < s$, если $\lambda \leqslant \mu$. Итак, в терминах меток на нулевом этапе мы имеем следующие условия существования и предшествования: $E_k^0(a_k(\lambda)$, если метка λ существует, $P_{rs}^0(a_r(\lambda)$ предшествует $a_s(\mu))$ $\begin{pmatrix} \lambda < \mu \text{ если } r > s \\ \lambda \leqslant \mu \text{ если } r < s \end{pmatrix}$.
Пусть $\lambda_1, \ldots, \lambda_m$ — множество целых чисел; рассмотрим условия типа $\lambda_t < \lambda_u$, $\lambda_t \leqslant \lambda_u$. Всякие условия, получающиеся с помощью логического сложения и умножения из условий подобных неравенств, будем называть условиями (L). Покажем, что условия E_k^l существования коммутатора c_k с меткой $(\lambda_1, \ldots, \lambda_m)$ на i-ом этапе являются условиями (L) для

чисел $\lambda_1, \ldots, \lambda_m$, а условия предшествования P^i_{rs} коммутатора c_r коммутатору c_s в несобранной части на i-ом этапе являются условиями (L) для чисел $\lambda_1, \ldots, \lambda_m$, $\mu_1, \ldots, \mu_q$, если $(\lambda_1, \ldots, \lambda_m)$ — метка коммутатора c_r, а $(\mu_1, \ldots, \mu_q)$ — метка коммутатора c_s. Как мы заметили, на нулевом этапе условия существования и предшествования были условиями (L). Докажем по индукции, что это верно на любом этапе. Пусть утверждение верно для i-ого этапа. Чтобы показать его истинность для $(i+1)$-ого этапа, сравним тождества (2.53) и (2.54). Для $R_{j_1} = R_{j_2} = \ldots = R_{j_s} = c_{i+1}$ мы собирали сначала R_{j_1}, затем R_{j_2}, и, наконец, R_{j_s}. На каждом шаге мы производили замену SR на $RS[S, R]$. При этом любые коммутаторы, существовавшие на i-ом этапе и отличные от c_{i+1}, сохраняются также на $(i+1)$-ом этапе в том же порядке. Таким образом, для таких коммутаторов $E^{i+1}_k = E^i_k$ и $P^{i+1}_{rs} = P^i_{rs}$. Следовательно, нам нужно только рассмотреть условия существования коммутаторов c_k, возникающих на $(i+1)$-ом этапе, и предшествования P^{i+1}_{rs}, где или один из коммутаторов c_r, c_s, или оба возникли на рассматриваемом этапе. Коммутатор, возникший на $(i+1)$-ом этапе, имеет вид $c_k = \left[c_j, R_{u_1}, \ldots, R_{u_{m-1}}\right]$, где $r_{u_i} = c_{i+1}$. Он был получен перестановкой R_{u_1} с c_j, затем R_{u_2} с возникшим при этом коммутатором и т. д., пока, наконец, мы не поменяли местами R_{u_m} с коммутатором $\left[c_j, R_{u_1}, \ldots, R_{u_{m-1}}\right]$. При этом все коммутаторы $R_{u_1}, \ldots, R_{u_m}$ равны c_{i+1}. E^{i+1}_k — логическое произведение условий существования коммутаторов c_j, $R_{u_1}, \ldots, R_{u_m}$ на i-ом этапе и условий предшествования, согласно которым на i-ом этапе коммутаторы $c_j, R_{u_1}, \ldots, R_{u+m}$ расположены именно в рассматриваемом порядке. Таким образом, E^{i+1}_k — условие (L) для метки коммутатора c_k. На $(i+1)$-ом этапе коммутатор $[S, R]$ возникает в произведении $SR = RS[S, R]$ непосредственно за элементом S, но перед всеми коммутаторами, следующими за S. Мы должны найти условие предшествования P^{i+1}_{rs}, где $c_r = c_{j_1}$ или $c_r = [c_{j_1}, R_{u_1}, \ldots, R_{u_m}]$ и $c_s = c_{j_2}$ или $c_s = [c_{j_2}, R_{v_1}, \ldots, R_{v_w})]$. Если $c_{j_1} \neq c_{j_2}$, то $P^{i+1}_{rs} = P^i_{j_1 j_2}$. Если же $c_{j_1} = c_{j_2}$, то условие P^{i+1}_{rs} зависит от коммутаторов R_{u_i}, R_{v_j}. Пусть e — наибольшее целое число, такое, что $R_{u_1} = R_{v_1}, \ldots, R_{u_e} = R_{v_e}$. Тогда c_r предшествует c_s, если (1) $m = e$ и не существует коммутатора $R_{u_{e+1}}$ (в этом случае c_s есть коммутатор от коммутатора c_r), или (2) коммутатор $R_{v_{e+1}}$ предшествует $R_{u_{e+1}}$. Тогда P^{i+1}_{rs} — логическая сумма условий предшествования (для этапов, предшествующих $(i+1)$-му), которые поэтому являются также условиями (L) для меток коммутатора c_r и c_s.

Лемма 2.4.4.1. *[7, лемма 12.3.1] Число последовательностей $\lambda_1, \ldots, \lambda_m$ $(1 \leqslant \lambda_i \leqslant n)$, удовлетворяющих данным условиям (L), выражается в виде полинома от n: $b_1\binom{n}{1} + b_2\binom{n}{2} + \ldots + b_m\binom{n}{m}$, где b_i — числа, определяемые данным условием (L), но не зависящие от n.*

Доказательство. Разобьем индексы $1, \ldots, m$ на непересекающиеся множества $S_1, S_2, \ldots, S_t$. Выберем t чисел $v_1 < v_2 < \ldots < v_t \leqslant n$. Если в некоторой последовательности $\lambda_1, \lambda_2, \ldots, \lambda$ имеет место $\lambda_j = v_i$ для $j \in S_i$, то тем самым определено упорядочение чисел λ_i по величине. (Все до сих пор делалось некоторым произвольным образом.) Для любого возможного выбора чисел λ_i существует некоторый порядок указанного типа (т. е. подходящее разбиение $S_1, \ldots, S_t$ и набор чисел $v_1 < \ldots < v_t \leqslant n$). Число возможных выборов $v_1 < v_2 < \ldots < v_t \leqslant n$ равно $\binom{n}{t}$. При подобном упорядочении чисел λ_i (при фиксированном разбиении $S_1, S_2, \ldots, S_t$ и всевозможных выборах $v_1, v_2 < \ldots < v_t \leqslant n$) или все последовательности $\lambda_1, \ldots, \lambda_m$ данного типа упорядочения удовлетворяют условиям (L), или ни одна из них не удовлетворяет этим условиям. Следовательно, число последовательностей $\lambda_1, \ldots, \lambda_m$, удовлетворяющих данным условиям (L), есть полином $b_1\binom{n}{1} + b_2\binom{n}{2} + \ldots + b_m\binom{n}{m}$, где b_t — число возможных упорядочений с t различными значениями, удовлетворяющими условиям (L), и, очевидно, числа b_t зависят то этих условий, но не от n. $\boxtimes$

Например, если числа $\lambda_1, \lambda_2, \lambda_3$ удовлетворяют условиям (L) $\lambda_1 < \lambda_2$, $\lambda_3 \leqslant \lambda_2$, то возможны следующие упорядочения, удовлетворяющие условиям (L):

1) $\lambda_1 = v_1$, $\lambda_2 = \lambda_3 = v_2$, $v_1 < v_2$,
2) $\lambda_1 = \lambda_3 = v_1$, $\lambda_2 = v_2$, $v_1 < v_2$,
3) $\lambda_1 = v_1$, $\lambda_3 = v_2$, $\lambda_2 = v_3$, $v_1 < v_2 < v_3$,
4) $\lambda_3 = v_1$, $\lambda_1 = v_2$, $\lambda_2 = v_3$, $v_1 < v_2 < v_3$,

а число последовательностей $\lambda_1, \lambda_2, \lambda_3$, удовлетворяющих условиям (L), равно $2\binom{n}{2} + 2\binom{n}{3}$.

Мы уже показали, что показатель степени e_i коммутатора c_i в тождестве (2.53) равен числу коммутаторов, равных c_i в несобранной части слова на $(i-1)$-ом этапе, и что это число можно охарактеризовать как число последовательностей $\lambda_1, \ldots, \lambda_m$, удовлетворяющих определенным условиям (L), где m — вес коммутатора c_i. Таким образом, в лемме 2.4.4.1 говорится об этих показателях степени. Сформулируем полученные результаты в виде теоремы.

Теорема 2.4.4.2. *[7, теорема 12.3.1] Произведение $(a_1 a_2 \ldots a_r)^n$ представимо в виде $(a_1 a_2 \ldots a_r)^n = a_1^n a_2^n \ldots a_r^n c_{r+1}^{e_{r+1}} \ldots c_i^{e_i} R_1 \ldots R_t$, где $c_{r+1}, \ldots, c_i$ — выписанные в принятом порядке базисные коммутаторы элементов $a_1, \ldots, a_r$, а $R_1, \ldots, R_t$ — базисные коммутаторы, также выписанные здесь в некотором порядке, причем $c_i < R_1$. При $1 \leqslant j \leqslant i$, $e_j = b_1\binom{n}{1} + b_2\binom{n}{2} + \ldots + b_m\binom{n}{m}$, где m — вес коммутатора c_j, а $b_1, \ldots, b_m$ — неотрицательные целые числа, зависящие только от c_j и не зависящие от n.*

Отсюда легко вывести важное следствие для случая, когда G — p-группа класса нильпотентности, меньшего p. Собрав все коммутаторы весов, меньших p, мы сведем несобранную часть к единице. Более того, при $n = p^\alpha$ все показатели степени кратны n, так как $\binom{n}{i}$, $i \leqslant p-1$, есть биномиальный коэффициент.

Следствие 2.4.4.3. *[7, следствие 12.3.1] Если p-группа P имеет класс нильпотентности, меньший, чем p, то при $n = p^\alpha$ имеет место равенство*

$$(a_1 a_2 \ldots a_r)^n = a_1^n a_2^n \ldots a_r^n S_1^n S_2^n \ldots S_t^n,$$

где $S_1, S_2, \ldots, S_t$ — элементы, принадлежащие коммутанту подгруппы, порожденной элементами $a_1, a_2, \ldots, a_r$.

§5 Регулярные p-группы

Определение 2.4.5.1. [7, стр. 205] Будем называть p-группу P *регулярной*, если для любых двух элементов a и b и любого $n = p^\alpha$ имеет место равенство

$$(ab)^n = a^n b^n S_1^n \ldots S_t^n, \tag{2.55}$$

где $S_1, \ldots, S_t$ — подходящие элементы коммутанта группы, порожденной элементами a и b.

Следующие утверждения легко получаются из этого определения и следствия 2.4.4.3:

1) любая p-группа, класс нильпотентности которой меньше p, регулярна;
2) любая p-группа, порядок которой не больше p^p регулярна;

3) группа P регулярна, если любая подгруппа, порожденная двумя ее элементами регулярна;

4) любая подгруппа и факторгруппа регулярной группы регулярна.

Для любого p существует нерегулярная группа порядка p^{p+1}, а именно силовская подгруппа симметрической группы S_{p^2} степени p^2. Эта группа порождается двумя элементами порядка p и содержит элементы порядка p^2. Как будет показано, такое явление невозможно в регулярной группе.

Теорема 2.4.5.2. *[7, теорема 12.4.1] В регулярной p-группе при $n = p^\alpha$ имеет место тождество $a^n b^n = (ab)^n S_1^n = (abS_2)^n$, где S_1 и S_2 — элементы из коммутанта $\gamma_2(\langle a, b\rangle)$ группы $\langle a, b\rangle$, порожденной элементами a и b.*

Следствие 2.4.5.3. *[7, следствие 12.4.1] В регулярной p-группе при $n = p^\alpha$ справедливы равенства $a_1^n a_2^n \dots a_r^n = (a_1 a_2 \dots a_r S_2)^n = (a_1 \dots a_r)^n s_1^n$, где $S_1, S_2 \in \gamma_2(\langle a_1, \dots, a_r\rangle)$.*

Доказательство. Будем доказывать теорему и следствие одновременно. В абелевой группе теорема и следствие справедливы, причем $S_1 = S_2 = e$. Для доказательства теорема для произвольной подгруппы H применим индукцию. Предположим, что для любой собственной подгруппы группы H теорема и ее следствие верны. Заметим, что если группа H порождается элементами $a_1, \dots, a_r$, то ее коммутант $\gamma_2(H)$ является ее собственной подгруппой. Из тождества (2.55) сразу следует, что

$$a^n b^n = (ab)^n s_t^{-n} \dots S_1^{-n}. \tag{2.56}$$

По предположению индукции $S_t^{-n} \dots S_1^{-n} = S^n$, где $S \in \gamma_2(H)$. Но если $H = \langle a, b\rangle$ — неабелева группа, то $\langle \gamma_2(H), ab\rangle$ — собственная подгруппа группы H, откуда по индукции $(ab)^n S^n = (abS_2)^n$. Таким образом, теорема справедлива для группы H. Применяя теорему $r-1$ раз к произведению $a_1^n a_2^n \dots a_r^n$, получаем $a_1^n a_2^n \dots a_r^n = (a_1 a_2 \dots a_r)^n S_1^n \dots S_{r-1}^n$, где $S_1, \dots, S_{r-1} \in \gamma_2(H)$. Применяя к подгруппе $\gamma_2(H)$ следствие, получаем $a_1^n a_2^n \dots a_r^n = (a_1 a_2 \dots a_r)^n S^n$, а применяя теорему, получаем $(a_1 a_2 \dots a_r)^n S^n = (a_1 a_2 \dots a_r T)^n$. ⊠

Теорема 2.4.5.4. *[7, теорема 12.4.2] Конечная p-группа p регулярна тогда и только тогда, когда для любых элементов $a, b \in P$ имеет место равенство*

$$a^p b^p p = (ab)^p S^p, \tag{2.57}$$

где S — элемент коммутанта группы, порожденной элементами a и b.

Доказательство. Условие (2.57), конечно, выполняется в регулярной p-группе; это частный случай теоремы 2.4.5.2. Докажем обратное утверждение: из условия (2.57) вытекает условие

$$a^n b^n = (ab)^n S_1^n,\ n = p^\alpha,\ S_1 \in \gamma_2(\langle a, b\rangle). \tag{2.58}$$

Для этого покажем сначала по индукции справедливость равенств

$$a_1^p a_2^p \dots a_r^p = (a_1 a_2 \dots a_r)^p S_1^p = (a_1 a_2 \dots a_r S_2)^p, \tag{2.59}$$

где $S_1, S_2 \in \gamma_2(\langle a_1, \dots, a_r\rangle)$. Если H — абелева группа, то эти равенства, конечно, выполняются при $S_1 = S_2 = 1$. Если равенство (2.59) выполняется для любой собственной подгруппы группы H, то применяя соотношение (2.57) $r-1$ раз, получаем $a_1^p a_2^p \dots a_r^p = (a_1 \dots a_r)^p u_1^p \dots u_{r-1}^p$, где $u_1, \dots, u_{r-1} \in \gamma_2(H)$. По предположению индукции $u_1^p \dots u_{r-1}^p = S_1^p$. Но элементы $b = a_1 a_2 \dots a_r$ и S_1 порождают собственную подгруппу группы H, откуда $(a_1 a_2 \dots a_r)^p S_1^p = (a_1 \dots a_r S_2)^p$, и тождество (2.59) установлено.

Докажем вспомогательную лемму.

Лемма 2.4.5.5. *[7, лемма 12.4.1] Если справедливо соотношение* (2.57), *то* $x^{-p}y^{-p}x^py^p = S^p$, *где* S *— элемент коммутанта группы* $\langle x, y\rangle$.

Доказательство. $x^py^p = (xy)^pS_1^p$, $y^px^p = (yx)^pS_2^p$, откуда $x^{-p}y^{-p}x^py^p = S_2^{-p}(yx)^{-p}(xy)^p$ S_1^p, но, кроме того, $(y, x)^{-p}(x, y)^p = (x^{-1}y^{-1}xy)^pS_3^p = [x, y]^pS_3^p$, следовательно, $x^{-p}y^{-p}x^py^p = S_2^{-p}[x, y]^pS_3^pS_1^p = S^p$. ⊠

Вернемся к доказательству теоремы. Из леммы 2.4.5.5 следует, что любой коммутатор элементов $a_1^p, a_2^p, \dots, a_r^p$ является p-й степенью некоторого элемента коммутанта группы $\langle a_1, \dots, a_r\rangle$.

Из (2.57) имеем

$$a^{p^2}b^{p^2} = (a^pb^p)^pS_1^p = [(ab)^pS_2^p]^pS_1^p = (ab)^{p^2}S_2^{p^2}S_3^pS_1^p, \tag{2.60}$$

где S_1 — элемент коммутанта группы $\langle a^p, b^p\rangle$, а S_3 — элемент коммутанта группы $\langle (ab)^p, S_2^p\rangle$. В силу леммы 2.4.5.5 оба эти элемента являются p-ми степенями элементов коммутанта группы $\langle a, b\rangle$, откуда

$$a^{p^2}b^{p^2} = (ab)^{p^2}S_2^{p^2}S_4^{p^2}S_5^{p^2}, \tag{2.61}$$

т. е. соотношение (2.58) справедливо при $n = p^2$. Аналогичные рассуждения с применением леммы дают возможность доказать справедливость соотношения (2.58) для $n = p^\alpha$ в предположении, что оно верно для $n = p^\alpha$, т. е. закончить доказательство соотношения (2.58) по индукции. ⊠

Теорема 2.4.5.6. *[7, теорема 12.4.3] Если* P *— регулярная* p*-группа и* $n = p^\alpha$, *то*

1) из $[a^n, b] = 1$ *следует* $[a, b]^n = 1$, *и обратно;*

2) если $[a^n, b] = 1$, *то* $[a, b^n] = 1$;

3) коммутатор S, *содержащий элемент* u, *имеет порядок, не превосходящий порядка элемента* u *по модулю* Z, *где* Z *— центр группы* P;

4) порядок произведения $a_1a_2\dots a_r$ *не больше порядка каждого из элементов* $a_1, a_2, \dots, a_r$.

Доказательство. В абелевой p-группе эти свойства тривиальны. Предположим, что теорема верна для всех собственных подгрупп неабелевой группы P. Применяя тождество (2.58) к равенству

$$a^{-n}b^{-1}a^nb = (a^{-1})^n(b^{-1}ab)^n = (a^{-1}b^{-1}ab)^ns^n, \tag{2.62}$$

где s — элемент коммутанта группы $\langle a, b^{-1}ab\rangle \leqslant\rangle a, b\rangle$, получаем

$$(a^n, b) = (a, b)^ns_1^n. \tag{2.63}$$

Если теперь $[a^n, b] = 1$, то порядок a в факторгруппе по центру Z группы $\langle a, b\rangle$ не больше n, откуда в силу свойства (3) в собственной подгруппе $K = \langle a, b^{-1}ab\rangle = \langle a, [a, b]\rangle < \langle a, b\rangle$ при $u = a$ любой коммутатор из подгруппы K включает элемент a, и его порядок не больше n. Элемент s_1 в равенстве (2.63) равен произведению коммутаторов из подгруппы K, и в силу свойства (4) для подгруппы K порядок элемента s_1 не больше n. Таким образом, если $[a^n, b] = 1$, то в (2.63) $s_1^n = 1$, откуда $[a, b]^n = 1$. Обратно, если $[a, b]^n = 1$, то в подгруппе $K = \langle a, [a, b]\rangle = \langle a, u\rangle$, где $u = [a, b]$, порядок элемента u в K/Z (Z — центр подгруппы K) не превосходит n, и в каждом коммутаторе встречается элемент u. Тогда в силу свойства (3) подгруппы K все коммутаторы этой подгруппы имеют порядок, не превосходящий n, откуда, используя свойство (4) коммутанта $\gamma_2(K)$ группы K, получаем, что порядок элемента s_1 не больше n.

Таким образом, из условия $[a,b]^n = 1$ следует, что $s_1^n = 1$, откуда $[a^n, b] = 1$ в силу (2.63). Этим установлено свойство (1) группы, из которого сразу следует свойство (2). Действительно, $[a, b^n] = [a,b]^n s^n$, где $s \in \gamma(\langle a, b\rangle)$. Как и выше можно доказать, что $s^n = 1$. Поскольку $[a,b]^n = 1$ отсюда следует, что $[a, b^n] = 1$. Свойство (3) получается повторным применением свойства (1) (очевидно).

Осталось доказать свойство (4) для группы P. Если $a^n = 1$, $b^n = 1$, то в силу свойства (3) порядок любого коммутатора, в котором встречается элемент a или b, не превосходит n. Следовательно, элемент S_1 из равенства (2.58)равен произведению коммутаторов, порядки которых не превосходят n; применяя свойство (4) для собственной подгруппы P', получаем, что порядок элемента S_1 не больше, чем n. Следовательно, $S_1^n = 1$, и поэтому $(ab)^n = 1$. Таким образом, порядок произведения двух сомножителей не превосходит порядка каждого из сомножителей, откуда повторным применением этого свойства легко получить аналогичное утверждение для r сомножителей. ⊠

Теорема 2.4.5.7. *[7, теорема 12.4.4] Если $a^n = b^n$ при $n = p^\alpha$, то $(ab^{-1})^n = 1$, и обратно.*

Доказательство. В силу теоремы 2.4.5.6 достаточно доказать лишь «и обратно». Пусть $a^n b^{-n} = (ab^{-1})^n s_1^n$, $(ab^{-1}) = 1$ и $\langle a, b\rangle = \langle a, ab^{-1}\rangle$. Тогда из свойства (3) для элемента $u = ab^{-1}$ получаем $s_1^n = 1$, откуда $a^n = b^n$. ⊠

Теорема 2.4.5.8. *[7, теорема 12.4.5] В регулярной p-группе P элементы вида a^{p^α}, где $a \in P$, образуют характеристическую подгруппу $C^\alpha(P)$, а элементы, порядки которых не превышают p^α, — характеристическую подгруппу $C_\alpha(P)$.*

Доказательство. В силу предыдущих теорем доказательство очевидно. ⊠

Глава 3

Разрешимые группы

3.1 Общие свойства и примеры

§1 Определения

Теорема 3.1.1.1. *[1, теорема 19.1.1] Для произвольной группы G равносильны следующие утверждения:*

а) группа G обладает субнормальной матрешкой с абелевыми секциями,

б) группа G обладает нормальной матрешкой с абелевыми секциями,

в) ряд коммутантов $G \geqslant G' \geqslant \ldots \geqslant G^{(n)} \geqslant \ldots$ группы G через конечное число шагов обрывается на единице, т. е. является (конечной) матрешкой,

г) группа G удовлетворяет одному из тождеств $\delta_n(x_1, \ldots, x_{2^n}) = 1$, $n = 0, 1, 2, \ldots$, где $\delta_0(x) = x$, $\delta_{n+1}(x_1, \ldots, x_{2^{n+1}}) = [\delta_n(x_1, \ldots, x_{2^n}), \delta_n(x_1, \ldots, x_{2^n})]$.

