Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ТЕОРИЯ ГРУПП

III СЕМЕСТР

Лектор: *Богданов Илья Игоревич*

Автор 2020: *Даниил Дрябин*
Дополнил 2022: *Даниил Максимов*
Проект на Github

осень 2022

Содержание

1 Основные понятия теории групп

1.1 Повторение изученного

Определение 1.1. *Группой* называется множество G с определенной на нем бинарной операцией $\cdot : G^2 \to G$ такой, что:

1. (Ассоциативность) $\forall a, b, c \in G : a(bc) = (ab)c$
2. (Существование нейтрального элемента) $\exists e \in G : \forall a \in G : ae = ea = a$
3. (Существование обратного элемента) $\forall a \in G : \exists a^{-1} \in G : aa^{-1} = a^{-1}a = e$

Напоминание. Нейтральный элемент в группе единственен, как и обратный элемент к каждому элементу группы.

Определение 1.2. *Порядком группы* G называется мощность множества G. Обозначение — $|G|$.

Определение 1.3. *Порядком элемента* $a \in G$ называется минимальное число $n \in \mathbb{N}$ такое, что $a^n = e$. Если такого числа не существует, порядок a считается равным ∞. Обозначение — $\operatorname{ord} a$.

Определение 1.4. Пусть G — группа. *Подгруппой* G называется множество $H \subset G, H \neq \varnothing$ такое, что:

1. $\forall a, b \in H : ab \in H$
2. $\forall a \in H : a^{-1} \in H$

Иными словами, множество H само является группой с той же операцией. Обозначение — $H \leqslant G$.

Определение 1.5. Группа G называется *абелевой*, если операция в ней коммутативна: $\forall a, b \in G : ab = ba$.

Пример. Рассмотрим несколько примеров групп:

1. $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$
2. $(R, +)$, $(R^*, \cdot)$, где R — произвольное кольцо
3. $(V, +)$, где V — произвольное линейное пространство
4. $(S_n, \circ)$ — *группа перестановок*

Далее групповая операция в записи группы будет опускаться, если она восстанавливается из контекста.

Напоминание. $\forall \sigma \in S_n : \sigma$ раскладывается в произведение независимых циклов.

Напоминание. *Беспорядком* в перестановке $\sigma \in S_n$ называется пара $(i, j) \in \{1, \ldots, n\}^2$ такая, что $i < j$, но $\sigma(i) > \sigma(j)$. *Знаком перестановки* $\sigma \in S_n$ называется число $(-1)^{N(\sigma)}$, где $N(\sigma)$ — количество беспорядков в σ. Обозначение — $\operatorname{sgn} \sigma$.

Напоминание. $\forall \sigma, \tau \in S_n : \operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$.

Определение 1.6. *Изоморфизмом групп* G и H называется биекция $\varphi : G \to H$ такая, что $\forall a, b \in G : \varphi(ab) = \varphi(a)\varphi(b)$. Группы G и H называются *изоморфными*, если существует соответствующий изоморфизм. Обозначение — $G \cong H$.

Напоминание (Теорема Кэли)**.** $\forall G, |G| = n : \exists H \leqslant S_n : G \cong H$.

Пример. Рассмотрим несколько примеров групп и подгрупп в них:

1. $\mathrm{GL}_n(\mathbb{F}) = (M_n(\mathbb{F}))^* = \{A \in M_n(\mathbb{F})\colon \det A \neq 0\}$, где $\mathbb{F}$ — произвольное поле. GL означает general linear

2. $\mathrm{SL}_n(\mathbb{F}) = \{A \in M_n(\mathbb{F})\colon \det A = 1\} \leqslant \mathrm{GL}_n(\mathbb{F})$, где $\mathbb{F}$ — произвольное поле. SL означает special linear

3. $\mathcal{O}_n = \{A \in M_n(\mathbb{R}) : A^T A = E\} \leqslant \mathrm{GL}_n(\mathbb{R})$ - группа ортогональных матриц

4. $\mathcal{U}_n = \{A \in M_n(\mathbb{C}) : A^T \overline{A} = E\} \leqslant \mathrm{GL}_n(\mathbb{C})$ - группа унитарных матриц

5. $\mathbb{T} = \{z \in \mathbb{C}\colon |z| = 1\} \leqslant \mathbb{C}^*$

6. $\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\} \leqslant \mathbb{T} \leqslant \mathbb{C}^*$ - группа комплексного корня n-й степени из единицы

7. $A_n = \{\sigma \in S_n : \operatorname{sgn}\sigma = 1\} \leqslant S_n$ - подгруппа чётных перестановок

8. $\mathcal{O}_2$ символизирует все ортогональные преобразования на плоскости. Среди них есть те, что образуют особенные *подгруппы Диэдра* $D_n \leqslant \mathcal{O}_2$ - это группы самосовмещений правильного n-угольника, то есть $\forall \varphi \in D_n\ \varphi(P_n) = P_n$, если P_n - это множество точек такого n-угольника.

Определение 1.7. Пусть G — группа, $M \subset G$. *Подгруппой, порожденной* M, называется наименьшая по включению подгруппа в G, содержащая M. Обозначение — $\langle M \rangle$.

Напоминание. Если G — группа, $M \subset G$, то $\langle M \rangle$ можно представить в следующем виде:

$$M = \{m_1^{\varepsilon_1} \cdots m_k^{\varepsilon_k} : m_1, \dots, m_k \in M, \varepsilon_1, \dots, \varepsilon_k \in \{\pm 1\}\}$$

Определение 1.8. Группа G называется *циклической*, если $\exists a \in G : \langle a \rangle = G$, то есть $G = \{a^n : n \in \mathbb{Z}\}$.

Напоминание. Если группа G — циклическая, то либо $G \cong \mathbb{Z}$ (если G бесконечна), либо $G \cong \mathbb{Z}_n$ (если G конечна). Более того, если $H \leqslant G$, то H — тоже циклическая, причем либо $H \cong n\mathbb{Z}, n \in \mathbb{N} \cup \{0\}$, либо $H \cong k\mathbb{Z}_n, k \in \mathbb{N}, k \mid n$.

Определение 1.9. Пусть G — группа, $A, B \subset G$. Тогда, определим следующие операции на множествах:

1. $AB := \{ab : a \in A, b \in B\}$

2. $A = \{a\} \Rightarrow aB := AB$

3. $A^{-1} := \{a^{-1} : a \in A\}$

Замечание. Введённые операции совершенно не означают, что мы сделали множество подмножеств само по себе группой. Тем не менее, верна ассоциативность:

$$\forall A, B, C \subset G \quad (AB)C = A(BC) = \{abc\colon a \in A, b \in B, c \in C\}$$

Замечание. Если $H \leqslant G$, то $HH = H^{-1} = H$

Определение 1.10. Пусть G — группа, $H \leqslant G$, $a \in G$. Тогда *левым смежным классом a по подгруппе H* называется $aH = \{ah : h \in H\}$, *правым смежным классом a по подгруппе H* — Ha. Обозначение множества всех левых смежных классов по H в G — G/H, правых смежных классов — $H\backslash G$.

Утверждение 1.1. *Пусть G — группа, $H \leqslant G$, $a, b \in G$. Тогда следующие утверждения эквивалентны:*

1. $aH \cap bH \neq \varnothing$
2. $b^{-1}a \in H$
3. $aH = bH$
4. $a \in bH$

Доказательство.

- ▷ $(1 \Rightarrow 2)$ По условию, $\exists h_1, h_2 \in H : ah_1 = bh_2$, откуда $b^{-1}a = h_2h_1^{-1} \in H$
- ▷ $(2 \Rightarrow 3)$ Поскольку H — группа и $b^{-1}a \in H$, то $(b^{-1}a)H = H$, и, следовательно, $aH = bH$
- ▷ $(3 \Rightarrow 4)$ Заметим, что $a = ae$, поэтому $a \in aH = bH$
- ▷ $(4 \Rightarrow 1)$ Поскольку $a = ae$ и $a \in bH$, то $a \in aH \cap bH$, следовательно, $aH \cap bH \neq \varnothing$

□

Замечание. Аналогичное утверждение для правых смежных классов будет верно, если заменить в формулировке второго пункта $b^{-1}a \in H$ на $ab^{-1} \in H$.

Теорема 1.1 (Лагранжа)**.** *Пусть G — конечная группа, $H \leqslant G$. Тогда верно равенство:*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|$$

Доказательство. Если смежные классы пересекаются хотя бы по одному элементу, то они совпадают. Тогда, поскольку $\forall a \in G : a \in aH$, G разбивается на непересекающиеся смежные классы порядка $|H|$, откуда и следует требуемое равенство. □

Напоминание. Из теоремы выше, в частности, следует, что если G — конечная группа, то имеет место 3 факта:

1. $\forall H \leqslant G \quad |H| \mid |G|$
2. $\forall a \in G \quad \operatorname{ord} a \mid |G|$

3. $\forall a \in G \quad a^{|G|} = e$

Утверждение 1.2. *Пусть G — группа. Тогда $\forall H \leqslant G : |G/H| = |H \backslash G|$.*

Доказательство. Сопоставление $aH \mapsto (aH)^{-1} = Ha^{-1}$ является биекцией, поскольку оно обратимо, из чего следует и сюръективность, и инъективность. □

Определение 1.11. Пусть G — группа, $H \leqslant G$. *Индексом H в G* называется величина $|G/H| = |H \backslash G|$. Обозначение — $|G : H|$.

Упражнение. *Если $K \leqslant H \leqslant G$, то имеет место равенство*

$$|G : K| = |G : H| \cdot |H : K|$$

при условии, что $|G : H|$ и $|H : K|$ конечны (Оно верно и в общем случае, только надо говорить не о порядках, а о биекциях между множествами).

1.2 Нормальные подгруппы

Определение 1.12. Пусть G — группа, $g, x \in G$. Элементом, *сопряженным к g с помощью x*, называется $g^x := x^{-1}gx \in G$. Элементы $g_1, g_2 \in G$ называются *сопряженными*, если $\exists x \in G : g_1 = g_2^x$.

Замечание. Пусть G — группа, $H \leqslant G$, $g \in G$. Будем обозначать $g^{-1}Hg$ как H^g.

Утверждение 1.3. *Пусть G — группа. Тогда:*

1. $\forall g, x, y \in G : g^{xy} = (g^x)^y$
2. $\forall g_1, g_2, x \in G : (g_1g_2)^x = g_1^x g_2^x$

Доказательство. Произведем непосредственную проверку:

1. $(g^x)^y = y^{-1}(x^{-1}gx)y = (xy)^{-1}g(xy) = g^{xy}$
2. $g_1^x g_2^x = (x^{-1}g_1x)(x^{-1}g_2x) = x^{-1}(g_1g_2)x = (g_1g_2)^x$

□

Утверждение 1.4. *Сопряженность является отношением эквивалентности в группе G.*

Доказательство. Произведем непосредственную проверку:

▷ (Рефлексивность) $\forall g \in G : g = g^e$

▷ (Симметричность) Если $g_2 = g_1^x$, то $g_2^{x^{-1}} = (g_1^x)^{x^{-1}} = g_1^e = g_1$

▷ (Транзитивность) Если $g_2 = g_1^x$, $g_3 = g_2^y$, то $g_3 = (g_1^x)^y = g_1^{xy}$

□

Определение 1.13. Пусть G — группа, $g \in G$. *Классом сопряженности* элемента g называется множество g^G, то есть класс эквивалентности по отношению сопряженности, содержащий g.

Определение 1.14. Пусть G — группа, $H \leqslant G$. Подгруппа H называется *нормальной в* G, если $\forall g \in G\ gH = Hg$. Обозначение — $H \trianglelefteqslant G$.

Утверждение 1.5. *Определение выше имеет ряд эквивалентных формулировок:*

1. $G/H = H \backslash G$
2. $\forall g \in G : H^g = H$
3. $\forall g \in G : gH \subset Hg$
4. $\forall g \in G : H^g \subset H$

Доказательство.

- (опр. $\Leftrightarrow$ 1) В сторону 1 очевидно, а в обратную предположим противное: $gH \neq Hg$. Но по условию это должно быть эквивалентно $gH \cap Hg = \varnothing$. Тем не менее, $gH \cap Hg \supset \{g\}$, а потому определение выполнено
- (опр. $\Leftrightarrow$ 2) Очевидно
- (опр. $\Leftrightarrow$ 3) Если выполнено условие 3, то тогда
$$\forall g \in G\ g^{-1}H \subset Hg^{-1} \Longleftrightarrow \forall g \in G\ Hg \subset gH$$
- ($3 \Leftrightarrow 4$) Очевидно

□

Пример. Рассмотрим несколько примеров нормальных подгрупп в соответствующих группах:

1. $\forall H \leqslant G : H \trianglelefteqslant G$, где G — абелева группа
2. $G \trianglelefteqslant G$, $\{e\} \trianglelefteqslant G$, где G — произвольная группа
3. $A_n \trianglelefteqslant S_n$, поскольку $\forall \sigma \in S_n, \forall \tau \in A_n \quad \operatorname{sgn}(\sigma\tau\sigma^{-1}) = \operatorname{sgn}\tau = 1$, то есть $\forall \sigma \in S_n : \sigma A_n \sigma^{-1} \subset A_n$

Пример. Продемонстрируем ненормальную подгруппу. Рассмотрим S_3 и подгруппу $H = \langle(1\ 2)\rangle = \{(1\ 2), e\}$. Проверим сопряжение H:

$$(1\ 2)^{(1\ 3)} = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H$$

Упражнение. *Пусть G — группа, $H \leqslant G$. Тогда $H \trianglelefteqslant G \Leftrightarrow H$ — объединение некоторого количества классов сопряженности в G.*

Утверждение 1.6. *Пусть G — группа, $H_1 \trianglelefteqslant G$, $H_2 \trianglelefteqslant G$. Тогда $H_1 \cap H_2 \trianglelefteqslant G$.*

Доказательство. $\forall g \in G\quad g(H_1 \cap H_2)g^{-1} \subset (gH_1g^{-1}) \cap (gH_2g^{-1}) = H_1 \cap H_2$. □

Утверждение 1.7. *Пусть G — группа, $H \trianglelefteqslant G$, $K \leqslant G$. Тогда:*

1. $HK \leqslant G$

2. *Если $K \trianglelefteq G$, то $HK \trianglelefteq G$*

Доказательство. Заметим, что $HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH$. Воспользуемся этим свойством:

1. $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$, поэтому HK замкнуто относительно умножения, и, аналогично, $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$
2. $\forall g \in G : g(HK)g^{-1} = (gHg^{-1})(gKg^{-1}) = HK$

$\square$

Пример. Требование, что хотя бы одна подгруппа нормальна, существенно. Рассмотрим подгруппы $S_3 \geqslant \langle(1\ 2)\rangle, \langle(1\ 3)\rangle$. Тогда $\langle(1\ 2)\rangle\langle(1\ 3)\rangle \not\leqslant S_3$, ибо

$$|\langle(1\ 2)\rangle\langle(1\ 3)\rangle| = 2 \cdot 2 = 4 \nmid |S_3| = 6$$

Утверждение 1.8. *Пусть $H, K \leqslant G$, $H \cap K = \{e\}$. Тогда*

$$|HK| = |H| \cdot |K|$$

Доказательство. Заметим факт: если $h_1, h_2 \in H$, $k_1, k_2 \in K$ и при этом $h_1k_1 = h_2k_2$, то $h_1 = h_2$ и $k_1 = k_2$. Действительно

$$h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\} \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} = e$$

$\square$

Упражнение. *Если $H, K \leqslant G$, $|G| < \infty$, $H \cap K = L$, то имеет место равенство:*

$$|HK| = \frac{|H| \cdot |K|}{|L|}$$

Утверждение 1.9. *Пусть G — группа, $H \leqslant G$, $|G : H| = 2$. Тогда $H \trianglelefteq G$.*

Доказательство. По условию, $G/H = \{H, G \backslash H\} = H \backslash G$. $\square$

Замечание. Покажем, что $|S_n : A_n| = 2$ при $n \geqslant 2$. Действительно, сопоставление $\sigma \mapsto (1, 2)\sigma$ осуществляет биекцию между A_n и $S_n \backslash A_n$, поэтому $S_n/A_n = \{A_n, (1, 2)A_n\}$.

Упражнение. *Пусть G — группа, $g_1, g_2 \in G$. Докажите, что тогда $g_1^G g_2^G$ — объединение нескольких классов сопряженности, причем необязательно одного.*

Пример. Пусть $\sigma \in S_n$. Представим σ в виде произведения независимых циклов, $\sigma = (a_1 \dots a_k)(b_1 \dots b_l) \dots$, и рассмотрим σ^τ для произвольного $\tau \in S_n$. Если $a_i' := \tau^{-1}(a_i), i \in \{1, \dots, k\}$, то $\sigma^\tau(a_i') = (\tau^{-1}\sigma\tau)(a_i') = a_{i+1}'$. Значит, $\sigma^\tau = (a_1' \dots a_k')(b_1' \dots b_l') \dots$, и, следовательно, σ^{S_n} состоит из перестановок того же циклического типа, что и σ, причем из всех, потому что по каждой такой перестановке легко восстанавливается соответствующая $\tau \in S_n$.

1.3 Гомоморфизмы групп и факторгруппа

Определение 1.15. Пусть G, H — группы. *Гомоморфизмом групп* G *и* H называется отображение $\varphi\colon G \to H$ такое, что

$$\forall g_1, g_2 \in G \quad \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

Замечание. Дадим определение всех остальных нужных морфизмов:

- *Эпиморфизм* — это сюръективный гомоморфизм
- *Мономорфизм* — это инъективный гомоморфизм
- *Изоморфизм* — это биективный гомоморфизм
- *Эндоморфизм* — это гомоморфизм группы в себя
- *Автоморфизм* — это изоморфизм группы в себя

Пример. Рассмотрим несколько примеров гомоморфизмов групп:

1. Любой изоморфизм групп, в частности, автоморфизм $\varphi(g) = g$
2. $\varphi : G \to H$, $\forall g \in G : \varphi(g) = e$, где G, H — произвольные группы
3. Сопряжение при помощи $x \in G$, где G — произвольная группа, поскольку $\forall g_1, g_2 \in G : (g_1 g_2)^x = g_1^x g_2^x$ (более того, сопряжение — это автоморфизм, поскольку существует обратное отображение: $\forall g \in G : \varphi^{-1}(g) = g^{x^{-1}}$)
4. $\det : \mathrm{GL}_n(F) \to F^*$, поскольку $\forall A, B \in \mathrm{GL}_n(F) : \det(AB) = \det A \det B$
5. $\mathrm{sgn} : S_n \to \mathbb{Q}^*$, поскольку $\forall \sigma, \tau \in S_n : \mathrm{sgn}(\sigma\tau) = \mathrm{sgn}\,\sigma\,\mathrm{sgn}\,\tau$
6. Отображение $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ такое, что $\forall a \in \mathbb{Z} : \varphi(a) = a + n\mathbb{Z}$, поскольку $\forall a, b \in \mathbb{Z} : \varphi(a+b) = (a+b) + n\mathbb{Z} = \varphi(a) + \varphi(b)$

Утверждение 1.10. *Пусть* $\varphi\colon G_1 \to G_2$ *- гомоморфизм. Тогда верно 2 утверждения:*

1. $\varphi(e_1) = e_2$ *- нейтральный элемент переходит в нейтральный элемент*
2. $\forall a \in G_1 \quad \varphi(a^{-1}) = \varphi(a)^{-1}$

Доказательство.

1. $\varphi(e_1) = \varphi(e_1^2) = \varphi(e_1) \cdot \varphi(e_1) \Rightarrow \varphi(e_1) = \varphi(e_1) \cdot \varphi(e_1)^{-1} = e_2$
2. $\varphi(e_1) = \varphi(a \cdot a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) = e_2 \Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$

□

Определение 1.16. Пусть G, H — группы, $\varphi : G \to H$ — гомоморфизм G и H. Тогда:

- *Образом* φ называется $\operatorname{Im}\varphi := \{\varphi(g) : g \in G\} = \varphi(G)$
- *Ядром* φ называется $\operatorname{Ker}\varphi := \{g \in G : \varphi(g) = e\} = \varphi^{-1}(e)$

Замечание. Далее мы часто будем обозначать $\varphi(g)$ как $\overline{g}$.

