Алгебра
Семестр 3

Ю.Г. Прохоров

Москва

2011

Содержание

1 Группы, подгруппы, теорема Лагранжа

Определение. *Группой* называется непустое множество G с операцией $G \times G \to G$, $(a, b) \mapsto a \circ b$, удовлетворяющей следующим свойствам:

(1) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a,\, b,\, c \in G$ (закон ассоциативности);

(2) $\exists 1 \in G \quad a \circ 1 = 1 \circ a = a \quad \forall a \in G$ (существование единичного элемента);

(3) $\forall a \in G\ \exists a^{-1} \in G \quad a \circ a^{-1} = a^{-1} \circ a = 1$ (существование обратного элемента).

Группа называется *абелевой* * (или коммутативной) если выполнено свойство

- $a \circ b = b \circ a \quad \forall a,\, b \in G$ (коммутативность).

Группа G называется *конечной*, если она состоит из конечного числа элементов. В этом случае число ее элементов называется *порядком* этой группы и обозначается $|G|$. Подмножество $H \subset G$ группы называется *подгруппой*, если H является группой с той же операцией.

*Niels Henrik Abel – норвежский математик (1802 – 1829)

Примеры. (1) S_n – *симметрическая* группа (группа подстановок), $\mathrm{A}_n \subset \mathrm{S}_n$ – *знакопеременная* группа (подгруппа четных подстановок).

(2) $\mathrm{GL}_n(\Bbbk)$ – *полная линейная группа* над полем $\Bbbk$ (группа невырожденных матриц размера $n \times n$), $SL_n(\Bbbk) \subset \mathrm{GL}_n(\Bbbk)$ – *специальная линейная группа* (подгруппа матриц с определителем 1).

(3) Q_8 – *группа кватернионов*, подгруппа в $\mathrm{GL}_2(\mathbb{C})$, состоящая из восьми элементов $\pm\mathbf{1}$, $\pm\mathbf{i}$, $\pm\mathbf{j}$, $\pm\mathbf{k}$, где

$$\mathbf{1} := E, \quad \mathbf{i} := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

(4) $\boldsymbol{\mu}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ – группа корней степени n из 1.

(5) $\mathbb{Z}_n$ – группа классов вычетов (с операцией сложения).

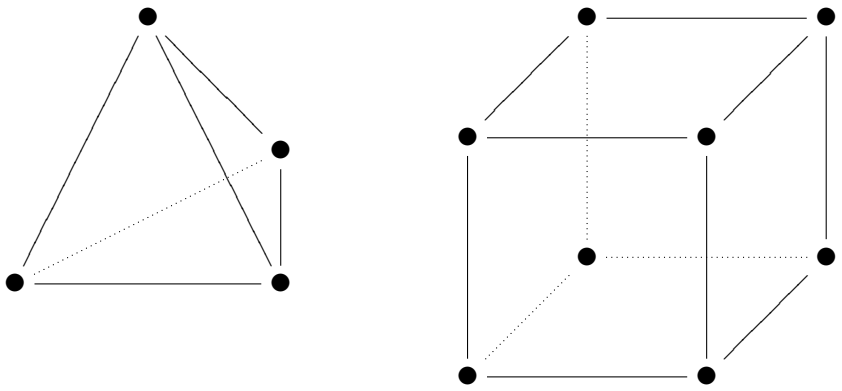
(6) Отображение аффинного пространства $\mathbb{A}^n_{\Bbbk}$ в себя называется называется аффинным преобразованием, если образ любой прямой – прямая. Все аффинные преобразования $\mathbb{A}^n_{\Bbbk}$ образуют *группу аффинных преобразований* $\mathrm{Aff}_n(\Bbbk)$. Она содержит подгруппу параллельных переносов $\mathrm{TranAff}_n(\Bbbk)$.

(7) Отображение евклидова пространства $\mathbb{E}^n$ в себя называется называется движением, если оно сохраняет расстоя-

ния. Все движения $\mathbb{E}^n$ образуют *группу движений* EAff_n, которая является подгруппой в $\mathrm{Aff}_n(\mathbb{R})$.

(8) Все движения евклидова пространства $\mathbb{E}^2$, переводящие в себя правильный n-угольник Γ_n, образуют подгруппу $\mathrm{D}_n \subset \mathrm{EAff}_2$. Она называется *группой диэдра*.

(9) Все движения евклидова пространства $\mathbb{E}^3$, переводящие в себя правильный тетраэдр (соответственно, куб), образуют подгруппу в EAff_3, *группу движений тетраэдра* (соответственно, *куба*).



Аналогично определяется группа движений икосаэдра.

Определение. Пусть G – группа и пусть $S \subset G$ – подмножество. Положим

$$\langle S \rangle := \{a_1^{n_1} \cdots a_m^{n_m} \mid a_i \in S, \quad n_i \in \mathbb{Z}\}.$$

Ясно, что $\langle S\rangle$ – подгруппа в G. Говорят, что группа G *порождается* множеством S, если $\langle S\rangle = G$. Иначе говоря, любой элемент $g \in G$ представляется в виде произведения степеней элементов из S.

Примеры. (1) Симметрическая группа S_n порождается транспозициями.

(2) Полная линейная группа $\mathrm{GL}_n(\Bbbk)$ порождается элементарными матрицами.

(3) Группа $\boldsymbol{\mu}_n$ порождается любым первообразным корнем из 1.

Замечание. Не всякая группа порождается конечным числом элементов. Например, группа $\mathbb{R}^+$ несчётна, поэтому не может порождаться конечным числом элементов.

Задача. Докажите, что группы $\mathbb{Q}^+$ и $\mathbb{Q}^*$ не могут быть порождены конечным числом элементов.

Задача. Является ли конечно порожденной группа $\mathbb{Q}/\mathbb{Z}$?

Определение. Для любых подмножеств A, $B \subset G$ группы G положим

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

В частности, для подгруппы $H \subset G$ и элемента $a \in H$ подмножество

$$aH := \{ah \mid h \in H\}$$

называется *левым смежным классом*. Аналогично определяются правые смежные классы.

Множество всех смежных классов обозначается G/H. Мощность множества G/H обозначается $[G : H]$ и называется *индексом* подгруппы H.

Заметим, что запись смежного класса в виде gH не является единственной:

Лемма. $gH = g'H \iff \exists\ h \in H \quad g' = gh$.

Доказательство. Если $gH = g'H$, то $g' \in gH$ и тогда $g' = gh$ для некоторого $h \in H$. Обратно, если $g' = gh$ для некоторого $h \in H$, то $g'h' = ghh' \in gH$ и поэтому $g'H \subset gH$. Аналогично доказывается обратное включение. □

Теорема. *Пусть G – группа и пусть $H \subset G$ – любая подгруппа.*

(1) *Группа G является объединением левых смежных классов $gH \in G/H$.*

(2) *Если два левых смежных класса g_1H и g_2H пересекаются, то они совпадают.*

(3) *Все левые смежные классы равномощны.*

Аналогичные утверждения верны для правых смежных классов.

Доказательство. (1) очевидно, поскольку $g \in gH$.

(2) Пусть $g \in g_1H \cap g_2H$. Тогда $g = g_1h_1 = g_2h_2$ для некоторых $h_1, h_2 \in H$. Отсюда $g_2 = g_1(h_1h_2^{-1})$ и $g_1H = g_2H$ по лемме.

(3) Отображение $H \to gH$, $h \mapsto gh$ является биекцией. $\square$

Следствие (теорема Лагранжа)**.** [†] *Если G – конечная группа, то*

$$|G| = |H|\ [G : H].$$

[†]Joseph Louis Lagrange – французский математик, астроном и механик итальянского происхождения (1736 –1813)

2 Теорема о гомоморфизме

2.1 Нормальные подгруппы

Определение. Подгруппа $H \subset G$ группы G называется *нормальной* (обозначается $H \lhd G$), если $gHg^{-1} \subset H \quad \forall g \in G$.

Замечание. На самом деле, в условиях выше верно равенство $gHg^{-1} = H$. (Докажите самостоятельно).

Примеры. (1) В абелевой группе любая подгруппа нормальна.

(2) В любой группе G имеются тривиальные нормальные подгруппы G и $\{1\}$.

(3) $SL_n(\Bbbk) \lhd \mathrm{GL}_n(\Bbbk)$.

Замечание. Говорят, что элементы g и g' группы G сопряжены, если существует $x \in G$ такой, что $g' = xgx^{-1}$. (Не путайте с комплексным сопряжением!) Несложно проверить, что отношение сопряженности является отношением эквивалентности. Таким образом, группа G разбивается на непересекающееся объединение *классов сопряженных элементов*. Подгруппа H является нормальной тогда и только тогда, когда она составлена из классов сопряженных элементов.

Определение. *Центром* группы G называется подмножество

$$Z(G) := \{z \in G \mid gz = zg \quad \forall g \in G\}.$$

Очевидно, что центр – подгруппа и она нормальна (докажите самостоятельно). Более того, любая подгруппа $H \subset Z(G)$ нормальна в G.

Задача. Подгруппа $H \subset G$ порядка 2 нормальна тогда и только тогда, когда H содержится в центре. В частности, S_n не содержит нормальных подгрупп порядка 2.

Например, $Z(\mathrm{GL}_n(\Bbbk))$ состоит из скалярных матриц, а $Z(SL_n(\Bbbk))$ состоит из скалярных матриц с определителем 1.

Предложение. *Следующие условия эквивалентны:*

(1) $H \lhd G$;

(2) $gH = Hg \quad \forall g \in G$.

Доказательство. Пусть $H \lhd G$, пусть $g \in G$ и пусть $gh \in gH$, где $h \in H$. Тогда $ghg^{-1} = h' \in H$. Следовательно, $gh = h'g \in Hg$ и поэтому $gH \subset Hg$. Обратное включение доказывается аналогично.

Пусть $gH = Hg \quad \forall g \in G$ и пусть $h \in H$. Тогда $gh \in Hg$. Следовательно, $gh = h'g$ для некоторого $h' \in H$ и поэтому $ghg^{-1} = h' \in H$. Это означает, что $H \lhd G$. □

Следствие. *Подгруппа индекса 2 нормальна.*

Примеры. (1) $\mathrm{D}_n \rhd R_n$, где R_n – подгруппа поворотов.

(2) В каждый правильный $2n$-угольник можно вписать правильный n-угольник. Это задает вложение D_n в D_{2n} как нормальной подгруппы.

(3) $\mathrm{Q}_8 \rhd \langle \mathbf{i} \rangle$, $\langle \mathbf{j} \rangle$, $\langle \mathbf{k} \rangle$.

(4) $\mathrm{S}_n \rhd \mathrm{A}_n$.

2.2 Изоморфизмы и автоморфизмы групп

Определение. *Изоморфизм* групп – это отображение $\varphi : G \to G_1$, которое является биекцией и удовлетворяет условию

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \forall a, b \in G.$$

Группы G и G_1 называются *изоморфными* (обозначается $G \simeq G_1$), если между ними существует по крайней мере один изоморфизм.

Пример. Отображение

$$\exp : \mathbb{R}^+ \to \mathbb{R}_{>0}, \qquad a \mapsto e^a$$

является изоморфизмом групп.

Задача. Изоморфны ли группы $\mathbb{Q}^+$ и $\mathbb{Q}^*$?

Определение. Изоморфизм группы на себя называется *автоморфизмом*. Иначе говоря, автоморфизм – это отображение $\varphi : G \to G$ группы на себя, которое является биекцией и удовлетворяет условию $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a,\, b \in G$.

Примеры. (1) Тождественное отображение – автоморфизм.

(2) Отображение $\varphi(a) = a^{-1}$ является автоморфизмом тогда и только тогда, когда группа абелева.

(3) Комплексное сопряжение $\varphi(z) = \bar{z}$ является автоморфизмом в группах $\mathbb{C}$ и $\mathbb{C}^*$.

(4) Отображение $\varphi(A) = (A^{-1})^{\mathrm{T}}$ является автоморфизмом полной линейной группы $\mathrm{GL}_n(\Bbbk)$, а также и специальной линейной группы $SL_n(\Bbbk)$.

Задача. Когда отображение $a \mapsto a^2$ является автоморфизмом?

Замечание. Все автоморфизмы $\mathrm{Aut}(G)$ группы G образуют группу с операцией – композиция отображений.

Определение. Отображение

$$\varphi_g : a \mapsto gag^{-1}$$

называется *внутренним автоморфизмом* группы.

Очевидно, что φ_g – действительно автоморфизм (проверьте самостоятельно). Внутренние автоморфизмы образуют подгруппу $\mathrm{Int}(G) \subset \mathrm{Aut}(G)$.

Примеры. (1) $\mathrm{Aut}(\mathrm{S}_3) = \mathrm{Int}(\mathrm{S}_3) \simeq \mathrm{S}_3$;

(2) $\mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$.

Замечание. Подгруппа $H \subset G$ является нормальной тогда и только тогда, когда $\varphi_g(H) \subset H$ для любого внутреннего автоморфизма φ_g.

Пример. Рассмотрим следующее подмножество в симметрической группе S_4:

$$\mathrm{V}_4 := \{(1),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}.$$

Несложно проверить, что это подгруппа. Она называется *четверной группой Клейна*. Любой внутренний автоморфизм S_4 сохраняет четность и порядки элементов. Так как V_4 – единственная нециклическая подгруппа порядка 4 состоящая только из четных подстановок, то она нормальна.

2.3 Факторгруппы

Пусть H – нормальная подгруппа группы G (в мультипликативной записи). Напомним, что через G/H мы обозначаем множество всех левых смежных классов. Определим умножение

смежных классов следующим образом:

$$(aH) \cdot (bH) = (ab)H.$$

Лемма. *Определенное выше умножение не зависит от способа записи смежных классов.*

Доказательство. Пусть $aH = a'H$ и $bH = b'H$. Тогда $a' = ah_1$ и $b' = bh_2$ для некоторых $h_1, h_2 \in H$. Имеем

$$a'b' = (ah_1)(bh_2) = (ab)(b^{-1}h_1b)h_2,$$

где $b^{-1}h_1b \in H$ (поскольку $H \lhd G$). Следовательно, $a'b' = abh$ для $h := (b^{-1}h_1b)h_2 \in H$ и поэтому $(aH) \cdot (bH) = (ab)H$. □

Предложение. *G/H является группой с определенным выше умножением.*

Доказательство. По определению имеем

$$(aH \cdot bH) \cdot cH = (ab)cH = a(bc)H = aH \cdot (bH \cdot cH).$$

Это доказывает ассоциативность операции. Нейтральным элементом в G/H является тривиальный смежный класс $1H = H$, а обратным к элементу aH является элемент $a^{-1}H$. □

Пример. Пусть $G := \mathbb{C}^*$ и пусть $H := \{z \mid |z = 1|\}$. Каждый элемент $z \in \mathbb{C}^*$ единственным образом записывается в виде $z = \alpha z_0$, где $\alpha \in \mathbb{R}_{>0}$, $z_0 \in H$. Поэтому каждый смежный класс G/H можно однозначно записать в виде αH, $\alpha \in \mathbb{R}_{>0}$. Следовательно, $G/H \simeq \mathbb{R}_{>0}$.

Пример. Факторгруппа $\mathrm{GL}_n(\Bbbk)$ по подгруппе скалярных матриц (центру $\mathrm{GL}_n(\Bbbk)$) изоморфна проективной линейной группе $\mathrm{PGL}_n(\Bbbk)$, группе проективных преобразований проективного пространства $\mathbb{P}^{n-1}$.

Заметим, что если $H \subset G$ – нетривиальная нормальная подгруппа, то изучение G может быть "сведено" к изучению "меньших" групп H и G/H. Группа G называется *простой*, если любая ее нормальная подгруппа тривиальна (т. е. совпадает с G или с $\{1\}$). Примером простой группы является циклическая группа простого порядка. Однако, когда говорят о простых группах, обычно имеют в виду неабелевы простые группы.

2.4 Теорема о гомоморфизме групп

Определение. Отображение $\varphi : G \to G_1$ групп называется *гомоморфизмом* если

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in G.$$

Гомоморфизм $G \to G$ группы в себя называется *эндоморфизмом.*

Замечание. Пусть группа G порождается элементами $a_1, \ldots, a_n$. Если для двух гомоморфизмов $\varphi_1 : G \to G_1$ и $\varphi_2 : G \to G_1$ имеем $\varphi_1(a_i) = \varphi_2(a_i)$ для всех i, то $\varphi_1 = \varphi_2$.

Примеры. (1) Определитель $\det : \mathrm{GL}_n(\Bbbk) \to \Bbbk^*$ является гомоморфизмом групп.

(2) Знак подстановки $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ является гомоморфизмом групп.

(3) В абелевой аддитивной группе для любого $n \in \mathbb{Z}$ отображение $a \mapsto na$ является гомоморфизмом группы в себя.

(4) Экспонента $\exp : \mathbb{R} \to \mathbb{R}^*$, $a \mapsto e^a$ является гомоморфизмом групп.

(5) Взятие модуля $|\cdot| : \mathbb{C}^* \to \mathbb{R}_{>0}$, $z \mapsto |z|$ является гомоморфизмом групп.

(6) Пусть $H \lhd G$ и пусть G/H – факторгруппа. Отображение $\pi : G \to G/H$, $a \mapsto aH$ является гомоморфизмом групп.

Определение. Подмножество

$$\mathrm{Ker}(\varphi) := \{a \in G \mid \varphi(a) = 1\}$$

называется ядром гомоморфизма $\varphi : G \to G_1$.

Лемма. *Пусть $\varphi : G \to G_1$ – гомоморфизм групп. Тогда его ядро $\mathrm{Ker}(\varphi)$ является подгруппой в G, а его и образ $\mathrm{Im}(\varphi) = \varphi(G)$ – подгруппой в G_1.*

Доказательство. Проверим, например, первое:

$$a_1,\, a_2 \in \operatorname{Ker}(\varphi) \Longleftrightarrow \varphi(a_1) = \varphi(a_2) = 1 \Longrightarrow$$
$$\Longrightarrow \varphi(a_1 a_2^{-1}) = \varphi(a_1)\varphi(a_2)^{-1} = 1 \Longleftrightarrow a_1 a_2^{-1} \in \operatorname{Ker}(\varphi).$$

□

Замечание. Гомоморфизм $\varphi : G \to G_1$ является инъективным тогда и только тогда, когда $\operatorname{Ker}(\varphi) = \{1\}$.

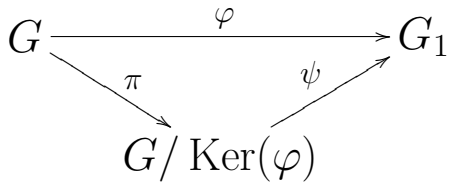
Теорема. *Пусть $\varphi : G \to G_1$ – гомоморфизм групп. Тогда*

(1) $\operatorname{Ker}(\varphi) \lhd G$.

(2) *Имеется естественный изоморфизм*

$$\psi : G/\operatorname{Ker}(\varphi) \to \varphi(G)$$

такой, что $\varphi = \psi \circ \pi$, где $\pi : G \to G/\operatorname{Ker}(\varphi)$ – естественный гомоморфизм в факторгруппу. В этом случае говорят, что диаграмма



коммутативна.

Доказательство. Положим $H := \mathrm{Ker}(\varphi)$. Для любого $b \in G$ имеем

$$a \in H \;\Rightarrow\; \varphi(a) = 0 \;\Rightarrow\; \varphi(bab^{-1}) = 0 \;\Rightarrow\; bab^{-1} \in H.$$

Следовательно, H – нормальная подгруппа.

Определим ψ следующим образом: $\psi(aH) = \varphi(a)$. Во-первых проверяем, что это определение корректно. Пусть $aH = a'H$. Тогда $a' = ah$ для некоторого $h \in H$. Отсюда

$$\psi(a'H) = \varphi(ah) = \varphi(a)\varphi(h) = \varphi(a) = \psi(aH).$$

Далее проверяем, что ψ – гомоморфизм:

$$\psi(aH \cdot bH) = \psi((ab)H) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aH)\psi(bH).$$

Далее

$$\psi(aH) = 1 \;\Leftrightarrow\; \varphi(a) = 1 \;\Leftrightarrow\; a \in H \;\Leftrightarrow\; aH = H.$$

Следовательно, ψ инъективно. Наконец, ψ сюръективно по построению. □

Примеры. (1) $\mathrm{S}_n \,/\, \mathrm{A}_n \simeq \{\pm 1\}$;

(2) $\mathrm{GL}_n(\Bbbk)/\,\mathrm{SL}_n(\Bbbk) \simeq \Bbbk^*$;

(3) $\mathbb{R}^*/\{\pm 1\} \simeq \mathbb{R}_{>0}$;

(4) $\mathbb{C}^*/\boldsymbol{\mu}_n \simeq \mathbb{C}^*$.

Предложение. $\mathrm{Int}(G) \simeq G/Z(G)$.

Доказательство. Отображение

$$\Psi : G \longrightarrow \mathrm{Int}(G), \qquad g \longmapsto \varphi_g$$

является сюръективным гомоморфизмом групп, причем $\mathrm{Ker}(\Psi) = Z(G)$ (проверьте самостоятельно!). □

Задача. Докажите, что подгруппа внутренних автоморфизмов $\mathrm{Int}(G)$ нормальна во всей группе автоморфизмов $\mathrm{Aut}(G)$.

Задача. Докажите, что группа автоморфизмов неабелевой группы не может быть циклической. Может ли она быть абелевой?

3 Прямые произведения групп

Определение. Пусть $G_1,\ldots, G_n$ – группы. Их (*внешним*) *прямым произведением* называется декартово произведение

$$G_1 \times \cdots \times G_n := \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

с покомпонентным умножением:

$$(g_1, \ldots, g_n)(g'_1, \ldots, g'_n) = (g_1 g'_1, \ldots, g_n g'_n).$$

В случае, когда в группах G_i операция аддитивна (сложение), вместо прямого произведения обычно используется понятие *прямой суммы*, которая обозначается $G_1 \oplus \cdots \oplus G_n$.

Определение. Пусть G – группа и пусть $G_1,\ldots, G_n$ – ее подгруппы. Говорят, что G является (*внутренним*) *прямым произведением* этих подгрупп, если любой элемент $g \in G$ однозначно представляется в виде

$$g = g_1 \cdots g_n, \qquad g_i \in G_i.$$

причем $g_i g_j = g_j g_i \quad \forall g_i \in G_i,\, g_j \in G_j$.

Предложение. (1) *Если группа G является внутренним прямым произведением своих подгрупп $G_1,\ldots, G_n$, то G изоморфна их внешнему прямому произведению: $G \simeq G_1 \times \cdots \times G_n$.*

(2) *Обратно, если* $G = G_1 \times \cdots \times G_n$ *– внешнее прямое произведение, то* G *содержит подгруппы* $H_i \subset G$, $i = 1, \ldots, n$ *такие, что* $H_i \simeq G_i$ *и* G *является внутренним прямым произведением подгрупп* $H_1, \ldots, H_n$.

Доказательство. (1) Определим отображение $\Psi : G_1 \times \cdots \times G_n \longrightarrow G$, $(g_1, \ldots, g_n) \longmapsto g_1 \cdots g_n$. По определению это отображение инъективно и сюръективно. Более того, оно является гомоморфизмом

$$\Psi((g_1, \ldots, g_n) \cdot (g_1', \ldots, g_n')) = \Psi(g_1 g_1', \ldots, g_n g_n') =$$
$$= g_1 g_1' \cdots g_n g_n' = g_1 \cdots g_n g_1' \cdots g_n' = \Psi(g_1, \ldots, g_n)\Psi(g_1', \ldots, g_n').$$

(2) Положим

$$H_i := \{(1, \ldots, 1, \underset{\substack{\uparrow \\ i}}{g_i}, 1, \ldots, 1) \mid g_i \in G_i\} \subset G.$$

Ясно, что $H_i \simeq G_i$. Более того, для любого $g \in G$ имеем $g = (g_1, \ldots, g_n)$, $g_i \in G_i$. Поэтому имеет место однозначное разложение в произведение элементов групп H_i:

$$g = (g_1, 1, \ldots, 1)(1, g_2, \ldots, 1) \cdots (1, \ldots, 1, g_n).$$

Очевидно также, что элементы из H_i и H_j коммутируют при $i \neq j$. □

Предложение. *Группа G является внутренним прямым произведением двух своих подгрупп G_1, G_2 тогда и только тогда, когда*

(1) $G_1 \lhd G$, $G_2 \lhd G$,

(2) $G_1 \cap G_2 = \{1\}$,

(3) $\langle G_1,\ G_2\rangle = G$.

Доказательство. Докажем достаточность условий (1)–(3). Пусть условия (1)–(3) выполнены. Для $g_1 \in G_1$, $g_2 \in G_2$ имеем

$$G_1 \ni g_1(g_2 g_1^{-1} g_2^{-1}) = g_1 g_2 g_1^{-1} g_2^{-1} = (g_1 g_2 g_1^{-1}) g_2^{-1} \in G_2.$$

Следовательно, $g_1 g_2 g_1^{-1} g_2^{-1} \in G_1 \cap G_2$, $\quad g_1 g_2 g_1^{-1} g_2^{-1} = 1$ и поэтому $g_1 g_2 = g_2 g_1$. Тогда в подгруппе $\langle G_1,\ G_2\rangle$ любое произведение можно упорядочить, т. е. привести к виду $g_1 g_2$, где $g_1 \in G_1$, $g_2 \in G_2$. Так как $\langle G_1,\ G_2\rangle = G$, то в таком виде записывается любой элемент $g \in G$. Наконец, если $g_1 g_2 = g_1' g_2'$ для $g_1, g_1' \in G_1$, $g_2, g_2' \in G_2$, то

$$G_1 \ni g_1'^{-1} g_1 = g_2' g_2^{-1} \in G_2.$$

Следовательно, $g_1'^{-1} g_1 = g_2' g_2^{-1} \in G_1 \cap G_2$, и поэтому $g_1 = g_1'$, $g_2 = g_2'$.

Необходимость условий (1)–(3) предлагается проверить самостоятельно. $\square$

Примеры. (1) $\mathbb{Q}^* = \mathbb{Q}_{>0} \times \{\pm 1\}$, $\mathbb{R}^* = \mathbb{R}_{>0} \times \{\pm 1\}$.

(2) Четверная группа Клейна имеет три различных разложения в нетривиальное прямое произведение: пусть H_1, H_2 и H_3 – циклические подгруппы порожденные подстановками $(1,2)(3,4)$, $(1,3)(2,4)$ и $(1,4)(2,3)$, соответственно. Тогда

$$\mathrm{V}_4 = H_1 \times H_2 = H_1 \times H_3 = H_2 \times H_3.$$

(3) $\mathbb{C}^* = \mathbb{R}_{>0} \times \{z \mid |z| = 1\}$.

(4) Пусть $\mathrm{GL}_n^+(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$ – подгруппа, состоящая из матриц с положительным определителем. Тогда $\mathrm{GL}_n^+(\mathbb{R}) = SL_n(\mathbb{R}) \times \{\lambda E \mid \lambda > 0\}$.

(5) Для нечетного n группа $\mathrm{O}_n(\mathbb{R})$ ортогональных $n \times n$-матриц является прямым произведением группы $\mathrm{SO}_n(\mathbb{R}) = \mathrm{O}_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R})$ ортогональных матриц с определителем 1 и группы $\{\pm 1\}$.

(6) Группа $\mathbb{Z}$ не является нетривиальной прямой суммой. Действительно, любые две нетривиальные подгруппы в $\mathbb{Z}$ пересекаются нетривиально.

Предложение. *Циклическая группа порядка n является прямым произведением своих подгрупп порядков n_1 и n_2 тогда и только тогда, когда $n = n_1 n_2$ и $(n_1, n_2) = 1$.*

Доказательство. Пусть a – порождающий элемент нашей группы G.

Достаточность. Пусть $n = n_1 n_2$ и $(n_1, , n_2) = 1$. Положим $G_1 := \langle a^{n_1} \rangle$ и $G_2 := \langle a^{n_2} \rangle$. Если $b \in G_1 \cap G_2$, то $b = a^{n_1 m_1} = a^{n_2 m_2}$ для некоторых m_1, $m_2 \in \mathbb{Z}$. Тогда $a^{n_1 m_1 - n_2 m_2} = 1$. Поэтому $n_1 m_1 - n_2 m_2 \equiv 0 \mod n$, $m_1 \equiv 0 \mod n_2$, $m_2 \equiv 0 \mod n_1$ и $b = 1$. Следовательно, $G_1 \cap G_2 = \{1\}$. По теореме о наибольшем общем делителе $n_1 u_1 + n_2 u_2 = 1$ для некоторых $u_i \in \mathbb{Z}$. Отсюда для любого $a^k \in G$ имеем $a^k = a^{n_1 u_1 k} a^{n_2 u_2 k} \in G_1 G_2$ и поэтому $G = G_1 \times G_2$. Наконец, $|G_i| = |a^{n_i}| = n/(n, n_i) = n/n_i$.

Необходимость. Пусть $G = G_1 \times G_2$, где $|G_i| = n_i$. Тогда $n_1 n_2 = |G_1 \times G_2| = |G| = n$. Так как G_i – циклические группы, то мы можем записать $G_i := \langle a_i \rangle$ для некоторых $a_i \in G$. Причем $|a_i| = n_i$ и $a = a_1^{k_1} a_2^{k_2}$ для некоторых $k_i \in \mathbb{Z}$. Предположим, что $(n_1, n_2) \neq 1$ и пусть p – простой делитель n_1 и n_2. Тогда

$$a^{n/p} = (a_1^{n_1})^{k_1 n_2/p} (a_2^{n_2})^{k_2 n_1/p} = 1.$$

Следовательно, $|a| < n$. Противоречие. □

Определение. Примарная циклическая группа – это циклическая группа порядка p^k, где p – простое число.

Следствие. *Любая конечная циклическая группа является прямым произведением примарных циклических групп. Примарная циклическая группа не разлагается в нетривиальное прямое произведение.*

Задача. Докажите, что группа всех движений куба является прямым произведением подгруппы собственных движений и $\{\pm E\}$.

3.1 Лемма о факторизации по сомножителям

Лемма. *Пусть* $G = G_1 \times \cdots \times G_n$ *и пусть* $H_i \lhd G_i$ *– нормальные подгруппы. Пусть*

$$H := H_1 \times \cdots \times H_n \subset G.$$

Тогда $H \lhd G$ *и*

$$G/H \simeq G_1/H_1 \times \cdots \times G_n/H_n.$$

Доказательство. Пусть $\pi_i : G_i \to G_i/H_i$ – канонические гомоморфизмы на факторгруппы и пусть

$$p_i : G \longrightarrow G_i, \quad (g_1, \ldots, g_n) \longmapsto (1, \ldots, g_i, \ldots, 1)$$

– проекция на i-ую компоненту. Рассмотрим композицию

$$\varphi_i : G \xrightarrow{p_i} G_i \xrightarrow{\pi_i} G_i/H_i$$

и отображение

$$\varphi : G \longrightarrow G_1/H_1 \times \cdots \times G_n/H_n, \quad \varphi(g) = (\varphi_1(g), \ldots, \varphi_n(g)).$$

Ясно, что φ является гомоморфизмом. Более того, он сюръективен поскольку элементы вида $(1, \ldots, g_i H_i, \ldots, 1) \quad \forall g_i \in G_i$ лежат в образе. Далее для $g = (g_1, \ldots, g_n) \in G$ имеем

$$\varphi(g) = 1 \Longleftrightarrow \varphi_i(g) = 1, \forall i \Longleftrightarrow g_i \in H_i, \forall i \Longleftrightarrow g \in H.$$

Таким образом,

$$\mathrm{Ker}(\varphi) = H.$$

Следовательно, $H \lhd G$ и $G/H \simeq G_1/H_1 \times \cdots \times G_n/H_n$ по теореме о гомоморфизме. $\square$

4 Полупрямые произведения групп

Определение (внутреннее определение)**.** Пусть G – группа и пусть G_1, $G_2 \subset G$ – ее подгруппы. Говорят, что G есть *полупрямое произведение* G_1 и G_2 (обозначается $G = G_1 \rtimes G_2$) если

(1) $G = G_1 \cdot G_2$,

(2) $G_1 \cap G_2 = \{1\}$,

(3) $G_1 \lhd G$.