Доказательство. в)$\Longrightarrow$б)$\Longrightarrow$а). Очевидно.

а)$\Longrightarrow$в). Пусть группа G обладает субнормальной матрешкой с абелевыми секциями: $1 = H_0 < H_1 < \ldots < H_s = G$. Так как факторгруппа G/H_{s-1} абелева, то $G' \leqslant H_{s-1}$. Предположим, что уже установлено включение $G^{(k)} \leqslant H_{s-k}$, $1 \leqslant k < s$. Ввиду коммутативности секции H_{s-k}/H_{s-k-1} коммутант $(G^{(k)})' = G^{(k+1)}$ содержится в H_{s-k-1}. Отсюда $G^{(s)} = 1$. Следовательно, доказана равносильность первых трех утверждений.

Эквивалентность утверждений в) и г) очевидна. ⊠

Из доказательства теоремы 3.1.1.1 видно, что на разрешимых группах ступени разрешимости $\leqslant n$ и только на них выполняется тождество $\delta_n = 1$. Следовательно, класс разрешимых групп ступени разрешимости $\leqslant n$ есть многообразие. Непосредственным следствием этого замечания является замкнутость класса разрешимых групп относительно взятия подгрупп, гомоморфных образов и конечных прямых произведений, а также декартовых произведений при условии ограниченности ступеней разрешимости сомножителей. Прямое (декартово) произведение произвольных разрешимых групп может не быть разрешимой группой.

§2 Полицикличность и сверхразрешимость

Определение 3.1.2.1. [1, стр. 185] Разрешимая группа называется *сверхразрешимой*, если она обладает нормальной (а не просто субнормальной) матрешкой с циклическими секциями.

Теорема 3.1.2.2. *[1, теорема 19.2.2] Коммутант сверхразрешимой группы нильпотентен.*

Доказательство. Пусть в группе G задана нормальная полициклическая матрешка $1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G$, и пусть G' — коммутант группы G. Тогда ряд $1 = H_0 \leqslant H_1 \leqslant \ldots \leqslant H_n = G'$, где $H_i = G_i \cap G'$, является нормальной полициклической матрешкой в G'. Покажем, что на самом деле она центральна в G', т. е. $[g', H_{i+1}] \leqslant H_i$ для всех $i = 0, 1, 2, \ldots, n-1$. Очевидно, сопряжения группы G элементами из G индуцируют автоморфизмы в секциях H_{i+1}/H_i. Так как группа автоморфизмов циклической группы абелева, то коммутант G' должен индуцировать во всех секциях H_{i+1}/H_i тождественное преобразование. Но это и означает, что центральность матрешки. ⊠

Определение 3.1.2.3. [1, стр. 185] Пусть G — конечная группа порядка $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где p_i — простые числа, $p_1 > \ldots > p_k$. Нормальная матрешка $1 = H_0 < H_1 < \ldots < H_k = G$ называется *силовской матрешкой* группы G, если секция H_{i+1}/H_i, $i = 0, 1, \ldots, k-1$, является силовской p_{i+1}-подгруппой группы G/H_i. (Иногда в этом определении не требуют упорядоченности $p_1 > \ldots > p_k$.)

Теорема 3.1.2.4. *[1, теорема 19.2.3] Конечная сверхразрешимая группа обладает силовской матрешкой.*

Доказательство. Пусть p — наибольший простой делитель порядка сверхразрешимой группы G, и пусть H — какая-нибудь ее нормальная подгруппа простого порядка q. Факторгруппа G/H сверхразрешима и $|G/H| < |G|$. По индуктивным соображениям можно считать, что в факторгруппе G/H силовская p-подгруппа P/H нормальна. При $p = q$ подгруппа P будет силовской p-подгруппой в G и $P \trianglelefteq G$. Если $p \neq q$, то в G/H найдется нормальная подгруппа H_1/H порядка p. По теореме Силова, как легко видеть, силовская p-подгруппа H_2 группы H_1 единственна и потому ввиду соотношения $H_1 \trianglelefteq G$ нормальна в G. Таким образом, можно сразу считать, что $p = q$, следовательно, выполнен уже разобранный случай. ⊠

3.2 Конечные разрешимые группы

§1 Холловы и картеровы подгруппы

Определение 3.2.1.1. Натуральное число k называется *холловым делителем* числа n, если $k | n$ и $\left(k, \frac{n}{k}\right) = 1$. Всякую подгруппу конечной группы G, порядок которой является некоторым холловым делителем порядка группы G, называют *холловой подгруппой*.

Теорема 3.2.1.2. (Ф. Холл). *[1, теорема 20.1.1] Пусть G — конечная разрешимая группа порядка n и k — холлов делитель числа n. Тогда*

1) в группе G существует по крайней мере одна подгруппа порядка k;

2) любые две подгруппы порядка k сопряжены в G;

3) любая подгруппа порядка $k' | k$ содержится в подгруппе порядка k.

Доказательство. Индукция по n. Допустим, что все утверждения теоремы справеливы для произвольной конечной разрешимой группы, порядок которой меньше n. Обозначим через A минимальную нормальную подгруппу группы G. Ясно, что A является элементарной абелевой подгруппой порядка p^α, где p — некоторое простое число.

Если $p|k$, то ввиду индуктивного допущения в факторгруппе G/A существует подгруппа B/A порядка k/p^m. Тогда порядок B равен k. Кроме того, любые подгруппы B_1, B_2 порядка k содержат, очевидно, подгруппу A. По индукции подгруппы B_1/A и B_2/A сопряжены в G/A. Следовательно, подгруппы B_1, B_2 сопряжены в G.

Пусть теперь p не делит k. Обозначим через D наибольшую нормальную подгруппу группы G, порядок которой взаимно прост с k, а через H/D — минимальную нормальную подгруппу группы G/D. Порядок H/D имеет вид $q^s, q^s|k$.

Если нормализатор $N_G(Q)$ силовской q-подгруппы Q из H совпадает с G, то $Q \trianglelefteq G$ и доказательство проводится также, как и при допущении, что $p|k$.

Пусть $N_G(Q) \neq G$. Из равенства $G = N_G(Q)H = N_G(Q)D$ (первое см. лемму Фраттини 2.2.1.3, второе из первого, поскольку $H = QD$) следует, что порядок $N_G(Q)$ делится на k. Отсюда ввиду индуктивных предположений вытекает существование в $N_G(Q)$, а, значит, и в группе G, подгруппы порядка k.

Возьмем две подгруппы B_1, B_2 порядка k. Пересечения $B_1 \cap H$, $B_2 \cap H$ являются в H силовскими q-подгруппами, поэтому, ввиду их сопряженности, можно считать, что $B_1 \cap H = B_2 \cap H = Q$. Подгруппа Q, очевидно, нормальна в подгруппе $\langle B_1, B_2\rangle$. На основании индукции подгруппы B_1/Q и B_2/Q сопряжены в $\langle B_1, B_2\rangle/Q$. Отсюда следует сопряженность подгрупп B_1, B_2.

Итак, утверждения 1) и 2) доказаны. Докажем 3).

Пусть B' — подгруппа порядка k'. При $p|k$ порядок подгруппы AB', очевидно, делит k. В силу индуктивного допущения подгруппа AB'/A содержится в некоторой подгруппе порядка k/p^m. Тогда AB' содержится в некоторой группе порядка k. Пусть теперь p не делит k. На основании индуктивных предположений подгруппа AB'/A содержится в подгруппе C/A порядка k. На том же основании можно считать, что $C = G$. По доказанному п. 1) в G существует подгруппа B порядка k. Очевидно, произведение AB совпадает с G и потому $AB'B = G$. Из формул $|G| = \frac{|AB'|\cdot|B|}{|AB'\cap B|}$, $|G| = p^m k$, $|AB'| = p^m k'$, $|B| = k$ получаем, что порядок $D = AB' \cap B$ равен k'. По доказанному п. 2) подгруппы B' и D сопряжены в AB': $B' = D^g$. Отсюда следует, что B' содержится в подгруппе B^g порядка k. ⊠

Определение 3.2.1.3. [1, стр. 189] Подгруппа H группы G называется *картеровой*, если H нильпотентна и совпадает со своим нормализатором в G.

Предложение 3.2.1.4. (Обобщенная лемма Фраттини). *[1, упражнение 17.1.9] Пусть A — нормальная подгруппа группы G и B — такая подгруппа из A, что $B, B' \leqslant A$ сопряжены в G. Тогда $G = A \cdot N_G(B)$.*

Доказательство. Пусть $g \in G$. Тогда $B^g = B' \leqslant A$. Следовательно, существует такой $a \in A$, что $B^a = B'$. Отсюда $ga^{-1} \in N_G(B)$. ⊠

Теорема 3.2.1.5. (Картер). *[1, теорема 20.1.4] Конечная разрешимая группа G обладает по крайней мере одной картеровой подгруппой и любые две картеровы подгруппы группы G сопряжены между собой.*

Доказательство. Индукция по порядку группы G.

Пусть A — минимальная нормальная подгруппа группы G и $|A| = p^m$. В силу индуктивного предположения факторгруппа G/A обладает картеровой подгруппой, скажем, K'/A. Пусть Q — холлова p'-подгруппа группы K'. Покажем, что $K = N_{K'}(Q)$ будет картеровой подгруппой в G.

Действительно, по обобщенной лемме Фраттини (предложение 3.2.1.4) имеем $K' = N_{K'}(Q) \cdot QA = KA$. Подгруппа K разлагается в прямое произведение нильпотентных подгрупп Q и $K \cap P$, где P — силовская p-подгруппа группы K' (так как при гомоморфизм $K' \longrightarrow K'/A$ является изоморфизмом на K). Далее, пусть $K^g = K$. Так как $A \trianglelefteq G$ и $K' = KA$, то $K'^g = K'$ и, следовательно, $g \in K'$. Нормализатор холловой подгруппы совпадает со своим нормализатором (это очевидно), поэтому элемент g содержится в K.

Пусть теперь K_1, K_2 — картеровы подгруппы группы G. Докажем их сопряженность в G.

Сначала докажем, что K_iA/A, $i = 1, 2$, является картеровой подгруппой группы G/A. Нильпотентность подгруппы K_iA/A очевидна. Если $(K_iA)^g = K_iA$, $g \notin K_iA$, то $|K_iA| < |G|$ и, значит, в силу индуктивного предположения, примененного к картеровым подгруппам из K_iA существует такой элемент $a \in K_iA$, что $K_i^g = K_i^a$ или $K_i^{ga^{-1}} = K_i$. Но подгруппа K_i совпадает со своим нормализатором, поэтому $ga^{-1} \in K_i$, что противоречит допущению $g \notin K_iA$.

Легко понять, что холлова p'-подгруппа Q_i из K_i является холловой p'-подгруппой группы K_iA. Кроме того, нормализатор $N_{K_iA}(Q_i)$ подгруппы Q_i в KA_i нильпотентен и содержит K_i. Следовательно, K_i совпадает с $N_{K_iA}(Q_i)$. По индуктивному допущению картеровы подгруппы K_1A/A, K_2A/A сопряжены между собой. Поэтому можно считать, что $K_1A = K_2A$. Как было отмечено, подгруппа K_i совпадает с нормализатором $N_{K_1A}(Q_i)$. Но холловы p'-подгруппы Q_1, Q_2 групп K_1, K_2, являющиеся холловыми p'-подгруппами группы K_1A, сопряжены между собой. Поэтому сопряжены и их нормализаторы. ⊠

§2 О полной приводимости представлений

Определение 3.2.2.1. [1, стр. 190] Пусть V — линейное пространство над полем K, G — группа линейных преобразований пространства V. Если в V существует собственное подпространство, допустимое относительно G, то группу G называют *приводимой.* В противном случае группу G называют *неприводимой* или *неприводимо действующей* на пространстве V. Группа G называется *вполне приводимой*, если для всякого допустимого подпространства $U \leqslant V$ существует допустимое дополнение, т. е. такое допустимое подпространство W, что $V = U \oplus W$.

Произвольный гомоморфизм φ абстрактной группы G в группу линейных преобразований n-мерного векторного пространства над полем K назвается *линейным представлением* группы G. Если группа линейных преобразований G^{φ} неприводима (приводима, вполне приводима), представление φ назвается *неприводимым* (соответственно *приводимым, вполне приводимым*). Произвольный гомоморфизм ψ группы G в группу матриц $Gl_n(K)$ называется *матричным представлением.*

Теорема 3.2.2.2. (Машке). *[1, теорема 20.2.2] Пусть φ — представление конечной группы G линейным преобразованиями линейного пространства V над полем K. Если порядок G не делится на характеристику поля K, то представление φ вполне приводимо.*

Доказательство. Будем считать, что G действует на V в силу представления φ. Пусть U — допустимое относительно G подпространство из V. Обозначим через W какое-нибудь дополнение подпространства U, $V = U \oplus W$. Далее, обозначим через π_W проектирование V на подпространство W и положим $vt = \frac{1}{m} \sum_{g \in G} vg^{-1}\pi_w g$, $v \in V$, где m — порядок группы G. Отображение t является линейным преобразованием пространства V. При фиксированном $h \in G$ элемент gh вместе с g пробегает все элементы группы G. Поэтому справедливы равентсва $(vt)h = \frac{1}{m}\sum_g vh\cdot h^{-1}g^{-1}\pi_W gh = (vh)t$, из которых следует допустимость линейного подпространства $W_0 = Vt$ относительно G.

Остается установить разложение $V = U\oplus W_0$. Произвольный элемент $v\in V$ представим в виде суммы $v = (v-vt)+vt, vt\in W_0$. Первое слагаемое $v-vt$ равно $v-\frac{1}{m}\sum_g vg^{-1}\pi_W g = \frac{1}{m}\sum_g (vg^{-1}-vg^{-1}\pi_W)g$. Так как $vg^{-1}-vg^{-1}\pi_W\in U$ и U допустимо, то $v-vt$ принадлежит U. Отсюда следует равенство $V = U+W_0$. Предположим, наконец, что $v\in U\cap W_0$. Так как $v\in U$, U допустимо относительно G и для любого элемента $u\in U$ проекция $u\pi_W$ равна 0, то

$$vt = 0. \tag{3.1}$$

С другой стороны, элемент v принадлежит W_0, поэтому существует такой элемент $v'\in V$, что

$$v't = v. \tag{3.2}$$

Но тогда $vt = v't^2$. Как было отмечено выше, $v'-v't\in U$ и, значит, $v't-v't^2 = 0$. Отсюда $vt = v't$, что вместе с равенствами (3.1), (3.2) влечет $v = 0$. ⊠

Предложение 3.2.2.3. (Обобщенная теорема Машке). *[1, упражнение 20.2.4] Пусть G — конечная группа линейных преобразований линейного пространства V над полем характеристики $p>0$, P — силовская p-подгруппа группы G. Если G-допустимое подпространство U обладает P-допустимым дополнением, то U обладает также G-допустимым дополнением.*

Доказательство. Пусть $V = U\oplus W$, где W есть P-допустимое подпространство. Обозначим через π_W проектирование V на подпространство W и положим

$$vt = \frac{1}{m}\sum_{g\in S} vg^{-1}\pi_W g,\ \ v\in V,$$

где $m = |G:P|$ и S — некоторое множество элементов, выбранных по одному в каждом правом смежном классе группы G по подгруппе P. Очевидно, проектирование π_W перестановочно с каждым элементом группы P. Дальнейшие рассуждения повторяют доказательство теоремы Машке. ⊠

Теорема 3.2.2.4. (Шур). *[1, теорема 20.2.6] Пусть конечная группа G порядка n содержит такую нормальную подгруппу A порядка k, что $(k,n/k) = 1$. Тогда A обладает по крайней мере одним дополнением, т. е. подгруппой B с условиями $G = A\cdot B$, $A\cap B = 1$.*

Доказательство. а) Пусть сначала A абелева и имеет простой период p. По теореме Фробениуса можно считать G подгруппой сплетения $W = A\wr B$, $B = G/A$, причем $W = G\cdot\overline{A}$, $G\cap\overline{A} = A$, где $\overline{A} = \mathrm{Fun}(B,A)$. Так как $|G:A|$ не делится на p и $A\lhd W$, то ввиду теоремы Машке3.2.2.2 существует такая нормальная в W подгруппа C, что $\overline{A} = A\times C$. (Группу $\overline{A}$ мы можем рассматривать как векторное пространство над полем $GF(P)$ с естественным образом определенным действием группы G, которое, очевидно, будет линейным.) Из соотношений $W/C = \overline{A}/C\cdot BC/C$, $\overline{A}\cap BC = C$ и естественного изоморфизма $\varphi : W/C\longrightarrow G$ следует, что $G = AD$, где D — образ подгруппы BC/C относительно φ.

б) Теперь докажем теорему в общих предположениях. Доказательство будем вести индукцией по порядку группы. Допустим, что теорема неверна для выбранной группы G, но справедлива для всякой группы меньшего порядка. Отметим, что существование дополнения к подгруппе A равносильно существованию в G подгруппы порядка $l = \frac{n}{k}$, так как $(l, k) = 1$.

Пусть P — силовская p-подгруппа из A. Так как $G = A \cdot N_G(P)$, то $N_G(P)$ обладает нормальной подгруппой $A \cap N_G(P)$, порядок которой вэаимно прост с индексом $l = |N_G(P) : (A \cap N_G(P)|$. Поэтому, если $|N_G(P)| < n$, то по индуктивному предположнию подгруппа $N_G(P)$, а следовательно, и группа G, обладает подгруппой порядка l, что противоречит выбору G. Значит, всякая силовская p-подгруппа из A нормальна в G, и поэтому коммутант $A' < A$ (A нильпотентна). Пусть $A' \neq 1$. Тогда группа G/A' удовлетворяет условиям теоремы и $|G/A'| < n$. Следовательно, в G/A' существует подгруппа C/A' порядка l. Применяя индуктивное предположение к группе C, приходим к существованию в ней подгруппы порядка l. Из полученного противоречия с выбором G вытекает коммутативность A. Если далее $p|k$, $A^p \neq 1$, то беря A^p в роли A' получаем аналогичное противоречие. Значит, A абелева периода p. Противоречие с а). ⊠

Отметим, (без доказательства) что любые два l-дополнения сопряжены в G.

Лемма 3.2.2.5. *[1, лемма 20.2.7] Группа линейных преобразований линейного пространства V над полем K вполне приводима тогда и только тогда, когда V разлагается в прямую сумму допустимых неприводимых подпространств.*

Доказательство. Легко получается с помощью индукции. ⊠

Лемма 3.2.2.6. *[1, лемма 20.2.8] Неприводимое представление абелевой группы G над алгебраически замкнутым полем одномерно.*

Доказательство. Очевидно, поскольку любая конечная абелева группа имеет общий собственный вектор в векторном пространстве над алгебраически замкнутым полем. ⊠

§3 Критерий сверхразрешимости

Предложение 3.2.3.1. *[1, упражнение 11.3.6] Пусть G — конечная группа и $A \leqslant G$. Если индекс $|G : A|$ меньше некоторого простого делитель p порядка группы G, то пересечение $\cap_{g \in G} A^g$ содержит силовские p-подгруппы группы G и, в частности, отлично от единицы.*

Доказательство. Ясно, что ядром подстановочного представления группы G на смежных классах по подгруппе A является группа $K(A) = \cap_{g \in G} A^g$, которая, следовательно, нормальна в G. Кроме того, так как это подстановочное представление дает гомоморфный образ порядка $\leqslant n!$, где $n = |G : A|$ и $n < p$, то мы получаем, что $K(A)$ содержит некоторую (а, значит, все) силовские p-подгруппы группы G. ⊠

Теорема 3.2.3.2. (Хупперт). *[1, теорема 20.1.3] Конечная группа сверхразрешима тогда и только тогда, когда все ее максимальные подгруппы имеют простые индексы.*

Доказательство. Необходимость очевидна, докажем достаточность.

Пусть максимальные подгруппы группы G имеют простые индексы, и пусть доказано, что все группы с таким условием, имеющие порядки $< |G|$, сверхразрешимы. Докажем сначала разрешимость группы G. Обозначим через p наибольший простой делитель порядка $|G|$ и через M' какую-нибудь максимальную подгруппу, содержащую силовскую p-подгруппу группы G. Тогда $|G : M'| < p$ и, согласно предложению 3.2.3.1 пересечение

$M'' = \cap_{g \in G} M'^g$ отлично от единицы и, конечно, нормально в G. Таким образом, некоторая минимальная нормальная подгруппа M группы G отлична от G. Возьмем силовскую q-подгруппу Q из M по наибольшему простому делителю q порядка $|M|$ и предположим, что $N_G(Q) \neq 1$. Так как $N_G(Q)M = G$ (лемма 2.2.1.3), то для произвольной максимальной подгруппы $H \geqslant N_G(Q)$ группы G тем более выполняется равенство $HM = G$, откуда $|G : H| = |M : (M \cap H)|$. Простой индекс $|M : (M \cap H)| = q'$ делит число $|M : N_M(Q)|$, взаимно простое с q, следовательно, $q' < q$. Снова ввиду предложения 3.2.3.1 можно утверждать, что в M существует собственная нормальная подгруппа M_0, содержащая все q-элементы из M. Этим же свойством обладает и всякая подгруппа, сопряженная в M_0. Поэтому пересечение $\cap_{g \in G} M_0^g$ отлично от 1, M и нормально в G, что противоречит выбору M. Из полученного следует, что $N_G(Q) = G$, т. е. $Q \trianglelefteq G$, и, значит, $Q = M$. Таким образом, в группе G есть разрешимая нормальная подгруппа M, факторгруппа по которой согласно индукции сверхразрешима. Отсюда получается разрешимость G.

Как мы знаем, минимальная нормальная подгруппа M разрешимой группы G абелева и разлагается в прямое произведение циклических групп простого порядка q. Остается доказать, что $|M| = q$, или по крайней мере существование в G какой-либо циклической нормальной подгруппы. Рассмотрим две возможности.

1) Наибольший простой делитель p порядка группы G больше q. В этом случае в G/M найдется нормальная подгруппа A/M (теорема 3.1.2.4). При $N_G(P) = G$, где $P < A$ — подгруппа порядка p, в группе G существует циклическая нормальная подгруппа, что влечет сверхразрешимость G. Если $N_G(P) \neq G$, то максимальная подгруппа $H \geqslant N_G(P)$ не содержит M (иначе было бы $G = N_G(P)A = HPM \leqslant H$), откуда $G = HM$ и пересечение $H \cap M$ нормально в G. Ввиду минимальности M это пересечение равно единице и, следовательно, так как индекс $|G : H|$ прост, порядок M равен q.

