Теория групп

И. И. Богданов
Конспект подготовил Александр Васильев

ФИВТ МФТИ
2016

Оглавление

Глава 1

Группы и подгруппы

1.1 Основные понятия

Определение 1.1. *Группа* — это непустое множество G с бинарной операцией $\cdot$, обладающей следующими свойствами:

- Ассоциативность: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Существование нейтрального элемента: $\exists e \in G$: $\forall a \in G \ \ ae = ea = a$
- Существование обратного элемента: $\forall a \in g \ \ \exists a^{-1} \in G$: $aa^{-1} = a^{-1}a = e$

Обозначение — $(G, \cdot)$, если операция очевидна — просто G. Группа называется *абелевой*, если операция $\cdot$ коммутативна ($a \cdot b = b \cdot a$).

Замечание. Нейтральный и обратные элементы единственны.

Определение 1.2. *Подгруппа* $H < G$ — это непустое подмножество $H \subseteq G$, замкнутое относительно операций: $\forall a, b \in H \ \ a \cdot b \in H$, $\forall a \in H \ \ a^{-1} \in H$.

Замечание. H — также группа, с той же операцией (ограниченной на H).

Определение 1.3. *Порядок группы* — число её элементов $|G|$. *Порядок элемента* группы $g \in G$ — это наименьшее $n \in \mathbb{N}$ такое, что $g^n = e$ (и ∞, если такого n нет). Обозначение: $|g|$ или $\operatorname{ord} g$.

Определение 1.4. Если $M \subset G$, то *подгруппа, порождённая* M — это пересечение всех подгрупп, содержащих M. Также $\langle M \rangle = \{a_1 \dots a_n \mid a_i \in M \vee a_i^{-1} \in M\}$. Обозначение: $\langle M \rangle$. Если существует $g \in G$ такой, что $\langle g \rangle = G$, то группа G — *циклическая.*

Пример. $\langle G \rangle = G$, $\langle \varnothing \rangle = \{e\}$.

Замечание. $\operatorname{ord} g = |\langle g \rangle|$.

Определение 1.5. Биекция $\varphi : G \to H$, сохраняющая операцию ($\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$), называется *изоморфизмом групп* G и H. Если он существует, то G и H *изоморфны* ($G \cong H$).

1.2 Примеры групп

1. $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$ — единственные (с точностью до изоморфизма) циклические группы. Подгруппа циклической группы — также циклическая.
2. $(F, +)$, $(F^*, \cdot)$, где F — поле.
3. $(V, +)$, где V — линейное пространство.
4. S_n — группа перестановок n элементов (т. е. биекций $\{1, \dots, n\} \to \{1, \dots, n\}$) относительно композиции. Перестановку можно записать в виде таблицы, или же в виде произведение независимых циклов (цикл $\pi = (a_1 \dots a_k)$ — это перестановка такая, что $\pi(a_i) = a_{i+1}$ для $i = 1, \dots, k-1$ и $\pi(a_k) = a_1$, остальные элементы неподвижны). Кроме того, S_n порождается множеством всех транспозиций. Знак перестановки $\sigma \in S_n$ есть $(-1)^\sigma = \operatorname{sgn}\sigma = (-1)^{N(\sigma)}$, где $N(\sigma)$ — число инверсий в σ (совпадает по чётности с количеством транспозиций в любом разложении σ).
5. $GL_n(F)$ — группа невырожденных матриц над F относительно умножения.
6. $GL(V)$, где V — линейное пространство над F, — обратимые преобразования V относительно композиции. $GL(V) \cong GL_{\dim V}(F)$.
7. Подгруппы этих групп, в частности:
   - $A_n < S_n$ — подгруппа всех чётных перестановок.
   - $SL_n(F) < GL_n(F)$ — подгруппа всех матриц с единичным определителем.
   - $O_n < GL_n(\mathbb{R})$ — подгруппа всех ортогональных матриц.
   - $\mathbb{C}_n < \mathbb{C}^*$: $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$, $\mathbb{C}_n \cong \mathbb{Z}_n$.

1.3 Смежные классы

Определение 1.6. Пусть $H < G$, $g \in G$. *Левый смежный класс* элемента g по H — это gH, *правый* — Hg, где $AB = \{ab \mid a \in A, b \in B\}$ для $A, B \subset G$ (вместо одного элемента подразумевается множество из этого элемента). G/H — множество всех левых смежных классов по H, $H\backslash G$ — правых.

Замечание. Для любых $a, b \in G$ $aH \cap bH \neq \varnothing \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH = bH \Leftrightarrow b \in aH$. Значит, левые (правые) смежные классы — разбиение G.

Утверждение 1.1. *Пусть $H < G$. Тогда G/H равномощно $H\backslash G$.*

Доказательство. Построим биекцию $\varphi : G/H \to H\backslash G$: $\varphi(gH) = Hg^{-1}$. Заметим, что $\varphi(gH) = Hg^{-1} = H^{-1}g^{-1} = (gH)^{-1}$, а тогда φ корректно определено и является отображением из G/H в $H\backslash G$. Биективность следует из существования $\varphi^{-1} : Hg \mapsto g^{-1}H$. ■

Замечание. Отображение $gH \mapsto Hg$ не всегда корректно определено.

Определение 1.7. Если $H < G$, то *индексом* H в G называется $|G : H| = |G/H| = |H\backslash G|$.

Теорема 1.1 (Лагранжа)**.** *Для конечной группы* $|G| = |H| \cdot |G : H|$.

Следствие. $|H|$ *делит* $|G|$*, и для любого* $g \in G$ $|g|$ *делит* $|G|$.

1.4 Нормальные подгруппы

Определение 1.8. Пусть $H < G$. H называется *нормальной подгруппой* в G ($H \lhd G$), если $\forall g \in G\ gH = Hg$.

Замечание. Эквивалентно: $H = g^{-1}Hg$.

Примеры.

1. $G \lhd G$.
2. $\{e\} \lhd G$.
3. Если G — абелева, то все подгруппы нормальны.
4. $A_n \lhd S_n$. Действительно, если $\sigma \in A_n$, то $\sigma A_n = A_n = A_n\sigma$. Иначе, $\sigma A_n = S_n \setminus A_n = A_n\sigma$.
5. $\langle(1\ 2)\rangle \not\lhd S_3$. $\langle(1\ 2)\rangle = \{\mathrm{id}, (1\ 2)\}$. $(1\ 3)\langle(1\ 2)\rangle = \{(1\ 3), (1\ 2\ 3)\}$, но $\langle(1\ 2)\rangle(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$.

Утверждение 1.2. *Пусть* $H < G$, $|G : H| = 2$. *Тогда* $H \lhd G$.

Доказательство. G разбивается на левые смежные классы по H, один из них — $H = eH$, а значит другой — $G \setminus H$. Аналогично, правые смежные классы — H и $G \setminus H$. Значит, если $g \in H$, то $gH = Hg = H$. Если же $g \in G \setminus H$, то $gH = G \setminus H = Hg$. ■

Утверждение 1.3. *Пусть* $H_1, H_2 \lhd G$. *Тогда* $H_1 \cap H_2 \lhd G$.

Доказательство. $H_1 \cap H_2 < G$ — тривиально. Проверим, что для произвольного $g \in G$ верно $g^{-1}(H_1 \cap H_2)g = H_1 \cap H_2$. $\forall h \in H_1 \cap H_2\ g^{-1}hg \in H_1 \wedge g^{-1}hg \in H_2 \Rightarrow g^{-1}hg \in H_1 \cap H_2$. Мы показали, что $\forall g \in G\ g^{-1}(H_1 \cap H_2)g \subseteq H_1 \cap H_2$. Этого достаточно: $g(H_1 \cap H_2)g^{-1} \subseteq H_1 \cap H_2 \Rightarrow H_1 \cap H_2 = g^{-1}g(H_1 \cap H_2)g^{-1}g \subseteq g^{-1}(H_1 \cap H_2)g$. ■

Замечание. Если $H < G$ и $\forall g \in G\ g^{-1}Hg \subseteq H$, то $\forall g \in G\ g^{-1}Hg = H$.

Утверждение 1.4. *Пусть* $H \lhd G$, $K < G$. *Тогда* $HK = \{hk : h \in H, k \in K\} < G$. *Если* $K \lhd G$, *то и* $HK \lhd G$.

Доказательство. Покажем, что $HK = KH$. Действительно, $HK = \bigcup_{k\in K} Hk = \bigcup_{k\in K} kH = KH$. Теперь покажем, что $HK < G$: $(HK)(HK) = H(KH)K = HHKK = HK$; $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$.

Если же $K \lhd G$, то $\forall g \in G\ gHK = HgK = HKg \Rightarrow HK \lhd G$. ■

1.5 Сопряжение

Определение 1.9. Пусть G — группа, $g, x \in G$. Тогда элементом, *сопряжённым* к g при помощи x, называется $g^x = x^{-1}gx$.

Пример. Две матрицы одного преобразования в различных базисах сопряжены в $GL_n(F)$, их сопрягает матрица перехода.

Утверждение 1.5.

1. $g^{xy} = (g^x)^y$

2. $(g_1g_2)^x = g_1^x g_2^x$

3. $(g^{-1})^x = (g^x)^{-1}$

Доказательство.

1. $g^{xy} = y^{-1}x^{-1}gxy = y^{-1}g^x y = (g^x)^y$.

2. $g_1^x g_2^x = x^{-1}g_1xx^{-1}g_2x = x^{-1}g_1g_2x = (g_1g_2)^x$.

3. $g^x(g^{-1})^x = (gg^{-1})^x = e^x = e \Rightarrow (g^x)^{-1} = (g^{-1})^x$.

■

Утверждение 1.6. *Отношение сопряжённости — это отношение эквивалентности.*

Доказательство.

1. Рефлексивность: $g = g^e$.

2. Симметричность: g^x сопряжён к g, то $g = (g^x)^{x^{-1}}$.

3. Транзитивность: $g_2 = g_1^x$, $g_3 = g_2^y$, то $g_3 = (g_1^x)^y = g_1^{xy}$. ■

Определение 1.10. Класс элемента g относительно этого отношения — *класс сопряжённости* этого элемента g. Обозначение: g^G.

Утверждение 1.7. *Пусть $H < G$. Тогда $H \lhd G \Leftrightarrow H$ есть объединение нескольких классов сопряжённости.*

Доказательство. $H \lhd G \Leftrightarrow \forall g \in G\ H = g^{-1}Hg \Rightarrow$ вместе с любым элементом $h \in H$, $h^G \subseteq H \Rightarrow H = \bigcup_{h \in H} h^G$.

Наоборот, если $H = \bigcup_{\alpha \in A} g_\alpha^G$, то $g^{-1}Hg = \bigcup_{\alpha \in A} (g_\alpha^G)^g = \bigcup_{\alpha \in A} g_\alpha^G = H$. ■

Упражнение. Пусть $g_1, g_2 \in G$. Тогда $g_1^G \cdot g_2^G$ — объединение нескольких классов сопряжённости, но не обязательно одного.

1.6 Гомоморфизмы групп

Определение 1.11. Пусть G, H — группы. Отображение $\varphi : G \to H$ называется *гомоморфизмом групп*, если $\forall g_1, g_2 \in G\ \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$. *Образ* гомоморфизма — это $\operatorname{Im}\varphi = \varphi(G) = \{\varphi(g) \mid g \in G\}$. *Ядро* гомоморфизма $\operatorname{Ker}\varphi = \varphi^{-1}(e_H)$. Гомоморфизм называется *эпиморфизмом*, если $\operatorname{Im}\varphi = H$, и *мономорфизмом*, если φ — инъекция.

Утверждение 1.8. *Пусть $\varphi : G \to H$ — гомоморфизм. Тогда:*

1. $\varphi(e_G) = e_H$.
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Доказательство.

1. $\varphi(e) = \varphi(e^2) = \varphi(e)\varphi(e) \Rightarrow e = \varphi(e)$.
2. $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e) = e$.

■

Утверждение 1.9. *Гомоморфизм $\varphi : G \to H$ является мономорфизмом* $\Leftrightarrow \operatorname{Ker}\varphi = \{e\}$.

Доказательство. $\varphi(e) = e \Rightarrow e \in \operatorname{Ker}\varphi$. Если φ — мономорфизм, то $\forall e \neq g \in G\ \varphi(g) \neq \varphi(e) \Rightarrow \operatorname{Ker}\varphi = \{e\}$. Если $\exists g_1 \neq g_2$: $\varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g_1^{-1}g_2) = \varphi(g_1)^{-1}\varphi(g_2) = e \Rightarrow e \neq g_1^{-1}g_2 \in \operatorname{Ker}\varphi$. ■

Примеры.

1. $\varphi : G \to H$, $\varphi(g) = e$.
2. $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(a) = a \pmod n$; $\operatorname{Ker}\varphi = n\mathbb{Z}$.
3. $\varphi : GL_n(F) \to F^*$, $\varphi(A) = \det A$; $\operatorname{Ker}\varphi = SL_n$.
4. Изоморфизм является гомоморфизмом. В частности, существуют изоморфизмы группы *на себя* (*автоморфизмы*). Например, если $x \in G$, то $\varphi_x : g \mapsto g^x$ — автоморфизм.

Утверждение 1.10. *Пусть $\varphi : G \to H$ — гомоморфизм групп. Тогда* $\operatorname{Im}\varphi < H$, $\operatorname{Ker}\varphi \lhd G$.

Доказательство. Если $h_1, h_2 \in \operatorname{Im}\varphi$, то $h_i = \varphi(g_i)$. $g_i \in G \Rightarrow h_1h_2 = \varphi(g_1g_2) \in \operatorname{Im}\varphi$, $h_1^{-1} = \varphi(g_1^{-1}) \in \operatorname{Im}\varphi$. Значит, $\operatorname{Im}\varphi < H$.

Если $g_1, g_2 \in \operatorname{Ker}\varphi$, то $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = e$, $\varphi(g_1^{-1}) = e \Rightarrow g_1g_2, g_1^{-1} \in \operatorname{Ker}\varphi \Rightarrow \operatorname{Ker}\varphi < G$. Кроме того, $\varphi(x^{-1} \cdot \operatorname{Ker}\varphi \cdot x) = \varphi(x)^{-1} \cdot \varphi(\operatorname{Ker}\varphi) \cdot \varphi(x) = \varphi(x)^{-1}\varphi(x) = e \Rightarrow \forall x \in G\ x^{-1}\operatorname{Ker}\varphi \cdot x \subseteq \operatorname{Ker}\varphi \Rightarrow \operatorname{Ker}\varphi \lhd G$. ■

Замечание. Если $K < H$, то $\varphi : K \to H$, $\varphi(k) = k$ — это гомоморфизм, $\operatorname{Im}\varphi = K$.

Пусть $K \lhd G$. Рассмотрим G/K — множество левых смежных классов по K. Если $aK, bK \in G/K$, то $aK \cdot bK = a(Kb)K = abKK = abK \in G/K$ (в силу нормальности).

Теорема 1.2. $(G/K, \cdot)$ — *группа.*

Доказательство. Ассоциативность следует из ассоциативности в G. Нейтральный элемент — это $K = eK$, обратный к aK — $a^{-1}K$. ■

Определение 1.12. Полученная группа — *факторгруппа* группы G по нормальной подгруппе K.

Теорема 1.3. *Отображение* $\pi : G \to G/K$, $\pi(g) = gK$, *является эпиморфизмом,* $\operatorname{Ker}\pi = K$.

Доказательство. $\pi(g_1g_2) = g_1g_2K = g_1K \cdot g_2K = \pi(g_1)\pi(g_2) \Rightarrow \pi$ — гомоморфизм. Любой $gK \in G/K$ есть $\pi(g) \Rightarrow \pi$ — эпиморфизм. $g \in \operatorname{Ker}\pi \Leftrightarrow \pi(g) = gK = K \Leftrightarrow g \in K$. Итак, $\operatorname{Ker}\pi = K$. ■

Определение 1.13. π — *естественный* эпиморфизм $G \to G/K$.

Теорема 1.4 (основная теорема о гомоморфизмах групп)**.** *Пусть* $\varphi : G \to H$ — *гомоморфизм групп,* $\operatorname{Ker}\varphi = K$. *Тогда* $K \lhd G$ *и* $\operatorname{Im}\varphi \cong G/K$.
Наоборот, если $K \lhd G$, *то существует эпиморфизм групп* $\pi : G \to G/K$, $\operatorname{Ker}\varphi = K$.

Доказательство. Осталось доказать изоморфность образу: $\operatorname{Im}\varphi \cong G/K$.