Утверждение 1.11. *Пусть G, H — группы, $\varphi : G \to H$ — гомоморфизм, $K := \operatorname{Ker}\varphi$. Тогда $\forall g \in G : \varphi^{-1}(\overline{g}) = gK = Kg$.*

Доказательство. Пусть $a \in G$. Тогда $a \in \varphi^{-1}(\overline{g}) \Leftrightarrow \overline{a} = \overline{g} \Leftrightarrow e = \overline{g}^{-1}\overline{a} = \overline{g^{-1}a} \Leftrightarrow g^{-1}a \in$ $\in \operatorname{Ker}\varphi = K \Leftrightarrow a \in gK$. Аналогично доказывается, что $a \in \varphi^{-1}(\overline{g}) \Leftrightarrow a \in Kg$. □

Следствие. φ — мономорфизм $\Leftrightarrow \operatorname{Ker}\varphi = \{e\}$.

Утверждение 1.12. *Пусть G, H — группы, $\varphi : G \to H$ — гомоморфизм. Тогда:*

1. $\operatorname{Im}\varphi \leqslant H$
2. $\operatorname{Ker}\varphi \trianglelefteq G$

Доказательство.

1. Если $h_1, h_2 \in \operatorname{Im}\varphi$, то $h_1 = \overline{g_1}$, $h_2 = \overline{g_2}$, откуда $h_1h_2 = \overline{g_1g_2} \in \operatorname{Im}\varphi$ и $h_1^{-1} = \overline{g_1^{-1}} \in \operatorname{Im}\varphi$
2. Если $g_1, g_2 \in \operatorname{Ker}\varphi$, то $\overline{g_1} = \overline{g_2} = e$, откуда $\overline{g_1g_2} = e$ и $\overline{g_1^{-1}} = e$, и, более того, $\forall g \in G \;\; gK = Kg = \varphi^{-1}(\overline{g})$

□

Замечание. Пусть $H \leqslant G$. Тогда существует гомоморфизм $\varphi \colon H \to G$ тривиального вида:

$$\forall h \in H \quad \varphi(h) = h \Rightarrow \operatorname{Im}\varphi = H$$

Замечание. Если G, H — группы, $\varphi : G \to H$ — гомоморфизм и $G' \leqslant G$, то $\varphi|_{G'} \colon G' \to$ $\to H$ — тоже гомоморфизм, поэтому $\varphi(G') = \operatorname{Im}\varphi|_{G'} \leqslant H$. С другой стороны, если $H' \leqslant H$, то существует гомоморфизм $\psi = \operatorname{id}|_{H'} : H' \to H$ такой, что $H' = \operatorname{Im}\psi$.

Определение 1.17. Пусть G — группа, $K \trianglelefteq G$. Тогда, мы можем ввести операцию умножения на G/K, совпадающую с умножением подмножеств группы:

$$\forall g_1, g_2 \in G \quad (g_1K)\cdot(g_2K) = g_1(Kg_2)K = g_1g_2KK = g_1g_2K$$

Замечание. Несмотря на то, что мы смогли показать замкнутость умножения в G/K, надо ещё проверить корректность, то есть независимость от выбранного представителя класса смежности.

Пусть $g_1' = g_1k_1$, $g_2' = g_2k_2$. Тогда:

$$g_1'g_2'e = g_1k_1g_2k_2 = g_1g_2k_1'k_2 \Rightarrow g_1'g_2'K \cap g_1g_2K \neq \{e\} \Rightarrow g_1'g_2'K = g_1g_2K$$

Утверждение 1.13. *Пусть G — группа, $K \trianglelefteq G$. Тогда $(G/K, \cdot)$ — группа.*

Доказательство. Проверим непосредственно, что множество G/K является группой:

- ▷ (Ассоциативность)

$$\forall g_1K, g_2K, g_3K \in G/K \quad (g_1Kg_2K)g_3K = (g_1g_2g_3)K = g_1K(g_2Kg_3K)$$

- ▷ (Нейтральный элемент) $\exists eK = K \in G/K \mid \forall gK \in G/K \quad (gK)K = K(gK) = gK$

▷ (Обратный элемент)

$$\forall gK \in G/K\ \exists (gK)^{-1} = g^{-1}K \in G/K \mid (gK)(gK)^{-1} = (gK)^{-1}(gK) = K$$

□

Определение 1.18. Пусть G — группа, $K \trianglelefteqslant G$. Группа G/K называется *факторгруппой G по K*.

Определение 1.19. *Коммутативной диаграммой* называется рисунок, где отображены алгебраические структуры и функции, отображающие их друг в друга - морфизмы. Коммутативность диаграммы означает, что композиция морфизмов вдоль любого направленного пути зависит только от начала и конца пути (то есть композиции, полученные разными путями, должны давать равный результат).

Теорема 1.2 (Основная теорема о гомоморфизме)**.**

1. *Пусть G — группа, $K \trianglelefteqslant G$. Тогда $\exists \pi : G \to G/K$ — эпиморфизм такой, что $\operatorname{Ker}\pi = K$.*

2. *Пусть G, H — группы, $\varphi : G \to H$ — гомоморфизм. Тогда $\operatorname{Im}\varphi \simeq G/\operatorname{Ker}\varphi$.*

Доказательство. Традиционно эту теорему показывают при помощи *коммутативной диаграммы*, которая отражает 2 соотношения: $\varphi = \Theta \circ \pi$ и $\pi = \psi \circ \varphi$

$$\begin{tikzcd}
G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & \operatorname{Im}\varphi \leqslant H \arrow[dl, dashed, "\psi"'] \\
& G/\operatorname{Ker}\varphi \arrow[ur, dashed, "\Theta"'] &
\end{tikzcd}$$

1. Очевидно хмочется определить $\pi\colon G \to G/K$ следующим образом:

$$\forall g \in G \quad \pi(g) = gK$$

Это уже эпиморфизм из доказанных выше свойств. Остаётся показать, что ядро действительно совпадает с подгруппой:

$$\operatorname{Ker}\pi = \{g \in G\colon \pi(g) = gK = K\} = K$$

2. Обозначим $K_\varphi := \operatorname{Ker}\varphi \trianglelefteqslant G$. Тогда, нам нужно построить $\psi\colon \operatorname{Im}\varphi \to G/K_\varphi$ - изоморфизм. Мы уже доказали, что такое прообраз элемента из образа G, а потому логично рассмотреть такую ψ:

$$\forall g \in G \quad \psi(\overline{g}) = gK_\varphi$$

Проверим, что полученная функция задаёт изоморфизм:

▷ (Гомоморфизм)

$$\forall \overline{g_1}, \overline{g_2} \in \operatorname{Im}\varphi \quad \psi(\overline{g_1} \cdot \overline{g_2}) = \psi(\overline{g_1 g_2}) = g_1 g_2 K_\varphi = (g_1 K_\varphi)(g_2 K_\varphi) = \psi(\overline{g_1})\psi(\overline{g_2})$$

▷ (Сюръективность)

$$\forall gK_\varphi \in G/K_\varphi \quad \psi(\overline{g}) = gK_\varphi$$

▷ (Инъективность) Как уже известно, достаточно проверить тривиальность ядра:

$$\forall \overline{g} \in \operatorname{Im}\varphi \quad \psi(\overline{g}) = K \Rightarrow gK = K \Rightarrow g \in K \Rightarrow \overline{g} = \overline{e}$$

Теорема доказана, но убедимся непосредственно в том, что диаграмма коммутативна, то есть $\Theta \circ \pi = \varphi$, или $\Theta^{-1} \circ \varphi = \psi \circ \varphi = \pi$:

$$\forall g \in G : \psi(\varphi(g)) = \psi(\overline{g}) = gK = \pi(g)$$

□

Замечание. «Гомоморфный образ группы, будь во имя коммунизма изоморфен факторгруппе по ядру гомоморфизма!»

Замечание. Есть и другая версия стишка, позволяющая доказать недостижимость коммунизма:

«Гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма до победы коммунизма»

Так как математическая истина вечна, то коммунизм никогда не победит.

Замечание. Эпиморфизм π называется *каноническим эпиморфизмом.*

Пример. В группе перестановок у нас есть функция знака, которая тоже является гомоморфизмом (при $n \geqslant 2$):

$$\operatorname{sgn}\colon S_n \to \mathbb{C}_2 = (\{\pm 1\}, \cdot) \simeq \mathbb{Z}_2$$

Верно 2 вещи: $\operatorname{Im}\operatorname{sgn} = \mathbb{C}_2$ и $\operatorname{Ker}\operatorname{sgn} = A_n \trianglelefteq S_n$. Стало быть

$$S_n/A_n \simeq \mathbb{C}_2 \simeq \mathbb{Z}_2$$

Теорема 1.3 (Первая теорема об изоморфизме)**.** *Пусть G – группа, $K \trianglelefteq G$, $H \leqslant G$. Тогда $HK = KH \leqslant G$, $K \cap H \trianglelefteq H$ и $HK/K \simeq H/(K \cap H)$.*

Доказательство. Первое утверждение теоремы уже было доказано, поэтому докажем оставшиеся два. Для этого рассмотрим канонический эпиморфизм $\pi : G \to G/K$ и $\forall g \in G$ обозначим $\overline{g} := \pi(g)$.

Пусть $\varphi := \pi|_H : H \to G/K$. Тогда $\operatorname{Ker}\varphi = \operatorname{Ker}\pi \cap H = K \cap H$, откуда $K \cap H \trianglelefteq H$. $\operatorname{Im}\varphi = \{\overline{h} : h \in H\} = \{hK : h \in H\} = HK/K$, поскольку $HK/K = \{hkK : h \in H, k \in \in K\} = \{hK : h \in H\}$. По основной теореме о гомоморфизме, $HK/K \cong H/(K \cap H)$. □

Пример. Положим $G = S_4$, за $H = S_3$, а $K = V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ - четверная группа Клейна. Заметим, что $V_4 \trianglelefteq S_4$ - это так, потому что V_4 состоит из двух классов сопряженности. Более того, $HK = S_3V_4 = S_4$. Стало быть

$$S_4/V_4 = HK/K \simeq H/(H \cap K) = S_3/\{e\} \simeq S_3$$

Теорема 1.4 (Вторая теорема об изоморфизме, или теорема о соответствии)**.** *Пусть G – группа, $K \trianglelefteq G$, $K \leqslant H \leqslant G$*

1. *Каждой такой подгруппе H сопоставляется $\overline{H} = H/K \leqslant G/K = \overline{G}$. При этом соответствие $H \mapsto \overline{H}$ - это биекция между между множеством подгрупп со свойством как у H и подгрупп в $\overline{G}$.*

2. *Имеет место эквивалентность $H \trianglelefteq G \Leftrightarrow \overline{H} \trianglelefteq \overline{G}$. Если нормальность присутствует, тогда верен изоморфизм:*

$$G/H \cong \overline{G}/\overline{H} = (G/K)/(H/K)$$

Замечание. Шуточно говоря, второе свойство утверждает возможность сократить дробь на K.

Утверждение 1.14. *Если $\varphi\colon G_1 \to G_2$ - гомоморфизм, то есть 2 свойства:*

- ▷ $\forall H \leqslant G_1 \Rightarrow \varphi(H) \leqslant G_2$
- ▷ $\forall D \leqslant G_2 \Rightarrow \varphi^{-1}(D) \leqslant G_1$

Доказательство. Для доказательства достаточно показать замкнутость соответствующих множеств относительно операции своей группы:

- ▷ 1. $\forall a, b \in H \quad \varphi(a) \cdot \varphi(b) = \varphi(ab)$, где $ab \in H$, то есть $\varphi(ab) \in \varphi(H)$
  2. $\forall a \in H\ \varphi(a) \cdot \varphi(a^{-1}) = \varphi(e) = e$, откуда $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H)$
- ▷ 1. $\forall a, b \in \varphi^{-1}(D)$ верно, что $\varphi(a), \varphi(b) \in D \Rightarrow \varphi(a) \cdot \varphi(b) = \varphi(ab) \in D \Rightarrow ab \in \varphi^{-1}(D)$
  2. $\forall a \in \varphi^{-1}(D) \Rightarrow \varphi(a) \in D \Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1} \in D \Rightarrow a^{-1} \in \varphi^{-1}(D)$

□

Доказательство.

1. Рассмотрим канонический эпиморфизм $\pi : G \to G/K = \overline{G}$. Тогда

$$\forall K \leqslant H \leqslant G : \pi(H) = \overline{H} = H/K \leqslant G/K$$

С другой стороны, любой прообраз можно записать в следующем виде:

$$\forall L \leqslant \overline{G} \ \ \pi^{-1}(L) = \bigcup_{gK \in L} gK \leqslant G$$

Проверим, что π осуществляет требуемую биекцию. Действительно, $\pi^{-1} \circ \pi = \mathrm{id}$, поскольку $\pi^{-1}(\pi(H)) = H$ (H — объединение нескольких левых смежных классов по K), и $\pi \circ \pi^{-1} = \mathrm{id}$, ибо $\forall L \leqslant \overline{G} : \pi(\pi^{-1}(L)) = L$.

2. Если $H \trianglelefteq G$, то $\forall g \in G : gH = Hg$, поэтому, применяя эпиморфизм π, получаем, что $\forall \overline{g} \in \overline{G} : \overline{g}\overline{H} = \overline{H}\overline{g}$, то есть $\overline{H} \trianglelefteq \overline{G}$. Пусть теперь, наоборот, $\overline{H} \trianglelefteq \overline{G}$. Рассмотрим канонический эпиморфизм $\pi' : \overline{G} \to \overline{G}/\overline{H}$. Тогда $\varphi := \pi' \circ \pi : G \to \overline{G} \to \overline{G}/\overline{H}$ — тоже эпиморфизм, причем

$$\operatorname{Ker} \varphi = \pi^{-1}((\pi')^{-1}(\overline{H})) = \pi^{-1}(\overline{H}) = H$$

Значит, $H \trianglelefteq G$, и, по основной теореме о гомоморфизме, $G/H \cong \overline{G}/\overline{H}$.

$\square$

Пример. Рассмотрим $G = \mathbb{Z}$ и $G \geqslant n\mathbb{Z} \geqslant k\mathbb{Z}$, тогда $n \mid k$, $\overline{H} = n\mathbb{Z}/k\mathbb{Z} = n \cdot \mathbb{Z}_k$. Вторая теорема утверждает, что

$$\overline{G}/\overline{H} = \mathbb{Z}_k/n\mathbb{Z}_k \cong \mathbb{Z}_n$$

Упражнение. *Укажите в явном виде изоморфизм $G/H \to \overline{G}/\overline{H}$ из предыдущей теоремы.*

1.4 Действие группы на множестве

Замечание. Многие группы оказываются группами преобразований над множествами. Примерами будут $S_n, D_n, \mathrm{GL}_n(\mathbb{F}), \mathcal{O}_n, \mathcal{U}_n$. Идея того, что любую группу можно *интерпретировать* как группу преобразований, является одной из ключевых в теории групп.

Определение 1.20. Пусть G — группа, Ω — множество. Будем говорить, что определено *действие группы G на множестве Ω*, если для каждого $g \in G$ и $\omega \in \Omega$ определен элемент $g\omega := g(\omega) \in \Omega$, причем выполнены следующие свойства:

1. $\forall g_1, g_2 \in G : \forall \omega \in \Omega \quad (g_1 g_2)\omega = g_1(g_2\omega)$
2. $\forall \omega \in \Omega \quad e\omega = \omega$

Определение 1.21. Пусть G — группа, Ω — множество. Определим группу $S(\Omega) := \{\sigma : \Omega \to \Omega : \sigma$ — биекция$\}$. Тогда *действие группы G на множестве* Ω — это гомоморфизм $\varphi : G \to S(\Omega)$.

Утверждение 1.15. *Данные выше определения действия группы G на множестве Ω эквивалентны.*

Доказательство.

- $(1 \Rightarrow 2)$ $\forall g \in G$ определим $I_g \colon \Omega \to \Omega$ так, что

$$\forall w \in \Omega \quad I_g(\omega) := g\omega$$

Нужно проверить гомоморфность и биективность каждой I_g. Начнём с первого:

$$(I_g \circ I_h)(\omega) = g(h(\omega)) = (gh)(\omega) = I_{gh}(\omega)$$

Теперь проверим, что I_g — это биекция. Действительно, $I_e = \mathrm{id}$, поэтому $\forall g \in G$: $I_g \circ I_{g^{-1}} = I_{g^{-1}} \circ I_g = \mathrm{id}$. Значит, $\varphi(g) = I_g$ — гомоморфизм групп G и $S(\Omega)$.

- $(2 \Rightarrow 1)$ Для каждого $g \in G$ определим $g\omega := \varphi(g)(\omega)$. Тогда

  1. $(g_1 g_2)\omega = \varphi(g_1 g_2)(\omega) = \varphi(g_1)(\varphi(g_2)(\omega)) = g_1(g_2\omega)$
  2. $e\omega = \varphi(e)(\omega) = \mathrm{id}(\omega) = \omega$

$\square$

Определение 1.22. Пусть группа G действует на множество Ω. *Ядром действия* называется ядро соответствующего гомоморфизма $\varphi : G \to S(\Omega)$, то есть

$$\operatorname{Ker} \varphi = \{g \in G \mid \forall \omega \in \Omega \ \ \varphi(g)\omega = g\omega = \omega\}$$

Замечание. Ядро действия группы G — это нормальная подгруппа в G, поскольку это ядро гомоморфизма.

Определение 1.23. Пусть группа G действует на множество Ω. Действие называется *точным*, или *эффективным*, если его ядро тривиально, то есть равно $\{e\}$.

Определение 1.24. Действие называется *свободным*, если $\forall g \in G, g \neq e : \forall \omega \in \Omega : g\omega \neq \omega$.

Пример. Рассмотрим несколько примеров действий групп на соответствующих множествах:

1. S_n действует на $X_n := \{1, \ldots, n\}$ с гомоморфизмом id, а если $\forall \sigma \in S_n$ и $\forall x, y \in X_n$ положить $\sigma(x, y) := (\sigma(x), \sigma(y))$, то результатом будет действие S_n на X_n^2

2. $\mathrm{GL}_n(F)$ действует на F^n, $\forall A \in \mathrm{GL}_n(F) : \forall v \in F^n : A(v) = Av$, и, аналогично, $\mathrm{GL}_n(F)$ действует на любом линейном пространстве V над полем F таком, что $\dim V = n$, а также на множестве всех подпространств V

3. *Группа диэдра* $D_n = \{\varphi \in \mathcal{O}_2 : \varphi(\mathcal{P}_n) = \mathcal{P}_n\} \leqslant \mathcal{O}_2$, где $\mathcal{P}_n$ — правильный n-угольник в V_2, действует на плоскости V_2 и на множестве вершин или ребер $\mathcal{P}_n$ (в последних двух случаях имеет место гомоморфизм $\mathcal{D}_n \to S_n$)

Определение 1.25. Пусть группа G действует на множество Ω. *Орбитой* элемента $x \in \Omega$ называется $G(x) := \{g(x) : g \in G\}$.

Определение 1.26. Пусть группа G действует на множество Ω. Элементы $x, y \in \Omega$ называются *эквивалентными относительно действия* G, если $x \in G(y)$.

Утверждение 1.16. *Эквивалентность относительно действия является отношением эквивалентности, причем класс эквивалентности элемента $x \in \Omega$ — это $G(x)$.*

Доказательство. Произведем непосредственную проверку:

▷ (Рефлексивность) $e(x) = x$, поэтому $x \in G(x)$

▷ (Симметричность) Если $x \in G(y)$, то $x = g(y), g \in G$ и $g^{-1}(x) = g^{-1}(g(y)) = e(y) = y$, поэтому $y \in G(x)$

▷ (Транзитивность) Если $x = g(y), y = g'(z)$, то $x = (gg')(z)$ и $x \in G(z)$

□

Замечание. Если ω_1 и ω_2 эквивалентны, то $G(\omega_1) = G(\omega_2)$ по уже доказанному утверждению. Говорят, что всё Ω *разбивается на орбиты*; множество классов обозначатеся через Ω/G.