Число q является наибольшим простым делителем порядка группы G. В данной ситуации ввиду сверхразрешимости группы G/M и теоремы 3.1.2.4 силовская q-подгруппа G_q нормальна в G. Из нормальности центра Z подгруппы G_q в группе G и $Z \cap M \neq 1$ (см. 2.1.2.3) следует $M \leqslant Z$.

Если $M = G_q$, то в факторгруппе G/M найдется нормальная подгруппа A/M простого порядка p, отличного от q. Тогда сверхразрешимость G доказывается так же, как в случае 1).

Пусть теперь $M \neq G_q$. Обозначим через B/M нормальную подгруппу группы G/M порядка q. Очевидно, подгруппа B абелева. Все элементы группы B имеют порядок q, в противном случае BD^q была бы искомой подгруппой порядка q, нормальной в группе G.

Предположим сначала, что B не лежит в центре Z. Разумеется, B принадлежит второму гиперцентру группы G_q. В силу сверхразрешимости группы G/B существует такая матрешка $1 < B = B_0 < B_1 < \ldots < B_s = G_q$, что $B_i \trianglelefteq G$, $|B_{i+1} : B_i| = q$. Найдется такой номер k, что $B \leqslant Z(B_k)$, но $B \not\leqslant Z(B_{k+1}$. Пусть $B = \langle M, b \rangle$, $B_{k+1} = \langle B_k, b_{k+1} \rangle$. Тогда совокупность всевозможных элементов вида $[b, x]$, $x \in B_{k+1}$ будет подгруппой порядка q, нормальной в G. Действительно, для произвольных элементов $x = c_1 b_{k+1}^l$, $y = c_2 b_{k+1}^m$, $c_1, c_2 \in B_k$, $g \in G$, имеем: $[b, x][b, y] = [b, b_{k+1}^l][b, b_{k+1}^m] = [b, b_{k+1}]^{l+m}$, $[b, b_{k+1}]^g = [b^g, b_{k+1}^g] = [ab^n, c_2 b_{k+1}^r] = [b, b_{k+1}]^{n+r}$, где a, c_3 — некоторые элементы соответственно из M и B_k.

Таким образом, можно считать, что B принадлежит центру группы G_q. Далее, группу B можно рассматривать как векторное пространство над полем $GF(q)$, а группу F автоморфизмов B, индуцированных внутренними автоморфизмами группы G, — как группу линейных преобразований этого пространства. Так как $B \leqslant Z$, то порядок группы F, изоморфной $G/C_G(B)$, взаимно прост с q. Поэтому на основании теоремы Машке 3.2.2.2

допустимое относительно F подпростанство M имеет в B допустимое дополнение A размерности 1. На групповом языке это означает, что A является циклической нормальной подгруппой группы G. ⊠

3.3 Разрешимые группы с условиями максимальности и минимальности

§1 Определения и примеры

Определение 3.3.1.1. [1, стр. 229] Говорят, что группа удовлетворяет *условию минимальности (для подгрупп)* или короче, *условию* min, если всякий убывающий ряд ее подгрупп $H_1 \geqslant H_2 \geqslant \ldots$ обрывается, т. е. $H_n = H_{n+1} = \ldots$ при некотором n. Говорят, что группа удовлетворяет *условию максимальности (для подгрупп)* или, короче, *условию* max, если всякий возрастающий ряд ее подгрупп $H_1 \leqslant H_2 \leqslant \ldots$ обрывается, т. е. $H_n = H_{n+1} = \ldots$ при некотором n.

Предложение 3.3.1.2. *[1, упражнение 24.1.1] Условие* max *равносильно условию, что все подгруппы рассматриваемой группы конечно порождены.*

Доказательство. Пусть H — некоторая подгруппа группы G. Пусть h_1 — некоторый нетривиальный элемент из H. Определим $H_1 = \langle h_1 \rangle$. Если группа H_{i-1} уже определена, пусть h_i — некоторый элемент подгруппы H, не лежащий в H_{i-1} (если таковой имеется) и $h_i = e$ в противном случае. Положим $H_i = \langle H_{i-1}, h_i \rangle$. Тогда ряд подгрупп $H_1 \leqslant H_2 \leqslant \ldots$ на некотором шаге n обрывается. Следовательно, элементы $h_1, \ldots, h_n$ порождают H.

Обратно, пусть любая подгруппа из G кончно порождена. Предположим, что некоторый ряд $H_1 < H_2 < \ldots$ не стабилизируется. Ясно, что $\cup_i H_i = H$ — подгруппа группы G. Поскольку подгруппа H конечно порождена, существует последовательность $h_1, \ldots, h_n$, порождающая H. Поскольку каждый из h_i лежит в некоторой подгруппе H_j. Возьмем такой номер m, что все h_i лежат в H_m. Но тогда $H = H_m$, противоречие. ⊠

Предложение 3.3.1.3. *[1, упражнение 24.1.2] Условия* min *и* max *сохраняются при переходе к подгруппам, гомоморфным образам и расширениям.*

Доказательство. Утверждение предложения для условия max легко следует из предыдущего предложения.

Докажем теперь утверждение для условия min. Сохранение условия min для подгрупп и гомоморфных образов очевидны. Пусть $H_1 \geqslant H_2 \geqslant \ldots$ — некоторый ряд подгрупп группы G, которая содержит нормальную подгруппу H такую, что группы H и G/H удовлетворяют условию min. Тогда $H_1H/H \geqslant H_2H/H \geqslant \ldots$ — убывающий ряд группы G/H, поэтому на некотором шаге n он стабилизируется. Таким образом, ряд $H_n \geqslant H_{n+1} \geqslant \ldots$ лежит в H и, следовательно, на некотором шаге m стабилизируется. Таким образом, ряд $H_1 \geqslant H_2 \geqslant \ldots$ на $m + n$-ом шаге стабилизируется. ⊠

Определение 3.3.1.4. [1, пример 24.1.3] Назовем *черниковской группой* расширение прямого произведения конечного числа квазициклических групп (вообще говоря, по различным простым числам) при помощи конечной группы. Всякая черниковская группа удовлетворяет условию min. Всякая почти полициклическая группа удовлетворяет условию max.

Теорема 3.3.1.5. (С. Н. Черников). *[1, теорема 24.1.4] Всякая разрешимая группа G с условием минимальности является черниковской.*

Доказательство. Ввиду условия минимальности группа G содержит подгруппу H конечного индекса, не содержащую других подгрупп конечного индекса. Так как пересечение двух подгрупп конечного индекса само имеет конечный индекс, то H единственна, а потому нормальна. Если H абелева, то для всякого простого числа p группа $H/H^p \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots$ конечна (т. к. в противном случае получим противоречие с условием минимальности), а потому $H = H^p$, т. е. H — полная абелева группа. По теореме 1.2.4.1 она разлагается в прямое произведение квазициклических групп. Ввиду условия минимальности их число конечно. Тем самым для абелевой группы H теорема доказана.

Пусть теперь G бесконечна и неабелева. Возьмем в H неединичную абелеву нормальную подгруппу A (например, последний неединичный коммутант). Покажем, что A лежит в центре группы H. В самом деле, A — абелева группа с условием минимальности, а потому по предыдущему содержит лишь конечное число элементов любого заданного порядка. Значит, каждый элемент a из A имеет в H лишь конечное число сопряженных элементов, откуда $|H : C_H(a)| < \infty$. Так как H не содержит подгрупп конечного индекса, то $C_H(a) = H$ и $A \leqslant Z(H)$.

Покажем теперь, что подгруппа H нильпотентна. Мы сделаем это индукцией по ее ступени разрешимости k. Так как, по предыдущему, $H^{(k-1)} \leqslant Z(H)$, то $H/Z(H)$ разрешима ступени $\leqslant k-1$. По индуктивному предположению, примененному к группе $G/Z(H)$, группа $H/Z(H)$ нильпотентна, а потому и сама группа H нильпотентна.

Покажем, наконец, что H абелева. Пусть B — максимальная абелева нормальная подгруппа в H. По доказанному ранее, $B \leqslant Z(H)$. Но в нильпотентной группе максимальная абелева подгруппа совпадает со своим централизатором (теорема 2.1.2.5), откуда $B = H$. ⊠

Теорема 3.3.1.6. *[1, теорема 24.1.7] Группа G тогда и только тогда разрешима и удовлетворяет условию* max*, когда она полициклическая.*

Доказательство. Достаточность уже отмечалась. Докажем необходимость. Пусть G удовлетворяет условию max и имеет конечную разрешимую матрешку $1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G$. Так как ее секции G_{i+1}/G_i тоже удовлетворяют условию max (см. 3.3.1.3), то они конечно порождены и, значит, разлагаются в прямые произведения циклических групп (теорема 1.1.3.4). Это позволяет уплотнить данную матрешку до полициклической матрешки. ⊠

Отметим описание абелевых подгрупп с условиями min и max, полученное в ходе доказательств теорем 3.3.1.5 и 3.3.1.6.

Предложение 3.3.1.7. *[1, упражнение 24.1.8] Абелева группа тогда и только тогда удовлетворяет условию* min*, когда она разлагается в прямое произведение конечного числа квазициклических групп и конечных циклических групп.*

Абелева группа тогда и только тогда удовлетворяет условию max*, когда она разлагается в прямое произведения конечного числа циклических групп.*

§2 Перенос с абелевых подгрупп на разрешимую группу

Определение 3.3.2.1. [1, стр. 232] Пусть A — нормальная подгруппа группы G. Будем говорить, что A min-*неприводима* относительно G, если всякая нормальная подгруппа H

группы G, содержащаяся в A и отличная от A, конечна. Двойственным образом, будем говорить, что A max-*неприводима* относительно G, если для всякой нормальной подгруппы H группы G, содержащейся в A и отличной от 1, факторгруппа A/H периодическая.

Лемма 3.3.2.2. *[1, лемма 24.2.1] Пусть $A \trianglelefteq G$, обе группы A, G/A абелевы и A не центральна в G.*

а) Если A min-неприводима относительно G, то существует такая подгруппа X, что $G = XA$ и $|X \cap A| < \infty$.

б) Если A — группа без кручения конечного ранга, max-неприводимая относительно G, то существует такая подгруппа X, что $|G : XA| < \infty$ и $X \cap A = 1$.

Доказательство. Можно сразу считать, что подгруппа A бесконечна — иначе имели бы случай а) и достаточно было бы взять $X = G$. Возьмем в группе G элемент x, для которого $[A, x] \neq 1$, и покажем, что его централизатор $X = C_G(x)$ — искомая подгруппа в обоих случаях. Очевидно, отображение $\theta : a \mapsto [a, x]$ есть эндоморфизм подгруппы A. Более того, он перестановочен со всеми сопряжениями группы G, т. е. $[a, x]^g = [a^g, x]$ для всех $a \in A$, $g \in G$, так как $x^g \equiv x (\mathrm{mod}\ A)$ (см. предложение 2.1.4.4).

а) Поскольку $\mathrm{Ker}\ \theta < A$ и A min-неприводима относительно G, то $\mathrm{Ker}\ \theta$ или, что то же самое, пересечение $X \cap A$ конечно. Тогда образ A^θ бесконечен, откуда, снова ввиду min-неприводимости, $A = A^\theta = [A, x]$. Теперь ясно, что для всякого $g \in G$ существует $a \in A$ с условием $[g, x] = [a, x]$, откуда $ga^{-1} \in X$ и, следовательно, $G = AX$.

б) Так как $\mathrm{Ker}\ \theta < A$, группа $A/\mathrm{Ker}\ \theta \cong A^\theta$ не имеет кручения (очевидно, поскольку $[a^n, x] = [a, x]^n$ и A не имеет кручения), а A max-неприводима относительно G, то $\mathrm{Ker}\ \theta = 1$ или, что то же самое, $X \cap A = 1$. Поскольку для любой абелевой группы G и ее подгруппы A справедливо $\dim G = \dim A + \dim G/A$, факторгруппа A/A^θ конечна; пусть m — ее порядок. Группа G индуцирует в A/A^θ (сопряжениями) группу автоморфизмов, изоморфную группе G/C, где $C = C_G(A/A^\theta)$, поэтому G/C также конечна. Если $c \in C$, то $[c, x^m] \in A^\theta = [A, x]$. Далее $[c^m, x] \equiv [c, x]^m (\mathrm{mod}\ [C, x, C])$, $[C, x, C] \leqslant [A, C] \leqslant [A, x]$, так что $[c^m, x] = [a, x]$ для некоторого $a \in A$. Отсюда $c^m a^{-1} \in X$, $c^m \in XA$. Следовательно, факторгруппа G/XA периодическая, и остается доказать, что она конечно порождена.

Пусть $a_1, \ldots, a_m$ — представители смежных классов группы A по подгруппе $[A, x]$. Для каждого $j = 1, \ldots, m$ выберем в G элемент g_j в условием $a_j = [g_j, x]$, а если такого элемента не существует, то положим $g_j = 1$. Для каждого $g \in G$ имеем $[g, x] = a_i[b_i, x]$ при подходящих i и $b_i \in A$. Следовательно, $[gb_i^{-1}, x] = a_i = [g_i, x]$, откуда, $gb_i^{-1}g_i^{-1} \in X$, $g \in \langle g_1, \ldots, g_m, X, A\rangle$. Теперь ясно, что группа G/XA конечно порождена. ⊠

Теорема 3.3.2.3. (С. Н. Черников). *[1, теорема 24.2.2] Разрешимая группа G, у которой все абелевы подгруппы удовлетворяют условию* min, *является черниковской.*

Доказательство. Индукция по ступени разрешимости группы G. Ясно, что если G удовлетворяет условию min для абелевых подгрупп и A — ее абелева нормальная подгруппа, то достаточно доказать, что факторгруппа G/A тоже удовлетворяет условию min для абелевых подгрупп.

Допустим сначала, что A конечна, и докажем, что каждая абелева подгруппа B/A группы G/A действительно удовлетворяет условию min. Группа $B/C_B(A)$ также конечна (она изоморфна подгруппе из $\mathrm{Aut}\ A$) и, разумеется, $A \leqslant C_B(A)$. Будем считать поэтому, что $[A, B] = 1$, причем A уже не обязательно конечна. Возьмем в B какую-нибудь максимальную абелеву нормальную подгруппу M. Очевидно, $A \leqslant M$, а так как B нильпотентна

($B/Z(B)$ абелева, так как $A \leqslant Z(B)$), то $M = C_B(M)$ (см. 2.1.2.5). Легко видеть, что отображение $\tau : B/M \longrightarrow \mathrm{Hom}(M/A, A)$, определенное правилом $(bM)^\tau : xA \longrightarrow [x, b]$, является вложением. Так как B (и даже вся G) периодическая, а M удовлетворяет условию min, то достаточно убедиться, что периодическая часть группы $\mathrm{Hom}(M/A, A)$ конечна. Ввиду 3.3.1.7 $M/A = P \oplus Q$, где P — полная, Q — конечная группы, поэтому достаточно проверить, что всякий периодический элемент φ из $\mathrm{Hom}(M/A, A)$ действует на P тривиально. Но это действительно так: если бы φ отображал какой-то элемент $x \in P$ не в нуль, то для всякого $n \geqslant 1$ гомоморфизм $n\varphi$ отображал бы элементы множества $\frac{1}{n}x$ также не в нуль.

Пусть теперь группа A бесконечна. Разложив ее в G-допустимую матрешку с примарными секциями, конечными или полными, мы видим, что достаточно изучить случай, когда A — полная абелева p-группа. Докажем, что в этом случае всякая абелева подгруппа B/A группы G/A также удовлетворяет условию min. Так как для $A = 1$ утверждение тривиально, воспользуемся индукцией по рангу группы A. Предположим сначала, что A min-приводима относительно B, т. е. содержит неединичную полную собственную B-допустимую подгруппу H. Так как полная подгруппа абелевой группы выделяется в ней прямым множителем (теорема 1.2.2.3) и ранг конечного прямого произведения квазициклических p-групп равен числу сомножителей, то получаем такую картину: $1 < H < A < B$, причем ранг H меньше ранга A, ранг A/H меньше ранга A. Применяя предположение индукции, делаем вывод, что ранг B/H конечен, откуда ранг B/A конечен. Пусть теперь A min-неприводима относительно B. Можно считать также, что $[A, B] \neq 1$, так как противоположный случай был рассмотрен выше. По лемме 3.3.2.2a) B содержит такую подгруппу X, что $B = XA$ и $|X \cap A| < \infty$. Согласно разобранному выше случаю (когда A конечна) подгруппа X удовлетворяет условию min, а потому B и B/A также ему удовлетворяют. ⊠

Теорема 3.3.2.4. (А. И. Мальцев). *[1, теорема 24.2.3] Разрешимая группа, у которой все абелевы подгруппы удовлетворяют условию* max, *является полициклической.*

Доказательство. Проводится аналогично предыдущему доказательству. Пусть G удовлетворяет условию max для абелевых подгрупп, A — ее абелева нормальная подгруппа; докажем, что группа G/A также удовлетворяет условию max.

Сначала опять допустим, что $[A, B] = 1$ (этим, в частности, охватывается случай, когда A конечна, поскольку тогда B_0 — подгруппа без кручения, является абелевой подгруппой конечного индекса в B). Пусть M, τ имеют тот же смысл, что и в предыдущем доказательстве. Так как M/A и A — конечно порожденные абелевы группы, то таковы и аддитивная группа $\mathrm{Hom}(M/A, A)$ и вложенная в нее группа B/M. Следовательно, B и вместе с ней B/A удовлетворяют условию max.

Переходя к общему случаю, можно считать, что A не имеет кручения, так как ее периодическая часть A_0 конечна и, значит, над A_0 можно подняться, согласно предыдущему. Докажем опять, что всякая абелева подгруппа B/A группы G/A удовлетворяет условию max. Так как при $A = 1$ это тривиально, воспользуемся индукцией по рангу группы A. Предположим сначала, что A max-приводима относительно B, т. е. содержит неединичную B-допустимую подгруппу H с непериодической факторгруппой A/H. Пусть T/H — периодическая часть группы A/H. Так как в конечно порожденных абелевых группах без кручения ранг совпадает с размерностью, а при факторизации размерности складываются, то картина такова: $1 < H < T < A < B$, где ранг H меньше ранга A, T/H конечна и ранг A/T меньше ранга A. Отсюда ранг B/A конечен. Пусть теперь A max-неприводима относительно B. Можно считать, что $[A, B] \neq 1$. Тогда утверждение теоремы немедленно следует из леммы 3.3.2.2б). $\boxtimes$

Отметим, что нами попутно доказана более сильная теорема.

Теорема 3.3.2.5. *[1, теорема 24.2.4] Пусть A — абелева нормальная подгруппа группы G. Если G удовлетворяет условию $\min$ (соответственно $\max$) для абелевых подгрупп, то G/Z также удовлетворяет условию $\min$ (соответственно $\max$) для абелевых подгрупп.*

Предложение 3.3.2.6. *[1, упражнение 24.2.5] Если в разрешимой группе все абелевы подгруппы конечны, то она сама конечна. (Доказательство очевидно.)*

§3 О локально разрешимых группах

Лемма 3.3.3.1. *[1, лемма 24.3.1] Всякая локально конечная p-группа G с условием $\min$ для абелевых подгрупп является разрешимой черниковской.*

Доказательство. а) Ввиду теоремы 3.3.2.3 достаточно доказать, что G разрешима. Так как в неразрешимой группе существуют счетные неразрешимые подгруппы, то можно предполагать, что G счетна и отлична от единицы.

б) Центр $Z(G)$ группы G отличен от единицы. В самом деле, так как G счетна, то ее можно представить в виде объединения возрастающей последовательности конечных подгрупп $1 < G_1 < G_2 < \ldots$. Пусть $Z_i = Z(G_i)$, $i = 1, 2, \ldots$. Так как центра конечной p-группы отличен от единицы, то все $Z_i \neq 1$. Порожденная ими подгруппа $Z = \langle Z_1, Z_2, \ldots \rangle$ абелева, а потому удовлетворяет условию $\min$. Учитывая строение абелевых групп с условием $\min$ (предложение 3.3.1.7), видим, что элементы z из Z с условием $z^p = 1$ составляют конечную подгруппу P. Так как $P \leqslant G_i$ для некоторого i, то $P \cap Z_{j+1} \geqslant P \cap Z_{j+1} \geqslant \ldots$ и, значит, $P \cap Z_j = P \cap Z_{j+1} = \ldots$ для некоторого j. Ясно, что $1 < P \cap Z_j \leqslant Z(G)$.

в) Все гиперцентры группы G разрешимы. Пусть, напротив, α-й гиперцентр $\zeta_\alpha G$ группы G неразрешим, причем α — первое порядковое число с этим свойством. Ясно, что оно предельное и больше нуля. Положим для краткости $L = \zeta_\alpha G$ и выберем в L какую-нибудь максимальную абелеву нормальную подгруппу M. Очевидно, L является ZA-группой, поэтому, ввиду предложения 3.5.1.8, $M = C_L(M)$. Пусть A/M — максимальная абелева нормальная подгруппа группы L/M. По теореме 3.3.2.5 A/M удовлетворяет условию $\min$. Очевидно, M также удовлетворяет этому условию и может быть представлена в виде объединения возрастающей матрешки с элементарными абелевыми секциями S. Пусть $1 = M_1 < M_2 < \ldots$ — такая матрешка. Так как $C_A(M_1) \geqslant C_A(M_2) \geqslant \ldots$, то найдется номер i, для которого $C_A(M_i) = C_A(M_{i+1}) = \ldots = C_A(M) = M$. Группа $A/M \cong A/C_A(M_i)$ вкладывается в $\mathrm{Aut}\ M_i$, а потому конечна. Но тогда и L/M конечна (так как является группой автоморфизмов конечной абелевой группы). Значит, L разрешима.