Отметим, что, в отличие от прямого, определение полупрямого произведения не симметрично. Полупрямое произведение является прямым тогда и только тогда, когда выполнено также $G_2 \lhd G$.

Примеры. (1) Для группы диэдра имеем $\mathrm{D}_n = \langle r \rangle \rtimes \langle s \rangle$, где $\langle r \rangle$ – подгруппа поворотов, а $s \in \mathrm{D}_n$ – любая симметрия.

(2) $\mathrm{S}_n = \mathrm{A}_n \rtimes \langle (i, j) \rangle$.

(3) $\mathrm{Aff}_n(\Bbbk) = \mathrm{TranAff}_n(\Bbbk) \rtimes \mathrm{GL}_n(\Bbbk)$, где $\mathrm{GL}_n(\Bbbk)$ отождествляется с подгруппой аффинных преобразований с (фиксированной) неподвижной точкой.

(4) Для ортогональной группы нечетной размерности имеем $\mathrm{O}_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R}) \rtimes \langle -E \rangle$, где $\mathrm{SO}_n(\mathbb{R})$ – специальная орто-

гональная группа (группа ортогональных матриц с определителем 1).

Замечание. Пусть $G = G_1 \rtimes G_2$.

(1) Для любого элемента $g \in G$ имеет место единственное разложение $g = g_1 g_2$, $g_i \in G_i$. Действительно, если $g_1 g_2 = g_1' g_2'$, то

$$G_2 \ni g_2 g_2'^{-1} = g_1^{-1} g_1' \in G_1$$

Следовательно, $g_2 g_2'^{-1} = g_1^{-1} g_1' = 1$, $g_1 = g_1'$ и $g_2 = g_2'$. В частности, отсюда следует, что для конечных групп G_1 и G_2 порядок полупрямого произведения $G_1 \rtimes G_2$ равен произведению порядков G_1 и G_2.

(2) Умножение элементов $g_1 g_2$ и $g_1' g_2'$ может быть выполнено по правилу

$$(g_1 g_2) \cdot (g_1' g_2') = \big(g_1 (g_2 g_1' g_2^{-1})\big)(g_2 g_2') = \big(g_1 \varphi_{g_2}(g_1')\big)(g_2 g_2'),$$

где $\varphi_{g_2} : G_1 \to G_1$ – ограничение на подгруппу G_1 внутреннего автоморфизма

$$G \longrightarrow G, \qquad x \longmapsto g_2 x g_2^{-1}.$$

Это подводит нас к следующему определению.

Определение (внешнее определение)**.** Пусть даны две группы G_1 и G_2 и задан гомоморфизм $\phi : G_2 \to \mathrm{Aut}(G_1)$. Определим умножение на декартовом произведении G_1 и G_2 следующим образом:

$$(g_1,\, g_2) \cdot (g_1',\, g_2') = (g_1\phi(g_2)(g_1'),\, g_2 g_2').$$

Лемма. *Определенное выше умножение определяет группу.*

Доказательство. Проверим ассоциативность. Имеем

$$A := (g_1,\, g_2) \cdot ((g_1',\, g_2') \cdot (g_1'',\, g_2'')) =$$
$$= (g_1,\, g_2) \cdot (g_1'\phi(g_2')(g_1''),\, g_2' g_2'') = (g_1\phi(g_2)(g_1'\phi(g_2')(g_1'')),\, g_1 g_2' g_2'').$$

$$B := ((g_1,\, g_2) \cdot (g_1',\, g_2')) \cdot (g_1'',\, g_2'') =$$
$$= (g_1\phi(g_2)(g_1'),\, g_2 g_2') \cdot (g_1'',\, g_2'') = (g_1\phi(g_2)(g_1')\phi(g_2 g_2')(g_1''),\, g_1 g_2' g_2'').$$

Так как

$$g_1\phi(g_2)(g_1'\phi(g_2')(g_1'')) = g_1\phi(g_2)(g_1')\phi(g_2)(\phi(g_2')(g_1'')) =$$
$$= g_1\phi(g_2)(g_1')\phi(g_2 g_2')(g_1''),$$

то $A = B$. Единицей в $G_1 \rtimes G_2$ является $(1, 1)$:

$$(g_1,\, g_2) \cdot (1,\, 1) = (g_1\phi(g_2)(1),\, g_2) = (g_1,\, g_2),$$

$$(1,\, 1) \cdot (g_1,\, g_2) = (\phi(1)(g_1),\, g_2) = (g_1,\, g_2).$$

Для обратного элемента положим $(g_1,\, g_2)^{-1} = (\phi(g_2)^{-1}(g_1^{-1}),\, g_2^{-1})$. Действительно,

$$(g_1,\, g_2)\cdot(\phi(g_2)^{-1}(g_1^{-1}),\, g_2^{-1}) = (g_1\phi(g_2)(\phi(g_2)^{-1}(g_1^{-1})),\, g_2g_2^{-1}) = (1,1).$$

□

Замечание. Определенное выше внешнее полупрямое произведение является прямым тогда и только тогда, когда $\phi : G_2 \to \mathrm{Aut}(G_1)$ – тривиальный гомоморфизм, т.е. $\phi(G_2) = \{1\}$.

Предложение. (1) *Если группа G является внутренним полупрямым произведением своих подгрупп $G_1 \underset{внут}{\rtimes} G_2$, то G изоморфна их внешнему полупрямому произведению: $G \simeq G_1 \underset{внеш}{\rtimes} G_2$, где гомоморфизм $\phi : G_2 \to \mathrm{Aut}(G_1)$ – это отображение элемента $h \in G_2$ в гомоморфизм, индуцированный на нормальной подгруппе G_1 внутренним автоморфизмом*

$$\varphi_h : G \longrightarrow G, \quad x \longmapsto hxh^{-1}.$$

(2) *Обратно, если $G = G_1 \underset{внеш}{\rtimes} G_2$ – внешнее полупрямое произведение, то G содержит подгруппы H_1, $H_2 \subset G$ такие, что $H_i \simeq G_i$ и G является внутренним полупрямым произведением $H_1 \underset{внут}{\rtimes} H_2$.*

Доказательство. (1) Определим отображение

$$\Psi : G_1 \underset{\text{внеш}}{\rtimes} G_2 \longrightarrow G, \qquad (g_1,\, g_2) \longmapsto g_1 g_2.$$

Оно является гомоморфизмом:

$$\begin{aligned}\Psi((g_1, g_2) \cdot (g_1', g_2')) = \Psi((g_1\phi(g_2)(g_1'),\, g_2 g_2')) = g_1\phi(g_2)(g_1')g_2 g_2' = \\ = g_1(g_2 g_1' g_2^{-1})g_2 g_2' = g_1 g_2 g_1' g_2' = \Psi(g_1, g_2)\Psi(g_1', g_2'),\end{aligned}$$

а согласно замечанию Ψ инъективно и сюръективно.

(2) Положим

$$H_1 := \{(g_1,\, 1) \mid g_1 \in G_1\}, \qquad H_2 := \{(1,\, g_2) \mid g_2 \in G_2\} \subset G.$$

Ясно, что $H_i \simeq G_i$ и $H_1 \cap H_2 = \{(1,\, 1)\}$. Более того, для любого $g = (g_1,\, g_2) \in G$ имеет место однозначное разложение в произведение элементов групп H_i:

$$g = (g_1,\, 1)(1,\, g_2).$$

Наконец, для $(g_1',\, 1) \in H_1$ и $g = (g_1,\, g_2) \in G$ имеем

$$g(g_1',\, 1)g^{-1} = (g_1,\, 1)(1,\, g_2)(g_1',\, 1)(1,\, g_2)^{-1}(g_1,\, 1)^{-1} \in H_1.$$

□

Пример. Несложно проверить, что группа автоморфизмов циклической группы $\boldsymbol{\mu}_n$ абелева. Если $n = p$ – простое число,

то $|\operatorname{Aut}(\boldsymbol{\mu}_p)| = p-1$ (более того, из одного результата о конечных полях следует, что $\operatorname{Aut}(\boldsymbol{\mu}_p)$ – циклическая группа). Пусть теперь p и q – различные простые числа. Мы можем предположить, что $p > q$ и пусть $p \equiv 1 \mod q$. Тогда $\operatorname{Aut}(\boldsymbol{\mu}_p)$ содержит циклическую подгруппу порядка q и поэтому существует инъективный гомоморфизм $\phi : \boldsymbol{\mu}_q \to \operatorname{Aut}(\boldsymbol{\mu}_p)$. Следовательно, имеется нетривиальное полупрямое произведение $\boldsymbol{\mu}_p \rtimes \boldsymbol{\mu}_q$ – неабелева группа порядка pq.

5 Абелевы группы

Все абелевы группы будут рассматриваться с аддитивной операцией (операцией сложения). В аддитивной абелевой группе определено умножение на целые числа: для $a \in A$, $n \in \mathbb{Z}$ положим

$$na := \begin{cases} \underbrace{a + \cdots + a}_{n} & \text{если } n > 0, \\ 0 & \text{если } n = 0, \\ -na & \text{если } n < 0. \end{cases}$$

Эта операция удовлетворяет следующим свойствам:

(1) $(nm)a = n(ma) \quad \forall n,\, m \in \mathbb{Z} \quad \forall a \in A$;

(2) $(n+m)a = na + ma \quad \forall n,\, m \in \mathbb{Z} \quad \forall a \in A$;

(3) $n(a+b) = na + nb \quad \forall n \in \mathbb{Z} \quad \forall a,\, b \in A$;

(4) $1a = a \quad \forall a \in A$.

Заметим, что эти свойства совпадают с аксиомами в определении векторного пространства. (За исключением того, что $\mathbb{Z}$ не является полем и поэтому равенство $na = 0$ не влечет $a = 0$.) Таким образом, мы можем рассматривать целочисленные линейные комбинации элементов $a_1, \ldots, a_r \in A$

$$n_1 a_1 + \cdots + n_r a_r, \qquad n_i \in \mathbb{Z}.$$

Абелева группа A *порождается* элементами $a_1, \ldots, a_r \in A$, если любой элемент $a \in A$ представляется в виде целочисленной линейной комбинации элементов $a_1, \ldots, a_r$. В этом случае (т.е. если существует конечный набор порождающих) группа называется *конечно порожденной*.

5.1 Свободные абелевы группы.

Определение. Элементы $a_1, \ldots, a_r$ называются *линейно зависимыми*, если некоторая их нетривиальная целочисленная линейная комбинация равна нулю. Набор элементов $a_1, \ldots, a_r$ называется *базисом* абелевой группы A, если выполнены два условия

(1) $a_1, \ldots, a_r$ порождают A;

(2) $a_1, \ldots, a_r$ линейно независимы.

Абелева группа, обладающая базисом, называется *свободной абелевой группой*.

Замечание. Несложно видеть, что элементы $a_1, \ldots, a_r \in A$ образуют базис тогда и только тогда, когда любой элемент $a \in A$ *однозначно* представляется в виде целочисленной линейной комбинации

$$a = n_1 a_1 + \cdots + n_r a_r, \quad n_i \in \mathbb{Z}.$$

Примеры. (1) Обозначим $\mathbb{Z}^r := \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r}$. Эта группа обладает стандартным базисом

$$a_i := (0, 0, \ldots, \underset{\uparrow}{1}, \ldots, 0)$$
$$\scriptstyle i$$

и поэтому она свободна.

(2) Если в группе есть нетривиальный элемент конечного порядка, то она не является свободной.

(3) Группа $\mathbb{Q}^+$ не является свободной.

Замечание. Любая свободная конечно порожденная абелева группа F изоморфна $\mathbb{Z}^r$ для некоторого r. Действительно, если $a_1, \ldots, a_r$ – базис F, то отображение

$$\varphi : \mathbb{Z}^r \longrightarrow F, \quad (n_1, \ldots, n_r) \longmapsto \sum n_i a_i$$

является изоморфизмом.

Предложение. *Пусть F – свободная конечно порожденная абелева группа с базисом $e_1, \ldots, e_r$.*

(1) *Если элементы $b_1, \ldots, b_m \in F$ линейно независимы, то $m \leq r$.*

(2) *Любой базис F содержит r элементов.*

Доказательство. (2) следует из (1). Докажем (1). Пусть $F_{\mathbb{Q}}$ – векторное пространство над $\mathbb{Q}$ с тем же базисом $e_1, \ldots, e_r$. Определим отображение

$$\iota : F \longrightarrow F_{\mathbb{Q}}, \qquad \sum n_i e_i \longmapsto \sum n_i e_i \in F_{\mathbb{Q}}.$$

Ясно что это инъективный гомоморфизм абелевых групп. Поэтому если элементы $b_1, \ldots, b_m \in F$ линейно зависимы в F, то и их образы в $F_{\mathbb{Q}}$ также линейно зависимы. Наоборот, если $b_1, \ldots, b_m \in F$ и их образы в $F_{\mathbb{Q}}$ линейно зависимы, то домножая линейную комбинацию на знаменатели коэффициентов, получим, что и сами $b_1, \ldots, b_m$ линейно зависимы в F.

Теперь предположим, что в нашей ситуации $m > r$. Тогда мы получим противоречие с леммой о линейной зависимости для векторных пространств. □

Число элементов базиса свободной абелевой группы F называется ее *рангом* и обозначается $\operatorname{rk} F$.

Теорема. *Подгруппа свободной конечно порожденной абелевой группы свободна и конечно порождена.*

Доказательство. Пусть F – свободная конечно порожденная абелева группа и пусть E – любая подгруппа в F. Доказательство проведем индукцией по рангу группы F. Если $\operatorname{rk} F = 1$, то группа F – циклическая. Тогда любая ее подгруппа – также циклическая, что и доказывает утверждение в этом случае.

Предположим, что утверждение верно для групп F ранга $< r$ и докажем его для $\operatorname{rk} F = r$. Пусть $f_1, \ldots, f_r$ – базис F. Рассмотрим подгруппы $F' := \langle f_1 \rangle$ и $F'' := \langle f_2, \ldots, f_r \rangle$ – свободные конечно порожденные абелевы группы ранга 1 и $r-1$, соответственно. Любой элемент $x \in F$ однозначно представляется в виде $x = x' + x''$, где $x' \in F'$, $x'' \in F''$. Таким образом, $F = F' \oplus F''$. Рассмотрим проекцию

$$\pi : F \longrightarrow F'', \quad x = x' + x'' \longmapsto x'', \quad \text{где } x' \in F',\, x'' \in F''.$$

Ясно, что π – сюръективный гомоморфизм и $\operatorname{Ker}(\pi) = F'$. Поэтому множество $E'' = \pi(E)$ является подгруппой в F''. Положим $E' := F' \cap E = \operatorname{Ker}(\pi) \cap E$. По теореме о гомоморфизме $E'' \simeq E/E'$. Ясно, что E' – циклическая группа (поскольку это подгруппа циклической группы $F' = \langle f_1 \rangle$). Пусть $e_0 \in E'$ – порождающий элемент.

По предположению индукции E'' – свободная конечно порожденная абелева группа. Пусть $e_1'', \ldots, e_m''$ – базис E'' и пусть $e_1, \ldots, e_m \in E$ – элементы такие, что $\pi(e_i) = e_i''$. Мы можем считать, что $E' \neq \{0\}$ (иначе $E \simeq E''$).

Мы утверждаем, что $e_0, e_1, \ldots, e_m$ – базис E. Действительно, пусть $x \in E$. Запишем

$$\pi(x) = x_1 e_1'' + \cdots + x_m e_m''$$

для некоторых $x_i \in \mathbb{Z}$. Положим

$$y := x_1 e_1 + \cdots + x_m e_m \in E.$$

Тогда $\pi(x-y)=0 \Longrightarrow x-y \in \mathrm{Ker}(\pi) \Longrightarrow x-y \in E' \Longrightarrow$ $x-y=x_0e_0$ для некоторого $x_0 \in \mathbb{Z}$. Отсюда

$$x = x_0e_0 + y = x_0e_0 + x_1e_1 + \cdots + x_me_m.$$

Предположим, что элементы $e_0, \ldots, e_m$ линейно зависимы, т. е.

$$0 = x_0e_0 + x_1e_1 + \cdots + x_me_m$$

для $x_i \in \mathbb{Z}$. Тогда

$$0 = \pi(0) = \pi(x_0e_0 + \cdots + x_me_m) = x_1e_1'' + \cdots + x_me_m''.$$

С другой стороны, $e_1, \ldots, e_m$ – базис E''. Следовательно, $x_i = 0$ $\forall i = 1, \ldots, m$. Отсюда $x_0e_0 = 0$ и $x_0 = 0$ поскольку $e_0 \neq 0$ (и F – свободная абелева группа). $\square$

5.2 Универсальное свойство свободных абелевых групп.

Лемма. *Пусть A – конечно порожденная абелева группа и пусть $a_1, \ldots, a_r$ – некоторое множество ее порождающих. Тогда существует свободная абелева группа F ранга r с базисом $f_1, \ldots, f_r$ и сюръективный гомоморфизм $\varphi : F \to A$ такой, что*

$$\varphi(f_i) = a_i \qquad \forall i.$$

Доказательство. Положим

$$\varphi\left(\sum n_i f_i\right) = \sum n_i a_i.$$

Это отображение корректно определено, поскольку любой элемент $f \in F$ однозначно записывается в виде $f = \sum n_i f_i$. Свойство гомоморфизма легко проверяется. Так как $a_1, \ldots, a_r$ порождают A, то φ сюръективен. □

Следствие. *Любая конечно порожденная абелева группа A с r образующими изоморфна факторгруппе F/E свободной абелевой группы F ранга r по подгруппе $E \subset F$ (которая также является свободной абелевой группой).*

5.3 Целочисленные матрицы и элементарные преобразования

Пусть M – некоторая матрица и пусть $M_1, \ldots, M_r$ – набор ее столбцов. *Целочисленным элементарным преобразованием* столбцов называется одно из следующих:

(1) прибавление к столбцу M_i другого столбца M_j, $j \neq i$, умноженного на целое число λ: $M_i' = M_i + \lambda M_j$;

(2) умножение столбца M_i на ± 1: $M_i' = \pm M_i$.

Аналогично определяются целочисленные элементарные преобразования строк.

Целочисленная элементарная матрица – это матрица, полученная из единичной при помощи одного целочисленного элементарного преобразования.

Замечание. Перестановка столбцов может быть представлена как композиция целочисленных элементарных преобразований.

Замечание. Целочисленные элементарные преобразования обратимы, т. е. если от матрицы M к матрице M' можно прийти при помощи цепочки целочисленных элементарных преобразований, то и от M' к матрице M можно прийти при помощи некоторой цепочки целочисленных элементарных преобразований.

Теорема. *Любая (необязательно квадратная) целочисленная матрица M целочисленными элементарными преобразованиями строк и столбцов может быть приведена к диагональному виду (т.е. к виду $M' = (m'_{i,j})$ с $m'_{i,j} = 0$ при $i \neq j$).*

Доказательство. Проведем доказательство индукцией по суммарному размеру матрицы. База индукции очевидна.

Для целочисленной матрицы $L = (\lambda_{i,j})$ положим

$$\delta(L) := \min\{\lambda_{i,j} \mid \lambda_{i,j} > 0\}.$$

Пусть $\mathcal{S}$ – множество всех матриц, которые можно получить из M целочисленными элементарными преобразованиями

строк и столбцов и пусть

$$\delta := \min\{\delta(N) \mid N \in \mathcal{S}\}.$$

Этот минимум достигается для некоторой матрицы N:

$$\exists N = (\lambda_{i,j}), \quad \delta = \delta(N) = \lambda_{i_0,j_0}.$$

Переставляя строки и столбцы матрицы N, можно добиться того, что $(i_0, j_0) = (1, 1)$, т. е. $\delta = \lambda_{1,1}$. В частности, $\lambda_{1,1} \neq 0$. Обозначим i-ую строку матрицы N через N_i. Предположим, что $\lambda_{i,1} \neq 0$. Разделим $\lambda_{i,1}$ на $\lambda_{1,1}$ с остатком:

$$\lambda_{i,1} = \lambda_{1,1} q_i + s_i, \quad q_i,\, s_i \in \mathbb{Z}, \quad 0 \leq s_i < \lambda_{1,1}$$

и сделаем целочисленное элементарное преобразование $N_i' = N_i - q_i N_1$. В новой матрице $N' = (\lambda_{i,j}')$ имеем $\lambda_{1,1}' = \lambda_{1,1}$ и

$$0 \leq \lambda_{i,1}' = \lambda_{i,1} - \lambda_{1,1} q_i = s_i < \lambda_{1,1} = \delta.$$

По нашему предположению $\lambda_{i,1}' = 0$. Применяя аналогичные преобразования для всех $i > 1$ мы добьемся того, что $\lambda_{i,1}' = 0$ $\forall i > 1$. Аналогично, поступаем со столбцами и добьемся того, что $\lambda_{1,j}' = 0 \quad \forall j > 1$. Таким образом, новая матрица N' имеет вид

$$N' = \begin{pmatrix} \lambda_{1,1} & 0 & \cdots & 0 \\ 0 & \lambda_{2,2}' & \cdots & \lambda_{2,m}' \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \lambda_{n,2}' & \cdots & \lambda_{n,m}' \end{pmatrix}$$

По предположению индукции матрица

$$K' = \begin{pmatrix} \lambda'_{2,2} & \cdots & \lambda'_{2,m} \\ \cdots\cdots & \cdots & \cdots\cdots \\ \lambda'_{n,2} & \cdots & \lambda'_{n,m} \end{pmatrix}$$

может быть приведена к диагональному виду целочисленными элементарными преобразованиями. Это доказывает утверждение. □

Следствие. *Любая квадратная целочисленная матрица с определителем* ± 1 *является произведением элементарных целочисленных.*

Лемма. *Пусть* F *– свободная абелева группа и пусть* $f_1, \ldots, f_r$ *– ее базис. Пусть* $M = (\lambda_{i,j})$ *– целочисленная* $r \times r$*-матрица. Положим*

$$\begin{aligned} f'_1 &= \lambda_{1,1} f_1 + \cdots + \lambda_{r,1} f_r, \\ f'_2 &= \lambda_{1,2} f_1 + \cdots + \lambda_{r,2} f_r, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ f'_r &= \lambda_{1,r} f_1 + \cdots + \lambda_{r,r} f_r. \end{aligned}$$

т. е. $(f'_1, \ldots, f'_r) = (f_1, \ldots, f_r) \cdot M$*. Тогда элементы* $f'_1, \ldots, f'_r$ *образуют базис* F *если и только если* $|M| = \pm 1$*.*

Доказательство. Докажем достаточность условия. Пусть $|M| = \pm 1$. Тогда обратная матрица $M^{-1} = (\mu_{i,j})$ – также цело-

численная и мы имеем $(f_1, \ldots, f_r) = (f'_1, \ldots, f'_r) \cdot M^{-1}$, т. е.

$$(*) \qquad \begin{array}{rcl} f_1 & = & \mu_{1,1} f'_1 + \cdots + \mu_{r,1} f'_r, \\ f_2 & = & \mu_{1,2} f'_1 + \cdots + \mu_{r,2} f'_r, \\ \ldots & \ldots & \ldots \\ f_r & = & \mu_{1,r} f'_1 + \cdots + \mu_{r,r} f'_r. \end{array}$$

Поэтому элементы $f'_1, \ldots, f'_r$ порождают F. Если эти элементы линейно зависимы, то они также линейно зависимы в $F_{\mathbb{Q}}$. Это противоречит лемме о линейной зависимости для векторных пространств.

Для доказательства необходимости предположим, что $f'_1, \ldots, f'_r$ – базис F. Тогда элементы $f_1, \ldots, f_r$ можно выразить через $f'_1, \ldots, f'_r$ в виде (*). Целочисленная матрица $M' := (\mu_{i,j})$ будет обратной к M. □

5.4 Теорема о согласованных базисах

Теорема. *Пусть F – свободная абелева группа и пусть $E \subset F$ – ее подгруппа. Тогда существуют базисы $f_1, \ldots, f_r \in F$ и $e_1, \ldots, e_m \in E$ такие, что $e_i = \mu_i f_i$, $i = 1, \ldots, m$, $\mu_i \in \mathbb{Z}$.*

Доказательство. Выберем любые базисы

$$a_1, \ldots, a_r \in F, \qquad b_1, \ldots, b_m \in E$$

и выразим b_i через a_j:

$$b_i = \sum_{j=1}^{m} \lambda_{j,i} a_j, \quad \lambda_{j,i} \in \mathbb{Z}, \quad i = 1, \ldots, r.$$

Рассмотрим матрицу $M = (\lambda_{j,i})$. Таким образом,

$$(b_1, \ldots, b_m) = (a_1, \ldots, a_r) \cdot M.$$

Согласно теореме о целочисленных элементарных преобразованиях существуют целочисленные квадратные матрицы T и S такие, что $|S| = \pm 1$, $|T| = \pm 1$ и

$$M' := TMS = \begin{pmatrix} \mu_1 & 0 & 0 & \cdots & 0 \\ 0 & \mu_2 & 0 & \cdots & 0 \\ 0 & 0 & \mu_3 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

Выберем новые базисы следующим образом

$$(f_1, \ldots, f_r) = (a_1, \ldots, a_r) \cdot T^{-1}, \quad (e_1, \ldots, e_m) = (b_1, \ldots, b_m) \cdot S.$$

Тогда

$$(f_1, \ldots, f_r) \cdot M' = (a_1, \ldots, a_r) \cdot T^{-1}TMS = \\ = (b_1, \ldots, b_m) \cdot S = (e_1, \ldots, e_m).$$

Это доказывает утверждение. □

Теорема. *Любая конечно порожденная абелева группа A является прямой суммой бесконечных циклических и примарных циклических подгрупп. Число этих подгрупп и их порядки определяются группой A однозначно.*

Замечание. Теорема перестает быть верной, если отказаться от условия конечной порождённости группы. Например, группа $\mathbb{Q}^+$ не может быть разложена в нетривиальную прямую сумму.

Доказательство существования разложения. Согласно универсальному свойству свободных абелевых групп $A \simeq F/E$, где F – свободная абелева группа, а $E \subset F$ – ее подгруппа. По теореме о согласованных базисах существуют базисы $f_1, \ldots, f_r \in F$ и $e_1, \ldots, e_m \in E$ такие, что $e_i = \mu_i f_i$, $i = 1, \ldots, m$. Положим $F_i := \langle f_i \rangle$ и $E_i := \langle e_i \rangle$ при $i = 1, \ldots, m$ и $E_i := \{0\}$ при $i = m, \ldots, r$. Напомним лемму о факторизации по сомножителям (в аддитивной форме).

Лемма. *Пусть $F_1, \ldots, F_n$ – абелевы группы, пусть $F = F_1 \oplus \cdots \oplus F_n$ и пусть $E_i \subset F_i$ – подгруппы. Положим*

$$E := E_1 \oplus \cdots \oplus E_n \subset F.$$

Тогда

$$F/E \simeq F_1/E_1 \oplus \cdots \oplus F_n/E_n.$$

В нашей ситуации все группы F_i/E_i – циклические. Далее каждая конечная циклическая группа может быть разложена в прямую сумму примарных циклических. $\square$

Лемма. *В абелевой группе A множество всех элементов конечного порядка образует подгруппу* $\mathrm{Tor}(A)$. *Факторгруппа* $A/\mathrm{Tor}(A)$ *не имеет нетривиальных элементов конечного порядка.*

Доказательство. Если a, $b \in \mathrm{Tor}(A)$, то существуют n, $m \in \mathbb{Z} \setminus \{0\}$ такие, что $na = 0$ и $mb = 0$. Тогда $nm(a - b) = 0$, т. е. $a - b \in \mathrm{Tor}(A)$. Следовательно, $\mathrm{Tor}(A)$ – подгруппа. Обозначим через $\pi : A \to A/\mathrm{Tor}(A)$ канонический гомоморфизм. Предположим, что $\pi(a)$ – элемент конечного порядка. Тогда $\pi(na) = n\pi(a) = 0$ для некоторого $n \in \mathbb{Z} \setminus \{0\}$. Следовательно, $na \in \mathrm{Ker}(\pi) = \mathrm{Tor}(A)$. Поэтому существует $m \in \mathbb{Z} \setminus \{0\}$ такое, что $mna = 0$, т. е. $a \in \mathrm{Tor}(A) = \mathrm{Ker}(\pi)$ и тогда $\pi(a) = 0$. □

Пример. Если $\Bbbk$ – поле, то $\mathrm{Tor}(\Bbbk^*)$ – подгруппа всех корней из 1. Подгруппа $\mathrm{Tor}(\Bbbk^+)$ нетривиальна тогда и только тогда, когда $\mathrm{char}(\Bbbk) \neq 0$ и в этом случае $\mathrm{Tor}(\Bbbk^+) = \Bbbk^+$.

Аналогично доказывается следующее утверждение.

Лемма. *Пусть A – абелева группа и пусть p – простое число. Положим*

$$\mathrm{Tor}_{(p)}(A) := \{a \in A \mid \exists k \in \mathbb{N} \quad p^k a = 0\}$$

Тогда $\mathrm{Tor}_{(p)}(A)$ *– подгруппа и факторгруппа* $A/\mathrm{Tor}_{(p)}(A)$ *не имеет нетривиальных элементов порядка* p^k.

Определение. Подгруппа $\mathrm{Tor}(A)$ называется *периодической частью* абелевой группы (или ее *подгруппой кручения*). Подгруппа $\mathrm{Tor}_{(p)}(A)$ называется *p-примарной частью* абелевой группы.

Доказательство единственности разложения. Пусть

$$A = \bigoplus_i A_i$$

– разложение конечно порожденной абелевой группы в прямую сумму бесконечных циклических и примарных циклических групп. Перепишем наше разложение в виде

$$A = \Big(\bigoplus_{p,i} A_{p,i}\Big) \oplus \Big(\bigoplus_i A_{\infty,i}\Big),$$

где $A_{p,i}$ – p-примарные циклические группы (p – простое), а $A_{\infty,i}$ – бесконечные циклические группы. Ясно, что $\oplus_{p,i} A_{p,i}$ – конечная группа, содержащаяся в $\mathrm{Tor}(A)$. С другой стороны, любой элемент $A \setminus \oplus_{p,i} A_{p,i}$ имеет бесконечный порядок. Таким образом, подгруппа $\oplus_{p,i} A_{p,i} = \mathrm{Tor}(A)$ определена однозначно. Поэтому определена однозначно и свободная подгруппа подгруппа $\oplus_i A_{\infty,i} \simeq A/\mathrm{Tor}(A)$, а также количество слагаемых в $\oplus_i A_{\infty,i}$, равное ее рангу.

Далее, рассмотрим подгруппы $\oplus_i A_{p,i} \subset \mathrm{Tor}_{(p)}(A)$. Как и выше, так как порядок любого элемента $A \setminus \oplus_i A_{p,i}$ или бесконечен

или делится на простое $p' \neq p$, то $\oplus_i A_{p,i} = \mathrm{Tor}_{(p)}(A)$. Следовательно, подгруппы $\oplus_i A_{p,i}$ также определены однозначно. Таким образом, остается доказать, следующую лемму.

Лемма. *Пусть B – абелева группа порядка p^k. Тогда в любом разложении $B = B_1 \oplus \cdots \oplus B_n$ в прямую сумму циклических подгрупп число этих подгрупп и их порядки не зависят от выбора разложения.*

Доказательство. Проведем доказательство индукцией по k. База индукции очевидна. Предположим, что лемма верна для всех групп B порядка $p^{k'}$, $k' < k$.