Пример. Рассмотрим действие $\mathcal{O}_n$ на $\mathbb{R}^n$, имеющее вид $A(x) = Ax$. Если на $\mathbb{R}^n$ введено стандартное скалярное произведение, то нетрудно показать, что $\mathcal{O}_n(x) = \{y \in \mathbb{R}^n : ||y|| = ||x||\}$.

Определение 1.27. Пусть группа G действует на множество Ω. *Стабилизатором*, или *станционарной подгруппой* элемента $x \in \Omega$ называется $\mathrm{St}(x) := \{g \in G : gx = x\}$.

Замечание. Очевидно, что $\mathrm{St}(x) \leqslant G$.

Утверждение 1.17. *Пусть* $x, y \in \Omega$, $y \in G(x)$, *причём* $y = g_0 x, g_0 \in G$. *Тогда*

$$\{g \in G\colon gx = y\} = g_0 \operatorname{St}(x) = \operatorname{St}(y) g_0$$

Доказательство.

1. $gx = y \Leftrightarrow g_0^{-1} gx = g_0^{-1} y = x \Leftrightarrow g_0^{-1} g \in \operatorname{St}(x) \Leftrightarrow g \in g_0 \operatorname{St}(x)$
2. $gx = y \Leftrightarrow g g_0^{-1} g_0 x = y \Leftrightarrow (g g_0^{-1}) y = y \Leftrightarrow g g_0^{-1} \in \operatorname{St}(y) \Leftrightarrow g \in \operatorname{St}(y) g_0$

□

Следствие. Если $x, y \in \Omega$ эквивалентны относительно действия G, $y = g_0 x, g_0 \in G$, то $\operatorname{St}(y) = g_0 \operatorname{St}(x) g_0^{-1}$, то есть $\operatorname{St}(x)$ и $\operatorname{St}(y)$ сопряжены.

Следствие. $|G(x)| = |G : \operatorname{St}(x)|$. В частности, если группа G конечна, то $|G(x)| = \frac{|G|}{|\operatorname{St}(x)|}$.

Доказательство. Построим биекцию $\varphi : G(x) \to G/\operatorname{St}(x)$ следующим образом:

$$\forall y \in G(x), y = g_0 x \quad \varphi(y) = \{g \in G : gx = y\} = g_0 \operatorname{St}(x)$$

Согласно уже доказаному утверждению, отображение корректно. Осталось проверить биективность:

▷ Инъективность. Пусть $\varphi(y) = \varphi(z)$, то

$$\{g \in G\colon gx = y\} = \{g \in G\colon gx = z\} \Longrightarrow \exists g \in \varphi(y),\ \ y = gx = z$$

▷ Сюръективность. Она выполнена по простой причине:

$$\forall g_1 \operatorname{St}(x) \in G/\operatorname{St}(x)\ \exists y = g_1 x \in \Omega \ \Big|\ \varphi(y) = g_1 \operatorname{St}(x)$$

□

Теорема 1.5. *(Формула орбит) Пусть группа* G *действует на конечное множество* Ω, $\Omega_1, \ldots, \Omega_k$ *— орбиты действия,* $x_i \in \Omega_i, i \in \{1, \ldots, k\}$ *— представители орбит. Тогда:*

$$|\Omega| = \sum_{i=1}^{k} |\Omega_i| = \sum_{i=1}^{k} |G : \operatorname{St}(x_i)|$$

Доказательство. Первое равенство тривиально, а второе справедливо в силу следствия из предыдущего утверждения. □

Пример. Группа G действует на себя *левыми сдвигами*, $\forall g, x \in G\ g(x) = gx$. Очевидно, это действие (а чтобы получить аналогичное действие *правыми сдвигами*, следует задать его как $g(x) = xg^{-1}$). Данное действие точно, и, более того, свободно. Оно определяет гомоморфизм $\varphi\colon G \to S(G)$, и, в силу точности, это мономорфизм, поэтому $G \cong \varphi(G) \leqslant S(G)$ — получена теорема Кэли.

Замечание. Пусть группа G действует на множества Ω_1 и Ω_2. Эти два действия называются *эквивалентными*, или *изоморфными*, если существует биекция $\mu\colon \Omega_1 \to \Omega_2$ такая, что

$$\forall g \in G\ \forall \omega \in \Omega_1\quad \mu(g(\omega)) = g(\mu(\omega))$$

В этом смысле действия G на себя левыми и правыми сдвигами изоморфны, и изоморфизм имеет вид $\mu(x) = x^{-1}$, $\forall g, x \in G\quad \mu(g(x)) = (gx)^{-1} = x^{-1}g^{-1} = g(\mu(x))$.

Пример. Пусть G — группа, $H \leqslant G$. Тогда G действует на G/H левыми сдвигами:

$$\forall g \in G : \forall xH \in G/H : g(xH) = gxH$$

Найдем $\mathrm{St}(xH)$:

$$g \in \mathrm{St}(xH) \Leftrightarrow gxH = xH \Leftrightarrow g^x = x^{-1}gxH = H \Leftrightarrow g \in H^{(x^{-1})}$$

Значит, если обозначить гомоморфизм действия как φ, то его ядро запишется следующим образом:

$$\operatorname{Ker}\varphi = \{g \in G\colon \forall xH \in G/H,\ g(xH) = xH\} = \bigcap_{x \in G} xHx^{-1}$$

Утверждение 1.18. *В рамках последнего примера, $K := \operatorname{Ker}\varphi$ является наибольшей по включению подгруппой H такой, что $K \trianglelefteqslant G$.*

Доказательство. Пусть $L \leqslant H$, $L \trianglelefteqslant G$. Тогда

$$\forall x \in G\quad L = x^{-1}Lx \leqslant x^{-1}Hx \Rightarrow L \leqslant K$$

□

Упражнение. *Пусть $H \leqslant G$, $|G : H| = n \in \mathbb{N}$. Докажите, что тогда верно следующее:*

$$\exists K \leqslant H, K \trianglelefteqslant G \;\big|\; |G : K| \leqslant n!$$

Пример. Группа G действует на себя сопряжениями:

$$\forall g, x \in G\quad g(x) := x^{g^{-1}} = gxg^{-1}$$

Проверим, что это действительно действие (это же и объяснит, почему надо именно так его определять):

1. $$\forall g_1, g_2, x \in G\quad g_1(g_2(x)) = g_1g_2xg_2^{-1}g_1^{-1} = (g_1g_2)x(g_1g_2)^{-1} = (g_1g_2)(x)$$

2. $$\forall x \in G\quad e(x) = exe^{-1} = x$$

Определение 1.28. Рассмотрим действие группы G на себя сопряжениями. Тогда *стабилизатор элемента $x \in G$* носит собственное название — *централизатор элемента $C_G(x)$*:

$$C_G(x) = \{g \in G\colon gxg^{-1} = x\} = \{g \in G\colon gx = xg\}$$

Определение 1.29. Рассмотрим действие группы G на себя сопряжениями ($\varphi\colon G \to S(G)$). Тогда *центром группы* G называется ядро этого действия:

$$\operatorname{Ker}\varphi = \{g \in G\colon \forall x \in G\ gx = xg\} = \bigcap_{x\in G} \operatorname{St}(x)$$

Замечание. Легко видеть, что $C_G(x)$ — это наибольшая по включению подгруппа $H \leqslant G$ такая, что $x \in H$ и $x \in Z(H)$.

Действительно, x коммутирует со всеми элементами $C_G(x)$, причём мы взяли все такие элементы.

Утверждение 1.19. *Пусть G — конечная группа, действующая на себя сопряжениями, и $a \in G$. Тогда $|a^G| \mid \frac{|G|}{\operatorname{ord} a}$.*

Доказательство. Поскольку a^G — орбита a относительно действия сопряжениями, $|a^G| = |G : \operatorname{St}(a)| = |G : C_G(a)| = \frac{|G|}{|C_G(a)|}$. Заметим, что $a \in C_G(a)$, тогда $\langle a\rangle \leqslant C_G(a)$ и $\operatorname{ord} a = |\langle a\rangle| \mid |C_G(a)| = \frac{|G|}{|a^G|}$, поэтому $|a^G| \mid \frac{|G|}{\operatorname{ord} a}$. □

Определение 1.30. Все автоморфизмы группы G образуют *группу автоморфизмов* $\operatorname{Aut} G \leqslant S(G)$. Автоморфизм $\psi \in \operatorname{Aut} G$ называется *внутренним*, если $\psi = I_g$ для некоторого $g \in G$. Множество всех внутренних автоморфизмов обозначается как $\operatorname{Inn} G$.

Замечание. Тогда если $\varphi\colon G \to S(G)$ — гомоморфизм действия группы сопряжениями на себя, то $\operatorname{Im}\varphi = \operatorname{Inn} G \leqslant \operatorname{Aut} G$. Более того, поскольку $\operatorname{Im}\varphi = \operatorname{Inn} G$ и $\operatorname{Ker}\varphi = Z(G)$, то, по основной теореме о гомоморфизме, $\operatorname{Inn} G \cong G/Z(G)$.

Пример. Рассмотрим несколько примеров внутренних автоморфизмов:

1. Если группа G — абелева, то $\operatorname{Inn} G = \{\mathrm{id}\}$
2. Если $G = S_n, n \geqslant 3$, то $Z(S_n) = \{e\}$ (поскольку каждая перестановка в $Z(S_n)$ должна коммутировать со всеми транспозициями), следовательно, $\operatorname{Inn} G \cong S_n$

Упражнение. *Докажите, что* $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$.

Определение 1.31. Естественно, множество $\operatorname{Aut} G \setminus \operatorname{Inn} G$ называется *множеством внешних автоморфизмов группы* G.

Пример. Пусть G — группа, Ω — множество всех подгрупп в G. Тогда G действует на Ω сопряжениями:

$$\forall H \in \Omega, g \in G\ \ g(H) = gHg^{-1}$$

Определение 1.32. Пусть группа G действует на множество всех своих подгрупп. Тогда для $H \leqslant G$ *нормализатором* называется её стабилизатор:

$$N(H) := \operatorname{St}(H) = \{g \in G\colon gHg^{-1} = H\} = \{g \in G\colon gH = Hg\}$$

Замечание. $N(H)$ является наибольшей по включению подгруппой в G такой, что H нормальна в этой подгруппе.

Определение 1.33. Конечная группа G называется *p-группой*, если $|G| = p^n$, где $n \in \mathbb{N}$, p — простое число.

Теорема 1.6. *Пусть G — p-группа. Тогда $Z(G) \neq \{e\}$.*

Доказательство. Рассмотрим действие G сопряжениями на себя и воспользуемся формулой орбит:

$$|\Omega| = |G| = \sum_i |\Omega_i| = \sum_i |x_i^G|$$

Заметим такую цепочку равносильных утверждений:

$$g \in Z(G) \Leftrightarrow C_G(g) = G \Leftrightarrow g^G = \{g\}$$

Значит, среди представителей орбит есть такие, что их орбита состоит только из них. Не умаляя общности, скажем, что такими были только первые l. Получим такое равенство:

$$p^n = |G| = \sum_{i=1}^{k} |x_i^G| = \underbrace{|Z(G)|}_{l} + \sum_{i=l+1}^{k} |G \colon C_G(x_i)|$$

Что можно сказать про оставшиеся слагаемые? Так как элементы с $C_G(g) = G$ лежат только в центре, то индексы оставшихся заведомо больше единицы. При этом как $|G|$, так и $|C_G(x_i)|$ кратны p. Стало быть, вся сумма делится на p и оставшееся слагаемое - тоже:

$$p \mid l = |Z(G)| \geqslant 1 \Longrightarrow |Z(G)| \geqslant p$$

□

Пример. Не все p-группы являются абелевыми. Рассмотрим, например, $G \leqslant \mathrm{GL}_3(\mathbb{Z}_p)$ — верхнетреугольные матрицы с единичной диагональю. Тогда $|G| = p^3$, и легко показать, что в G есть некоммутирующие элементы.

С другой стороны, если G — такая конечная группа, что $|G| = p$, то $\forall g \in G \backslash \{e\} : \mathrm{ord}\, g = p$ по теореме Лагранжа, тогда G — циклическая и потому абелева.

Теорема 1.7. *Пусть G — неабелева группа. Тогда $G/Z(G)$ не является циклической.*

Доказательство. По условию, $Z(G) \neq G$, и, как уже было показано, $Z(G) \trianglelefteqslant G$. Предположим, что $G/Z(G) = \langle aZ(G) \rangle$ для некоторого $a \in G$. Пусть $g_1, g_2 \in G$, тогда $g_1 Z(G) = a^{n_1} Z(G)$ и $g_2 Z(G) = a^{n_2} Z(G)$ в силу нормальности $Z(G)$, поэтому $g_1 = a^{n_1} z_1$ и $g_2 = a^{n_2} z_2$, $z_1, z_2 \in Z(G)$. Тогда $g_1 g_2 = a^{n_1} z_1 a^{n_2} z_2 = a^{n_2} z_2 a^{n_1} z_1 = g_2 g_1$, и, в силу произвольности g_1, g_2, G — абелева, но это неверно. □

Следствие. Пусть G — такая конечная группа, что $|G| = p^2$. Тогда G — абелева.

Доказательство. Предположим, что G не является абелевой, то есть $Z(G) \neq G$, тогда $|Z(G)| = p$, поскольку центр нетривиален. Но тогда $|G/Z(G)| = p$ и группа $G/Z(G)$ — циклическая, следовательно, G является абелевой — противоречие. □

1.5 Лемма Бернсайда

Определение 1.34. Действие группы G на множестве Ω называется *транзитивным*, если Ω является единственной орбитой действия. Иными словами, $\forall \omega_1, \omega_2 \in \Omega : \exists g \in G : g(\omega_1) = \omega_2$.

Пример. S_n действует на $\{1, \ldots, n\}$ транзитивно, а $S_{n-1} \leqslant S_n$ действует на $\{1, \ldots, n\}$ нетранзитивно.

Теорема 1.8 (Лемма Бернсайда)**.** *Пусть конечная группа G действует на множестве Ω транзитивно. Для $\forall g \in G$ обозначим $F(g) := |\{\omega \in \Omega : g\omega = \omega\}|$. Тогда:*

$$\sum_{g \in G} F(g) = |G|$$

Доказательство. Положим $S := \{(g, \omega) \in G \times \Omega \colon g\omega = \omega\}$. Посчитаем это множество двумя способами:

- ▷ С одной стороны, можно просуммировать множество пар при фиксированном ω. Это будет ничто иное как $\operatorname{St}(\omega)$:

$$|S| = \sum_{\omega \in \Omega} |\operatorname{St}(\omega)| = \sum_{\omega \in \Omega} \frac{|G|}{|G(\omega)|} = \sum_{\omega \in \Omega} \frac{|G|}{|\Omega|} = |G|$$

- ▷ С другой стороны, можно написать аналогичную сумму по преобразованиям $g \in G$:

$$|S| = \sum_{g \in G} |\{\omega \in \Omega \colon g\omega = \omega\}| = \sum_{g \in G} F(g)$$

$\square$

Следствие (Лемма Бернсайда, другая формулировка)**.** Пусть конечная группа G действует на множестве Ω, $F(g)$ определено как в последней теореме. Тогда:

$$|\Omega/G| = \frac{1}{|G|} \sum_{g \in G} F(g)$$

Доказательство. Пусть $k := |\Omega/G|$. Представим Ω в виде $\Omega = \bigsqcup_{i=1}^{k} \Omega_i$, где $\Omega_1, \ldots, \Omega_k$ — орбиты действия. Тогда $\forall i \in \{1, \ldots, k\} : G$ действует на Ω_i транзитивно (значит, в частности, Ω конечно). Для $\forall g \in G$ положим $F_i(g) := |\{\omega \in \Omega_i : g\omega = \omega\}|$ и воспользуемся леммой Бернсайда:

$$\sum_{g \in G} F(g) = \sum_{g \in G} \sum_{i=1}^{k} F_i(g) = \sum_{i=1}^{k} |G| = k|G| \Rightarrow k = \frac{1}{|G|} \sum_{g \in G} F(g)$$

$\square$

Замечание. Формально стоит требовать $|\Omega| < \infty$ в последнем следствии, но, вообще говоря, даже так равенство будет выполнено (с двух сторон просто могут быть бесконечности из-за $|\Omega| = +\infty$).

Пример. Рассмотрим ожерелья из p бусинок ($p > 2$ — простое число), в которых каждая бусинка покрашена в один из k цветов. Найдем количество различных ожерелий (с точностью до поворота и переворота). Пусть Ω — множество неподвижных ожерелий, то есть не допускающих повороты и перевороты, тогда $|\Omega| = k^p$. Группа $G = \mathcal{D}_p$ действует на Ω, и искомая величина — это $|\Omega/G|$, поскольку элементы одной орбиты отличаются друг от друга только композицией поворотов и переворотов. Элементы G имеют один из следующих видов:

- ▷ Если $g = \mathrm{id}$, то $F(g) = |\Omega| = k^p$
- ▷ Если g — поворот на $2\pi\frac{k}{p}$, $0 < k < p$, то $F(g) = k$ в силу простоты p, поскольку любая фиксированная бусинка совпадает по цвету с бусинками, в которые она переходит при повороте на $2\pi\frac{k}{p}, 2\pi\frac{2k}{p}, \ldots, 2\pi\frac{(p-1)k}{p}$, и полученные таким образом бусинки образуют все ожерелье
- ▷ Если g — переворот, то есть симметрия, то $F(g) = k^{\frac{p+1}{2}}$, поскольку $\frac{p+1}{2}$ подряд идущих бусинок, начиная с той, через которую проходит ось симметрии, однозначно задают цвета оставшихся

Применим теперь лемму Бернсайда:

$$|\Omega/G| = \frac{k^p + (p-1)k + pk^{\frac{p+1}{2}}}{2p}$$

Следствие. При помощи леммы Бернсайда, либо из этого примера, либо из аналогичного без отражений, можно доказать малую теорему Ферма.

Определение 1.35. Пусть G действует на множестве Ω. Обозначим за $\Omega^{[k]}$ такое множество:

$$\Omega^{[k]} = \{(\omega_1, \ldots, \omega_k) \in \Omega^k \colon i \neq j \Rightarrow \omega_i \neq \omega_j\}$$

Действие *называется k-транзитивным*, если выполнено условие:

$$\forall (\omega_1, \ldots, \omega_k), (\delta_1, \ldots, \delta_k) \in \Omega^{[k]}\ \exists g \in G \colon (g\omega_1, \ldots, g\omega_k) = (\delta_1, \ldots, \delta_k)$$

Другими словами, G действует на $\Omega^{[k]}$ транзитивно.

Упражнение. *Пусть группа G действует на множестве Ω, причем действие 2-транзитивно. Для $\forall g \in G$ обозначим $F(g) := |\{a \in \Omega : ga = a\}|$. Докажите, что выполнено следующее равенство:*

$$\sum_{g \in G} F(g)^2 = 2|G|$$

2 Виды групп и теоретико-групповые конструкции

2.1 Прямое произведение групп

Определение 2.1. Пусть A, B — группы. Тогда их *(внешним) прямым произведением* называется группа $G = A \times B$ со следующей операцией:

$$\forall (a_1, b_1), (a_2, b_2) \in G \quad (a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

Замечание. Действительно, G является группой: ассоциативность очевидна, нейтральный элемент в G — это $e = (e_A, e_B)$, и $\forall (a, b) \in G \quad (a, b)^{-1} = (a^{-1}, b^{-1})$.

Утверждение 2.1. *Пусть A, B — группы, $G = A \times B$. Тогда:*

1. $A \times \{e_B\} \trianglelefteq G$, $\{e_A\} \times B \trianglelefteq G$
2. $A \times B \cong B \times A$
3. *Если C — группа, то* $(A \times B) \times C \cong A \times (B \times C)$

Доказательство.