г) Группа G разрешима. В самом деле, если $\zeta_\beta G < G$, то из теоремы 3.3.2.5 следует, что факторгруппа $G/\zeta_\beta G$ удовлетворяет условию $\min$ для абелевых подгрупп (так как $\zeta_\beta G$ разрешима). Ввиду б) центр этой факторгруппы отличен от единицы, а потому $\zeta_\beta G < \zeta_{\beta+1} G$. Таким образом, последовательность гиперцентров $\{\zeta_\beta G\}$ доходит до всей группы G, а потому, снова ввиду в), G должна быть разрешимой. $\boxtimes$

Лемма 3.3.3.2. *[1, лемма 24.3.2] Пусть G — локально конечная группа, p — простое число, $S = X/Y$ — секция группы G и $S_1 < S_2 < \ldots$ — бесконечная возрастающая* *последовательность конечных p-подгрупп группы S. Тогда в X существует такая возрастающая последовательность конечных p-подгрупп $P_1 < P_2 < \ldots$, что $S_i = P_iY/Y$, $i = 1, 2, \ldots$.*

Доказательство. Возьмем в смежных классах по Y, составляющих (конечную) секцию S_i, по представителю и породим ими подгруппу F_i. Так как G локально конечна, то F_i конечна и, очевидно, $S_i = F_iY/Y$. Можно считать при этом, что $F_1 \leqslant F_2 \leqslant \ldots$. Выберем в каждой подгруппе F_i по силовской p-подгруппе P_1 так, чтобы было $P_1 \leqslant P_2 \leqslant \ldots$. Так как при гомоморфизмах конечных групп силовские подгруппы переходят в силовские, а при факторизации F_i по $F_i \cap Y$ получается p-группа (изоморфная S_i), то $P_i(F_i \cap Y) = F_i$. Теперь ясно, что F_iYP_iY и $P_1 < P_2 < \ldots$. ⊠

Лемма 3.3.3.3. *[1, лемма 24.3.3] Пусть G — локально конечная группа. Если G удовлетворяет условию* min *для абелевых подгрупп, то она не имеет бесконечных элементарных абелевых секций. Если в G все силовские подгруппы конечны, то и в любой ее секции тоже.*

Доказательство. Допустим, что G удовлетворяет условию min для абелевых подгрупп и обладает счетной элементарной абелевой секцией S. Пусть $S_1 < S_2 \ldots$ — возрастающая последовательность конечных подгрупп из S, дающая в объединении S, $P_1 < P_2 < \ldots$ — соответствующая ей в силу предыдущей леммы последовательность p-подгрупп группы G. Так как группа $P \cup P_i$ удовлетворяет условию min для абелевых подгрупп, то она черниковская (лемма 3.3.3.1). Значит, ранги всех P_i ограничены. Это, однако, невозможно, так как ранги групп S_i неограничены. Второе утверждение леммы следует из 3.3.3.2 совсем очевидным образом. ⊠

Теорема 3.3.3.4. (С. Н. Черников). *[1, лемма 24.3.4] Всякая локально разрешимая группа с условием минимальности для абелевых подгрупп является разрешимой черниковской.*

Доказательство. Пусть G — локально разрешимая группа с условием min для абелевых подгрупп. По локальной теореме А. И. Мальцева 3.5.2.2 G обладает некоторой RI-матрешкой. Пусть $\mathcal{M}$ — неуплотняемая RI-матрешка группы G. Очевидно, каждая секция S этой матрешки — периодическая абелева автоморфно простая группа, поэтому S — элементарная абелева группа. По лемме 3.3.3.3 она к тому же конечна.

Пусть R — подгруппа, порожденная в G всеми квазициклическими подгруппами. Так как R не содержит подгрупп конечного индекса, от она стабилизирует матрешку $\mathcal{M}$, т. е. индуцирует в каждой ее секции S единичную группу автоморфизмов. Значит, R обладает центральной матрешкой (см. 3.5.1.6). Так как R локально конечна, то она локально нильпотентна. Ввиду 2.3.1.7 и 3.3.3.1 она черниковская, а так как не содержит собственных подгрупп конечного индекса, то абелева.

Факторгруппа G/R уже не содержит квазициклических подгрупп. В самом деле, допустим, что такая подгруппа H/R существует, т. е. в G найдутся элементы $1 = a_1, a_2, \ldots$ такие, что $H = \langle a_1, a_2, \ldots \rangle \cdot R$ и $a_{i+1}^p \equiv a_i (\mathrm{mod}\ R)$, $i = 1, 2, \ldots$. Группа H, действуя в группе R сопряжениями, индуцирует в ней автоморфизмы. Если хотя бы один из них был бы нетождественным, то взяв элемент из R, который им передвигается, и добавив все элементы из R того же порядка, мы получили бы конечное множество M, на котором H действует нетождественно. Подгруппа $H_0 = C_H(M)$ имеет конечный индекс. Так как $H/H_0 \cong (HR)/(H_0R)$ и H/R не содержит собственных подгрупп конечного индекса, то получаем противоречие. Значит, H поэлементно перестановочна с R. Заметив это, мы заменим сейчас элементы $1 = a+1, a_2, \ldots$ на $1 = b_1, b_2, \ldots$ с условием $b_i \equiv a_i (\mathrm{mod}\ R)$, $b_{i+1} = b_i$, $i = 1, 2 \ldots$. Это можно сделать, так как R — делимая группа. Построенные таким образом элементы $b_1, b_2, \ldots$, очевидно, порождают в G квазициклическую подгруппу, не лежащую в R, что противоречит выбору R.

Так как, по доказанному, группа G/R не содержит квазициклических подгрупп и удовлетворяет условию min для абелевых подгрупп (теореме 3.3.2.5), то все ее абелевы и все ее силовские подгруппы конечны (см. 3.3.1.7 и 3.3.3.1 соответственно). Докажем, что сама G/R конечна.

Итак, пусть G — локально разрешимая группа, у которой все абелевы и все силовские подгруппы конечны. Надо доказать, что G сама конечна. Так как каждая бесконечная группа содержит счетные подгруппы, то достаточно доказать, что G не может быть счетной. Пусть, напротив, она счетна. Так как G локально конечна (см. предложение 3.3.2.6), то ее можно представить в виде объединения возрастающей последовательности конечных подгрупп $G_1 < G_2 < \ldots$.

Так как каждая G_n конечна и разрешима, то она содержит некоторую нормальную элементарную абелеву p_n-подгруппу A_n. Если среди простых чисел $p_1, p_2, \ldots$ имеется лишь конечное число различных, то, переходя к подходящей подпоследовательности, можно считать, что все p_n совпадают с некоторым p. Пусть $A = \langle A_1, A_2, \ldots \rangle = A_1 A_2 \ldots$. Так как силовские подгруппы в G конечны, то A конечна. но тогда среди подгрупп $A_1, A_2, \ldots$ найдется бесконечно много совпадающих, т. е. G обладает конечной нормальной элементарной абелевой подгруппой K_1.

Ввиду 3.3.2.6 и 3.3.3.3 в локально разрешимой группе G/K_1 все абелевы и все силовские подгруппы снова конечны. Повторим проведенное выше рассуждение для G/K_1, взятой вместо группы G. Если при этом в G/K_1 найдется конечная нормальная элементарная абелева подгруппа K_2/K_1, то повторим рассуждение для G/K_2, и т. д. В конце концов мы либо построим в G бесконечную возрастающую последовательность нормальных подгрупп с конечными элементарными абелевыми секциями, либо придем к факторгруппе G/K_{i_0} для которой процесс выделения групп A_n связан с последовательностью простых чисел p_n, содержащей бесконечно много различных членов.

В первом случае рассмотрим группу $K = \cup_i K_i$. Для каждого простого числа p она может иметь лишь конечное число секция K_{i+1}/K_i, порядки которых делятся на p (так как силовские подгруппы в G конечны), а потому множество $\pi(K)$ всех простых делителей порядков элементов из K бесконечно. Далее, для всякого $p \in \pi(K)$ множество элементов из K порядка p конечно, так как все силовские p-подгруппы группы K лежат в некотором K_i. Пусть $p_1 \in \pi(K)$, a_1 — элемент из K порядка p_1 и $C_1 = C_K(a_1)$. Так как $|K : C_1| = |a_1^K| < \infty$, то множество $\pi_1 = \pi(C_1)$ снова бесконечно. Возьмем в π_i элемент $p_2 \neq p_1$ и в C_1 элемент a_2 порядка p_2. Так как подгруппа $C_2 = C_K(a_1, a_2) = C_K(a_1) \cap C_K(a_2)$ имеет в K конечный индекс, то множество $\pi_2 = \pi(C_2)$ бесконечно. Возьмем в π_2 элемент $p_3 \neq p_1, p_2$ и в c_2 элемент a_3 порядка p_3. Продолжая эти рассуждения, получим попарно перестановочные элементы $a_1, a_2, \ldots$ порядков $p_1, p_2, \ldots$ соответственно. Так как порожденная ими абелева подгруппа бесконечна, то первый случай на самом деле не возможен.

Переходя ко второму случаю, будем считать, что уже для самой группы G последовательность $p_1, p_2, \ldots$ содержит бесконечно много различных простых чисел. Более того. можно считать, что уже сами числа $p_1, p_2, \ldots$ различны — иначе мы просто опустили бы те группы G_n, которым отвечают повторяющиеся p_n.

Последовательность групп $A_1, A_2, \ldots$ не может содержать бесконечной подпоследовательности циклических групп. В самом деле, пусть, напротив, $A_{k_1}, A_{k_2}, \ldots$ — такая подпоследовательность. Положим $B_j = \langle A_{k_j}, A_{k_{j+1}}, \ldots \rangle$, $j = 1, 2 \ldots$. Так как группа B_1 обладает нормальной матрешкой $B_1 > B_2 > \ldots$ с циклическими секциями, то ее коммутант B_1' обладает центральной матрешкой (см. 3.5.1.7). Так как группа B_1' локально конечна, то она локально нильпотентна, а потому разлагается в прямое произведение своих силовских подгрупп (см. 2.3.1.7). Но ее силовские подгруппы являются циклическими, поэтому B_1' абелева. Таким образом, группа B_1 разрешима, а потому конечна (см. 3.3.2.6). Это однако, невозможно по самому определению группы B_1.

Итак, среди групп $A_1, A_2, \ldots$ число циклических подгрупп не более, чем конечно; можно считать поэтому, что их нет совсем. Так как A_i и A_j при $i \neq j$ — нециклические элементарные абелевы группы различных периодов, то в произведении A_iA_j существует элемент порядка p_ip_j, а потому в группах A_i и A_j существуют перестановочные элементы a_i и a_j. Рассмотрим всевозможные пары (a_1, a_i), где $a_i \in A_i$, $a_1a_i = a_ia_1$, $i = 1, 2, \ldots$. Так как группа A_1 конечна, то существует неединичный элемент b_1, централизатор которого в G содержит бесконечную подгруппу N_1, не содержащую b_1. Так как N_1 удовлетворяет тем же условиям, что и G, то в N_1 существует неединичный элемент b_2, централизатор которого в G содержит бесконечную подгруппу N_2, не содержащую b_2 и т. д. Очевидно, что элементы $b_1, b_2, \ldots$ попарно перестановочны и порождают бесконечную подгруппу. Противоречие. ⊠

3.4 Разрешимые группы конечного ранга

§1 Перенос с абелевых подгрупп на разрешимую группу

Здесь будет доказана следующая основная теорема.

Теорема 3.4.1.1. (М. И. Каргаполов). *[1, теорема 25.2.1] Всякая разрешимая группа, у которой ранги абелевых подгрупп конечны, сама имеет конечный ранг.*

Для доказательства данной теоремы с помощью индукции по ступени разрешимости достаточно доказать следующую теорему.

Теорема 3.4.1.2. *[1, теорема 25.2.2] Пусть A — абелева нормальная подгруппа группы G. Если ранги абелевых подгрупп группы G конечны, то ранги абелевых подгрупп группы G/A тоже конечны.*

Начнем с лемм.

Лемма 3.4.1.3. *[1, лемма 25.2.3] Пусть A — периодическая абелева нормальная подгруппа группы G. Если A имеет конечный ранг, а G/A содержит свободную абелеву подгруппу счетной степени, то и G содержит свободную абелеву подгруппу счетной степени.*

Доказательство. Пусть $x_1A, x_2A, \ldots$ — счетная база свободной абелевой подгруппы группы G/A и $A_{ij} = \langle x_i, x_j \rangle$. Тогда коммутант A_{ij}' группы A_{ij} порождается всевозможными элементами, сопряженными с коммутатором $[x_i, x_j]$. Так как все они лежат в A, а абелева группа конечного ранга и конечного периода конечна, то A_{ij}' конечен. Тогда индекс его централизатора должен быть конечен, поэтому A_{ij}' централизуется некоторым элементом $x_j^{n_{ij}}$, $n_{ij} > 0$. В частности, $[x_i, x_j^{n_{ij}}, x_j^{n_{ij}}] = 1$, откуда индукцией по m (с использованием коммутаторных соотношений 2.1.4.4) получается, что $[x_i, x_j^{n_{ij}m}] = [x_i, x_j^{n_{ij}}]^m$, $m = 1, 2, \ldots$. В частности, при $m = |A_{ij}'|$ имеем $[x_i, x_j^{n_{ij}m}] = 1$. Положим $m_{ij} = n_{ij}|A_{ij}'|$, $m_1 = 1$, $m_j =$

$m_{1j}m_{2j}\dots m_{j-1,j}$ при $j>1$. Ясно, что $\langle x_1^{m_1}, x_2^{m_2}, \dots\rangle$ — свободная абелева группа счетной степени. ⊠

Лемма 3.4.1.4. *[1, лемма 25.2.4] Локально конечная p-группа, у которой ранги всех абелевых подгрупп конечны, является разрешимой черниковской группой.*

Доказательство. Действительно, для абелевых p-групп условие конечности ранга и условие min совпадают. ⊠

Лемма 3.4.1.5. *[1, лемма 25.2.5] Пусть G — локально конечная группа, у которой ранги абелевых подгрупп конечны, p — простое число. Тогда*

а) ранги p-секций силовских p-подгрупп группы G конечны и ограничены в совокупности,

б) ранги p-секций группы G не превосходят s_p, где s_p — максимум рангов силовских p-подгрупп группы G,

в) $s_p \leqslant \frac{1}{2}(5a_p+1)a_p$, где a_p — максимум рангов абелевых p-подгрупп группы G.

Доказательство. а) По лемме 3.4.1.4 ранги всех силовских p-подгрупп группы G конечны; покажем, что они ограничены в совокупности. Пусть, напротив, существует последовательность конечных p-подгрупп $P_1, P_2, \dots$ неограниченных рангов. Тогда найдется аналогичная последовательность, для которой каждое $Q_i = \langle P_1, \dots, P_i\rangle$ — p-группа. Подправленные таким образом $P_1, P_2, \dots$ порождают p-подгруппу неограниченного ранга, противоречие.

б) Пусть L/M — некоторая p-секция. Пусть P — силовская p-подгруппа группы L. Так как при гомоморфизме $L \longrightarrow L/M$ силовская p-подгруппа отображается на силовскую p-подгруппу, то $L = PM$, откуда ранг $L/M \leqslant$ ранг $P \leqslant s_p$.

в) Пусть P — силовская p-подгруппа группы G ранга s_p. Так как P черниковская (см. 3.4.1.4), то она содержит такую максимальную абелеву нормальную подгруппу M, что P/M — конечная p-группа. Далее, P является ZA-группой (см. доказательство леммы 3.3.3.1), поэтому, ввиду 3.5.1.8, P/M изоморфно вкладывается в Aut M. Группа P/M изоморфно вкладывается в группу автоморфизмов группы M (так как $C_P(M) = M$). Пусть $M = B \oplus C$, где B — конечная, а C — делимая часть группы M. Пусть l' — такое натуральное число, что $B^{p^{l'}} = 1$ и $l = \max(l', 2)$ покажем, что любой p-элемент, централизующий подгруппу $\Omega_l(M)$ централизует M. Действительно, предположим противное. Пусть $h \in P/M$ — некоторый элемент. Поскольку он оставляет на месте все решения уравнения $p^2x = 1$, он представим в виде $e + p^2a$ для некоторой матрицы $a \in GL_n(\mathbb{Z}_{p^\infty})$ (здесь n — ранг группы C). Тогда $(e+p^2a)^m = e + \binom{m}{1}p^2a + \ldots + p^{2m}a^m$ и поскольку $p^2a \neq 1$ (если элемент h действует нетривиально), то для любого m имеем $h^m \neq 1$, что противоречит ограниченности группы P/M. Таким образом, можно считать, что P/M — группа автоморфизмов конечной абелевой группы. Тогда $M = A^{(1)} \oplus A^{(2)} \oplus \ldots \oplus A^{(l)}$, где каждое $A^{(i)}$ — прямая сумма подгрупп, порожденных первообразными элементами порядка p^i (первообразными в том смысле, что в M из них уже не извлекается корень p-ой степени). Тогда P/M вкладывается в прямое произведение групп $GL_{k_1}(\mathbb{Z}_p) \times \ldots \times GL_{k_l}(\mathbb{Z}_{p^l})$, где k_i — количество циклических слагаемых в слагаемом $A^{(i)}$, причем $\sum k_i \leqslant a_p$. Из соображений индукции можно считать, что $P/M \leqslant GL_{a_p}(\mathbb{Z}_{p^l})$. Далее, нетрудно проверить, что ранг силовской p-подгруппы группы $GL_n(\mathbb{Z}_{p^m})$ не превосходит $\frac{1}{2}(5n-1)n$ (и не зависит от m). Это доказательство приведено в примере 25.1.1 из [1] и мы не будем на нем останавливаться. Таким образом, ранг $P/M \leqslant \frac{1}{2}(5a_p-1)a_p$, откуда $s_p \leqslant a_p + \frac{1}{2}(5a_p-1)a_p = \frac{1}{2}(5a_p+1)a_p$. ⊠

Предложение 3.4.1.6. *[1, упражнение 25.2.6] В условиях леммы 3.4.1.5 каждая p-секция группы G — черниковская группа.*

Лемма 3.4.1.7. *[1, лемма 25.2.7] Пусть G — локально конечная группа, A — ее нормальная подгруппа, являющаяся прямым произведением своих силовских подгрупп, а G/A абелева. Если ранги абелевых подгрупп группы G конечны, то G сама имеет конечный ранг.*

Доказательство. а) Можно считать, что силовские подгруппы S_p/A группы G/A по каждому простому числу p конечны. В самом деле, согласно 3.4.1.6 каждая группа S_p/A черниковская, а потому ее ранг совпадает с рангом слоя S_p^*/A, т. е. максимальной подгруппы периода p. Если мы докажем, что ранг группы $G^* = \langle S_p^* | p - \text{простое число}\rangle$ конечен, то это будет означать конечность рангов групп A и G^*/A, а потому и G/A, и, значит всей группы G.

б) Силовские подгруппы группы G (а также любой ее подгруппы) сопряжены. В самом деле, каждая силовская p-подгруппа G_{p_i} группы G должна содержать (единственную) силовскую p-подгруппу A_p группы A. Так как G_{p_1}/A_p конечна, то $G_{p_i} = X_{p_i}A_p$, где X_{p_i} — конечная p-группа. Если Y_{p_i}, Y_{p_j} — силовские p-подгруппы конечной группы $\langle X_{p_i}, X_{p_j}\rangle$, содержащие X_{p_i}, X_{p_j}, соответственно, то $G_{p_i} = Y_{p_i}A_p$, $G_{p_j} = Y_{p_j}A_p$, поэтому по теореме Силова, G_{p_i} и G_{p_j} сопряжены в G.

в) Достаточно доказать, что $G = TA$ для некоторой подгруппы T, являющейся прямым произведением своих силовских подгрупп T_p. Действительно, если H_p — абелева подгруппа наибольшего ранга группы T_p, то все такие H_p порождают абелеву подгруппу (в T), которая должна иметь конечный ранг, скажем, r. По лемме 3.4.1.5в) ранг каждой T_p не превосходит $\frac{1}{2}(5r + 1)r$, а потому ранг T конечен. По тем же соображениям ранг A и, значит, ранг всей группы G также конечен.

г) Построение требуемой группы T.

Пусть $p_1 = 2, p_2 = 3, \ldots$ — последовательность простых чисел, S_i/A — силовская p_i-подгруппа группы G/A. Рассмотрим две последовательности подгрупп $G = N_0 \geqslant N_1 \geqslant \ldots$ и $P_1, P_2, P_2, \ldots$, где P_{i+1} — силовская p_{i+1}-подгруппа группы N_i, $N_{i+1} = N_{N_i}(P_{i+1})$, и покажем, что $G = N_iA$ для всех $i = 0, 1, 2, \ldots$. Для $i = 0$ это тривиально; перейдем от i к $i + 1$. Очевидно, P_{i+1} — силовская p_{i+1}-подгруппа пересечения $N_i \cap S_{i+1}$, нормального в N_i (так как G/A абелева, любая группа S_i нормальна в G), поэтому, по обобщенной лемме Фраттини 3.2.1.4, $N_i = N_{i+1}(N_i \cap S_{i+1})$. Но $N_i \cap S_{i+1} = P_{i+1}(N_i \cap A)$, поскольку секция $(N_i \cap S_{i+1})/(N_i \cap A)$ — конечная абелева p-группа. Отсюда $N_i = N_{i+1}(N_i \cap A)$ и $G = N_iA = N_{i+1}A$.

Согласно 3.4.1.6 группа P_i удовлетворяет условию min, поэтому ряд ее подгрупп $N_1 \cap P_i \geqslant N_2 \cap P_i \geqslant \ldots$ обрывается, т. е. $N_{k(i)} \cap P_i = N_{k(i)+1} \cap P_i = \ldots$ для некоторого $k(i) \geqslant i$; обозначим эти пересечения T_i. Если $k \geqslant k(i)$ и P — произвольная p_i-подгруппа группы N_k, то P нормализует подгруппу P_i (так как $N_k \leqslant N_{k(i)} \leqslant N_i$), поэтому $P \leqslant N_k \cap P_i = T_i$ и, значит, T_i — единственная силовская p_i-подгруппа группы N_k. Отсюда следует, что $[T_i, T_j] = 1$ при $i \neq j$ и, значит, подгруппа $T = \langle T_1, T_2, \ldots\rangle$ — прямое произведение ее силовских подгрупп $T_1, T_2, \ldots$.

Группа T — искомая. В самом деле, осталось убедиться только, что $G = TA$. Так как $G = \langle S_1, S_2, \ldots\rangle A$, то для этого достаточно установить равенство $S_i = T_iA$. Но $S_i = (N_kA) \cap S_i = (N_k \cap S_i)A$, и если $k \geqslant k(i)$, то $N_k \cap S_i = T_i(N_k \cap A)$. Следовательно, $S_i = T_iA$. ⊠

Доказательство. Теоремы 3.4.1.2. Очевидно, достаточно дать доказательство только в двух крайних случаях, когда A — периодическая подгруппа и когда A не имеет кручения, так как в общем случае можно подняться по матрешке $1 \leqslant A_0 \leqslant A$, где A_0 — периодическая часть группы A.

Предположим сначала, что A периодическая, и покажем, что ранги абелевых подгрупп группы G/A конечны. Пусть, напротив, G/A содержит абелеву подгруппу B/A бесконечного ранга. По лемме 3.4.1.7 ее периодическая часть B_0/A должна иметь конечный ранг, а потому группа без кручения B/B_0 должна быть бесконечного ранга. Тогда B/B_0 имеет бесконечную размерность, а потому содержит собственную абелеву подгруппу счетной степени, что противоречит лемме 3.4.1.3.

Теперь разберем второй случай: подгруппа A не имеет кручения. Покажем, что в этом случае всякая абелева подгруппа B/A группы G/A также имеет конечный ранг. Мы будем следовать той схеме и тем обозначениям, какие применялись выше для доказательства теорем 3.3.2.3 и 3.3.2.4.