Определим $\psi : G/K \to \operatorname{Im}\varphi$ так: $\psi(aK) = \varphi(aK) = \varphi(a)\varphi(K) = \varphi(a)$. Если $\varphi(a) \in \operatorname{Im}\varphi$, то $\varphi(a) = \psi(aK) \Rightarrow \psi$ — сюръекция. Если $\psi(aK) = \psi(bK)$, то $\varphi(a) = \varphi(b) \Rightarrow \varphi(a^{-1}b) = e \Rightarrow a^{-1}b \in \operatorname{Ker}\varphi = K \Rightarrow b \in aK \Rightarrow bK = aK$. Итак, ψ — инъекция.

Теперь покажем что ψ сохраняет операции: $\psi(aK) \cdot \psi(bK) = \varphi(a)\varphi(b) = \varphi(ab) = \psi(abK) = \psi(aK \cdot bK)$. Значит, ψ — изоморфизм. ■

Замечание. Если $h \in \operatorname{Im}\varphi$, то $\psi^{-1}(h) = \varphi^{-1}(h)$.

Примеры.

1. $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(a) = a \mod n$. $\operatorname{Ker}\varphi = n\mathbb{Z}$, $\operatorname{Im}\varphi = \mathbb{Z}_n \Rightarrow \mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.
2. $\det : GL_n(F) \to F^*$. $\operatorname{Im}\det = F^*$; $\operatorname{Ker}\det = SL_n(F) \Rightarrow GL_n(F)/SL_n(F) \cong F^*$.

Упражнение. $S_n/A_n \cong ?$.

Теорема 1.5 (первая теорема об изоморфизме)**.** *Пусть* $H \lhd G$, $K < G$. *Тогда:*

1. $HK = KH < G$.
2. $K \cap H \lhd K$.
3. $HK/H \cong K/(H \cap K)$.

Доказательство. Первый пункт уже доказан. Второй и третий следуют из рассмотрения естественного эпиморфизма: $\pi : G \to G/H$. Тогда $\pi_{HK} := \pi\big|_{HK}$ и $\pi_K := \pi\big|_K$ — гомоморфизмы групп. $\operatorname{Im}\pi_{HK} = \pi(HK) = \pi(H)\pi(K) = \pi(K) = \operatorname{Im}\pi_K$. $\operatorname{Ker}\pi_{HK} = H$, $\operatorname{Ker}\pi_K = K \cap H$. Тогда $HK/H \cong \operatorname{Im}\pi_{HK} = \operatorname{Im}\pi_K \cong K/(H \cap K)$. ■

Замечание. Явный вид изоморфизма: $k(H \cap K) \in K/(H \cap K) \leftrightarrow kH \in HK/H$.

Замечание. $K \cap H \lhd K$, поскольку $K \cap H = \operatorname{Ker}\pi_K$.

Пример. Пусть $G = S_4$, $H = V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Нетрудно поверить, что $V_4 \lhd S_4$ (V_4 называется четверной группой Клейна). Положим $K = S_3 < S_4$. $H \cap K = \{id\}$. Это значит, что $\forall h_i \in H, k_i \in K \;\; h_1k_1 = h_2k_2 \Rightarrow H \ni h_2^{-1}h_1 = k_2k_1^{-1} \in K \Rightarrow h_1 = h_2, k_1 = k_2$. Значит, $|HK| = |H| \cdot |K| = 24 \Rightarrow HK = S_4$. Применяя первую теорему об изоморфизме, имеем $S_4/V_4 = HK/H \cong K/H \cap K = S_3/\{id\} \cong S_3$.

Теорема 1.6 (Вторая теорема об изоморфизме, или теорема о соответствии)**.** *Пусть G — группа, $H \lhd G$, обозначим $\overline{G} := G/H$. Тогда:*

1. *Для подгруппы $K < G$ такой, что $H < K$, обозначим $\overline{K} := K/H$. Тогда $\overline{K} < \overline{G}$.*
2. *Соответствие $K \leftrightarrow \overline{K}$ — биекция между подгруппами в G, содержащими H, и подгруппами в $\bar{G}$.*
3. *Если $H < K < G$, то $K \lhd G \Leftrightarrow \overline{K} \lhd \overline{G}$, и в этом случае $G/K \cong \overline{G}/\overline{K}$.*

Доказательство. Рассмотрим естественный эпиморфизм $\pi : G \to G/H$ ($\pi(g) = gH$). Тогда $\pi(K) = KH/H = K/H = \overline{K}$. Наоборот, если $L < \overline{G}$, то $H < \pi^{-1}(L) < G$ (если $a, b \in \pi^{-1}(L)$, то $ab, a^{-1} \in \pi^{-1}(L)$). При этом, $\pi(\pi^{-1}(L)) = L$, ибо π — сюръекция; кроме того, для любой такой $K < G$

$$\pi^{-1}(\pi(K)) = \pi^{-1}(\overline{K}) = \bigcup_{kH \in \overline{K}} kH = \bigcup_{k \in K} kH = K.$$

Итак, π осуществляет требуемую биекцию $K \to \overline{K}$.

Если $K \lhd G$, то $g^{-1}Kg = K \Rightarrow \pi(g)^{-1}\pi(K)\pi(g) = \pi(K)$ для любого $g \in G$. Поскольку π — сюръекция, $\pi(K) = \overline{K} \lhd \overline{G}$.

Пусть $\overline{K} \lhd \overline{G}$. Тогда существует естественный эпиморфизм $\pi' : \overline{G} \to \overline{G}/\overline{K}$. Рассмотрим $\pi' \circ \pi : G \to \overline{G}/\overline{K}$. Это — эпиморфизм, при этом $\operatorname{Ker}(\pi' \circ \pi) = \pi^{-1}(\pi'^{-1}(e)) = \pi^{-1}(\overline{K}) = K$. Значит, $\overline{G}/\overline{K} = \operatorname{Im}(\pi' \circ \pi) \cong G/\operatorname{Ker}(\pi' \circ \pi) = G/K$ по основной теореме о гомоморфизмах (и $K = \operatorname{Ker}(\pi' \circ \pi) \lhd G$). ■

Пример. Пусть $m, n \in \mathbb{N}$. Тогда $\mathbb{Z} \rhd n\mathbb{Z} \rhd mn\mathbb{Z}$ (и $\mathbb{Z} \rhd mn\mathbb{Z}$). Значит, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$, $\mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}_{mn}$, а $n(\mathbb{Z}/mn\mathbb{Z}) = n\mathbb{Z}_{mn}$. Следовательно, $\mathbb{Z}_{mn}/n\mathbb{Z}_{mn} = (\mathbb{Z}/mn\mathbb{Z})/(n\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Как применить пункты 1 и 2? Все подгруппы $\mathbb{Z}$ имеют вид $k\mathbb{Z}$, $k \in \mathbb{Z}$. Тогда все подгруппы $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ есть подгруппы вида $k\mathbb{Z}/n\mathbb{Z}$, где $n\mathbb{Z} < k\mathbb{Z}$ (т. е. $k \mid n$). Значит, подгруппы в $\mathbb{Z}_n$ — это подгруппы вида $(n/k)\mathbb{Z}_n$, где $k \mid n$, т. е. $l\mathbb{Z}_n$, где $l \mid n$.

1.7 Действие группы на множество

Определение 1.14. Пусть G — группа, Ω — множество. Говорим, что определено *действие группы* G на множестве Ω, если определено отображение $G \times \Omega \to \Omega$ (т. е. для любых $g \in G$, $\omega \in \Omega$ определён $g(\omega) \in \Omega$), удовлетворяющее следующим свойствам:

1. $(gh)(\omega) = g(h(\omega))$
2. $e(\omega) = \omega$

Определение 1.15. *Действие группы* G на множество Ω — это гомоморфизм $G \to S(\Omega)$, где $S(\Omega)$ — группа всех биекций множества Ω в себя.

Утверждение 1.11. *Данные определения эквивалентны.*

Доказательство. Пусть задано действие G на Ω по определению 1.14. Положим для $g \in G$ $I_g : \Omega \to \Omega$, $I_g(\omega) = g(\omega)$. Тогда $I_{gh}(\omega) = (gh)(\omega) = g(h(\omega)) = I_g \circ I_h(\omega)$, т. е. $I_{gh} = I_g \circ I_h$. Кроме того, $I_g \circ I_{g^{-1}} = I_e = I_{g^{-1}} I_g$, причём $I_e = \mathrm{id}$. Т. е. $I_{g^{-1}}$ — это обратное отображение к I_g, а значит I_g — биекция. Итак, $g \mapsto I_g$ — это требуемый гомоморфизм.

Наоборот, пусть $g \mapsto I_g$ — гомоморфизм $G \to S(\Omega)$, то положим $g(\omega) = I_g(\omega)$. Тогда $(gh)(\omega) = I_{gh}(\omega) = I_g \circ I_h(\omega) = g(h(\omega))$, т. е. первое свойство доказано. Кроме того, $I_e = id$, т. е. $e(\omega) = \omega$. ■

Определение 1.16. Пусть $\varphi : G \to S(\Omega)$ — действие группы на множестве. Тогда *ядром* этого действия называется $\operatorname{Ker}\varphi = \{g \in G \mid \forall \omega \in \Omega \ g(\omega) = \omega\}$. Действие называется *точным* (или *эффективным*), если $\operatorname{Ker}\varphi = \{e\}$, т. е. если φ — мономорфизм.

Примеры.

1. $G = GL(V)$ действует на V: $\varphi \in GL(V)$, $v \in V$, то $\varphi(v) = \varphi(v)$ (точно).
2. S_n действует на $\{1, \ldots, n\}$ тривиальным образом (точно).
3. Если G действует на Ω, то можно определить действие G на Ω^2: $g((\omega_1, \omega_2)) = (g(\omega_1), g(\omega_2))$.
4. Рассмотрим группу O_2 — всех преобразований плоскости, и в R^2 рассмотрим правильный n-угольник D_n с центром в O Тогда можно определить группу диэдра $D_n = \{\varphi \in O_2 \mid \varphi(D_n) = D_n\}$. Тогда D_n действует на:
   (a) Плоскость R^2
   (b) Вершины n-угольника
   (c) Стороны n-угольника
   (d) Множество точке n-угольника

Определение 1.17. Пусть G действует на Ω, $\omega \in \Omega$ Тогда *орбитой* элемента ω называется $G(\omega) = \{g(\omega) \mid g \in G\}$. Два элемента $\omega_1, \omega_2 \in \Omega$ *эквивалентны* относительно действия, если $\omega_2 \in G(\omega_1)$.

Утверждение 1.12. *Определённое отношение является отношением эквивалентности, его классы — это орбиты действия.*

Доказательство. $\omega_1 = e(\omega_1)$, т. е. отношение рефлексивно. Если $\omega_2 \in G(\omega_1)$, то $\omega_2 = g(\omega_1) \Rightarrow g^{-1}(\omega_2) = g^{-1}(g(\omega_1)) = e(\omega_1) = \omega_1 \Rightarrow \omega_1 \in G(\omega_2)$ — отношение симметрично. Если $\omega_2 = g_1(\omega_1)$, $\omega_3 = g_2(\omega_2)$, то $\omega_3 = g_2(g_1(\omega_1)) = (g_2 \circ g_1)(\omega_1)$ — транзитивность.

Наконец, $\{\omega' \mid \omega' \in G(\omega)\} = G(\omega)$. ■

Следствие. *Ω разбивается на орбиты действия.*

Определение 1.18. Действие называется *транзитивным*, если у него одна орбита, т. е. $\forall \omega, \omega' \in \Omega \ \exists g \in G$: $\omega' = g(\omega)$.

Пример. У действия $GL(V)$ на V две орбиты: $\{0\}$ и $V \setminus \{0\}$.

Определение 1.19. Пусть G действует на Ω, $\omega \in \Omega$. Тогда $\mathrm{St}(\omega) = \{g \in G \mid g(\omega) = \omega\}$ называется *стабилизатором* (*стационарной подгруппой*) элемента ω.

Утверждение 1.13. $\mathrm{St}(\omega) < G$

Доказательство. Если $g, h \in St(\omega)$, то $(gh)(\omega) = g(h(\omega)) = \omega \Rightarrow gh \in \mathrm{St}(\omega)$. $g^{-1}(\omega) = g^{-1}(g(\omega)) = e(\omega) = \omega \Rightarrow g^{-1} \in \mathrm{St}(\omega)$. ■

Утверждение 1.14. *Пусть G действует на Ω, $\omega \in \Omega$, $\omega' \in G(\omega)$; пусть $\omega' = g'(\omega)$. Тогда $\{g \in G \mid \omega' = g(\omega)\} = g'St(\omega) = St(\omega')g'$*

Доказательство. $\omega' = g(\omega) \Leftrightarrow g'^{-1}(\omega') = (g'^{-1}g)(\omega) \Leftrightarrow \omega = (g'^{-1}g)(\omega) \Leftrightarrow g'^{-1}g \in St(\omega) \Leftrightarrow g \in g'St(\omega)$. Наоборот, $\omega' = g(\omega) \Leftrightarrow \omega = g^{-1}(\omega') \Leftrightarrow g^{-1} \in g'^{-1}\,\mathrm{St}(\omega') \Leftrightarrow g \in \mathrm{St}(\omega')g'$. ■

Следствие. $\mathrm{St}(\omega) = g'^{-1}St(\omega')g'$, *т. е. стабилизаторы двух элементов одной орбиты сопряжены.*

Следствие. $|G(\omega)| = |G : St(\omega)|$ *(если $G(\omega)$ — конечна, то $|G(\omega)| = \frac{|G|}{|St(\omega)|}$).*

Доказательство. Сопоставим любому $\omega' \in G(\omega)$ множество $\{g \in G \mid \omega' = g(\omega)\}$. Это множество — левый смежный класс по $\mathrm{St}(\omega)$. Ясно, что разным элементам в $G(\omega)$ соответствуют разные смежные классы и любому смежному классу соответствует $\omega' \in G(\omega)$. Итак, мы придумали биекцию между $G(\omega)$ и $G/\mathrm{St}(\omega)$. ■

Теорема 1.7 (формула орбит)**.** *Пусть группа G действует на множество $\Omega = \Omega_1 \sqcup \cdots \sqcup \Omega_k$, где Ω_i — орбиты действия, пусть $\omega_i \in \Omega_i$. Тогда*

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

1.7.1 Примеры действия группы

Действие на себя левыми сдвигами

$\Omega = G$, $\forall g, \omega \in G \;\; g(\omega) = g \cdot \omega$. Орбиты – вся G (т. е. действие транзитивно), ядро тривиально ($g \neq e \Rightarrow g\omega \neq \omega$; такое действие называется *свободным*). $\mathrm{St}(\omega) = e$. Это значит, что верна теорема Кэли:

Теорема 1.8 (Кэли)**.** *Пусть G — группа. Тогда в $S(G)$ есть подгруппа $H \cong G$.*

Доказательство. Действие левыми сдвигами определяет гомоморфизм $\varphi : G \to S(\Omega) = S(G)$, причём $\mathrm{Ker}\,\varphi = \{e\}$. Значит, φ — мономорфизм, $G \cong \mathrm{Im}\,\varphi < S(G)$. ■

Действие на смежные классы сдвигами

Пусть $H < G$. Тогда G действует левыми сдвигами на $\Omega = G/H$: $\forall g, x \in G \;\; g(xH) = gxH$ $(g_1(g_2(xH)) = g_1g_2xH = (g_1g_2)(xH)$. Орбита — G/H. Стабилизатор xH — это $\{g \mid gxH = xH\}$. Но $gxH = xH \Leftrightarrow gx \in xH \Leftrightarrow g \in xHx^{-1}$. Значит, ядро

действия есть

$$K = \bigcap_{x \in G} xHx^{-1} = \bigcap_{x \in G} \mathrm{St}(xH).$$

Утверждение 1.15. *K — наибольшая по включению подгруппа в H, которая нормальна в G.*

Доказательство. $K \lhd G$, т. к. это — ядро действия. Наоборот, если $K' \lhd G$, $K' < H$, то $\forall x \in G\ K' = xK'x^{-1} < xHx^{-1} \Rightarrow K' < \bigcap_{x \in G} xHx^{-1} = K$ ■

Упражнение. Пусть $H < G$, $|G : H| = n$. Тогда существует $L \lhd G$ такая, что $|G : L| \mid n!$.

Аналогичные действия правыми сдвигами определяются так: $g(\omega) = \omega g^{-1}$. $g(h(\omega)) = \omega h^{-1} g^{-1} = \omega (gh)^{-1} = (gh)(\omega)$, $e(\omega) = \omega$.

Действие сопряжением на себя

$\Omega = G$, $g(\omega) = \omega^{g^{-1}}$. Проверка: $g(h(\omega)) = (\omega^{h^{-1}})^{g^{-1}} = \omega^{h^{-1}g^{-1}} = \omega^{(gh)^{-1}} = (gh)(\omega)$, $e(\omega) = \omega$. Орбита $G(\omega) = \omega^G$ — класс сопряжённости, стабилизатор: $g\omega g^{-1} = \omega \Leftrightarrow g\omega = \omega g$, т. е. $\mathrm{St}(\omega) = \{g \in G \mid g\omega = \omega g\}$ — *централизатор* элемента ω, обозначается $C_G(\omega)$. Разумеется, $C_G(\omega)$ — наибольшая по включению подгруппа, все элементы которой перестановочны с ω. Ядро действия есть

$$\bigcap_{\omega \in G} C_G(\omega) = \{g \in G \mid \forall \omega \in G\ g\omega = \omega g\} = Z(G).$$

Это множество называется *центром* группы.