1. Очевидно, $A \times \{e_B\} \leqslant G$, и, более того:

   $$\forall (a, e_B) \in A \times \{e_B\}, (a', b') \in G \quad (a', b')(a, e_B)((a')^{-1}, (b')^{-1}) = (a^{(a')^{-1}}, e_B) \in A \times \{e_B\}$$

   Поэтому $A \times \{e_B\} \trianglelefteq G$ (вторая часть утверждения доказывается аналогично)

2. Предъявим изоморфизм: $(a, b) \mapsto (b, a)$
3. Предъявим изоморфизм: $((a, b), c) \mapsto (a, (b, c))$

□

Замечание. В силу «ассоциативности» прямого произведения, мы будем опускать скобки в прямых произведениях трех и более групп, записывая их в следующем виде:

$$A_1 \times \dots \times A_k = \prod_{i=1}^{k} A_i = \{(a_1, \dots, a_k) : a_1 \in A_1, \dots, a_k \in A_k\}$$

Утверждение 2.2. *Пусть A, B — группы, $A_1 \trianglelefteq A, B_1 \trianglelefteq B$. Тогда $A_1 \times B_1 \trianglelefteq A \times B$, при этом $(A \times B)/(A_1 \times B_1) \cong (A/A_1) \times (B/B_1)$.*

Доказательство. Пусть $\pi_A : A \to A/A_1$, $\pi_B : B \to B/B_1$ — канонические эпиморфизмы. Рассмотрим $\pi := \pi_A \times \pi_B : (A \times B) \to (A/A_1) \times (B/B_1)$ — такое отображение, что $\forall (a, b) \in A \times B : \pi((a, b)) = (\pi_A(a), \pi_B(b))$. Тогда π — это гомоморфизм, причем сюръективный в силу сюръективности π_A, π_B. $\operatorname{Im} \pi = (A/A_1) \times (B/B_1)$, $\operatorname{Ker} \pi = \operatorname{Ker} \pi_A \times \operatorname{Ker} \pi_B = A_1 \times B_1$, и, следовательно, $A_1 \times B_1 \trianglelefteq A \times B$. Наконец, по основной теореме о гомоморфизме, $(A \times B)/(A_1 \times B_1) \cong (A/A_1) \times (B/B_1)$, причем изоморфизм имеет следующий вид: $(a, b)(A_1 \times B_1) \mapsto (aA_1, bB_1)$. □

Замечание. Легко видеть, что $A \times \{e_B\} \cong A$, $\{e_A\} \times B \cong B$, поэтому далее мы будем отождествлять эти подгруппы с A и B. Тогда, по утверждению выше:

$$(A \times B)/A \cong (A/A) \times (B/\{e_B\}) \cong \{A\} \times B \cong B$$

Замечание. Если группы A и B — абелевы, их прямое произведение часто обозначается как $A \oplus B$.

Теорема 2.1. *Пусть G — группа, $A, B \trianglelefteq G$, причем $A \cap B = \{e\}$ и $AB = G$. Тогда $G \cong A \times B$.*

Доказательство. Сначала заметим, что есть коммутативность такого вида: $\forall a \in A, b \in B$ $ab = ba$. Действительно, проверим это так:

$$ab(ba)^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in A \cap B \Rightarrow ab(ba)^{-1} = e \Rightarrow ab = ba$$

Построим изоморфизм $\varphi\colon A \times B \to G$ следующим образом: $\varphi((a, b)) = ab$. Проверим свойства изоморфизма:

▷ Гомоморфизм:

$$\forall (a_1, b_1), (a_2, b_2) \in A \times B \quad \varphi((a_1, b_1)(a_2, b_2)) = (a_1 a_2)(b_1 b_2) = (a_1 b_1)(a_2 b_2) = \varphi((a_1, b_1)) \cdot \varphi((a_2, b_2))$$

▷ Инъективность:

$$\operatorname{Ker} \varphi = \{(a, b) \in A \times B \colon ab = e\} = \{(a, b) \in A \times B \colon a = b^{-1}\} = \{(e, e)\}$$

▷ Сюръективность: $\operatorname{Im} \varphi = AB = G$

Значит, φ действительно является изоморфизмом G и $A \times B$. □

Определение 2.2. Если G — группа, $A, B \trianglelefteq G$, причём $A \cap B = \{e\}$ и $AB = G$, то G называется *внутренним прямым произведением* своих подгрупп A и B.

Определение 2.3. Пусть G — группа, $A \trianglelefteq G$, $B \leqslant G$. Если $A \cap B = \{e\}$ и $AB = G$, то G называется *полупрямым произведением* A и B. Обозначение — $G = A \leftthreetimes B$.

Замечание. Рассмотрим канонический эпиморфизм $\pi\colon G \to G/A$ (в обозначениях определения выше). Тогда, по первой теореме об изоморфизме, $G/A = AB/A \cong B/(A \cap B) \cong B$, как и в случае внутреннего прямого произведения.

Пример. Рассмотрим несколько полупрямых произведений:

1. $S_n = A_n \leftthreetimes \langle (12) \rangle$ (если $n \geqslant 2$)
2. $S_4 = V_4 \leftthreetimes S_3$

Замечание. Пусть G — группа, $A \trianglelefteq G$, $B \leqslant G$, и $G = A \leftthreetimes B$. Рассмотрим действие B на A сопряжениями: $\forall b \in B, a \in A$ $b(a) = bab^{-1} \in A$, поскольку $A \trianglelefteq G$. Данному действию соответствует гомоморфизм $\varphi\colon B \to S(A)$. Более того, поскольку $\forall b \in B$ $bAb^{-1} = A$ и сопряжение с помощью b^{-1} — это автоморфизм G, то это также автоморфизм A. Значит, на самом деле $\varphi\colon B \to \operatorname{Aut} A \leqslant S(A)$. Структура полупрямого произведения однозначно (точнее, не более чем однозначно) задается группами A, B и гомоморфизмом φ (здесь, в отличие от внутреннего произведения, нет коммутативности между элементами из A и B):

$$(a_1b_1)(a_2b_2) = a_1b_1a_2b_2 = a_1(b_1a_2b_1^{-1})b_1b_2 = a_1\varphi_{b_1}(a_2)b_1b_2$$

Определение 2.4. Пусть A, B — группы, $\varphi : B \to \operatorname{Aut} A$. Определим на $G = A \times B$ операцию следующим образом: $\forall (a_1, b_1), (a_2, b_2) \in G : (a_1, b_1)(a_2, b_2) = (a_1\varphi_{b_1}(a_2), b_1b_2)$. Полученная конструкция называется *полупрямым произведением* A *и* B*, заданным гомоморфизмом* φ. Обозначение — $G = A \leftthreetimes_\varphi B$.

Упражнение. *Докажите, что* $G = A \leftthreetimes_\varphi B$ *является группой, причем* $A \leftthreetimes_\varphi \{e_B\} \cong A$, $\{e_A\} \leftthreetimes_\varphi B \cong B$ *и* $G = A \leftthreetimes B$ *(в смысле первого определения).*

Замечание. Если группа G является полупрямым произведением $A \trianglelefteqslant G$ и $B \leqslant G$, и $\varphi : B \to \operatorname{Aut} A$ — соответствующий действию B на A сопряжениями гомоморфизм, то, как и в случае прямого произведения, $A \leftthreetimes_\varphi B \cong G$, и изоморфизм имеет вид $(a, b) \mapsto ab$.

Отметим также, что прямое произведение является частным случаем полупрямого: гомоморфизм, описанный выше, каждому элементу $b \in B$ сопоставляет $\varphi_b = \mathrm{id}$.

2.2 Коммутант группы

Определение 2.5. Пусть G — группа, $x, y \in G$. *Коммутатором* элементов x и y называется элемент $[x, y] := xyx^{-1}y^{-1}$.

Утверждение 2.3. *Пусть* G *— группа,* $x, y \in G$*. Тогда:*

1. $xy = [x, y]yx$
2. $xy = yx \Leftrightarrow [x, y] = e$
3. $[x, y]^{-1} = [y, x]$
4. $\forall g \in G : [x, y]^g = [x^g, y^g]$

Доказательство.

1. $[x, y]yx = xyx^{-1}y^{-1}yx = xy$
2. $xy = yx \Leftrightarrow xyx^{-1}y^{-1} = e \Leftrightarrow [x, y] = e$
3. $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$
4. Данное равенство можно проверить непосредственно, но оно следует из того, что сопряжение с помощью $g \in G$ — это автоморфизм G

□

Замечание. Пусть $\varphi : G \to A$ — гомоморфизм групп G и A, причем A — абелева. Тогда $\varphi([x, y]) = [\varphi(x), \varphi(y)] = e$, поскольку $\varphi(x)$ и $\varphi(y)$ коммутируют.

Определение 2.6. Пусть G — группа. *Коммутантом* группы G называется $G' := \langle [x, y] : x, y \in G\rangle \leqslant G$. Рекурсивно определяется *n-ный коммутант* $G^{(n)} := (G^{(n-1)})' \leqslant G^{(n-1)}$.

Определение 2.7. Пусть G — группа, $K, H \leqslant G$. *Взаимным коммутантом* K и H называется $[K, H] := \langle [k, h] : k \in K, h \in H \rangle$.

Замечание. Определения имеют именно такой вид, потому что возможна ситуация, когда $\{[x, y] : x, y \in G\}$ не является подгрупой в G. Отметим также, что $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$.

Утверждение 2.4. *Пусть $\varphi : G \to H$ — гомоморфизм групп G и H. Тогда $\varphi(G') \leqslant H'$. Более того, если φ — эпиморфизм, то $\varphi(G') = H'$.*

Доказательство. Поскольку $G' = \langle [x, y] : x, y \in G \rangle$, то $\varphi(G') = \langle \varphi([x, y]) : x, y \in G \rangle = \langle [\varphi(x), \varphi(y)] : x, y \in G \rangle \leqslant \langle [p, q] : p, q \in H \rangle$. Если же φ — эпиморфизм, то последнее включение тоже становится равенством. $\square$

Следствие. Пусть G — группа, $K \trianglelefteqslant G$. Тогда $K' \trianglelefteqslant G$.

Доказательство. Рассмотрим $g \in G$. Сопряжение с помощью g — это автоморфизм $I_g : G \to G$, $\forall x \in G : I_g(x) = x^g$. Следовательно, $I_g(K) = K$, то есть $I_g|_K : K \to K$ — автоморфизм, и, по утверждению выше, $I_g(K') = K'$, тогда, в силу произвольности g, $K' \trianglelefteqslant G$. $\square$

Следствие. $G' \trianglelefteqslant G$, и, по индукции, $\forall n \in \mathbb{N} : G^{(n)} \trianglelefteqslant G$.

Теорема 2.2. *Пусть G — группа. Тогда:*

1. *Если $G' \leqslant K \leqslant G$, то $K \trianglelefteqslant G$ и G/K — абелева.*
2. *Если $K \trianglelefteqslant G$ и G/K — абелева, то $G' \leqslant K$.*

Доказательство.

1. Рассмотрим канонический эпиморфизм $\pi : G \to G/G'$. Тогда $\{G'\} = \pi(G') = (G/G')'$. Поскольку G' — нейтральный элемент в G/G', все коммутаторы в G/G' единичны, поэтому G/G' — абелева. По второй теореме об изоморфизме, подгруппе $G' \leqslant K \leqslant G$ соответствует $\overline{K} = K/G' \leqslant \overline{G} = G/G'$, и, более того, $\overline{K} \trianglelefteqslant \overline{G} \Leftrightarrow K \trianglelefteqslant G$. Поскольку $\overline{G}$ — абелева, $\overline{K} \trianglelefteqslant \overline{G}$, значит, и $K \trianglelefteqslant G$. Наконец, $G/K \cong \overline{G}/\overline{K}$ — абелева группа.
2. Рассмотрим канонический эпиморфизм $\pi : G \to G/K$. Тогда $\pi(G') = (G/K)' = \{K\}$. Значит, $G' \leqslant \operatorname{Ker} \pi = K$.

$\square$

Замечание. Согласно теореме выше, G' — наименьшая по включению нормальная подгруппа в G такая, что G/G' — абелева.

Упражнение. *Пусть G — группа, $H \trianglelefteqslant G$, $K = [G, H]$. Докажите, что K — это наименьшая нормальная подгруппа в G такая, что $H/K \leqslant Z(G/K)$.*

Определение 2.8. Пусть G — группа, $M \subset G$. *Нормальной подгруппой, порожденной M*, называется $\langle M \rangle_{norm} = \bigcap_{\substack{H \trianglelefteqslant G \\ M \subset H}} H$

Замечание. Конечно, $\langle M \rangle_{norm} \trianglelefteqslant G$ как пересечение некоторого числа нормальных подгрупп.

Утверждение 2.5. *Пусть G — группа, $M \subset G$. Тогда $\langle M \rangle_{norm} = \langle M^G \rangle$.*

Доказательство.

- $\geqslant$ Если $H \trianglelefteq G$, $M \subset H$, то, в силу нормальности группы H, $M^G \subset H$, тогда $M^G \subset \langle M \rangle_{norm}$, и, так как $\langle M \rangle_{norm}$ — группа, $\langle M^G \rangle \leqslant \langle M \rangle_{norm}$

- $\leqslant$ Заметим, что $\forall g \in G \ \ (M^G)^g = M^G$. Следовательно:

$$\forall g \in G \quad \langle M^G \rangle = \bigcap_{\substack{H \leqslant G \\ M^G \subset H}} H = \bigcap_{\substack{H \leqslant G \\ M^G \subset H^{(g^{-1})}}} H = \bigcap_{\substack{K \leqslant G \\ M^G \subset K}} K^g = \left(\bigcap_{\substack{K \leqslant G \\ M^G \subset K}} K \right)^g = \langle M^G \rangle^g$$

  То есть $\langle M^G \rangle \trianglelefteq G$, и поэтому $\langle M \rangle_{norm} \leqslant \langle M^G \rangle$

Поскольку доказаны оба включения, $\langle M \rangle_{norm} = \langle M^G \rangle$. □

Утверждение 2.6. *Пусть G — группа, $M \subset G$, $G = \langle M \rangle$. Тогда $G' = \langle [m_1, m_2] \colon m_1, m_2 \in M \rangle_{norm}$.*

Доказательство. Обозначим $\langle [m_1, m_2] \colon m_1, m_2 \in M \rangle_{norm}$ через H и докажем, что $H = G'$.

- $\leqslant$ Поскольку все коммутаторы лежат в G' и $G' \trianglelefteq G$, то $H \leqslant G'$

- $\geqslant$ Рассмотрим канонический эпиморфизм $\pi \colon G \to G/H$, тогда $\forall m_1, m_2 \in M \colon [\overline{m_1}, \overline{m_2}] = \overline{[m_1, m_2]} = e$, тогда, поскольку $G/H = \langle \overline{m} \colon m \in M \rangle$, то G/H — абелева, и потому $G' \leqslant H$

□

Замечание. Центр и коммутант группы G показывают, насколько G «близка» к абелевой группе: для абелевой группы A верно, что $Z(A) = A$, $A' = \{e\}$.

2.3 Разрешимые группы

Определение 2.9. Группа G называется *разрешимой*, если $\exists n \in \mathbb{N} : G^{(n)} = \{e\}$. Наименьшее $n \in \mathbb{N}$, для которого это выполнено, называется *степенью разрешимости* G.

Замечание. Разрешимые группы степени 1 — это абелевы группы. Разрешимые группы степени 2 часто называют *метаабелевыми.*

Замечание. Если G — конечная группа, то последовательность вида $G \geqslant G' \geqslant G'' \geqslant \ldots$ обязательно стабилизируется, но необязательно на $\{e\}$.

Утверждение 2.7. *Пусть G — разрешимая группа, $H \leqslant G$. Тогда H тоже разрешима.*

Доказательство. Достаточно заметить, что $H \leqslant G \Rightarrow H' \leqslant G' \Rightarrow \cdots \Rightarrow H^{(n)} \leqslant G^{(n)} = \{e\}$. □

Теорема 2.3. *Пусть G — группа, $K \trianglelefteq G$. Тогда G разрешима $\Leftrightarrow$ K и G/K разрешимы.*

Доказательство.

- $\Rightarrow$ Если G разрешима, то $K \leqslant G$ разрешима, и, поскольку при каноническом эпиморфизме $\pi \colon G \to G/K$ выполнено равенство $\pi(G') = (G/K)'$, то, по индукции, $(G/K)^{(n)} = \pi(G^{(n)}) = \{K\}$

$\Leftarrow$ Если $K^{(m)} = \{e\}$ и $(G/K)^{(n)} = \{K\}$, то, снова рассматриавя канонический эпиморфизм, получаем, что $\pi(G^{(n)}) = (G/K)^{(n)} = \{K\} \Rightarrow G^{(n)} \leqslant \operatorname{Ker} \pi = K \Rightarrow G^{(n+m)} \leqslant K^{(m)} = \{e\}$

□

Следствие. Пусть G — группа, $K_1, K_2 \trianglelefteq G$ разрешимы. Тогда группа K_1K_2 разрешима.

Доказательство. Заметим, что $K_1 \trianglelefteq K_1K_2$ и, по первой теореме об изоморфизме, $K_1K_2/K_1 \cong K_2/(K_1 \cap K_2)$. Группы K_1 и K_1K_2/K_1 разрешимы, поэтому K_1K_2 разрешима. □

Следствие. Пусть G — конечная группа. Тогда в G существует наибольшая по включению разрешимая нормальная подгруппа K.

Доказательство. Пусть $K_1, \ldots, K_m \trianglelefteq G$ — это все разрешимые нормальные подгруппы в G. Тогда, обобщая предыдущее следствие на случай m нормальных подгрупп в G по индукции, получаем, что $K = K_1 \cdots K_m \trianglelefteq G$ — нормальная разрешимая подгруппа, причем $K_1, \ldots, K_m \leqslant K$. □

Пример. (Применение доказанных следствий для разрешимости групп)

A_4 — разрешимая подгруппа. Действительно, $V_4 \trianglelefteq A_4$ — абелева, а также $A_4/V_4 \cong \mathbb{Z}_3$ — тоже абелева.

S_4 — разрешимая группа. В самом деле, теперь $A_4 \trianglelefteq S_4$, причём $S_4/A_4 \cong \mathbb{Z}_2$ — абелева группа.

Утверждение 2.8. *Если G — p-группа, то G разрешима.*

Доказательство. Пусть $|G| = p^n$. Будем вести индукцию по n:

- База $n = 1$: если $|G| = p$, то $G \cong \mathbb{Z}_p$ — циклическая и, в частности, абелева, а потому разрешима.
- Переход $n > 1$: по теореме о центре p-группы уже знаем, что $Z(G) \neq \{e\}$. Если $Z(G) = G$, то группа абелева и всё доказано. Иначе $|Z(G)|, |G/Z(G)| < p^n$ — это p-группы меньшего порядка. Пользуясь предположением индукции, получаем, что они обе разрешимы. Тогда и G разрешима.

□

Теорема 2.4. *Пусть G — группа. Тогда следующие утверждения эквивалентны:*

1. *G разрешима*
2. *В G существует ряд $G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_n = \{e\}$ такой, что $\forall i \in \{1, \ldots, n\}$ $G_i \trianglelefteq G$ и G_{i-1}/G_i — абелева (нормальный ряд с абелевыми факторами)*
3. *В G существует ряд $G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_n = \{e\}$ такой, что $\forall i \in \{1, \ldots, n\}$ $G_i \trianglelefteq G_{i-1}$ и G_{i-1}/G_i — абелева (субнормальный ряд с абелевыми факторами)*

Доказательство.

▷ (1 ⇒ 2) Достаточно расмотреть ряд $G \geqslant G' \geqslant \ldots \geqslant G^{(n)} = \{e\}$, и по свойствам коммутантов все необходимые свойства будут выполнены.

▷ (2 ⇒ 3) Заметим, что нормальный ряд также является и субнормальным: если $\forall i \in \{1, \ldots, n\}\ G_i \trianglelefteqslant G$, то $\forall i \in \{1, \ldots, n\}\ G_i \trianglelefteqslant G_{i-1}$.

▷ (3 ⇒ 1) Докажем, что $\forall i \in \{0, \ldots, n\}\ G^{(i)} \leqslant G_i$, по индукцией по i:

- База $i = 0$: тривиально
- Переход $i > 0$: поскольку $G_i \trianglelefteqslant G_{i-1}$ и G_{i-1}/G_i — абелева, то $(G_{i-1})' \leqslant G_i$. Это доказывает переход индукции:

$$G^{(i)} = (G^{(i-1)})' \leqslant (G_{i-1})' \leqslant G_i$$

Остаётся посмотреть на последний член субнормального ряда: $\{e\} = G_n \geqslant G^{(n)}$ по доказанной индукции.