Предположим, что $[B, A] = 1$. Пусть вновь M — некоторая максимальная абелева нормальная подгруппа. Тогда, согласно этой схеме, достаточно убедиться, что ранг группы $\mathrm{Hom}(M/A, A)$ конечен. Так как M/A и A — абелевы группы конечного ранга, причем A без кручения, то группа $\mathrm{Hom}(M/A, A)$ изоморфна подгруппе аддитивной группы (прямоугольных) матриц над полем $\mathbb{Q}$, а потому действительно имеет конечный ранг.

Можно считать далее, что $[A, B] \neq 1$. Предположим сначала, что A max-приводима относительно B, т. е. содержит неединичную B-допустимую подгруппу H с непериодической факторгруппой A/H. Пусть T/H — периодическая часть группы A/H. Тогда мы вновь можем подняться по матрешке $1 < H \leqslant T < A < B$. Пусть теперь A max-неприводима относительно B. Тогда по лемме 3.3.2.2.б) существует такая подгруппа X, что $|B : XA| < \infty$ и $X \cap A = 1$. Так как подгруппа $X \cong XA/A$ абелева, то она, а потому и подгруппы XA и B имеют конечные ранги. Но тогда и B/A должна иметь конечный ранг. ⊠

3.5 Обобщения разрешимости

§1 Классы Куроша-Черникова

Определение 3.5.1.1. [1, стр. 209] Система $\mathcal{M}$ подгрупп группы G называется *субнормальной матрешкой*, если она

1) содержит 1 и G;

2) линейно упорядочена по вложению, т. е. для всяких A, B из $\mathcal{M}$ либо $A \leqslant B$, либо $B \leqslant A$;

3) замкнута относительно объединений и пересечений, в частности, вместе с каждым $A \neq G$ содержит пересечение $A^\sharp$ всех $H \in \mathcal{M}$ с условием $H > A$ и вместе с каждым $B \neq 1$ содержит объединение $B^\flat$ всех $H \in \mathcal{M}$ с условием $H < B$;

4) удовлетворяет условию $A \trianglelefteq A^\sharp$ для всех $A \in \mathcal{M}$, $A \neq G$.

Факторгруппы $A^\sharp/A$ называются *секциями* субнормальной матрешки $\mathcal{M}$. Говорят, что $\mathcal{M}$ *вполне упорядочена по возрастанию*, если $A^\sharp \neq A$ для всех $A \neq G$, и *вполне упорядочена по убыванию*, если $B^\flat \neq B$ для всех $B \neq 1$. Субнормальная матрешка назвается *нормальной*, если все ее члены нармальны в группе. Если одна субнормальная матрешка содержит другую, то первая называется *уплотнением* второй. Матрешка $\mathcal{M}$ назвается *центральной*, если все ее секции центральны, т. е. $A^\sharp/A \leqslant Z(G/A)$ для всех $A \in \mathcal{M}$, $A \neq G$, или, что равносильно, $[A^\sharp, G] \leqslant A$ для всех $A \in \mathcal{M}$, $A \neq G$. Наконец, субнормальную матрешку называют *разрешимой*, если все ее секции абелевы.

Возникают следующие *классы Куроша-Черникова*:

RN: группа обладает разрешимой субнормальной матрешкой;

RN^*: группа обладает разрешимой субнормальной матрешкой, вполне упорядоченной по возрастанию:

$\overline{RN}$: всякую субнормальную матрешку можно уплотнить до разрешимой субнормальной матрешки;

RI: группа обладает разрешимой нормальной матрешкой;

RI^*: группа обладает разрешимой нормальной матрешкой, вполне упорядоченной по возрастанию;

$\overline{RI}$: всякую нормальную матрешку можно уплотнить до разрешимой нормальной матрешки;

Z: группа обладает центральной матрешкой;

ZA: группа обладает центральной матрешкой, вполне упорядоченной по возрастанию;

ZD: группа обладает центральной матрешкой, вполне упорядоченной по убыванию;

$\overline{Z}$: всякую нормальную матрешку можно уплотнить до центральной матрешки;

$\widetilde{N}$: всякую подгруппу можно включить в субнормальную матрешку;

N: всякую подгруппу можно включить в субнормальную матрешку, вполне упорядоченную по возрастанию.

Сформулируем для дальнейшего использования ряд предложений, доказательство которых тривиально.

Предложение 3.5.1.2. *[1, упражнение 22.1.1] Условие N равносильно нормализаторному условию.*

Предложение 3.5.1.3. *[1, упражнение 22.1.2] Для конечных групп условия RN, RN^*, $\overline{RN}$, RI, RI^*, $\overline{RI}$ равносильны разрешимости, а условия Z, ZA, ZD, $\overline{Z}$, $\widetilde{N}$, N — нильпотентности.*

Предложение 3.5.1.4. *[1, упражнение 22.1.3] Группа тогда и только тогда обладает свойством $\overline{RI}$ (соответственно $\overline{Z}$), когда все ее гомоморфные образы обладают свойством RI (соответственно Z).*

Предложение 3.5.1.5. *[1, упражнение 22.1.4] Свойства RN^*, RI^*, ZA, $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\widetilde{N}$, N переносятся на гомоморфные образы.*

Многие свойства разрешимых и нильпотентных групп без труда переносятся (вместе с доказательством) на их обобщения.

Предложение 3.5.1.6. *[1, упражнение 22.1.5] Стабилизатор произвольной нормальной матрешки обладает центральной матрешкой. (см. 2.1.3.1)*

Предложение 3.5.1.7. *[1, упражнение 22.1.6] Коммутант всякой группы, обладающей нормальной матрешкой с циклическими секциями, обладает центральной матрешкой. (см. 3.1.2.2)*

Предложение 3.5.1.8. *[1, упражнение 22.1.7] Во всякой ZA-группе G всякая максимальная нормальная абелева подгруппа совпадает со своим централизатором. (см. 2.1.2.5)*

§2 Локальная теорема

Определение 3.5.2.1. [1, стр. 214] Система M_i, $i \in I$, подмножеств множества M называется его *локальным покрытием*, если любой элемент из M содержится в некотором M_i и любые два множества M_i, M_j содержатся в некотором третьем множестве M_k.

Говорят, что *группа G локально обладает свойством σ*, если существует локальное покрытие, состоящее из конечно порожденных подгрупп со свойством σ.

Говорят, что для свойства групп (и соответствующего класса групп) справедлива *локальная теорема*, если всякая группа, локально обладающая этим свойством, сама обладает им. Так локальная теорема справедлива в классе абелевых групп и не справедлива в классе конечных групп.

Теорема 3.5.2.2. (А. И. Мальцев). *[1, теорема 22.3.1] Для свойств RN, Z, $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\widetilde{N}$ справедлива локальная теорема.*

Доказательство. Перейдем от языка субнормальных матрешек к языку предикатов. Для этого с каждой субнормальной матрешкой $\mathcal{M}$ подгрупп группы G свяжем предикат P на G, полагая $P(x, y) =$ И тогда и только тогда, когда в матрешке $\mathcal{M}$ существует подгруппа, содержащая x и не содержащая y. Ясно, что P удовлетворяет следующим универсальным аксиомам (кванторы опущены):

1) $\neg P(x, x)$,
2) $P(x, y) \wedge P(y, z) \longrightarrow P(x, z)$,
3) $P(x, z) \wedge \neg P(y, z) \longrightarrow P(x, y)$,
4) $P(x, z) \wedge P(y, z) \longrightarrow P(xy^{-1}, z)$,
5) $x \neq 1 \longrightarrow P(1, x)$,
6) $P(x, y) \longrightarrow P(y^{-1}xy, y)$.

Обозначим $A_y = \{x | x \in G, P(x, y) = \text{И}\}, y \neq 1$. Нетрудно проверить, что $A_y = \cup_{y \notin A \in \mathcal{M}} A$, $A = \cap_{y \notin A} A_y$ $(A \in \mathcal{M}, A \neq G)$, т. е. $A_y \in \mathcal{M}$ и каждое $A \in \mathcal{M}$, $A \neq G$, представимо в виде пересечения подгрупп A_y.

Обратно, пусть на G задан предикат P со свойствами 1)–6). Множества A_y составляют систему подгрупп линейно упорядоченную по вложению. Если мы добавим к этой системе G, а также объединения и пересечения любых подсистем, то получится субнормальная матрешка подгрупп в группе G. Из 1)–3) легко следует, что указанные переходы от $\mathcal{M}$ и от P к $\mathcal{M}$ взаимно обратны, а потому осуществляют искомый перевод на язык ИП.

Основные понятия теории классов Куроша-Черникова после перевода на язык ИП будут выглядеть так:

7) разрешимость матрешки: $x \neq 1 \wedge \neg P(x, y) \wedge \neg P(y, x) \longrightarrow P([x, y], x)$,
8) нормальность матрешки: $P(x, y) \longrightarrow P(z^{-1}xz, y)$,
9) центральность матрешки: $x \neq 1 \longrightarrow P([x, y], x)$.

Охарактеризуем еще трехчленные матрешки $1 \leqslant A \leqslant G$ на языке ИП. Очевидно, для этого к аксиомам 1)–6) надо добавить аксиому

10) трехчленность матрешки: $x \neq 1 \wedge P(x, y) \longrightarrow \neg P(y, z)$.

Свойства RN, RI, Z записываются теперь формулами

RN: $(\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (7)$,

RI: $(\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (7) \wedge (8))$,

Z: $(\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (9))$,

а свойства $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\widetilde{N}$, говорящие об уплотняемости, записываются формулами

$\overline{RN}$: $(\forall P)((P$ — субн.$) \longrightarrow (\exists Q)((Q$ — разр. субн.$) \wedge (\forall u))(\forall v)(P(u,v) \longrightarrow Q(u,v))))$,
$\overline{RI}$: $(\forall P)((P$ — норм.$) \longrightarrow (\exists Q)((Q$ — центр.$) \wedge (\forall u)(\forall v)(P(u,v) \longrightarrow Q(u,v))))$,
$\overline{Z}$: $(\forall P)((P$ — норм.$) \longrightarrow (\exists Q)((Q$ — центр.$) \wedge (\forall u)(\forall v)(P(u,v) \longrightarrow Q(u,v))))$,
$\widetilde{N}$: $(\forall P)((P$ — трехчл.$) \longrightarrow (\exists Q)((Q$ — субн.$) \wedge (\forall u)(\forall v)(P(u,v) \longrightarrow Q(u,v))))$,

где сокращенные записи должны быть заменены очевидными комбинациями формул 1)–10). Поскольку все семь свойств оказались квазиуниверсальными, остается сослаться на локальную теорему Мальцева из логики. $\boxtimes$

Глава 4

Конечные и периодические группы

4.1 Группы подстановок

§1 Циклы

Все результаты данного параграфа хорошо известны и мы приведем их без доказательства для дальнейших ссылок.

Теорема 4.1.1.1. *[7, теорема 5.1.1] Пусть π — произвольная подстановка элементов некоторого множества S. Множество S можно разбить на такие непересекающиеся подмножества (орбиты), что π индуцирует цикл на каждом из них.*

Теорема 4.1.1.2. *[7, теорема 5.1.2] Порядок подстановки π равен наименьшему общему кратному длин ее циклов.*

Теорема 4.1.1.3. *[7, теорема 5.1.3] Две подстановки сопряжены в симметрической группе тогда и только тогда, когда они имеют одинаковое число каждой длины.*

§2 Транзитивность

Теорема 4.1.2.1. *[7, теорема 5.2.1] Пусть G — группа подстановок множества символов $X = \{x_1, \dots, x_n\}$, S — некоторое подмножество множества X. Тогда подстановки из группы G, оставляющие на месте символы из S, образуют подгруппу K. Подстановки, переставляющие между собой символы из S, образуют подгруппу H, которая содержит K в качестве нормального делителя.*

Определение 4.1.2.2. [7, стр. 67] Группа подстановок G элементов $x_1, \dots, x_n$ называется *транзитивной* на подмножестве S множества $\{x_1, \dots, c_n\}$ если $SG = S$ и для любых $x_i, x_j \in S$ существует $\sigma \in G$ такая, что $x_i\sigma = x_j$. Подмножество S называется *областью транзитивности* или *орбитой* группы G.

Теорема 4.1.2.3. *[7, теорема 5.2.2] Для любого элемента x_i множество x_iG является орбитой группы G.*

Теорема 4.1.2.4. *[7, теорема 5.2.3] Пусть S — некоторая орбита группы подстановок G, и $x_1 \in S$. Пусть H — подгруппа группы G, оставляющая на месте x_1. Для каждого $x_i \in S$ выберем такую подстановку $\sigma_i \in G$, что $x_1\sigma_i = x_i$. Тогда $G = H \cup H\sigma_2 \cup \dots \cup H\sigma_i \cup \dots$.*

Следствие 4.1.2.5. *[7, следствие 5.2.1] Если порядок орбиты S группы G равен r, то подгруппа H, оставляющая на месте один элемент, имеет индекс r в G.*

Определение 4.1.2.6. [7, стр. 68] Группа G называется k-кратно транзитивной на множестве S, если она транзитивна на S и если любое упорядоченное множество, состоящее из k различных элементов множества S, может быть переведено в любое другое упорядоченное множество из k различных элементов множества S некоторой подстановкой из группы G.

§3 Представление группы подстановками

Определение 4.1.3.1. [7, стр. 68] Будем называть группу подстановок P *представлением* группы G, если существует гомоморфизм из G в P. Если гомоморфизм является изоморфизмом, то представление называется *точным*.

Определение 4.1.3.2. [7, стр. 69] Группа P_1 подстановок множества S_1 изоморфна как группа подстановок, группе P_2 подстановок множества S_2, если существует изоморфизм $\pi_{P_1} \rightleftarrows \pi_{P_2}$ и взаимно однозначное соответствие $x_i \rightleftarrows y_i$ между множествами S_1 и S_2 такое, что $x_i\pi_{P_1} = x_j$ тогда и только тогда, когда $y_i\pi_{P_2} = y_j$. Изоморфные группы подстановок называются *подобными*.

Теорема 4.1.3.3. *[7, теорема 5.3.1] Пусть G — группа и H — ее подгруппа. Тогда имеют место следующие утверждения:*

а) каждому элементу $g \in G$ соответствует следующая подстановка левых смежных классов по H: $\pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$, $x \in G$;

б) отображение $g \longrightarrow \pi(g)$ есть представление группы G транзитивной группой подстановок множества левых смежных классов по подгруппе H, причем $\pi(g)$ оставляет H на месте в том и только в том случае, когда $g \in H$.

Обратно, пусть $g \longrightarrow \pi(g)$ есть представление группы G транзитивной группой подстановок P множества элементов S. Тогда справедливы следующие утверждения:

в) если s_1 — некоторый элемент из S, множество элементов $g \in G$, таких, что подстановки $\pi(g)$ оставляют элемент s_1 на месте, образуют подгруппу H группы G;

г) между элементами множества S и левыми смежными классами по H можно установить взаимно однозначное соответствие так, чтобы группа подстановок P была изоморфна группе подстановок, описанной в первой части теоремы.

Доказательство. Утверждения а), б) и в) очевидны. Утверждение д) легко следует из теоремы 4.1.2.4. ⊠

Определение 4.1.3.4. Точное транзитивное представление группы G называется *регулярным*, если стабилизатор точки тривиален.

Теорема 4.1.3.5. *[7, теорема 5.3.2] Элементы, переходящие при представлении $g \longrightarrow \pi(g)$ (см. теорему 4.1.3.3) в единицу, образуют наибольшую нормальную (в G) подгруппу группы H, а поэтому представление точно тогда и только тогда, когда H не содержит собственных нормальных подгрупп группы G.*

Доказательство. Пусть $Hxg = Hx$ для всех $x \in G$. Тогда $x^{-1}Hxg = x^{-1}Hx$, откуда $g \in \cap_{x\in G} H^x :=$ Kore H. Ясно, что Kore H — наибольшая нормальная подгруппа группы H. ⊠

Следствие 4.1.3.6. *[7, следствие 5.3.1] Единственным точным транзитивным представлением абелевой группы служит регулярное представление.*

Теорема 4.1.3.7. *[7, теорема 5.3.3] Два точных представления группы G подстановками множеств смежных классов группы G по подгруппам H_1 и H_2 подобны в том и только в том случае, когда существует такой автоморфизм α группы G, что $H_1^\alpha = H_2$.*

§4 Интранзитивные группы. Подпрямые произведения

Определение 4.1.4.1. [7, стр.76] Пусть G — группа подстановок, и пусть S_i, $i \in I$ (I — множество индексов) — различные орбиты группы G. Если вместо подстановок группы G рассматривать только подстановки множества S_i, то последние образуют группу G_i. Для любого $i \in I$ элемент $g \in G$ определяет элемент $g_i \in G_i$, а именно, подстановку символов из S_i, индуцируемую элементом g.

Кроме того мы можем положить

$$g = \prod_{i \in I} g_i, \tag{4.1}$$

рассматривая g как элемент декартова произведения групп G_i, так как групповая операция в группе G согласуется с этой же операцией в декартовом произведении $\prod_i G_i$. Таким образом, интранзитивную группу можно рассматривать как подгруппу декартова произведения транзитивных групп. Мы будем говорить, что G есть *подпрямое произведение групп G_i*.

Более точно, некоторая группа G называется *подпрямым произведением групп G_i*, если:

1) G — подгруппа декартова произведения групп G_i;

2) для любого элемента $g_j \in G_j$ существует по меньшей мере один элемент $g \in G$, j-ой компонентой которого является g_j.

Это второе условие требует, чтобы проекция группы G на j-ый множитель была сюръективна.

Теорема 4.1.4.2. *[7, теорема 5.5.1] Пусть G^* — подпрямое произведение групп G_i и G_j, $H_{ij} = G^* \cap G_i \times 1$ и $H_{ji} = G^* \cap 1 \times G_j$. Тогда подгруппа H_{ij} нормальна в G_i, H_{ji} — в G_j, причем существует изоморфизм между факторгруппами $G_i/H_{ij} \cong K \cong G_j/H_{ji}$, такой, что элемент (g_1, g_2), $g_1 \in G_i$, $g_2 \in G_j$ принадлежит подгруппе G^* тогда и только тогда, когда g_1 и g_2 имеют общий образ при гомоморфизмах $G_i \longrightarrow K$, $G_j \longrightarrow K$.*

§5 Примитивные группы

Определение 4.1.5.1. [7, стр. 77] Предположим, $G \neq 1$ — группа подстановок некоторого множества, которое может быть разбито на непересекающиеся подмножества $S_1, \ldots, S_m$ так, что любая подстановка из группы G либо отображает все множество S_i на себя, либо на другое множество S_j. Если такое разбиение можно провести нетривиальным образом, т. е. так, чтобы подмножеств было больше одного и чтобы не все они имели по одному элементу, то группа G называется *импримитивной*, а множества $S_1, \ldots, S_m$ — областями импримитивности. Из определения ясно, что интранзитивная группа тем более импримитивна. Если группа G не импримитивна, то она называется примитивной. Таким образом, примитивная группа есть транзитивная группа, основное множество которой нельзя разбить на собственные подмножества, переводимые одно в другое этой группой подстановок.

Теорема 4.1.5.2. *[7, теорема 5.6.1] Пусть G — транзитивная, но импримитивная группа. Пусть S_1 — одна из областей импримитивности, y_1 — один из элементов множества S_1 и H — стабилизатор точки y_1. Тогда элементы группы G, отображающие S_1 на себя, образуют подгруппу K, причем $H < K < G$. Число областей импримитивности равно индексу $|G : K|$, и каждая область импримитивности состоит из $|K : H|$ элементов. Обратно, если G — транзитивная группа и H — стабилизатор y_1, и если существует подгруппа K, такая, что $G > K > H$, то группа G импримитивна и одна из ее областей импримитивности состоит из $|K : H|$ элементов, в которые подстановки из подгруппы K переводят элемент y_1. Существует $|G : K|$ областей импримитивности, соответствующих левым смежным классам по K. Таким образом, группа подстановок G примитивна тогда и только тогда, когда ее стабилизатор точки является максимальной подгруппой.*

Теорема 4.1.5.3. *[7, теорема 5.6.2] Пусть G — примитивная не циклическая группа подстановок на n символах, H — ее транзитивная подгруппа подстановок на m символах, оставляющая остальные $n - m$ символов на месте. Тогда*

1) если H примитивна, то G $(n - m + 1)$-кратно транзитивна;

2) в любом случае группа G дважды транзитивна.

Доказательство. Докажем сначала второе утверждение. Достаточно доказать, что любой стабилизатор точки действует транзитивно на оставшемся множестве точек. Действительно, пусть H — стабилизатор некоторой точки x_1 и $K = x_2H$ — орбита, порождаемая некоторой точкой x_2 относительно подгруппы H. Предположим, что $K \cap \{x_1\} \neq S$ и рассмотрим подгруппу L группы G, которая оставляет на месте множество K. Она содержит H и ее индекс равен $|S|/|K|$. Таким образом, если K — не одноэлементное множество, то $H \neq L$, откуда, по теореме 4.1.5.2, $L = G$, что противоречит примитивности группы G. Следовательно, K — одноэлементное множество. Тогда группа H тривиальна и, следовательно, группа G циклическая, что противоречит условию теоремы.

Докажем первое утверждение. Ясно, что H транзитивна на m символах. Понятно также, что любая подгруппа, сопряженная с H, также примитивна на m символах и оставляет неподвижными остальные $n - m$ символов. Если бы такие множества для всех сопряженных с H подгрупп либо не пересекались, либо совпадали, то тогда они бы образовывали область импримитивности для группы G. Таким образом, существует такая сопряженная с H подгруппа H', что H действует на множестве $x_1, \dots, x_r, y_1, \dots, y_s$, H' действует на множестве $z_1, \dots, z_r, y_1, \dots, y_s$, $r + s = m$, $0 < r < m$ и число r с таким условием минимально. Покажем, что $r = 1$.