Замечание. $Z(G) \lhd G$.

Утверждение 1.16. *Если G — конечная группа, $\omega \in G$, то $|\omega^G| \mid \frac{|G|}{|\omega|}$.*

Доказательство.

$$|\omega^G| = |G(\omega)| = \frac{|G|}{|\mathrm{St}(\omega)|} = \frac{|G|}{|C_G(\omega)|}.$$

Однако, $\omega \in C_G(\omega) \Rightarrow \langle\omega\rangle < C_G(\omega) \Rightarrow |\omega| = |\langle\omega\rangle| \mid |C_G(\omega)|$. Значит, $|\omega^G| = \frac{|G|}{|C_G(\omega)|} \mid \frac{|G|}{|\omega|}$ Равенство достигается, если $C_G(\omega)$ тривиален (степени ω). ■

Определение 1.20. *Автоморфизм* группы G — это изоморфизм $G \to G$. Множество всех автоморфизмов G обозначается $\mathrm{Aut}(G)$, это — группа относительно композиции.

Автоморфизм $\varphi \in \mathrm{Aut}(G)$ называется *внутренним*, если $\exists h \in G\colon \forall g \in G\ \varphi(g) = g^h$. Множество всех внутренних автоморфизмов обозначается через $\mathrm{Inn}(G)$.

Утверждение 1.17. $\mathrm{Inn}(G) < \mathrm{Aut}(G)$. *Более того,* $\mathrm{Inn}(G) \cong G/Z(G)$.

Доказательство. Рассмотрим действие G на себя сопряжениями. Это — гомоморфизм $I : G \to S(G)$, образ элемента $g \in G$ обозначим I_g. Тогда $\forall g \in G\ I_g \in \mathrm{Aut}(G)$: $I_g(xy) = (xy)^{g^{-1}} = x^{g^{-1}} y^{g^{-1}} = I_g(x) I_g(y)$ (кроме того, I_g — биекция). Значит, $I : G \to \mathrm{Aut}(G) < S(G)$, $\mathrm{Inn}(G) = \mathrm{Im}\, I < \mathrm{Aut}(G)$, $\mathrm{Im}\, I \cong G/\mathrm{Ker}\, I = G/Z(G)$. ■

Упражнение. $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$

Действие сопряжением на подгруппы

Ω — множество подгрупп G, $g(H) = H^{g^{-1}} = gHg^{-1} < G$. Орбита подгруппы H — все подгруппы, сопряжённые с H. Стабилизатор H $\mathrm{St}(H) = \{g \in G \mid gH = Hg\} = N_G(H)$ — *нормализатор* подгруппы H. $N_G(H)$ — наибольшая (по включению) подгруппа в G, в которой H нормальная.

Замечание. Количество подгрупп, сопряжённых с H есть $|G : N_G(H)|$.

Глава 2

Свойства групп

2.1 p-группы

Определение 2.1. Пусть p — простое число. Группа G называется p-группой, если $|G| = p^n$, $n \in \mathbb{N} \setminus \{0\}$.

Пример. Если $|G| = p$, то по теореме Лагранжа порядок $e \neq g \in G$ равен p, т. е. $| < g > | = p = |G| \Rightarrow G = \langle g \rangle$. Значит, G циклическая и абелева.

Теорема 2.1. *Пусть G — p-группа. Тогда $Z(G) \neq \{e\}$.*

Доказательство. Рассмотрим действие G на себя сопряжением. Орбиты — классы сопряжённости, если $g \in Z(G)$, то $g^G = \{g\}$, иначе $g \notin Z(G) \Rightarrow 1 < |g^G| = |G : C_G(g)| = p^k$. k зависит от g, но $k \geqslant 1$. Выберем представителей g_i для каждого класса сопряжённости, $i \in \{1, \ldots, n\}$, тогда по формуле орбит:

$$p^n = |G| = \sum_{i=1}^{n} |g_i^G| = |Z(G)| + \sum_{|g_i^G|>1} |G : C_G(g_i)|.$$

Второе слагаемое — сумма нетривиальных степеней p, но тогда $p \mid |Z(G)| \Rightarrow |Z(G)| > 1$. ■

Теорема 2.2. *Пусть G — не абелева группа. Тогда $G/Z(G)$ — не циклическая.*

Замечание. $Z(G) \lhd G \Rightarrow$ можем рассматривать факторгруппу. Условие неабелевости важно, так как иначе $G = Z(G)$, и тогда $G/Z(G)$ тривиальна, а потому циклична.

Доказательство. Пусть это не верно. Положим $Z = Z(G)$, и $G/Z = \langle aZ \rangle$, $a \in G \Rightarrow$ все левые смежные классы имеют вид $a^k \cdot Z$, $k \in \mathbb{Z}$, т. к. G/Z циклична. Рассмотрим произвольные $g, h \in G$: $g = a^k x$, $h = a^l y$, $k, l \in \mathbb{Z}$, $x, y \in Z$. Но тогда $gh = a^k x a^l y = a^l y a^k x = hg$, ведь x и y коммутируют со всеми элементами. Значит, G абелева, противоречие. ■

Следствие. *Если $|G| = p^2$, где p — простое, то G — абелева.*

Доказательство. G — p-группа $\Rightarrow Z(G) \neq \{e\}$, т. е. $|Z(G)| = p$ или $|Z(G)| = p^2$. Во втором случае $Z(G) = G$, т. е. G — абелева. Если же $|Z(G)| = p$, то $|G/Z(G)| = p \Rightarrow G/Z(G)$ — циклическая, тогда G всё равно должна быть абелевой. ■

Пример. Рассмотрим в $GL_3(\mathbb{Z}_p)$ подгруппу $UT_3(\mathbb{Z}_p)$ унитреугольных матриц, т. к. матриц вида

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

это действительно подгруппа. $|UT_3(\mathbb{Z}_p)| = p^3$, и она не абелева, т. к.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Упражнение. Какой у $Z(UT_3(\mathbb{Z}_p))$ центр? $|Z(UT_3(\mathbb{Z}_p))| \in \{p, p^2\}$.

2.2 Лемма Бернсайда

Теорема 2.3. *Пусть конечная группа G действует на Ω транзитивно. Определим для $g \in G$ $F(g) = |\{\omega \in \Omega \mid g(\omega) = \omega\}|$. Тогда*

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

Доказательство. Занумеруем $G = \{g_i\}_1^n$ и $\Omega = \{\omega_i\}_1^k$, обозначим

$$(i,j) = \begin{cases} 1, & \text{если } g_i(w_j) = w_j \\ 0, & \text{иначе} \end{cases},$$

тогда

$$F(g_i) = \sum_{j=1}^{k} (i,j),$$
$$\sum_{g \in G} F(g) = \sum_{i,j} (i,j).$$

Заметим, что

$$\sum_{i=1}^{n} (i,j) = |\operatorname{St}(w_j)| = \frac{|G|}{|G(w_j)|} = \frac{|G|}{|\Omega|},$$

а тогда сумма всех (i,j) — это $\frac{|G|}{|\Omega|} \cdot |\Omega| = |G|$. ■

Если G действует на Ω, то можем определить действие на Ω^2: $g((\omega_1, \omega_2)) = (g(\omega_1), g(\omega_2))$.

Определение 2.2. Действие G на Ω называется *2-транзитивным*, если действие G на Ω^2 транзитивно.

Упражнение. Если действие 2-транзитивно, то $\sum_{g \in G} F(G)^2 = 2|G|$.

Следствие (Лемма Бернсайда)**.** *Пусть конечная группа G действует на конечное Ω, обозначим за Ω/G множество орбит этого действия. Тогда*

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

Доказательство. Пусть $\Omega/G = \{\Omega_i\}_{i=1}^{k}$, тогда тем же действием G действует на Ω_i транзитивно. Обозначим $F_i(g) = |\{w \in \Omega_i \mid g(w) = w\}|$. Тогда по теореме $\sum_{g\in G} F_i(G) = |G|$, при этом $F(G) = \sum_{i=1}^{k} F_i(G)$, а тогда

$$\sum_{g\in G} F(g) = \sum_{i=1}^{k}\sum_{g\in G} F_i(g) = k\cdot|G| = |\Omega/G|\cdot|G|. \qquad \blacksquare$$

Пример. Пусть p — нечётное простое число, $k \in \mathbb{N}$. Нужно найти количество ожерелий из p бусин, которые могут иметь k разных цветов, повороты и перевороты отождествляются. Если бы они не отождествлялись, ответом было бы k^p. Обозначим множество фиксированных ожерелий за Ω, на него действует группа диэдра D_p, тогда искомое число — $|\Omega/D_p|$. Орбита — одно ожерелье с точностью до поворотов и переворотов. По лемме Бернсайда, достаточно найти $F(g)$ для любого $g \in D_p$.

1. $g = e$, $F(g) = |\Omega| = k^p$.
2. g — осевая симметрия, $F(g) = k^{(p+1)/2}$.
3. g — нетривиальный поворот. Тогда он сохранит элемент только если все бусины имеют один цвет, т. к. p — простое, т. е. $F(g) = k$.

Итого, $|\Omega/D_p| = \frac{1}{2p}(k^p + k^{(p+1)/2}\cdot p + k(p-1))$.

2.3 Прямое произведение групп

Определение 2.3. Пусть G_1, G_2 — группы. Их (внешним) *прямым произведением* называется множество $G = G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$ с операцией $(g_1, g_2)\cdot(g_1', g_2') = (g_1g_1', g_2g_2')$.

Утверждение 2.1. *Если G_1, G_2 — группы, то $G_1 \times G_2$ — группа.*

Доказательство. Ассоциативность следует из ассоциативности G_1 и G_2, нейтральным будет (e_1, e_2) а обратным к (g_1, g_2) — (g_1^{-1}, g_2^{-1}). $\blacksquare$

Утверждение 2.2. *Для групп G_1, G_2, G_3 верно:*

1. $G_1 \cong G_1 \times \{e\} \lhd G_1 \times G_2$
2. $G_1 \times G_2 \cong G_2 \times G_1$
3. $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$

Доказательство.

1. Очевидно, $G_1 \times \{e\} < G_1 \times G_2$. При этом,

$$(g_1', g_2')^{-1}(g_1, e)(g_1', g_2') = (g_1'^{-1} g_1 g_1', e) \in G_1 \times \{e\} \Rightarrow G_1 \times \{e\} \lhd G_1 \times G_2.$$

   Изоморфизм же осуществляется отображением $\varphi : g \mapsto (g, e)$.

2. Изоморфизм осуществляется отображением $(g_1, g_2) \mapsto (g_2, g_1)$.

3. Изоморфизм — $((g_1, g_2), g_3) \mapsto (g_1, (g_2, g_3))$. ■

Замечание. Таким образом можно определить $G_1 \times \cdots \times G_k$. Более того, аналогично можно определить и прямое произведение бесконечного числа групп: $\prod_{\alpha \in I} G_\alpha$, где I — произвольное множество индексов.

Теорема 2.4. *Пусть $A, B \lhd G$, $AB = G$, $A \cap B = \{e\}$. Тогда $G \cong A \times B$.*

Доказательство. Покажем, что $\forall a \in A, b \in B \;\; ab = ba$. Действительно, рассмотрим $aba^{-1}b^{-1}$: $aba^{-1} \in B$ и $ba^{-1}b^{-1} \in A$ из их нормальности, а тогда $aba^{-1}b^{-1} \in A \cap B = \{e\}$, т. е. $aba^{-1}b^{-1} = e \Rightarrow ab = ba$.

Построим отображение $\varphi : A \times B \to G$: $\varphi : (a, b) \mapsto ab$. Тогда $\varphi((a_1, b_1) \cdot (a_2, b_2)) = \varphi((a_1 a_2, b_1 b_2)) = a_1 a_2 b_1 b_2 = a_1 b_1 a_2 b_2 = \varphi((a_1, b_1)) \cdot \varphi((a_2, b_2)) \Rightarrow \varphi$ — гомоморфизм. Т. к. $AB = G$, $\operatorname{Im}\varphi = AB = G$. Наконец, если $(a, b) \in \operatorname{Ker}\varphi$, то $ab = e \Rightarrow a = b^{-1} \in A \cap B = \{e\} \Rightarrow a = b = e \Rightarrow \operatorname{Ker}\varphi = \{(e, e)\}$. Значит, φ — изоморфизм. ■

Определение 2.4. В ситуации, описанной в теореме, G является *внутренним прямым произведением* A и B.

Замечание. $G/A = AB/A \cong B/B \cap A = B/\{e\} \cong B$ по первой теореме об изоморфизме. Аналогично, $G/B = A$.

Утверждение 2.3. *Пусть $G = A \times B$ — прямое произведение групп A и B. Пусть $A_1 \lhd A$, $B_1 \lhd B$. Тогда $A_1 \times B_1 \lhd A \times B$, причём $(A \times B)/(A_1 \times B_1) = (A/A_1) \times (B/B_1)$.*

Доказательство. Пусть $\overline{A} = A/A_1$, $\overline{B} = B/B_1$, и пусть $\pi_A : A \to \overline{A}$, $\pi_B : B \to \overline{B}$ — соответствующие канонические эпиморфизмы. Рассмотрим $\pi = \pi_A \times \pi_B : A \times B \to \overline{A} \times \overline{B}$, $\pi(a, b) = (\pi_A(a), \pi_B(b))$. Нетрудно видеть, что π — эпиморфизм групп. $\operatorname{Ker}\pi = \operatorname{Ker}\pi_A \times \operatorname{Ker}\pi_B = A_1 \times B_1$. Итак, $\overline{A} \times \overline{B} = \operatorname{Im}\pi \cong (A \times B)/\operatorname{Ker}\pi = (A \times B)/(A_1 \times B_1)$ (и $A_1 \times B_1 = \operatorname{Ker}\pi \lhd G$). ■

В заключение, рассмотрим более общую ситуацию. Пусть $A \lhd G$, $B < G$, причём $AB = G$, $A \cap B = \{e\}$. В этом случае, G называется полупрямым произведением A и B: $G = A \leftthreetimes B$.

Примеры.

1. $S_n = A_n \leftthreetimes \langle (1, 2) \rangle$, $n \geqslant 2$. (но $S_n \not\cong A_n \times \langle (1, 2) \rangle$ при $n \geqslant 3$, ибо $Z(S_n) = \{e\}$).

2. $S_4 = V_4 \leftthreetimes S_3$.

Как описать полупрямые произведения групп? Пусть $G = A \leftthreetimes B$, $\forall b \in B \;\; bAb^{-1} = A$. Значит, группа B действует сопряжением на A, т. е. возникает гомоморфизм

$\psi : B \to \operatorname{Aut} A$: $[\psi(b)](a) = bab^{-1} = a^{b^{-1}}$. Задание групп A, B и гомоморфизма ψ однозначно задаёт G. Действительно, для любого $g \in G$ существует единственное разложение $g = ab$, $a \in A$, $b \in B$. Умножение задаётся так:

$$(a_1, b_1)(a_2, b_2) = a_1 b_1 a_2 b_2 = a_1 (b_1 a_2 b_1^{-1}) b_1 b_2 = \underbrace{a_1}_{\in A} \underbrace{[\psi(b_1)](a_2)}_{\in A} \underbrace{b_1 b_2}_{\in B}$$

Упражнение. Пусть A, B — группы, $\psi : B \to \operatorname{Aut} A$ — гомоморфизм. Тогда можно определить группу так: $G = A \times B$, $(a_1, b_1)(a_2, b_2) = (a_1 \cdot [\psi(b_1)](a_2), b_1 b_2)$.

2.4 Коммутант

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

Утверждение 2.4. *Для любых $x, y \in G$ верно:*

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

Доказательство.

1. Следует из следующего свойства.
2. $[x, y] \cdot yx = xyx^{-1}y^{-1}yx = xy$.
3. $[x, y]^{-1} = yxy^{-1}x^{-1} = [y, x]$.
4. Следует из того, что сопряжение — автоморфизм.

■

Замечание. Если $\varphi : G \to A$ — гомоморфизм в абелеву группу A, то $\varphi([x, y]) = [\varphi(x), \varphi(y)] = e$.

Определение 2.6. Пусть G — группа, тогда $G' = \langle \{[x, y] \mid x, y \in G\} \rangle$ называется *коммутантом* группы G.

Более общо: если $K, H < G$, то их взаимным коммутантом называется подгруппа $[K, H] = \langle \{[k, h] \mid k \in K, h \in H\} \rangle$. Таким образом, $G' = [G, G]$.