□

Замечание. В доказательстве выше мы предъявили существование ряда, явно построив его из коммутантов группы. Несложно понять, что наименьшая длина нормального или субнормального ряда с абелевыми факторами — всегда степень разрешимости G.

Замечание. Мы могли бы доказать разрешимость S_4, сославшись на соответствующий ряд:

$$\{e\} \trianglelefteqslant V_4 \trianglelefteqslant S_4$$

Следствие. Если G — разрешимая группа, то $G' \neq G$.

Теорема 2.5. *Пусть G — p-группа, $|G| = p^n$. Тогда $\forall k \in \mathbb{N}, k \leqslant n\ \exists H \trianglelefteqslant G\ |H| = p^k$.*

Доказательство. Проведём индукцию по n:

▷ База $n = 1$: доказывать нечего

▷ Переход $n > 1$: пусть $Z = Z(G) \neq \{e\}$. Пусть $e \neq a \in Z$. Тогда $\operatorname{ord} a = p^l$. Стало быть, $\operatorname{ord} a^{p^{l-1}} = p$ — нашли элемент порядка p. Обозначим $b = a^{p^{l-1}}$, тогда $K = \langle b \rangle \leqslant Z$, $|K| = p$ и $K \trianglelefteqslant G$ как подгруппа центра.

Если надо было найти ответ для $k = 1$, то мы это уже сделали. Иначе рассмотрим канонический эпиморфизм $\pi\colon G \to G/K$, тогда $\overline{G} = G/K$, $|\overline{G}| = p^{n-1}$. По предположению индукции, существует $\overline{L} \trianglelefteqslant \overline{G}$, $|\overline{L}| = p^{k-1}$. По второй теореме об изоморфизме $\overline{L} \mapsto L$, причём $L \trianglelefteqslant G$ из-за $\overline{L}$. Остаётся заметить, что $|L| = p^{k-1} \cdot p = p^k$

□

Замечание. Термин «разрешимости» пришёл из теории Галуа. Эваристу Галуа удалось построить для уравнений с рациональными многочленами некоторую группу и показать, что уравнение разрешимо в радикалах тогда и только тогда, когда соответствующая группа будет разрешимой.

2.4 Простые группы

Определение 2.10. Пусть G — группа, $|G| > 1$. G называется *простой*, если в ней нет нормальных подгрупп, отличных от $\{e\}$ и G.

Замечание. Пусть G — конечная разрешимая группа. Рассмотрим максимальный субнормальный ряд (факторы не обязательно абелевы, поэтому разрешимость мы не затрагиваем. Требуется лишь нормальность) $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_n = \{e\}$, в котором все группы различны. Тогда $\forall i \in \{1, \dots, n\}$ G_{i-1}/G_i — простая, поскольку иначе $\exists H/G_i \trianglelefteq G_{i-1}/G_i$ и, по второй теореме об изоморфизме, $H \trianglelefteq G_{i-1}$. При этом $G_i \trianglelefteq H$, коль скоро G_i нормальна в бо́льшей группе G_{i-1}. Стало быть, можем вставить H в наш ряд, а это невозможно по максимальности.

Замечание. Существует *теорема Жордана-Гёльдера*, гласящая, что в любых двух наибольших по включению нормальных (субнормальных) рядах соответствующие фактор-группы изоморфны (с точностью до перестановки).

Утверждение 2.9. *Абелева группа A — простая $\Leftrightarrow$ $A \cong \mathbb{Z}_p$, где число p — простое.*

Доказательство.

$\Rightarrow$ Коль скоро A — простая, то $\exists a \in A \backslash \{e\}$. Рассмотрим 2 ситуации:

- $\operatorname{ord} a = n$. Тогда возьмём любой простой множитель $p \mid n$. Положим $b = a^{n/p} \in A$, для которого $\operatorname{ord} b = p$. В силу абелевости A, имеем нормальную подгруппу $\langle b \rangle \trianglelefteq A$. В силу простоты, $A \cong \mathbb{Z}_p$ (и, соответственно, $n = p$).
- $\operatorname{ord} a = \infty$. Поймём, что такой ситуации не может быть в принципе. Посмотрим на $H = \langle a^2 \rangle$. Тогда $a \notin H$ и, следовательно, $H \neq \{e\} \wedge H \neq G$, то есть G непроста.

$\Leftarrow$ Если $A \cong \mathbb{Z}_p$, то $\forall B \leqslant A$ $|B| = 1$ или $|B| = p$, то есть $B = \{e\}$ или $B = A$, поэтому A — простая.

□

Утверждение 2.10. *Пусть G — конечная группа, $H \leqslant G$, причем $|G : H| = 2$, и $h \in H$. Если $C_G(h) \neq C_H(h)$, то $h^G = h^H$. В противном случае, $|h^G| = 2|h^H|$.*

Доказательство. Коль скоро $|G : H| = 2$, то $H \trianglelefteq G$ и верно такое разбиение G:

$$\forall g \in G \backslash H \quad G = H \sqcup gH = H \sqcup Hg$$

▷ $C_G(h) \neq C_H(h)$. Возьмём $g \in C_G(h) \backslash C_H(h)$, для которого $gh = hg$ и $g \notin H$. Значит, с его помощью мы разбиваем g на 2 класса: $G = H \sqcup gH$. Осталась цепочка равенств:

$$h^G = h^{H \sqcup gH} = h^H \cup h^{gH} = h^H \cup (h^g)^H = h^H$$

▷ Теперь $C_G(h) = C_H(h)$. Тогда $\forall g \in G \backslash H$ $h^g \notin h^H$. Действительно, если бы это было так, то:

$$h^g = h^x,\ x \in H \Rightarrow h^{gx^{-1}} = h^{xx^{-1}} = h \Rightarrow gx^{-1} \in C_G(h) = C_H(h) \leqslant H$$

Но в то же время $gx^{-1} \notin H$. Значит, для такого элемента g имеет место равенство $h^G = h^H \sqcup h^{gH}$ и остаётся доказать, что классы равномощны. Для этого построим явно биекцию между h^H и $h^{Hg} = h^{gH}$ как $x \mapsto x^g$ (обратное отображение имеет явный вид $y \mapsto y^{g^{-1}}$, что доказывает биективность).

□

Теорема 2.6. A_5 *является простой группой*

Доказательство. Отметим, что $|A_5| = 60$. Доказательство состоит в том, чтобы рассмотреть всевозможные $\{e\} \neq H \trianglelefteq A_5$, причём мы знаем их вид — объединение классов сопряженности и, более того, $|H| \mid 60$. Пользуясь доказанным утверждением, перечислим все классы сопряженности элементов $h \in A_5$ в A_5 и S_5:

h^{S_5}	$g \in C_{S_5}(h) \backslash C_{A_5}(h)$	h^{A_5}	$\|h^{A_5}\|$
id^{S_5}	(12)	id^{S_5}	1
$(123)^{S_5}$	(45)	$(123)^{S_5}$	$\frac{A_5^3}{3} = 20$
$((12)(34))^{S_5}$	(12)	$((12)(34))^{S_5}$	$\frac{C_5^2 C_3^2}{2} = 15$
$(12345)^{S_5}$	—	$(12345)^{A_5}$	$\frac{1}{2}\frac{P_5}{5} = 12$
		$(12354)^{A_5}$	$\frac{1}{2}\frac{P_5}{5} = 12$

Поясним отсутствие элемента из разности централизаторов для последнего класса: $|(12345)^{S_5}| = 24 \nmid 60$, то есть по формуле мощности орбиты это точно не один класс в A_5. Остается непосредственно убедиться, что сумма мощностей никаких двух и более классов сопряженности в A_5 не является собственным делителем $|A_5| = 60$:

- ▷ $H \supseteq (123)^{S_5}$. Тогда $|H| \geqslant 21$ и, чтобы $|H|$ делило 60, оно должно стать хотя бы 30, то есть содержать минимум ещё один класс сопряженности, а это уже точно больше 30 и такое возможно лишь при $H = G$.
- ▷ Если $H \supseteq ((12)(34))^{S_5}$ и не содержит $(123)^{S_5}$, то $|H| \geqslant 16$ и нам снова нужен как минимум ещё один из оставшихся классов, но ни сумма с 12, ни сумма с 24 элементами не даёт делитель 60.
- ▷ Остаётся 3 варианта с классами по 12 элементов, но ни один из них не подойдёт по соображениям делимости.

Значит, в A_5 нет подгрупп, отличных от единицы или всей группы, то есть A_5 проста. □

Теорема 2.7. $\forall n \in \mathbb{N}, n \geqslant 5$ *группа* A_n *— простая.*

Доказательство. Проведем теперь индукцию по n:

- ▷ База $n = 5$: доказано предыдущей теоремой.
- ▷ Переход $n > 5$: Рассмотрим произвольную $H \trianglelefteq A_n$, $H \neq \{\mathrm{id}\}$. Сделаем переход в 2 шага:

  1. Покажем, что $\exists \tau \in H \colon \exists i \in \{1, \dots, n\}$, $\tau(i) = i$ — в H есть перестановка с неподвижной точкой. Без ограничения общности, пусть $\sigma \in H$ и $\sigma(1) = 2$. Если мы найдём $\sigma' \in H \colon \sigma' \neq \sigma \wedge \sigma'(1) = 2$, то $\tau := \sigma' \circ \sigma^{-1}$. В силу того, что $n \geqslant 6$, у нас есть $i \notin \{1, 2\}$ такое, что $\sigma(i) = j \notin \{1, 2\}$. Если $\sigma(i) = i = j$, то мы уже нашли

требуемое ($\tau = \sigma$). Иначе дополнительно возьмём $k, l \notin \{1, 2, i, j\}$. Утверждается, что подходящей σ' будет такая перестановка:

$$\sigma' = \sigma^{(jkl)} = (jkl)^{-1}\sigma(jkl)$$

Действительно, $\sigma' \in H$ из-за нормальности H и $\sigma'(1) = 2$, ибо сопряжение никак не задевает эти значения в силу выбора. С другой стороны, $\sigma' \neq \sigma$, ибо $\sigma'(i) = l \neq j = \sigma(i)$.

2. Без ограничения общности, пусть $\exists \sigma \in H \backslash \{\mathrm{id}\} \mid \sigma(n) = n$, то есть $\sigma \in A_{n-1}$. Тогда посмотрим на $L := H \cap A_{n-1} \trianglelefteq A_{n-1}$. По предположению индукции, $L = A_{n-1}$, поскольку L нетривиальна, и, следовательно, $(123) \in L \subset H \Rightarrow \langle (123)^{A_n} \rangle = A_n \leqslant H$, то есть $H = A_n$

$\square$

Замечание. Группа A_4 — уже не простая, поскольку $V_4 \trianglelefteq A_4$.

Замечание. Можно показать, что если $\mathbb{F}$ — поле, $k \geqslant 2$, то группа $\mathrm{PSL}_k(\mathbb{F}) := \mathrm{SL}_k(\mathbb{F})/Z(\mathrm{SL}_k(\mathbb{F}))$ проста при $|\mathbb{F}| \geqslant 4$ или $k \geqslant 3$ ($Z(\mathrm{SL}_k(\mathbb{F})) = \{\alpha E : \alpha \in \mathbb{F}, \alpha^k = 1\}$).

Упражнение. *Докажите, что* $\mathrm{PSL}_2(\mathbb{Z}_2) \cong S_3$.

Замечание. Можно также показать, что $\mathrm{PSL}_2(\mathbb{Z}_3) \cong A_4$ и, кроме того, $\mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{Z}_5) \cong A_5$.

Замечание. На данный момент классификация конечных простых групп *считается* завершенной. Она состоит из конечного числа бесконечных серий и конечного числа так называемых *спорадических* групп, не попадающих ни в одну из серий.

Утверждение 2.11. *Пусть G — неабелева простая группа. Тогда $G' = G$.*

Доказательство. $G' \neq \{e\}$ в силу неабелевости G, и $G' \trianglelefteq G$, следовательно, $G' = G$. $\square$

Следствие. $\forall n \in \mathbb{N}, n \geqslant 5$: группа A_n неразрешима.

Теорема 2.8. *Группа $\mathrm{SO}_3 = \{A \in \mathcal{O}_3 : \det A = 1\}$ — простая.*

Доказательство. Воспользуемся следующим фактом из линейной алгебры: $\forall A \in \mathrm{SO}_3 : \exists S \in \mathrm{SO}_3$:

$$S^{-1}AS = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}$$

Рассмотрим $H \trianglelefteq \mathrm{SO}_3, H \neq \{E\}$. Пусть $A \in H, A \neq E$ — вращение на угол α вокруг некоторой оси, тогда A^{SO_3} — это все вращения на угол α (то есть вокруг любой оси в пространстве), и $A^{\mathrm{SO}_3} \subset H$.

Пусть $B(\beta)$ — вращение на угол β вокруг оси, подобранной так, что $B(\beta)$ не коммутирует с A при $\beta = \beta_0$, то есть $A^{B(\beta_0)} \neq A$. Положим $C(\beta) := (A^{B(\beta)})^{-1}A$. Заметим, что тогда $C(0) = E$ и $C(\beta_0) \neq E$, причем элементы C — непрерывные функции β. Если $C(\beta)$ — это вращение на угол $\mu(\beta)$, то, поскольку след матрицы инвариантен относительно замены базиса и $1 + 2\cos\mu = \operatorname{tr} C(\beta)$, $\mu(\beta)$ — тоже непрерывная функция β. Значит, H содержит хотя бы по одному повороту на каждый угол из отрезка $[0, \mu(\beta_0)]$, $\mu(\beta_0) \neq 0$, и, следовательно, содержит все такие повороты. Но тогда H содержит и все повороты на углы из отрезков $[0, 2\mu(\beta_0)], [0, 3\mu(\beta_0)], \ldots, [0, 2\pi]$. Значит, $H = \mathrm{SO}_3$. $\square$

Замечание. Группа SO_n проста при $n \geqslant 3$, кроме $n = 4$.

3 Задание групп

3.1 Свободные группы

Определение 3.1. Пусть F_n — группа, $F_n = \langle f_1, \ldots, f_n \rangle$. Такая группа F_n называется *свободной со свободными образующими* $f_1, \ldots, f_n \in F_n$, если для любой группы G выполнено *универсальное свойство*:

$$\forall g_1, \ldots, g_n \in G \ \exists \varphi \colon F_n \to G \text{ — гомоморфизм } \Big| \ \forall i \in \{1, \ldots, n\} \quad \varphi(f_i) = g_i$$

Замечание. Если такой гомоморфизм существует, то он единственен, поскольку F_n порождена элементами $f_1, \ldots, f_n$.

Замечание. Аналогичным образом можно определить и свободные группы с бесконечным количеством свободных образующих.

Замечание. Если $G = \langle g_1, \ldots, g_n \rangle$, то $G = \operatorname{Im} \varphi \cong F_n / \operatorname{Ker} \varphi$, то есть свободная группа как минимум своими факторами задаёт все группы, порождённые n элементами.

Теорема 3.1. *Свободная группа F_n со свободными образующими $f_1, \ldots, f_n$ существует.*

Доказательство. Заведём алфавит символов $\Sigma = \{f_1, \ldots, f_n, f_1^{-1}, \ldots, f_n^{-1}\}$. Тогда F_n как множество можно описать следующим образом:

$$F_n = \{w \in \Sigma^* \colon \forall i \in \{1, \ldots, n\} \ w \text{ не содержит подслов } f_i f_i^{-1} \text{ и } f_i^{-1} f_i\}$$

Определим операцию на F_n следующим образом: если $w_1, w_2 \in F_n$, то сократим взаимно обратные элементы алфавита с конца w_1 и начала w_2, получив w_1' и w_2', и положим $w_1 \cdot w_2 := w_1' w_2'$.

Докажем, что F_n — действительно группа:

▷ (Нейтральный элемент) $\exists \varepsilon \in F_n \ \big| \ \forall w \in F_n \quad w \cdot \varepsilon = \varepsilon \cdot w = w$.

▷ (Обратный элемент) Пусть $w \in F_n, w = f_{i_1}^{\alpha_1} \ldots f_{i_k}^{\alpha_k}$, где $f_{i_j} \in \{f_1, \ldots, f_n\}$ и $\alpha_{i_j} \in \{\pm 1\}$. Тогда $\exists w^{-1} = f_{i_k}^{-\alpha_k} \ldots f_{i_1}^{-\alpha_1} \in F_n \ \big| \ w \cdot w^{-1} = w^{-1} \cdot w = \varepsilon$.

▷ (Ассоциативность) Докажем, что $\forall a, b, c \in F_n : (ab)c = a(bc)$ индукцией по $|b|$.

- База $|b| = 0$: это соответствует только $b = \varepsilon$, свойство ассоциативности тривиально.
- База $|b| = 1$: нужно сделать разбор случаев, чем заканчивается a и начинается c.
- Переход $|b| > 1$: пусть $b = xb'$, $x \in \Sigma$. Тогда

$$(ab)c = (a(xb'))c = ((ax)b')c = (ax)(b'c) = a(x(b'c)) = a((xb')c) = a(bc)$$

Проверим теперь, что F_n — свободная группа. Пусть G — произвольная группа, $g_1, \ldots, g_n \in G$. Определим $\varphi \colon F_n \to G$ следующим образом: $\varphi(f_{i_1}^{\alpha_1} \ldots f_{i_k}^{\alpha_k}) = g_{i_1}^{\alpha_1} \ldots g_{i_k}^{\alpha_k}$. Тогда, по определению, $\forall i \in \{1, \ldots, n\} \ \varphi(f_i) = g_i$. Наконец, φ — гомоморфизм, поскольку $\forall w_1, w_2 \in F_n$ в записях $\varphi(w_1 w_2)$ и $\varphi(w_1)\varphi(w_2)$ сокращаются одни и те же элементы. □

Теорема 3.2. *Пусть F_n — свободная группа со свободными образующими $f_1, \ldots, f_n$, G_n — свободная группа со свободными образующими $g_1, \ldots, g_n$. Тогда существует изоморфизм $\varphi\colon F_n \to G_n$ такой, что $\forall i \in \{1, \ldots, n\}$ $\varphi(f_i) = g_i$.*

Доказательство. По определению свободной группы, существует гомоморфизм $\varphi : F_n \to G_n$ такой, что $\forall i \in \{1, \ldots, n\}$ $\varphi(f_i) = g_i$, и, аналогично, существует гомоморфизм ψ $G_n \to F_n$ такой, что $\forall i \in \{1, \ldots, n\}$ $\psi(g_i) = f_i$. Тогда $\psi \circ \varphi = \mathrm{id}_{F_n}$, $\varphi \circ \psi = \mathrm{id}_{G_n}$, поэтому эти гомоморфизмы биективны и взаимно обратны. □

Пример. Рассмотрим $F_1 = \{f_1^n : n \in \mathbb{Z}\}$. Легко видеть, что $F_1 \cong \mathbb{Z}$.

Замечание. При $n \geqslant 2$ группа F_n — уже неабелева, например, потому, что $f_1 f_2 \neq f_2 f_1$.

Упражнение. *Пусть $G = \mathrm{SL}_2(\mathbb{Z}[x])$. Рассмотрим следующую подгруппу в G:*

$$F = \left\langle \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right\rangle \leqslant G$$

Докажите, что F — свободная группа с соответствующими свободными образующими.

Определение 3.2. Пусть $w \in F_n$, G — группа, $g_1, \ldots, g_n \in G$. Тогда *значение w в группе G* — это $w(g_1, \ldots, g_n) := \varphi(w)$, где φ — гомоморфизм F_n и G такой, что $\forall i \in \{1, \ldots, n\}$ $\varphi(f_i) = g_i$.

3.2 Образующие и соотношения

Определение 3.3. Пусть F_n — свободная группа, $S \subseteq F_n$, G — группа, $g_1, \ldots, g_n \in G$, $G = \langle g_1, \ldots, g_n \rangle$. Положим $K := \langle S \rangle_{norm}$. Говорят, что G *задается образующими $g_1, \ldots, g_n$ и соотношениями S*, если $K = \operatorname{Ker} \varphi$, где φ — гомоморфизм F_n и G такой, что $\forall i \in \{1, \ldots, n\}$ $\varphi(f_i) = g_i$.