Пусть, напротив, $r > 1$. Поскольку H' примитивна, существует некоторый элемент $h' \in H'$, который u элементов из множества $\{z_1, \dots, z_r\}$ переводит в это же множество, а оставшиеся $r - u$ элементов — в множество $\{y_1, \dots, y_s\}$, причем $0 < u < r$ (так как в противном случае множество $\{z_1, \dots, z_r\}$ было бы областью импримитивности. Рассмотрим группу $H^{h'}$. Эта подгруппа переставляет r элементов вида x (поскольку на этих элементах элемент h действует тривиально), $r - u$ элементов вида z (так как в эти элементы h переводит некоторые из элементов y) и $s - r + u$ элементов вида y (поскольку такое количество элементов h переставляет). Таким образом, эта группа переставляет $s + u$ элементов, которые переставляет также группа H, что противоречит выбору группы H'. Таким образом, группа $\langle H, H' \rangle$ действует на множестве из $m + 1$-ого элемента, она примитивна и стабилизатор точки действует на остальных элементах транзитивно, следовательно она дважды транзитивна. Заменяя теперь группу H на $H_1 = \langle H, H' \rangle$ и повторяя предыдущие рассуждения получаем примитвную группу H_2, которая действует на множестве из $m+2$ элементов и трижды транзитивна. Повторяя этот процесс до тех пор, пока не дойдем до G, которая, следовательно, будет $(n-m+1)$-кратно транзитивной. $\boxtimes$

§6 Кратно-транзитивные группы

Теорема 4.1.6.1. *[7, теорема 5.7.1] Пусть G — t-кратно транзитивная группа степени n. Пусть H — подгруппа, оставляющая на месте t букв, и P — силовская p-подгруппа группы H, которая оставляет на месте $w \geqslant t$ букв. Тогда нормализатор подгруппы P в группе G является t-кратно транзитивной группой на множестве из w букв, инвариантных относительно P.*

Доказательство. Пусть $a_1, \ldots, a_t$ и $b_1, \ldots, b_t$ — упорядоченных множества, в каждом из которых по t букв, причем оба являются подмножествами множества из w букв , причем оба являются подмножествами множества из w букв, инвариантных относительно P. Тогда, так как группа G t-кратно транзитивна, существует элемент x из G, переводящий a_i в b_i при $i = 1, \ldots, t$. Тогда $x^{-1}Px$ оставляет на месте $b_1, \ldots, b_t$, а, значит, подгруппы P и $x^{-1}Px$ являются силовскими подгруппами группы G, оставляющими на месте $b_1, \ldots, b_t$. Тогда эти подгруппы сопряжены в группе, относительно которой множество $\{b_1, \ldots, b_t\}$ поэлементно инвариантно. Поэтому для некоторой подстановки y, оставляющей на месте $b_1, \ldots, b_t$ имеет место равенство $(P^x)^y = P$. Если $z = xy$, то $P^z = P$, причем подстановка z переводит элементы $a_1, \ldots, a_t$ в элементы $b_1, \ldots, b_t$. Значит, в нормализаторе подгруппы существует элемент, отображающий любое упорядоченное подмножество, состоящее из t букв множества из w букв, оставляемых на месте подгруппой P, на любое другое упорядоченное подмножество того же самого множества из w букв. $\boxtimes$

Теорема 4.1.6.2. *[7, теорема 5.7.2] Для целого числа n вида $n = kp+r$, где p — простое число, $p > k$, $r > k$, группа подстановок степени n, за исключением случая $k = 1$ и $r = 2$, не может быть $(r+1)$-кратно транзитивной, если только она не совпадает с группами S_n и A_n.*

Доказательство. Предположим, что группа G степени n $(r+1)$-кратно транзитивна. Подгруппа H, оставляющая на месте первые r букв $1, 2, \ldots, r$, транзитивна тогда на остальных kp буквах. Поэтому порядок группы H делится на p, а сама она содержит нетривиальную силовскую p-подгруппу P. Стабилизатор точки группы H имеет индекс kp в группе H, а поэтому его порядок не делится на высшую степень числа p, которая делит порядок группы H. Следовательно, подгруппа P должна переставлять каждый из kp символов, на которых подгруппа H транзитивна. Далее, так как $kp < p^2$, подгруппа P не содержит транзитивной подгруппы степени p^2. Так как число символов в каждой орбите группы P должно делить порядок P, то группа P, рассматриваемая как группа подстановок kp символов, обладает в точности k орбитами, по p символов в каждой. В каждой орбите группа P действует как циклическая группа порядка p. Поэтому P есть подпрямое произведение k циклических групп порядка и степени p каждая. Значит, любой элемент из P имеет порядок p; кроме того P — абелева группа.

Пусть N — нормализатор подгруппы P в G. По теореме 4.1.6.1 нормализатор N действует как симметрическая группа S_r на первых буквах из основного множества букв для группы G. Рассмотрим сначала случай, когда $r \geqslant 5$. Пусть N_1 — подгруппа группы N, являющаяся знакопеременной группой A_r тех же r букв. Группа A_r является простой неабелевой группой. Тогда группа N_1 переставляет орбиты $T_1, \ldots, T_k$, поэтому группа N_1 является подпрямым произведении групп A_r и B, где B — некоторая подгруппа группы S_{kp}. Поскольку группа A_r проста, из теоремы 4.1.4.2 следует, что этот гомоморфный образ является прямым произведением групп A_r и B. Следовательно, группа N_1 содержит некоторый цикл длины 3 (a, b, c). Так как группа G 5-транзитивна $(r \geqslant 5)$, она содержит все циклы длины 3, значит, совпадает либо с A_n, либо с S_n.

Приведенные выше рассуждения существенно используют предположение $r \geqslant 5$. Остается рассмотреть случаи $r = 3$, $k = 1$ или 2; $r = 4$, $k - 1, 2$ или 3. Они рассматриваются простым перебором и ввиду громоздкости мы здесь это доказательство приводить не будем. ⊠

4.2 Мономиальные представления и перемещение

§1 Мономиальные представления

Определение 4.2.1.1. [7, стр. 224] Рассмотрим множество S символов $u_1, \ldots, u_n$, которые разрешается умножать слева на элементы группы H по следующим правилам: $1u_i = u_i$, где 1 — единица группы H, и $h_1(h_2u_i) = (h_1h_2)u_i$. Мономиальной подстановкой M называется отображение вида $u_i \longrightarrow h_{ij}u_j$, $i = 1, \ldots 1, \ldots, n$, $j = j(i)$, где $u_1 \longrightarrow u_j$ — подстановка множества S. Произведение двух отображений M_1 и M_2 определяется как композиция. Если сопоставить отображению $M_1 : u_i \longrightarrow h_{ij}u_j$ матрицу (h_{ij}), в которой i-я строка и j-й столбец состоят из нулей, кроме места (i, j), где стоит элемент h_{ij}, то умножению отображение соответствующих матриц.

В группе M всех мономиальных подстановок отображения $u_i \longrightarrow h_{ii}u_i$ образуют инвариантную подгруппу D, а факторгруппа M/D изоморфна подгруппе симметрической группы степени n. Будем говорить, что группа G мономиальных подстановок *транзитивна*, если соответствующая группа подстановок транзитивна.

Теорема 4.2.1.2. *[7, теорема 14.1] Пусть группа G содержит подгруппу K и $G = K \cup Kx_2 \cup \ldots \cup Kx_n$. Пусть также $K \longrightarrow H$ — гомоморфизм подгруппы K на группу H. Тогда транзитивное мономиальное представление группы G над группой H осуществляется следующим образом: для элемента $g \in G$ пусть $x_ig = k_{ij}x_j$, $i = 1, \ldots, n$, $j = j(i)$, $k_{ij} \in K$; пусть также h_{ij} — образ элемента k_{ij} при гомоморфизме $K \longrightarrow H$, тогда отображение $g^\pi : u_i \longrightarrow h_{ij}u_j$ является транзитивным мономиальным представлением группы G над группой H. Обратно, любое транзитивное мономиальное представление есть или представление подобного типа, или сопряженное такому представлению относительно группы D.*

Доказательство. Доказательство проводится аналогично соответствующей теореме о транзитивном подстановочном представлении. ⊠

§2 Перемещение

Пусть имеем мономиальное представление R группы G над группой H

$$\varphi g : u_i \longrightarrow h_{ij}u_j, \ i = 1, \ldots, n, j = j(i), \tag{4.2}$$

где число n конечно. Тогда, как легко заметить, отображение

$$g \longrightarrow \prod_{i=1}^{n} h_{ij} (\mathrm{mod}\ H') \tag{4.3}$$

является гомоморфизмом группы G в факторгруппу H/H', где H' — коммутант группы H. Рассмотрим частный случай, когда $H = K$:

$$G = K \cup Kx_2 \cup \ldots \cup Kx_n. \tag{4.4}$$

Если $\varphi(z) = x_j$ для $z = kx_j$, $k \in K$, то

$$V_{G \longrightarrow K}(g) \equiv \prod_{i=1}^{n} x_i g \varphi(x_i g)^{-1} (\mathrm{mod}\ K') \tag{4.5}$$

и отображение $V_{G \longrightarrow K}(g)$ является гомоморфизмом группы G в группу K/K'. Этот гомоморфизм называется *перемещением* группы G в группу K.

Теорема 4.2.2.1. *[7, теорема 14.2.1] 1) Отображение $g \longrightarrow V_{G \longrightarrow K}(g)$ является гомоморфизмом G в факторгруппу K/K'.*

2) Перемещение $V_{G \longrightarrow K}(g)$ не зависит от выбора представителей x_i.

3) Если $G > K > T$, то $V_{G \longrightarrow T}(g) = V_{K \longrightarrow T}[V_{G \longrightarrow K}(g)]$.

Доказательство. Мы докажем все три свойства, исходя прямо из определения перемещения (4.5). Относительно первого свойства заметим, что если $x_i g_i = k_{ij} x_j$ $(i = 1, \ldots, n)$, $x_j g_2 = k_{js} x_s$, $(j = 1, \ldots, n)$, то $V_{g \longrightarrow K}(g_1) \equiv \prod_i k_{ij} (\mathrm{mod}\ K')$, $V_{g \longrightarrow K}(g_2) \equiv \prod_j k_{js} (\mathrm{mod}\ K')$ и $V_{g \longrightarrow K}(g_1 g_2) \equiv \prod_j (k^*_{is}) (\mathrm{mod}\ K')$, где $k^*_{is} = k_{ij} k_{js}$.

Докажем второе свойство. Пусть представители смежных классов первой и второй систем связаны соотношением $x^*_i = a_i x_i$ и $x_i g k_{ij} x_j$. Тогда $x^*_i g = a_i x_i g = a_i k_{ij} x_j = a_i k_{ij} a_j^{-1} x^*_j$. При первом выборе представителей $V(g) \equiv \prod_i k_{ij} (\mathrm{mod}\ K')$, а при втором $V(g) \equiv \prod_i (a_i k_{ij} a_j^{-1}) \equiv \prod_i a_i \cdot \prod k_{ij} \cdot \prod a_j^{-1} \equiv \prod_i k_{ij} (\mathrm{mod}\ K')$.

Установим, наконец, третье свойство. Пусть $G = K \cup Kx_2 \cup \ldots \cup Kx_n$, $K = T \cup Ty_2 \cup \ldots \cup Ty_m$. Тогда $G = T \cup Ty_2 \cup \ldots \cup Ty_m \cup \ldots \cup Tx_i \cup Ty_2 x_i \cup \ldots \cup Ty_m x_i \cup \ldots \cup Tx_n \cup Ty_2 x_n \cup \ldots \cup Ty_m x_n$. Пусть теперь для $g \in G$ $x_i g = k_{ij} x_j$ и $y_r k_{ij} = t_{ijrs} y_s$. Таким образом, $y_r x_i g = t_{ijrs} y_s x_j$. Отсюда $V_{G \longrightarrow T}(g) \equiv \prod_{i,r} t_{ijrs} (\mathrm{mod}\ T')$ и $V_{G \longrightarrow K}(g) \equiv \prod_j k_{ij} (\mathrm{mod}\ K')$. Далее, $V_{k \longrightarrow T}(k_{ij}) \equiv \prod_r t_{ijrs} (\mathrm{mod}\ T')$. Следовательно, $V_{G \longrightarrow K}(g) \equiv \prod_i V_{k \longrightarrow T}(k_{ij}) (\mathrm{mod}\ T') \equiv V_{k \longrightarrow T}(\prod_i k_{ij}) (\mathrm{mod}\ T') \equiv V_{k \longrightarrow T}[V_{G \longrightarrow K}(g)]$. ⊠

§3 Теорема Бернсайда

Лемма 4.2.3.1. *[7, лемма 14.3.1] Если два множества K_1 и K_2 инвариантны в силовской подгруппе P группы G и сопряжены в G, то они сопряжены в $N_G(P)$.*

Доказательство. Пусть $x^{-1} K_1 x = K_2$, $x \in G$. Так как множество K_1 инвариантно в P, то множество $K_2 = x^{-1} K_1 x$ инвариантно в $x^{-1} P x = Q$. Таким образом, подгруппы P и Q содержатся в нормализаторе множества K_2 и, следовательно, являясь силовскими подгруппами, сопряжены в $N_G(K_2)$. Итак, $y^{-1} Q y = P$, где y — такой элемент, что $y^{-1} k_2 y = k_2$. Поэтому при $z = xy$ имеем $z^{-1} P z = P$, $z^{-1} K_1 z = K_2$. ⊠

Теорема 4.2.3.2. *[7, теорема 14.3.1] Если силовская подгруппа P конечной группы G содержится в центре своего нормализатора, то группа G обладает таким нормальным делителем H, что в качестве представителей смежных классов по H можно выбрать элементы группы P.*

Доказательство. Так как подгруппа P содержится в центре нормализатора $N_G(P)$, P — абелева группа и $P' = 1$. Рассмотрим перемещение $V_{G\longrightarrow P}$. Пусть $u \in P$, вычислим $V_{G\longrightarrow P}(u)$. Для этого возьмем в качестве представителей смежных классов по P элементы вида $x_i, x_iu, \ldots, x_iu^{r-1}$, где $x_iu^r \in Px_i$ и $x_iu^j \notin Px_i$ при $j < r$. При этом $x_iu^{j-1} \cdot u\varphi(x_iu^j)^{-1} = x_iu^{j-1} \cdot u(x_iu)^{-1} = x_iu^ju^{-j}x_i^{-1} = 1$ для $j < r$ и $x_iu^{r-1} \cdot u\varphi(x_iu^r)^{-1} = x_iu^rx_i^{-1}$. Следовательно, для каждого цикла длины r в представлении элемента u подстановкой множества левых смежных классов по P в произведении для перемещения $V_{G\longrightarrow P}(u)$ встречается член $x_iu^rx_i^{-1}$, а остальные члены (из этого же произведения)раны единице. Таким образом, $V_{G\longrightarrow P}(u) = \prod_i x_iu^rx_i^{-1}$. Далее, элемент $x_iu^rx_i^{-1} \in P$ сопряжен с u^r в группе G, а так как P — абелева группа, оба элемента инвариантны в P. Для некоторого $y \in N_G(P)$, по лемме 4.2.3.1, $x_iu^rx_i^{-1} = y^{-1}u^ry$. По условию, подгруппа P содержится в центре своего нормализатора, откуда $y^{-1}u^ry = u^r$. Следовательно, $V_{G\longrightarrow P}(u) \equiv \prod u^r \equiv u^n$, где $n = |G : P|$ — сумма длин всех циклов. Поскольку P — силовская подгруппа порядка, скажем, p^s, отсюда ясно, что $P \not| n = |G : P|$. Таким образом, при перемещении G на подгруппу P последняя изоморфно отображается на себя и $V_{G\longrightarrow P}(G) = P$, так как, очевидно, $V_{G\longrightarrow P}(G)$ содержится в P. Ядром этого гомоморфизма является искомая группа H индекса p^s в группе G и порядка $n = |G : P|$. ⊠

§4 Теоремы Ф. Холла, Грюна и Виландта

Определение 4.2.4.1. [7, стр. 229] Пусть H — подгруппа группы G, а B — подгруппа группы H. Будем говорить, что подгруппа B *сильно замкнута* в H (по отношению к G), если $H \cap B^x \leqslant B$, где x — любой элемент из G, и *слабо замкнута* в H, если из включения $B^x \leqslant H$ следует, что $b^x = B$

Говорят, что группа G *p-нормальна*, если центр Z силовской p-подгруппы P является центром любой другой силовской p-подгруппы P_1, которая его содержит.

В дальнейшем мы будем иногда писать $V(g)$ вместо $V_{G\longrightarrow H}(g)$. Если $G = H \cup Hx_2 \cup \ldots \cup Hx_n$, то $V(g) \equiv \prod_{i=1}^{n} x_ig\varphi(x_ig)^{-1} (\mathrm{mod}\ H')$.

Для элемента $g \in G$ и чисел $i = 1, \ldots, n$ определяем числа i_g из условия $x_igx_{i_g}^{-1} \in H$. Тогда при фиксированном g соответствие $i \longrightarrow i_g$ — подстановка $\pi(g)$ транзитивного представления группы G подстановками левых смежных классов по подгруппе H. Таким образом, имеем $V(g) \equiv \prod_i x_igx_{i_g}^{-1}$. Подстановка $\pi(g)$ разлагается на ряд циклов, включая циклы длины 1, соответствующие буквам, остающимся на месте. Выберем по одному символу из каждого цикла и обозначим множество выбранных символов через $C_H(g)$. Если $i \in C_H(g)$, то пусть r_i — порядок цикла, в котором встречается символ i. Тогда $\sum_{i\in C_H(g)} r_i = n$.

Лемма 4.2.4.2. *[7, лемма 14.4.1] $V(g) \equiv \prod_{i\in C_H(g)} x_ig^{r_i}x_i^{-1}$, где $x_ig^{r_i}x_i^{-1}$ — наименьшая степень элемента $x_igx_i^{-1}$, содержащаяся в подгруппе H.*

Доказательство. Проводится аналогично доказательству теоремы 4.2.3.2. ⊠

Определение 4.2.4.3. [7, стр. 231] Будем называть произведение всех циклов длины один *диагональным сомножителем* $d(g)$ перемещения $V(g)$ и записывать $d(g) \equiv$

$\prod_{i=i_g} x_i g x_i^{-1} (\mathrm{mod}\ H_0)$. Ясно, что это определение не зависит ни от порядка сомножителей, ни от выбора представителей x_i.

Лемма 4.2.4.4. *[7, лемма 14.4.2] Если u и v — сопряженные элементы группы G, то $d(u) = d(v)$ и $d(u^{-1}) = [d(u)]^{-1}$.*

Доказательство. Пусть $v = t^{-1}ut$. Тогда равенство $i_u = i$ равносильно равенству $i_{tv} = i_t$, откуда, по определению, $d(v) \equiv \prod_{i=i_u} x_{i_t} v x_{i_t}^{-1} \equiv \prod_{i=i_u} (x_{i_t} t^{-1} x_i^{-1})(x_i u x_i^{-1})(x_i t x_{i_t}^{-1}) \equiv \prod_{i=i_u} (x_i u x_i^{-1}) \equiv d(u)$. Кроме этого, равенство $i = i_u$ равносильно равенству $i = i_{u^{-1}}$, откуда следует второе утверждение леммы. $\boxtimes$

Для элемента $h \in H$ определим функцию $D^*(h) \equiv h^{-1}d(h)$. Тогда, по лемме 4.2.4.4, $h \equiv d(h)[d^*(h)]^{-1} \equiv d(h)d^*(h^{-1})$ и $d(h^r) \equiv d(x_i h^r x_i^{-1})$, и поэтому, если $x_i h^r x_i^{-1} \in H$, имеем $x_i h^r x_i^{-1} \equiv d(h^r)d^*(x_i h^{-r} x_i^{-1}) \equiv h^r d^*(h^r) d^*(x_i h^{-r} x_i^{-1})$; и, наконец, применяя лемму 4.2.4.2, получаем лемму.

Лемма 4.2.4.5. *[7, лемма 14.4.3] Если $h \in H$, то $V(h) \equiv h^n \prod_{i \in C_H(h)} d^*(h^{r_i}) d^*(x_i h^{-r_i} x_i^{-1})$.*

Заметим, что сравнение по модулю H' можно заменить сравнением по произвольной группе H_0, содержащей H'. Тогда получаем следующее следствие.

Следствие 4.2.4.6. *[7, следствие 14.4.1] Если $d^*(h) \in H_0$ для всех $h \in H$, то для любого элемента $h \in H$ справедливо равенство $V(h) = h^n$.*

Глава 5

Группы, заданные порождающими и соотношениями

5.1 Свободные группы и многообразия

§1 Определение

Определение 5.1.1.1. [1, стр. 123] Пусть I — множество. Зафиксируем два множества символов $X = \{x_i | i \in I\}$ и $X^{-1} = \{x_i^{-1} | i \in I\}$. *Слово в алфавите* X — это пустая (обозначается 1) или конечная последовательность символов из $X \cup X^{-1}$. Число элементов этой последовательности называется *длиной слова*. Слово назовем *сократимым*, если оно содержит соседние символы вида $x_i^{\varepsilon} x_i^{-\varepsilon}$, $\varepsilon = \pm 1$. Будем говорить, что два слова u и v *эквивалентны* (в символах: $u \sim v$), если v можно получить из u через конечное число вставок и сокращений слов вида $x_i^{\varepsilon} x_i^{-\varepsilon}$. Ясно, что отношение $\sim$ симметрично, рефлексивно и транзитивно. Все слова, эквивалентные u, образуют класс эквивалентных слов, который мы обозначим через $[u]$.

Теорема 5.1.1.2. *[1, теорема 14.1.1] Пусть $X = \{x_i | i \in I\}$. На множестве $\mathbf{F}(X)$ классов эквивалентных слов в алфавите $X \cup X^{-1}$ определим умножение, полагая $[u][v] = [uv]$. Это определение не зависит от случайного выбора представителей в классах. Множество $\mathbf{F}(X)$ является группой относительно этого умножения.*

Доказательство. Тривиально. ⊠

Определение 5.1.1.3. [1, стр. 127] Группа $\mathbf{F}(X)$ называется *свободной группой со свободным порождающим множеством* X, а мощность множества X называется *степенью (свободы)*.

Теорема 5.1.1.4. *[1, теорема 14.1.5] Пусть группа G порождается множеством $M = \{g_i | i \in I\}$. Возьмем алфавит $X = \{x_i | i \in I\}$. Отображение $X \longrightarrow M$ по правилу $x_i \mapsto g_i$ единственным образом продолжается до гомоморфизма $\mathbf{F}(X) \longrightarrow G$.*

Доказательство. Тривиально. ⊠

Определение 5.1.1.5. [1, стр. 128] Элементы ядра H гомоморфизма $\mathbf{F}(X) \longrightarrow G$ называются *соотношениями* группы G в алфавите X. Если множество H' соотношений таково, что его нормальное замыкание совпадает с H, то H' называется *определяющим множеством соотношений в алфавите* X. Так как $G \cong \mathbf{F}(X)/H$, то задание алфавита X и множества H' полностью определяет группу G. Пара X, H' называется *генетическим кодом* или, короче, *генетикой* группы G; символическая запись $G = \langle X || H' \rangle$. Конечно, одна и та же группа допускает много различных генетических кодов. Особый интерес представляют группы, допускающие конечную генетику, они называются *конечно определенными.*

Если $\varphi : X \longrightarrow Y$ — отображение множеств, w — слово в алфавите X, т. е. $w = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$, $x_i \in X$, $\varepsilon_i = \pm 1$, то через w^φ условимся обозначать такое же слово от образов элементов $x \in X$ относительно φ, т. е. $w^\varphi = (x_1^\varphi)^{\varepsilon_1} \dots (x_n^\varphi)^{\varepsilon_n}$.