Рассмотрим отображение $\varphi : B \to B$, $b \mapsto pb$. Ясно, что это гомоморфизм и его ядро состоит из элементов p-кручения (элементов порядка p и 1). Обозначим $K := \mathrm{Ker}(\varphi)$ и $K_i := K \cap B_i$. Тогда каждая K_i – циклическая группа порядка p. Мы утверждаем, что $K = K_1 \oplus \cdots \oplus K_n$. Действительно, для любого $x \in K \subset B$ существует единственное разложение

$$x = x_1 + \cdots x_n,$$

где $x_i \in B_i$. Так как

$$0 = px = px_1 + \cdots + px_n$$

и последнее разложение также единственно, то $px_i = 0$ для всех i, т. е. $x_i \in K_i$. По лемме о факторизации по слагаемым

$$B/K \simeq B_1/K_1 \oplus \cdots \oplus B_n/K_n,$$

где все группы B_i/K_i – циклические (возможно, тривиальные) группы порядков $|B_i/K_i| = |B_i|/p$. По предположению индукции числа $|B_i|/p$ определены однозначно. Следовательно, определены однозначно и числа B_i. □

□

Следствие. *Конечно порожденная абелева группа A является свободной тогда и только тогда, когда ее подгруппа кручения тривиальна.*

Следствие. *Если порядок конечной абелевой группы A делится на m, то в A имеется подгруппа порядка m.*

Доказательство. Пусть $|A| = n$ и пусть p_0 – простой делитель n. Достаточно доказать, что в A имеется подгруппа индекса p_0 (далее можно продолжить индукцией по индексу подгруппы). Разложим A в сумму примарных циклических подгрупп

$$A = \bigoplus_{p,i} A_{p,i}$$

и заменим одно из слагаемых A_{p_0,i_0} на

$$A'_{p_0,i_0} = p_0 A_{p_0,i_0} := \{p_0 a \mid a \in A_{p_0,i_0}\}.$$

В остальных случаях положим $A'_{p,i} = A_{p,i}$. Тогда

$$A' := \bigoplus_{p,i} A'_{p,i}$$

– нужная нам подгруппа. □

Заметим, что это утверждение не верно для неабелевых групп. (Приведите пример!)

Определение. *Показателем* (или *экспонентой*) конечной абелевой группы A наименьшее общее кратное порядков всех ее элементов. Показатель мы будем обозначать через $\exp(A)$.

Пусть конечная абелева группа разложена в прямую сумму примарных циклических групп $A = \bigoplus_{p,i} A_{p,i}$, пусть $n_{p,i} = p^{k_{p,i}}$ – порядки этих групп. По основной теореме этого параграфа набор чисел $n_{p,i}$ определяется группой A однозначно. Эти числа называются *элементарными делителями* группы.

Предложение. *Экспонента конечной абелевой группы A равна наименьшему общему кратному её элементарных делителей. В группе A существует элемент порядка* $\exp(A)$.

Доказательство. Положим $n = \text{НОК}\ \{n_{p,i}\}$, где $n_{p,i}$ – элементарные делители группы. Тогда порядок любого элемента A делит n. Следовательно, и $\exp(A)$ делит n. Поэтому предложение непосредственно следует из следующей леммы. □

Лемма. *В группе A существует элемент порядка n.*

Доказательство. Пусть $A_{p,i} = \langle a_{p,i} \rangle$. Упорядочим группы $A_{p,i}$ так, что для каждого p числа $n_{p,i}$ не возрастают. Таким образом, $n_{p,1} = p^{k_p}$ – максимальное среди всех $n_{p,i} = p^{k_{p,i}}$ для фиксированного p. Пусть $A_{p,1} = \langle a_p \rangle$. Положим $:= \prod_p a_p$. Тогда $n = \prod_p p^{k_p}$ и

$$|a| = \text{НОК}\,\{|a_i|\} = \text{НОК}\,\{p^{k_p}\} = n$$

поскольку в абелевой группе порядок суммы элементов взаимно простых порядков равен произведению их порядков. □

Лемма. *Пусть в абелевой группе A порядки элементов a и b взаимно просты. Тогда порядок их суммы равен произведению порядков:* $|a + b| = |a||b|$.

Доказательство. Положим $|a| = \alpha$, $|b| = \beta$ и $|a+b| = \gamma$. Ясно, что $\alpha\beta(a + b) = 0$. Поэтому γ делит $\alpha\beta$. Так как $(\alpha,\, \beta) = 1$, то $\alpha u + \beta v = 1$ для некоторых $\alpha,\, \beta \in \mathbb{Z}$. Отсюда

$$a = (\alpha u + \beta v)a = \beta v a = \beta v(a + b),$$

$$b = (\alpha u + \beta v)b = \alpha u a = \alpha u(a + b).$$

Следовательно, элементы a и b принадлежат циклической подгруппе, порожденной $a+b$, и по теореме Лагранжа α и β делят γ. □

Следствие. *Конечная абелева группа A является циклической тогда и только тогда, когда* $\exp(A) = |A|$.

6 Дискретные подгруппы в $\mathbb{R}^n$

Определение. Подгруппа $A \subset \mathbb{R}^n$ называется *дискретной* если существует такая окрестность $U \ni 0$ начала координат, что $U \cap A = \{0\}$.

Лемма. *Пусть $A \subset \mathbb{R}^n$ – дискретная подгруппа. Тогда существует $\delta > 0$ такое, что для любых различных $a, b \in A$ мы имеем $\|a - b\| \geq \delta$.*

Доказательство. Возьмем окрестность $U \ni 0$ такую, что $U \cap A = \{0\}$. Она содержит шар U_δ с центром в 0 некоторого радиуса $\delta > 0$. Тогда если $\|a - b\| < \delta$, то $0 \neq a - b \in U_\delta \cap A$. Противоречие. □

Лемма. *Если $A \subset \mathbb{R}^n$ – дискретная подгруппа и $K \subset \mathbb{R}^n$ – компактное множество, то пересечение $K \cap A$ конечно.*

Доказательство. Пусть δ – такое как в предыдущей лемме. Для каждого $x \in K$ пусть U_x – открытый шар радиуса $< \delta/2$ с центром в x. Эти шары покрывают K. Из этого покрытия можно выбрать конечное подпокрытие U_{v_i}, т.е. $K = \cup_i U_{x_i}$. По конструкции каждый шар U_{x_i} содержит не более одного элемента A. □

Теорема. *Дискретная подгруппа в $\mathbb{R}^n$ свободна (и конечно порождена).*

Доказательство. Поскольку $\mathbb{R}^n$ не имеет кручения, то достаточно доказать, что группа A конечно порождена. Пусть $e_1, \ldots, e_m \in A$ – максимальная линейно независимая над $\mathbb{R}$ система. Положим

$$K := \left\{ \sum \alpha_i e_i \mid 0 \leq \alpha_i \leq 1 \right\}.$$

Поскольку множество K замкнуто и ограничено, то оно компактно. Следовательно, пересечение $K \cap A$ конечно. Тогда группа A порождается элементами $e_1, \ldots, e_m$ и конечным множеством $K \cap A$. Действительно, любой элемент $a \in A$ можно записать в виде

$$a = \sum \beta_i e_i, \quad \beta_i \in \mathbb{R}.$$

Тогда

$$a = \sum [\beta_i] e_i + \sum \{\beta_i\} e_i, \quad \sum \{\beta_i\} e_i \in K \cap A.$$

□

Пример. Подгруппа $\mathbb{Q}^n \subset \mathbb{R}^n$ не является дискретной.

Теорема. *Пусть $A \subset \mathbb{R}^n$ – дискретная подгруппа и пусть $e_1, \ldots, e_m$ – ее базис. Тогда $e_1, \ldots, e_m$ линейно независимы над $\mathbb{R}$.*

Доказательство. Предположим, что

$$e_1 = \sum_{i=2}^{m} \alpha_i e_i, \quad \alpha_i \in \mathbb{R}.$$

Рассмотрим множество

$$K := \left\{ \sum \beta_2 e_2 + \cdots + \beta_m e_m \mid 0 \leq \beta_i \leq 1 \right\}.$$

Оно компактно и поэтому пересечение $K \cap A$ конечно. Далее для любого $t \in \mathbb{Z}$

$$te_1 = \sum_{i=2}^{m} [t\alpha_i] e_i + \sum_{i=2}^{m} \{t\alpha_i\} e_i$$

Вторая сумма содержится в $K \cap A$. Поэтому для некоторых $t_1 \neq t_2$ эти вторые суммы совпадут. Тогда

$$t_1 e_1 - t_2 e_1 = \sum_{i=2}^{m} ([t_1\alpha_i] - [t_2\alpha_i]) e_i \in \langle e_2, \ldots, e_m \rangle.$$

Противоречие. □

Пример. Подгруппа $A \subset \mathbb{R}$, порожденная 1 и $\sqrt{2}$ не является дискретной поскольку ее базис линейно зависим над $\mathbb{R}$.

7 Коммутант

Определение. *Коммутатором* элементов a, $b \in G$ называется

$$[a, b] := aba^{-1}b^{-1}.$$

Коммутантом группы G называется множество всевозможных произведений всех коммутаторов. Коммутант обозначается через $[G, G]$ или, более кратко, через G'.

Лемма. *Коммутант группы является подгруппой.*

Доказательство. Если a, $b \in G$, то $[a, b]^{-1} = [b, a] \in G'$. □

Пример. Группа G абелева $\Longleftrightarrow G' = \{1\}$.

Теорема. (1) *Пусть $\varphi : G \to G_1$ – гомоморфизм групп. Тогда $\varphi(G') = \varphi(G)'$.*

(2) *Коммутант переходит в себя при всех автоморфизмах группы: $\varphi(G') = G' \quad \forall \varphi \in \mathrm{Aut}(G)$.*

(3) *$G' \lhd G$.*

(4) *Факторгруппа G/G' абелева.*

(5) *Для некоторой нормальной подгруппы N факторгруппа G/N абелева тогда и только тогда, когда $N \supset G'$.*

Процесс факторизации по коммутанту называется *абелианизацией* группы.

Доказательство. (1) Заметим, что $\varphi([a,b]) = [\varphi(a), \varphi(b)]$. Поэтому

$$\varphi([a_1,b_1]\cdots[a_n,b_n]) = [\varphi(a_1),\varphi(b_1)]\cdots[\varphi(a_n),\varphi(b_n)] \in \varphi(G)'.$$

Следовательно, $\varphi(G') \subset \varphi(G)'$. Обратно, если $c \in \varphi(G)'$, то c имеет вид

$$c = [\varphi(a_1),\varphi(b_1)]\cdots[\varphi(a_n),\varphi(b_n)] = \varphi([a_1,b_1]\cdots[a_n,b_n]) \in \varphi(G').$$

(2) следует из (1), а (3) следует из (2). Утверждение (4) является частным случаем (5). Докажем (5). Пусть $\pi : G \to G/N$ – естественный гомоморфизм. Тогда согласно (1) имеем $\pi(G') = (G/N)'$. Поэтому G/N – абелева $\iff \pi(G') = \{1\} \iff G' \subset N$. □

Задача. Пусть G – группа и пусть $H \subset G$ – ее подгруппа. Докажите, что если $H \supset G'$, то $H \lhd G$.

Пример. Вычислим коммутант группы диэдра D_n. Напомним, что $\mathrm{D}_n = \langle r,\, s\rangle$, где r – поворот на угол $2\pi/n$, а s – симметрия относительно оси, проходящей через центр и одну из вершин. Имеются соотношения $r^n = s^2 = 1$ и $srs^{-1} = r^{-1}$. Таким образом, $[r,s] = r^{-2} \in \mathrm{D}_n'$ и поэтому $\langle r^2\rangle \subset \mathrm{D}_n'$. С другой стороны, $\langle r^2\rangle \lhd \mathrm{D}_n$ и факторгруппа $\mathrm{D}_n/\langle r^2\rangle$ имеет порядок ≤ 4 и потому

абелева. Следовательно, $\langle r^2 \rangle \supset \mathrm{D}'_n$ и по теореме $\langle r^2 \rangle = \mathrm{D}'_n$. Если n нечетно, то $\mathrm{D}'_n = \langle r^2 \rangle = \langle r \rangle$ – подгруппа индекса 2, а если n четно, то $\mathrm{D}'_n = \langle r^2 \rangle \neq \langle r \rangle$ – подгруппа индекса 4.

Задача. Вычислите коммутант группы A_4.

8 Разрешимые группы

По индукции определим n-й коммутант группы G правилом $G^{(n+1)} = (G^{(n)})'$. Таким образом, имеется последовательность вложенных подгрупп:

$$G \supset G' \supset G'' \supset \cdots \supset G^{(n)} \supset \cdots .$$

Группа называется *разрешимой*, если $G^{(n)} = \{1\}$ для некоторого n. Абелева группа всегда разрешима поскольку для нее $G' = \{1\}$.

Замечание. Подгруппа H разрешимой группы H всегда разрешима так как $H^{(n)} \subset G^{(n)}$.

Теорема. *Пусть G – группа и пусть $N \lhd G$. Тогда группа G разрешима $\Longleftrightarrow$ разрешимы группы N и G/N.*

Доказательство. Рассмотрим естественный гомоморфизм $\pi : G \to G/N$. Имеем $\pi(G') = (G/N)'$. По индукции доказываем, что $\pi(G^{(n)}) = (G/N)^{(n)}$.

Пусть G разрешима. Тогда

$$(G/N)^{(n)} = \pi(G^{(n)}) = \{1\}$$

для некоторого n. Поэтому разрешимы N и G/N (см. замечание).

Обратно, предположим, что N и G/N разрешимы. Тогда существует n такое, что

$$\pi(G^{(n)}) = (G/N)^{(n)} = \{1\}.$$

Следовательно, $G^{(n)} \subset N$. Так как N разрешима, то существует m такое, что

$$G^{(n+m)} = (G^{(n)})^{(m)} \subset N^{(m)} = \{1\}.$$

□

Задача. Докажите, что группы D_n и S_4 разрешимы.

Теорема. *Группа $T_n(\Bbbk)$ невырожденных верхнетреугольных $n \times n$-матриц над полем $\Bbbk$ разрешима.*

Доказательство. Индукция по n. База индукции $n = 1$ очевидна поскольку $T_1(\Bbbk) \simeq \Bbbk^*$. Рассмотрим отображение $\varphi : T_n(\Bbbk) \longrightarrow T_{n-1}(\Bbbk)$,

$$\varphi : \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n-1} & a_{1,n} \\ 0 & a_{2,2} & \cdots & a_{2,n-1} & a_{2,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & a_{n,n} \end{pmatrix} \longmapsto \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n-1} \\ 0 & a_{2,2} & \cdots & a_{2,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a_{n-1,n-1} \end{pmatrix}$$

(вычеркивание последней строки и последнего столбца). Ясно, что φ – сюръективный гомоморфизм. По предположению

индукции группа $T_{n-1}(\Bbbk)$ разрешима. Докажем разрешимость группы

$$K_n = \mathrm{Ker}(\varphi) = \left\{ \begin{pmatrix} 1 & 0 & 0 & \cdots & b_1 \\ 0 & 1 & 0 & \cdots & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & b_n \end{pmatrix} \quad \middle| \quad b_1, \ldots, b_n \in \Bbbk \right\}$$

Рассмотрим сюръективный гомоморфизм

$$\psi : K_n \to \Bbbk^* \qquad \begin{pmatrix} 1 & 0 & 0 & \cdots & b_1 \\ 0 & 1 & 0 & \cdots & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & b_n \end{pmatrix} \longmapsto b_n$$

Так как образ и ядро

$$\mathrm{Ker}(\psi) = \left\{ \begin{pmatrix} 1 & 0 & 0 & \cdots & b_1 \\ 0 & 1 & 0 & \cdots & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \quad \middle| \quad b_1, \ldots, b_{n-1} \in \Bbbk \right\}$$

гомоморфизма ψ являются абелевыми группами, то и группа K_n разрешима. □

Теорема. *При $n \geq 5$ знакопеременная группа A_n не является разрешимой. Более того, $\mathrm{A}'_n = \mathrm{A}_n$.*

Доказательство. Пусть $i,\ j,\ k,\ l,\ m \in \{1, \ldots, n\}$ – попарно различные числа. Рассмотрим тройные циклы $\sigma := (i, j, k)$ и $\tau := (k, l, m)$. Тогда

$$\mathrm{A}'_5 \ni [\sigma, \tau] = (i, j, k)(k, l, m)(i, k, j)(k, m, l) = (i, l, k).$$

Отсюда видно, что A'_5 содержит все тройные циклы. Теперь утверждение легко выводится из следующей леммы. □

Лемма. *Знакопеременная группа* A_n *порождается тройными циклами.*

Доказательство. Поскольку симметрическая группа порождается транспозициями, то любой элемент $\sigma \in \mathrm{A}_n$ представляется в виде произведения четного числа транспозиций. Поэтому достаточно доказать, что произведение пары различных транспозиций $\tau_1 = (i, j)$ и $\tau_2 = (k, l)$ равно произведению некоторых тройных циклов. Если все элементы $i,\ j,\ k,\ l$ попарно различны, то $\tau_1\tau_2 = (i, j, k)(j, k, l)$. Если же, например, $j = l$, а $i \neq j \neq k \neq i$, то

$$\tau_1\tau_2 = (i, j)(k, j) = (i, j, k).$$

Это доказывает лемму. □

Задача. Вычислите коммутант группы S_n.

Теорема. *Если поле* $\Bbbk$ *содержит более трех элементов, то специальная линейная группа* $\mathrm{SL}_n(\Bbbk)$ *не является разрешимой. Более того,* $\mathrm{SL}_n(\Bbbk)' = \mathrm{SL}_n(\Bbbk)$.

Замечание. На самом деле, можно доказать более сильное утверждение: если $\mathrm{SL}_n(\Bbbk)' \neq \mathrm{SL}_n(\Bbbk)$, то $n = 2$ и поле $\Bbbk$ содержит ≤ 3 элементов.

Доказательство. Проведем вычисление для $n = 2$. Для рассмотрения общего случая нужно лишь дополнить наши матрицы многоточиями. Имеем

$$\left[\begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix}, \begin{pmatrix}1 & \mu\\ 0 & 1\end{pmatrix}\right] = \begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix}\begin{pmatrix}1 & \mu\\ 0 & 1\end{pmatrix}\begin{pmatrix}\lambda^{-1} & 0\\ 0 & \lambda\end{pmatrix}\begin{pmatrix}1 & \mu\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \eta\\ 0 & 1\end{pmatrix}$$

где $\eta := \mu(\lambda^2 - 1)$. Если $\lambda \neq \pm 1$, то элемент η может принимать любые значения. Аналогичное вычисление проводится для нижне-треугольных матриц. Следовательно, $\mathrm{SL}_n(\Bbbk)'$ содержит все элементарные матрицы типа I. Теперь утверждение легко выводится из следующей леммы. □

Лемма. *Группа* $\mathrm{SL}_n(\Bbbk)$ *порождается элементарными матрицами типа I.*

Доказательство. Утверждение эквивалентно тому, что любую матрицу $A = (a_{i,j})$ с определителем 1 можно элементарными преобразованиями типа I привести к единичной. Пусть $A_1, \ldots,$

A_n – строки матрицы. Если $a_{2,1} = 0$, то преобразованием вида $A'_2 = A_2 + A_i$ для некоторого i мы добъёмся того, что $a'_{2,1} \neq 0$. Далее преобразованием вида $A'_1 = A_1 + \lambda A_2$ добъёмся того, что $a'_{1,1} = 1$. Наконец, преобразованиями вида $A'_i = A_i + \lambda A_1$, $i > 1$ обнуляем первый столбец: $a'_{i,1} = 0$, $i > 1$. Продолжая по индукции, приводим матрицу A к унитреугольному виду:

$$A' = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Как и в стандартном алгоритме Гаусса эта матрица приводится к улучшенному ступенчатому виду, который будет единичной матрицей. □

Задача. Вычислите коммутанты групп $\mathrm{SL}_2(\mathbb{Z}_2)$ и $\mathrm{SL}_2(\mathbb{Z}_3)$.

9 Действия групп

Определение. Пусть G – группа и Ω – непустое множество. Говорят, что группа G *действует* на множестве Ω (обозначается $G : \Omega$), если задано отображение

$$G \times \Omega \longrightarrow \Omega, \quad (g, x) \longmapsto g * x$$

такое, что выполняются следующие два свойства:

(1) $(g_1 g_2) * x = g_1 * (g_2 * x) \quad \forall g_1,\, g_2 \in G \quad \forall x \in \Omega$

(2) $1 * x = x \quad \forall x \in \Omega.$

Замечание. Для действия $G : \Omega$ и элемента $g \in G$ определим отображение

$$\sigma_g : \Omega \longrightarrow \Omega, \quad x \longmapsto g * x.$$

По определению $\forall g_1,\, g_2 \in G$, $\forall x \in \Omega$ имеем

$$(\sigma_{g_1} \circ \sigma_{g_2})(x) = \sigma_{g_1}(\sigma_{g_2}(x)) = g_1 * (g_2 * x) = (g_1 g_2) * x = \sigma_{g_1 g_2}(x)$$

и σ_1 – тождественное отображение. Таким образом, $\sigma_{g_1} \circ \sigma_{g_2} = \sigma_{g_1 g_2}$. В частности, $\sigma_{g^{-1}}$ – обратное отображение к σ_g. Следовательно, σ_g – биекция. Более того, отображение

$$\Psi : G \longrightarrow \mathrm{S}_\Omega, \quad g \longmapsto \sigma_g$$

является гомоморфизмом в группу подстановок множества Ω.

Обратно, любой гомоморфизмом $\Psi : G \to \mathrm{S}_\Omega$ определяет действие $G : \Omega$ по правилу $g * x = \Psi(g)(x)$. (Проверьте!).

Ядром эффективности действия $G : \Omega$ называется подгруппа

$$\{g \in G \mid g * x = x \quad \forall x \in \Omega\}$$

Ясно, что ядро эффективности совпадает с ядром гомоморфизма Ψ (выше). Действие называется *эффективным*, если его ядро эффективности тривиально.

Определение. Пусть $G : \Omega$ – действие группы G. *Орбитой* элемента $x \in \Omega$ называется следующее множество в Ω

$$\mathrm{Orb}(x) := \{g * x \mid g \in G\}.$$

Подмножество в G

$$\mathrm{St}(x) := \{g \in G \mid g * x = x\}$$

называется *стационарной подгруппой* или *стабилизатором* элемента x. Несложно проверить, что это действительно подгруппа.

Таким образом, ядро эффективности – пересечение стационарных подгрупп всех элементов Ω. Действие называется *транзитивным*, если множество Ω совпадает с орбитой некоторого своего элемента: $\Omega = \mathrm{Orb}(x)$.

Предложение. *Пусть $G : \Omega$ – действие группы G.*

(1) *Если $y \in \mathrm{Orb}(x)$, то $\mathrm{Orb}(y) = \mathrm{Orb}(x)$.*

(2) *Если* $\mathrm{Orb}(x) \cap \mathrm{Orb}(y) \neq \emptyset$, *то* $\mathrm{Orb}(x) = \mathrm{Orb}(y)$.

(3) *Множество* Ω *представляется в виде непересекающегося объединения орбит:* $\Omega = \cup_{x \in \Omega} \mathrm{Orb}(x)$.

Доказательство. (1) $y \in \mathrm{Orb}(x) \Longleftrightarrow \exists g_0 \in G \quad y = g_0 * x \Longrightarrow \forall g \in G \quad g * y = (gg_0) * x \in \mathrm{Orb}(x)$. Следовательно, $\mathrm{Orb}(y) \subset \mathrm{Orb}(x)$. Аналогично, $\forall g \in G \quad g * x = (gg_0^{-1}) * x \in \mathrm{Orb}(y)$ и поэтому имеет место обратное включение.

(2) Пусть $z \in \mathrm{Orb}(x) \cap \mathrm{Orb}(y)$. Тогда, согласно (1), имеем $\mathrm{Orb}(x) = \mathrm{Orb}(z) = \mathrm{Orb}(y)$.

Утверждение (3) следует из (2) поскольку $x \in \mathrm{Orb}(x)$. $\square$

Примеры. (1) Для любой группы G и для любого множества Ω имеется тривиальное действие $g * x = x \quad \forall g \in G \quad \forall x \in \Omega$.

(2) По определению группа подстановок S_n действует на множестве $\Omega = \{1, \ldots, n\}$. Это действие транзитивно. Стабилизатор элемента – группа подстановок S_{n-1} элементов $1, \ldots, \hat{k}, \ldots, n$.

(3) Полная линейная группа $\mathrm{GL}_n(\Bbbk)$ действует на векторном пространстве $V = \Bbbk^n$. При этом имеется две орбиты – $V \setminus \{0\}$ и $\{0\}$.

(4) Группа $\mathrm{SO}_3(\mathbb{R})$ транзитивно действует на двумерной сфере $S^2 = \{x \in \mathbb{R}^3 \mid \|x\| = 1\}$.

(5) Группа $U := \{z \in \mathbb{C} \mid |z| = 1\}$ умножениями действует на комплексной плоскости $\mathbb{C}$. Орбиты действия – множества комплексных чисел с фиксированным модулем.

(6) Группа $\mathrm{SL}_2(\mathbb{R})$ действует на пополненной комплексной плоскости $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ по правилу

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * z = \frac{az+b}{cz+d}.$$

(7) С каждым действием $G : \Omega$ связаны несколько других действий.

- Действие на множестве всех подмножеств $G : 2^\Omega$, где для $X \subset \Omega$ полагаем $g * X := \{g * x \mid x \in X\}$.
- Действие на декартовом произведении $G : \Omega \times \cdots \times \Omega$ по правилу $g * (x_1, \ldots, x_n) := (g * x_1, \ldots, g * x_n)$.
- Пусть $G : \Omega$ – действие группы G и пусть $H \subset G$ – подгруппа. Тогда имеется естественное действие $H : \Omega$ – *ограничение* действия $G : \Omega$.

Определение. Пусть $G : \Omega$ – действие группы G. Подмножество $\Omega' \subset \Omega$ называется *инвариантным*, если $g * x \in \Omega'$ для всех $g \in G$ и для всех $x \in \Omega'$. Инвариантное подмножество является объединением (некоторых) орбит. Для $x \in \Omega'$ формула $g * x$ задает действие на Ω', которое называется *действием на инвариантном подмножестве*.

Каждая группа имеет несколько естественных действий на себе:

Пример. Пусть G – группа и пусть $H \subset G$ – ее подгруппа (возможно $G = H$). Тогда имеется действие $H : G$ *левыми сдвигами* или *левое регулярное* действие:

$$h * g = hg \quad \forall h \in H,\ \forall g \in G.$$

Орбиты этого действия – правые смежные классы, а стабилизатор любого элемента тривиален. Аналогично определяется действие H на G *правыми сдвигами*:

$$h * g = gh^{-1} \quad \forall h \in H,\ \forall g \in G.$$

Пример. Для любой группы G имеется действие $G : G$ на себе сопряжениями:

$$g * x = gxg^{-1}.$$

Орбитами действия являются классы сопряженных элементов. Стабилизатор элемента $x \in G$ в этом случае называется *централизатором* и обозначается $Z(x)$. Он состоит из всех элементов G, коммутирующих с x:

$$Z(x) := \mathrm{St}(x) = \{g \in G \mid gx = xg\}.$$

Рассмотрим, например, действие группы S_4 на себе сопряжениями и ее действие на инвариантном подмножестве

$$\Omega = \{(12)(34),\ (13)(24),\ (14)(23)\} = \mathrm{V}_4 \setminus \{(1)\}.$$

Последнее действие индуцирует гомоморфизм $\mathrm{S}_4 \to \mathrm{S}_\Omega \simeq \mathrm{S}_3$, ядром которого является V_4. Следовательно, $\mathrm{S}_4 / \mathrm{V}_4 \simeq \mathrm{S}_3$.

Пример. Любая группа G действует на множестве Ω своих подгрупп сопряжениями:

$$g * H = gHg^{-1}.$$

При этом стабилизатор элемента $H \in \Omega$ имеет вид

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}$$

он обозначается $N_G(H)$ (или просто $N(H)$) и называется *нормализатором* H. Нормализотор – максимальная подгруппа G, в которой H нормальна. В частности, $N_G(H) = G \iff H \lhd G$. Ясно также, что $N(H) \supset H$.

Пример. Пусть G – группа и пусть $H \subset G$ – ее подгруппа. Имеется действие группы G (сдвигами) на множестве левых смежных классов:

$$G : G/H, \qquad g * aH = (ga)H.$$

Это действие транзитивно, а для стабилизатора имеем $\mathrm{St}(aH) = aHa^{-1}$.

Теорема (Теорема Кэли)**.** * *Пусть G – конечная группа порядка n. Тогда G является подгруппой группы подстановок S_n.*

*Arthur Cayley – английский математик (1821 – 1895)

Доказательство. Занумеруем элементы группы: $G := \{g_1, \ldots, g_n\}$ и рассмотрим действие $G : G$ левыми сдвигами. Так как стабилизатор любого элемента тривиален, то гомоморфизм $G \to \mathrm{S}_n$, индуцированный действием, инъективен. □

Предложение. *Пусть $G : \Omega$ – действие группы G и пусть $x \in \Omega$. Существует естественная биекция между множеством левых смежных классов $G/\operatorname{St}(x)$ и орбитой элемента x:*

$$\phi : G/\operatorname{St}(x) \longrightarrow \operatorname{Orb}(x), \quad g\operatorname{St}(x) \longmapsto g * x.$$

Доказательство. Проверим корректность определения ϕ. Пусть $g\operatorname{St}(x) = g'\operatorname{St}(x)$. Тогда существует $h \in \operatorname{St}(x)$ такой, что $g' = gh$. По определению стабилизатора $h * x = x$. Отсюда

$$\phi(g'\operatorname{St}(x)) = (gh) * x = g * (h * x) = g * x = \phi(g\operatorname{St}(x)).$$

Отображение сюръективно по определению орбиты. Проверим его инъективность. Пусть $\phi(g'\operatorname{St}(x)) = \phi(g\operatorname{St}(x))$. Тогда имеем последовательно $g * x = g' * x$, $(g^{-1}g') * x = x$, $g^{-1}g' \in \operatorname{St}(x)$ и $g\operatorname{St}(x) = g'\operatorname{St}(x)$. □

Замечание. Построенная биекция ϕ является *изоморфизмом действий* $G : \Omega$ и $G : G/\operatorname{St}(x)$. Это означает, что

$$\phi(h * x) = h * \phi(x) \qquad \forall h \in G.$$

Следствие.

$$|\operatorname{Orb}(x)| = [G : \operatorname{St}(x)].$$

Следствие. *Предположим, что группа G конечна. Тогда*

$$|G| = |\operatorname{St}(x)| \cdot |\operatorname{Orb}(x)|.$$

Рассмотрим еще несколько примеров.

Пример. Группа диэдра D_n естественным образом действует на вершинах правильного n-угольника. Занумеровав эти вершины, получим гомоморфизм $\mathrm{D}_n \to \mathrm{S}_n$. Поскольку любое движение однозначно определяется образами вершин n-угольника, то этот гомоморфизм инъективен. Следовательно, имеется вложение $\mathrm{D}_n \hookrightarrow \mathrm{S}_n$. Для $n = 3$ из совпадения порядков групп получим изоморфизм $\mathrm{D}_3 \simeq \mathrm{S}_3$.

Пример. Группа тетраэдра T действует на вершинах этого тетраэдра. Как и выше, получаем инъективный гомоморфизм $T \hookrightarrow \mathrm{S}_4$. Из совпадения порядков получим изоморфизм $T \simeq \mathrm{S}_4$.

Пример. Рассмотрим группу собственных движений куба O. Она действует на больших диагоналях куба. Это задает инъективный гомоморфизм $O \hookrightarrow \mathrm{S}_4$. Из совпадения порядков получим изоморфизм $O \simeq \mathrm{S}_4$. С другой стороны, рассматривая действие на множестве трех прямых, соединяющих центры противоположных граней, мы получим сюръективный гомоморфизм $O \simeq \mathrm{S}_4 \to \mathrm{S}_3$.

Задача. Найдите порядок группы движений икосаэдра.

Пример. Проективная линейная группа $\mathrm{PGL}_n(\Bbbk)$ естественным образом действует на проективном пространстве $\mathbb{P}^{n-1}$. Пусть теперь $\Bbbk = \mathbb{F}_q$ – конечное поле, содержащее q элементов и пусть $n = 2$. Тогда $|\mathrm{GL}_2(\Bbbk)| = (q^2-1)(q^2-q)$, а $|\mathrm{PGL}_2(\Bbbk)| = (q^2-1)q$. Так как в этом случае проективная прямая содержит $q+1$ элемент, то это действие индуцирует вложение $\mathrm{PGL}_2(\Bbbk) \hookrightarrow \mathrm{S}_{q+1}$. Отсюда немедленно получаем $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathrm{S}_3$ и $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathrm{S}_4$.