Обозначение — $G = \langle g_1, \ldots, g_n \mid S|_{f_i \mapsto g_i} = e \rangle$, где $S|_{f_i \mapsto g_i}$ — множество слов, полученных формальной подстановкой символов $g_1, \ldots, g_n$ вместо $f_1, \ldots, f_n$ в слова из S.

Замечание. В терминах определения выше, $G = \langle g_1, \ldots, g_n \rangle = \operatorname{Im} \varphi \cong F_n / K$. Значит, группа G задается образующими и соотношением однозначно. Кроме того, $\forall w \in S$ $w(g_1, \ldots, g_n) = \varphi(w) = e$, и, неформально говоря, все соотношения элементов G следуют из соотношений S.

Пример. $\mathbb{Z}_n \cong \langle a \mid a^n \rangle$, поскольку $\langle n \rangle_{norm} = n\mathbb{Z}$ и $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} \cong F_1/n\mathbb{Z}$. Этот факт также можно записать в виде $\mathbb{Z}_n \cong \langle a \mid a^n = e \rangle$.

Замечание. Отметим, что $F_n = \langle f_1, \ldots, f_n \mid \varnothing \rangle$: на элементы F_n не накладывается никаких соотношений.

Теорема 3.3. *(Универсальное свойство группы, заданной образующими и соотношениями) Пусть $S \subseteq F_n$, $G = \langle g_1, \ldots, g_n \mid S|_{f_i \mapsto g_i} \rangle$, H — группа, и $h_1, \ldots, h_n \in H$ таковы, что $\forall w \in S$ $w(h_1, \ldots, h_n) = e$. Тогда сущетвует $\varphi\colon G \to H$ — гомоморфизм такой, что $\forall i \in \{1, \ldots, n\}$ $\varphi(g_i) = h_i$.*

Доказательство. Будем считать, что $H = \langle h_1, \ldots, h_n \rangle$ (если есть что-то лишнее, то мы об этом «забудем», ведь строим просто гомоморфизм).

Пусть $\psi\colon F_n \to G$, $\psi(f_i) = g_i$. В силу задания группы G соотношениями, имеем $\operatorname{Ker}\psi = K = \langle S \rangle_{norm}$. В силу универсального свойства свободной группы, у нас есть гомоморфизм $\Theta\colon F_n \to H$, имеющий вид $\Theta(f_i) = h_i$. По условию

$$\Theta(S) = e \Rightarrow S \leqslant \operatorname{Ker}\Theta =: L \trianglelefteq F_n$$

Стало быть, $K = \langle S \rangle_{norm} \leqslant L$. По второй теореме об изоморфизме получаем такую цепочку:

$$H \cong F_n/L \cong (F_n/K)/(L/K)$$

При этом, естественно $L/K \trianglelefteq F_n/K$. Как и в построении этого изоморфизма, можно рассмотреть канонический эпиморфизм $\pi\colon F_n/K \to (F_n/K)/(L/K)$, заменив множество значений сразу на F_n/L. При этом $aK \mapsto aL$, а изоморфизмы для G и H утверждают, что $g_i \mapsto f_iK$ и $h_i \mapsto f_iL$, то есть сквозной гомоморфизм φ будет соблюдать равенство $\varphi(g_i) = h_i$. □

Замечание. Построенный φ единственен.

Упражнение. *Если в G выполняются соотношения из S, и она удовлетворяет универсальному свойству, то она и задана соотношениями из S.*

Далее конспект не отредактирован с 2020 года.

Пример. Рассмотрим $G := \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle$. Поскольку $a^2 = b^2 = e$, то элементы группы G — это слова из a, b, в которых нет подряд идущих одинаковых символов. Более того, $abab = e \Rightarrow ab = ba$, поэтому $G = \{e, a, b, ab\}$ и $|G| \leqslant 4$.

Покажем, что $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Рассмотрим в $H := \mathbb{Z}_2 \times \mathbb{Z}_2$ элементы $a' = (\overline{1}, \overline{0})$, $b' = (\overline{0}, \overline{1})$. Тогда $a'^2 = b'^2 = (a'b')^2 = e$, и, по предыдущей теореме, $\exists \varphi : G \to H$ — гомоморфизм такой, что $\varphi(a) = a'$, $\varphi(b) = b'$. Значит, $\operatorname{Im}\varphi = H$, тогда $|G| = 4$ и $G \cong H$.

Замечание. Пусть $G = \langle g_1, \ldots, g_n \mid S \rangle$. Чтобы выяснить, что это за группа, можно описать все различные элементы G. Однако этот способ нельзя алгоритмизовать, потому что в общем случае нельзя алгоритмически определить, равны ли два слова из символов $g_1, \ldots, g_n$ при заданных соотношениях S.

4 Строение групп

4.1 Теоремы Силова

Определение 4.1. Пусть G — конечная группа, $|G| = n$, p — простой делитель числа n, $n = p^k s$, $(p, s) = 1$. Тогда подгруппа $H \leqslant G$ такая, что $|H| = p^k$, называется *силовской p-подгруппой* группы G.

Замечание. Если G — конечная группа, $|G| = n$, $t \mid n$, то необязательно в G есть подгруппа порядка t. Например, в группе A_4, $|A_4| = 12$ нет подгруппы порядка 6.

Теорема 4.1. *(Теоремы Силова) Пусть G — конечная группа, $|G| = n$, p — простой делитель числа n, $n = p^k s$, $(p, s) = 1$. Обозначим через N_p количество силовских p-подгрупп в G Тогда:*

1. *В G существует силовская p-подгруппа, то есть $N_p > 0$*

1'. *Любая p-подгруппа в G содержится в некоторой силовской*

2. *Все силовские p-подгруппы в G сопряжены*

3. *$N_p \equiv_p 1$*

3'. *$N_p \mid s$*

Доказательство 1 и 3. Положим $\Omega := \{M \subset G : |M| = p^k\}$ и рассмотрим действие G на Ω левыми сдвигами: $\forall g \in G : \forall M \in \Omega : g(M) = gM$. Если для некоторого $M \in \Omega$ его стабилизатор — это $H \leqslant G$, то $M = HM = \bigcup_{m \in M} Hm$, то есть M разбивается на непересекающиеся правые смежные классы по H. В частности, это означает, что $|H| \mid |M| = p^k$, то есть $|H| = p^l, l \leqslant k$. Тогда

$$|H| = p^k \Leftrightarrow \exists g \in G \colon M = Hg \Leftrightarrow |G(M)| = |G : H| = s$$

Если же $|H| = p^l, l < k$, то $|G(M)| = |G : H| = p^{k-l}s \equiv_p 0$. Обозначим через $\Omega_1, \ldots, \Omega_r$ орбиты действия и воспользуемся формулой орбит:

$$\binom{n}{p^k} = |\Omega| = \sum_{i=1}^{r} |\Omega_i| = \sum_{i=1}^{r} |G : \mathrm{St}(M_i)| \equiv_p N_p s$$

Заметим, что полученное сравнение для $N_p s$ зависит лишь от числа n, но не от конкретного вида группы. Значит, мы имеем право рассмотреть конкретную группу порядка n, например, $\mathbb{Z}_n$. У неё единственная силовская p-подгруппа — это $s\mathbb{Z}_n$, поэтому в данном случае $N_p = 1$ и $\binom{n}{p^k} \equiv_p s$. Возвращаясь к общему случаю, получаем, что

$$s \equiv_p \binom{n}{p^k} \equiv_p N_p s \Longrightarrow p \mid (N_p - 1)s \Longrightarrow N_p \equiv_p 1$$

□

Доказательство 1' и 2. Пусть $P \leqslant G$ — силовская p-подгруппа, а Q — p-подгруппа в G. Рассмотрим действие Q на G/P левыми сдвигами: $\forall q \in Q, gP \in G/P\ q(gP) = qgP$.

Обозначим через $\Omega_1, \ldots, \Omega_r$ орбиты действия и воспользуемся формулой орбит:

$$s = |G/P| = \sum_{i=1}^{r} |\Omega_i| = \sum_{i=1}^{r} |Q : \mathrm{St}(\omega_i)|$$

Поскольку правая часть — это сумма выражений вида p^l, $l \in \mathbb{Z}$, и $p \nmid s$, то

$$\exists i \in \{1, \ldots, r\} \mid |Q : \mathrm{St}(\omega_i)| = 1 \Leftrightarrow \mathrm{St}(w_i) = Q$$

Пусть $\omega_i = gP$, тогда $QgP = gP \Rightarrow QP^{g^{-1}} = P^{g^{-1}} \Rightarrow Q \leqslant P^{g^{-1}}$, причем подгруппа $P^{g^{-1}}$ — силовская. Если же Q — тоже силовская p-подгруппа в G, то $|Q| = |P|$, поэтому $Q = P^{g^{-1}}$. □

Доказательство 3'. Пусть $P \leqslant G$ — силовская p-подгруппа. Тогда все силовские p-подгруппы имеют вид P^g, $g \in G$. Они образуют орбиту P^G при действии G на множестве своих подгрупп сопряжениями. Тогда $N_p = \frac{|G|}{|N_G(P)|}$ и, поскольку $P \leqslant N_G(P)$ (так как любой элемент P при сопряжении P даст просто P), $N_p \mid s$. □

Замечание. Пусть G — конечная группа, $|G| = n$, p — простой делитель числа n, $n = p^k s$, $(p, s) = 1$. Обозначим через $N_p(l)$ число подгрупп порядка p^l, $l \leqslant k$. Аналогично доказательству выше, можно показать, что $N_p(l) \equiv_p 1$.

Утверждение 4.1. *Пусть $p < q$ — простые числа. Тогда любая группа порядка pq разрешима и, более того, она изоморфна $\mathbb{Z}_q \rightthreetimes \mathbb{Z}_p$*

Доказательство. Пусть $|G| = pq$. По теореме Силова, в ней есть силовские p- и q-подгруппы. Обозначим таковыми $|H_p| = p$, $|H_q| = q$. В силу простоты порядка этих подгрупп, для них есть изоморфизм $H_p \cong \mathbb{Z}_p$ и $H_q \cong \mathbb{Z}_q$. Более того, по теореме Силова:

$$N_q \equiv 1 \pmod q \wedge N_q \mid p < q \Rightarrow N_q = 1$$

Это означает, что действие сопряжениями на H_q даёт всегда её же. Стало быть, $H_q \trianglelefteq G$. Осталось сказать, что $H_q \cap H_p = \{e\}$. Это так, ибо порядок пересечения должен делится на порядки этих групп. Стало быть, $H_q \rightthreetimes H_p = G$. Про полупрямое произведение мы знаем, что $G/H_q \cong H_p$, и притом H_p, H_q абелевы. Стало быть, G разрешима. □

Теорема 4.2. *Пусть G — конечная группа. Тогда:*

1. *Если P — силовская p-подгруппа в G, то $P \trianglelefteq G \Leftrightarrow N_p = 1$*
2. *Все силовские подгруппы нормальны в G тогда и только тогда, когда их внутренее прямое произведение является самой G*

Доказательство.

1. $\Leftarrow$ Если $N_p = 1$, то $\forall g \in G : P^g = P$, поэтому $P \trianglelefteq G$.

   $\Rightarrow$ Если $P \trianglelefteq G$, то любая другая силовская p-подгруппа в G имеет вид $P^g, g \in G$. Тогда, поскольку $\forall g \in G$ $P^g = P$, $N_p = 1$.

2. $\Leftarrow$ Если $G = P_1 \times \ldots \times P_m$, то из определения прямого произведения, $\forall i \in \{1, \ldots, m\}$ $P_i \trianglelefteq G$. При этом, если посмотреть на любой $p \mid |G|$, то в силу равенства $|G| = |P_1| \cdot \ldots \cdot |P_m|$ будет существовать P_i (и ровно одна для всей G из-за предыдущего пункта) — силовская p-подгруппа.

$\Rightarrow$ Проведем индукцию по m. База, $m = 1$, тривиальна. Пусть теперь $m > 1$. Положим $H := P_1 \dots P_{m-1} \trianglelefteq G$. Тогда в H есть силовские подгруппы $P_1, \dots, P_{m-1}$, и, более того, все они нормальны в H. По предположению индукции, $H = P_1 \times \dots \times P_{m-1}$. Поскольку $(|H|, |P_m|) = 1$, то $H \cap P_m = \{e\} \Rightarrow HP_m = G$, и $G = P_1 \times \dots \times P_m$.

□

4.2 Свободные абелевы группы

В данном разделе и далее рассматриваемые группы будут абелевыми, и операция в них будет обозначаться через $+$.

Пример. Группа $\mathbb{Q}$ не является конечнопорожденной. Она не является циклической, и любые две нетривиальных подгруппы в ней имеют нетривиальное пересечение.

Замечание. Если $(n, k) = 1$, то $\mathbb{Z}_n \oplus \mathbb{Z}_k \cong \mathbb{Z}_{nk}$, поскольку $\mathrm{ord}(\overline{1}, \overline{1})$ в этой группе равен nk.

Определение 4.2. Пусть G — абелева группа. Система элементов $(e_1, \dots, e_k)$ группы G называется *независимой*, если $\forall n_1, \dots, n_k \in \mathbb{Z} \quad \sum_{i=1}^{k} n_i e_i = 0 \Rightarrow n_1 = \ldots = n_k = 0$.

Определение 4.3. Система $(e_1, \dots, e_k)$ называется *базисом* в G, если она независима и $G = \langle e_1, \dots, e_k \rangle$.

Замечание. Любая непустая система в $\mathbb{Z}_n$ зависима.

Утверждение 4.2. *Пусть $(e_1, \dots, e_k)$ — базис в абелевой группе G. Тогда $\forall g \in G \ \exists! n_1, \dots, n_k \in \mathbb{Z} \quad g = \sum_{i=1}^{k} n_i e_i$.*

Доказательство. Существование коэффициентов $n_1, \dots, n_k$ следует из определения базиса. Если же $g = \sum_{i=1}^{k} n_i e_i = \sum_{i=1}^{k} m_i e_i$, то $\sum_{i=1}^{k} (n_i - m_i) e_i = 0$, откуда $\forall i \in \{1, \dots, k\} \ n_i = m_i$. □

Определение 4.4. Абелева группа G называется *свободной абелевой группой ранга k*, если в ней существует базис из k элементов.

Утверждение 4.3. *Пусть G — свободная абелева группа ранга k. Тогда $G \cong \mathbb{Z}^k$.*

Доказательство. Пусть $(e_1, \dots, e_k)$ — базис в G. Рассмотрим отображение $\varphi : \mathbb{Z}^k \to G$ такое, что $\forall (n_1, \dots, n_k) \in \mathbb{Z}^k : \varphi((n_1, \dots, n_k)) = \sum_{i=1}^{k} n_i e_i$. Очевидно, это гомоморфизм, причем биективный в силу предыдущего утверждения. □

Замечание. Группа $\mathbb{Z}^k$ обладает базисом. Например, им является система $e_1 = (1, 0, \dots, 0), \dots, e_k = (0, \dots, 0, 1)$.

Утверждение 4.4. *(Универсальное свойство свободной абелевой группы) Пусть G — свободная абелева группа с базисом $(e_1, \dots, e_n)$. Тогда для любой абелевой группы A выполнено универсальное свойство:*

$$\forall a_1, \dots, a_n \in A \ \exists \varphi \colon G \to A \text{ — \textit{гомоморфизм}} \ \Big| \ \forall i \in \{1, \dots, n\} \ \varphi(e_i) = a_i$$

Доказательство. Отображение φ задается однозначно:

$$\forall g \in G,\ g = \sum_{i=1}^{n} k_i e_i \Rightarrow \varphi(g) = \sum_{i=1}^{n} k_i a_i$$

Определение корректно в силу единственности разложения каждого элемента по базису. Остается проверить, что полученное отображение действительно является гомоморфизмом:

$$\forall g, h \in G, g = \sum_{i=1}^{n} k_i e_i, h = \sum_{i=1}^{n} l_i e_i \Rightarrow \varphi(g)+\varphi(h) = \sum_{i=1}^{n} k_i a_i + \sum_{i=1}^{n} l_i a_i = \sum_{i=1}^{n} (k_i+l_i) a_i = \varphi(g+h)$$

□

Утверждение 4.5. *Пусть G — свободная абелева группа с базисом $(e_1, \ldots, e_n)$. Тогда:*

$$G \cong \langle a_1, \ldots, a_n \mid \forall i, j \in \{1, \ldots, n\}\ [a_i, a_j] = e \rangle \cong F_n / F_n'$$

где F_n — свободная группа порядка n.

Доказательство. Положим $H := \langle a_1, \ldots, a_n \mid \forall i, j \in \{1, \ldots, n\}\ [a_i, a_j] = e \rangle$. Группа H — абелева, поскольку все ее порождающие коммутируют. Тогда, по универсальному свойству G, существует гомоморфизм $\varphi : G \to H$ такой, что $\forall i \in \{1, \ldots, n\} : \varphi(e_i) = a_i$. Поскольку G — абелева, то соотношения, задающие H, выполнены и в G, и, по универсальному свойству H, существует гомоморфизм $\psi : H \to G$ такой, что $\forall i \in \{1, \ldots, n\} : \psi(a_i) = e_i$. Остается заметить, что $\varphi \circ \psi = \mathrm{id}_H$, $\psi \circ \varphi = \mathrm{id}_G$, поэтому этим гомоморфизмы биективны и взаимно обратны. Наконец, по определению группы, заданной образующими и соотношениями, $H \cong F_n / \langle [a_i, a_j] : i, j \in \{1, \ldots, n\} \rangle_{norm} \cong F_n / F_n'$. □

Замечание. Изоморфизмы в утверждении выше имеют следующий вид: $e_i \mapsto a_i \mapsto \overline{f_i} = f_i F_n'$.

Теорема 4.3. *Пусть G — свободная абелева группа, $(e_1, \ldots, e_n)$ и $(e_1', \ldots, e_k')$ — два базиса в G. Тогда $n = k$.*

Доказательство. Пусть без ограничения общности $n < k$. Поскольку $(e_1, \ldots, e_n)$ — базис, то $(e_1', \ldots, e_k') = (e_1, \ldots, e_n) S$ для некоторой матрицы $S \in M_{n \times k}(\mathbb{Z}) \subset M_{n \times k}(\mathbb{Q})$. По основной лемме о линейной зависимости, столбцы S линейно зависимы над $\mathbb{Q}$: $\exists \overline{q} \in \mathbb{Q}^k, \overline{q} \neq \overline{0} : S\overline{q} = \overline{0}$. Можно считать, что $\overline{q} \in \mathbb{Z}^k$, поскольку умножение всех элементов столбца на наименьшее общее кратное их знаменателей сохраняет равенство. Но тогда $(e_1', \ldots, e_k')\overline{q} = 0$, то есть система $(e_1', \ldots, e_k')$ зависима — противоречие. □

Определение 4.5. Пусть G — свободная абелева группа. Ее *рангом* называется число элементов в любом базисе в G.

Замечание. Мы доказали, что любая система из $n + 1$ элемента в свободной абелевой группе ранга n зависима, но из этого не следует, что один из элементов такой системы выражается через остальные. Например, система $(2, 3)$ в $\mathbb{Z}$ зависима, но 2 и 3 не выражаются друг через друга.

Теорема 4.4. *Пусть G — свободная абелева группа, $(e_1, \ldots, e_n)$ — базис в G. Рассмотрим $(e_1', \ldots, e_n') = (e_1, \ldots, e_n) S$, $S \in M_n(\mathbb{Z})$. Тогда $(e_1', \ldots, e_n')$ — базис в $G \Leftrightarrow \det S = \pm 1$.*

Доказательство.

- $\Rightarrow$ Если $(e'_1, \ldots, e'_n)$ — базис в G, то $(e_1, \ldots, e_n) = (e'_1, \ldots, e'_n)T = (e_1, \ldots, e_n)ST$, $T \in M_n(\mathbb{Z})$. В силу единственности разложения, $ST = E$, тогда, поскольку определители S и T целочисленны, $|\det S| = |\det T| = 1$.