Замечание. $\{[x, y] \mid x, y \in G\}$ не обязательно является подгруппой в G.

Упражнение. Привести соответствующий пример.

Утверждение 2.5. *Пусть $\varphi : G \to H$ — гомоморфизм групп. Тогда $\varphi(G') < H'$. Более того, если φ — эпиморфизм, то $\varphi(G') = H'$.*

Доказательство. Для любых x, y $\varphi([x, y]) = [\varphi(x), \varphi(y)] \in H'$. Значит, $\varphi(\{[x, y] \mid x, y \in G\}) \subseteq H' \Rightarrow \varphi(G') = \langle \{\varphi([x, y]) \mid x, y \in G\} \rangle \subseteq H'$. Если же φ — эпиморфизм, то $\forall a, b \in H \ \exists x, y \in G$: $\varphi(x) = a, \varphi(y) = b$. Тогда $[a, b] = \varphi([x, y]) \in \varphi(G') \Rightarrow H' \subseteq \varphi(G') \Rightarrow \varphi(G') = H'$. ■

Следствие. $K \lhd G \Rightarrow K' \lhd G$.

Доказательство. Пусть $g \in G$, $I_g \in \operatorname{Aut} G$, $I_g(x) = x^{g^{-1}}$. Тогда, т. к. $K \lhd G$, то $I_g(K) = K$, т. е. $I_g\big|_K : K \to K$ — автоморфизм группы K. Значит, $I_g(K') = K'$, т. е. $gK'g^{-1} = K' \Rightarrow K' \lhd G$. ■

Определение 2.7. $G'' = (G')'$, по индукции, $G^{(n)} = (G^{(n-1)})'$. Подгруппа $G^{(n)}$ называется *n-м коммутантом* группы G.

Следствие. *$G' \lhd G$; более того, $G^{(n)} \lhd G$.*

Доказательство. Индукция по n. При $n = 0$, $G \lhd G$. Шаг индукции — предыдущее следствие. ■

Теорема 2.5. *Для группы G верно:*

1. *G/G' — абелева группа.*
2. *Если $G' < K < G$, то $K \lhd G$.*
3. *Если $K \lhd G$, причём G/K — абелева, то $G' < K$.*

Замечание. Это значит, что G' — наименьшая по включению нормальная подгруппа, факторгруппа по которой Абелева.

Доказательство.

1. Пусть $\pi : G \to G/G'$ — канонический эпиморфизм, тогда $\forall x, y \in G\ [\pi(x), \pi(y)] = \pi([x, y]) = e \Rightarrow \pi(x)$ и $\pi(y)$ коммутируют. Поскольку π — эпиморфизм, то G/G' — абелева.
2. Рассмотрим $\pi(K) = K/G' < G/G'$. Поскольку G/G' — абелева, то $K/G' \lhd G/G'$, и по второй теореме об изоморфизме $K \lhd G$.
3. Пусть G/K — абелева. Рассмотрим канонический эпиморфизм $\pi' : G \to G/K$. Тогда $\pi'([x, y]) = [\pi'(x), \pi'(y)] = e \Rightarrow [x, y] \in \operatorname{Ker} \pi' = K$ для произвольных $x, y \in G$. Значит, $G' < K$.

■

Замечание. Наоборот, если $G' < K < G$,то $G/K \cong (G/G')/(K/G')$ — абелева.

Замечание. В конце доказательства мы, по сути, увидели, что для любого гомоморфизма $\varphi : G \to A$, где A — абелева, $\operatorname{Ker} \varphi > G'$.

Упражнение. Пусть $H \lhd G$, $K = [G, H]$. Тогда K — наименьшая подгруппа такая, что $H/K < Z(G/K)$.

Определение 2.8. Пусть G — группа, $M \subseteq G$. Тогда *нормальная подгруппа, порождённая множеством M*, есть

$$\langle M \rangle_{\text{норм}} = \bigcap_{H \lhd G, M \subseteq H} H.$$

Утверждение 2.6. *$\langle M \rangle_{норм} = \langle M^G \rangle$, где $M^G = \{m^g \mid m \in M, g \in G\}$.*

Доказательство. Если $H \lhd G$, $M \subseteq H$, то $M^G \subseteq H$. Значит, $\langle M^G \rangle = \bigcap_{H<G, H \supseteq M^G} H \subseteq \bigcap_{H \lhd G, H \supseteq M} H = \langle M \rangle_{\text{норм}}$. Наоборот, $\langle M^G \rangle \lhd G$, т. к. $\forall g \in G\ \langle M^G \rangle^g = \langle M^{Gg} \rangle = \langle M^G \rangle$, поэтому $\langle M \rangle_{\text{норм}} \subseteq \langle M^G \rangle$. ■

Утверждение 2.7. *Пусть $G = \langle M \rangle$. Тогда $G' = \langle\{[m_1, m_2] \mid m_1, m_2 \in M\}\rangle_{норм}$.*

Доказательство. Обозначим правую часть равенства через H. Раз $G' \lhd G$ и $[m_1, m_2] \in G'$ для любых $m_1, m_2 \in M$, получаем $H < G'$.

Наоборот, рассмотрим G/H и канонический эпиморфизм $\pi : G \to G/H$; $[\pi(m_1), \pi(m_2)] = \pi([m_1, m_2]) = e$ для произвольных $m_1, m_2 \in M$. Итак, $G/H = \langle\pi(M)\rangle$, и любые два элемента из $\pi(M)$ коммутируют. Значит, G/H — абелева, откуда $G' < H$.

Значит, $G' = H$. ■

Упражнение. Приведите пример, когда $G' \neq \langle\{[m_1, m_2] \mid m_1, m_2 \in M\}\rangle$.

Замечание. Для группы G обе подгруппы $Z(G)$ и G' показывают, насколько «далека» G от абелевой.

2.5 Разрешимые группы

Определение 2.9. Группа G называется *разрешимой*, если существует такое $n \in \mathbb{N}$, что $G^{(n)} = \{e\}$.

Пример. $S_3' = A_3 = \langle(1\ 2\ 3)\rangle$, A_3 — абелева, а потому $A_3' = \{e\} = S_3^{(2)}$. Значит, S_3 — разрешима.

Замечание. Наименьшее n такое, что $G^{(n)} = \{e\}$, называется *ступенью разрешимости.*

Теорема 2.6. *Пусть $K \lhd G$. Тогда G разрешима $\Leftrightarrow$ K и G/K разрешимы.*

Доказательство.

$\Rightarrow$ $K < G \Rightarrow K^{(n)} < G^{(n)}$. Значит, K разрешимо. Пусть $\pi : G \to G/K$ — канонический эпиморфизм. Тогда $(G/K)' = \pi(G')$, и по индукции $(G/K)^{(n)} = \pi(G^{(n)})$. Т. к. $G^{(n)} = \{e\}$ при некотором n, $(G/K)^{(n)} = \{K\} \Rightarrow G/K$ разрешима.

$\Leftarrow$ Пусть $K^{(n)} = \{e\}$, $(G/K)^{(l)} = \{e\}$. Тогда $\pi(G^{(l)}) = (G/K)^{(l)} = \{e\}$, т. е. $G^{(l)} < \operatorname{Ker}\pi = K$. Значит, $G^{(l+n)} = (G^{(l)})^{(n)} < K^{(n)} = \{e\}$. ■

Следствие. *Пусть $K_1, K_2 \lhd G$ — разрешимые (нормальные) подгруппы. Тогда $K_1 \cdot K_2 \lhd G$ также разрешима.*

Доказательство. Заметим, что $K_1 \lhd K_1 \cdot K_2$; K_1 — разрешима по условию, $(K_1 \cdot K_2)/K_1 \cong K_2/(K_1 \cap K_2)$ (по первой теореме об изоморфизме) — также разрешима, т. к. разрешимы K_1 и K_2 (по теореме). Значит, $K_1 \cdot K_2$ также разрешима. ■

Следствие. *В любой конечной группе G существует наибольшая по включению нормальная разрешимая подгруппа (это просто произведение всех нормальных разрешимых подгрупп).*

Теорема 2.7. *Пусть G — группа. Тогда равносильны следующие утверждения:*

1. *G — разрешима.*

2. *Существует цепочка подгрупп* $G = G_0 > G_1 > \cdots > G_k = \{e\}$ *такая, что* $G_i \lhd G$ *и* G_i/G_{i+1} *— абелева.*

3. *Существует цепочка подгрупп* $G = G_0 > G_1 > \cdots > G_k = \{e\}$ *такая, что* $G_{i+1} \lhd G_i$ *и* G_i/G_{i+1} *— абелева.*

Доказательство.

$1 \Rightarrow 2$ Положим $G_i = G^{(i)}$. Т. к. G — разрешима, $G^{(k)} = \{e\}$ при некотором k. Уже доказано, что $G^{(i)} \lhd G$ и $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ — абелева.

$2 \Rightarrow 3$ Тривиально.

$3 \Rightarrow 1$ Покажем, что $G^{(i)} < G_i$. При $i = 0$ это верно. Пусть $G^{(i)} < G_i$, тогда рассмотрим канонический эпиморфизм $\pi_i : G_i \to G_i/G_{i+1}$. $\pi_i(G^{(i)}) < G_i/G_{i+1}$, т. е. $\pi_i(G^{(i)})$ — абелева группа. Это значит, что у гомоморфизма $\pi_i\big|_{G^{(i)}}$ ядро содержит $(G^{(i)})' = G^{(i+1)}$, т. е. $G^{(i+1)} < \operatorname{Ker}\pi_i \cap G^{(i)} < \operatorname{Ker}\pi_i = G_{i+1}$. Итак, $G^{(k)} < G_k = \{e\} \Rightarrow G^{(k)} = \{e\}$, т. е. G разрешима. ■

Замечание. Цепочка в (2) называется *нормальным рядом подгрупп с абелевыми факторами*. Цепочка в (3) называется *субнормальным рядом подгрупп с абелевыми факторами*.

Утверждение 2.8. *Любая p-группа разрешима.*

Доказательство. Пусть G — p-группа, $|G| = p^n$. Докажем, что G разрешима индукцией по n. При $n = 1$ G — циклическая $\Rightarrow$ абелева $\Rightarrow G' = \{e\}$. Пусть $n > 1$. Положим $Z = Z(G) \neq \{e\}$. Если $Z = G$, то G абелева, а потому разрешима. Иначе $|Z| = p^k$, $|G/Z| = p^{n-k}$, где $1 \leqslant k \leqslant n-1$. Значит, Z и G/Z разрешимы по предположению индукции, а по теореме разрешима и G. ■

Замечание. Из этого доказательства можно получить нормальный ряд подгрупп с абелевыми факторами. Положим $H_0 = \{e\}$, $H_1 = Z(G)$; $H_2 = \pi^{-1}(Z(G/H_1))$, где $\pi : G \to G/H_1$ — канонический эпиморфизм. Аналогично строятся $H_3, \ldots, H_k$. Тогда $\{e\} = H_0 < H_1 < \cdots < H_k = G$ — требуемый нормальный ряд.

Теорема 2.8. *Пусть G — p-группа, $|G| = p^n$. Тогда для любого $0 \leqslant k \leqslant n-1$ $\exists H \lhd G$: $|H| = p^k$.*

Доказательство. Индукция по k. Если $k = 0$, то $H = \{e\}$. Пусть $k > 0$. Обозначим $Z = Z(G) \neq \{e\}$. Если $e \neq g \in Z$, то $\operatorname{ord} g = p^l$. Положим $h = g^{p^{l-1}}$; тогда $\operatorname{ord} h = p$. Пусть $H = \langle h \rangle \Rightarrow |H| = p$. Более того, $H < Z \Rightarrow H \lhd G$. В группе G/H по предположению индукции найдётся нормальная подгруппа порядка p^{k-1}; по второй теореме об изоморфизме эта подгруппа имеет вид K/H, где $H < K \lhd G$. Итак, $K \lhd G$ и $|K| = |K/H| \cdot |H| = p^{k-1} \cdot p = p^k$. ■

Замечание. Т. к. любая p-группа G разрешима, $G' \neq G$.

Упражнение. Докажите, что S_4 разрешима.

2.6 Простые группы

Определение 2.10. Группа G называется *простой*, если в ней ровно две нормальных подгруппы: G и $\{e\}$.

Замечание. Группа из одного элемента не является простой.

Пусть G — произвольная группа, $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{e\}$ — субнормальный ряд подгрупп ($G_i \neq G_{i+1}$). Если G_i/G_{i+1} — не простая, то существует нетривиальная $H/G_{i+1} \lhd G_i/G_{i+1}$, тогда H можно вставить между G_i и G_{i+1}, ибо $G_i \rhd H \rhd G_{i+1}$. Если эта процедура закончится (в частности, это так для всех конечных групп), то получим субнормальный ряд с простыми факторам.

Замечание. Полученный субнормальный ряд называется *композиционным рядом* группы G.

Для любых двух композиционных рядов группы G наборы факторов совпадают с точностью до перестановки и изоморфизма (теорема Жордана-Гёльдера).

Утверждение 2.9. *Абелева группа проста* $\Leftrightarrow G \cong \mathbb{Z}_p$ *при простом* p.

Доказательство. Пусть G — абелева простая группа, $e \neq g \in G$. Тогда $\langle g \rangle \lhd G \Rightarrow \langle g \rangle = G$. Значит, $G \cong \mathbb{Z}$ или $G \cong \mathbb{Z}_n$. Если $G \cong \mathbb{Z}$, то $\mathbb{Z} \rhd 2\mathbb{Z} — G$ не проста. Пусть $G \cong \mathbb{Z}_n$ и n — составное, т. е. $n = kl$, $k, l > 1$. Тогда $\mathbb{Z}_n \rhd k\mathbb{Z}_n \neq \mathbb{Z}_n \Rightarrow G$ непроста.

Если $G \cong \mathbb{Z}_p$, то $\forall H < G \ |H| \mid p$, т. е. $|H| = p$ или $|H| = 1$, а значит $H = G$ или $H = \{e\} — G$ проста. ■

Теорема 2.9. *Группа* A_5 *проста.*

Лемма 2.1. *Пусть* $H \lhd G$, $|G : H| = 2$, $h \in H$. *Тогда, если* $C_G(h) \neq C_H(h)$, *то* $h^H = h^G$. *В противном случае* $h^G = h^H \cup h_1^H$ *и* $|h^H| = |h_1^H|$ *для некоторого* $h_1 \in H^G$.

Доказательство. Напоминание: $C_G(h) = \{g \in G \mid hg = gh\}$, $|h^G| = |G : C_G(h)|$.

Пусть существует $g \in C_G(h) \setminus C_H(h) = C_G(h) \setminus H$. Тогда $G = H \cup gH = H \cup Hg$. Значит, $h^G = h^H \cup h^{gH} = h^H \cup (h^g)^H = h^H$, т. к. $g \in C_G(h)$.

Пусть $h^G = h^H$. Тогда $\forall g \in G \setminus H \ h^g = h^x$, $x \in H \Rightarrow h^{gx^{-1}} = h \Rightarrow gx^{-1} \in C_G(h) \setminus H$. В этом случае $C_G(h) \neq C_H(h)$. Значит, если $C_G(h) = C_H(h)$, то $h^G \neq h^H$, но $h^G = h^H \cup (h^g)^H$, где $g \in G \setminus H$. Обозначим $h_1 = h^g \Rightarrow h^G = h^G \sqcup h_1^H$. Наконец, $h_1^H = h^{gH} = h^{Hg}$, тогда биекция между h^H и h_1^H задаётся очень просто: $h^H \ni x \mapsto x^g \in h^{Hg}$. Итак, $|h^H| = |h_1^H|$. ■

Доказательство теоремы. Пусть $H \lhd A_5$, $H \neq \{e\}$. Тогда H есть объединение нескольких классов сопряжённости в A_5. Пусть $\sigma = (a_1 \ldots a_k) \in S_n$. Тогда $\sigma^{\tau^{-1}} = \tau\sigma\tau^{-1} = (\tau(a_1) \ldots \tau(a_k))$.