Задача. Докажите, что $\mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathrm{A}_5$.

Задача. Пусть p – наименьший простой делитель порядка группы G. Предположим, что в G имеется подгруппа H индекса p. Докажите, что $H \lhd G$. *Указание.* Рассмотрите действие $H : G/H$.

9.1 p-группы.

Определение. p-группой называется группа порядка p^k, где p – простое.

Теорема. *Центр p-группы нетривиален.*

Доказательство. Рассмотрим действие $G : G$ сопряжениями:

$$g * x = gxg^{-1}.$$

Тогда одноэлементные орбиты – это в точности элементы центра группы. Поэтому имеем разложение в непересекающееся объединение

$$G = Z(G) \cup \left(\bigcup_{|\operatorname{Orb}(x)|>1} \operatorname{Orb}(x) \right).$$

Так как число элементов орбиты делит порядок группы, то $|\operatorname{Orb}(x)| = p^l$, $l \geq 0$ для всех $x \in G$. Таким образом, получаем

$$p^k = |G| = |Z(G)| + \sum_{|\operatorname{Orb}(x)|>1} |\operatorname{Orb}(x)| = |Z(G)| + \sum p^{l_i},$$

где $l_i > 0$. Следовательно, $|Z(G)|$ делится на p. □

Следствие. *Любая (конечная) p-группа разрешима.*

Доказательство. Индукция по порядку группы. □

Следствие. *Группа порядка p^2 является абелевой.*

Доказательство. Если $|G| = p^2$, то согласно теореме, $|Z(G)| = p^2$ или p. Второй случай невозможен по следующей лемме. □

Лемма. *Для неабелевой группы G факторгруппа $G/Z(G)$ не может быть циклической.*

Доказательство. Пусть $\pi : G \to G/Z(G)$ – естественный гомоморфизм. Предположим, что $G/Z(G)$ – циклическая и порождается элементом $\bar{a}$. Выберем любой элемент $a \in G$ такой, что $\pi(a) = \bar{a}$. Тогда любой элемент $g \in G$ представляется в виде $g = a^k z$, где $z \in Z(G)$. Ясно, что такие элементы коммутируют между собой. $\square$

Следующий пример показывает, что группа порядка p^3 необязательно абелева.

Пример. Группа верхних унитреугольных 3×3-матриц

$$\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \middle| \quad a,\, b,\, c \in \mathbb{Z}_p \right\} \subset \mathrm{GL}_3(\mathbb{Z}_p)$$

имеет порядок p^3 и не является абелевой.

10 Теоремы Силова

Теорема (первая теорема Силова)**.** * *Пусть G – конечная группа порядка $n = p^k m$, где p – простое. Тогда в G существует подгруппа порядка p^k.*

Доказательство. Докажем теорему индукцией по n. База индукции очевидна. Предположим, что теорема верна для всех групп порядков $n' < n$. Рассмотрим действие $G : G$ сопряжениями:

$$g * x = gxg^{-1}.$$

Тогда

$$\mathrm{St}(x) = Z(x) := \{g \in G \mid gx = xg\}$$

– централизатор x. Орбиты этого действия – классы сопряженных элементов, а одноэлементные орбиты – это в точности элементы центра группы. Таким образом, имеем следующее разложение G в непересекающееся объединение:

$$G = Z(G) \cup \left(\bigcup_{|\mathrm{Orb}(x)|>1} \mathrm{Orb}(x) \right).$$

Имеются две возможности:

*Ludwig Sylow – норвежский математик (1832–1918).

(1) Существует элемент $x \in G \setminus Z(G)$ такой, что $p \nmid |\operatorname{Orb}(x)|$. Так как

$$n = |Z(x)| \cdot |\operatorname{Orb}(x)|,$$

то $p^k \mid |Z(x)|$ и $|Z(x)| < n$. По предположению индукции в $Z(x)$ существует подгруппа порядка p^k.

(2) Для всех $x \in G \setminus Z(G)$ имеем $p \mid |\operatorname{Orb}(x)|$. Тогда $p \mid |Z(G)|$ и по основной теореме об абелевых группах в $Z(G)$ существует элемент z порядка p. Подгруппа $\langle z \rangle$ нормальна в G. Пусть $G_1 := G/\langle z \rangle$ и пусть $\pi : G \to G_1$ – естественный гомоморфизм. Тогда $|G_1| = p^{k-1}m$ и по предположению индукции в G_1 существует подгруппа P_1 порядка p^{k-1}. Положим $P := \pi^{-1}(P_1)$. Тогда $P \subset G$ – подгруппа (проверьте!) Так как $P \supset \langle z \rangle$, то $P/\langle z \rangle \simeq P_1$ и поэтому $|P| = p^k$.

□

Определение. Пусть G – конечная группа порядка $n = p^k m$, где p – простое и m не делится на p. Подгруппа $G_p \subset G$ порядка p^k называется *силовской p-подгруппой*. Множество всех силовских p-подгрупп мы обозначим через $\operatorname{Syl}_p(G)$.

Примеры. (1) Пусть $G = \mathrm{S}_p$ – симметрическая группа (p – простое). Тогда любая силовская p-подгруппа – циклическая и порождается циклом длины p.

(2) Пусть $\Bbbk = \mathbb{Z}_p$ – поле из p элементов и пусть $G = \mathrm{GL}_2(\Bbbk)$ – полная линейная группа. Ее порядок равен $(p^2-1)(p^2-p)$. Следовательно подгруппа верхних унитреугольных матриц

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad \middle| \quad a \in \mathbb{Z}_p \right\}$$

является силовской.

Теорема (вторая теорема Силова)**.** *Пусть G – конечная группа.*

(1) *Любая p-подгруппа $H \subset G$ содержится в некоторой силовской.*

(2) *Все силовские подгруппы сопряжены.*

Доказательство. Пусть $G_p \in \mathrm{Syl}_p(G)$. Рассмотрим действие группы G сдвигами на множестве левых смежных классов G/G_p и его ограничение на подгруппу H. Пусть

$$G/G_p = \bigcup_{xG_p \in G/G_p} \mathrm{Orb}(xG_p)$$

– разложение множества G/G_p в непересекающееся объединение орбит действия $H : G/G_p$. Число элементов любой орбиты делит порядок группы H и поэтому имеет вид p^k, $k \geq 0$. С другой стороны, число элементов множества G/G_p не делится на

p. Следовательно, существует орбита $\mathrm{Orb}(yG_p)$, состоящая из одного элемента. Это означает, что для всех $h \in H$ мы имеем $hyG_p = yG_p$, т. е. существует элемент $g \in G_p$ (зависящий от h) такой, что $hy = yg$. Иначе говоря,

$$\forall h \in H \qquad y^{-1}hy \in G_p.$$

Последнее эквивалентно тому, что $y^{-1}Hy \subset G_p$. Отсюда

$$(*) \qquad H \subset yG_py^{-1},$$

что доказывает (1).

Пусть $G_p^o \in \mathrm{Syl}_p(G)$ – другая силовская подгруппа. Полагая $H = G_p^o$ в $(^*)$ получим утверждение (2). □

Следствие. *Число силовских p-подгрупп равно индексу нормализатора одной из них:* $|\mathrm{Syl}_p(G)| = [G : N(G_p)]$.

Следствие. *Силовская p-подгруппа нормальна тогда и только тогда, когда она единственна.*

Теорема (третья теорема Силова)**.** $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$.

Доказательство. Положим $\Omega := \mathrm{Syl}_p(G)$. Рассмотрим действие $G : \Omega$ сопряжениями. По второй теореме Силова это действие транзитивно. Зафиксируем теперь силовскую подгруппу $G_p \in \mathrm{Syl}_p(G)$ и рассмотрим ограничение действия $G : \Omega$ на подгруппу G_p. Это действие необязательно транзитивно. Пусть

$\Omega = \cup\Omega_i$ – разложение в непересекающееся объединение орбит. Имеем $|\Omega_i| = p^{k_i}$, $k_i \geq 0$ и $\sum p^{k_i} = |\Omega|$. Орбита $\mathrm{Orb}(G_p) = \{G_p\}$ состоит из одного элемента. Предположим, что существует другая одноэлементная орбита $\Omega_i = \{G'_p\}$, $G'_p \in \mathrm{Syl}_p(G)$, $G_p \neq G'_p$. Тогда $gG'_pg^{-1} = G'_p \quad \forall g \in G_p$. Таким образом, $G_p \subset N(G'_p)$. Если $G_p \neq G'_p$, то группа $N(G'_p)$ содержит две различные силовские подгруппы. Это противоречит следствию выше (поскольку G_p – нормальная силовская подгруппа в $N(G_p)$). Следовательно, существует единственная одноэлементная орбита $\mathrm{Orb}(G_p) = \{G_p\}$. Отсюда $|\Omega| \equiv 1 \mod p$. □

10.1 Применения теорем Силова

Теорема. *Группа порядка pq, где p и q – простые числа, разрешима.*

Доказательство. Мы можем считать, что $p > q$. Пусть $|G| = pq$ и пусть $G_p \in \mathrm{Syl}_p(G)$. Достаточно доказать, что $G_p \lhd G$ (и тогда разрешимость G будет следовать из цикличности G_p и G/G_p). Имеем

$$|\mathrm{Syl}_p(G)| = [G : N(G_p)].$$

Так как $G \supset N(G_p) \supset G_p$, то по теореме Лагранжа $|N(G_P) = p$ или pq. Если G_p не является нормальной, то $|\mathrm{Syl}_p(G)| = q$. С другой стороны, $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$ по третьей теореме Силова. Противоречие. □

Замечание. Если в условиях предыдущей теоремы $p > q$ и $p \not\equiv 1 \mod q$, то и $G_q \lhd G$. Следовательно, $G = G_p \times G_q$ и поэтому G – циклическая. Если же $p \equiv 1 \mod q$, то $G = G_p \rtimes G_q$. Постройте пример такого полупрямого произведения.

Задача. Пусть p и q – простые числа. Докажите, что группы порядков p^2q и p^3q разрешимы.

11 Простые группы

Напомним, что группа называется простой, если она не содержит нетривиальных нормальных подгрупп.

Замечание. Простая неабелева группа G не может быть разрешимой, поскольку для нее $G' = G$.

Задача. Пусть G – конечная группа такая, что ее силовская 2-подгруппа – циклическая. Докажите, что G не может быть простой. *Указание.* Используйте теорему Кэли и нормальность A_n в S_n.

Мы рассмотрим две серии простых групп: знакопеременные группы и специальные проективные линейные группы.

Теорема. *При $n \geq 5$ группа A_n проста.*

Напомним, что при $n \leq 3$ группы A_n являются циклическими, а A_4 содержит нормальную подгруппу V_4 (четверную группу Клейна).

Лемма. *Пусть $\sigma \in \mathrm{S}_n$ и пусть*

$$\sigma = \sigma_1 \cdots \sigma_r = (i_1^1, i_2^1, \ldots, i_{m_1}^1) \cdots (i_1^r, i_2^r, \ldots, i_{m_r}^r)$$

– разложение в произведение независимых циклов. Тогда для $\tau \in \mathrm{S}_n$ разложение подстановки $\tau \circ \sigma \circ \tau^{-1}$ в произведение независимых циклов имеет вид

$$\tau \circ \sigma \circ \tau^{-1} = \Big(\tau(i_1^1), \tau(i_2^1), \ldots, \tau(i_{m_1}^1)\Big) \cdots \Big(\tau(i_1^r), \tau(i_2^r), \ldots, \tau(i_{m_r}^r)\Big).$$

Доказательство. Имеем

$$\tau \circ \sigma \circ \tau^{-1} \left(\tau(i_k^l)\right) = \tau \circ \sigma(i_k^l) = \tau(i_{k+1}^l)$$

где нижний индекс у i_k^l мы рассматриваем по модулю m_l. Это и доказывает равенство. □

Следствие. *Классы сопряженных элементов в* S_n *– это в точности элементы, имеющие одинаковое циклическое строение.*

Пример. Имеются следующие классы сопряженных элементов в S_5.

- четные: $\{(1)\}$, $\{(i,j)(k,l)\}$, $\{(i,j,k)\}$, $\{(i,j,k,l,m)\}$,
- нечетные: $\{(i,j)\}$, $\{(i,j,k,l)\}$, $\{(i,j,k)(l,m)\}$,

где все i, j, k, l, m – различные числа из $\{1,\ldots,5\}$.

Простое доказательство теоремы для случая $n = 5$. Найдем классы сопряженных элементов в A_5. Для этого перечислим четные классы сопряженных элементов в S_5 (тривиальный класс мы не рассматриваем):

σ	$\lvert \mathrm{Orb}_{\mathrm{S}_5}(\sigma)\rvert$	$\lvert Z_{\mathrm{S}_5}(\sigma)\rvert$	$Z_{\mathrm{S}_5}(\sigma)$	$Z_{\mathrm{A}_5}(\sigma)$	$\lvert \mathrm{Orb}_{\mathrm{A}_5}(\sigma)\rvert$
(i,j,k)	20	6	$\langle\sigma,\,(l,m)\rangle$	$\langle\sigma\rangle$	20
$(i,j)(k,l)$	15	8	$\langle \mathrm{V}_4,\,(i,k,j,l)\rangle$	V_4	15
(i,j,k,l,m)	24	5	$\langle\sigma\rangle$	$\langle\sigma\rangle$	12

Таким образом, четные классы сопряженных элементов S_5 вида $\{(1)\}$, $\{(i,j,k)\}$, $\{(i,j)(k,l)\}$ остаются классами сопряженных элементов и в A_5, а класс $\{(i,j,k,l,m)\}$ распадается на два класса в A_5.

Пусть $H \lhd \mathrm{A}_5$. Тогда подгруппа H составлена из классов сопряженных элементов. Следовательно,

$$|H| = 1 + 20x_1 + 15x_2 + 12x_3,$$

где x_1, $x_2 \in \{0, 1\}$, $x_3 \in \{0, 1, 2\}$. По теореме Лагранжа $|H|$ делит 60. Легко проверить, что это невозможно. □

Задача. Опишите классы сопряженных элементов в A_6.

Лемма. *Пусть $H \lhd \mathrm{S}_n$, $n \geq 5$. Тогда $H = \{1\}$, A_n или S_n.*

Доказательство. Предположим, что $H \neq \{1\}$ и пусть $\sigma \in H$ – нетривиальный элемент (мы можем считать, что a – элемент простого порядка). Разложим σ в произведение циклов независимых циклов и пусть $(i_1, i_2, \ldots, i_m)$ – цикл наибольшей длины в разложении. Таким образом, $\sigma = (i_1, i_2, \ldots, i_m)\tau$, где τ – произведение остальных циклов (возможно пустое). Сначала предположим, что $m \geq 3$. Тогда H содержит подстановку

$$\sigma' = (i_1, i_2)\sigma(i_1, i_2)^{-1} = (i_1, i_2)(i_1, i_2, \ldots, i_m)(i_1, i_2)^{-1}\tau = (i_2, i_1, \ldots, i_m)\tau.$$

Поэтому

$$\sigma'\sigma^{-1} = (i_2, i_1, \ldots, i_m)\tau\tau^{-1}(i_1, i_2, \ldots, i_m)^{-1} = (i_1, i_2, i_3) \in H.$$

Следовательно, H содержит все тройные циклы. Поскольку A_n порождается тройными циклами, $H \supset \mathrm{A}_n$.

Пусть теперь $m = 2$. Тогда σ имеет вид $(i_1, j_1) \cdots (i_k, j_k)$. Если $k = 1$, то $H = \mathrm{S}_n$ (поскольку S_n порождается транспозициями). Пусть $k \geq 2$. Тогда

$$H \ni (i_1, i_2)\sigma(i_1, i_2)^{-1}\sigma = (i_1, i_2)(j_1, j_2).$$

Следовательно, H содержит все подстановки вида $(i_1, i_2)(j_1, j_2)$, где i_1, i_2, j_1, j_2 попарно различны. Тогда для k отличного от i_1, i_2, j_1, j_2 имеем

$$H \ni (i_1, i_2)(j_1, j_2)(j_1, j_2)(i_2, k) = (i_1, i_2, k),$$

т.е. H содержит тройные циклы. Как и выше получаем $H \supset \mathrm{A}_n$. □

Доказательство теоремы. Пусть $H_1 \lhd \mathrm{A}_n$ и пусть H_1 не является нормальной подгруппой в S_n. Выберем подгруппу H_1 так, что ее порядок максимален. Рассмотрим действие S_n сопряжениями на множестве Ω всех подгрупп. Поскольку нормализатор $N(H_1) = N_{\mathrm{S}_n}(H_1)$ содержит A_n, то $|\operatorname{Orb}(H_1)| \leq 2$. По нашему предположению $|\operatorname{Orb}(H_1)| = 2$. Таким образом, $N(H_1) = \mathrm{A}_n$ и $\operatorname{Orb}(H_1) = \{H_1, H_2\}$, где H_2 – сопряженная с H_1 (подстановкой из S_n) подгруппа. Поэтому H_2 – подгруппа индекса 2 в S_n и по

лемме $N(H_2) = \mathrm{A}_n$. Таким образом,

$$\sigma H_1 \sigma^{-1} = \begin{cases} H_1 & \text{если } \sigma \in \mathrm{A}_n, \\ H_2 & \text{если } \sigma \in \mathrm{S}_n \setminus \mathrm{A}_n, \end{cases}$$

$$\sigma H_2 \sigma^{-1} = \begin{cases} H_2 & \text{если } \sigma \in \mathrm{A}_n, \\ H_1 & \text{если } \sigma \in \mathrm{S}_n \setminus \mathrm{A}_n. \end{cases}$$

Отсюда следует, что $H_1 \cap H_2 \lhd \mathrm{S}_n$ и по лемме $H_1 \cap H_2 = \{1\}$. Группы H_1 и H_2 образуют прямое произведение в A_n: $H_1 \times H_2 \subset \mathrm{A}_n$. Более того, $H_1 \times H_2 \lhd \mathrm{A}_n$ (проверьте самостоятельно). По нашему выбору H_1 имеем $H_1 \times H_2 = \mathrm{A}_n$. В частности, $|\,\mathrm{A}_n\,| = |H_1| \cdot |H_2| = |H_1|^2$. Так как $|H_1|$ делится на 3, то по первой теореме Силова в H_1 существует элемент σ порядка 3. Ясно, что он – произведение тройных циклов. Если $\sigma = (i, j, k)$, то

$$H_1 \ni \sigma^2 = (i, k, j) = (k, j)(i, j, k)(k, j)^{-1} \in H_2.$$

Противоречие. Поэтому σ можно представить в виде $\sigma = (i, j, k)(l, m, r)\tau$, где все i, j, k, l, m, r различны, а τ – произведение остальных независимых циклов (возможно пустое). Тогда как и выше для $\delta = (i, l)(j, m)(k, r)$ имеем

$$H_2 \ni \delta\sigma\delta^{-1} = (l, m, r)(i, j, k)\tau = \sigma \in H_1.$$

Последнее противоречие доказывает теорему. □

Напомним, что проективная линейная группа $\mathrm{PGL}_n(\Bbbk)$ – это $\mathrm{GL}_n(\Bbbk)/\{\lambda E \mid \lambda \in \Bbbk^*\}$, а специальная проективная линейная группа $\mathrm{PSL}_n(\Bbbk)$ – это образ $\mathrm{SL}_n(\Bbbk)$ в $\mathrm{PGL}_n(\Bbbk)$.

Задача. Докажите, что $\mathrm{PSL}_n(\Bbbk)$ – нормальная подгруппа в $\mathrm{PGL}_n(\Bbbk)$ для любого поля $\Bbbk$. Чему равен индекс $[\mathrm{PGL}_n(\Bbbk) : \mathrm{PSL}_n(\Bbbk)]$?

Теорема. *Группа* $\mathrm{PSL}_2(\mathbb{C}) \simeq \mathrm{PGL}_2(\mathbb{C})$ *проста.*

Доказательство основывается на следующей лемме.

Лемма. *Пусть* $N \lhd \mathrm{SL}_2(\mathbb{C})$ *нетривиальная нормальная подгруппа, содержащая* $-E$. *Тогда* $N = \{\pm E\}$.

Доказательство. Положим

$$D_\lambda := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \qquad T_\mu := \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$

Пусть $A \in N$ и $A \neq \pm E$. Согласно теореме о жордановой нормальной форме, мы можем также считать, что A имеет жорданову форму, т. е. $A = D_\lambda$ или T_1. Докажем, что матрицы T_μ принадлежат N для любого $\mu \in \mathbb{C}$. Действительно, если $A = T_1$, то для любого $\lambda \in \mathbb{C}^*$ имеем

$$N \ni D_\lambda A D_\lambda^{-1} = T_{\lambda^2},$$

где $\mu := \lambda^2$ принимает любые ненулевые значения. Если же $A = D_\lambda$ для $\lambda \neq 0, \pm 1$, то

$$N \ni A^{-1}(T_\nu A T_\nu^{-1}) = D_{\lambda^{-1}} T_\nu D_\lambda T_{-\nu} = T_{\nu(\lambda^{-2}-1)}.$$

Так как $\lambda^{-2} - 1 \neq 0$, то $\mu := \nu(\lambda^{-2} - 1)$ принимает любые значения. Таким образом, $T_\mu \in N$ и

$$N \ni \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} T_\mu \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = (T_{-\mu})^{\mathrm{t}}.$$

Это означает, что N содержит все элементарные матрицы типа I. Так как $\mathrm{SL}_2(\mathbb{C})$ порождается такими матрицами, то $N = \mathrm{SL}_2(\mathbb{C})$. Противоречие. □

Доказательство теоремы. Пусть $N \lhd \mathrm{PSL}_2(\mathbb{C})$ нетривиальная нормальная подгруппа, пусть $\pi : \mathrm{SL}_2(\mathbb{C}) \to \mathrm{PSL}_2(\mathbb{C})$ – естественный гомоморфизм и пусть $\tilde{N} := \pi^{-1}(N)$. Тогда $\tilde{N} \lhd \mathrm{SL}_2(\mathbb{C})$, $\tilde{N} \neq \mathrm{SL}_2(\mathbb{C})$ и $\tilde{N} \neq \{\pm E\}$. Согласно лемме мы имеем противоречие. □

На самом деле, верен более общий результат:

Теорема. *При $n \geq 2$ группа $\mathrm{PSL}_n(\Bbbk)$ проста за исключением двух случаев: $\mathrm{PSL}_2(\mathbb{F}_2)$ и $\mathrm{PSL}_2(\mathbb{F}_3)$, где $\mathbb{F}_q$ – поле из q элементов.*

Замечание. Имеют место изоморфизмы:

- $\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathrm{S}_3$,
- $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathrm{A}_4$,
- $\mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathrm{A}_5$,
- $\mathrm{PSL}_2(\mathbb{F}_9) \simeq \mathrm{A}_6$.

Мы дадим набросок доказательства для еще одного случая:

Теорема. *Группа* $\mathrm{PSL}_2(\mathbb{R})$ *проста.*

Доказательство. Пусть $N \lhd \mathrm{SL}_2(\mathbb{R})$ нетривиальная нормальная подгруппа, содержащая $-E$. Как и в комплексном случае, достаточно доказать, что $N = \{\pm E\}$. Пусть $A \in N$, $A \neq \pm E$. Пусть

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Тогда

$$B := CAC^{-1}A^{-1} = \begin{pmatrix} c^2 + d^2 & -ac - bd \\ -ac - bd & a^2 + b^2 \end{pmatrix} \in N.$$

Заменяя A на $D_\lambda A D_\lambda^{-1}$ мы можем считать, что матрица A не является ортогональной. Тогда $B \neq \pm E$. Таким образом, N содержит симметрическую матрицу $\neq \pm E$. Эта матрица сопряжена диагональной. Поэтому мы можем считать, что $D_\lambda \in N$

для $\lambda \neq \pm 1$. Далее, как и в доказательстве для комплексного случая, получаем, что группа N содержит все матрицы T_μ, а также и все транспонированные к ним. Так как $\mathrm{SL}_2(\mathbb{R})$ порождается элементарными матрицами типа I, то $N = \mathrm{SL}_2(\mathbb{R})$. Противоречие доказывает теорему. $\square$

Пример. Группа $\mathrm{PSL}_2(\mathbb{Z})$ не является простой. Это следует из того, что для любого $n \in \mathbb{N}$ группа $\mathrm{SL}_2(\mathbb{Z})$ содержит нормальную подгруппу

$$\Gamma(n) := \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv E \mod n\}.$$

12 Кольца, идеалы, гомоморфизмы колец

Определение. *Кольцом* называется непустое множество R с двумя операциями: сложением $(+)$ и умножением $(\cdot)$ такими, что

(1) R является абелевой группой относительно сложения;

(2) $a(b+c) = ab + ac, \quad (a+b)c = ac + bc \quad \forall a,\, b,\, c \in R.$

Кольцо называется *ассоциативным*, если выполнено свойство

$$(ab)c = a(bc) \qquad \forall a,\, b,\, c \in R.$$

Кольцо называется *коммутативным*, если выполнено свойство

$$ab = ba \qquad \forall a,\, b \in R.$$

Единицей кольца называется элемент $1 \in R$ такой, что

$$1 \neq 0 \quad \text{и} \quad 1a = a1 = a \qquad \forall a \in R.$$

(если такой существует).

Примеры. (1) Классическими примерами коммутативных ассоциативных колец с единицей являются кольцо целых чисел $\mathbb{Z}$, кольца вычетов $\mathbb{Z}_n$ и кольца многочленов $R[x]$

(над коммутативным ассоциативным кольцом с единицей). Целые четные числа образуют коммутативное ассоциативное кольцо без единицы.

(2) Напомним, что эндоморфизмом группы называется любой гомоморфизм этой группы в себя. Пусть A – абелева группа с аддитивной операцией и пусть $\mathrm{End}(A)$ – множество всех эндоморфизмов A. Определим сложение эндоморфизмов формулой

$$(\varphi + \psi)(a) = \varphi(a) + \psi(a).$$

а за умножение возьмем композицию. Тогда $\mathrm{End}(A)$ становится ассоциативным кольцом с единицей.

(3) Множество $\mathscr{O}_{z_0}$ функций комплексного переменного, аналитических в точке $z_0 \in \mathbb{C}$, является коммутативным ассоциативным кольцом.

(4) Пусть R – ассоциативное кольцо. Определим новое умножение на R формулой

$$[a, b] = ab - ba.$$

Тогда R с этим новым умножением также является кольцом (в общем случае некоммутативным и неассоциативным). Имеют место соотношения

$$[a, b] = -[b, a] \qquad \forall a,\, b \in R,$$

$[[a,b],c]+[[b,c],a]+[[c,a],b]=0 \quad \forall a,\ b,\ c \in R \quad$ (тождество Якоби).

Кольца, в которых выполняются эти свойства называются *кольцами Ли*[*]. Другим примером кольца Ли является $R=\mathbb{R}^3$ с векторным умножением.

Определение. *Делителями нуля* в кольце R называются элементы $a,\ b \in R$ такие, что $ab=0$, но $a \neq 0,\ b \neq 0$.

Например, делители нуля в кольце матриц $\mathrm{Mat}_n(\Bbbk)$ – это в точности ненулевые вырожденные матрицы. Делители нуля в кольце вычетов $\mathbb{Z}_n$ – это ненулевые классы вычетов, имеющие общий делитель с n.

Определение. Если R – кольцо с единицей, то элемент $a \in R$ называется *обратимым*, если $\exists a^{-1} \in R \quad aa^{-1}=a^{-1}a=1$.

Множество всех обратимых элементов кольца с единицей мы будем обозначать R^*. Если кольцо R ассоциативно, то R^* – группа. Например, $\mathbb{Z}^*=\{\pm 1\}$, $\mathrm{Mat}_n(\Bbbk)^*=\mathrm{GL}_n(\Bbbk)$.

Определение. Говорят, что R – *кольцо с делением*, если в R имеется единица и любой ненулевой элемент является обратимым, т. е. $R^*=R\backslash\{0\}$. *Телом* называется ассоциативное кольцо с делением. *Поле* – это коммутативное тело.

[*]Sophus Lie – норвежский математик (1842 – 1899)

Определение. Подгруппа $I \subset R$ аддитивной группы кольца называется (двусторонним) *идеалом*, если $aI \subset I$ и $Ia \subset I$ для любого $a \in R$.

Пример. В каждом кольце имеется идеал $(0) := \{0\}$ называется *нулевым*. Все кольцо R – также идеал.

Пример. Четные числа – идеал в кольце $\mathbb{Z}$.

Пример. Пусть $R = C[a, b]$ – кольцо действительных непрерывных функций на отрезке. Функции, обращающиеся в нуль а некоторой точке образуют идеал

$$I_c := \{f \in C[a, b] \mid f(c) = 0\}.$$

Пример. В кольце матриц $\mathrm{Mat}_n(\Bbbk)$ аддитивная подгруппа

$$I := \left\{ \begin{pmatrix} 0 & * & \cdots & * \\ \cdots & \cdots & \cdots & \cdots \\ 0 & * & \cdots & * \end{pmatrix} \right\}$$

(матриц с нулевым левым столбцом) идеалом не является. Однако она является *левым идеалом*: $\forall A \in I$, $\forall B \in \mathrm{Mat}_n(\Bbbk)$ $BA \in I$.

Определение. Пусть R – коммутативное ассоциативное кольцо и пусть $a_1, \ldots, a_n \in R$. Множество

$$(a_1, \ldots, a_n) := \{a_1 b_1 + \cdots a_n b_n \mid b_i \in R\}$$

является идеалом в R. Он называется *идеалом, порожденным элементами* $a_1, \ldots, a_n$. Это наименьший идеал, содержащий $a_1, \ldots, a_n$. Если R – кольцо с единицей, то $(1) = R$. Этот идеал называется *единичным*.

Примеры. (1) Пусть R – коммутативное ассоциативное кольцо с единицей. Если некоторый идеал I содержит обратимый элемент, то он является единичным: $a \in I \Longrightarrow 1 = aa^{-1} \in I \Longrightarrow I = (1) = R$. Любой идеал в поле является или нулевым или единичным.

Определение. *Гомоморфизмом колец* называется отображение $\varphi : R \to R_1$ такое, что $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ для любых элементов a, $b \in R$. Таким образом, гомоморфизм колец является гомоморфизмом их аддитивных групп. Как обычно в алгебре, биективный гомоморфизм называется *изоморфизмом*. Изоморфизм кольца на себя называется *автоморфизмом*. Если R и R_1 – кольца с единицами 1 и $1'$, то обычно считается, что гомоморфизм колец $\varphi : R \to R_1$ единицу переводит в единицу, т.е. $\varphi(1) = 1'$ (это свойство автоматически не выполняется).

Примеры. (1) Отображение $\mathbb{Z} \to \mathbb{Z}_n$, переводящее целое число в его класс вычетов, является гомоморфизмом колец.

(2) Для каждого вектора $\mathbf{a} = (a_1, \ldots, a_n) \in \Bbbk^n$ отображение $\varphi_{\mathbf{a}} : \Bbbk[t_1, \ldots, t_n] \to \Bbbk$, $f \mapsto f(\mathbf{a})$ является гомоморфизмом.

(3) Если R – кольцо с единицей, то отображение

$$\mathbb{Z} \longrightarrow R, \qquad n \longmapsto n \cdot 1$$

является гомоморфизмом.

Определение. Пусть I – идеал кольца R. На факторгруппе R/I аддитивной группы определим умножение по правилу $(a+I)(b+I) = ab+I$. Несложно проверить, что это определение не зависит от вида записи смежных классов $a+I$ и $b+I$: если $a+I = a'+I$ и $b+I = b'+I$, то $a' = a+c$ и $b' = b+d$ для некоторых c, $d \in I$. Отсюда

$$a'b' - ab = ad + cb + cd \in I$$

и поэтому $a'b' + I = ab + I$. Кольцо R/I называется *факторкольцом.*

Теорема (теорема о гомоморфизме колец)**.** *Пусть* $\varphi : R \to R_1$ *– гомоморфизм колец. Тогда*

(1) $\mathrm{Ker}(\varphi)$ *– идеал в* R.