- $\Leftarrow$ Если $\det S = \pm 1$, то, по формуле Крамера, $S^{-1} \in M_n(\mathbb{Z})$. Тогда $(e_1, \ldots, e_n) = (e'_1, \ldots, e'_n)S^{-1}$, поэтому $G = \langle e'_1, \ldots, e'_n \rangle$. Наконец, система $(e'_1, \ldots, e'_n)$ независима: если для некоторого $\overline{z} \in \mathbb{Z}^n$ $(e'_1, \ldots, e'_n)\overline{z} = 0$, то тогда $(e_1, \ldots, e_n)S\overline{z} = 0$, откуда $S\overline{z} = \overline{0}$, и, в силу невырожденности S, $\overline{z} = \overline{0}$.

$\square$

Замечание. В ходе доказательства теоремы мы также получили, что $(M_n(\mathbb{Z}))^* = \{S \in M_n(\mathbb{Z}) : \det S = \pm 1\}$. Эта группа обозначается через $\mathrm{GL}_n(\mathbb{Z})$.

Замечание. Для любой абелевой группы $A = \langle a_1, \ldots, a_n \rangle$ существует гомоморфизм $\varphi : \mathbb{Z}^n \to A$ такой, что $\forall i \in \{1, \ldots, n\} : \varphi(e_i) = a_i$. Этот гомоморфизм сюръективен, тогда, по основной теореме о гомоморфизме, $A \cong \mathbb{Z}^n / \operatorname{Ker} \varphi$.

Теорема 4.5. *Пусть G — свободная абелева группа ранга n, $H \leqslant G$. Тогда H — свободная абелева группа ранга k, $k \leqslant n$.*

Доказательство. Проведем индукцию по n. База, $n = 0$, тривиальна, поскольку в этом случае $G = H = \{e\}$.

Пусть теперь $n \geqslant 1$, $(e_1, \ldots, e_n)$ — базис в G. Рассмотрим гомоморфизм $\varphi : G \to \mathbb{Z}$ такой, что $\varphi(e_n) = 1$, $\forall i \in \{1, \ldots, n-1\} : \varphi(e_i) = 0$. Тогда $G_1 := \langle e_1, \ldots, e_{n-1} \rangle = \operatorname{Ker} \varphi$ — свободная абелева группа ранга $n-1$. Пусть $\psi := \varphi|_H$, $H_1 := \operatorname{Ker} \psi = G_1 \cap H \leqslant G_1$. По предположению индукции, H_1 — свободная абелева группа с базисом $(h_1, \ldots, h_l)$, $l \leqslant n-1$. Если $\operatorname{Im} \psi = \{0\}$, то $H = H_1$. Иначе — $\operatorname{Im} \psi = m\mathbb{Z}$, $m \geqslant 1$. Выберем h_{l+1} из $\psi^{-1}(m)$ и докажем, что $(h_1, \ldots, h_{l+1})$ — базис в H.

С одной стороны, $\forall h \in H : \exists h' \in \operatorname{Ker} \psi : h = h' + \frac{\psi(h)}{m} h_{l+1}$, поэтому $H = \langle h_1, \ldots, h_{l+1} \rangle$. С другой стороны, если $\sum_{i=1}^{l+1} \alpha_i h_i = 0$, то:

$$0 = \psi\left(\sum_{i=1}^{l+1} \alpha_i h_i\right) = \sum_{i=1}^{l+1} \alpha_i \psi(h_i) = \alpha_{k+1} m$$

Значит, $\alpha_{l+1} = 0$. Но тогда, в силу независимости $(h_1, \ldots, h_l)$, $\alpha_1 = \cdots = \alpha_l = 0$, и $(h_1, \ldots, h_{l+1})$ независима. $\square$

Замечание (Теорема Нильсена-Шрайера)**.** Пусть F_n — свободная группа, $H \leqslant F_n$. Тогда H — тоже свободная группа, однако число свободных порождающих в H может превышать n и даже быть бесконечным.

Пример. Пусть $F_2 = \langle a, b \rangle$ — свободная группа со свободными образующими a, b. Тогда $H = \langle a^k b a^k : k \in \mathbb{N} \rangle \leqslant F_2$ — свободная группа со свободными образующими $a^k b a^k$, $k \in \mathbb{N}$.

Замечание. Если G— свободная абелева группа и $H \leqslant G$ — свободная абелева группа того же ранга, что и G, то необязательно $H = G$. Например, $2\mathbb{Z} \neq \mathbb{Z}$.

Упражнение. *Рассмотрим линейное пространство $\mathbb{R}^n$ с базисом $(\overline{e_1}, \ldots, \overline{e_n})$. $\Gamma := \langle \overline{e_1}, \ldots, \overline{e_n} \rangle \leqslant \mathbb{R}^n$ — свободная абелева группа, также называемая решеткой. Тогда:*

1. *Фундаментальный объем, то есть* $V(\Gamma) := |V(\overline{e_1}, \ldots, \overline{e_n})|$*, не зависит от выбора базиса в* Γ

2. *Если* $\Gamma_1 \leqslant \Gamma_2$ *— две решетки ранга* n *в* $\mathbb{R}^n$*, то* $|\Gamma_2 : \Gamma_1| = \frac{V(\Gamma_1)}{V(\Gamma_2)}$

Решение.

1. Пусть $e = (\overline{e_1}, \ldots, \overline{e_n})$ и $e' = (\overline{e'_1}, \ldots, \overline{e'_n})$ — два базиса в Γ, $\Gamma(e)$, $\Gamma(e')$ — матрицы Грама этих базисов. Если S — матрица перехода из e в e', то $|\det S| = 1$, поэтому $V(e') = \sqrt{\det \Gamma(e')} = \sqrt{\det\left(S^T \Gamma(e) S\right)} = \sqrt{\det \Gamma(e)} = V(e)$.

2. Данное утверждение следует из теоремы о согласованных базисах из следующего раздела.

4.3 Конечнопорожденные абелевы группы

Утверждение 4.6. *Пусть* $A \in M_{n\times k}(\mathbb{Z})$*. Тогда* $\exists P \in \mathrm{GL}_n(\mathbb{Z}) : \exists Q \in \mathrm{GL}_k(\mathbb{Z}) : \exists D = \mathrm{diag}(u_1, u_2, \ldots) \in M_{n\times k}(\mathbb{Z})$*,* $u_1, u_2, \ldots \geqslant 0$*,* $u_1 \mid u_2 \mid \cdots : A = PDQ$*.*

Доказательство. Уточним формулировку утверждения: мы будем получать D из A, используя целочисленные элементарные преобразования строк (и столбцов), обратные преобразования к которым также целочисленны:

1. Прибавление к строке (столбцу) другой строки (другого столбца) с целочисленным коэффициентом

2. Перестановка строк (столбцов) местами

3. Умножение строки (столбца) на ± 1

Если мы получим таким образом матрицу D требуемого вида, то $D = P'AQ', P' \in \mathrm{GL}_n(\mathbb{Z}), Q' \in \mathrm{GL}_k(\mathbb{Z})$, откуда $A = (P')^{-1} D (Q')^{-1}$. Проведем индукцию по $\min(n, k)$, без ограничения общности считая, что $\min(n, k) = k$. Базовыми случаями будем считать $k = 0$ и $A = 0$, оба этих случая тривиальны.

Пусть теперь $k \geqslant 1$ и $A \neq 0$. Получим из A указанными выше преобразованиями матрицу $B = (b_{ij}) \in M_{n\times k}(\mathbb{Z})$ такую, что $b_{11} > 0$ и число b_{11} минимально. В силу минимальности b_{11}, $\forall i \in \{1, \ldots, n\} : b_{11} \mid b_{i1}$ и $\forall j \in \{1, \ldots, k\} : b_{11} \mid b_{1j}$. Тогда, вычитая из остальных строк первую с соответствующим коэффициентом и делая то же самое со столбцами, мы приведем B к виду $C = \mathrm{diag}(b_{11}, C')$, где $C' = (c_{ij}) \in M_{(n-1)\times(k-1)}(\mathbb{Z})$. Заметим теперь, что, в силу минимальности b_{11}, $\forall i \in \{1, \ldots, n-1\} : \forall j \in \{1, \ldots, k-1\} : b_{11} \mid c_{ij}$. Значит, к C' достаточно применить предположение индукции, поскольку преобразования строк и столбцов C' сохраняют первую строку и первый столбец C. □

Замечание. Представление матрицы A в таком виде, как в утверждении выше, называется ее *нормальной формой Смита.*

Следствие. Группа $\mathrm{GL}_n(\mathbb{Z})$ порождается матрицами целочисленных элементарных преобразований.

Доказательство. Рассмотрим матрицу $A \in \mathrm{GL}_n(\mathbb{Z})$ и ее нормальную форму Смита $A = PDQ$. Из доказательства утверждения выше следует, что P, Q — это произведения элементарных целочисленных матриц, а D — диагональная матрица с неотрицательными элементами такая, что $|\det D| = 1$. Значит, $D = E$ и $A = PQ$. □

Упражнение. *Докажите, что матрица D в нормальной форме Смита матрицы A определена однозначно.*

Решение. Обозначим через $g_i(A)$ НОД миноров матрицы A порядка i. Легко проверить, что целочисленные элементарные преобразования строк и столбцов сохраняют величину g_i. Тогда, в силу предыдущего следствия, для любой нормальной формы Смита $A = PDQ$ выполнено $g_i(A) = g_i(D)$. Но $g_i(D) = u_1 \cdots u_i$, значит, элементы D заданы однозначно: $u_1 = g_1(A), \forall i \in \{2, \ldots, \min(n,k)\} : u_i = \frac{g_i(A)}{g_{i-1}(A)}$.

Теорема 4.6. *Пусть G — свободная абелева группа ранга n и $H \leqslant G$ — свободная абелева группа ранга $k \leqslant n$. Тогда в G и H существуют базисы $(g_1, \ldots, g_n)$ и $(h_1, \ldots, h_k)$ такие, что $\forall i \in \{1, \ldots, k\} : h_i = u_i g_i, u_i \in \mathbb{Z}, u_i \geqslant 1$, причем $u_1 \mid \cdots \mid u_k$.*

Доказательство. Пусть $(e_1, \ldots, e_n)$ — базис в G, $(a_1, \ldots, a_k)$ — базис в H. Тогда $(a_1, \ldots, a_k) = (e_1, \ldots, e_n)A$, где $A \in M_{n\times k}(\mathbb{Z})$. Пусть $A = PDQ$ — нормальная форма Смита матрицы A. Тогда базисы $(g_1, \ldots, g_n) = (e_1, \ldots, e_n)P$, $(h_1, \ldots, h_k) = (a_1, \ldots, a_k)Q^{-1}$ являются искомыми. □

Замечание. Базисы в G и H из теоремы выше называются *согласованными.*

Следствие. Пусть A — конечнопорожденная абелева группа. Тогда $A \cong Z^l \oplus \mathbb{Z}_{u_1} \oplus \cdots \oplus \mathbb{Z}_{u_k}$, где $l, u_1, \ldots, u_k \in \mathbb{Z}$, $l \geqslant 0$, $u_1, \ldots, u_k \geqslant 1$, $u_1 \mid \cdots \mid u_k$.

Доказательство. Пусть $A = \langle a_1, \ldots, a_n \rangle$. Тогда $A \cong G/H$, где G — свободная абелева группа ранга n, $H \leqslant G$ — свободная абелева группа ранга k. Выберем в G и H согласованные базисы $(g_1, \ldots, g_n)$ и $(h_1, \ldots, h_k)$. Заметим теперь, что $G = \langle g_1 \rangle \oplus \cdots \oplus \langle g_n \rangle$, $H = \langle h_1 \rangle \oplus \cdots \oplus \langle h_k \rangle$ и, более того, $\forall i \in \{1, \ldots, k\} : \langle h_i \rangle \leqslant \langle g_i \rangle$. Тогда, считая, что $h_{k+1} = \cdots = h_n = 0$, получим:

$$A \cong G/H \cong \bigoplus_{i=1}^{n} \langle g_i \rangle / \langle h_i \rangle \cong \mathbb{Z}_{u_1} \oplus \cdots \oplus \mathbb{Z}_{u_k} \oplus \mathbb{Z}^{n-k}$$

□

Замечание. Возможна ситуация, в которой несколько первых прямых слагаемых в разложении A в доказательстве следствия выше — это нулевые подгруппы.

Утверждение 4.7. *Пусть $n \in \mathbb{N}$, $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ — каноническое разложение n. Тогда $\mathbb{Z}_n \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$.*

Доказательство. Положим $G := \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$ и рассмотрим элемент $g := (\overline{1}, \ldots, \overline{1}) \in G$. Тогда $\operatorname{ord} g = \text{НОК}(p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}) = \prod_{i=1}^{k} p_i^{\alpha_i} = n$. Значит, $G = \langle g \rangle$ и $G \cong \mathbb{Z}_n$. □

Определение 4.6. Пусть p — простое число, $\alpha \in \mathbb{N}$. Группа $\mathbb{Z}_{p^\alpha}$ называется *примарной циклической группой.*

Следствие. Пусть G — конечнопорожденная абелева группа. Тогда G представима в виде прямой суммы $\mathbb{Z}^k$ и примарных циклических групп:

$$G \cong \mathbb{Z}^k \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha_t}}$$

Замечание. Числа в наборе $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ могут совпадать.

Определение 4.7. Пусть G — абелева группа. Ее *периодической частью*, или *подгруппой кручения*, называется $\operatorname{Tor} G := \{g \in G : \operatorname{ord} g \in \mathbb{N}\}$.

Утверждение 4.8. *Пусть G — абелева группа. Тогда $\operatorname{Tor} G \leqslant G$.*

Доказательство. Пусть $a, b \in \operatorname{Tor} G$, то есть $\exists n, k \in \mathbb{N} : na = 0,\ kb = 0$. Тогда $n(-a) = -na = 0$ и $nk(a+b) = k(na) + n(kb) = 0$, поэтому $-a \in \operatorname{Tor} G$ и $a + b \in \operatorname{Tor} G$. □

Замечание. Для неабелевой группы G утверждение выше необязательно верно. Например, произведение двух вращений на угол π в SO_3 может быть вращением на угол, не являющийся рациональным кратным π.

Утверждение 4.9. *Пусть G — абелева группа. Тогда $G/\operatorname{Tor} G$ — это группа без кручения, то есть $\operatorname{Tor}(G/\operatorname{Tor} G) = \{\operatorname{Tor} G\}$.*

Доказательство. Если $a + \operatorname{Tor} G \in G/\operatorname{Tor} G$ и $n(a + \operatorname{Tor} G) = \operatorname{Tor} G$ для некоторого $n \in \mathbb{N}$, то $na \in \operatorname{Tor} G$, но тогда и $a \in \operatorname{Tor} G$. □

Утверждение 4.10. *Если $G = \mathbb{Z}^k \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha_t}}$, то $\operatorname{Tor} G = \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha_t}}$, и $G/\operatorname{Tor} G \cong \mathbb{Z}^k$.*

Доказательство. Положим $H := \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha_t}}$. Если $g \in H$, то $g \in \operatorname{Tor} G$. Если же $g \notin H$, то одна из первых k компонент g — ненулевая, поэтому порядок g бесконечен. Тогда:

$$G/\operatorname{Tor} G = G/(\{(\underbrace{0, \ldots, 0}_{k})\} \oplus H) \cong \mathbb{Z}^k/\{(\underbrace{0, \ldots, 0}_{k})\} \oplus H/H \cong \mathbb{Z}^k$$

□

Следствие. Пусть G — конечнопорожденная группа, представимая в следущем виде:

$$G \cong \mathbb{Z}^k \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha_t}} \tag{*}$$

Тогда G однозначно задает k и $\mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha_t}} \cong \operatorname{Tor} G$.

Доказательство. Вторая часть утверждения уже доказана, а первая верна потому, что при $l \neq k$ у $\mathbb{Z}^l$ и $\mathbb{Z}^k$ различное число базисных элементов, поэтому $\mathbb{Z}^l \ncong \mathbb{Z}^k$. □

Утверждение 4.11. *Пусть G — конечная группа, $q_1, \ldots, q_s$ — все простые делители $|G|$, $Q_{q_1}, \ldots, Q_{q_s} \leqslant G$ — соответствующие силовские подгруппы в G. Тогда $\forall i \in \{1, \ldots, s\}$: Q_{q_i} — это прямая сумма всех слагаемых в (*), для которых $p_j = q_i$.*

Доказательство. Заметим, что произведение порядков слагаемых в (*), для которых $p_j = q_i$, — это наибольшая степень q_i, входящая в $|G|$, то есть $|Q_{q_i}|$. Но все силовские подгруппы в абелевой группе нормальны и потому единственны, что и означает требуемое. □

Следствие. Конечная группа G однозначно задает прямые суммы всех слагаемых с одним и тем же p_j.

Утверждение 4.12. *Пусть q — простое число, H — q-группа, и $H = \mathbb{Z}_{q^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{q^{\alpha_t}}$. Тогда H однозначно задает набор $\alpha_1, \ldots, \alpha_t$.*

Доказательство. Проведем индукцию по $|H|$. Если $|H| = q$, то тогда $H \cong \mathbb{Z}_q$. Пусть теперь $|H| = q^n, n > 1$. Тогда рассмотрим $qH = \{qh : h \in H\} \cong \mathbb{Z}_{q^{\alpha_1 - 1}} \oplus \dots \oplus \mathbb{Z}_{q^{\alpha_t - 1}}$, поэтому $H/qH = \underbrace{\mathbb{Z}_q \oplus \dots \oplus \mathbb{Z}_q}_{t}$, $|H/qH| = q^t$. Значит, число t задано однозначно. По предположению индукции для qH, те числа из набора $\alpha_1, \dots, \alpha_t$, которые больше единицы, заданы однозначно. Но и количество единиц задано однозначно в силу однозначности t. □

Теорема 4.7. *Пусть G — конечнопорожденная абелева группа. Тогда G представима в виде прямой суммы $\mathbb{Z}^k$ и примарных циклических групп:*

$$G \cong \mathbb{Z}^k \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{\alpha_t}}$$

Более того, в любом таком представлении G одно и то же число k и один и тот же набор $p_1^{\alpha_1}, \dots, p_t^{\alpha_t}$.

Доказательство. Существование такого разложения уже было доказано. Единственность выполнена в силу утверждений выше. □

Следствие. Пусть G — конечнопорожденная абелева группа без кручения, то есть $\operatorname{Tor} G = \{0\}$. Тогда G — свободная абелева группа.

Пример. Сами подгруппы, образующие разложение, могут быть заданы неоднозначно.

1. $G = \mathbb{Z}_p^n$ — линейное пространство над $\mathbb{Z}_p$, поэтому для любого базиса $(\overline{e_1}, \dots, \overline{e_n})$ в $\mathbb{Z}_p^n$ выполнено $G = \langle \overline{e_1} \rangle \oplus \dots \oplus \langle \overline{e_n} \rangle$
2. $G = \mathbb{Z} \oplus \mathbb{Z}_2 = \langle (1, \overline{1}) \rangle \oplus \langle (0, \overline{1}) \rangle$

Замечание. Рассмотрим разложение $G \cong Z^l \oplus \mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_k}$, где $l, u_1, \dots, u_k \in \mathbb{Z}$, $l \geqslant 0$, $u_1, \dots, u_k > 1$, $u_1 \mid \dots \mid u_k$. Теорема выше позволяет показать, что $l, u_1, \dots, u_k$ также заданы однозначно.

Следствие. Пусть F — поле, $G \leqslant F^*$ — конечная подгруппа. Тогда G — циклическая. В частности, если F конечно, то F^* — циклическая группа.

Доказательство. Рассмотрим разложение $G \cong \mathbb{Z}_{u_1} \oplus \dots \oplus \mathbb{Z}_{u_k}$, где $u_1, \dots, u_k \in \mathbb{Z}$, $u_1, \dots, u_k > 1$, $u_1 \mid \dots \mid u_k$, тогда $|G| = u_1 \cdots u_k$. Для любого элемента $g \in G$ выполнено $g^{u_k} = 1$. Значит, все элементы G — это корни многочлена $x^{u_k} - 1$, то есть $|G| \leqslant u_k$. Следовательно, $k = 1$ и $G \cong \mathbb{Z}_{u_k}$. □

5 Кольца и поля

5.1 Идеалы колец и факторкольцо

Напоминание. *Кольцом* называется множество R с определенными на нем бинарными операциями $+$ и $\cdot$ такими, что:

1. $(R, +)$ — абелева группа
2. $\forall a, b, c \in R : a(bc) = (ab)c$ (то есть $(R, \cdot)$ является *полугруппой*)
3. $\forall a, b, c \in R : a(b + c) = ab + ac$, $(a + b)c = ac + bc$

R называется *кольцом с единицей*, если в нем есть нейтральный элемент относительно умножения, обозначаемый через 1.