Значит, классы сопряжённости (и их мощности) элементов A_5 в S_5 и в A_5 таковы:

в S_5	в A_5
$e^{S_5} = \{e\}$	$\lvert\{e\}\rvert = 1$
$(1\,2\,3)^{S_5} = \{(i\,j\,k)\}$	$(4\,5) \in C_{S_5}((1\,2\,3)) \setminus A_5$, то есть $\lvert(1\,2\,3)^{A_5}\rvert = \lvert\{(i\,j\,k)\}\rvert = 20$
$((1\,2)(3\,4))^{S_5} = \{(i\,j)(k\,l)\}$	$(3\,4) \in C_{S_5}((1\,2)(3\,4)) \setminus A_5$, то есть $\lvert((1\,2)(3\,4))^{A_5}\rvert = \lvert\{(i\,j)(k\,l)\}\rvert = 15$
$(1\,2\,3\,4\,5)^{S_5} = \{(i\,j\,k\,l\,m)\}$	$24 \nmid \lvert A_5\rvert = 60 \Rightarrow$ два класса: $\lvert(1\,2\,3\,4\,5)^{A_5}\rvert = 12$, $\lvert(1\,2\,3\,5\,4)^{A_5}\rvert = 12$

Из тех чисел $1, 20, 15, 12, 12$ нельзя составить нетривиальную сумму, делящую $|A_5| = 60$ и содержащую 1. Значит, раз $|H| \mid 60$ и $e \in H$, $|H| = 60$ и $H = A_5$. ■

Теорема 2.10. *При $n \geqslant 5$ группа A_n проста.*

Замечание. $A_4 \rhd V_4$.

Доказательство. Уже знаем: $A_n = \langle\{(i\,j\,k)\}\rangle$, A_n действует на $\{1, \ldots, n\}$ и $\mathrm{St}(i) \cong A_{n-1}$.

Индукция по $n \geqslant 5$, база уже доказана. Пусть теперь $n \geqslant 6$, $\{e\} \neq H \lhd A_n$.

Докажем, что существует нетривиальная перестановка $e \neq \sigma \in H$ такая, что $\exists i$: $\sigma \in \mathrm{St}(i)$. Рассмотрим $e \neq \tau \in H$. Б. о. о. $\tau = (1\,2\ldots)\ldots$ — разложение τ в произведение независимых циклов. $\tau \in A_n \Rightarrow \tau$ нетривиально переставляет хотя бы 3 элемента. Значит, $\exists k$: $\tau(k) \notin \{1, 2, k\}$ (возможно, $k \in \{1, 2\}$). Пусть $\tau(k) = l$. Наконец, пусть $p, q \notin \{1, 2, k, l\}$, $p \neq q$, $p, q \in \{1, \ldots, n\}$. Обозначим $\tau_1 = \tau^{(l,p,q)}$, тогда $\tau_1(1) = 2$, $\tau_1(k) = q$. Значит, $(\tau_1\tau^{-1})(2) = 2$, $(\tau_1\tau^{-1})(l) = q \neq l$, т. е. $e \neq \tau_1\tau^{-1} \in H \cap \mathrm{St}(2)$.

Пусть $e \neq \sigma \in H \cap \mathrm{St}(n)$. Тогда $H \cap \mathrm{St}(n) \lhd \mathrm{St}(n) \cong A_{n-1}$. Значит, $H \cap \mathrm{St}(n) = \mathrm{St}(n)$ по предположению индукции. В частности, $(1\,2\,3) \in H \Rightarrow (1\,2\,3)^{A_n} \subseteq H$, но $(1\,2\,3)^{A_n} = \{(i\,j\,k)\}$. Т. о. $H > \langle(1\,2\,3)^{A_n}\rangle = A_n$. ■

Замечание. A_5 — неабелева простая группа наименьшего возможного порядка.

Замечание. Пусть F — поле. Тогда простой является группа

$$PSL_N(F) = SL_n(F)/Z(SL_N(F)),$$

где $Z(SL_n(F)) = \{\lambda E \mid \lambda \in F, \lambda^n = 1\}$, если

а) $n \geqslant 3$

б) $n = 2$ и $|F| \geqslant 4$.

Упражнение. $PSL_2(F_2) \cong S_3$, $PSL_2(F_3) \cong A_4$, $PSL_2(F_4) \cong PSL_2(F_5) \cong A_5$.

Теорема 2.11. *Группа SO_3 проста, где $SO_3 = O_3 \cap SL_3(\mathbb{R})$.*

Замечание. SO_3 — группа *вращений* трёхмерного евклидового пространства. Действительно, если $A \in SO_3$, то у A есть с. з. 1 и A реализует вращение вокруг соответствующего собственного вектора.

Доказательство. Как выглядят классы сопряжённости в SO_3? Пусть $g, h \in SO_3$, и пусть h — вращение вокруг l на угол α. Тогда ghg^{-1} — вращение на угол α вокруг $g(l)$, поскольку $h(x) = y \Rightarrow ghg^{-1}(gx) = g(y)$. Значит, h^{SO_3} состоит из всех вращений на угол α. Пусть $\{e\} \neq H \lhd SO_3$. Пусть $e \neq h \in H$ – пусть это вращение на α относительно l. Тогда в H содержатся все вращения на α. Пусть $l(\varphi)$ — прямая, образующая угол φ с l, $x(\varphi)$ — вращение вокруг $l(\varphi)$ на α. Тогда $x(\varphi) \in H$ (считаем, что $x(\varphi)$ непрерывно меняется при изменении φ). Положим $y(\varphi) = h(x(\varphi))^{-1}$. Тогда $y(0) = id$, а $y(\varphi)$ — вращение на некоторый угол $\beta(\varphi)$, $\beta(0) = 0$. $\beta(\varphi)$ — также непрерывная функция аргумента φ (β выражается через $\operatorname{tr} y(\varphi)$), β — не тождественный ноль. Значит, значения $\beta(\varphi)$ заметают некоторый интервал $[0, \alpha_0]$, $\alpha_0 > 0$, т. к. $y(\varphi) \in H$, в H лежат все вращения на углы $\gamma \in [0, \alpha_0] \Rightarrow$ в H лежат все вращения ■

Замечание. SO_n проста при $n = 3$ и $n \geqslant 5$.

2.7 Теоремы Силова

Пусть $|G| = n$, $k \mid n$. В таком случае *необязательно* существует $H < G$, $|H| = k$. Например, в группе A_4 нет $H < A_4$: $|H| = 6$. Иначе бы $|A_4 : H| = 2 \Rightarrow H \lhd A_4$, но классы сопряженности в A_4 имеют порядки 1, 3, 4, 4, и из этих порядков не составить 6.

Определение 2.11. Пусть G — конечная группа, $|G| = n = p^k s$, где p — простое, $k \geqslant 1$, $p \nmid s$. Тогда *силовской p-подгруппой* в G называется подгруппа $H < G$ такая, что $|H| = p^k$.

Теорема 2.12 (1-я теорема Силова)**.** *В любой конечной группе G, $p \mid n = |G|$, существует силовская p-подгруппа.*

Теорема 2.13 (2-я теорема Силова)**.** *Любая p-подгруппа группы G содержится в некоторой силовской p-подгруппе. Более того, все силовские p-подгруппы в G сопряжены.*

Теорема 2.14 (3-я теорема Силова)**.** *Пусть N_p — количество словских p-подгрупп в G. Тогда $N_p \equiv 1 \mod p$.*

Замечание. Во-первых, из второй теоремы следует, что все силовские p-подгруппы в G изоморфны. Во-вторых, уже известно, что в группе порядка p^k есть подгруппы любого порядка p^l, $l \leqslant k$. Значит, и в G есть такие (но они не обязательно изоморфны).

Доказательство 2-й теоремы при условии 1-й. Пусть P — силовская p-подгруппа в G, H — некоторая p-подгруппа в G, $|H| = p^t$. Рассмотрим действие группы H на $\Omega = G/P$ левыми сдвигами: $h(gP) = hgP$. Пусть $\Omega = \Omega_1 \sqcup \Omega_2 \sqcup \cdots \sqcup \Omega_m$ — разбиение на орбиты. Тогда для любого i выбрав $\omega_i \in \Omega_i$ $|\Omega_i| = |H : \mathrm{St}(\omega_i)| = p^{\alpha_i}$, $\alpha_i \in \mathbb{Z}_+$. Значит, по формуле орбит $s = \frac{n}{p^k} = |\Omega| = p^{\alpha_1} + \cdots + p^{\alpha_m}$. Поскольку $p \nmid s$, существует $\alpha_i = 0$, т. е. $\Omega_i = \{gP\}$, $g \in G$. Но $P_1 = gPg^{-1} < G$ — подгруппа, сопряженная с P. Итак, $H \cdot P_1 = P_1 \Rightarrow H \subseteq P_1 \Rightarrow H < P_1$, $|P_1| = p^k$. Наконец, если H —

силовская p-подгруппа, то $H < gPg^{-1}$, $|H| = |gPg^{-1}| \Rightarrow H = gPg^{-1}$, т. е. H и P сопряжены. ■

Доказательство 3-й (и 1-й) теоремы. Пусть $\Omega = \{M \subseteq G \mid |M| = p^k\}$, G действует на Ω левыми сдвигами: $g(M) = gM \in \Omega$. Пусть $M \in \Omega$, $H = \mathrm{St}(M)$. Это значит, что для любого $h \in H$ $hM = M \Rightarrow HM = M$. Но $HM = \bigcup_{m \in M} Hm$, т. е. M есть объединение правых смежных классов по H, откуда $|H| \mid |M| = p^k \Rightarrow |H| = p^t$, $t \in \mathbb{Z}$, а тогда $|G(M)| = |G : H| = sp^{k-t}$.

Заметим: если H — силовская p-подгруппа, то $M = HM = Hm$, $m \in M$. Наоборот, если K — произвольная силовская подгруппа, то для множества $M = Kg$ имеем $KM = M \Rightarrow K < \mathrm{St}(M) \Rightarrow K = \mathrm{St}(M)$. Итого: любая силовская p-подгруппа $K < G$ является стабилизатором ровно для $|G : K| = s$ подмножеств — своих правых смежных классов. В то же время, любой правый смежный класс силовской p-подгруппы будет левым для некоторой (возможно, другой) силовской p-подгруппы, а его орбита — всеми её левыми смежными классами.

Применим формулу орбит: если $\Omega = \Omega_1 \sqcup \cdots \sqcup \Omega_m$ — разбиение Ω на орбиты, то

$$C_n^{p^k} = |\Omega| = \sum_{i=1}^{m} |\Omega_i| = \sum_{i=1}^{m} s \cdot p^{k-t_i},$$

где среди чисел t_i есть ровно N_p чисел, равных k; для остальных же слагаемые будут кратны p. Значит,

$$C_n^{p^k} \equiv N_p \cdot s \pmod{p},$$

т. е. $N_p \mod p$ зависит только лишь от n, а не от того, какую группу порядка n мы выбрали.

Например, если $G = \mathbb{Z}_n$, то в ней ровно одна подгруппа порядка $p^k \Rightarrow N_p \equiv 1 \pmod{p}$ для любой G, $|G| = n$. ■

Упражнение. Пусть $0 \leqslant l \leqslant k$, и пусть $N_p(l)$ — количество подгрупп порядка p^l в группе G. Тогда $N_p(l) \equiv 1 \pmod{p}$.

Утверждение 2.10. *Пусть $p < q$ — простые числа. Тогда любая группа G, $|G| = pq$, разрешима.*

Доказательство. Пусть Q — силовская q-подгруппа в G, $|Q| = q$. Все силовские q-подгруппы сопряжены с ней, и их количество есть $N_q \equiv 1 \mod q$. Если $N_q = 1$, то $g^{-1}Qg = Q$ для любого $g \in G \Rightarrow Q \lhd G$, $|G/Q| = p$, т. е. Q и G/Q — циклические $\Rightarrow G$ — разрешима. Иначе в любой силовской q-подгруппе найдётся $q-1$ элементов порядка q, и все они различны $\Rightarrow |G| \geqslant N_q \cdot (q-1) \geqslant (q+1)(q-1) > pq$ — противоречие. ■

Теорема 2.15. *Пусть G — конечная группа, $p_1, \ldots, p_k$ — все различные простые делители $n = |G|$, а $P_1, \ldots, P_k$ — соответствующие силовские подгруппы в G. Тогда:*

1. $P_i \lhd G \Leftrightarrow N_{p_i} = 1$
2. $G = P_1 \times \cdots \times P_k \Leftrightarrow \forall i \; P_i \lhd G$

Доказательство.

1. Если $N_{p_i} = 1$, то P_i — единственная силовская p_i-подгруппа, а тогда $\forall g \in G \ gP_ig^{-1} = P_i \Rightarrow P_i \lhd G$. Наоборот, если $P_i \lhd G$, то по второй теореме Силова любая силовская p_i-подгруппа сопряжена с P_i, т. к. совпадает с P_i. Значит, $N_{p_i} = 1$.

2. Если $G = P_1 \times \cdots \times P_k$, то $P_i \lhd G$. Наоборот, если $P_i \lhd G$, докажем индукцией по t, что $P_1 \cdot \ldots \cdot P_t = P_1 \times \cdots \times P_t$. При $t = 1$ — доказывать нечего. Пусть $P_1 \cdot \ldots \cdot P_{t-1} = P_1 \times \cdots \times P_{t-1}$, тогда $|P_1 \ldots P_{t-1}|$ делится только на $p_1, \ldots, p_{t-1}$, а $|P_t|$ делится лишь на p_t. Отсюда $|P_1 \ldots P_{t-1} \cap P_t|$ делит $\mathrm{GCD}(|P_1 \ldots P_{t-1}|, |P_t|) \Rightarrow P_1 \ldots P_{t-1} \cap P_t = \{e\}$. Итак, $P_1 \ldots P_{t-1}, P_t \lhd P_1 \ldots P_t$, $P_1 \ldots P_{t-1} \cap P_t = \{e\}$, $P_1 \ldots P_{t-1} \cdot P_t = P_1 \ldots P_t \Rightarrow P_1 \ldots P_t = (P_1 \ldots P_{t-1}) \times P_t = P_1 \times \cdots \times P_t$. ■

Следствие. *Любая конечная абелева группа — прямое произведение своих силовских подгрупп.*

Глава 3

Задание групп

Как задать группу $\mathbb{Z}_n$ — циклическую группу из n элементов? Можно сказать, что она порождается одним элементом порядка n, а образующие и соотношения позволят записать это как $\mathbb{Z}_n \cong \langle a \mid a^n = e \rangle$.

3.1 Свободные группы

Определение 3.1. Пусть $F_n = \langle f_1, \ldots, f_n \rangle$ — группа. Она называется *свободной со свободными порождающими* $f_1, \ldots, f_n$, если выполняется универсальное свойство: для любой группы G и любых $g_1, \ldots, g_n \in G$ существует гомоморфизм $\varphi : F_n \to G$ такой, что $\varphi(f_i) = g_i$, $i = 1, \ldots, n$.

Замечание. Такой гомоморфизм φ единственен.

Замечание. Если $G = \langle g_1, \ldots, g_n \rangle$, то φ сюръективен, т. е. $G \cong F_n / \operatorname{Ker} \varphi$.

Пусть $f_1, \ldots, f_n$ — n различных символов. Выберем алфавит $A = \{f_1, \ldots, f_n, f_1^{-1}, \ldots, f_n^{-1}\}$. Теперь пусть F_n — множество всех слов в алфавите A (включая пустое слово Λ), в которые не входят подслова вида $f_i^{-1} f_i$ и $f_i f_i^{-1}$.

Пример. При $n = 1$ эти слова будут иметь вид Λ, $\underbrace{f_1 f_1 \ldots f_1}_{k}$ и $\underbrace{f_1^{-1} \ldots f_1^{-1}}_{k}$.

Пример. При $n = 2$ $f_1 f_2 f_2 f_1^{-1} \in F_n$, а $f_1 f_2 f_2^{-1} \notin F_n$.

Введём операцию: если $w_1, w_2 \in F_n$, то $w_1 \cdot w_2$ есть их конкатенация в которой осуществим «сокращения» взаимнообратных букв на стыке слов, тогда $w_1 \cdot w_2 \in F_n$.

Пример. $(f_1 f_2 f_3) \cdot (f_3^{-1} f_2^{-1} f_1) = f_1 f_1$.

Теорема 3.1. $(F_n, \cdot)$ — *свободная группа со свободными образующими* $f_1, \ldots, f_n$.

Доказательство. Для начала, покажем, что $(F_n, \cdot)$ — группа.

1. Нейтральный элемент — Λ: $\Lambda \cdot w = w \cdot \Lambda = w$
2. Если $w = f_{i_1}^{\varepsilon_1} \cdot \cdots \cdot f_{i_k}^{\varepsilon_k}$, то $w^{-1} = f_{i_k}^{-\varepsilon_k} \cdot \cdots \cdot f_{i_1}^{-\varepsilon_1} \in F_n$, а $w \cdot w^{-1} = \Lambda = w^{-1} \cdot w$.
3. Пусть $a, b, c \in F_n$. Пусть при перемножении $a \cdot b$ сокращается $p \cdot p^{-1}$, а при перемножении $b \cdot c$ — $q \cdot q^{-1}$.

Пусть в слове b подслова p^{-1} и q не пересекаются, и между ними есть хотя бы один символ. Тогда $b = p^{-1}b'q$, $a = a'p$, $c = q^{-1}c'$, и $b' \neq \Lambda$ (тут используется просто конкатенация). Значит, $ab = a'p \cdot p^{-1}b'q = a'b'q$, $b \cdot c = p^{-1}b'c'$, $(a \cdot b) \cdot c = a'b'q \cdot q^{-1}c' = a'b'c' = a'p \cdot p^{-1}b'c' = a \cdot (b \cdot c)$.