(2) *Имеется естественный изоморфизм* $\varphi(R) \simeq R/I$.

Доказательство. Положим $I := \mathrm{Ker}(\varphi)$. Воспользуемся теоремой о гомоморфизме групп. Из нее следует, что I – подгруппа аддитивной группы R и имеется естественный изоморфизм групп $\psi : R/I \to \varphi(R)$, $\psi(a+I) = \varphi(a)$. Остается доказать, что ψ – гомоморфизм колец:

$$\psi((a+I)(b+I)) = \psi(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(a+I)\psi(b+I).$$

□

12.1 Простота кольца матриц

Определение. Кольцо R называется *простым*, если оно не содержит нетривиальных (двусторонних) идеалов.

Задача. Докажите, что $\mathbb{R}^3$ с векторным умножением является простым кольцом.

Теорема. *Пусть R – ассоциативное кольцо с единицей и пусть $I \subset A := \mathrm{Mat}_n(R)$ – двусторонний идеал. Тогда существует единственный идеал $J \subset R$ такой, что $I = \mathrm{Mat}_n(J)$.*

Следствие. *Если R – тело, то $\mathrm{Mat}_n(R)$ – простое кольцо.*

Доказательство. Напомним, что матричной единицей называется матрица $E_{i,j}$, в которой на месте (i, j) стоит 1, а все остальные элементы равны 0. Матричные единицы перемножаются по

правилу

$$E_{i,j}E_{k,l} = \begin{cases} 0 & \text{если } j \neq k, \\ E_{i,l} & \text{если } j = k. \end{cases}$$

Положим

$$J := \{a \in R \mid aE_{1,1} \in I\}.$$

Проверим, что J – идеал в R:

$$b \in R, \quad a \in J \quad \Longrightarrow \quad aE_{1,1} \in I \quad \Longrightarrow$$
$$(ba)E_{1,1} = bEaE_{1,1} \in I \quad \Longrightarrow \quad ba \in J,$$

$$b \in R, \quad a \in J \quad \Longrightarrow \quad aE_{1,1} \in I \quad \Longrightarrow$$
$$(ab)E_{1,1} = aE_{1,1}bE \in I \quad \Longrightarrow \quad ab \in J.$$

Далее пусть $A = (a_{i,j}) \in I$. Тогда

$$a_{i,j}E_{1,1} = E_{1,i}AE_{j,1} \in I$$

и поэтому $a_{i,j} \in J$. Обратно, если $a_{i,j} \in J$ для всех i, j, то $a_{i,j}E_{1,1} \in I$. Отсюда

$$A = \sum a_{i,j}E_{i,j} = \sum_{i,j} E_{i,1}(a_{i,j}E_{1,1})E_{1,j} \in I.$$

Следовательно, $I = \mathrm{Mat}_n(J)$.

Единственность идеала J очевидна: если $I = \mathrm{Mat}_n(J) = \mathrm{Mat}_n(J')$, то для любой матрицы $A = (a_{i,j}) \in I$ имеем $a_{i,j} \in J$ и $a_{i,j} \in J'$. $\square$

13 Кольца главных идеалов

Пусть R – коммутативное ассоциативное кольцо с единицей. Идеалы, порожденные одним элементом, т. е. идеалы вида

$$(a) := \{ab \mid b \in R\}$$

называются *главными*. Говорят, что R – *кольцо главных идеалов*, если в нем каждый идеал является главным.

Примеры. (1) Ясно, что любое поле – кольцо главных идеалов, поскольку оно содержит всего два идеала: (0) и (1).

(2) Кольцо целых чисел $\mathbb{Z}$ является кольцом главных идеалов. Действительно, любой идеал является подгруппой, а подгруппа циклической группы $I \subset \mathbb{Z}$ – также циклическая. По этой же причине кольцо классов вычетов $\mathbb{Z}_n$ также является кольцом главных идеалов.

(3) Кольцо многочленов $\Bbbk[t]$ от одной переменной над полем также является кольцом главных идеалов. Действительно, пусть $I \subset \Bbbk[t]$ – ненулевой идеал. Выберем ненулевой многочлен $f \in I$ минимальной степени и пусть $g \in I$ – любой другой многочлен. Разделим g на f с остатком: $g = fq + r$, $\deg r < \deg f$. Тогда $r = g - fq \in I$ и по нашему предположению $r = 0$, т. е. $g = fq$.

(4) Кольцо многочленов $\Bbbk[t_1, \ldots, t_n]$ от нескольких переменных не является кольцом главных идеалов. Например, идеал

$$I := (t_1, \ldots, t_n) = \{f \in \Bbbk[t_1, \ldots, t_n] \mid f(0, \ldots, 0) = 0\}$$

не может быть порожден одним элементом. Аналогично, в кольце $\mathbb{Z}[t]$ идеал $(2, t)$ не порождается одним элементом.

Задача. Докажите, что для любого поля $\Bbbk$ кольцо формальных степенных рядов $\Bbbk[[t]]$ – кольцо главных идеалов. Опишите все идеалы в $\Bbbk[[t]]$.

Задача. Докажите, что кольцо $\mathscr{O}_{z_0}$ функций комплексного переменного, аналитических в точке $z_0 \in \mathbb{C}$, – кольцо главных идеалов.

Далее на протяжении настоящего параграфа мы предположим, что R – коммутативное ассоциативное кольцо с единицей без делителей нуля. Такое кольцо называется *областью*. В области имеет место понятие делимости: для $a \mid b$ для $a, b \in R$, если $b = ac$ для некоторого $c \in R$. Элементы $a, b \in R$ называются *ассоциированными*, если $b = au$ для некоторого $u \in R^*$. Отношение ассоциированности является отношением эквивалентности. Поэтому все кольцо разбивается на классы ассоциированных между собой элементов.

Ясно, что $a \mid b \iff b \in (a)$. Элементы a, $b \in R$ являются ассоциированными $\iff (a) = (b)$.

Элемент $a \in R \setminus \{0\}$ называется *неразложимым* если он делится только на обратимые и ассоциированные с ним элементы. Область называется *факториальной*, если в ней выполнена основная теорема арифметики: любой элемент $a \in R \setminus \{0\}$ разлагается в произведение неразложимых и это разложение единственно с точностью до порядка и ассоциированности.

Теорема. *Пусть R – область. Если R – кольцо главных идеалов, то оно факториально.*

Лемма. *В условиях теоремы у каждого необратимого элемента $a \in R$ имеется неразложимый множитель.*

Доказательство. По определению, если необратимый элемент $b \in R$ разложим, то у него существует необратимый множитель b' неассоциированный с b. Поэтому имеется последовательность необратимых неассоциированных между собой элементов $a_k \in R$ таких, что

$$a_1 \mid a, \quad a_2 \mid a_1, \ldots, \quad a_{k+1} \mid a_k, \ldots.$$

Если эта последовательность обрывается, то последний ее элемент a_n должен быть неразложимым делителем всех $a_{n-1}, \ldots, a_1$, a. Предположим, что последовательность бесконечна. Тогда она задает бесконечную возрастающую последовательность

идеалов

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_k) \subset \cdots .$$

Положим $I := \cup(a_k)$. Легко поверить, что I – идеал и $I \neq (1)$. По нашему предположению $I = (b)$ для некоторого $b \in R$. Так как $b \in (a_k)$ для некоторого k, то

$$(b) = (a_k) = (a_{k+1}) = \cdots .$$

Следовательно, элементы b, a_k, a_{k+1} ассоциированы. Противоречие. □

Доказательство теоремы. Существование. По индукции построим последовательности a_k и p_k, где $a_0 = a$, p_k – неразложимый делитель a_{k-1} и $a_k = a_{k-1}/p_k$. Таким образом, имеем

$$a = p_1 a_1, \quad a_1 = p_2 a_2, \quad \ldots \quad a_k = p_{k+1} a_{k+1}, \quad \ldots$$

Если процесс оборвется на некотором a_n, то $a = p_1 \cdots p_n$. Предположим, что процесс бесконечен. Имеем вложенную бесконечную цепочку идеалов

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_k) \subset \cdots .$$

Как и выше $\cup(a_k) = (b)$ для некоторого $b \in R$. Так как $b \in (a_k)$ для некоторого k, то

$$(b) = (a_k) = (a_{k+1}) = \cdots .$$

Следовательно, элементы b, a_k, a_{k+1} ассоциированы. Противоречие.

Единственность. Индукция по числу множителей с использованием следующей леммы. $\square$

Лемма. *В условиях теоремы если неразложимый элемент p делит $ab \in R$, то p делит a или p делит b.*

Доказательство. Рассмотрим идеал (a, p). По нашему предположению $(a, p) = (c)$ для некоторого $c \in R$. Тогда $c \mid p$ и поэтому или c обратим или он ассоциирован с p. Во втором случае $(a, p) = (p)$ и $p \mid a$. В первом случае имеем $c = au + pv$. Следовательно, p делит $b = abuc^{-1} + pbvc^{-1}$. $\square$

Задача. Докажите, что кольцо

$$\mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} \in \mathbb{C} \mid a,\, b \in \mathbb{Z}\}$$

не является факториальным.

Определение. Область R называется *евклидовым кольцом*, если существует отображение $\nu : R \setminus \{0\} \to \mathbb{N}$ такое, что

- $\nu(ab) \geq \nu(a)$, $\forall a,\, b \in R \setminus \{0\}$;
- (деление с остатком) $\forall a,\, b \in R \setminus \{0\} \quad \exists q,\, r \in R \quad a = bq + r$, причем $r = 0$ или $\nu(r) < \nu(b)$.

Пример. Кольцо целых чисел $\mathbb{Z}$ является евклидовым с $\nu(n) = |n|$. Кольцо многочленов $\Bbbk[t]$ над полем является евклидовым с $\nu(f) = \deg f$.

Задача. Докажите, что кольцо целых гауссовых чисел

$$\mathbb{Z}[i] := \{a + ib \in \mathbb{C} \mid a,\, b \in \mathbb{Z}\}$$

является евклидовым. *Указание.* Возьмите $\nu(a + ib) := a^2 + b^2$.

Теорема. *Евклидово кольцо является кольцом главных идеалов.*

Доказательство. Аналогично доказательству того, что $\Bbbk[t]$ – кольцо главных идеалов. Пусть I – ненулевой идеал. Выберем $a \in I \setminus \{0\}$ с наименьшим значением $\nu(a)$. Для любого другого элемента $b \in I \setminus \{0\}$ имеем $b = aq + r$, где неравенство $\nu(r) < \nu(a)$ невозможно по нашему предположению. Следовательно, $r = 0$ и $a \mid b$. □

Следствие. *Евклидово кольцо является факториальным.*

13.1 Модули над кольцами

Пусть R – ассоциативное кольцо с единицей. Абелева аддитивная группа M называется (левым) *модулем* над R или просто R-модулем, если определена операция $R \times M \to M$, $(a, x) \mapsto ax$ умножения элементов M на элементы R, удовлетворяющая аксиомам векторного пространства:

(1) $a(x+y) = ax + ay \qquad \forall a \in R, \quad \forall x,\, y \in M;$

(2) $(a+b)x = ax + bx \qquad \forall a,\, b \in R, \quad \forall x \in M;$

(3) $(ab)x = a(bx) \qquad \forall a,\, b \in R, \quad \forall x \in M;$

(4) $1x = x \qquad \forall x \in M.$

Примеры. (1) Любая аддитивная абелева группа является $\mathbb{Z}$-модулем.

(2) Кольцо R является модулем над собой.

(3) Если R – поле, то R-модули – это векторные пространства.

(4) Левые идеалы в кольце R являются R-модулями.

(5) Пусть V – векторное пространство над полем $\Bbbk$. Зафиксируем некоторый линейный оператор $\mathscr{A} : V \to V$. Тогда V является модулем над кольцом многочленов $\Bbbk[t]$ с умножением

$$f \cdot v = f(\mathscr{A})v \qquad f \in \Bbbk[t], \quad v \in V.$$

(6) Пусть $U \subset \mathbb{R}^n$ – открытая область и пусть $A^p(U)$ – пространство дифференциальных (например, бесконечно дифференцируемых) p-форм на U. Тогда $A^p(U)$ является модулем над кольцом $C^\infty(U)$ бесконечно дифференцируемых функций на U.

(7) Пусть $\phi : R \to R_1$ – гомоморфизм колец и пусть M_1 – модуль над кольцом R_1. Тогда M_1 является также модулем над R с умножением

$$ax = \phi(a)x \qquad a \in R, \quad x \in M_1.$$

В частности, для любого идеала $I \subset R$ факторкольцо R/I является R-модулем.

Для модулей можно определить все понятия, введенные для аддитивных абелевых групп и векторных пространств (такие как понятия изоморфизмов, прямых сумм, гомоморфизмов, подмодулей, фактормодулей). Для модулей также имеет место теорема о гомоморфизме. Говорят, что модуль M *порождается* элементами $x_1, \ldots, x_n \in M$, если любой элемент $x \in M$ представляется в виде $x = \sum a_i x_i$, $a_i \in R$. Модуль называется *свободным*, если такое представление единственно. Модуль называется *циклическим*, если он порождается одним элементом (т.е. $n = 1$).

Аналогично основной теореме о строении конечно порожденных абелевых групп можно доказать следующую.

Теорема. *Любой конечно порожденный модуль M над кольцом главных идеалов R является прямой суммой циклических модулей M_i изоморфных R или $R/(p_i^{k_i})$, где p_i – неразложимый элемент кольца R, а $k_i \in \mathbb{N}$. Эти модули M_i определяются модулем M однозначно с точностью до изоморфизма.*

Из этой теоремы легко выводится теорема о жордановой нормальной форме матрицы.

14 Поля

Пусть $\mathbb{K}$ – поле и пусть $\Bbbk$ – его подполе. В этом случае говорят, что $\mathbb{K}/\Bbbk$ – *расширение полей*. Ясно, что $\mathbb{K}$ является алгеброй (в частности, векторным пространством) над $\Bbbk$. Расширение $\mathbb{K}/\Bbbk$ называется *конечным*, если $\mathbb{K}$ конечномерно над $\Bbbk$. Размерность $\mathbb{K}$ как векторного пространства над $\Bbbk$ называется *степенью* расширения $\mathbb{K}/\Bbbk$ и обозначается $[\mathbb{K} : \Bbbk]$.

14.1 Простые поля

Пусть $\Bbbk$ – произвольное поле. Обозначим через M множество всех $m \in \mathbb{N}$ таких, что $\underbrace{1 + \cdots + 1}_{m} = 0$. *Характеристикой* $\mathrm{char}(\Bbbk)$ поля $\Bbbk$ называется число

$$\mathrm{char}(\Bbbk) = \begin{cases} \min M, & \text{если } M \neq \emptyset, \\ 0, & \text{если } M = \emptyset. \end{cases} \tag{1}$$

Таким образом, $\mathrm{char}(\Bbbk)$ – порядок единичного элемента 1 в аддитивной группе $\Bbbk$, если этот порядок конечен. Если же порядок 1 бесконечен, то характеристика поля считается равной нулю.

Напомним, что отображение

$$\phi\colon \mathbb{Z} \to \Bbbk, \qquad \phi(n) = n \cdot 1 \tag{2}$$

является гомоморфизмом колец. Непосредственно из определения характеристики получаем следующее

Утверждение. *Если* $\mathrm{char}(\Bbbk) = n$, *то* $\mathrm{Ker}(\phi) = (n)$. *В частности, гомоморфизм* ϕ *инъективен тогда и только тогда, когда* $\mathrm{char}(\Bbbk) = 0$.

Доказательство. Если $\mathrm{char}(\Bbbk) = 0$, то $\phi(m) = m \cdot 1 \neq 0$ для любого $m \in \mathbb{Z}$. Следовательно, $\mathrm{Ker}(\phi) = (0)$. Предположим, что $\mathrm{char}(\Bbbk) = n > 0$. Тогда n – порядок единицы в аддитивной группе поля. Очевидно, что для каждого $m \in (n)$ мы имеем $m = nk$, $k \in \mathbb{Z}$ и $\phi(m) = \phi(nk) = 0$. Следовательно, $\mathrm{Ker}(\phi) \supset (n)$. Обратно, пусть $m \in \mathrm{Ker}(\phi)$. Тогда $m \cdot 1 = 0$ и поэтому m делится на n, т.е. $m \in (n)$. Следовательно, имеется обратное включение $\mathrm{Ker}(\phi) \subset (n)$. □

Следствие. *Характеристика поля может быть или нулем, или простым числом.*

Доказательство. Предположим, что $\mathrm{char}(\Bbbk) = n > 0$. В обозначениях выше поле $\Bbbk$ содержит подкольцо $\phi(\mathbb{Z})$, которое по теореме о гомоморфизме изоморфно $\mathbb{Z}/(n) = \mathbb{Z}_n$. Если n не является простым, то $\mathbb{Z}_n \simeq \phi(\mathbb{Z})$ имеет делители нуля, что невозможно. □

Определение. Поле, не содержащее ни одного собственного подполя, называется *простым полем*.

Каждое поле $\Bbbk$ содержит единственное простое поле – пересечение всех подполей в $\Bbbk$. Примерами простых полей являются поле рациональных чисел $\mathbb{Q}$ и поля вычетов $\mathbb{Z}_p$ по простому модулю p. Верно и обратное:

Теорема. *Любое простое поле* $\Bbbk$ *изоморфно* $\mathbb{Q}$ *или* $\mathbb{Z}_p$.

Доказательство. Рассмотрим сначала случай $\operatorname{char}(\Bbbk) = p > 0$. Из утверждения и теоремы о гомоморфизме получаем, что $\operatorname{Im}(\phi) \simeq \mathbb{Z}/\operatorname{Ker}(\phi) = \mathbb{Z}_p$ является подполем в $\Bbbk$, а так как $\Bbbk$ – простое, то $\operatorname{Im}(\phi)$ совпадает с $\Bbbk$.

Теперь рассмотрим случай $\operatorname{char}(\Bbbk) = 0$. Тогда гомоморфизм ϕ инъективен. Продолжим этот гомоморфизм до отображения $\psi : \mathbb{Q} \to \Bbbk$ по правилу

$$\psi\left(\frac{n}{m}\right) = \frac{\phi(n)}{\phi(m)}.$$

Во-первых, проверим корректность этой формулы:

$$\frac{n}{m} = \frac{n'}{m'} \quad \Longleftrightarrow \quad nm' = n'm \quad \Longrightarrow$$

$$\Longrightarrow \phi(n)\phi(m') = \phi(n')\phi(m) \quad \Longleftrightarrow \quad \frac{\phi(n)}{\phi(m)} = \frac{\phi(n')}{\phi(m')}.$$

Далее мы видим, что ψ – гомоморфизм колец:

$$\psi\left(\frac{n}{m}+\frac{n'}{m'}\right)=\psi\left(\frac{nm'+n'm}{mm'}\right)=\frac{\phi(nm'+n'm)}{\phi(mm')}=$$
$$=\frac{\phi(n)\phi(m')+\phi(n')\phi(m)}{\phi(m)\phi(m')}=\frac{\phi(n)}{\phi(m)}+\frac{\phi(n')}{\phi(m')}=\psi\left(\frac{n}{m}\right)+\psi\left(\frac{n'}{m'}\right),$$

$$\psi\left(\frac{n}{m}\cdot\frac{n'}{m'}\right)=\psi\left(\frac{nn'}{mm'}\right)=\frac{\phi(nn')}{\phi(mm')}=$$
$$=\frac{\phi(n)\phi(n')}{\phi(m)\phi(m')}=\frac{\phi(n)}{\phi(m)}\cdot\frac{\phi(n')}{\phi(m')}=\psi\left(\frac{n}{m}\right)\cdot\psi\left(\frac{n'}{m'}\right).$$

Так как $\psi(1)=1$, то ψ – вложение полей, а так как $\Bbbk$ – простое, то ψ – изоморфизм. □

14.2 Расширения полей

Пусть $\mathbb{K}/\Bbbk$ – любое расширение полей. Для элементов $\vartheta_1,\ldots,\vartheta_n\in\mathbb{K}$ обозначим через $\Bbbk[\vartheta_1,\ldots,\vartheta_n]$ (соответственно, через $\Bbbk(\vartheta_1,\ldots,\vartheta_n)$) – наименьшее подкольцо (соответственно подполе) в $\mathbb{K}$, содержащее $\Bbbk$ и все $\vartheta_1,\ldots,\vartheta_n$. Ясно, что

$$\Bbbk[\vartheta_1,\ldots,\vartheta_n]=\Big\{\sum\alpha_{k_1,\ldots,k_n}\vartheta_1^{k_1}\cdots\vartheta_n^{k_n}\mid\alpha_{k_1,\ldots,k_n}\in\Bbbk,\ k_j\geq 0\Big\},$$

$$\Bbbk(\vartheta_1,\ldots,\vartheta_n)=\Big\{\tfrac{\beta}{\gamma}\mid\beta,\gamma\in\Bbbk[\vartheta_1,\ldots,\vartheta_n],\quad\gamma\neq 0\Big\}.$$

Будем говорить, что расширения $\mathbb{K}/\Bbbk$ и $\mathbb{K}'/\Bbbk$ *изоморфны* над $\Bbbk$, если существует изоморфизм полей $\varphi : \mathbb{K} \to \mathbb{K}'$ такой, что его ограничение $\varphi|_{\Bbbk}$ является тождественным отображением.

Определение. Мы скажем, что элемент $\vartheta \in \mathbb{K}$ *алгебраичен* над $\Bbbk$, если существует ненулевой многочлен $f \in \Bbbk[t]$, для которого $f(\vartheta) = 0$. В противном случае элемент ϑ называется *трансцендентным* над $\Bbbk$. Расширение полей $\mathbb{K}/\Bbbk$ называется *алгебраическим*, если каждый элемент $\vartheta \in \mathbb{K}$ алгебраичен над $\Bbbk$.

Пример. (i) Пусть $\Bbbk = \mathbb{Q}$, а $\mathbb{K} = \mathbb{C}$. Хорошо известно, что множество $\mathbb{Q}[t]$ всех многочленов над $\mathbb{Q}$ счетно. Поэтому и счетно множество всех алгебраических элементов $A \subset \mathbb{C}$. Однако множество $\mathbb{C}$ несчётно. Это показывает, что трансцендентных над $\mathbb{Q}$ элементов поля $\mathbb{C}$ "существенно больше" чем алгебраических.

(ii) Для независимой переменной t, пусть $\Bbbk(t)$ – поле рациональных дробей над $\Bbbk$. Любой элемент $f \in \Bbbk(t) \setminus \Bbbk$ является трансцендентным.

Определение. Пусть $\mathbb{K}/\Bbbk$ – любое расширение полей и пусть $\vartheta \in \mathbb{K}$ – алгебраический над $\Bbbk$ элемент.

Ненулевой многочлен $\mu_\vartheta^{\Bbbk}(t) \in \Bbbk[t]$ минимальной степени, для которого ϑ является корнем, называется *минимальным многочленом* элемента ϑ над $\Bbbk$. Если это не приводит к путанице, вместо $\mu_\vartheta^{\Bbbk}(t)$ мы будем писать просто μ_ϑ или даже μ.

Отметим, что отображение $\mathscr{A}_\vartheta\colon \mathbb{K} \to \mathbb{K}$, заданное формулой $\mathscr{A}_\vartheta(\beta) = \vartheta\beta$, является линейным оператором. Здесь $\mathbb{K}$ рассматривается как (возможно бесконечномерное) векторное пространство над $\Bbbk$. Многочлен μ_ϑ совпадает с минимальным многочленом этого линейного оператора.

Предложение. (1) *Если $f \in \Bbbk[t]$ – многочлен такой, что $f(\vartheta) = 0$, то f делится на минимальный многочлен μ_ϑ. В частности, минимальный многочлен определен однозначно с точностью до постоянного множителя.*

(2) *Минимальный многочлен μ неприводим в $\Bbbk[t]$.*

Доказательство. Разделим f на $\mu = \mu_\vartheta$ с остатком:

$$f = \mu g + r.$$

Тогда

$$0 = f(\vartheta) = \mu(\vartheta)g(\vartheta) + r(\vartheta) = r(\vartheta).$$

Так как $\deg r < \deg \mu$, то $r = 0$. Это доказывает (i).

Для доказательства второго утверждения предположим, что $\mu = \mu_1\mu_2$. Тогда $\mu_1(\vartheta) = 0$ или $\mu_2(\vartheta) = 0$. Это противоречит минимальности многочлена μ. □

Теорема. *Пусть $\Bbbk$ – поле и пусть $f \in \Bbbk[t]$ – многочлен положительной степени.*

(1) *Следующие три условия эквивалентны:*

(a) *многочлен f неприводим,*

(b) *факторкольцо $\Bbbk[t]/(f)$ является полем,*

(c) *факторкольцо $\Bbbk[t]/(f)$ не имеет делителей нуля.*

(2) *Пусть многочлен f неприводим. Если $\mathbb{L}/\Bbbk$ – расширение полей такое, что f имеет корень $\theta \in \mathbb{L}$, то существует изоморфизм*

$$\varphi : \Bbbk[t]/(f) \to \Bbbk(\theta), \quad t \mapsto \theta,$$

являющийся тождественным отображением на $\Bbbk$.

Доказательство. (1) Докажем (a) $\Longrightarrow$ (b). Пусть $\pi : \Bbbk[t] \to \Bbbk[t]/(f)$ – естественный гомоморфизм. Рассмотрим ненулевой элемент $\bar{g} = g + (f) \in \Bbbk[t]/(f)$. Таким образом, $\bar{g} = \pi(g)$, где $g \in \Bbbk[t]$ – многочлен такой, что $g \notin (f)$. Последнее означает, что f и g взаимно просты (поскольку f неприводим). По теореме о наибольшем общем делителе существуют многочлены u, $v \in \Bbbk[t]$ такие, что $1 = fu + gv$. Отсюда

$$1 = \pi(1) = \pi(f)\pi(u) + \pi(g)\pi(v) = \bar{g}\pi(v).$$

Следовательно, любой ненулевой элемент $\bar{g} \in \Bbbk[t]/(f)$ обратим и поэтому $\Bbbk[t]/(f)$ – поле.

Импликация (b) $\Longrightarrow$ (c) очевидна. Для доказательства (c) $\Longrightarrow$ (a) предположим, что $f = f_1 f_2$, где $f_i \notin (f)$. Тогда в $\Bbbk[t]/(f)$ имеем

$$\pi(f_1)\pi(f_2) = \pi(f_1 f_2) = \pi(f) = 0,$$

т.е. $\pi(f_1)$, $\pi(f_2)$ – делители нуля. Противоречие.

(2) Рассмотрим отображение

$$\psi : \Bbbk[t] \longrightarrow \mathbb{L}, \qquad h \longmapsto h(\theta).$$

Ясно, что ψ – гомоморфизм. Его ядро является главным идеалом: $\mathrm{Ker}(\psi) = (h)$. С другой стороны, $f \in \mathrm{Ker}(\psi)$ и f неприводим. Поэтому $\mathrm{Ker}(\psi) = (f)$. По теореме о гомоморфизме $\psi(\Bbbk[t]) \simeq \Bbbk[t]/(f)$. □

Замечание. Построенное выше расширение называется *присоединением к полю корня неприводимого многочлена.* Действительно, поле $\Bbbk$ естественно вкладывается в $\Bbbk[t]/(f)$ (как композиция $\Bbbk \hookrightarrow \Bbbk[t] \xrightarrow{\pi} \Bbbk[t]/(f)$), а согласно (2) образ $\theta := \pi(t)$ является корнем многочлена f. Степень расширения $[\Bbbk[t]/(f) : \Bbbk]$ равна степени многочлена f.

Предложение. *Пусть $\mathbb{K}/\Bbbk$ – расширение полей. Элемент $\vartheta \in \mathbb{K}$ алгебраичен над $\Bbbk$ тогда и только тогда, когда степень расширения $[\Bbbk(\vartheta) : \Bbbk]$ конечна.*

Доказательство. Достаточность. Пусть $n = [\Bbbk(\vartheta) : \Bbbk] < \infty$. Тогда элементы $1, \vartheta, \vartheta^2, \ldots, \vartheta^n$ линейно зависимы над $\Bbbk$. Следовательно, $\sum_{i=0}^{n} \lambda_i \vartheta^i = 0$ для некоторых $\lambda_i \in \Bbbk$, т.е. $f(\theta) = 0$, где $f = \sum_{i=0}^{n} \lambda_i t^i$.

Необходимость. Пусть $\theta \in \mathbb{K}$ – алгебраический над $\Bbbk$ элемент и пусть $f \in \Bbbk[t]$ – ненулевой многочлен такой, что $f(\theta) =$

0. Мы можем считать, что f неприводим. Согласно предложению выше $\Bbbk(\theta) \simeq \Bbbk[t]/(f)$ является конечным расширением поля $\Bbbk$. $\square$

Следствие. *Если $\mathbb{K}/\Bbbk$ – конечное расширение, то любой элемент $\beta \in \mathbb{K}$ является алгебраическим над $\Bbbk$.*

Теорема (теорема о башне полей)**.** *Пусть $\mathbb{L}/\mathbb{K}$ и $\mathbb{K}/\Bbbk$ – конечные расширения полей, пусть $m := [\mathbb{L} : \mathbb{K}]$ и $n := [\mathbb{K} : \Bbbk]$. Тогда $\mathbb{L}/\Bbbk$ – конечное расширения полей и $[\mathbb{L} : \Bbbk] = nm$.*

Доказательство. Пусть $a_1, \ldots, a_n \in \mathbb{K}$ – базис $\mathbb{K}/\Bbbk$ и пусть $b_1, \ldots, b_m \in \mathbb{L}$ – базис $\mathbb{L}/\mathbb{K}$. Докажем, что элементы $a_i b_j \in \mathbb{L}$, $i = 1, \ldots, n$, $j = 1, \ldots, m$ образуют базис $\mathbb{L}/\Bbbk$.

Предположим, что

$$\sum_{i,j} \lambda_{i,j} a_i b_j = 0$$

для $\lambda_{i,j} \in \Bbbk$. Тогда

$$0 = \sum_{i,j} \lambda_{i,j} a_i b_j = \sum_j \left(\sum_i \lambda_{i,j} a_i \right) b_j.$$

Так как $b_1, \ldots, b_m \in \mathbb{L}$ – базис $\mathbb{L}/\mathbb{K}$, а $\sum_i \lambda_{i,j} a_i \in \mathbb{K}$, то $\sum_i \lambda_{i,j} a_i = 0 \quad \forall j$. Так как $a_1, \ldots, a_n \in \mathbb{K}$ – базис $\mathbb{K}/\Bbbk$, то $\lambda_{i,j} = 0 \quad \forall i, \forall j$. Следовательно, элементы $a_i b_j \in \mathbb{L}$ линейно независимы над $\Bbbk$.

Пусть $c \in \mathbb{L}$. Снова так как $b_1, \ldots, b_m \in \mathbb{L}$ – базис $\mathbb{L}/\mathbb{K}$, то имеет место разложение $c = \sum_j \mu_j b_j$ для некоторых $\mu_j \in \mathbb{K}$, а так как $a_1, \ldots, a_n \in \mathbb{K}$ – базис $\mathbb{K}/\Bbbk$, то $\mu_j = \sum_i \lambda_{i,j} a_i$ для некоторых $\lambda_{i,j} \in \Bbbk$. Таким образом,

$$c = \sum_j \left(\sum_i \lambda_{i,j} a_i \right) b_j = \sum_{i,j} \lambda_{i,j} a_i b_j,$$

т. е. элементы $a_i b_j \in \mathbb{L}$ порождают $\mathbb{L}$ как векторное пространство над $\Bbbk$. □

Предложение. *Если $\mathbb{K}/\Bbbk$ – любое расширение полей, то элементы поля $\mathbb{K}$, алгебраические над $\Bbbk$, также образуют поле.*

Доказательство. Достаточно доказать, что для любых двух алгебраических элементов α, $\beta \in \mathbb{K}$ элементы $\alpha \pm \beta$, $\alpha\beta$ и α/β также являются алгебраическими. Согласно следствию для этого достаточно доказать, что расширение $\Bbbk(\alpha, \beta)/\Bbbk$ конечно. Но $\Bbbk(\alpha, \beta) = \Bbbk(\alpha)(\beta)$. Расширения $\Bbbk(\alpha)/\Bbbk$ и $\Bbbk(\alpha)(\beta)/\Bbbk(\alpha)$ конечны. Требуемый факт теперь легко выводится из теоремы о башне полей. □

Пример. Пусть $\bar{\mathbb{Q}} \subset \mathbb{C}$ – множество всех алгебраических над $\mathbb{Q}$ элементов. Тогда $\bar{\mathbb{Q}}$ – поле. Оно называется *полем алгебраических чисел.*

Задача. Докажите, что поле $\bar{\mathbb{Q}}$ алгебраически замкнуто.