Пример. Рассмотрим несколько примеров колец:

1. $\mathbb{Z}$, $\mathbb{Z}_n$
2. $F[x]$, где F — произвольное поле
3. $M_n(F)$, где F — произвольное поле

Напоминание. *Алгеброй* над полем F называется множество R с определенными на нем бинарными операциями $+$ и $\cdot$ и операцией умножения на скаляры из F такими, что:

1. $(R, +, \cdot)$ — кольцо
2. R — линейное пространство над F
3. $\forall \alpha \in F : \forall a, b \in A : \alpha(ab) = (\alpha a)b = a(\alpha b)$

R называется *алгеброй с единицей*, если в ней есть нейтральный элемент относительно умножения, обозначаемый через 1.

Замечание. Мы всегда предполагаем, что 0 и 1 в кольце или алгебре не совпадают.

Определение 5.1. *Подкольцом* кольца R называется множество $S \subset R$, $S \neq \varnothing$, замкнутое относительно сложения, умножения и взятия обратного элемента относительно сложения. Обозначение — $S \leqslant R$.

Подалгеброй алгебры R над полем F называется $S \leqslant R$ — подкольцо, замкнутое относительно умножения на скаляры из F. Если R — кольцо (алгебра) с единицей, то S называется *подкольцом (подалгеброй) с единицей* при условии, что $1 \in S$.

Замечание. $M_n(F) \supset M_{n-1}(F)$, но единицы в этих кольцах различны, поэтому $M_{n-1}(F)$ — подкольцо в $M_n(F)$, но не подкольцо с единицей.

Замечание. Если R — алгебра с единицей 1 над полем F, то тогда $F \cdot 1 \leqslant R$ — подалгебра, изоморфная F, причем $F \cdot 1$ содержится в центре алгебры.

Определение 5.2. Пусть R, S — кольца. *Гомоморфизмом колец* R и S называется отображение $\varphi : R \to S$ такое, что $\forall x, y \in R : \varphi(x + y) = \varphi(x) + \varphi(y)$, $\varphi(xy) = \varphi(x)\varphi(y)$.

Если R, S — кольца с единицей, то φ называется *гомоморфизмом колец с единицей* при условии, что $\varphi(1) = 1$.

Замечание. Гомоморфизм алгебр над одним полем F — это гомоморфизм колец, являющийся при этом линейным отображением.

Определение 5.3. Пусть R, S — кольца, $\varphi : R \to S$ — гомоморфизм R и S. Тогда:

- ▷ *Образом* φ называется $\operatorname{Im}\varphi := \varphi(R)$
- ▷ *Ядром* φ называется $\operatorname{Ker}\varphi := \varphi^{-1}(0)$

Определение 5.4. Пусть R — кольцо (алгебра), $I \subset R$. I называется *идеалом* R, если:

1. $(I, +) \leqslant (R, +)$ (в случае, когда R — алгебра, I должно быть подпространством в R)
2. $\forall a \in R : aI \subset I, Ia \subset I$

Обозначение — $I \trianglelefteq R$.

Напоминание. В любом кольце R выполнено свойство $\forall a \in R : 0a = a0 = 0$.

Утверждение 5.1. *Пусть $\varphi : R \to S$ — гомоморфизм колец (алгебр). Тогда $\operatorname{Im}\varphi \leqslant S$ и $\operatorname{Ker}\varphi \trianglelefteq R$.*

Доказательство.

1. Пусть $a, b \in \operatorname{Im}\varphi$, то есть $a = \varphi(x), b = \varphi(y), x, y \in R$. Тогда $a + b = \varphi(a + b), -a = \varphi(-x), ab = \varphi(xy) \in \operatorname{Im}\varphi$ (а в случае гомоморфизма алгебр $\forall \alpha \in F : \alpha a = \alpha\varphi(x) = \varphi(\alpha x) \in \operatorname{Im}\varphi$) поэтому $\operatorname{Im}\varphi \leqslant S$.
2. Пусть $x, y \in \operatorname{Ker}\varphi$, тогда $\varphi(x + y) = \varphi(x) + \varphi(y) = 0$, $\varphi(-x) = -\varphi(x) = 0$ (а в случае гомоморфизма алгебр $\forall \alpha \in F : \varphi(\alpha x) = \alpha\varphi(x) = 0$). Наконец, $\forall a \in R : \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)0 = 0$ и, аналогично, $\forall a \in R : \varphi(xa) = 0$. Значит, $\operatorname{Ker}\varphi \trianglelefteq R$.

□

Определение 5.5. Пусть R — кольцо, $I \trianglelefteq R$, $I \neq R$. Тогда R/I — аддитивная факторгруппа. Определим умножение на R/I следующим образом: $\forall a, b \in R : (a + I)(b + I) := ab + I$.

Замечание. В отличии от случая факторгруппы, здесь операция задана не инвариантным образом, поэтому требуется проверить корректность определения. Пусть $a' \in a + I$, тогда $a' = a + x, x \in I$, поэтому $a'b = ab + xb \in ab + I$. Аналогично проверяется независимость от выбора представителя во втором множителе.

Теорема 5.1. *Пусть R — кольцо, $I \trianglelefteq R$, $I \neq R$. Тогда $(R/I, +, \cdot)$ — кольцо. Более того, отображение $\pi : R \to R/I$, $\forall a \in R : \pi(a) = a + I$, является сюръективным гомоморфизмом колец.*

Доказательство. Проверим сначала, что φ сохраняет операции:

- ▷ (Сложение) $\forall a, b \in I : \pi(a + b) = a + b + I = (a + I) + (b + I) = \pi(a) + \pi(b)$
- ▷ (Умножение) $\forall a, b \in I : \pi(ab) = ab + I = (a + I)(b + I) = \pi(a)\pi(b)$

Отображение π сюръективно и сохраняет операции, из чего следует, что R/I — кольцо, а π — гомоморфизм колец. □

Определение 5.6. Пусть R — кольцо, $I \trianglelefteq R$, $I \neq R$. Кольцо R/I называется *факторкольцом* R по I.

Замечание. В терминах теоремы выше, $\operatorname{Ker}\pi = I$ аналогично случаю факторгруппы. Значит, любой идеал является ядром некоторого гомоморфизма.

Замечание. Если R — кольцо с единицей 1, $I \trianglelefteq R$. Легко видеть, что тогда $I \neq R \Leftrightarrow 1 \notin I$. При $I \neq R$ факторкольцо I/R является кольцом с единицей $1 + I \neq I$.

Теорема 5.2 (Основная теорема о гомоморфизмах колец)**.**

1. *Пусть R — кольцо, $I \trianglelefteq R$, $I \neq R$. Тогда $\exists \pi : R \to R/I$ — эпиморфизм колец такой, что* $\operatorname{Ker}\varphi = I$.

2. *Пусть R, S — кольца, $\varphi : R \to S$ — гомоморфизм колец. Тогда $I := \operatorname{Ker}\varphi \trianglelefteq R$, и, более того,* $\operatorname{Im}\varphi \cong R/I$.

Доказательство. Большая часть теоремы уже была доказана выше, остается доказать лишь последнее утверждение. Мы уже знаем, что $(\operatorname{Im}\varphi, +) \cong (R/I, +)$, причем этот изоморфизм групп имеет вид $\Theta : \operatorname{Im}\varphi \to R/I$, $\forall x \in \operatorname{Im}\varphi : \Theta(x) = \varphi^{-1}(x)$. Проверим, что Θ сохраняет умножение: $\forall x, y \in \operatorname{Im}\varphi : \forall a \in \varphi^{-1}(x) : \forall b \in \varphi^{-1}(y) : ab \in \varphi^{-1}(xy) \Rightarrow \Theta(x) = a + I, \Theta(y) = b + I, \Theta(xy) = ab + I$, поэтому $\Theta(xy) = \Theta(x)\Theta(y)$. $\square$

Замечание. Аналогично случаю групп, Θ^{-1} имеет следующий вид: $\forall a + I \in R/I : \Theta^{-1}(a + I) = \varphi(a)$. Кроме того, имеет место аналогичная коммутативная диаграмма:

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & \operatorname{Im}\varphi \leqslant S \\ & R/I \arrow[ur, "\Theta"'] & \end{tikzcd}$$

Замечание. Если R — алгебра с единицей, то понятия идеала в R как в кольце и как в алгебре эквивалентны, поскольку $F \cong F \cdot 1 \leqslant R$. Дальнейшая теория для гомоморфизмов алгебр (вне зависимости от наличия единицы в R) строится аналогоично, но с некоторым дополнением.

Определение 5.7. Пусть V — линейное пространство над полем F, $U \leqslant V$. Тогда $(U, +) \leqslant (V, +)$, поэтому можно определить факторгруппу $(V/U, +) = \{\overline{v} + U : \overline{v} \in V\}$. Определим умножение на скаляры из F на V/U следующим образом: $\forall \alpha \in F : \forall \overline{v} \in V : \alpha(\overline{v} + U) := \alpha v + U$.

Замечание. Корректность определения выше проверяется аналогично случаю колец. Далее аналогичным образом можно доказать, что $\pi : V \to V/U$, $\forall \overline{v} \in V : \pi(\overline{v}) = \overline{v} + U$ — сюръективное линейное отображение такое, что $\operatorname{Ker}\pi = U$, поэтому V/U — линейное пространство, называемое *факторпространством.*

Наконец, если R — алгебра, $I \trianglelefteq R$, $I \neq R$, то R/I — алгебра, и также имеет место основная теорема о гомоморфизмах алгебр.

Упражнение. *Пусть V — конечномерное линейное пространство, $\varphi \in \mathcal{L}(V)$, $U \leqslant V$ инвариантно относительно φ. Тогда в базисе, согласованном с U, матрица φ имеет вид:*

$$\varphi \underset{e}{\leftrightarrow} A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

Докажите, что D — это матрица оператора $\psi \in \mathcal{L}(V/U)$ такого, что $\forall \overline{v} \in V : \psi(\overline{v} + U) = \varphi(\overline{v}) + U$.

Решение. Проверим сначала, что оператор ψ определен корректно. Пусть $\overline{v} + U = \overline{w} + U$, тогда $\overline{v} - \overline{w} \in U$ и $\overline{v} = \overline{w} + \overline{u}, \overline{u} \in U$. Значит, $\psi(\overline{v} + U) = \varphi(\overline{v}) + U = \varphi(\overline{w} + \overline{u}) + U = \varphi(\overline{w}) + U$.

Пусть теперь $e = (\overline{e_1}, \dots, \overline{e_n})$ — такой базис в V, что $(\overline{e_1}, \dots, \overline{e_k})$ — базис в U. Легко убедиться, что тогда $(\overline{e_{k+1}} + U, \dots, \overline{e_n} + U)$ — базис в V/U. Значит, в данном базисе D — это матрица оператора ψ.

Замечание. Аналогично случаю групп, имеют место теоремы об изоморфизмах колец и алгебр.

Определение 5.8. Пусть R — кольцо, $I \trianglelefteq R$, $I \neq R$. I называется *максимальным идеалом*, если $\forall J \trianglelefteq R, I \subsetneq J : J = R$.

Определение 5.9. Пусть R — кольцо, $a \in R$. *Главным идеалом, порожденным a*, называется наименьший по включению идеал, содержащий a. Обозначение — (a).

Замечание. Если R — коммутативное кольцо с единицей, то $(a) = aR := \{ar : r \in R\}$, а если R — некоммутативное кольцо с единицей, то $(a) = RaR := \{\sum_{i=1}^{n} r_i a s_i : \forall i \in \{1, \dots, n\} : r_i, s_i \in R\}$.

Теорема 5.3. *Пусть R — коммутативное кольцо с единицей, $I \trianglelefteq R$, $I \neq R$. Тогда I максимален $\Leftrightarrow$ R/I — поле.*

Доказательство.

- $\Leftarrow$ Пусть I не максимален, то есть $\exists J \trianglelefteq R : J \neq R, I \subsetneq J$. Легко показать, что тогда $J/I \trianglelefteq R/I$, причем $J/I \neq \{I\}$ и $J/I \neq R/I$. Но в поле любой ненулевой идеал совпадает со всем полем, поскольку он содержит единицу поля, — противоречие.

- $\Rightarrow$ Пусть I максимален, $a + I \in R/I$, $a \notin I$. Рассмотрим идеал $J = I + (a) \trianglelefteq R$. В силу максимальности I, $J = R$. Значит, $1 \in J$, то есть единица представима в виде $1 = x + ar, x \in I, r \in R$. Значит, $(a + I)(r + I) = (1 - x) + I = 1 + I$. Поскольку $1 + I$ — это единица в R/I, то $a + I$ обратим в I и, в силу произвольности a, R/I — поле.

$\square$

Замечание. Если p — простое число, то $p\mathbb{Z} \trianglelefteq \mathbb{Z}$ — максимальный идеал, поэтому $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ — поле.

Замечание. Некоммутативное кольцо с единицей без нетривиальных идеалов может содержать необратимые элементы, поэтому теорема выше для некоммутативных колец неверна.

Упражнение. *Пусть F — поле. Докажите, что в кольце $M_n(F)$ нет нетривиальных идеалов.*

Решение. Пусть $I \trianglelefteq M_n(F)$ и $I \neq \{0\}$. Все матрицы одного ранга можно привести к одному и тому же упрощенному виду элементарными преобразованиями и $M_n(F)I, IM_n(F) \subset I$. Следовательно, если I содержит одну матрицу ранга k, то I содержит все матрицы ранга k.

Поскольку $I \neq \{0\}$, то в I есть матрица ненулевого ранга. Значит, I содержит все матрицы этого ранга, и из них легко получить с помощью сложения матрицы произвольного ранга. Таким образом, I содержит все матрицы произвольного ранга, то есть $I = M_n(F)$.

Определение 5.10. Кольцо, не имеющее нетривиальных идеалов, называется *простым.*

5.2 Кольцо многочленов над полем

Напоминание. *Кольцо многочленов над полем* F — это множество формальных записей вида $a_n x^n + \ldots + a_0$, $\forall i \in \{0, \ldots, n\} : a_i \in F$. Обозначение — $F[x]$.

Теорема 5.4. *Пусть F — поле. Тогда:*

1. *Любой идеал в $F[x]$ — главный*
2. *Если $p \in F[x]$, то идеал (p) максимален $\Leftrightarrow$ многочлен p неприводим над F.*

Доказательство.

1. Пусть $I \trianglelefteq F[x]$. Если $I = \{0\}$, то $I = (0)$. В противном случае выберем многочлен $p \in I$, $p \neq 0$, наименьшей степени. Тогда, из соображений деления с остатком, $\forall g \in I : p \mid g$. Значит, $(p) = pF[x] = I$.
2. Если $p \in F$, $p \neq 0$, то $(p) = (1) = F[x]$ — не максимальный идеал. Если $p = p_1 p_2$, $\deg p_1, \deg p_2 < \deg p$, то $(p_1), (p_2) \supset (p)$. Пусть теперь p неприводим. Тогда рассмотрим $J = (q) \trianglelefteq F[x]$, $J \supset (p)$. Значит, $q \mid p$, и либо p, q ассоциированы, либо $q \in F$. В первом случае $(p) = (q)$, а во втором — $(q) = (1) = F[x]$.

$\square$

Замечание. Если $p \in F[x]$ неприводим, то в поле $K := F[x]/p$ есть подполе, изоморфное p, имеющее вид $\{\overline{\alpha} = \alpha + (p) : \alpha \in F\}$. Поэтому можно считать, что $F \leqslant K$. Кроме того, $\overline{x} = x + (p) \in K$, и $p(\overline{x}) = p(x) + (p) = (p)$. Поскольку (p) — нулевой элемент в K, то $\overline{x}$ — это корень p в поле K.

Определение 5.11. Пусть R — коммутативное кольцо, $S \leqslant R$. Тогда:

- R называется *расширением* кольца S.
- *Расширением кольца S элементами $a_1, \ldots, a_k \in R$* называется наименьшее по включению подкольцо в R, которое содержит S и $a_1, \ldots, a_k$. Обозначение — $S[a_1, \ldots, a_k]$.

Замечание. $S[a_1, \ldots, a_k] = \{p(a_1, \ldots, a_k) : p \in S[x_1, \ldots, x_k]\}$.

Определение 5.12. Пусть K — поле, $F \leqslant K$. Тогда:

- K называется *расширением* поля F.
- *Расширением поля F элементами $a_1, \ldots, a_k \in K$* называется наименьшее по включению подполе в K, которое содержит F и $a_1, \ldots, a_k$. Обозначение — $F(a_1, \ldots, a_k)$.

Замечание. Аналогично случаю колец, выполнено равенство:

$$F(a_1, \ldots, a_k) = \left\{ \frac{p(a_1, \ldots, a_k)}{q(a_1, \ldots, a_k)} : p, q \in F[x_1, \ldots, x_k], q(a_1, \ldots, a_k) \neq 0 \right\}$$

Определение 5.13. Если поле K — расширение поля F, то K — это линейное пространство над F. Размерность K называется *степенью расширения*. Обозначение — $[K : F]$. Расширение называется *конечным*, если его степень конечна.

Замечание. Если F, K, L — поля такие, что $F \leqslant K \leqslant L$ и оба расширения конечны, то $[L : F] = [L : K][K : F]$.

Определение 5.14. Пусть K — расширение поля F, $a \in K$. Элемент a называется *алгебраическим над* F, если $\exists p \in F[x], p \neq 0 : p(a) = 0$. Многочлен наименьшей степени, удовлетворяющий этому условию, называется *минимальным многочленом* элемента a.

Теорема 5.5. *Пусть K — расширение поля F, $a \in K$. Тогда:*

1. *a — алгебраический над F $\Leftrightarrow$ расширение $F(a)$ конечно*
2. *Если расширение $F(a)$ конечно, то $F(a) = F[a] \cong F[x]/(p)$, где p — минимальный многочлен элемента a*

Доказательство.

1. Рассмотрим поле $F(a)$ и систему элементов $\{1, a, a^2, \ldots\}$ в нем. Если a — не алгебраический над F, то эта система линейно независима над F, поэтому $[F(a) : F] = \infty$. Если же a — алгебраический над F, то для некоторого $p \in F[x], \deg p = n \geqslant 1$ выполнено $p(a) = 0$. Отсюда a^n выражается через $1, \ldots, a^{n-1}$, и, по индукции, $\forall k \in \mathbb{N} : a^{n+k}$ выражается через $1, \ldots, a^{n-1}$. Значит, $\dim F[a] \leqslant n$, и, в силу следующего пункта, $\dim F(a) \leqslant n$.

2. Рассмотрим p — минимальный многочлен элемента a. В силу минимальности, p неприводим над F, и $F[x]/(p)$ — это поле. Рассмотрим гомоморфизм колец $\varphi : F[x] \to K$, $\forall q \in F[x] : \varphi(q) = q(a)$. Пусть $I := \operatorname{Ker} \varphi$, тогда $p \in I$ и $(p) \subset I$. Поскольку идеал (p) максимален и $I \neq F[x]$, то $I = (p)$. Тогда, по основной теореме о гомоморфизмах колец, $F[x]/(p) \cong \operatorname{Im} \varphi = F[a]$. Но $F[x]/(p)$ — поле, поэтому $F[a]$ — тоже поле и $F[a] = F(a)$.

□

Следствие. Если K — расширение поля F и $a_1, \ldots, a_k \in K$ — алгебраические над F, то и все элементы в $F(a_1, \ldots, a_k)$ — тоже алгебраические, поскольку степень $[F(a_1, \ldots, a_k) : F]$ конечна.

Замечание. Мы доказали, что расширение поля корнем неприводимого многочлена единственно с точностью до изоморфизма. Отсюда можно получить индукцией по степени многочлена, что поле разложения любого многочлена единственно с точностью до изоморфизма. Следовательно, поле порядка p^n, полученное как поле разложения многочлена $x^{p^n} - x$ над $\mathbb{Z}_p$, единственно с точностью до изоморфизма.