Пусть теперь p^{-1} и q пересекаются или $b = p^{-1}q$, тогда $b = rb's$, $p^{-1} = rb'$, $q = b's$ (возможно, b' пусто). В этом случае $a = a'b'^{-1}r^{-1}$, $c = s^{-1}b'^{-1}c'$. Тогда $a \cdot b = a'b'^{-1}r^{-1} \cdot rb's = a's$, $b \cdot c = rc'$; $(a \cdot b) \cdot c = a's \cdot s^{-1}b'^{-1}c' = a' \cdot b'^{-1}c'$, а $a \cdot (b \cdot c) = a'b'^{-1}r^{-1} \cdot rc' = a'b'^{-1} \cdot c'$. Если $b' \neq \Lambda$, дальше сокращений не будет, т. к. $a'b'^{-1}, b'^{-1}c' \in F_n$ как фрагменты слов без сокращений, и тогда оба слова есть $a'b'^{-1}c'$. Если же $b' = \Lambda$, оба слова равны $a' \cdot c'$.

Теперь докажем свободность. Ясно, что $F_n = \langle f_1, \ldots, f_n \rangle$. Далее, если $g_1, \ldots, g_n \in G$ определим $\varphi : F_n \to G$, $\varphi(\Lambda) = e$, $\varphi(f_{i_1}^{\varepsilon_1} \ldots f_{i_k}^{\varepsilon_k}) = g_{i_1}^{\varepsilon_1} \ldots g_{i_k}^{\varepsilon_k}$. Тогда, если $w_1, w_2 \in F_n$, имеем $\varphi(w_1) \cdot \varphi(w_2) = w_1(g_1, \ldots, g_n) \cdot w_2(g_1, \ldots, g_n) = \varphi(w_1 \cdot w_2)$ (здесь скобки обозначают подстановку вместо $f_1, \ldots, f_n$). Тогда φ — требуемый гомоморфизм ($\varphi(f_i) = g_i$). ■

Замечание. Аналогичным образом строится и свободная группа с множеством свободных образующих произвольной мощности.

Утверждение 3.1. *Пусть F_n и G_n — две свободные группы с n свободными образующими каждая. Тогда $F_n \cong G_n$ (и существует изоморфизм, переводящий свободные образующие в свободные образующие).*

Доказательство. Пусть $f_1, \ldots, f_n$ — свободные образующие в F_n, $g_1, \ldots, g_n$ — в группе G. Тогда существуют гомоморфизмы $\varphi : F_n \to G_n$ и $\psi : G_n \to F_n$, при том $\varphi(f_i) = g_i$, $\psi(g_i) = f_i$. Их композиция — гомоморфизм $\varphi \circ \psi : G_n \to G_n$, при этом $\varphi \circ \psi(g_i) = g_i$, а тогда $\varphi \circ \psi = id_{G_n}$ (т. к. $G_n = \langle g_1, \ldots, g_n \rangle$). Аналогично, $\psi \circ \varphi = id_{F_n} \Rightarrow \varphi$, ψ — изоморфизмы. ■

Замечание. $F_1 = \langle f_1 \rangle \cong \mathbb{Z}$.

Утверждение 3.2. *Для $n \geqslant 2$ F_n — не абелева.*

Доказательство. Существует G такая, что $\exists g_1, g_2 \in G$: $g_1 g_2 \neq g_2 g_1$. С другой стороны, существует $\varphi : F_n \to G$, $\varphi(f_1) = g_1$ и $\varphi(f_2) = g_2$, а значит $\varphi(f_1 f_2) = g_1 g_2 \neq g_2 g_1 = \varphi(f_2 f_1)$, тогда $f_1 f_2 \neq f_2 f_1$, т. е. F_n — не абелева. ■

Упражнение. Пусть $G = SL_2(\mathbb{Z}[x])$, тогда

$$F_2 \cong \langle \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \rangle < G.$$

3.2 Соотношения

Определение 3.2. Пусть $G = \langle g_1, \ldots, g_n \rangle$ — группа, $F_n = \langle f_1, \ldots, f_n \rangle_{\text{своб}}$ — свободная группа, а $w_1, \ldots, w_k \in F_n$. Обозначим через $w_i(g_1, \ldots, g_n)$ слово, полученное заменой f_i на g_i и f_i^{-1} на g_i^{-1}. Пусть $K = \langle w_1, \ldots, w_k \rangle_{\text{норм}}$, $\varphi : F_n \to G$ —

гомоморфизм, $\varphi(f_i) = g_i$. Тогда G *задана образующими* $g_1, \dots, g_n$ *с соотношениями* $w_i(g_1, \dots, g_n) = e$, если $\operatorname{Ker}\varphi = K$. Обозначение:

$$G = \langle g_1, \dots, g_n \mid w_1(g_1, \dots, g_n) = e, \dots, w_k(g_1, \dots, g_n) = e \rangle.$$

Замечание. $G = \operatorname{Im}\varphi \cong F_n/K$. Наоборот, если $G = F_n/K$, $g_i = f_iK$, то

$$G = \langle g_1, \dots, g_n \mid w_1(g_1, \dots, g_n) = e, \dots, w_k(g_1, \dots, g_n) = e \rangle.$$

Замечание. Вопрос о том, тривиальна ли G (или равны ли в G два элемента), алгоритмически не разрешим.

Теорема 3.2 (универсальное свойство группы, заданной образующими и соотношениями)**.** *Пусть* $G = \langle g_1, \dots, g_n \mid w_i(g_1, \dots, g_n) = e \rangle$. *Пусть* H *— группа,* $h_1, \dots, h_n \in H$ *и* $w_i(h_1, \dots, h_n) = e$. *Тогда существует гомоморфизм* $\theta : G \to H$, $\theta(g_i) = h_i$.

Доказательство. Пусть $\varphi : F_n \to G$, $\varphi(f_i) = g_i$; $\psi : F_n \to H$, $\psi(f_i) = h_i$. Пусть $K = \operatorname{Ker}\varphi = \langle w_1, \dots, w_k \rangle_{\text{норм}}$, пусть $L = \operatorname{Ker}\psi$. Тогда $K, L \lhd F_n$. Более того,

$$w_i \in L \Rightarrow L > \langle w_1, \dots, w_k \rangle_{\text{норм}} = K.$$

Значит, $\operatorname{Im}\psi \cong F_n/L \cong (F_n/K)/(L/K) \cong G/G_1$, где $G_1 \lhd G$, по второй теореме об изоморфизме, и при этом изоморфизме элементы g_iG_1 соответствуют элементам h_i. Значит, канонический эпиморфизм $\pi : G \to G/G_1 \cong \operatorname{Im}\psi$ — это требуемый гомоморфизм. ■

Пример. $G = \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle$. Пусть $g \in G$. Тогда $g = a^{i_1}b^{j_1}a^{i_2}\dots$, $i_k, j_k \in \mathbb{Z}$. Можно считать, что $i_k, j_k \in \{0, 1\}$. Значит, $g = aba\dots$ или $g = baba\dots$. Наконец, $abab = e$, длина произведения, можно считать, меньше четырёх: $abab = e = baba = b(abab)b^{-1}$. Итак, элементы нашей группы — только e, a, b, ab, ba, aba, bab. Далее, $aba = (abab)b^{-1} = b^{-1} = b$ и $bab = a$, $ab = (abab)b^{-1}a^{-1} = ba$. Итого, $G = \{e, a, b, ab\}$ (не факт, что они различны). Почему не меньше? Рассмотрим $H = \mathbb{Z}_2 \times \mathbb{Z}_2$, $a' = (1, 0)$, $b' = (0, 1)$. Тогда $a'^2 = b'^2 = (a'b')^2 = e$ — все соотношения выполнены. По универсальному свойству существует $\varphi : G \to H$, $\varphi(a) = a'$, $\varphi(b) = b'$, при этом $\operatorname{Im}\varphi = \langle \varphi(a), \varphi(b) \rangle = \langle a', b' \rangle = H$. Итак, $|\operatorname{Im}\varphi| = 4 \Rightarrow |G| \geqslant 4$. Значит, $|G| = 4 \Rightarrow \varphi$ — изоморфизм. Итак, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Замечание. Можно было бы построить группу H иначе: $H = \{e, a, b, ab\}$ и вычислить таблицу умножения: например, $a \cdot ab = b$, $ab \cdot a = aba = b$.

Пример. Рассмотрим группу кватернионов:

$$Q_8 = \langle a, b \mid a^4 = e, a^2 = b^2, bab^{-1} = a^{-1} \rangle$$

($a^2 = b^2$ значит то же, что и $a^2b^{-2} = e$). В этом случае можем любой элемент записать как $h = a^{i_1}b^{j_1}\dots$, $i_k \in \{0, 1, 2\}$ и $j_k \in \{0, 1\}$ (ибо $a^2 = b^2$). Итак, $g = a^{i_1}ba^{i_2}b\dots$. Если элементов b хотя бы два, можно воспользоваться $ba = a^{-1}b = a^3b$. Отсюда $ba^kb = a^{3k}b^2 = a^{3k+2}$. Итого, $g = a^i$ или $g = a^{i_1}ba^{i_2} = a^jb$. Итак, $|Q_8| \leqslant 8$.

Рассмотрим группу $M_{2\times 2}(\mathbb{C})$ и её элементы $A = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Тогда $A^2 = -E = B^2$, $A^4 = E$, $BA = \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right) = A^{-1}B$. Значит, существует гомоморфизм $\varphi : Q_8 \to M_{2\times 2}(\mathbb{C})$, для которого $\varphi(a) = A$, $\varphi(b) = B$ и, следовательно, $|Q_8| \geqslant |\operatorname{Im}\varphi| \geqslant 8$: $\operatorname{Im}\varphi > \langle A\rangle$, $\operatorname{Im}\varphi \ni B \notin \langle A\rangle$.

Итак, $|\operatorname{Im}\varphi| = 8 = |Q_8|$, и $Q_8 \cong \operatorname{Im}\varphi = \langle A, B\rangle$.

Глава 4

Конечно порождённые абелевы группы

Во время работы с абелевыми группами мы считаем, что операция — это «+», а вместо a^n пишем na.

Мы уже встречали следующие абелевы группы:

1. Циклические: $\mathbb{Z}$ или $\mathbb{Z}_n$ (и изоморфные им).
2. $\mathbb{Z}^l \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ — также конечно порождена (она порождена $k+l$ элементами вида $(0, \ldots, 0, 1, 0, \ldots, 0)$).

Наша цель — доказать, что все конечно порождённые абелевы группы изоморфны таким.

Замечание. Если $\mathrm{GCD}(n, k) = 1$, то $\mathbb{Z}_n \times \mathbb{Z}_k \cong \mathbb{Z}_{nk}$. Действительно, элемент $(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_k$ имеет порядок $nk \Rightarrow \mathbb{Z}_n \times \mathbb{Z}_k = \langle (1, 1) \rangle \cong \mathbb{Z}_{nk}$. Значит, наше представление не единственно.

Замечание. Условие конечно порождённости существенно. Например, группа $(\mathbb{Q}, +)$ не представима в выписанном виде. Более того, она неразложима в нетривиальное прямое произведение, т. к. в ней нет двух нетривиальных подгрупп, пересекающихся по $\{0\}$.

4.1 Конечно порождённые абелевы группы без кручения

Определение 4.1. Пусть A — абелева группа. Её *периодической частью* (или *кручением*) называется

$$T(A) = \{a \in A \mid \operatorname{ord} a < \infty\}.$$

Группа A называется *абелевой группой без кручения*, если $T(A) = \{0\}$.

Утверждение 4.1. *Если A — абелева группа, то $T(A) < A$.*

Доказательство. $0 \in T(A) \Rightarrow T(A) \neq \varnothing$. Если $a, b \in T(A)$, то $\exists n, k \in \mathbb{N}$: $na = kb = 0$. Тогда $n \cdot (-a) = -na = 0 \Rightarrow -a \in T(A)$ и $nk(a + b) = nka + nkb = k \cdot 0 + n \cdot 0 = 0 \Rightarrow a + b \in T(A)$. Значит, $T(A) < A$. ∎

Замечание. Периодическая часть неабелевой группы не обязательно подгруппа. Скажем, в O_2 все осевые симметрии имеют порядок 2, но их произведение может быть поворотом бесконечного порядка.

Пусть A — конечно порождённая абелева группа без кручения.

Определение 4.2. Пусть $a_1, \dots, a_n \in A$. Система элементов $a_1, \dots, a_n$ называется *независимой*, если

$$\forall k_1, \dots, k_n \in \mathbb{Z} \ \sum_{i=1}^{n} k_i a_i = 0 \Rightarrow k_1 = \dots = k_n = 0.$$

Эта система называется *базисом* группы A, если она независима и $\langle a_1, \dots, a_n \rangle = A$.

Замечание. Если $a_1, \dots, a_n$ — базис в A, то $\forall b \in A \ \exists! k_1, \dots, k_n \in \mathbb{Z}$: $b = \sum_{i=1}^{n} k_i a_i$

Лемма 4.1. *Пусть $A = \langle a_1, \dots, a_n \rangle$, и $b_1, \dots, b_k \in A$, $k > n$. Тогда система $b_1, \dots, b_k$ — зависима.*

Доказательство. Поскольку $b_i \in \langle a_1, \dots, a_n \rangle$, $(b_1, \dots, b_k) = (a_1, \dots, a_n)S$, где $S \in M_{n \times k}[\mathbb{Z}] \subseteq M_{n \times k}[\mathbb{Q}]$. Так как $k > n$, столбцы S линейно зависимы над Q, т. е. существует $0 \neq x' \in M_{k \times 1}[\mathbb{Q}]$ такой, что $Sx' = 0$. Домножив x' на произведение знаменателей элементов из x', получим $x \in M_{k \times 1}[\mathbb{Z}]$. Значит, $(b_1, \dots, b_k)x = (a_1, \dots, a_n)Sx = 0$. Т. к. $x \neq 0$, $(b_1, \dots, b_k)$ — зависимы. ■

Теорема 4.1. *Пусть A — конечно порождённая абелева группа без кручения, тогда в A есть базис. Более того, любые два базиса в A равномощны.*

Доказательство. Предположим противное. Тогда любая порождающая группу система зависима. Из всех конечных порождающих систем выберем систему из наименьшего числа элементов $a_1, \dots, a_n$. Пусть $s_1, \dots, s_n$ — коэффициенты зависимости: $\sum_{i=1}^{n} s_i a_i = 0$, не все s_i — нули. Из всех таких систем $a_1, \dots, a_n, s_1, \dots, s_n$ выберем такую, в которой $0 \neq |s_1|$ минимален.

1. Можно считать, что $s_1 > 0$ (иначе домножим s_i на -1).

2. Если $s_1 = 1$, то $a_1 + \sum_{i=2}^{n} s_i a_i = 0 \Rightarrow a_1 = -\sum_{i=2}^{n} s_i a_i \Rightarrow A = \langle a_2, \dots, a_n \rangle$, противоречие.

3. $s_1 > 1$. Пусть $s_1 \nmid s_i$ при некотором $i \geqslant 2$. Тогда $s_i = qs_1 + r$, $q \in \mathbb{Z}$, $r \in \mathbb{N}$ и $0 < r < s_1$. Значит, $0 = \sum_{j=1}^{n} s_j a_j = s_1 a_1 + (qs_1 + r)a_i + \sum_{2 \leqslant j \leqslant n, j \neq i} s_j a_j = s_1(a_1 + qa_i) + ra_i + \sum_{2 \leqslant j \leqslant n, j \neq i} s_j a_j$. Заметим, что $A = \langle a_1 + qa_i, a_2, \dots, a_n \rangle$, т. к. $a_1 = (a_1 + qa_i) - qa_i$. Для новой системы порождающих есть зависимость, в которой встречается коэффициент $0 \neq |r| < |s_1|$ — противоречие с выбором системы.

4. Итак, $s_1 > 1$, $s_1 \mid s_i$. Тогда $0 = \sum_{i=1}^{n} s_i a_i = s_1(\sum_{i=1}^{n} \frac{s_i}{s_1} a_i) \Rightarrow \sum_{i=1}^{n} \frac{s_i}{s_1} a_i \in T(A) \Rightarrow \sum_{i=1}^{n} \frac{s_i}{s_1} a_i = 0 \Rightarrow a_1 = -\sum_{i=2}^{n} \frac{s_i}{s_1} a_i$. Противоречие.