Пример. Пусть $\mathbb{K}/\mathbb{R}$ – алгебраическое расширение. Тогда $\mathbb{K} = \mathbb{R}$ или $\mathbb{K} \simeq \mathbb{C}$ (как поле над $\mathbb{R}$).

14.3 Поле разложения многочлена

Определение. Пусть $\Bbbk$ – произвольное поле. *Полем разложения* многочлена $f \in \Bbbk[t]$ называется поле $\mathbb{K} \supset \Bbbk$ такое, что f над $\mathbb{K}$ разлагается на линейные множители:

$$f = c\prod(t - \alpha_i),$$

где $c \in \Bbbk$, а $\alpha_i \in \mathbb{K}$ и корни α_i порождают $\mathbb{K}$ над $\Bbbk$.

Теорема. *Пусть $\Bbbk$ – поле и $f \in \Bbbk[t]$ – некоторый многочлен. Существует поле $\mathbb{K} \supset \Bbbk$, являющееся полем разложения для f над $\Bbbk$. Любые два таких поля $\mathbb{K}$ изоморфны над $\Bbbk$.*

Доказательство. Доказательство существования. Индукция по степени $n = \deg f$. База индукции очевидна. Предположим, что утверждение верно для всех многочленов степени $< n$. Пусть f_1 – неприводимый множитель f. Присоединим к $\Bbbk$ корень f_1, т.е. рассмотрим расширение $\mathbb{K}_1/\Bbbk$, $\mathbb{K}_1 = \Bbbk[t]/(f_1)$. Пусть θ_1 – корень f_1 в $\mathbb{K}_1$. Запишем $f = (t-\theta_1)g$. Так как $\deg g < n$, то для g над $\mathbb{K}_1$ существует поле разложения $\mathbb{L}$. Таким образом, f разлагается на линейные множители в $\mathbb{L}$:

$$f = c(t - \theta_1)\cdots(t - \theta_n).$$

Положим $\mathbb{K} := \Bbbk(\theta_1, \ldots, \theta_n)$.

Доказательство единственности. Предположим, что существует два поля разложения $\mathbb{K}$ и $\mathbb{K}^\sharp$ для f над $\Bbbk$. Построим изоморфизм $\mathbb{K} \simeq \mathbb{K}^\sharp$ над $\Bbbk$. Пусть f_1 – неприводимый множитель f степени > 1. Пусть θ_1 – корень f_1 в $\mathbb{K}$ и пусть $\mathbb{K}_1 := \Bbbk(\theta_1)$. По индукции построим цепочку полей

$$\Bbbk \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_m = \mathbb{K}$$

следующим образом. Если $\mathbb{K}_{l-1} \neq \mathbb{K}$, то многочлен f имеет неприводимый множитель $f_l \in \mathbb{K}_{l-1}[t]$ степени > 1. Пусть θ_l – корень f_l в $\mathbb{K}$ и пусть $\mathbb{K}_l := \mathbb{K}_{l-1}(\theta_l)$. Процесс оборвется поскольку наша цепочка – возрастающая цепочка векторных пространств над $\Bbbk$ размерности $\leq n$.

Далее по индукции доказываем, что для каждого $l = 1, \ldots, m$ существует изоморфизм $\varphi_l : \mathbb{K}_l \to \mathbb{K}^\sharp$ на некоторое подполе в $\mathbb{K}_l^\sharp \subset \mathbb{K}^\sharp$. Для $l = 1$, пусть $\theta_1^\sharp$ – корень f_1 в $\mathbb{K}^\sharp$. Тогда

$$\Bbbk(\theta_1^\sharp) \simeq \Bbbk[t]/(f_1) \simeq \Bbbk(\theta_1) = \mathbb{K}_1.$$

Следовательно, существует изоморфизм $\varphi_1 : \mathbb{K}_1 \to \Bbbk(\theta_1^\sharp) \subset \mathbb{K}^\sharp$.

Предположим, что изоморфизм $\varphi_{l-1} : \mathbb{K}_{l-1} \to \mathbb{K}^\sharp$ построен. Положим $\mathbb{K}_{l-1}^\sharp := \varphi_{l-1}(\mathbb{K}_{l-1})$. Пусть $f_l^\sharp \in \mathbb{K}_{l-1}^\sharp[t]$ – многочлен, полученный применением φ_{l-1} ко всем коэффициентам f_l. Этот многочлен неприводим над $\mathbb{K}_{l-1}^\sharp$ и имеет корень $\theta_l^\sharp \in \mathbb{K}^\sharp$. Тогда

$$\mathbb{K}_l = \mathbb{K}_{l-1}(\theta_l) \simeq \mathbb{K}_{l-1}[t]/(f_l) \simeq \mathbb{K}_{l-1}^\sharp[t]/(f_l^\sharp) \simeq \mathbb{K}_{l-1}^\sharp(\theta_l^\sharp).$$

Следовательно, существует изоморфизм

$$\varphi_l : \mathbb{K}_l \to \mathbb{K}_{l-1}^\sharp(\theta_l^\sharp) \subset \mathbb{K}^\sharp.$$

На последнем шаге мы получим изоморфизм

$$\varphi = \varphi_l : \mathbb{K}_m = \mathbb{K} \to \mathbb{K}_m^\sharp \subset \mathbb{K}^\sharp.$$

Так как $f^\sharp$ разлагается в $\mathbb{K}_m^\sharp$ на линейные множители, то $\mathbb{K}_m^\sharp = \mathbb{K}^\sharp$. □

Замечание. Пусть $f \in \Bbbk[t]$ и пусть $\mathbb{K}$ – его поле разложения f над $\Bbbk$. Мы считаем, что f не имеет корней в $\Bbbk$. По конструкции и по теореме о башне полей $[\mathbb{K} : \Bbbk] \leq n!$, причем при $n = 2$ имеет место равенство. При $n = 3$ степень $[\mathbb{K} : \Bbbk]$ зависит от дискриминанта D многочлена f:

$$[\mathbb{K} : \Bbbk] = \begin{cases} 3 & \text{если } \sqrt{D} \in \Bbbk \\ 6 & \text{если } \sqrt{D} \notin \Bbbk \end{cases}$$

Действительно, пусть $\sqrt{D} \in \Bbbk$. По формулам Виета

$$\theta_2 + \theta_3,\ \theta_2\theta_3 \in \Bbbk(\theta_1).$$

С другой стороны, с точностью до знака имеем

$$\Bbbk \ni \sqrt{D} = (\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3) = (\theta_1^2 - (\theta_2 + \theta_3)\theta_1 + \theta_2\theta_3)(\theta_2 - \theta_3).$$

Поэтому $\theta_2 - \theta_3 \in \Bbbk(\theta_1)$, а отсюда и $\theta_2, \theta_3 \in \Bbbk(\theta_1)$, т.е. $\Bbbk(\theta_1) = \mathbb{K}$. Следовательно, $[\mathbb{K} : \Bbbk] = 3$.

Предположим, что $\mathbb{K} \neq \Bbbk(\theta_1)$. Тогда, как и выше,

$$\theta_2 + \theta_3,\ \theta_2\theta_3 \in \Bbbk(\theta_1).$$

С другой стороны, $\theta_2 - \theta_3 \notin \Bbbk(\theta_1)$. Поэтому и $\sqrt{D} \notin \Bbbk$. В этом случае

$$[\mathbb{K} : \Bbbk] = [\Bbbk(\theta_1 : \Bbbk] \cdot [\Bbbk(\theta_1, \theta_2) : \Bbbk(\theta_1)] = 6.$$

textcolorwebgreenЗадачи. (1) Пусть $\Bbbk$ – поле. Могут ли быть изоморфны мультипликативная и аддитивная группы $\Bbbk$?

(2) Докажите, что аддитивная группа поля $\Bbbk$ является циклической тогда и только тогда, когда $\Bbbk \simeq \mathbb{Z}_p$ (где p – простое).

(3) Докажите, что аддитивная группа поля конечно порождена тогда и только тогда, когда поле конечно.

14.4 Отображение Фробениуса

Пусть $\Bbbk$ – поле характеристики $p > 0$. Рассмотрим отображение

$$\varphi : \Bbbk \longrightarrow \Bbbk, \qquad a \longmapsto a^p.$$

Это отображение называется *отображением Фробениуса* *. Его образ мы обозначим через $\Bbbk^p$:

$$\Bbbk^p := \varphi(\Bbbk) = \{a^p \mid a \in \Bbbk\}.$$

Предложение. (1) *$\Bbbk^p$ является подполем в $\Bbbk$.*

(2) *φ является изоморфизмом между $\Bbbk$ и $\Bbbk^p$.*

(3) *Если поле $\Bbbk$ конечно, то $\Bbbk^p = \Bbbk$.*

Доказательство. Имеем $\varphi(ab) = (ab)^p = \varphi(a)\varphi(b)$ и

$$\varphi(a+b) = (a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} C_p^k a^k b^{p-k}.$$

В последней сумме биномиальные коэффициенты $C_p^k = \frac{p!}{(p-k)!k!}$ рассматриваются как целые числа. Так как все они делятся на p, то

$$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b).$$

Из этого следует, что $\varphi : \Bbbk \to \Bbbk$ – гомоморфизм колец. Так как ядро этого гомоморфизма тривиально, то φ является изоморфизмом между $\Bbbk$ и $\varphi(\Bbbk)$. В частности, $\varphi(\Bbbk)$ – поле. Это доказывает (1) и (2). Утверждение (3) следует из того, что в случае конечного поля $\Bbbk^p$ содержит столько же элементов, что и $\Bbbk$. □

*Ferdinand Georg Frobenius – немецкий математик (1849 – 1917).

Таким образом, если $\Bbbk^p = \Bbbk$, то отображение φ является автоморфизмом поля $\Bbbk$. Он называется *автоморфизмом Фробениуса*.

Задача. Докажите, что множество неподвижных точек

$$\{a \in \Bbbk \mid \varphi(a) = a\}$$

совпадает с простым подполем $\Bbbk_0 \subset \Bbbk$. Что представляет собой множество неподвижных точек отображения φ^k?

15 Конечные поля

В этом параграфе мы рассмотрим конечные поля, т. е. поля состоящие из конечного числа элементов. Напомним, что характеристика конечного поля $\Bbbk$ отлична от нуля, является простым числом p и $\Bbbk$ содержит простое подполе $\Bbbk_0$ изоморфное $\mathbb{Z}_p$.

Теорема (Первая теорема о строении конечных полей)**.** *Пусть* $\Bbbk$ – *конечное поле характеристики* $p > 0$ *и пусть* $\Bbbk_0$ – *его простое подполе. Тогда*

(1) *число элементов* $\Bbbk$ *равно* p^m, *где* $m = [\Bbbk : \Bbbk_0]$,

(2) $\Bbbk$ *является полем разложения многочлена* $t^q - t$ *над* $\Bbbk_0$.

Доказательство. Утверждение о числе элементов следует из того, что каждый элемент векторного пространства однозначно задается своими координатами $(x_1, \ldots, x_m)$ (в фиксированном базисе), а в нашем случае для каждой координаты x_i имеется ровно p возможностей, так как $x_i \in \Bbbk_0 \simeq \mathbb{Z}_p$.

По теореме Лагранжа порядок каждого элемента a группы $\Bbbk^*$ делит ее порядок. Поэтому $a^{p^m-1} - 1 = 0$ для любого $a \neq 0$. Очевидно, что тогда $a^{p^m} - a = 0$ для всех $a \in \Bbbk$. Таким образом, многочлен $t^q - t$ имеет q различных корней. С другой стороны, согласно теореме Безу многочлен $t^q - t$ имеет не более q корней (с учетом кратностей). Поэтому этот многочлен имеет

только простые корни и разлагается на линейные множители в $\Bbbk$. Более того, поскольку каждый элемент $\Bbbk$ является корнем $t^q - t$, то $\Bbbk$ – поле разложения многочлена $t^q - t$ над $\Bbbk_0$. Теорема доказана. □

Теорема (Вторая теорема о строении конечных полей)**.** *Пусть $q = p^m$, p – простое. Поле разложения многочлена $t^q - t$ над $\mathbb{Z}_p$ содержит ровно q элементов и совпадает с множеством корней $t^q - t$.*

Следствие. *Конечное поле из p^m элементов существует и единственно с точностью до изоморфизма.*

Поле из $q = p^m$ элементов будет обозначатся через $\mathbb{F}_q$. Оно также называется *полем Галуа* [*].

Доказательство. Поле разложения $\mathbb{K}$ многочлена $t^q - t$ над $\mathbb{Z}_p$ конечно (поскольку является конечномерным пространством над $\mathbb{Z}_p$), а значит состоит из p^l элементов. Рассмотрим подмножество $M \subset \mathbb{K}$, состоящее из всех корней $t^q - t$. Заметим, что $a^q = a^{p^m} = \varphi^m(a)$, где $\varphi : \mathbb{K} \to \mathbb{K}$ – автоморфизм Фробениуса. Таким образом,

$$M = \{a \in \mathbb{K} \mid \varphi^m(a) = a\}$$

[*]Évariste Galois – французский математик (1811 – 1832)

– множество неподвижных элементов φ^m. Это множество замкнуто относительно операций:

$$a,\, b \in M \quad \Longrightarrow \quad \varphi^m(a) = a,\ \varphi^m(b) = b \quad \Longrightarrow$$
$$\Longrightarrow \quad \varphi^m(a \pm b) = \varphi^m(a) \pm \varphi^m(b) = a \pm b \in M$$

(аналогично для произведений и частных). Следовательно, M – поле. Многочлен $t^q - t$ разлагается на линейные множители в M, поэтому M – поле разложения для $t^q - t$ и $M = \mathbb{K}$. Так как

$$(t^q - t)' = qt^{q-1} - 1 = -1,$$

то $t^q - t$ не имеет кратных множителей и в $\mathbb{K}$ имеется ровно q элементов. □

Теорема. *Мультипликативная группа $\mathbb{F}_q^*$ конечного поля $\mathbb{F}_q$ является циклической.*

Доказательство. Пусть $m = \exp(\mathbb{F}_q^*)$. Тогда m делит $q - 1$. Следовательно, $a^m = 1$ для любого $a \in \mathbb{F}_q^*$, С другой стороны, по теореме Безу уравнение $t^m - 1 = 0$ имеет не более m корней, т. е. $q - 1 \leq m$. Таким образом, $q - 1 = m$. По свойству показателя абелевой группы в $\mathbb{F}_q^*$ существует элемент $c \in \mathbb{F}_q^*$ порядка $q - 1$. Это означает, что $\mathbb{F}_q^*$ – циклическая группа. Теорема доказана. □

Следствие. *Поле $\mathbb{K} := \mathbb{F}_q$, $q = p^m$ содержит подполе из r элементов тогда и только тогда, когда $r = q^d$. Это подполе единственно.*

Доказательство. Пусть $\Bbbk \subset \mathbb{F}_q$ подполе из r элементов. Рассмотрим $\mathbb{F}_q$ как векторное пространство над $\Bbbk$. Положим $d = \dim_{\Bbbk} \mathbb{F}_q$. Как и в доказательстве первой теоремы о строении конечных полей получаем, что $q = r^d$. Так как $\Bbbk^*$ – подгруппа порядка $r-1$ в циклической группе $\mathbb{F}_q^*$, то она единственна, а значит единственно и подполе $\Bbbk$.

Наоборот, пусть $q = r^d$. Так как $r-1$ делит $q-1 = r^d-1$, то в циклической группе $\mathbb{K}^*$ порядка $q-1$ найдется (единственная) подгруппа U порядка $r-1$. По теореме Лагранжа все элементы U являются корнями многочлена $t^{r-1}-1$. Пусть $\Bbbk := U \cup \{0\} \subset \mathbb{F}_q$. Ясно, что все элементы $\Bbbk$ являются корнями многочлена $t^r - t$. Как и в доказательстве второй теоремы о строении конечных полей легко показать, что $\Bbbk$ – поле (и оно содержит ровно r элементов). □

Следствие. *Для любого расширения конечных полей $\mathbb{K}/\Bbbk$ существует элемент $\vartheta \in \mathbb{K}$, который порождает $\mathbb{K}$ над $\Bbbk$ (т. е., $\mathbb{K} = \Bbbk(\vartheta)$).*

Следствие. *Пусть $f \in \mathbb{F}_q[t]$ – неприводимый многочлен степени d (где $q = p^m$). Тогда f является делителем $t^{q^d} - t$. Для любого d существует неприводимый многочлен степени d над $\mathbb{F}_q$.*

Доказательство. Пусть $\mathbb{K}$ – поле, полученное присоединением корня многочлена f к $\mathbb{F}_q$ (т. е. $\mathbb{K} = \mathbb{F}_q[t]/(f)$). Тогда $\mathbb{K}$ – конечное поле и размерность $\mathbb{K}$ как векторного пространства над $\mathbb{F}_q$

равна d. Получаем, что $\mathbb{K}$ состоит из q^d элементов и поэтому $\mathbb{K} \simeq \mathbb{F}_q$. Многочлены f и $t^{q^d} - t$ имеют общий корень в $\mathbb{K}$. Следовательно, $(f,\, t^{q^d} - t) \neq 1$. Но наибольший общий делитель многочленов может быть вычислен при помощи алгоритма Евклида и не зависит от основного поля. Так как многочлен f неприводим над $\mathbb{F}_q[t]$, то имеется единственная возможность

$$(f,\, t^{q^d} - t) = f.$$

Отсюда получается первое утверждение.

Для доказательства второго рассмотрим порождающий элемент ϑ поля $\mathbb{F}_{q^d}$ над $\mathbb{F}_q$. Пусть $\mu_\vartheta \in \mathbb{F}_q[t]$ – минимальный многочлен для ϑ. Тогда μ_ϑ неприводим и $\deg \mu_\vartheta = [\mathbb{F}_{q^d} : \mathbb{F}_q] = d$. Это доказывает следствие. □

Пример. Построим поле $\mathbb{F}_8$ из 8 элементов. Любой элемент из $\mathbb{F}_8$ может быть записан как линейная комбинация $\alpha_0 + \alpha_1\vartheta + \alpha_2\vartheta^2$, $\alpha_i \in \mathbb{F}_2$. Для составления таблицы умножения мы должны найти минимальный многочлен $\mu = \mu_\vartheta$ элемента ϑ. Воспользуемся последним следствием. Получим, что μ делит многочлен $(t^8 - t)/(t^2 - t) = t^6 + \cdots + 1$. Легко видеть, что

$$t^6 + \cdots + 1 = (t^3 + t + 1)(t^3 + t^2 + 1).$$

Таким образом, мы можем взять $\mu = t^3 + t + 1$ или $t^3 + t^2 + 1$. Выбрав в качестве μ один из этих двух многочленов, мы можем однозначно восстановить таблицу умножения. Например,

в первом случае мы имеем $\vartheta^3 = -\vartheta - 1 = \vartheta + 1$. Обе возможности приводят к изоморфным полям.

textcolorwebgreenЗадачи. Докажите, что мультипликативная группа поля $\Bbbk$ конечно порождена тогда и только тогда, когда поле конечно.

16 Понятие алгебры над полем

Определение. Пусть D – векторное пространство над полем $\Bbbk$. Говорят, что D является *алгеброй* над $\Bbbk$ если D является кольцом и умножение в кольце связано с умножением на скаляры следующим образом:

$$\lambda(ab) = (\lambda a)b = a(\lambda b) \qquad \forall a,\, b \in D, \quad \forall \lambda \in \Bbbk.$$

Алгебра называется *ассоциативной* (*коммутативной*, *без делителей нуля* и т.д.) если таковым является соответствующее кольцо.

Примеры. (1) Пусть D – векторное пространство над полем $\Bbbk$. Оно является алгеброй над $\Bbbk$ с нулевым умножением: $ab = 0 \quad \forall a,\, b \in \Bbbk$.

(2) Если $\mathbb{K}/\Bbbk$ – расширение полей, то $\mathbb{K}$ – алгебра над $\Bbbk$. В частности, $\mathbb{C}$ – (коммутативная и ассоциативная) алгебра с делением над $\mathbb{R}$.

(3) Все квадратные $n \times n$-матрицы над полем $\Bbbk$ образуют ассоциативную алгебру $\mathrm{Mat}_n(\Bbbk)$ с единицей над $\Bbbk$.

(4) Алгебра многочленов $\Bbbk[t_1, \ldots, t_n]$ – ассоциативная коммутативная алгебра с 1.

(5) Над полем $\mathbb{R}$ или $\mathbb{C}$ можно определить алгебру $\mathbb{R}\{t\}$ ($\mathbb{C}\{t\}$) сходящихся (например в 0), степенных рядов. Над любым полем определена алгебра *формальных степенных рядов* $\Bbbk[[t]]$.

(6) Все непрерывные (соответственно, дифференцируемые) функции на интервале образуют ассоциативную коммутативную алгебру $C(a,b)$ (соответственно, $D(a,b)$) с единицей над $\mathbb{R}$.

(7) Трехмерное векторное пространство $\mathbb{R}^3$ с операцией векторного умножения является неассоциативной алгеброй.

(8) С каждым векторным пространством над полем $\Bbbk$ связаны три ассоциативные алгебры: *тензорная* $\mathrm{T}^\bullet(V)$, *внешняя* $\bigwedge^\bullet(V)$ и *симметрическая* $\mathrm{S}^\bullet(V)$.

(9) Пусть G – группа (для простоты предположим, что G – конечная) и пусть D – векторное пространство над $\Bbbk$ с базисом e_g, $g \in G$. Определим умножение элементов базиса следующим образом: $e_g \cdot e_h = e_{gh}$. По линейности это умножение продолжается на все D. Мы получим ассоциативную алгебру с единицей. Она называется *групповой алгеброй* G и обозначается $\Bbbk[G]$.

Задача. Докажите, что групповая алгебра имеет делители нуля.

Пример. Пусть D – конечномерная алгебра над $\Bbbk$ с базисом $e_1, \ldots, e_n$. Тогда умножение в D однозначно определяется произведениями элементов $e_i e_j$. Действительно, для $a = \sum_i \lambda^i e_i \in D$ и $b = \sum_j \mu^j e_j \in D$ имеем (мы используем тензорные обозначения)

$$ab = \Big(\sum_i \lambda^i e_i\Big)\Big(\sum_j \mu^j e_j\Big) = \sum_{i,j} \lambda^i \mu^j e_i e_j.$$

С другой стороны, мы можем разложить элементы $e_i e_j$ по базису

$$e_i e_j = \sum_k \theta_{i,j}^k e_k.$$

Скаляры $\theta_{i,j}^k$ называются *структурными константами* алгебры.

Определение. *Гомоморфизм алгебр* (над одним и тем же полем $\Bbbk$) – это гомоморфизм колец, который является $\Bbbk$-линейным отображением. Аналогично определяются понятия изоморфизма и аввтоморфизма алгебр.

Пусть D, D_1 – алгебры над полем $\Bbbk$, пусть $\varphi : D \to D_1$ – $\Bbbk$-линейное отображение (как векторных пространств) и пусть $e_1, \ldots, e_n$ – базис D. Отображение φ является гомоморфизмом алгебр тогда и только тогда, когда

$$\varphi(e_i e_j) = \varphi(e_i)\varphi(e_j) \qquad \forall i,\, j.$$

Примеры. (1) Рассмотрим групповую алгебру $\Bbbk[G]$ конечной группы G. Отображение

$$\Bbbk[G] \longrightarrow \Bbbk, \qquad \sum \alpha_g e_g \longmapsto \sum \alpha_g$$

является гомоморфизмом алгебр.

(2) Если D – алгебра с единицей, то отображение

$$\Bbbk \longmapsto D, \qquad \alpha \longmapsto \alpha \cdot 1$$

является (инъективным) гомоморфизмом алгебр.

Определение. *Идеал в алгебре* – это идеал в кольце, который является векторным подпространством. Если $I \subset D$ – идеал в $\Bbbk$-алгебре, то на факторкольце D/I можно ввести умножение на скаляры формулой

$$\alpha(x + I) = \alpha x + I \qquad \alpha \in \Bbbk, \qquad x \in D.$$

Несложно проверить, что это определение корректно. Получившаяся алгебра называется *факторалгеброй*.

Примеры. (1) В групповой алгебре $\Bbbk[G]$ конечной группы G подмножество

$$I := \left\{ \sum \alpha_g e_g \;\middle|\; \sum \alpha_g = 0 \right\}$$

является идеалом. Факторалгебра $\Bbbk[G]/I$ изоморфна $\Bbbk$.

(2) По определению симметрическая алгебра $\mathrm{S}^\bullet(V)$ (соответственно, внешняя алгебра $\bigwedge^\bullet(V)$) является факторалгеброй тензорной алгебры $\mathrm{T}^\bullet(V)$ по (двустороннему) идеалу, порожденному всевозможными тензорами вида $T - \sigma(T)$ (соответственно, $T - \mathrm{sgn}(\sigma)\sigma(T)$), где $T \in \mathrm{T}^n(V)$, $\sigma \in \mathrm{S}_n$, а $\mathrm{sgn}(\sigma)$ – знак подстановки σ.

Верно следующее утверждение, которое несложно выводится из теоремы о гомоморфизме колец.

Теорема (теорема о гомоморфизме алгебр)**.** *Пусть $\varphi : D \to D_1$ – гомоморфизм алгебр над полем $\Bbbk$. Тогда*

(1) $\mathrm{Ker}(\varphi)$ – *идеал в алгебре D;*

(2) *имеется естественный изоморфизм $\varphi(D) \simeq D/I$.*

16.1 Конечномерные алгебры с делением

Лемма. *Пусть D – конечномерная ассоциативная алгебра с единицей над полем $\Bbbk$. Если в D нет делителей нуля, то D – алгебра с делением.*

Доказательство. Пусть $a \in A$, $a \neq 0$. Рассмотрим отображение

$$\varphi : D \longrightarrow D, \qquad x \longmapsto a \cdot x.$$

Ясно, что это отображение является линейным оператором. Поскольку в D нет делителей нуля, то φ невырожден. В частности, он сюръективен. Положим $a^{-1} = \varphi(1)$. $\square$

Лемма. *Пусть D – конечномерная ассоциативная алгебра с делением над алгебраически замкнутым полем $\Bbbk$. Тогда $D \simeq \Bbbk$.*

Доказательство. Пусть элемент $a \in D$ не имеет вида $a = \lambda 1$, $\lambda \in \Bbbk$. Как и выше, рассмотрим оператор

$$\varphi : D \longrightarrow D, \qquad x \longmapsto a \cdot x.$$

Над алгебраически замкнутым полем он имеет собственный вектор:

$$\exists x \in D,\ \exists \lambda \in \Bbbk \quad \varphi(x) = a \cdot x = \lambda x.$$

Но тогда $(a - \lambda 1)x = 0$, $a = \lambda 1$. Противоречие. $\square$

Задача. Пусть D – конечномерная ассоциативная алгебра над полем $\Bbbk$. Докажите, что если в D нет делителей нуля, то D – алгебра с единицей. *Указание.* Во-первых покажите, что для любых $b \in D$, $a \in D \setminus \{0\}$ уравнения $b = xa$ и $b = ax$ имеют единственные решения. Поэтому для $a \in D \setminus \{0\}$ существует $e \in D$ такой, что $ae = a$. Отсюда $be = xae = xa = b$, т.е. e – правая единица. Покажите аналогично, что существует левая единица e' и тогда $e' = e$.

17 Алгебры с делением над $\mathbb{R}$

17.1 Алгебра кватернионов

Определение. Рассмотрим четырехмерное действительное векторное пространство $\mathbb{H} = \mathbb{R}^4$ с базисом $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. Определим умножение элементов базиса так, чтобы $\mathbf{1}$ был бы единицей, а остальные элементы перемножались бы следующим образом:

	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$-\mathbf{1}$	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$-\mathbf{k}$	$-\mathbf{1}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$-\mathbf{1}$

Построенная алгебра называется *алгеброй кватернионов*. Она была предложена Гамильтоном в 1843 г. *

Замечание. Элементы $\pm\mathbf{1}$, $\pm\mathbf{i}$, $\pm\mathbf{j}$, $\pm\mathbf{k}$ перемножаются как элементы известной нам группы кватернионов Q_8. Отсюда, в частности, следует что умножение элементов базиса, а значит и произвольных элементов, ассоциативно.

Предложение. $\mathbb{H}$ – *ассоциативная алгебра с делением.*

Доказательство. Ассоциативность операции следует из замечания выше. Рассмотрим отображение

$$\mathbb{H} \to \mathbb{H}, \quad x = \alpha\,\mathbf{1} + \beta\,\mathbf{i} + \gamma\,\mathbf{j} + \delta\,\mathbf{k} \mapsto \overline{x} := \alpha\,\mathbf{1} - \beta\,\mathbf{i} - \gamma\,\mathbf{j} - \delta\,\mathbf{k},$$

*William Rowan Hamilton – ирландский математик и физик (1805 – 1865)

которое мы назовем *сопряжением*. Несложно проверить, что

$$\overline{\lambda x} = \lambda \overline{x}, \quad \overline{x+y} = \overline{x} + \overline{y}, \quad \overline{x \cdot y} = \overline{y} \cdot \overline{x}, \quad \forall x,\, y \in \mathbb{H},\ \forall \lambda \in \mathbb{R}.$$

Действительно, эти свойства достаточно проверить на базисных элементах, а последнее – простой перебор возможностей. Таким образом, сопряжение является *антиавтоморфизмом* алгебры. Для кватерниона

$$x = \alpha\,\mathbf{1} + \beta\,\mathbf{i} + \gamma\,\mathbf{j} + \delta\,\mathbf{k} \in \mathbb{H}$$

определим его *норму*

$$\|x\| := x \cdot \overline{x} = \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

Тогда

$$\|x \cdot y\| = x \cdot y \cdot \overline{x \cdot y} = x \cdot y \cdot \overline{y} \cdot \overline{x} = x \cdot \|y\| \cdot \overline{x} = \|x\| \cdot \|y\|.$$

Теперь несложно предъявить обратный элемент: если $x \neq 0$, то

$$x^{-1} = \frac{1}{\|x\|}\bar{x}.$$

□

Элементы вида $\lambda\,\mathbf{1}$, $\lambda \in \mathbb{R}$ мы отождествим с действительными числами, т. е. мы считаем, что $\mathbb{R} \subset \mathbb{H}$.