Теорема 5.1.1.6. *[1, теорема 14.1.12] Пусть G — группа, N — ее нормальная подгруппа, $N = \langle A || R \rangle$, $G/N = \langle B || S \rangle$, причем пересечение $A \cap B$ пусто. Пусть $\alpha : A \longrightarrow N$, $\beta : B \longrightarrow G/N$ — естественные отображения, соответствующие данным генетическим кодам, $\tau : G/N \longrightarrow G$ — какой нибудь выбор представителей в смежных классах. Подберем для каждого $s \in S$ слово t_s и для каждых $a \in A$, $b \in B$, $\varepsilon = \pm 1$ слово $u_{a,b,s}$ в алфавите A так, чтобы было $s^{\beta\tau} = t_s^\alpha$ и $(b^{\beta\tau})^{-\varepsilon} a^\alpha (b^{\beta\tau})^\varepsilon = u_{a,b,s}^\varepsilon$ (имеются в виду равенства в группе G). Тогда $G = \langle A \cup B || R \cup T \cup U \rangle$, где $T = \{s t_s^{-1} | s \in S\}$, $U = \{b^{-\varepsilon} a b^\varepsilon u_{a,b,s}^{-1} | a \in A, b \in B, \varepsilon - \pm 1\}$.*

Доказательство. Если g — элемент группы G, то $Ng = w^g$, где w — подходящее слово в алфавите B. Так как g и $w^{\beta\tau}$, принадлежат одному смежному классу по N, то $g = v^\alpha w^{\beta\tau}$, где v — подходящее слово в алфавите A. Таким образом, группа G порождается множеством $A^\alpha \cup B^{\beta\tau}$, и отображение $A \cup B \longrightarrow G$, действующее на множестве A как α, а на множестве B как $\beta\tau$ единственным образом продолжается до гомоморфизма $\gamma : \mathbf{F}(A \cup B) \longrightarrow G$, где $\mathbf{F}(X)$ обозначает свободную группу с базой X. Остается проверить, что $\operatorname{Ker} \gamma = R^* T^* U^*$, где R^*, T^*, U^* — нормальные замыкания в группе $\mathbf{F}(A \cup B)$ множеств R, T, U соответственно.

Ясно, что $R \cup T \cup U \subseteq \operatorname{Ker} \gamma$, поэтому $R^* T^* U^* \leqslant \operatorname{Ker} \gamma$.

Для доказательства противоположного включения возьмем в $\ker \gamma$ произвольный элемент $f = v_1 w_1 \dots v_k w_k$, где v_i — слова в алфавите A, w_i — слова в алфавите B, причем v_1 и w_k могут быть пустыми (понятно, что любой элемент из $\mathbf{F} A \cup B$ записывается в таком виде).

Докажем сначала индукцией по k, что $f \equiv vw (\operatorname{mod} U^*)$, где u, w — подходящие слова в алфавитах A, B соответственно. При $k = 1$ утверждение тривиально; перейдем от $k-1$ к k. Запишем f в виде $f = v_1 w_1 \dots (w_{k-1} v_k w_{k-1}^{-1}) w_{k-1} w_k$. Используя соотношения из U, слово в алфавите A — это легко доказать индукцией по длине слова w_{k-1}. Следовательно, $f \equiv v_1 w_1 \dots \overline{v_{k-1}} \overline{w_{k-1}} (\operatorname{mod} U^*)$, где $\overline{v_{k-1}}, \overline{w_{k-1}}$ — слова в алфавитах A, B соответственно, и остается сослаться на основное индуктивное предположение.

По условию, $f^\gamma = 1$, поэтому $v^\alpha w^{\beta\tau} = 1$ в группе G. Тогда $w^\beta = 1$ в факторгруппе G/N, и слово w является элементом нормального замыкания множества S в $\mathbf{F}(B)$. Записывая его как слово от элементов вида $r^{-1} s t_s^{-1} t_s r$, $s \in S$, $r \in \mathbf{F}(B)$, и используя соотношения из T, получим $w \equiv w' (\operatorname{mod} T^*)$, где w' — слово от элементов вида $r^{-1} t_s r$. В силу соотношений из U получаем $w' \equiv w'' (\operatorname{mod} U^*)$, где w'' — некоторое слово в алфавите A. Таким образом, $f \equiv f_0 (\operatorname{mod} T^* U^*)$, где $f_0 = v w'' \in \mathbf{F}(A)$. Так как $1 = f^\gamma = f_0^\alpha$, то $f_0 \equiv 1 (\operatorname{mod} R^*)$. Окончательно, $f \equiv 1 (\operatorname{mod} R^* T^* U^*)$. ⊠

§2 Матричное представление

Так как группы $\mathbf{F}_1, \mathbf{F}_2, \ldots$ вкладывается в $\mathbf{F}_\infty$, а $\mathbf{F}_\infty$ в $\mathbf{F}_2$, то достаточно найти в $SL_2(\mathbb{Z})$ свободную подгруппу степени 2.

Теорема 5.1.2.1. *[1, теорема 14.2.1] Пусть m — целое число $\geqslant 2$. Подгруппа, порожденная в $SL_2(\mathbb{Z})$ трансвекциями $t_{12}(m) = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, $t_{21}(m) = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$, порождается ими свободно, т. е. описывается пустым множеством соотношений.*

Доказательство. Обозначим для краткости $a = t_{12}(m)$, $b = t_{21}(m)$. Пусть w — чередующееся произведение ненулевых степеней элементов a, b в группе $SL_2(\mathbb{Z})$. Надо показать, что $w \neq e$. Если w начинается со степени b, то можно сопрячь w этой степенью и рассмотреть полученное произведение, которое начинается уже со степени a. Поэтому пусть $w = a^{\alpha_1} b^{\alpha_2} \ldots c^{\alpha_r}$, где $c = a$ или b, все $\alpha_i \neq 0$. Пусть z_i — верхняя строчка матрицы $a^{\alpha_1} b^{\alpha_2} \ldots c^{\alpha_i}$. Если $z_{2k-1} = (x_{2k-1}, x_{2k})$, то $z_{2k} = z_{2k-1} b^{\alpha_{2k}} = (x_{2k+1}, x_{2k})$, $z_{2k+1} = z_{2k} a^{\alpha_{2k+1}} = (x_{2k+1}, x_{2k+2})$, где $x_{2k+1} = x_{2k-1} + m\alpha_{2k} x_{2k}$, $x_{2k+2} = x_{2k} + m\alpha_{2k+1} x_{2k+1}$. Объединяя последние две формулы, получаем $x_{i+2} = x_i + m\alpha_{i+1} x_{i+1}$ для $i = 1, 2, \ldots, r-1$. Нам достаточно доказать, что с ростом i от 1 до $r-1$ числа $|x_i|$ возрастают. Для $i = 1, 2$ $x_1 = 1$, $x_2 = m\alpha_1$ и утверждение очевидно. Дальше ведем индукцию: $|x_{i+2}| \geqslant m|\alpha_{i+1}||x_{i+1}| - |x_i| \geqslant 2|x_{i+1}| - |x_i| \geqslant |x_{i+1}| + 1$. ⊠

Теорема 5.1.2.2. *[1, теорема 14.2.2] Пусть p — простое число. Любая свободная группа $\mathbf{F}(X)$ аппроксимируется конечными p-группами.*

Доказательство. Пусть X' — конечная часть множества X. Посылая остальные свободные порождающие в единицу, мы получим гомоморфизм $\mathbf{F}(X) \longrightarrow \mathbf{F}(X')$. Так как ядро таких гомоморфизмов пересекается по единице, то $\mathbf{F}(X)$ — поддекартово произведение счетных свободных групп. Таким образом, можно считать, что $\mathbf{F}(X)$ счетна, а потому по теореме 5.1.2.1 вложена в группу $SL_2(\mathbb{Z})$. Напомним, что главная конгруэнц-подгруппа $\Gamma_2(p)$ определяется следующим образом $\Gamma_2(m) = \{x | x \in SL_2(\mathbb{Z}), x =\equiv e (\mathrm{mod}\ m)\}$. Таким образом, группа $\mathbf{F}(X)$ вложена в главную конгруэнц-подгруппу $\Gamma_2(p)$ для любого простого p. Будучи ядрами гомоморфизмов $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}_{p^\alpha})$ подгруппы $\Gamma_(p^\alpha)$ — нормальные подгруппы конечных индексов в $SL_2(\mathbb{Z})$ и, очевидно, пересекаются по единице, $k = 1, 2, \ldots$. Поэтому, $\Gamma_2(p)$ — поддекартово произведение конечных групп $\Gamma_2(p)/\Gamma_2(p^k)$. Наконец,

$$(e + pz)^p = \sum_{i=0}^{p} \binom{p}{i} (pz)^i \equiv e (\mathrm{mod}\ p^2),$$

$$(e + p^2 z)^p = \sum_{i=0}^{p} \binom{p}{i} (p^2 z)^i \equiv e (\mathrm{mod}\ p^3),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

поэтому $\Gamma_2(p)/\Gamma_2(p^k)$ есть p-группа. ⊠

§3 Подгруппы

В этом пункте мы изложим метод Шрайера, позволяющий находить систему свободных порождающих для подгруппы свободной группы. В частности, мы докажем, что любая подгруппа свободной группы вновь является свободной группой.

Пусть H — подгруппа произвольной группы G. Зафиксируем в каждом правом смежном классе G по H по представителю. Для подгруппы H выбираем представителем 1. Функция, принимающая на любом правом смежном классе постоянное значение — фиксированный представитель этого класса, — называется (правой) *выбирающей функцией*. Непосредственно проверяется следующие свойства этой функции: $\overline{\overline{u}} = \overline{u}$ и $\overline{\overline{u}v} = \overline{uv}$, где $u, v \in G$, а $\overline{u}$ — фиксированный представитель класса Hu.

Теорема 5.1.3.1. *[1, теорема 14.3.1] Пусть M — порождающее множество группы G, H — ее подгруппа, $u \mapsto \overline{u}$ — функция, выбирающая правые представители G по H, S — множество выбранных представителей. Тогда $H = \langle sx\overline{sx}^{-1} | s \in S, x \in M\rangle$.*

Доказательство. Ясно, что элементы $sx\overline{sx}^{-1}$ содержатся в подгруппе H. Покажем, что любой элемент из H можно записать как произведение элементов $sx\overline{sx}^{-1}$ и элементов, к ним обратных. Непосредственно проверяется, что $(sx\overline{sx}^{-1})^{-1} = s'x^{-1}\overline{s'x^{-1}}^{-1}$, где $s' = \overline{sx}$, причем по s' однозначно восстанавливается $s = \overline{s'x^{-1}}$. Пусть теперь элемент $u = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$, $x_i \in M$, $\varepsilon_i = \pm 1$, взят из H. Мы должны записать его в виде слова от элементов вида $sx\overline{sx}^{-1}$. Обозначим $u_1 = 1$, $u_{i+1} = x_1^{\varepsilon_1} \dots x_i^{\varepsilon_i}$. Тогда искомой записью будет

$$u = \left(\overline{u}_1 x_1^{\varepsilon_1} \overline{u_1 x_1^{\varepsilon_1}}^{-1}\right) \left(\overline{u}_2 x_2^{\varepsilon_2} \overline{u_2 x_2^{\varepsilon_2}}^{-1}\right) \dots \left(\overline{u}_r x_r^{\varepsilon_r} \overline{u_r x_r^{\varepsilon_r}}^{-1}\right). \tag{5.1}$$

Действительно, $\overline{u_i x_i^{\varepsilon_i}}^{-1} \overline{u_{i+1}} = 1$, $i = 1, \dots, r-1$, поэтому правая часть соотношения (5.1) равна $\overline{u}_1 u \overline{u_r x_r^{\varepsilon_r}}^{-1} = 1 \cdot u \overline{u}^{-1} = 1 \cdot u \cdot 1 = u$. ⊠

Определение 5.1.3.2. [1, стр. 137] Множество элементов свободной группы, представимых несократимыми словами, называется *шрайеровым*, если вместе с каждым своим элементом оно содержит все его начальные отрезки.

Теорема 5.1.3.3. (Нильсен–Шрайер). *[1, теорема 14.3.5] Пусть X — произвольный алфавит, H — произвольная подгруппа свободной группы $F = \mathbf{F}(X)$. Существует по крайней мере одна шрайерова система представителей F по H. Если $u \mapsto \overline{u}$ — соответствующая ей выбирающая функция, то H свободно порождается нееденичными элементами $sx\overline{sx}^{-1}$, где s пробегает множество выбранных представителей, а x пробегает X.*

Доказательство. а) Существование шрайеровой системы представителей. Назовем *длиной смежного класса* группы F по подгруппе H длину самого короткого слова в нем. Построим шрайерову систему индукцией по длине класса.

Выберем пустое слово в качестве представителя для H. Если L – класс длины 1, то выберем любое слово длины 1 в качестве представителя этого класса. Пусть в классах длины, меньшей r, представители уже выбраны, т. е. на этих классах уже определена выбирающая функция $u \mapsto \overline{u}$, причем длина представителя совпадает с длиной класса. Пусть L — произвольный класс длины r. Возьмем в нем какое-нибудь слово $y_1 \dots y_r$, $y_i \in X \cup X^{-1}$, и объявим представителем класса L слово $\overline{y_1 \dots y_{r-1}} y_r$. Ясно, что так построенная система представителей шрайерова.

б) Пусть S — шрайерова система представителей F по H, $u \mapsto \overline{u}$ — соответствующая ей выбирающая функция. Покажем, что нееденичные элементы

$$sx\overline{sx}^{-1},\ s \in S,\ x \in X, \tag{5.2}$$

свободно порождают H. Из теоремы 5.1.3.1 мы уже знаем, что они порождают H. Остается доказать, что эти элементы не связаны нетривиальными соотношениями.

Прежде всего, каждое слово (5.2) несократимо. Действительно, сокращения могут начаться только на стыках с буквой x. Но если $s = s_1x^{-1}$, то $sx\overline{sx}^{-1} = s_1\overline{s_1}^{-1} = 1$, а если $\overline{sx}^{-1} = x^{-1}s_2^{-1}$, то $s = s_2$ и $sx\overline{sx}^{-1} = 1$.

Далее, пусть u, v — неединичные слова вида (5.2) или к ним обратные, причем $uv \neq 1$. Из доказательства теоремы 5.1.3.1 мы знаем, что $u = sx^{\varepsilon}\overline{sx^{\varepsilon}}^{-1}$, $v = ty^{\delta}\overline{ty^{\delta}}^{-1}$, $s, t \in S$, $x, y \in X$, $\varepsilon, \delta = \pm 1$. Ввиду несократимости слов u, v процесс сокращений в произведении uv может начаться только на стыке. Он заглохнет, не дойдя до x^{ε} слева и y^{δ} справа. Действительно, ввиду шрайеровости системы представителей, если процесс сокращений захватил бы сначала x^{ε}, то было бы $t \equiv s_1x^{-\varepsilon}w$, где $s_1 \equiv \overline{sx^{\varepsilon}}$, откуда $s_1x^{-\varepsilon}s^{-1} \equiv 1$. Но это невозможно, поскольку $u \neq 1$. Аналогично для y. Наконец, сократиться одновременно $x^{\varepsilon}, y^{\delta}$ также не могут, поскольку $uv \neq 1$.

Пусть теперь дано непустое слово в символах (5.2). Надо доказать, что если рассматривать его как слово в алфавите X и произвести все возможные сокращения, то останется непустое слово. Но действительно, ввиду сказанного выше, сокращения могут начинаться только на стыках слов (5.2) и прекращаются, не доходя до их сердцевин x^{ε}. ⊠

Теорема 5.1.3.4. *[1, теорема 14.3.7] Пусть $F = \mathbf{F}(x_1, \ldots, x_n)$, $H \leqslant F$, $|F : H| = j$. Если n, j — конечные числа, то H имеет степень $m = 1 + (n-1)j$.*

Доказательство. В обозначениях предыдущей теоремы пусть M — множество всех nj записей вида (5.2). Нам надо понять, когда эти записи изображают единицу. С этой целью обозначим через S_0 множество S без единицы и определим отображение $\tau : S_0 \longrightarrow M$, полагая

$$\begin{cases} s'x\overline{s'x}^{-1} \text{ при } s \equiv s'x, \ x \in X, \\ sx\overline{sx}^{-1} \text{ при } s \equiv s'x^{-1}, \ x \in X. \end{cases}$$

Непосредственно проверяется, что τ — взаимно однозначное отображение S_0 на те записи из M, которые отображают единицу. Так как степень H равна числу остальных записей, т. е. $nj - (j-1)$, то все доказано. ⊠

§4 Ряды централов и коммутантов

Теорема 5.1.4.1. (Магнус). *[1, теорема 14.4.4] Во всякой свободной группе F ω-й централ единице.*

Доказательство. а) Пусть сначала F счетна. По теореме 5.1.2.1 она вкладывается в конгруэнц-подгруппу $\Gamma_2(m)$, $m \geqslant 2$, поэтому достаточно убедиться, что ω-й централ группы $\Gamma_2(m)$ равен единице.

Возьмем матрицы $g = e + m^k a \in \Gamma_2(m^k)$ и $f = e + m^l b \in \Gamma_2(m^l)$. Пусть $g^{-1} = e + m^k a'$ и $f^{-1} = e + m^l b'$. Тогда коммутатор $[g, f] = (e + m^k a')(e + m^l b')(e + m^k a)(e + m^l b) = e + (m^k a' + m^k a + m^{2k a' a}) + (m^l b' + m^l b + m^{2l} b' b) + \ldots = e + \ldots$, где точками обозначены смешанные произведения типа $m^{2k+l} a' a b$. Ясно, что любое такое смешанное произведение сравнимо с нулевой матрицей по модулю m^{k+l}, а потому $[g, f] \in \Gamma_2(m^{k+l})$.

Проведенное вычисление показывает, что $[\Gamma_2(m^k), \Gamma_2(m^l) \leqslant \Gamma_2(m^{k+l}$, поэтому $\gamma_i \Gamma_2(m) \leqslant \Gamma_2(m^i)$. Поскольку $\cap_i \Gamma_2(m^i) = e$, то для счетных групп теорема доказана.

б) Пусть теперь F — произвольная свободная группа. Допустим, что ω-й централ F содержит неединичный элемент f. Возьмем для каждого $n = 1, 2, \ldots$ разложение f в произведение простых коммутаторов веса n, соберем все коммутируемые элементы и выразим их через порождающие элементы группы F. Ясно, что при этом будет использовано лишь счетное множество порождающих элементов. Это множество порождает свободную подгруппу. Так как она счетна и не подчиняется теореме Магнуса, то получаем противоречие с а). ⊠

Пусть u — слово в алфавите X. *Логарифмом u по основанию $x \in X$* называется целое число $\log_x u$, равное сумме показателей при букве x в слове u (очевидно, для эквивалентных слов значения логарифма одинаковы). Ясно, что отображение, сопоставляющее каждому u из $\mathbf{F}(X)$ набор его логарифмов $\log_x u$ по всем $x \in X$, является гомоморфизмом свободной группы $\mathbf{F}(X)$ на свободную абелеву группу того же ранга. Так как слова с одинаковыми логарифмами по всем основаниям лежат в одном смежном классе по коммутанту, то коммутант $[\mathbf{F}(X), \mathbf{F}(X)]$ будет к коммутанту свободной группы и т. д., мы получаем следующий результат:

Секции ряда коммутантов свободной группы — свободные абелевы группы.

§5 Тождества и многообразия

Определение 5.1.5.1. [1, стр. 142] Слово v в алфавите $x_1, x_2, \ldots$ называется *тождеством* на классе групп $\mathfrak{L}$, если на любой группе G из $\mathfrak{L}$ оно обращается в единицу, когда аргументы $x_1, x_2, \ldots$ пробегают G. Пусть V — множество слов в алфавите $x_1, x_2, \ldots$ G — группа. В общем случае слова из V не обязаны быть тождественными на G, и их значения на G порождают некоторую подгруппу

$$V(G) = \langle v(g_1, \ldots, g_{n(v)}) | v \in V, g \in G \rangle. \tag{5.3}$$

Эта подгруппа называется *вербальной* (=словесной) в G относительно V и в некотором смысле измеряет отклонение группы G от групп многообразия, определяемого тождествами V.

Подклассы, выделяемые в классе всех групп тождественными соотношениями, называются *многообразиями.*

Теорема 5.1.5.2. *[1, теорема 15.1.4] Пусть $\mathfrak{L}$ — многообразие групп, определяемое тождествами V. Пусть X — алфавит,*

$$\mathbf{F}_V(X) = \mathbf{F}(X)/V(\mathbf{F}(X)), \tag{5.4}$$

$*$ обозначает естественный гомоморфизм $\mathbf{F}(X) \longrightarrow \mathbf{F}_V(X)$. Если $X = \{x_i | i \in I\}$, G — группа из $\mathfrak{L}$ с порождающим множеством $\{g_i | i \in I\}$, то отображение $x_i^* \mapsto g_i$ единственным образом продолжается до гомоморфизма $\mathbf{F}_V(X) \longrightarrow G$. Другими словами, группы $\mathbf{F}_V(X)$ свободны в многообразии $\mathfrak{L}$. Ими исчерпываются все свободные группы из $\mathfrak{L}$.

Доказательство. а) Ясно, что для получения гомоморфизма $\mathbf{F}_V(X) \longrightarrow G$ надо слову от x_i^* сопоставить это же слово от g_i. Корректность и гомоморфность этого отображения проверяются непосредственно. Следовательно, $\mathbf{F}_V(X)$ — свободная группа в $\mathfrak{L}$.

б) Пусть F — свободная группа в $\mathfrak{L}$ со свободными порождающими f_i, $i \in I$. Отображение $f_i \mapsto x_i^*$ продолжается до гомоморфизма $F \longrightarrow \mathbf{F}_V(X)$, а отображение $x_i^* \mapsto f_i$ продолжается до гомоморфизма $\mathbf{F}_V(X) \longrightarrow F$. Отсюда $F \cong \mathbf{F}_V(X)$. ⊠

Определение 5.1.5.3. [1, стр. 144] Множество $\{x_i^* | i \in I\}$ называется *свободным порождающим множеством группы* $\mathbf{F}_V(X)$, а его мощность — *степенью свободы* группы $\mathbf{F}_V(X)$. Свободную группу степени $\mathfrak{n}$ в многообразии $\mathfrak{L}$ обозначают также $\mathbf{F}_\mathfrak{n}(\mathfrak{L})$.