Осталось показать, что любые два базиса равномощны. Пусть $(a_1, \dots, a_n)$ и $(b_1, \dots, b_k)$ базисы в A. Тогда каждая из этих систем порождает A и, по лемме, $k \leqslant n \leqslant k \Rightarrow k = n$. ■

Замечание. Пусть $a_1, \dots, a_n$ и $b_1, \dots, b_n$ — два базиса в A. Тогда $(a_1, \dots, a_n) = (b_1, \dots, b_n)S$ и $(b_1, \dots, b_n) = (a_1, \dots, a_n)T$, $S, T \in M_{n\times n}[\mathbb{Z}]$. Значит, $(a_1, \dots, a_n) = (a_1, \dots, a_n)TS$. Т. к. выражение через базис единственно, $TS = E \Rightarrow \det T \cdot \det S = 1$, а поскольку их определители также целочисленны, $\det S = \det T = \pm 1$. Наоборот, если $a_1, \dots, a_n$ — базис, $S \in M_{n\times n}[\mathbb{Z}]$, $\det S = \pm 1$, то $(a_1, \dots, a_n)S$ — тоже базис, т. к. $S^{-1} \in M_{n\times n}[\mathbb{Z}]$ по формуле Крамера.

Замечание. В условиях нашей теоремы если $a_1, \dots, a_n$ — базис в A, то

$$A = \langle a_1, \dots, a_n \rangle = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle \cong \mathbb{Z} \times \cdots \times \mathbb{Z} = \mathbb{Z}^n$$

Определение 4.3. Пусть $A = \langle a_1, \dots, a_k \rangle$ — абелева группа. A называется *свободной абелевой группой* со свободными порождающими $a_1, \dots, a_k$, если для любой абелевой группы B и элементов $b_1, \dots, b_k \in B$ существует гомоморфизм $\varphi : A \to B$ такой, что $\varphi(a_i) = b_i$, $i = 1, \dots, k$.

Замечание. Две свободные абелевы группы с одним и тем же количеством порождающих изоморфны — аналогично обычным.

Замечание. В качестве свободной абелевой группы с k порождающими можно взять

$$A = \langle a_1, \dots, a_k \mid [a_i, a_j] = e, 1 \leqslant i < j \leqslant k \rangle = F_k / \langle [f_i, f_j] \mid 1 \leqslant i < j \leqslant k \rangle_{\text{норм}} = F_k / F_k'$$

Теорема 4.2. *Свободная абелева группа с k свободными порождающими — это $\mathbb{Z}^k$ (с точностью до изоморфизма).*

Доказательство. Пусть $A = \mathbb{Z}^k$, положим $a_i = (0, \dots, 0, 1, 0, \dots, 0)$. Тогда $A = \langle a_1, \dots, a_k \rangle$, т. к. $(x_1, \dots, x_k) = \sum_{i=1}^k x_i a_i$. Кроме того, для любой абелевой группы B и для любых $b_1, \dots, b_k \in B$ можно определить $\varphi((x_1, \dots, x_k)) = \sum_{i=1}^k x_i b_i$. Тогда $\varphi : A \to B$ — гомоморфизм, и $\varphi(a_i) = b_i$. ■

4.2 Строение конечно порождённых абелевых групп

Следствие. *Пусть $A = \langle a_1, \dots, a_k \rangle$ — конечно порождённая абелева группа. Тогда существует $B \lhd \mathbb{Z}^k$ такая, что $A \cong \mathbb{Z}^k / B$.*

Доказательство. Пусть $c_1, \dots, c_k$ — свободные порождающие группы $\mathbb{Z}_k$. Тогда существует гомоморфизм $\varphi : \mathbb{Z}^k \to A$ такой, что $\varphi(c_i) = a_i$. Значит, $\operatorname{Im}\varphi = \langle \varphi(c_1), \dots, \varphi(c_k) \rangle = A$. Если $B = \operatorname{Ker}\varphi$, то $A \cong \mathbb{Z}^k / B$ по основной теореме о гомоморфизмах. ■

Итак, для описания конечно порождённых абелевых групп полезно исследовать подгруппы в $\mathbb{Z}^k$.

Теорема 4.3. *Пусть A — свободная абелева группа, $B < A$. Тогда B — также свободная абелева группа; причём в A и B существуют базисы $a_1, \dots, a_k$ и $b_1, \dots, b_l$ такие, что $k \geqslant l$, $b_i = m_i a_i$, $m_i \in \mathbb{N}$, и $m_1 \mid m_2 \mid \cdots \mid m_l$.*

Доказательство. Пусть $A \cong \mathbb{Z}^k$. Индукция по k.

База Если $k = 1$, то $A \cong \mathbb{Z}$, а $B \cong n\mathbb{Z}$, $n \in \mathbb{Z}_+$. Тогда можно положить $a_1 = 1$ и $b_1 = n$ (если $n > 0$) или $l = 0$ (если $n = 0$).

Переход Пусть $k > 1$. Если $B = 0$, то утверждение верно (при $l = 0$). Пусть теперь $B \neq 0$. Для любого базиса $a_1, \ldots, a_n$ в A и для любого $b \in B \setminus \{0\}$ существуют целые n_i такие, что $b = \sum_{i=1}^{k} n_i a_i$. Выберем базис $(a_1, \ldots, a_k)$ в A и $0 \neq b_1 \in B$ так, что $n_1 > 0$ и n_1 — наименьшее возможное.

1. Пусть $n_1 \nmid n_i$ при некотором $i \geqslant 2$. Тогда $n_i = qn_1 + r$, $q \in \mathbb{Z}$, $0 < r \leqslant n_1 - 1$. Тогда

$$b_1 = n_1 a_1 + n_i a_i + \sum_{j \geqslant 2, j \neq i} n_j a_j = n_1(a_1 + qa_i) + ra_i + \sum_{j \geqslant 2, j \neq i} n_j a_j.$$

   Значит, в базисе $(a_1 + qa_i, a_2, \ldots, a_k)$ разложение b_1 содержит коэффициент $r < n_1$ — противоречие с выбором. Значит, $n_1 \mid n_i$, $i \geqslant 2$. Положим $a_1' = \sum_{i=1}^{n} \frac{n_i}{n_1} a_i = a_1 + \sum_{i \geqslant 2} \frac{n_i}{n_1} a_i$. Тогда $(a_1', a_2, \ldots, a_k)$ — базис в A, причём $b_1 = n_1 a_1'$. Дальше будем считать, что $a_1' = a_1$.

2. Пусть $b \in B$, $b = \sum_{i=1}^{k} d_i a_i$. Предположим, что $n_1 \nmid d_1$, $d_1 = qn_1 + r$, $o < r < n$. Значит, $b - qb_1 = \sum_{i=1}^{k} (d_i - qn_i) a_i = ra_1 + \sum_{i=2}^{k} (d_i - qn_i) a_i$. Итак, в разложении элемента $b - qb_1 \in B$ по базису $(a_1, \ldots, a_k)$ есть коэффициент с $r < n_1$ — противоречит с выбором b_1. Т. к. $b_1 = n_1 a_1$, то $n_2 = n_3 = \cdots = n_k = 0$. Предположим, что $n_1 \nmid d_i$ при некотором $i \geqslant 2$. Положим $b_1' = b - \frac{d_1}{n_1} b_1 + b_1 \in B$, $b_1' = n_1 a_1 + \sum_{i=2}^{k} d_i a_i$. Тогда b_1' выражается через $(a_1, \ldots, a_k)$ с одним из коэффициентов равным n_1, применяя к нему старое рассуждение, получаем противоречие. Итак, $n_1 \mid d_i, i = 1, \ldots, k$. Это означает, что $B < n_1 A$.

3. Заметим, что $A = \langle a_1, \ldots, a_k \rangle = \langle a_1 \rangle \oplus \langle a_2, \ldots, a_k \rangle$. Обозначим $A^* = \langle a_2, \ldots, a_k \rangle$ и положим $B^* = B \cap A^*$, тогда $B = \langle b_1 \rangle \oplus B^*$. Действительно, $\forall b \in B$ $b = \sum_{i=1}^{k} d_i a_i$, и $n_1 \mid d_i$. Тогда $b = d_1 a_1 + \sum_{i=2}^{k} d_i a_i = d_1 a_1 + b^*$, где $d_1 a_1 = \frac{d_1}{n_1} b_1$, а $b^* = b - \frac{d_1}{n_1} b_1 \in B$, и $b^* \in A^* \Rightarrow b^* \in B^*$. Итак, $\langle b_1 \rangle + B^* = B$. Кроме того, $\langle b_1 \rangle \cap B^* \subseteq \langle a_1 \rangle \cap A^* = 0$. Значит, эта сумма — прямая. Применим предположение индукции к $B^* < A^*$. Получим согласованные базисы $(a_2', \ldots, a_k')$ в A^* и $(b_2, \ldots, b_l)$ в B^* такие, что $b_i = m_i a_i'$, $m_2 \mid \cdots \mid m_l$. Тогда $A = \langle a_1 \rangle \oplus \langle a_2', \ldots, a_k' \rangle \Rightarrow (a_1, a_2', \ldots, a_k')$ — базис в A. $B = \langle b_1 \rangle \oplus \langle b_2, \ldots, b_l \rangle$, причём $(b_2, \ldots, b_l)$ — базис в B^*, а тогда $(b_1, \ldots, b_l)$ — базис в B. Осталось выяснить, что $n_1 \mid m_2$.

   Это так, поскольку $B < n_1 A \Rightarrow$ коэффициенты разложения b_2 по базису $a_1, a_2', \ldots, a_k'$ делятся на n_1, т. е. $n_1 \mid m_2$. ■

Следствие. *Пусть C — конечно порождённая абелева группа. Тогда*

$$C \cong \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_l},$$

где $t \geqslant 0$ и m_i — натуральные числа, $m_i > 1$, причём $m_1 \mid m_2 \mid \cdots \mid m_l$.

Доказательство. Как мы знаем, $C \cong A/B$, где A — свободная абелева группа и $B < A$. Выберем в A и B согласованные базисы (из теоремы). Тогда $A = \langle a_1\rangle \times \cdots \times \langle a_k\rangle$, и $B = \langle b_1\rangle \times \cdots \times \langle b_l\rangle$, при этом $\langle b_i\rangle < \langle a_i\rangle$. Значит,

$$A/B \cong \langle a_1\rangle/\langle b_1\rangle \times \cdots \times \langle a_l\rangle/\langle b_l\rangle \times \langle a_{l+1}\rangle \times \cdots \times \langle a_k\rangle \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_l\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \cong \mathbb{Z}^{k-l} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_l}.$$

Наконец, если $m_i = 1$, то $\mathbb{Z}_{m_i} = \{0\}$ и этот сомножитель можно выкинуть. ■

Следствие. *Пусть C — конечно порождённая абелева группа. Тогда*

$$C \cong \mathbb{Z}^t \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}} \qquad (*)$$

где $p_1, \ldots, p_s$ — простые (не обязательно различные), а $\alpha_i \in \mathbb{N}$.

Доказательство. Если $m_i = p_1^{\alpha_1} \ldots p_d^{\alpha_d}$, то $\mathbb{Z}_{m_i} \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_d^{\alpha_d}}$. Осталось применить это к каждому сомножителю вида $\mathbb{Z}_{m_i}$. ■

Следующая цель — доказать единственность такого разложения (точнее, единственность набора из t и системы $(p_1^{\alpha_1}, \ldots, p_s^{\alpha_s})$ — с точностью до перестановки).

Утверждение 4.2. *Пусть C — группа вида (*). Тогда $T(C) = \{0\}^t \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ и $C/T(C) \cong \mathbb{Z}^t$.*

Доказательство. Пусть $x \in C$, $x = (x_1, \ldots, x_t, y_1, \ldots, y_s)$. Если $x_i \neq 0$, то $\operatorname{ord} x = \infty$, ибо $\forall n \in \mathbb{Z}_+ \ nx_i \neq 0$. Если $x_1 = \cdots = x_t = 0$, то $p_1^{\alpha_1} \ldots p_s^{\alpha_s} x = 0$. Итак, $T(C)$ охарактеризован.

Тогда $C/T(C) \cong (\mathbb{Z}/\{0\})^t \times \mathbb{Z}_{p_1}^{\alpha_1}/\mathbb{Z}_{p_1}^{\alpha_1} \times \cdots \times \mathbb{Z}_{p_s}^{\alpha_s}/\mathbb{Z}_{p_s}^{\alpha_s} \cong \mathbb{Z}^t$. ■

Теорема 4.4. *Пусть F — поле, а $G < F^*$, $|F| < \infty$. Тогда G — циклическая. В частности, если $|F| < \infty$, то F^* — циклическая.*

Доказательство. Поскольку $|G| < \infty$, G — конечно порождённая абелева группа $\Rightarrow G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, где $1 < m_1 \mid m_2 \mid \cdots \mid m_k$. Тогда $\forall g \in G \ g^{m_k} = 1$, т. е. все элементы G — это корни уравнения $x^{m_k} - 1 = 0 \Rightarrow$ их не более m_k, т. е. $|G| \leqslant m_k$. Значит, $k = 1$ и $G \cong \mathbb{Z}_{m_k}$. ■

4.2.1 Единственность представления

Пусть

$$A = \mathbb{Z}^t \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}},$$
$$B = \mathbb{Z}^u \times \mathbb{Z}_{q_1^{\beta_1}} \times \cdots \times \mathbb{Z}_{q_r^{\beta_r}},$$

p_i, q_i — простые. Пусть $A \cong B$, тогда хотим доказать, что $t = u$, $r = s$ и наборы $(p_1^{\alpha_1}, \ldots, p_s^{\alpha_s})$ и $(q_1^{\beta_1}, \ldots, q_r^{\beta_r})$ совпадают с точностью до перестановки.

Следствие. *$T(A) \cong T(B)$, $t = u$.*

Доказательство. Первое утверждение очевидно. Для второго: $\mathbb{Z}^t \cong A/T(A) \cong B/T(B) \cong \mathbb{Z}^u$. Итак, в этой группе существует базис из t и u элементов $\Rightarrow t = u$. ■

В дальнейшем можно считать, что $A = T(A)$, $B = T(B)$ (т. е. $t = u = 0$).

Утверждение 4.3. *Пусть $A = \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \ldots \mathbb{Z}_{p^{\alpha_k}} \times \mathbb{Z}_{p_2^{\gamma_2}} \times \cdots \times \mathbb{Z}_{p_l^{\gamma_l}}$, где $p_2, \ldots, p_l$ отличны от p. Тогда (единственная) силовская p-подгруппа в A есть $P_p = \mathbb{Z}_{p^{\alpha_1}} \times \ldots \mathbb{Z}_{p^{\alpha_k}} \times \{0\}^{l-1}$.*

Доказательство. Ясно, что $P_p < A$. $|A| = p^{\alpha_1+\dots+\alpha_k} \cdot \prod_{i=2}^{l} p_i^{\gamma_i}$, а $|P_p| = p^{\alpha_1+\dots+\alpha_k}$. Значит, P_p — силовская p-подгруппа. Наконец, $P_p \lhd A \Rightarrow N_p = 1$. ■

Следствие. *Достаточно доказать совпадение наборов $(p_i^{\alpha_i})$ и $(q_j^{\beta_j})$ для случая $p_1 = \dots = p_s = q_1 = \dots = q_r$.*

Утверждение 4.4. *Пусть $A = \mathbb{Z}_{p^{\alpha_1}} \times \dots \mathbb{Z}_{p^{\alpha_s}}$, $B = \mathbb{Z}_{p^{\beta_1}} \times \dots \mathbb{Z}_{p^{\beta_r}}$. Тогда, если $A \cong B$, то наборы $(\alpha_1, \dots, \alpha_s)$ и $(\beta_1, \dots, \beta_r)$ совпадают (с точностью до перестановки).*

Доказательство. Индукция по $|A|$. Если $|A| = p$, то $A \cong B \cong \mathbb{Z}_p$.

Пусть $|A| > p$. Тогда рассмотрим $pA = p\mathbb{Z}_{p^{\alpha_1}} \times \dots \times p\mathbb{Z}_{p^{\alpha_s}} \cong \mathbb{Z}_{p^{\alpha_1-1}} \times \dots \times \mathbb{Z}_{p^{\alpha_s-1}}$ и $pB = p\mathbb{Z}_{p^{\beta_1-1}} \times \dots \times p\mathbb{Z}_{p^{\beta_r-1}}$. Тогда, т. к. $pA \cong pB$, $|pA| = |pB|$. Но $|pA| = \frac{|A|}{p^s}$ и $|pB| = \frac{|B|}{p^r}$. Итак, $s = r$.

Кроме того, к pA и pB можно применить предположение индукции, получив, что наборы $(\alpha_1 - 1, \dots, \alpha_s - 1)$ и $(\beta_1 - 1, \dots, \beta_r - 1)$ совпадают с точностью до перестановки и, возможно, выкидывания нулей из этих наборов (случай $\alpha_i - 1 = 0$ соответствует тривиальному сомножителю $\mathbb{Z}_{p^0}$, который можно выкинуть). Но, так как $s = r$, нулей в них одинаковое количество $\Rightarrow$ он совпадают с точностью до перестановки, а значит, совпадают и наборы $(\alpha_1, \dots, \alpha_s)$ и $(\beta_1, \dots, \beta_r)$.