Подалгебра, порожденная $\mathbf{1}$ и $\mathbf{i}$, может быть отождествлена с комплексными числами $\mathbb{C}$ и тогда $\mathbb{H}$ становится $\mathbb{C}$-векторным

пространством с базисом $\mathbf{1}, \mathbf{j}$. В частности любой элемент $x \in \mathbb{H}$ однозначно записывается в виде

$$x = z_1 + z_2\,\mathbf{j}, \qquad z_1,\, z_2 \in \mathbb{C}.$$

Однако, $\mathbb{H}$ не является $\mathbb{C}$-алгеброй:

$$\mathbf{j}\,z = \bar{z}\,\mathbf{j} \qquad \forall z \in \langle \mathbf{1},\, \mathbf{i} \rangle = \mathbb{C}.$$

Замечание. Алгебру $\mathbb{H}$ можно реализовать как $\mathbb{R}$-подалгебру в алгебре $\mathrm{Mat}_2(\mathbb{C})$, порожденную, как векторное пространство над $\mathbb{R}$, матрицами

$$\mathbf{1} = E, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Вложение $\delta : \mathbb{H} \to \mathrm{Mat}_2(\mathbb{C})$ можно определить следующим, более инвариантным образом. Для $x = z_1 + z_2\,\mathbf{j} \in \mathbb{H}$, $z_i \in \mathbb{C}$ положим

$$\delta(x) = \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{C}).$$

Это отображение является инъективным гомоморфизмом $\mathbb{R}$-алгебр. Легко проверить, что

$$\|x\| = \det \delta(x).$$

Задача. Пусть $\Bbbk$ – произвольное поле. Зафиксируем элементы $\alpha, \beta \in \Bbbk$. Аналогично алгебре кватернионов определим алгебру *обобщенных кватернионов* $\mathbb{H}_{\alpha,\beta}$ как четырехмерную алгебру

над $\Bbbk$ с базисом $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ и умножением определенным так, что $\mathbb{H}_{\alpha,\beta}$ ассоциативна, $\mathbf{1}$ – единица и

$$\mathbf{i}^2 = -\alpha\,\mathbf{1} \quad \mathbf{j}^2 = -\beta\,\mathbf{1}, \quad \mathbf{k} = \mathbf{i}\cdot\mathbf{j}\,.$$

Составьте полную таблицу умножения элементов базиса. При каком условии на α и β построенная алгебра $\mathbb{H}_{\alpha,\beta}$ будет алгеброй с делением?

Предложение. (1) *Соотношение*

$$(x,\,y) = \frac{1}{2}(x\bar{y} + y\bar{x}) = \frac{1}{2}(x\bar{y} + \overline{x\bar{y}}) \in \mathbb{R}.$$

определяет симметрическую положительно определенную $\mathbb{R}$*-билинейную форму на* $\mathbb{H}$*. Базис* $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ *является ортонормированным для этой формы.*

(2) *Аналогично,*

$$\langle x,\,y\rangle = \frac{1}{2}(xy + \bar{y}\bar{x}) = \frac{1}{2}(xy + \overline{xy}) \in \mathbb{R}$$

– $\mathbb{R}$*-билинейная форма сигнатуры* $(1,3)$*.*

(3) *Соотношение*

$$x \times y = -\frac{1}{2}(x\bar{y} - y\bar{x}).$$

определяет новое умножение на $\mathbb{H}$. *Его ограничение на трехмерное подпространство*

$$\mathbb{E} := \langle \mathbf{i},\, \mathbf{j},\, \mathbf{k} \rangle = \langle \mathbf{1} \rangle^{\perp}$$

чисто мнимых кватернионов является кососимметрическим

$$x \times y = \frac{1}{2}(xy - yx), \qquad x \times y = -y \times x$$

и совпадает со стандартным векторным умножением на $\mathbb{R}^3$.

Доказательство. Все утверждения доказываются непосредственной проверкой. Проверим, например, (2). Для этого запишем элементы $x,\, y \in \mathbb{H}$ в виде $x = x_0 + x'$ и $y = y_0 + y'$, где $x_0,\, y_0 \in \langle \mathbf{1} \rangle$, а $x',\, y' \in \mathbb{E}$. Тогда

$$2\langle x,\, y \rangle = (x_0 + x')(y_0 + y') + (y_0 - y')(x_0 - x') = x_0 y_0 + x_0 y' + \\ + y_0 x' + x' y' + x_0 y_0 - x_0 y' - y_0 x' + y' x' = 2x_0 y_0 + x' y' + y' x'.$$

(Мы воспользовались тем, что x_0 и y_0 коммутируют со всеми элементами $\mathbb{H}$.) Запишем далее

$$x' = x_1\,\mathbf{i} + x_2\,\mathbf{j} + x_3\,\mathbf{k}, \qquad y' = y_1\,\mathbf{i} + y_2\,\mathbf{j} + y_3\,\mathbf{k}\,.$$

Тогда

$$x' y' + y' x' = -2x_1 y_1 - 2x_2 y_2 - 2x_3 y_3.$$

Следовательно,

$$\langle x,\, y\rangle = x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3.$$

Отсюда немедленно получаем (2). □

17.2 Гомоморфизм $\mathrm{SU}_2 \to \mathrm{SO}_3$

Рассмотрим подгруппу $U \subset \mathbb{H}^*$ мультипликативной группы алгебры кватернионов, состоящую из кватернионов нормы 1:

$$U := \{u \in \mathbb{H} \mid \|u\| = 1\}.$$

Лемма. *Построенный выше инъективный гомоморфизм $\mathbb{R}$-алгебр*

$$\delta : \mathbb{H} \longrightarrow \mathrm{Mat}_2(\mathbb{C}), \qquad x = z_1 + z_2\,\mathbf{j} \longmapsto \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix}$$

индуцирует изоморфизм групп $U \simeq \mathrm{SU}_2$.

Доказательство. Пусть $C \in \mathrm{SU}_2$. Так как $C^{-1} = \overline{C}^{\mathrm{t}}$, то по формуле для обратной матрицы получаем, что C имеет вид

$$C = \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix}, \qquad |z_1|^2 + |z_2|^2 = 1.$$

Обратно, любая матрица такого вида принадлежит SU_2. Поэтому SU_2 лежит в образе δ, ограничение отображения δ^{-1} на SU_2 определено и является изоморфизмом между SU_2 и U. □

Для каждого $u \in U$ рассмотрим $\mathbb{R}$-линейный оператор

$$\varphi_u : \mathbb{H} \longrightarrow \mathbb{H}, \qquad x \longmapsto uxu^{-1} = ux\bar{u}.$$

Лемма. *Оператор φ_u является ортогональным относительно скалярного произведения*

$$(x, y) = \frac{1}{2}(x\bar{y} + y\bar{x}).$$

Трехмерное подпространство

$$\mathbb{E} := \langle \mathbf{i}, \mathbf{j}, \mathbf{k} \rangle = \langle \mathbf{1} \rangle^{\perp}$$

чисто мнимых кватернионов является инвариантным для φ_u.

Доказательство. Проверим, что φ_u сохраняет билинейную форму $(\ ,\ )$:

$$(\varphi_u(x), \varphi_u(y)) = \frac{1}{2}(ux\bar{u}\overline{uy\bar{u}} + uy\bar{u}\overline{ux\bar{u}}) = \frac{1}{2}(ux\bar{y}\bar{u} + uy\bar{x}\bar{u}) =$$
$$= \frac{1}{2}u(x\bar{y} + y\bar{x})\bar{u} = \frac{1}{2}(x\bar{y} + y\bar{x})u\bar{u} = (x, y).$$

Так как $\varphi_u(\mathbf{1}) = \mathbf{1}$, то $\mathbb{E} = \langle \mathbf{1} \rangle^{\perp}$ является инвариантным. $\square$

Таким образом, каждому кватерниону $u \in U$ мы можем сопоставить ортогональный оператор $\varphi_u|_{\mathbb{E}}$ в трехмерном евклидовом пространстве $\mathbb{E}$. Так как $\varphi_u \circ \varphi_v = \varphi_{uv}$, то это соответствие

$$\Psi : U \longrightarrow \mathrm{O}(\mathbb{E}) = \mathrm{O}_3, \qquad u \longmapsto \varphi_u|_{\mathbb{E}}$$

является гомоморфизмом групп.

Теорема. *Построенный выше гомоморфизм* Ψ *индуцирует сюръективный гомоморфизм*

$$\mathrm{SU}_2 \longrightarrow \mathrm{SO}_3$$

с ядром $\{\pm E\}$.

Доказательство. Отображение

$$\Psi : U \subset \mathbb{H} = \mathbb{R}^4 \to \mathrm{O}_3 \subset \mathrm{Mat}_3(\mathbb{R})$$

является непрерывной функцией естественных координат в $\mathbb{H} = \mathbb{R}^4$. Рассмотрим его композицию

$$\gamma : U \xrightarrow{\Psi} \mathrm{Mat}_3(\mathbb{R}) \xrightarrow{\det} \mathbb{R}$$

с другой непрерывной функцией – определителем. Так как определитель ортогональной матрицы принимает значения ± 1, то $\gamma(U) \subset \{\pm 1\}$. С другой стороны, U топологически является трехмерной сферой S^3 в четырехмерном евклидовом пространстве $\mathbb{H} = \mathbb{R}^4$. Следовательно, множество U связно, а поэтому таковым должен быть и его образ при непрерывном отображении γ. Поэтому $\gamma(U) = \{1\}$ и $\Psi : U \subset \mathrm{SO}_3$.

Ясно, что

$$\mathrm{Ker}(\Psi) = \{u \in U \mid u\,\mathbf{i} = \mathbf{i}\,u,\ u\,\mathbf{j} = \mathbf{j}\,u,\ u\,\mathbf{k} = \mathbf{k}\,u\} = \{\pm\mathbf{1}\}.$$

Для

$$z = z_\theta := \cos(\theta/2) + \mathbf{i}\sin(\theta/2) \in U$$

имеем $\varphi_z(\mathbf{i}) = \mathbf{i}$,

$$\varphi_z(\mathbf{j}) = z\,\mathbf{j}\,\bar{z} = z^2\,\mathbf{j} = (\cos\theta)\,\mathbf{j} + (\sin\theta)\,\mathbf{k},$$

$$\varphi_z(\mathbf{k}) = z\,\mathbf{k}\,\bar{z} = z^2\,\mathbf{k} = -(\sin\theta)\,\mathbf{j} + (\cos\theta)\,\mathbf{k}\,.$$

Таким образом, $\Psi(U)$ содержит элемент

$$\Psi(z_\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

– поворот на произвольный угол θ вокруг $\mathbf{i}$. Аналогично, для

$$u = u_{\theta'} := \cos(\theta'/2) + \mathbf{j}\sin(\theta'/2) \in U$$

имеем $\varphi_u(\mathbf{j}) = \mathbf{j}$,

$$\varphi_u(\mathbf{i}) = u\,\mathbf{i}\,\bar{u} = u^2\,\mathbf{i} = (\cos\theta')\,\mathbf{i} - (\sin\theta')\,\mathbf{k},$$

$$\varphi_u(\mathbf{k}) = u\,\mathbf{k}\,\bar{u} = u^2\,\mathbf{k} = (\sin\theta')\,\mathbf{i} + (\cos\theta')\,\mathbf{k}\,.$$

Таким образом, $\Psi(U)$ содержит элемент

$$\Psi(u_{\theta'}) = \begin{pmatrix} \cos\theta' & 0 & \sin\theta' \\ 0 & 1 & 0 \\ -\sin\theta' & 0 & \cos\theta' \end{pmatrix}$$

– поворот на произвольный угол $-\theta'$ вокруг $\mathbf{j}$. Мы утверждаем, что всевозможные повороты $\Psi(z_\theta)$ и $\Psi(u_{\theta'})$ порождают SO_3. Действительно, пусть $B \in \mathrm{SO}_3$. Тогда

$$(e_1, e_2, e_3) = (\mathbf{i}, \mathbf{j}, \mathbf{k}) \cdot B$$

– ортонормированный базис $\mathbb{E}$. Достаточно показать, что композицией преобразований $\Psi(z_\theta)$ и $\Psi(u_{\theta'})$ этот базис можно перевести в базис $(\mathbf{i}, \mathbf{j}, \mathbf{k})$. Во-первых, поворотом вокруг вокруг $\mathbf{i}$ мы можем e_1 перевести в вектор плоскости $\langle \mathbf{i},\, \mathbf{k} \rangle$:

$$\Psi(z_\theta)(e_1) = e_1' \in \langle \mathbf{i},\, \mathbf{k} \rangle.$$

Так как $\|e_1'\| = 1 = \|\,\mathbf{i}\,\|$, то поворотом вокруг вокруг $\mathbf{j}$ мы можем e_1' перевести в $\mathbf{i}$. Таким образом, мы имеем новый ортонормированный базис $(e_1'' = \mathbf{i},\, e_2'',\, e_3'')$ – образ (e_1, e_2, e_3) при некоторой композиции $\Psi(u_{\theta'}) \circ \Psi(z_\theta)$. Так как $\mathbf{j}$ и e_2'' ортогональны $\mathbf{i}$, то $e_2'' \in \langle \mathbf{j},\, \mathbf{k} \rangle$ и поворотом вокруг вокруг $\mathbf{i}$ мы можем e_2'' перевести в $\mathbf{j}$. Снова мы получим ортонормированный базис $(e_1''' = \mathbf{i},\, e_2''' = \mathbf{j},\, e_3''')$ – образ (e_1, e_2, e_3) при некоторой композиции $\Psi(z_{\theta_1}) \circ \Psi(u_{\theta'}) \circ \Psi(z_\theta)$. Тогда $e_3''' = \pm\,\mathbf{k}$. Поскольку $\det B = 1$, то базис (e_1, e_2, e_3) и все базисы $(e_1',\, e_2',\, e_3')$, $(e_1'',\, e_2'',\, e_3'')$, $(e_1''',\, e_2''',\, e_3''')$ имеют ту же ориентацию, что и $(\mathbf{i}, \mathbf{j}, \mathbf{k})$. Отсюда получаем, что $e_3''' = \mathbf{k}$ и $B^{-1} = \Psi(z_{\theta_1}) \circ \Psi(u_{\theta'}) \circ \Psi(z_\theta)$. $\square$

17.3 Теорема Фробениуса

Теорема (теорема Фробениуса)**.** *Пусть D – конечномерная ассоциативная алгебра с делением над полем $\mathbb{R}$. Тогда $D \simeq \mathbb{R}$, $\mathbb{C}$ или $\mathbb{H}$.*

Лемма (коммутативный случай)**.** *Пусть D – конечномерная ассоциативная коммутативная алгебра с делением над полем $\mathbb{R}$. Тогда $D \simeq \mathbb{R}$ или $\mathbb{C}$.*

Доказательство. Отождествим $\mathbb{R}$ с подалгеброй D при помощи отображения $\lambda \mapsto \lambda 1$. Пусть $D \neq \mathbb{R}$ и пусть $a \in D \setminus \mathbb{R}$. Пусть D_1 – подалгебра, порожденная a и 1. Она коммутативна и без делителей нуля. Следовательно, D_1 – поле. минимальный многочлен $\mu(t)$ элемента a неприводим над $\mathbb{R}$, т.е. $D_1/\mathbb{R}$ – квадратичное расширение. Тогда $D_1 \simeq \mathbb{C}$. Так как D коммутативна, то D является алгеброй над $D_1 \simeq \mathbb{C}$. Поскольку поле $\mathbb{C}$ алгебраически замкнуто, то $D \simeq \mathbb{C}$. □

Доказательство теоремы. Как и выше, отождествим $\mathbb{R}$ с подалгеброй D при помощи отображения $\lambda \mapsto \lambda 1$. Пусть $Z \subset D$ – *центр алгебры*, т.е. множество элементов, коммутирующих со всеми элементами D. Ясно, что $Z \supset \mathbb{R}$ и Z – конечномерная ассоциативная коммутативная алгебра с делением над $\mathbb{R}$. Если $Z \neq \mathbb{R}$, то $Z \simeq \mathbb{C}$. С другой стороны, D является алгеброй над $Z \simeq \mathbb{C}$ и поле $\mathbb{C}$ алгебраически замкнуто. Поэтому $D \simeq \mathbb{C}$.

Далее мы всюду предполагаем, что $Z = \mathbb{R}$ и $D \neq Z$. Возьмем любой элемент $a \in D \setminus Z$. Пусть D_1 – подалгебра, порожденная a и Z. Она коммутативна и без делителей нуля. Следовательно, $D_1 \simeq \mathbb{C}$ и поэтому существует элемент $\mathbf{i} \in D_1$ такой, что $\mathbf{i}^2 = -1$. Рассмотрим отображение

$$\varphi : D \longrightarrow D, \quad x \longmapsto \mathbf{i}\, x\, \mathbf{i}^{-1} = -\,\mathbf{i}\, x\, \mathbf{i}\,.$$

Несложно проверяется, что φ – автоморфизм алгебры. В частности, φ – линейный оператор, причем φ^2 – тождественное отображение. Таким образом, минимальный многочлен оператора φ имеет вид $t^2 - 1$. Отсюда получаем, что оператор φ диагонализируем и D, как векторное пространство над $\mathbb{R}$, разлагается в прямую сумму $D = D_+ \oplus D_-$ собственных подпространств собственными значениями ± 1. Элементы D_+ коммутируют с $\mathbf{i}$, а, следовательно, и со всей подалгеброй $D_1 \simeq \mathbb{C}$. Следовательно, D_+ – ассоциативная алгебра с делением над $\mathbb{C}$ и поэтому $D_+ = D_1$.

Элементы D_- антикоммутируют с $\mathbf{i}$:

$$\mathbf{i}\, b = -b\, \mathbf{i} \quad \forall b \in D_-.$$

Возьмем любой элемент $0 \neq b \in D_-$ и рассмотрим оператор

$$\psi : D \longrightarrow D, \quad x \longmapsto bx.$$

Так как D – алгебра с делением, то ψ невырожден. Более того,

ψ переставляет подпространства D_+ и D_-. Действительно,

$$x \in D_+ \quad \Leftrightarrow \quad x\,\mathbf{i} = \mathbf{i}\,x \quad \Leftrightarrow \quad (bx)\,\mathbf{i}\,x = b\,\mathbf{i}\,x = -\,\mathbf{i}(bx) \quad \Leftrightarrow \quad bx \in D_-.$$

и аналогично

$$x \in D_- \qquad \Longleftrightarrow \qquad bx \in D_+.$$

В частности,

$$\dim D_- = \dim D_+ = 2, \qquad \dim D = 4.$$

Далее,

$$\varphi(b^2) = \varphi(b)^2 = (-b)^2 = b^2.$$

Следовательно, $b^2 \in D_+$. Таким образом, b^2 коммутирует с элементами 1, $\mathbf{i}$, b и $b\,\mathbf{i}$, составляющих базис D. Поэтому $c := b^2 \in Z = \mathbb{R}$. Оператор ψ не имеет действительных собственных значений, а его минимальный многочлен имеет вид $t^2 - c$ (где c рассматривается как действительное число). Поэтому $c < 0$. Положим

$$\mathbf{j} := \frac{b}{\sqrt{-c}}, \qquad \mathbf{k} := \mathbf{i}\,\mathbf{j}\,.$$

Несложно проверить, что для базисных элементах 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ в алгебре D выполняются те же соотношения, что и для соответствующих базисных элементов в $\mathbb{H}$. $\square$

18 Представления групп

Определение. *Представлением* группы G в векторном пространстве V над полем $\Bbbk$ называется любой гомоморфизм $\phi : G \to \mathrm{GL}(V)$ группы G в группу невырожденных операторов на пространстве V. Точнее говоря, представление – это пара (V, ϕ). Представление является частным случаем действия группы G на множестве V. *Ядро* представления ϕ – это ядро гомоморфизма $\phi : G \to \mathrm{GL}(V)$. Представление называется *точным*, если его ядро тривиально. Степень (или размерность) представления (V, ϕ) – это размерность пространства V. Она обозначается $\deg \phi$ (или $\dim \phi$).

Гомоморфизмом представлений $\pi : (V, \phi_1) \to (W, \phi_2)$ группы G называется $\Bbbk$-линейное отображение $\pi : V \to W$ такое, что $\pi \circ \phi_1(g) = \phi_2(g) \circ \pi$ для любого элемента $g \in G$, т.е. диаграмма

$$\begin{array}{ccc} V & \xrightarrow{\pi} & W \\ {\scriptstyle \phi_1(g)}\downarrow & & \downarrow{\scriptstyle \phi_2(g)} \\ V & \xrightarrow{\pi} & W \end{array}$$

коммутативна. *Ядром* (соотв. *образом*) гомоморфизма называется ядро (соотв. образ) линейного отображения π. Гомоморфизм π называется *изоморфизмом*, если π – изоморфизм соответствующих векторных пространств. В этом случае обратное отображение π^{-1} также является изоморфизмом представлений. Изоморфные представления называются иногда *эквива-*

лентными.

Замечание. Пусть $R := \Bbbk[G]$ групповая алгебра конечной группы G и пусть (V, ϕ) – некоторое представление G. Определим умножение $R \times V \to V$ следующим образом:

$$\left(\sum_{g\in G} \lambda_g e_g\right) \cdot x = \sum_{g\in G} \lambda_g \phi(g)(x), \qquad \sum_{g\in G} \lambda_g e_g \in R, \quad x \in V.$$

Тогда V становится левым модулем над R (проверьте!). Обратно, если векторное пространство V является левым модулем над R, то для любого $g \in G$ определен линейный оператор

$$\phi(g) : V \longrightarrow V, \qquad x \longmapsto e_g x.$$

Полученное отображение

$$\phi : G \to \mathrm{GL}(V), \qquad g \longmapsto \phi(g)$$

является представлением G. Таким образом, имеется взаимно однозначное соответствие между представлениями G и R-модулями (конечномерными над $\Bbbk$). При этом соответствии гомоморфизмам представлений соответствуют гомоморфизмы модулей.

Пусть (V, ϕ) – представление группы G. Зафиксировав базис $e_1, \ldots, e_n \in V$, мы можем записать все операторы $\phi(g)$ невы-

рожденными $n \times n$-матрицами. Мы получим *матричное представление* – гомоморфизм в группу $\phi : G \to \mathrm{GL}_n(\Bbbk)$. Гомоморфизм матричного представления $\phi_1 : G \to \mathrm{GL}_n(\Bbbk)$ в матричное представление $\phi_2 : G \to \mathrm{GL}_m(\Bbbk)$ задается $m \times n$-матрицей T (матрицей линейного отображения $\pi : V \to W$ в соответствующих базисах) такой, что $T\phi_1(g) = \phi_2(g)T$ для любого элемента $g \in G$. Матричные представления $\phi_1 : G \to \mathrm{GL}_n(\Bbbk)$ и $\phi_2 : G \to \mathrm{GL}_n(\Bbbk)$ изоморфны, если существует невырожденная $n \times n$-матрица такая, что $\phi_1(g) = T^{-1}\phi_2(g)T$ для любого $g \in G$.

Примеры. (1) Тривиальное представление – это гомоморфизм отображающий всю группу в тождественный оператор.

(2) Для конечной группы G рассмотрим векторное пространство V размерности $|G|$ с базисом e_g, $g \in G$ (занумерованным элементами группы). *Регулярным представлением* G называется представление, действующее на нашем базисе по правилу

$$\rho_{\mathrm{reg}}(h)(e_g) = e_{hg} \qquad \forall h \in G.$$

(По линейности действие продолжается на все V.) Например, регулярное представление циклической группы $G = \{1,\, a,\, a^2\}$ порядка 3 в базисе e_1, e_a, e_{a^2} задается мат-

рицами

$$a \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \qquad a^2 \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Имеется гомоморфизм (V, ρ_{reg}) в тривиальное одномерное представление, заданное формулой $\pi(\sum x_g e_g) = \sum x_g$.

(3) Симметрическая группа S_n имеет *перестановочное* представление $\rho_{\text{perm}} : \mathrm{S}_n \to \mathrm{GL}(V)$ в n-мерном пространстве V с базисом $e_1, \ldots, e_n$:

$$\rho_{\text{perm}}(\sigma)(e_i) = e_{\sigma(i)}.$$

Как и выше, имеется гомоморфизм (V, ρ_{perm}) в тривиальное одномерное представление, заданное формулой $\pi(\sum x_i e_i) = \sum x_i$.

(4) Одномерные представления – это гомоморфизмы в $\mathrm{GL}_1(\Bbbk) \simeq \Bbbk^*$. Одномерные представления изоморфны тогда и только тогда, когда они совпадают (как функции на G). Обозначим через $\mathrm{Hom}(G, \Bbbk^*)$ множество всех одномерных представлений группы G. Определим на $\mathrm{Hom}(G, \Bbbk^*)$ операцию умножения: для ϕ, $\phi' \in \hat{G}$ положим

$$\phi \cdot \phi' : G \longrightarrow \Bbbk^*, \quad g \longmapsto \phi(g)\phi'(g).$$

Ясно, что $\mathrm{Hom}(G, \Bbbk^*)$ – абелева группа относительно этой операции. Она называется *группой характеров*.

Определение. Пусть (V, ϕ) – представление группы G. Подпространство $W \subset V$ называется *инвариантным*, если $\phi(g)(x) \in W$ для любого элемента $g \in G$ и для любого вектора $x \in W$, т.е. подпространство W инвариантно относительно *всех* операторов $\phi(g)$, $g \in G$. В этом случае мы имеем представление $(W, \phi|_W)$

$$\phi|_W : G \to \mathrm{GL}(W), \qquad \phi|_W(g)(x) = \phi(g)(x) \quad \forall x \in W,$$

которое называется *подпредставлением*. Представление называется *неприводимым*, если у него нет нетривиальных подпредставлений. В противном случае представление называется *приводимым*.

Замечание. Для любого гомоморфизма представлений $\pi : (V, \phi) \to (W, \psi)$ его ядро и образ являются инвариантными подпространствами в V и W, соответственно (будет доказано позже). Соответствующие подпредставления (V, ϕ) и (W, ψ) называются ядром и образом π.

Замечание. Если мы выберем базис $e_1, \dots, e_m \in W$ и дополним до базиса $e_1, \dots, e_n \in V$ всего пространства, то в матричной записи матрицы $\phi(g)$ имеют угол нулей

$$\left(\begin{array}{c|c} A & * \\ \hline 0 & * \end{array}\right)$$

где A – матрица $\phi|_W(g)$ в базисе $e_1, \ldots, e_m$.

Пример. Любое нетривиальное подпредставление двумерного представления одномерно. Поэтому двумерное представление (V, ϕ) приводимо тогда и только тогда, когда существует вектор собственный для всех операторов $\phi(g)$.

Примеры. (1) Группа диэдра D_n по определению изоморфна подгруппе группы ортогональных матриц $\mathrm{O}_2(\mathbb{R})$. Таким образом, имеется стандартное представление $\phi : \mathrm{D}_n \hookrightarrow \mathrm{O}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})$. Ясно, что оно неприводимо при $n \geq 3$.

(2) Аналогично, группа кватернионов определяется вместе с вложением $\phi : \mathrm{Q}_8 \hookrightarrow \mathrm{GL}_2(\mathbb{C})$. Это представление также неприводимо.

Пример. Докажем, что любое неприводимое комплексное представление группы диэдра D_n имеет размерность ≤ 2. Пусть $\langle r \rangle \subset \mathrm{D}_n$ – подгруппа поворотов и пусть $s \in \mathrm{D}_n \setminus \langle r \rangle$ – некоторая симметрия. Пусть $\phi : \mathrm{D}_n \to \mathrm{GL}(V)$ – неприводимое комплексное представление размерности ≥ 2. Поскольку минимальный многочлен оператора $\phi(r)$ не имеет кратных корней, то $\phi(r)$ диагонализируем пространство V является прямой суммой собственных подпространств V_{ε_i}, где ε_i – корни степени n из 1. Так как $srs = r^{-1}$, то для $v \in V_{\varepsilon_i}$ имеем

$$\phi(r)\phi(s)(v) = \phi(s)\phi(r)^{-1}(v) = \varepsilon_i^{-1}\phi(s)(v),$$

т.е. $\phi(s)(v) \in V_{\varepsilon_i^{-1}}$. Отсюда видно, что подпространство $\langle v,\, \phi(s)(v)\rangle$, порожденное векторами v и $\phi(s)(v)$ является инвариантным. Из неприводимости представления (V, ϕ) получаем $\langle v,\, \phi(s)(v)\rangle = V$.

Одномерные представления

Будем говорить, что представление *комплексное* (соотв., *вещественное*), если основное поле $\Bbbk$ – это поле $\mathbb{C}$ (соотв., $\mathbb{R}$).

Теорема. (1) *Любое неприводимое комплексное представление абелевой группы одномерно.*

(2) *Число различных неприводимых комплексных представлений конечной абелевой группы равно ее порядку.*

Лемма. *Любое семейство попарно коммутирующих операторов $\mathscr{A}_\alpha \in \mathrm{GL}(V)$, $\alpha \in I$ в комплексном пространстве V имеет общий собственный вектор.*

Доказательство. Индукция по $n = \dim V$. База индукции $\dim V = 1$ очевидна. Предположим, что утверждение верно для всех пространств V размерности $< n$. Если все операторы $\mathscr{A}_\alpha$ скалярные, то утверждение очевидно. В противном случае существует $\mathscr{A}_\alpha$, не являющийся скалярным. Пусть λ – его собственное значение и пусть $V_\lambda \subset V$ – соответствующее собственное подпространство. Для любого $\mathscr{A}_\beta$ и любого $x \in V_\lambda$

имеем

$$\mathscr{A}_\alpha(\mathscr{A}_\beta(x)) = \mathscr{A}_\alpha \circ \mathscr{A}_\beta(x) = \mathscr{A}_\beta \circ \mathscr{A}_\alpha(x) = \mathscr{A}_\beta(\lambda x) = \lambda \mathscr{A}_\beta(x).$$

Таким образом, $\mathscr{A}_\beta(x) \in V_\lambda$, т.е. подпространство V_λ инвариантно относительно всех операторов $\mathscr{A}_\beta$. Согласно нашему выбору $\mathscr{A}_\alpha$ мы имеем $\dim V_\lambda < \dim V$ и по предположению индукции все операторы $\mathscr{A}_\beta$ имеют общий собственный вектор в V_λ. $\square$

Доказательство теоремы. Пусть G – абелева группа и пусть $\phi : G \to \mathrm{GL}(V)$ – ее неприводимое комплексное представление. Утверждение (1) следует из леммы, примененной к операторам $\phi(g)$, $g \in G$. Докажем (2). Для этого разложим группу G в произведение циклических: $G = G_1 \times \cdots \times G_r$, $G_i = \langle a_i \rangle$. Пусть $n_i := |G_i|$ и пусть $\varepsilon_i = \cos(2\pi/n_i) + \mathrm{i}\sin(2\pi/n_i)$ – первообразный корень степени n_i из 1. Для любого одномерного представления $\phi : G \to \mathbb{C}^*$ имеем $\phi(a_i)^{n_i} = \phi(a_i^{n_i}) = 1$. Поэтому $\phi(a_i) = \varepsilon_i^{s_i}$ для некоторых $0 \leq s_i < n_i$. Имеется r "базисных" представлений ϕ_i, заданных формулой

$$\phi_i(a_j) = \begin{cases} \varepsilon_i & \text{если } i = j, \\ 1 & \text{если } i \neq j. \end{cases}$$

т.е.

$$\phi_i(a_1^{k_1} \cdots a_r^{k_r}) = \varepsilon_i^{k_i}.$$

Поскольку $\mathrm{Hom}(G, \mathbb{C}^*)$ – абелева группа, то мы получаем также представления вида

$$\phi_1^{m_1} \cdots \phi_r^{m_r}.$$

Так как представление задается образами элементов a_i, то $\phi_1^{m_1} \cdots \phi_r^{m_r} = \phi \iff \phi_1^{m_1} \cdots \phi_r^{m_r}(a_i) = \phi(a_i)\ \forall i \iff \varepsilon_i^{m_i} = \varepsilon_i^{s_i}$ $\forall i \iff m_i \equiv s_i \mod n_i\ \forall i$. Таким образом, для представления $\phi_1^{m_1} \cdots \phi_r^{m_r}$ мы можем считать, что $0 \leq m_i < n_i\ \forall i$ и два представления $\phi_1^{m_1} \cdots \phi_r^{m_r}$ и $\phi_1^{m'_1} \cdots \phi_r^{m'_r}$, удовлетворяющие этому условию, совпадают тогда и только тогда, когда $(m_1, \ldots, m_r) = (m'_1, \ldots, m'_r)$. Мы получаем также, что различные представления $\phi_1^{m_1} \cdots \phi_r^{m_r}$ с $0 \leq m_i < n_i\ \forall i$ исчерпывают все одномерные представления группы G. Число таких представлений равно $n_1 \cdots n_r = |G|$. □

Замечание. Из доказательства теоремы следует, что для конечной абелевой группы G имеет место изоморфизм $G \simeq \mathrm{Hom}(G, \mathbb{C}^*)$. Однако этот изоморфизм не является каноническим.