Теорема 5.1.5.4. *[1, теорема 15.1.7] Пусть $\mathfrak{L}$ — многообразие групп, G — группа, свободная в $\mathfrak{L}$. Любая эндоморфно допустимая подгруппа H группы G вербальна.*

Доказательство. Возьмем в G свободно порождающее множество $\{g_i | i \in I\}$ и рассмотрим в $\mathbf{F}_\infty$ множество V слов $v(x_{i_1}, \ldots, x_{i_m}\})$ с условием, что $v(g_{i_1}, \ldots, g_{i_m}) \in H$. Покажем, что $H = V(G)$. Включение $H \leqslant V(G)$ очевидно. Обратно, пусть $v \in V$, $g'_i \in G$. Надо показать, что $v(g'_{i_1}, \ldots, g'_{i_m}) \in H$. Но ввиду свободы G в $\mathfrak{L}$ отображение $g_i \mapsto g'_i$ можно продолжить до гомоморфизма группы G. Так как $v(g_{i_1}, \ldots, g_{i_m}) \in H$ и H эндоморфно допустима, то $v(g'_{i_1}, \ldots, g'_{i_m}) \in H$. ⊠

Определение 5.1.5.5. [1, стр. 145] Два множества V, W называются *эквивалентными*, если они определяют одно и то же многообразие групп, или, что равносильно, если $V(\mathbf{F}_\infty) = W(\mathbf{F}_\infty)$.

§6 Другой подход к многообразиям

Определение 5.1.6.1. [1, стр. 145] Если $\mathfrak{L}$ — класс групп, то пусть $S\mathfrak{L}$, $Q\mathfrak{L}$, $C\mathfrak{L}$ обозначают соответственно замыкания этого класса относительно операций взятия подгрупп, гомоморфных образов и декартовых произведений. Если $\mathfrak{L}$ — многообразие, то, очевидно, $S\mathfrak{L} = \mathfrak{L}$, $Q\mathfrak{L} = \mathfrak{L}$, $C\mathfrak{L} = \mathfrak{L}$.

Теорема 5.1.6.2. (Биркгоф). *[1, теорема 15.2.1] Пусть $\mathfrak{L}$ — класс групп. Если $S\mathfrak{L} = \mathfrak{L}$, $Q\mathfrak{L} = \mathfrak{L}$, $C\mathfrak{L} = \mathfrak{L}$, то $\mathfrak{L}$ — многообразие.*

Доказательство. Пусть V — все тождества, истинные на $\mathfrak{L}$, $\overline{\mathfrak{L}}$ — многообразие, определяемое ими. Очевидно, $\mathfrak{L} \subseteq \overline{\mathfrak{L}}$ и надо убедиться, что $\overline{\mathfrak{L}} \subseteq \mathfrak{L}$. Поскольку $Q\mathfrak{L} = \mathfrak{L}$, то достаточно проверить, что любая группа F, свободная в $\overline{\mathfrak{L}}$, принадлежит $\mathfrak{L}$, а ввиду соотношений $C\mathfrak{L} = \mathfrak{L}$, $S\mathfrak{L} = \mathfrak{L}$ для этого достаточно вложить F в декартово произведение групп из $\mathfrak{L}$. Укажем такое вложение.

Согласно теореме 5.1.5.2 $F = \mathbf{F}(X)/V(\mathbf{F}(X))$ при подходящем алфавите $X = \{x_i | i \in I\}$. Для каждого слова $v(x_{i_1}, \ldots, x_{i_m})$, не принадлежащего множеству V возьмем в $\mathfrak{L}$ группу G_v, а в ней элементы g_{vi}, $i \in I$, на которых $v(g_{vi_1}, \ldots, g_{vi_m}) \neq 1$. Возьмем декартово произведение $\overline{\prod}_{v \notin V} G_v$, а в нем подгруппу, порожденную элементами f_i, $i \in I$, где $f_i(v) = g_{vi}$. Так как элементы f_i не подчиняются никаким соотношениям, кроме тождеств из V, то порожденная ими подгруппа изоморфна F. ⊠

Легко видеть, что в действительности мы доказали равенство $\overline{\mathfrak{L}} = QSC\mathfrak{L}$ для произвольного класса групп $\mathfrak{L}$.

5.2 Свободные произведения, в том числе с объединением

§1 Свободные произведения

Определение 5.2.1.1. *Свободным произведением $A * B$* групп

$$A = \langle a_1, \ldots, a_n || R_1(a_\nu), \ldots, R_p(a_\nu) \rangle \tag{5.5}$$

и

$$B = \langle b_1, \ldots, b_m || S_1(b_\mu), \ldots, S_q(b_\mu) \rangle \tag{5.6}$$

называется группа

$$A * B = \langle a_1, \ldots, a_n, b_1, \ldots, b_m || R_1(a_\nu), \ldots, R_p(a_\nu), S_1(b_\mu), \ldots, S_q(b_\mu) \rangle. \tag{5.7}$$

Группы A и B называются свободными множителями группы $A * B$.

Хотя в определении свободного произведения $A * B$ участвуют конкретные представления групп A и B, оно, тем не менее, не зависит от этих представлений.

Лемма 5.2.1.2. *[3, лемма 4.1] Свободное произведение $A * B$ однозначно определяется группами A и B. Более того, $A*B$ порождается двумя подгруппами $\overline{A}$ и $\overline{B}$, изоморфными группам A и B соответственно, такими, что $\overline{A} \cap \overline{B} = 1$.*

Доказательство. Предположим, что группы A и B заданы представлениями (5.5) и (5.6), и пусть также

$$A = \langle a'_1, \ldots, a'_s || R'_1(a'_\sigma), \ldots \rangle, \tag{5.8}$$

$$B = \langle b'_1, \ldots, b'_t || S'_1(b'_\tau), \ldots \rangle. \tag{5.9}$$

Тогда группа $A * B$, заданная представлением (5.7), может быть также задана представлением

$$A * B = \langle a'_1, \ldots, a'_s, b'_1, \ldots, b'_t || R_1(a'_\sigma), \ldots, S_1(b'_\tau), \ldots \rangle. \tag{5.10}$$

Изоморфизмы группы (5.5) на группу (5.8) и группы (5.6) на группу (5.9) определяют естественным образом гомоморфизм группы (5.7) на группу (5.10), так как определяющие слова из (5.7) отображаются в слова, равные 1 в группе (5.10). Но воспользовавшись изоморфизмами, обратными к изоморфизмам (5.5) на (5.8) и (5.6) на (5.9), мы получим гомоморфизм, обратный к гомоморфизму группы (5.7) на группу (5.10). Таким образом, $A * B$ определяется однозначно, с точностью до изоморфизма группами A и B.

Пусть $\overline{A}$ — подгруппа группы (5.7), порожденная элементами $a_1, \ldots, a_n$, и пусть $\overline{B}$ — подгруппа группы (5.7), порожденная элементами $b_1, \ldots, b_m$. Очевидно, что $A * B$ порождается подгруппами $\overline{A}$ и $\overline{B}$. Отображение a_ν в a_ν определяет гомоморфизм группы A на группу $\overline{A}$. Далее, гомоморфизм группы $A * B$ в группу A, определяемый отображением a_ν в a_ν и b_μ в 1 отображает $\overline{A}$ на A и является на $\overline{A}$ обратным к гомоморфизму A на $\overline{A}$. Таким образом, $A \cong \overline{A}$; аналогично, $B \cong \overline{B}$.

Наконец, если $g \in \overline{A} \cap \overline{B}$, то гомоморфизм группы $A * B$ в A, определенный выше, переводит g в 1 ввиду $g \in \overline{B}$. Но этот гомоморфизм взаимно однозначен на $\overline{A}$, откуда $g = 1$ и $\overline{A} \cap \overline{B} = 1$. ⊠

Определение 5.2.1.3. [3, стр. 191] Если $g \neq 1$ — элемент из $A * B$ и g лежит в A или в B, то свободный множитель группы $A * B$, содержащий g, обозначается через $F(g)$.

Определение 5.2.1.4. [3, стр. 192] Последовательность элементов $g_1, g_2, \ldots, g_n$ из $A * B$ называется *несократимой*, если $g_1 \neq 1$, g_i лежит в A или в B и g_i, g_{i+1} не лежат в одном и том же свободном множителе.

Пусть $W(a_\nu, b_\mu)$ — слово в $a_1, \ldots, a_n, b_1, \ldots, b_m$. Если $W(a_\nu, b_\mu) = W_1 W_2 \ldots W_r$, где каждое слово W_i непусто (хотя может определять 1 в $A * B$) и является словом только из a_ν

либо только из b_μ, а W_i и W_{i+1} не лежат в одном и том же свободном множителе группы $A * B$, то число r называется *слоговой длиной слова* W и обозначается $\lambda(W)$; слова $W_1, W_2, \ldots, W_r$ называются *слогами слова* W.

Слоговой длиной элемента g группы $A * B$ называется минимум слоговых длин слов, определяющих g. Таким образом, элемент 1 из $A*B$ имеет слоговую длину нуль; слоговая длина произвольного элемента, не лежащего ни в A, ни в B, $\geqslant 2$.

Теорема 5.2.1.5. *[3, теорема 4.1] Каждый элемент g группы $A * B$ единственным образом представим в виде произведения*

$$g = g_1 g_2 \ldots g_r, \tag{5.11}$$

где $g_1, g_2, \ldots, g_r$ — несократимая последовательность (правая часть равенства (5.11) *будет иногда называться несократимой записью элемента g).*

Доказательство. Так как группа $A*B$ порождается подгруппами A и B, произвольный элемент g этой группы представим в виде произведения $h_1, h_2, \ldots, h_n$, где каждый h_i лежит в A или в B. Если среди таких произведений, представляющих g, выбрать произведение $g_1 g_2 \ldots g_r$ с наименьшим количеством r членов, то последовательность $g_1, g_2, \ldots, g_r$ будет несократимой. Поэтому каждый элемент можно представить в виде (5.11).

Осталось доказать единственность. Для этого мы введем некоторую конкретную процедуру ρ превращения произвольного слова $W(a_\nu, b_\mu)$ в несократимую последовательность.

Определение 5.2.1.6. [3, стр. 193] *Несократимая форма $\rho(g_1, \ldots, g_n)$ последовательности элементов $g_1, \ldots, g_n$* каждый из которых лежит или в A или в B (и соседние члены могут быть из одного и того же множителя), определяется индуктивно следующим образом:

ρ(пустая последовательность)=пустая последовательность,

$$\rho(g_1) = \begin{cases} \text{пустая последовательность, если } g_1 = 1, \\ g_1, \quad \text{если } g_1 \neq 1. \end{cases}$$

Далее, если $\rho(g_1, \ldots, g_n) = (h_1, \ldots, h_r)$, то

$$\rho(g_1, \ldots, g_n, g_{n+1}) = \begin{cases} (h_1, \ldots, h_r), & \text{если } g_{n+1} = 1, \\ (h_1, \ldots, h_{r-1}), & \text{если } g_{n+1} = h_r^{-1}, \\ (h_1, \ldots, h_r \cdot g_{n+1}), & \text{если } g_{n+1} \neq h_r^{-1}, \text{ но } F(g_{n+1}) = F(h_r), \\ (h_1, \ldots, h_r, g_{n+1}), & \text{если } F(g_{n+1}) \neq F(h_r). \end{cases}$$

Наконец, для слова $W(a_\nu, b_\mu)$ процедура ρ определяется следующим образом:

Если $W_1, W_2, \ldots, W_n$ — слоги слова W и g_i — элемент группы A или B, определяемый слогом W_i, то $\rho(W_1, \ldots, W_n) = \rho(g_1, \ldots, g_n)$.

Для завершения доказательства теоремы достаточно установить следующие свойства процедуры ρ:

(а) $\rho(g_1, \ldots, g_n)$ является несократимой последовательностью длины, не превосходящей n;

(б) если $\rho(g_1, \ldots, g_n) = (h_1, \ldots, h_r)$, то $g_1 \ldots g_n = h_1 \ldots h_r$;

(в) если $g_1, \ldots, g_n$ — несократимая последовательность, то $\rho(g_1, \ldots, g_n) = (g_1, \ldots, g_n)$;

(г) $\rho(g_1, \ldots, g_k, g_{k+1}, \ldots, g_n) = \rho(\rho(g_1, \ldots, g_k), g_{k+1}, \ldots, g_n)$;

(д) $\rho(g_1, \ldots, g_n, 1) = \rho(g_1, \ldots, g_n)$;

(е) $\rho(g_1, \ldots, g_k, 1, g_{k+1}, \ldots, g_n) = \rho(g_1, \ldots, g_k, g_{k+1}, \ldots, g_n)$

(ж) если $F(g_n) = F(g_{n+1})$, то $\rho(g_1, \ldots, g_n, g_{n+1}) = \rho(g_1, \ldots, g_n \cdot g_{n+1})$;

(з) если $F(g_i) = F(g_{i+1})$, то $\rho(g_1, \dots, g_i, g_{i+1}, \dots, g_n) = \rho(g_1, \dots, g_i \cdot g_{i+1}, \dots g_n$.

Все эти свойства легко устанавливаются непосредственной проверкой. ☒

Следствие 5.2.1.7. *[3, следствие 4.1.1] Пусть A и B — такие подгруппы группы G, что $A \cap B = 1$, и пусть элемент из G однозначно представим в виде произведения $g = g_1 \dots g_n$, где $g_1, \dots, g_n$ — несократимая последовательность. Тогда G является свободным произведением групп A и B.*

Доказательство. Пусть $A = \langle a_1, \dots, a_n || R(a_\nu), \dots \rangle$ и $B = \langle b_1, \dots, b_m || S(b_\mu), \dots \rangle$. Тогда элементы $a_1, \dots, a_n, b_1, \dots, b_m$ порождают группу G, и слова $R(b_\nu), \dots, S(b_\mu), \dots$ равны единице в G. Тогда, очевидно, отображение $a_i \mapsto a_i$, $b_i \mapsto b_i$ продолжается до гомоморфизма $A*B \longrightarrow G$. Поскольку обратное отображение существует, данный гомоморфизм является изоморфизмом. ☒

Следствие 5.2.1.8. *[3, следствие 4.1.2] Пусть $G = A*B$, и пусть C — подгруппа группы A, D — подгруппа группы B. Если H — подгруппа группы G, порождаемая подгруппами C и D, то $H = c * D$.*

Следствие 5.2.1.9. *[3, следствие 4.1.3] Если $(g_1, g_2, \dots, g_r)$ — несократимая последовательность в $A * B$, то $\lambda(g_1 g_2 \dots g_r) = r$.*

Следствие 5.2.1.10. *[3, следствие 4.1.4] Произвольный элемент конечного порядка группы $A * B$ сопряжен с подходящим элементом конечного порядка из A или из B.*

Следствие 5.2.1.11. *[3, следствие 4.1.5] Если g — элемент группы $A * B$, и элементы a, a^g оба лежат в A, то $g \in A$. В частности, если $g \notin A$, то $A^g \cap A = 1$.*

Следствие 5.2.1.12. *[3, следствие 4.1.6] Пусть U и V — такие элементы группы $A*B$, что $UV = VU$. Тогда или U и V лежат в некоторой подгруппе, сопряженной с A или с B, или являются степенями некоторого элемента W.*

Доказательство. Если хотя бы один из элементов U и V равен 1, то они — степени подходящего элемента. Поэтому можно считать, что $U, V \neq 1$. Если, далее, V лежит в подгруппе, сопряженной со свободным множителем, например, в ${}^gA$, то $V^g \in A$ и $V^g \neq 1$. Так как $V^U = V$, то $(V^g)^{U^g} = V^g$ лежит в A. По предыдущему следствию $u^g \in A$ и потому $U \in^g A$.

Итак, мы должны доказать, что если два элемента из $A * B$ коммутируют и ни один из них не лежит в подгруппе, сопряженной с A или с B, то они являются степенями некоторого элемента. Предположим, что это неверно и выберем U и V таким образом, чтобы V был контрпримером минимальной слоговой длины. Далее для элемента V выбираем элемент U также наименьшей слоговой длины. Пусть $U = g_1 g_2 \dots g_r$ и $V = h_1 \dots h_s$ — несократимые записи элементов U и V; тогда $r \geqslant s$.

Если h_1 и h_s лежат в одном и том же сомножителе, то мы можем сократить длину V с помощью сопряжения элементом h_1, поэтому они лежат в разных сомножителях. Если h_1 и g_r лежат в разных сомножителях группы $A * B$, то $UV = g_1 g_2 \dots g_r h_1 h_2 \dots h_s$ есть несократимая запись элемента UV, откуда $\lambda(UV) = r + s$. Так как $UV = VU$, то $\lambda(VU) = r + s$ и потому $VU = h_1 h_2 \dots h_s g_1 g_2 \dots g_r$ есть несократимая запись элемента VU. Из единственности несократимой записи элемента $UV = VU$ в $A * B$ вытекает $r > s$ и $UV^{-1} = g_1 g_2 \dots g_{r-s}$, откуда легко получаем противоречие. Следовательно, h_1 и g_r лежат в одном сомножителе. Тогда h_s и g_r лежат в разных сомножителях. Применяя к V^{-1} предыдущее рассуждение вновь получаем противоречие. ☒

Определение 5.2.1.13. [3, стр. 199] Несократимая последовательность элементов $g_1, g_2, \ldots, g_r$ группы $A * B$ называется *циклически несократимой*, если g_1 и g_r лежат в разных сомножителях группы $A * B$.

Теорема 5.2.1.14. *[3, теорема 4.2] Каждый элемент g группы $A*B$ сопряжен с элементом $g_1 \ldots g_r$, где последовательноcть $g_1, g_2, \ldots, g_r$ циклически несократима. Более того, если $g_1, g_2, \ldots, g_r$ и $h_1, h_2, \ldots, h_s$ — такие две циклически несократимые последовательности, что элементы $g_1 g_2 \ldots g_r$ и $h_1 h_2 \ldots h_s$ являются циклическими перестановками друг друга; если же $r = 1$, то $s = 1$ и g_1 и h_1 сопряжены в одном из свободных множителей.*

Доказательство. Доказательство получается непосредственным вычислением и мы его здесь приводить не будем. ⊠

§2 Свободные произведения с объединенной подгруппой

Определение 5.2.2.1. [3, стр. 208] Если

$$G = \langle a_1, \ldots, a_n, b_1, \ldots, b_m || R(a_\nu), \ldots, S(b_\mu), \ldots, U_1(a_\nu) = V_1(b_\mu), \ldots, U_q(a_\nu) = V_q(b_\mu) \rangle \quad (5.12)$$

и A' — подгруппа, порожденная в G элементами $a_1, \ldots, a_n$, B' — подгруппа, порожденная в G элементами $b_1, \ldots, b_m$, H' — подгруппа, порожденная в A' элементами $U_1(a_\nu), \ldots, U_q(a_\nu)$, K' — подгруппа, порожденная в B' элементами $V_1(b_\mu), \ldots, V_q(b_\mu)$, то G называется *свободным произведением групп A' и B' с подгруппами H', K', объединенными относительно отображения $U_i(a_\nu) \longrightarrow V_i(b_\mu)$.*

Теорема 5.2.2.2. *[3, теорема 4.3] Пусть $A = \langle a_1, \ldots, a_n || R(a_\nu), \ldots \rangle$, $B = \langle b_1, \ldots, b_m || S(b_\mu), \ldots \rangle$ и G определяется соотношением* (5.12). *Пусть A' — подгруппа группы G, порожденная элементами $a_1, \ldots, a_n$, а B' — подгруппа группы G, порожденная элементами $b_1, \ldots, b_m$. Тогда $A \cong A'$ относительно $a_\nu \mapsto a_\nu$ и $B \cong B'$ относительно $b_\mu \mapsto b_\mu$ в том и только в том случае, если отображение $U_i(a_\nu) \longrightarrow V_i(b_\mu)$ индуцирует изоморфизм φ между подгруппой H, порождаемой в A элементами $U_i(a_\nu)$ и подгруппой K, порождаемой в B элементами $V_i(b_\mu)$.*

Доказательство. Предположим, что $A \cong A'$ относительно отображения $a_\nu \mapsto a_\nu$ и $B \cong B'$ относительно отображения $b_\mu \mapsto b_m u$. Если H' и K' — подгруппы группы G, порожденные в ней элементами $U_i(a_\nu)$ и $V_i(b_\mu)$ соответственно, то $H \cong H'$ при отображении $U_i(a_\nu) \longrightarrow U_i(a_\nu)$ и $K \cong K'$ при отображении $V_i(b_\mu) \longrightarrow V_i(b_\mu)$. Так как $U_i(a_\nu) \longrightarrow V_i(b_\mu)$ — тождественный изоморфизм H' на K', то это же отображение индуцирует изоморфизм φ группы H на группу K.

Обратно, предположим, что отображение $U_i(a_\nu) \longrightarrow V_i(b_\mu)$ индуцирует изоморфизм $\varphi : H \longrightarrow K$. Очевидно, что отображения $a_\nu \longrightarrow a_\nu$ и $b_\mu \longrightarrow b_\mu$ индуцируют гомоморфизмы A на A' и B на B' соответственно. Но показать, что эти гомоморфизмы в действительности являются изоморфизмами — нелегкая задача: для этого нам понадобится найти нормальную форму для элементов G. Поэтому мы откладываем завершение доказательства теоремы до лучших времен. ⊠

Список обозначений

$\langle M \rangle$ — подгруппа группы G, порожденная множеством M.

$\sum$ ($\overline{\sum}$) — прямая (декартова) сумма.

$\prod$ ($\overline{\prod}$) — прямое (декартово) произведение.

Если K — кольцо с единицей, то K^* и K^+ — мультипликативная и аддитивная группа кольца K.

$A[n]$ — множество всех $a \in A$, для которых $na = 0$.

В p-группе G для элемента g существует элемент h такой, что $h^{p^n} = g$ и не существует элемента l такого, что $l^{p^{n+1}} = g$, то n называется *высотой* элемента g.

Строка

$$A_1 \xrightarrow{\varphi_1} A_2 \xrightarrow{\varphi_2} \ldots \xrightarrow{\varphi_{n-1}} A_n,$$

где A_i — группы, а φ_i — гомоморфизмы, называется *точной*, если $\operatorname{Im} \varphi_i = \operatorname{Ker} \varphi_{i+1}$.

Пусть A — абелева группа, B — ее подгруппа. Подгруппа C группы A называется B-*высокой*, если $C \cap B = 0$, а для любой $C' > C$ имеем $C' \cap B \neq 0$.

$\overset{e}{\leqslant}$ — эндоморфно допустима, $\overset{a}{\leqslant}$ — автоморфно допустима.

Литература

[1] М. И. Каргаполов, Ю. И. Мерзляков. *Основы теории групп.* Изд. 4-е, М., Наука, Физматлит, 1996.

[2] А. Г. Курош. *Теория групп.* Изд. 3-е, М., Наука, 1067.

[3] В. Магнус, А. Каррас, Д. Солитэр, *Комбинаторная теория групп.* М., Наука, 1974.

[4] Ю. И. Мерзляков. *Рациональные группы. Часть 3 (линейные группы).* Новосибирск, 1975.

[5] Л. С. Понтрягин. *Непрерывные группы.* Изд. 3-е, М., Наука, 1973.

[6] Л. Фукс. *Бесконечные абелевы группы.* тт 1, 2, М., Мир, 1974, 1977.

[7] М. Холл. *Теория групп.* М., ИЛ, 1962.