Если $pA = \{0\}$, то $\alpha_1 = \dots = \alpha_s = \beta_1 = \dots = \beta_r = 1$, и утверждение также верно. ■

Теорема 4.5. *Пусть A — конечно порождённая абелева группа. Тогда*

$$A = \mathbb{Z}^t \times \mathbb{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}_{p_s^{\alpha_s}},$$

где $t \geqslant 0$, $s \geqslant 0$, p_i — простые числа, $\alpha_i \geqslant 1$. В любых таких представлениях группы A совпадают значения t, а также наборы $(p_1^{\alpha_1}, \dots, p_s^{\alpha_s})$ (с точностью до перестановки).

Замечание. Таких разложений может быть много.

1. В группе $\mathbb{Z}^t$ существует много базисов, любой базис $a_1, \dots, a_t$ даёт прямое разложение $\mathbb{Z}^t = \langle a_1 \rangle \times \dots \times \langle a_t \rangle$.

2. В группе $\mathbb{Z}_p \times \mathbb{Z}_p$ можно выбрать любые два элемента a и b, так что $a \notin \langle b \rangle$, $b \notin \langle a \rangle$ (тогда $a, b \neq 0$). В таком случае, $|\langle a, b \rangle| = p^2$, т. е. $\langle a, b \rangle = \mathbb{Z}_p \times \mathbb{Z}_p = \langle a \rangle \times \langle b \rangle$. По сути, $\mathbb{Z}_p^2$ — это двумерное пространство над полем $\mathbb{Z}_p$, а (a, b) — базис в нём.

3. Пусть $A = \mathbb{Z} \times \mathbb{Z}_2$. Выберем $a = (1, 1)$ и $b = (0, 1)$. Тогда $\langle a \rangle \cong \mathbb{Z}$, $\langle b \rangle \cong \mathbb{Z}_2$, и $A = \langle a \rangle \times \langle b \rangle$. («канонический» выбор — это $(1, 0)$, $(0, 1)$).

Упражнение. Мы доказали, что любая конечно порождённая группа A есть $A \cong \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$, где $t \geqslant 0$, $k \geqslant 0$, $m_i > 1$ и $m_1 \mid m_2 \mid \dots \mid m_k$. Докажите, что и в этом представлении все параметры восстанавливаются однозначно.

Замечание. Ещё одно следствие из теоремы о существовании согласованных базисов. Пусть $A = \mathbb{Z}^k$, B — подгруппа в A, порождённая столбцами некоторой

матрицы $M = (m_{ij}) \in M_{k\times n}(\mathbb{Z})$. Тогда в A и B существуют согласованные базисы $(a_1, \dots, a_k)$ и $(b_1, \dots, b_l)$ такие, что $b_i = d_i a_i$, $d_1 \mid d_2 \mid \dots \mid d_l$.

Замена базиса в A соответствует умножению M на матрицу перехода $S \in M_{k\times k}(\mathbb{Z})$, $\det S = \pm 1$. Можно показать, что переход к $(b_1, \dots, b_l, 0, \dots, 0)$ также можно осуществить с помощью матрицы перехода $T \in M_{n\times n}(\mathbb{Z})$, $\det T = \pm 1$. таким образом,

$$SMT = Diag(d_1, d_2, \dots, d_l, 0, \dots).$$

Полученная матрица называется *смитовой нормальной формой* матрицы M. В этом случае $A/B = \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_l} \times \mathbb{Z}^{k-l}$, где $d_1, \dots, d_l$ определяются однозначно. Таким образом, смитова нормальная форма матрицы M единственна.

Упражнение. Восполните пробелы.

Упражнение. $d_i = \mathrm{GCD}$(миноры матрицы M порядка i).

Глава 5

Кольца и поля

5.1 Базовые понятия теории колец

Определение 5.1. Кольцо — это множество с двумя операциями $(R, +, \cdot)$, для которых выполняются следующие свойства:

1. $(R, +)$ — абелева группа
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ и $(a + b) \cdot c = a \cdot c + b \cdot c$

Кольцо *коммутативно*, если $\forall a, b \in R\ a \cdot b = b \cdot a$.

Кольцо — *с единицей*, если $\exists 1 \in R$: $\forall a \in R\ 1 \cdot a = a \cdot 1 = a$.

Определение 5.2. Кольцо с единицей называется *алгеброй* на полем F, если $F \subseteq R$ и $\forall a \in R\ \forall f \in F\ af = fa$. В этом случае R — линейное пространство над F. *Размерность* алгебры — размерность этого линейного пространства.

Примеры.

1. Любое поле F — алгебра над F (а также над простым подполем $\mathbb{Q}$ или $\mathbb{Z}_p$).
2. $F[x]$ — алгебра над F.
3. $M_{m\times m}(F)$ — некоммутативная алгебра над F (отождествляем элементы $\lambda \in F$ со скалярными матрицами λE).

Определение 5.3. Пусть R, S — кольца. Отображение $\varphi : R \to S$, если

$$\forall a, b \in R\ \varphi(a + b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b)$$

Замечание. φ — гомоморфизм абелевых групп $(R, +)$ и $(S, +)$. В частности, $\varphi(0) = 0$ и $\varphi(-a) = -\varphi(a)$.

Определение 5.4. Пусть $\varphi : R \to S$ — гомоморфизм колец. *Образ* $\operatorname{Im}\varphi = \varphi(R)$, его *ядро* $\operatorname{Ker}\varphi = \varphi^{-1}(0)$.

Замечание. $\operatorname{Im}\varphi$ — подкольцо в S.

Определение 5.5. Пусть $\varnothing \neq I \subseteq R$. I называется *идеалом* кольца R (запись: $I \lhd R$), если I — подгруппа в $(R, +)$ и $\forall a \in R\ aI \subseteq I \supseteq Ia$.

Утверждение 5.1. *Пусть $\varphi : R \to S$ — гомоморфизм колец, тогда* $\operatorname{Ker}\varphi \lhd R$.

Доказательство. Т. к. φ — гомоморфизм колец, то φ — гомоморфизм аддитивных групп этих колец, т. е. $\operatorname{Ker}\varphi < (R,+)$. Пусть теперь $b \in \operatorname{Ker}\varphi$, $a \in R$. Тогда $\varphi(ab) = \varphi(a)\varphi(b) = \varphi(a)\cdot 0 = 0$, т. е. $ab \in \operatorname{Ker}\varphi \Rightarrow a\cdot\operatorname{Ker}\varphi \subseteq \operatorname{Ker}\varphi$. Аналогично, $(\operatorname{Ker}\varphi)\cdot a \subseteq \operatorname{Ker}\varphi$. ■

Пусть R — кольцо, $I \lhd R$. Тогда $(R/I,+)$ — группа. Определим на R/I умножение:

$$(a+I)\cdot(b+I) = ab+I.$$

Замечание. Произведение множеств $a+I$ и $b+I$ — не обязательно $ab+I$!

Упражнение. $(a+I)(b+I) \subseteq ab+I$

Проверим корректность умножения. Пусть $b+I = b'+I$ ($\Leftrightarrow b-b' \in I$). Значит, $a(b-b') = ab-ab' \in I \Rightarrow ab+I = ab'+I$. Итак, от выбора представителя b в $b+I$ произведение не зависит. Аналогично, оно не зависит от выбора представителя в $a+I$.

Теорема 5.1. *Пусть $I \lhd R$. Тогда $(R/I,+,\cdot)$ — кольцо. При этом существует канонический эпиморфизм колец $\pi : R \to R/I$, $\pi(a) = a+I$.*

Доказательство. Все аксиомы кольца проверяются рутинным образом. Например, дистрибутивность:

$$(a+I)\cdot((b+I)+(c+I)) = (a+I)\cdot((b+c)+I) = a(b+c)+I = (ab+ac)+I =$$
$$= (ab+I)+(ac+I) = (a+I)\cdot(b+I)+(a+I)\cdot(c+I).$$

Аналогично, проверка того, что π — эпиморфизм, рутинна. ■

Определение 5.6. Кольцо $(R/I,+,\cdot)$, описанное выше, называется *факторкольцом* R по идеалу I.

Теорема 5.2 (основная теорема о гомоморфизмах колец)**.** *Пусть $\varphi : R \to S$ — гомоморфизм колец. Тогда* $\operatorname{Ker}\varphi \lhd R$, $\operatorname{Im}\varphi$ *— подкольцо в S и при этом*

$$\operatorname{Im}\varphi \cong R/\operatorname{Ker}\varphi.$$

Доказательство. φ — это также гомоморфизм аддитивных групп, поэтому $\operatorname{Im}\varphi \cong R/\operatorname{Ker}\varphi$ как абелевы группы. Этот изоморфизм задаётся $\psi : \operatorname{Im}\varphi \to R/\operatorname{Ker}\varphi$, $\psi(x) = \varphi^{-1}(x)$.

Теперь осталось проверить, что ψ сохраняет умножение. Пусть $x = \varphi(a)$, $y = \varphi(b)$. Тогда $xy = \varphi(ab) \Rightarrow \psi(x) = a+I$, $\psi(y) = b+I$ и $\psi(xy) = ab+I = (a+I)(b+I)$, что и требовалось. ■

Замечание. Существуют аналоги первой и второй теоремы об изоморфизмах.

Определение 5.7. Пусть R — кольцо, $I \lhd R$. Тогда I называется *максимальным* идеалом, если

1. $I \neq R$.

2. Если $J \lhd R$ и $I \subset J$, то $J = I$ или $J = R$.

Утверждение 5.2. *Пусть R — коммутативное кольцо с единицей, I — максимальный идеал в R. Тогда R/I — поле.*

Доказательство. R/I — кольцо, при этом $R \neq I \Rightarrow R/I$ состоит более чем из одного элемента. Заметим: $1 \notin I$ (иначе $I \supseteq RI \supseteq R \cdot 1 = R$). Значит, $1 + I \neq I$ — единица кольца R/I.

Осталось проверить: любой $a + I \in R/I \setminus \{I\}$ обратим. Пусть $J = I + aR$. Тогда $J \lhd R$, $I \subseteq J$ и $a \in J \setminus I$. Значит, $J \neq I \Rightarrow J = R$. Значит, $1 \in J$, т. е. $1 = x + ab$, $x \in I$, $b \in R$. Тогда

$$(a + I) \cdot (b + I) = ab + I = ab + x + I = 1 + I.$$

Значит, $a + I$ обратим. ■

Замечание. Для коммутативных колец без единицы утверждение также верно.

Замечание. Для некоммутативных колец утверждение неверно; более того, ненулевые элементы факторкольца не обязательно обратимы. Например, в $M_{n\times n}(F)$ нет нетривиальных идеалов $\Rightarrow 0 \lhd M_{n\times n}(F)$ — максимален!

Определение 5.8. Пусть $a_1, \ldots, a_n \in R$. Тогда идеал, *порождённый* этими элементами это

$$(a_1, \ldots a_n) = \bigcap_{I \lhd R, a_i \in I} I.$$

Идеал называется *главным*, если он порождён одним элементом.

Замечание. Если R — коммутативное кольцо с единицей, то

$$(a_1, \ldots, a_n) = a_1 R + \cdots + a_n R.$$

Упражнение. Опишите $(a_1, \ldots, a_n)$ в некоммутативном кольце (с единицей).

Теорема 5.3. *Пусть F — поле, $R = F[x]$, $I \lhd R$. Тогда*

1. I — главный (т. е. $I = (f)$, $f \in R$).

2. I максимален $\Leftrightarrow$ f неприводим (над F).

Доказательство. Если $I = 0$, то $I = (0)$. Пусть $I \neq 0$ и пусть f — ненулевой многочлен наименьшей степени, лежащий в I. Тогда $(f) \subseteq I$. Пусть $g \in I$, тогда $g = qf + r$, где $q, r \in R$, $\deg r < \deg f$. Заметим, что $r = g - qf \in I \Rightarrow r = 0$ (иначе, это противоречит выбору f). Значит, $g = qf \in (f) \Rightarrow I \subseteq (f)$. Итак, $(f) = I$.

Если f — приводим, то $f = f_1 f_2$, $0 < \deg f_i < \deg f \Rightarrow f_1, f_2 \notin I$. Значит, $(f_1) \supseteq I$ и $R \neq (f_1) \neq I \Rightarrow I$ не максимален. Наоборот, пусть f неприводим, $J \lhd R$, $I \subseteq J$. Тогда $J = (g)$, $g \in R$. Так как $f \in J$, $g \mid f$, т. е. $\deg g = 0$ или $g = \alpha f$, $\alpha \in F^*$. В первом случае $J = (g) = (1) = R$, во втором — $J = (g) = (f) = I$. Итак, I максимален. ■

Следствие. *Если $f \in F[x]$ неприводим, то $F[x]/(f)$ — поле.*

5.2 Поле разложения многочлена

Определение 5.9. Пусть $R \subseteq S$ — коммутативные кольца, $s \in S$. Тогда $R[s]$ — подкольцо в s, порождённое R и s, т. е. пересечение всех подколец в S, содержащих R и s; при этом,

$$R[s] = \left\{ \sum_{i=0}^{n} r_i s^i \mid r_i \in R \right\}.$$

Пусть $F \subseteq K$ и F — поле, $a \in K$. Тогда $F(a)$ — подполе в K, порождённое F и a, т. е. $F(a)$ — это пересечение всех подполей K' в K, что $F \subseteq F$, $a \in K'$. Если $K = F(a)$, то K называется *расширением* поля F элементом a.

Утверждение 5.3. *Пусть F — поле, $f \in F[x]$ — неприводимый многочлен. Тогда существует расширение $K = F(a)$, где a — корень многочлена f. Более того, все такие расширения изоморфны, и они изоморфны $F[x]/(f)$. При этом, $K = F(a) = F[a]$.*

Доказательство. Положим $K = F[x]/(f)$ — поле. Для любого $b \in F$ отождествим $b + (f)$ с b.

Упражнение. Все элементы $b + (f)$ различны.

Пусть $a = x + (f)$. Тогда $f(a) = f(x) + (f) = (f) \Rightarrow a$ — корень многочлена f в K. Кроме того, разумеется, $K = F[a] = F(a)$. Итак, одно расширение построено, $K = F[a]$.

Пусть $L = F(c)$ — произвольное расширение поля F элементом таким, что $f(c) = 0$. Построим гомоморфизм $\varphi : F[x] \to L$, $\varphi(g) = g(c)$. Тогда $\operatorname{Im}\varphi \cong F[x]/\operatorname{Ker}\varphi$, при этом $f \in \operatorname{Ker}\varphi \Rightarrow (f) \subseteq \operatorname{Ker}\varphi$, и (f) — максимален. Значит, $\operatorname{Ker}\varphi = F[x]$ или $\operatorname{Ker}\varphi = (f)$. Первый случай невозможен, ибо $\varphi(1) = 1 \neq 0$, т. е. $1 \notin \operatorname{Ker}\varphi$. Итак, $\operatorname{Ker}\varphi = (f) \Rightarrow \operatorname{Im}\varphi \cong F[x]/(f) = K$. Значит, $\operatorname{Im}\varphi$ — подполе в L, содержащее $F = \varphi(F)$ и $c = \varphi(x)$. Значит, $\operatorname{Im}\varphi \supseteq F(c) = L \Rightarrow \operatorname{Im}\varphi = L \cong K$ (при этом изоморфизме элементу c соответствует $x + (f)$). ■

Следствие. *Пусть $f \in F[x]$, $\deg f > 0$. Тогда существует поле $K \supseteq F$ такое, что многочлен f раскладывается над K на линейные множители.*

Доказательство. Индукция по $\deg f$, база при $\deg f = 1$ тривиальна: $K = F$. Пусть теперь $\deg f > 1$, для многочленов меньших степеней это верно и f_1 — неприводимый делитель многочлена f. Тогда существует расширение $L = F[a]$, где a — корень f_1. Значит, над полем L многочлен f раскладывается как $f(x) = (x - a)g(x)$. Осталось применить предположение индукции к полю L и многочлену $g(x)$. ■

Определение 5.10. Пусть $f \in F[x]$, $\deg f > 0$. *Полем разложения* многочлена f над F называется поле $K \supseteq F$ такое, что

1. Над K f раскладывается на линейные множители.
2. K порождено корнями f и исходным полем.

Упражнение. Поле разложения многочлена f существует и единственно с точностью до изоморфизма.

Упражнение. Пусть p — простое число, тогда любое поле из p^n элементов есть поле разложения $x^p - x$ над $\mathbb{Z}_p$. Кроме того, это поле разложения действительно содержит ровно p^n элементов.