Предложение. *Пусть G – группа и пусть $\rho : G \to \Bbbk^*$ – ее одномерное представление. Имеется разложение в композицию*

$$\rho : G \xrightarrow{\pi} G/G' \xrightarrow{\phi} \Bbbk^*,$$

где π – естественный гомоморфизм на факторгруппу, а ϕ – некоторое одномерное представление G/G'. Таким образом, имеется взаимно однозначное соответствие между одномерными представлениями групп G и G/G'.

Доказательство. Так как $\rho(G) \subset \Bbbk^*$ – абелева группа, то $\mathrm{Ker}(\rho) \supset G'$. Следовательно, равенство $\pi(g_1) = \pi(g_2)$ влечет $\rho(g_1) = \rho(g_2)$ и поэтому отображение $\phi : G/G' \to \Bbbk^*$, заданное формулой

$$\phi(x) = \rho(\pi^{-1}(x))$$

корректно определено. Это отображение является гомоморфизмом (т.е. одномерным представлением). Действительно, пусть $\pi(\bar{x}) = x$ и $\pi(\bar{y}) = y$. Тогда $\pi(\bar{x}\bar{y}) = xy$ и

$$\phi(xy) = \rho(\bar{x}\bar{y}) = \rho(\bar{x})\rho(\bar{y}) = \phi(x)\phi(y).$$

□

Следствие. *Пусть G – конечная группа. Тогда число ее различных комплексных одномерных представлений равно $[G : G']$.*

Доказательство. Число одномерных представлений G равно числу одномерных представлений G/G'. Последняя группа является абелевой и (для случая поля комплексных чисел) число ее одномерных представлений равно ее порядку. □

Пример. Любое одномерное представление простой (неабелевой) группы является тривиальным. Симметрическая группа S_n имеет ровно два одномерных представления (при $\mathrm{char}(\Bbbk) \neq 2$): тривиальное и $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\} \subset \Bbbk^*$.

Вполне приводимые представления

Определение. Пусть (V, ϕ) – представление группы G. Если пространство V является прямой суммой инвариантных подпространств V_1 и V_2, то говорят, что представление ϕ есть *прямая сумма* представлений $\phi|_{V_1}$ и $\phi|_{V_2}$. Это обозначается $\phi = \phi|_{V_1} \oplus \phi|_{V_2}$.

Если мы выберем базисы $e_1, \dots, e_m \in V_1$ и $e_{m+1}, \dots, e_n \in V_2$, то в матричной записи матрицы $\phi(g)$ имеют блочно-диагональный вид

$$\left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right)$$

где A_i – матрица $\phi_{V_i}(g)$ в соответствующем базисе.

Пример. Перестановочное представление $\rho_{\mathrm{perm}} : \mathrm{S}_n \to \mathrm{GL}(V)$, $\dim V = n$ симметрической группы раскладывается в прямую сумму: имеются инвариантные подпространства $\langle \sum e_i \rangle$ и $\{\sum \lambda_i e_i \mid \sum \lambda_i = 0\}$ и все пространство V – прямая сумма этих подпространств.

Определение. Представление (V, ϕ) называется *вполне приводимым*, если для каждого инвариантного подпространства $W \subset V$ существует дополнительное подпространство $W' \subset V$ такое, что $\phi = \phi|_W \oplus \phi|_{W'}$.

Легко видеть, что вполне приводимое представление является прямой суммой неприводимых.

Теорема (теорема Машке)**.** * *Пусть G – конечная группа и пусть характеристика поля $\Bbbk$ или равна нулю или не делит порядок группы. Тогда любое представление группы G в векторном пространстве над $\Bbbk$ вполне приводимо.*

Мы докажем эту теорему только в случае поля комплексных чисел $\mathbb{C}$. Тогда она является непосредственным следствием из следующих двух лемм.

Определение. Пусть V – эрмитово пространство с эрмитовой формой $\langle \cdot, \cdot \rangle$. Представление $\phi : G \to \mathrm{GL}(V)$ называется *унитарным*, если для любого элемента $g \in G$ оператор $\phi(g)$ унитарен, т.е.

$$\langle \phi(g)(x),\, \phi(g)(y) \rangle = \langle x,\, y \rangle \qquad \forall x,\, y \in V.$$

Аналогично, для евклидова пространства определяется понятие *ортогонального* представления.

Лемма. *Унитарное представление является вполне приводимым.*

Доказательство. Пусть (V, ϕ) – унитарное представление группы G и пусть $W \subset V$ – инвариантное подпространство. Проверим, что его ортогональное дополнение $W^\perp \subset V$ также инвариантно. Действительно, пусть $x \in W^\perp$. Тогда $\langle x, y \rangle = 0$

*Heinrich Maschke – немецкий математик (1853 – 1908)

$\forall y \in W$. Поскольку подпространство W инвариантно, то для $\forall y \in W$ вектор $z := \phi(g)(y)$ также содержится в W $\forall g \in G$. Следовательно, $\forall z \in W$ $\forall g \in G$ имеем

$$0 = \langle x, \phi(g)^{-1}(z)\rangle = \langle \phi(g)(x), \phi(g) \circ \phi(g)^{-1}(z)\rangle,$$

т.е. $\phi(g)(x) \in W^{\perp}$. Таким образом, подпространство $W^{\perp} \subset V$ инвариантно. Так как $V = W \oplus W^{\perp}$, то это доказывает утверждение. □

Лемма. *Пусть $\phi : G \to \mathrm{GL}(V)$ – комплексное представление конечной группы. Тогда существует эрмитова форма $\langle \cdot, \cdot \rangle$ на V такая, что ϕ унитарно относительно этой формы.*

Доказательство. Пусть $(\ ,\ )$ – любая эрмитова форма на V. Положим

$$\langle x, y\rangle = \frac{1}{|G|} \sum_{h \in G} (\phi(h)(x), \phi(h)(y)).$$

Проверяем, что $\langle \cdot, \cdot \rangle$ – эрмитова форма на V:

$$\langle x_1 + x_2, y\rangle = \frac{1}{|G|} \sum_{h \in G} \big(\phi(h)(x_1 + x_2),\, \phi(h)(y)\big) =$$

$$= \frac{1}{|G|} \sum_{h \in G} \Big(\big(\phi(h)(x_1), \phi(h)(y)\big) + \big(\phi(h)(x_2),\, \phi(h)(y)\big)\Big) =$$

$$= \frac{1}{|G|} \sum_{h \in G} \big(\phi(h)(x_1),\, \phi(h)(y)\big) + \frac{1}{|G|} \sum_{h \in G} \big(\phi(h)(x_2),\, \phi(h)(y)\big) =$$

$$= \langle x_1,\, y\rangle + \langle x_2,\, y\rangle,$$

$$\langle \lambda x,\, y\rangle = \frac{1}{|G|}\sum_{h\in G}(\phi(h)(\lambda x),\, \phi(h)(y)) =$$

$$= \frac{1}{|G|}\sum_{h\in G}\lambda(\phi(h)(x),\, \phi(h)(y)) = \lambda\langle x,\, y\rangle,$$

$$\langle y,\, x\rangle = \frac{1}{|G|}\sum_{h\in G}(\phi(h)(y),\, \phi(h)(x)) =$$

$$= \frac{1}{|G|}\sum_{h\in G}\overline{(\phi(h)(x),\, \phi(h)(y))} = \overline{\langle x,\, y\rangle}.$$

Так как $(\phi(h)(x),\, \phi(h)(x)) \geq 0$ для любого $h \in G$, то

$$\langle x,\, x\rangle = \frac{1}{|G|}\sum_{h\in G}(\phi(h)(x),\, \phi(h)(x)) \geq 0.$$

Более того, равенство $\langle x,\, x\rangle = 0$ влечет $(\phi(h)(x),\, \phi(h)(x)) = 0$ и, следовательно, $x = 0$.

Наконец, проверим унитарность операторов $\phi(g)$ относительной новой эрмитовой формы:

$$\langle \phi(g)(x),\, \phi(g)(y)\rangle = \frac{1}{|G|}\sum_{h\in G}(\phi(h)(\phi(g)(x)),\, \phi(h)(\phi(g)(y))) =$$

$$= \frac{1}{|G|}\sum_{h\in G}(\phi(hg)(x),\, \phi(hg)(y)) = \frac{1}{|G|}\sum_{s\in G}(\phi(s)(x),\, \phi(s)(y)) =$$

$$= \langle x,\, y\rangle.$$

□

Замечание. Дословно повторяя предыдущие рассуждения с заменой слова “унитарное” на “ортогональное”, получим доказательство теоремы Машке для случая $\Bbbk = \mathbb{R}$.

Следующие примеры показывают, что условия теоремы Машке нельзя ослабить.

Примеры. (1) Бесконечная циклическая группа $G = \mathbb{Z}$ имеет представление

$$\phi : \mathbb{Z} \longrightarrow \mathrm{GL}_2(\Bbbk), \quad n \longmapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Это представление не является вполне приводимым: одномерное подпространство, порожденное первым базисным вектором, является инвариантным, но не имеет инвариантного прямого дополнения.

(2) Аналогично, над полем $\Bbbk$ характеристики $p > 0$ представление

$$\phi : \mathbb{Z}_p \longrightarrow \mathrm{GL}_2(\Bbbk), \quad n \longmapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

не является вполне приводимым.

Приведем еще несколько примеров построения новых представлений.

Примеры. Пусть (V, ϕ) – представление группы G.

(1) Пусть $V^\vee$ – двойственное к V пространство (пространство функционалов). Представление $(V^\vee, \phi^\vee)$

$$\phi^\vee(g)(f) = f \circ \phi(g)^{-1}, \qquad f \in V^\vee$$

называется *двойственным* представлением. Матрицей оператора $\phi^\vee(g)$ в двойственном базисе будет транспонированная матрица оператора $\phi(g)^{-1}$.

(2) Пусть $\varphi : G_1 \to G$ – гомоморфизм групп. Тогда композиция $(V, \phi \circ \varphi)$ является представлением G_1. В частности, если $G_1 = G$, то $(V, \phi \circ \varphi)$ – представление G. Если $\varphi : G \to G$ внутренний автоморфизм, то представления (V, ϕ) и $(V, \phi \circ \varphi)$ изоморфны.

(3) Композиция с определителем $\det \circ \phi : G \to \Bbbk^*$ является одномерным представлением G.

19 Характеры представлений

Определение. *Характером* представления $\phi : G \to \mathrm{GL}(V)$ называется функция

$$\chi_\phi : G \to \Bbbk, \qquad g \longmapsto \operatorname{Tr} \phi(g),$$

где $\operatorname{Tr} \mathscr{A}$ – след оператора $\mathscr{A}$.

Предложение (свойства характеров)**.** *Пусть (V, ϕ) – представление группы G над полем $\Bbbk$. Тогда*

(1) $\chi_\phi(1) = \dim V$;

(2) $\chi_\phi(hgh^{-1}) = \chi_\phi(g) \quad \forall h,\, g \in G$;

(3) *если группа G конечна и $\Bbbk = \mathbb{C}$, то* $\chi_\phi(g^{-1}) = \overline{\chi_\phi(g)} \quad \forall g \in G$.

Пусть (V_1, ϕ_1) и (V_2, ϕ_2)– два представления одной и той же группы G.

(4) $\chi_{\phi_1 \oplus \phi_2} = \chi_{\phi_1} + \chi_{\phi_2}$.

(5) *Если представления ϕ_1 и ϕ_2 изоморфны, то* $\chi_{\phi_1} = \chi_{\phi_2}$.

Доказательство. Утверждение (1) очевидно, а (2) следует из соотношения

$$\chi_\phi(hgh^{-1}) = \operatorname{Tr} \phi(hgh^{-1}) = \operatorname{Tr}\Big(\phi(h)\phi(g)\phi(h)^{-1}\Big) = \operatorname{Tr} \phi(g) = \chi_\phi(g).$$

Для доказательства (3) заметим, что для элемента $g \in G$ порядка m минимальный многочлен оператора $\phi(g)$ делит $t^m - 1$. В частности, этот многочлен не имеет кратных корней. Следовательно, оператор $\phi(g)$ диагонализируем: существует базис пространства V, в котором матрица $\phi(g)$ имеет диагональный вид с диагональными элементами $\varepsilon_1, \ldots, \varepsilon_n$ – корнями степени m из 1. Поэтому

$$\chi_\phi(g^{-1}) = \operatorname{Tr} \phi(g^{-1}) = \sum \varepsilon_i^{-1} = \sum \overline{\varepsilon_i} = \overline{\operatorname{Tr} \phi(g)} = \overline{\chi_\phi(g)}.$$

Утверждение (4) следует из матричного представления $\phi_1 \oplus \phi_2$. Наконец, для доказательства (5) запишем $\phi_2(g) = T^{-1}\phi_1(g)T$ (для некоторой невырожденной матрицы T). Отсюда

$$\chi_{\phi_2}(g) = \operatorname{Tr} \phi_2(g) = \operatorname{Tr}\Big(T^{-1}\phi_1(g)T\Big) = \operatorname{Tr} \phi_1(g) = \chi_{\phi_1}(g).$$

□

Напомним, что гомоморфизм представления (V, ϕ) в представление (W, ψ) – это линейное отображение $\pi : V \to W$ такое, что для любого элемента $g \in G$ диаграмма

$$\begin{array}{ccc} V & \xrightarrow{\pi} & W \\ {\scriptstyle \phi(g)}\downarrow & & \downarrow{\scriptstyle \psi(g)} \\ V & \xrightarrow{\pi} & W \end{array}$$

коммутативна (т.е. $\psi(g) \circ \pi = \pi \circ \phi(g)$).

Теорема (лемма Шура)**.** * *Пусть* (V, ϕ) *и* (W, ψ) *– непри-*

*Issai Schur – немецкий и израильский математик (1875 – 1941)

водимые комплексные представления группы G *и пусть* $\pi : (V, \phi) \to (W, \psi)$ *– гомоморфизм представлений.*

(1) *Если* $\phi \not\simeq \psi$, *то* $\pi = 0$.

(2) *Если* $\phi \simeq \psi$ *и* $\pi \neq 0$, *то* π *– изоморфизм.*

(3) *Более того, если* $V = W$ *и* $\phi = \psi$, *то* $\pi = \lambda \mathscr{E}$.

Доказательство. Положим $K := \mathrm{Ker}(\pi)$. Докажем, что подпространство $K \subset V$ инвариантно для любого оператора $\phi(g)$. Действительно, пусть $x \in K$. Тогда $\pi(x) = 0$ и

$$0 = \psi(g) \circ \pi(x) = \pi \circ \phi(g)(x) = \pi(\phi(g)(x)),$$

т.е. $\phi(g)(x) \in K$.

Если $K = V$, то $\pi = 0$ и все доказано. Предположим, что $K \neq V$. Поскольку представление ϕ неприводимо, то $K = \{0\}$, т.е. отображение π инъективно. Положим $U := \pi(V)$. Докажем, что подпространство $U \subset W$ инвариантно для любого оператора $\psi(g)$. Действительно, пусть $y \in U$. Тогда $y = \pi(x)$ для некоторого $x \in V$. Имеем

$$\psi(g)(y) = \psi(g) \circ \pi(x) = \pi \circ \phi(g)(x) = \pi(x'), \quad x' := \phi(g)(x).$$

Таким образом, $\psi(g)(y) \in U$, т.е. U инвариантно. Поскольку представление ψ неприводимо и $U \neq \{0\}$, то $U = W$, т.е. π – изоморфизм. Это доказывает (1) и (2).

Для доказательства (3) положим $\pi' := \pi - \lambda\mathscr{E}$, где λ – собственное значение оператора π. Заметим, что это новое π' удовлетворяет условию $\psi(g) \circ \pi' = \pi' \circ \phi(g)$ теоремы. Применим (2) к π'. Так как π' – не является изоморфизмом, то $\pi' = 0$. □

Начиная с этого места все представления – это *комплексные* представления некоторой *конечной* группы G.

Следствие. *Пусть* (V, ϕ) *и* (W, ψ) *– неприводимые представления конечной группы* G *и пусть* $\pi : V \to W$ *– любое линейное отображение. Рассмотрим линейное отображение* $\pi' : V \to W$ *заданное формулой*

$$\pi' = \frac{1}{|G|} \sum_{g \in G} \psi(g) \pi \phi(g)^{-1}.$$

(1) *Если* $\phi \not\simeq \psi$, *то* $\pi' = 0$.

(2) *Если* $V = W$ *и* $\phi = \psi$, *то* $\pi' = \lambda\mathscr{E}$, *где* $\lambda = \mathrm{Tr}(\pi)/\dim V$.

Доказательство. Для того, чтобы применить лемму Шура к π' сравним отображения $\psi(h) \circ \pi'$ и $\pi' \circ \phi(h)$, $h \in G$:

$$\psi(h) \circ \pi' = \frac{1}{|G|} \sum_{g \in G} \psi(h)\psi(g)\pi\phi(g)^{-1} = \frac{1}{|G|} \sum_{g \in G} \psi(hg)\pi\phi(g)^{-1},$$

$$\pi' \circ \phi(h) = \frac{1}{|G|} \sum_{g \in G} \psi(g) \pi \phi(g)^{-1} \phi(h) = \frac{1}{|G|} \sum_{g \in G} \psi(g) \pi \phi(h^{-1} g)^{-1} = \\ = \frac{1}{|G|} \sum_{s \in G} \psi(hs) \pi \phi(s)^{-1}.$$

Таким образом,

$$\psi(h) \circ \pi' = \pi' \circ \phi(h)$$

и по лемме Шура мы имеем (1) и утверждение $\pi' = \lambda \mathscr{E}$ в (2). Для доказательства последнего утверждения запишем

$$\lambda \dim V = \mathrm{Tr}(\lambda \mathscr{E}) = \mathrm{Tr}(\pi') = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\Big(\phi(g) \pi \phi(g)^{-1}\Big) = \mathrm{Tr}(\pi).$$

□

Следствие (матричная форма)**.** *Пусть* $\phi : G \to \mathrm{GL}_n(\mathbb{C})$ *и* $\psi : G \to \mathrm{GL}_m(\mathbb{C})$ *– неприводимые матричные представления конечной группы* G*. Запишем:*

$$\phi(g) = (b_{i,j}(g)), \qquad \psi(g) = (a_{i,j}(g)).$$

Тогда если $\phi \not\simeq \psi$*, то*

$$(*) \qquad \sum_{g \in G} a_{i,i_0}(g) b_{j_0,j}(g^{-1}) = 0$$

Если же $\phi = \psi$*,* $n = m$*,* $b_{i,j}(g) = a_{i,j}(g)$*, то*

$$(**) \qquad \frac{1}{|G|} \sum_{g \in G} a_{i,i_0}(g) a_{j_0,j}(g^{-1}) = \frac{\delta_{i,j} \delta_{i_0,j_0}}{n}.$$

Доказательство. Применим предыдущее следствие к отображению $\pi : \mathbb{C}^n \to \mathbb{C}^m$, которое задается матрицей $C = (c_{i,j})$, где

$$c_{i,j} = \begin{cases} 1 & \text{если } i = i_0,\ j = j_0, \\ 0 & \text{в противном случае.} \end{cases}$$

Тогда π', задается матрицей $C' = (c'_{i,j})$, где

$$c'_{i,j} = \frac{1}{|G|} \sum_{g \in G} \sum_{k,\, l} a_{i,k}(g) c_{k,l} b_{l,j}(g^{-1}) = \sum_{g \in G} a_{i,i_0}(g) b_{j_0,j}(g^{-1}).$$

Если $\phi \not\simeq \psi$, то $c'_{i,j} = 0$ и мы получаем $(*)$ по предыдущему следствию. В случае $b_{i,j}(g) = a_{i,j}(g)$ матрица C' должна быть скалярной, на диагонали которой стоят элементы

$$\frac{\operatorname{Tr}(\pi)}{\dim V} = \frac{\delta_{i_0,j_0}}{n}.$$

Это и доказывает $(**)$. □

Определение. Функция $f : G \to \Bbbk$ называется *центральной*, если она постоянна на классах сопряженных элементов: $f(hgh^{-1}) = f(g) \quad \forall h,\, g \in G$.

Обозначим через $\mathfrak{X}(G)$ множество всех центральных функций на G со значениями в $\mathbb{C}$. Ясно, что $\mathfrak{X}(G)$ является векторным пространством над $\mathbb{C}$, размерность которого равна числу

классов сопряженных элементов в G. Характеры представлений лежат в $\mathfrak{X}(G)$. Для $f_1\ f_2 \in \mathfrak{X}(G)$ положим

$$(f_1, f_2) = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

Несложно проверяется, что $(\ ,\ )$ – эрмитова форма на $\mathfrak{X}(G)$.

Теорема (соотношения ортогональности)**.** *Пусть* (V, ϕ) *и* (W, ψ) *– неприводимые представления конечной группы* G*. Тогда*

$$(\chi_\psi,\, \chi_\phi) = \begin{cases} 1 & \text{если } \phi \simeq \psi, \\ 0 & \text{если } \phi \not\simeq \psi. \end{cases}$$

Таким образом, характеры неприводимых представлений образуют *ортонормированную систему* в $\mathfrak{X}(G)$. Позднее мы покажем, что они образуют *ортонормированный базис* в $\mathfrak{X}(G)$.

Доказательство. Запишем представления в матричном виде: $\phi(g) = (b_{i,j}(g)), \quad \psi(g) = (a_{i,j}(g))$. Тогда $\chi_\phi(g) = \sum_i b_{i,j}(g)$, $\chi_\psi(g) = \sum_i a_{i,j}(g)$. Если $\phi \not\simeq \psi$, то соотношение $(*)$ для $i_0 = i$, $j_0 = j$ дает нам

$$0 = \sum_{g \in G} \sum_{i,j} a_{i,i}(g) b_{j,j}(g^{-1}) = \sum_{g \in G} \left(\sum_i a_{i,i}(g) \right) \left(\sum_j b_{j,j}(g^{-1}) \right) = \\ = \sum_{g \in G} \chi_\psi(g) \chi_\phi(g^{-1}) = |G|\ (\chi_\psi,\, \chi_\phi).$$

Пусть $\phi = \psi$. Воспользуемся $(**)$ для $i_0 = i$, $j_0 = j$:

$$1 = \sum_{i,j} \frac{\delta_{i,j}}{\dim V} = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} a_{i,i}(g) a_{j,j}(g^{-1}) =$$

$$= \frac{1}{|G|} \sum_{g \in G} \left(\sum_i a_{i,i}(g) \right) \left(\sum_j a_{j,j}(g^{-1}) \right) =$$

$$= \frac{1}{|G|} \sum_{g \in G} (\chi_\phi(g),\, \chi_\phi(g^{-1})) = (\chi_\phi,\, \chi_\phi).$$

□

Следствие. *Пусть (V, ϕ) – представление конечной группы G и пусть*

$$\phi = \bigoplus_i m_i \phi_i$$

– его разложение в прямую сумму различных неприводимых, где m_i – кратность вхождения ϕ_i в эту сумму. Тогда

$$(\chi_\phi,\, \chi_{\phi_j}) = m_j.$$

Доказательство. Так как $\chi_\phi = \sum m_i \chi_{\phi_i}$, то

$$(\chi_\phi,\, \chi_{\phi_j}) = \left(\sum_i m_i \chi_{\phi_i},\, \chi_{\phi_j} \right) = \sum_i m_i (\chi_{\phi_i},\, \chi_{\phi_j}) = m_j.$$

□

Следствие. *Пусть* (V, ϕ) *и* (V', ϕ') *– представления конечной группы* G*. Тогда*

$$(V, \phi) \simeq (V', \phi') \quad \Longleftrightarrow \quad \chi_\phi = \chi_{\phi'}.$$

Задача. Найдите условие при котором представление и двойственное к нему представление конечной группы изоморфны. Приведите примеры, когда они не изоморфны.

Следствие. *Пусть* (V, ϕ) *– представление конечной группы* G*. Тогда число и кратности представлений в разложении* ϕ *в прямую сумму неприводимых не зависит от способа разложения.*

Следствие. *Пусть* (V, ϕ) *– представление конечной группы* G *и пусть*

$$\phi = \bigoplus_i m_i \phi_i$$

– его разложение в прямую сумму различных неприводимых. Тогда

$$(\chi_\phi,\, \chi_\phi) = \sum_j m_j^2.$$

В частности, ϕ *неприводимо тогда и только тогда, когда* $(\chi_\phi,\, \chi_\phi) = 1$*.*

Теорема. *Любое неприводимое представление* ϕ_i *появляется в разложении регулярного представления в прямую сумму*

неприводимых

$$\rho_{\mathrm{reg}} = \bigoplus_i m_i \phi_i,$$

причем кратность вхождения ϕ_i в ρ_{reg} равна его степени:

$$m_i = \deg \phi_i.$$

Доказательство. В стандартном базисе регулярного представления все матрицы $\rho_{\mathrm{reg}}(g)$ имеют нули на главной диагонали при $g \neq 1$. Поэтому

$$\chi_{\rho_{\mathrm{reg}}} = \begin{cases} 0 & \text{если } g \neq 1, \\ |G| & \text{если } g = 1. \end{cases}$$

и, таким образом,

$$(\chi_{\rho_{\mathrm{reg}}},\, \chi_{\phi_i}) = \frac{1}{|G|} \cdot |G| \deg \phi_i = \deg \phi_i.$$

□

Следствие. *Число попарно неизоморфных неприводимых представлений конечной группы конечно.*

Следствие. *Пусть G – конечная группа и пусть $\phi_1, \ldots, \phi_r$ – все ее различные (попарно неизоморфные) неприводимые представления. Тогда*

$$|G| = \sum_i (\deg \phi_i)^2.$$

Теорема. *Число попарно неизоморфных неприводимых представлений конечной группы G равно числу ее классов сопряженных элементов.*

Лемма. *Пусть G – конечная группа, пусть $f : G \to \mathbb{C}$ – центральная функция и пусть (V, ϕ) – некоторое представление G. Рассмотрим оператор*

$$\pi := \sum_{g \in G} \overline{f(g)} \phi(g).$$

Если представление ϕ неприводимо, то $\pi = \lambda \mathscr{E}$, где

$$\lambda = \frac{(\chi_\phi,\, f) \cdot |G|}{\dim V}.$$

Доказательство. Сравним отображения $\phi(h) \circ \pi$ и $\pi \circ \phi(h)$, $h \in G$:

$$\phi(h) \circ \pi = \sum_{g \in G} \overline{f(g)} \phi(h)\phi(g) = \sum_{g \in G} \overline{f(g)} \phi(hg),$$

$$\pi \circ \phi(h) = \sum_{g \in G} \overline{f(g)} \phi(g)\phi(h) = \sum_{g \in G} \overline{f(g)} \phi(gh),$$

Положим $g' := h^{-1}gh$. Тогда $g = hg'h^{-1}$ и поэтому

$$\pi \circ \phi(h) = \sum_{g \in G} \overline{f(hg'h^{-1})} \phi(hg') = \sum_{g' \in G} \overline{f(g')} \phi(hg') = \phi(h) \circ \pi.$$

По лемме Шура $\pi = \lambda\mathscr{E}$. Наконец,

$$\lambda \dim V = \operatorname{Tr}(\lambda\mathscr{E}) = \operatorname{Tr}(\pi) = \sum_{g\in G} \overline{f(g)} \operatorname{Tr}(\phi(g)) = |G| \cdot (\chi_\phi,\, f).$$

□

Предложение. *Характеры неприводимых представлений конечной группы G образуют (ортонормированный) базис пространства $\mathfrak{X}(G)$.*

Доказательство. Пусть $\phi_1, \ldots, \phi_r$ – все неприводимые представления G, $\chi_1, \ldots, \chi_r$ – их характеры и пусть $f \in \mathfrak{X}(G)$. Предположим, что $(\chi_i,\, f) = 0$ для всех i. Для ϕ_i и для ρ_{reg} рассмотрим операторы как в лемме:

$$\pi_i := \sum_{g\in G} \overline{f(g)}\phi_i(g), \qquad \pi_{\text{reg}} := \sum_{g\in G} \overline{f(g)}\rho_{\text{reg}}(g).$$

По лемме и нашему предположению $\pi_i = 0$. Так как $\rho_{\text{reg}} = \sum m_i\phi_i$, где $m_i = \deg\phi_i$, то

$$\pi_{\text{reg}} = \sum_{g\in G} \overline{f(g)} \left(\sum_i m_i\phi_i \right) = \sum m_i\pi_i = 0.$$

С другой стороны,

$$\pi_{\text{reg}}(e_1) = \sum_{g\in G} \overline{f(g)}\rho_{\text{reg}}(g)(e_1) = \sum_{g\in G} \overline{f(g)}e_g.$$

Следовательно, $f = 0$. □

Доказательство теоремы. Следует из предложения и того, что $\dim \mathfrak{X}(G) = |G|$. $\square$

Очень важной характеристикой конечной группы является ее таблица характеров – квадратная таблица, столбцы которой соответствуют классам сопряженных элементов, а строки – различным неприводимым представлениям. Элементы таблицы – значения характеров соответствующих представлений на классах сопряженных элементов.

Пример. Найдем все неприводимые комплексные представления группы кватернионов Q_8 и построим ее таблицу характеров. Так как $\mathrm{Q}_8' = \{\pm \mathbf{1}\}$ и $\mathrm{Q}_8 \,/\, \mathrm{Q}_8' \simeq \{\pm 1\} \times \{\pm 1\}$, то Q_8 имеет ровно четыре одномерных представления. Они задаются следующей таблицей

	$\pm\mathbf{1}$	$\pm\mathbf{i}$	$\pm\mathbf{j}$	$\pm\mathbf{k}$
ϕ_0	1	1	1	1
ϕ_1	1	-1	1	-1
ϕ_2	1	1	-1	-1
ϕ_3	1	-1	-1	1

Так как $8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2$ – единственно возможное разложение порядка группы в сумму квадратов, из которых ровно четыре равны 1, то имеется ровно одно неприводимое представление ϕ размерности 2 (и нет представлений высшей

размерности). Представление ϕ – это стандартное вложение $\mathrm{Q}_8 \hookrightarrow \mathrm{GL}_2(\mathbb{C})$, фигурирующее в определении группы Q_8. Таблица характеров выглядит следующим образом:

	$\{\mathbf{1}\}$	$\{-\mathbf{1}\}$	$\{\mathbf{i}, -\mathbf{i}\}$	$\{\mathbf{j}, -\mathbf{j}\}$	$\{\mathbf{k}, -\mathbf{k}\}$
ϕ_0	1	1	1	1	1
ϕ_1	1	1	-1	1	-1
ϕ_2	1	1	1	-1	-1
ϕ_3	1	1	-1	-1	1
ϕ	2	-2	0	0	0

Задача. Для перестановочного представления $(V, \rho_{\mathrm{perm}})$ симметрической группы S_n имеем

$$\chi_{\rho_{\mathrm{perm}}}(\sigma) = |\{i \mid \sigma(i) = i\}|$$

(число неподвижных элементов подстановки). Вывести отсюда, что ρ_{perm} – прямая сумма *двух* неприводимых представлений: $\rho_{\mathrm{perm}} = 1 \oplus \rho'_{\mathrm{perm}}$, где 1 обозначает одномерное тривиальное представление на $\langle \sum e_i \rangle$, а ρ'_{perm} – неприводимое $(n-1)$-мерное представление в ортогональном дополнении.

Для $n = 3$ представление ρ'_{perm} – представление возникающее из изоморфизма между S_3 и группой диэдра $\mathrm{D}_3 \subset \mathrm{O}_3(\mathbb{R})$, а при $n = 4$ представление ρ'_{perm} – представление возникающее из изоморфизма между S_4 и группой движений тетраэдра.

Пример. Найдем все неприводимые комплексные представления симметрической группы S_4 и построим ее таблицу характеров. Согласно последней теореме их ровно пять. Так как $\mathrm{S}_4' = \mathrm{A}_4$ и $[\mathrm{S}_4 : \mathrm{A}_4] = 2$, то два представления 1 и sgn (знак подстановки) исчерпывают все одномерные представления. Трехмерное представление ρ'_{perm} неприводимо (см. выше). Поэтому неприводимо также и представление $\mathrm{sgn} \cdot \rho'_{\mathrm{perm}}$. Эти два представления не изоморфны: определители $\rho'_{\mathrm{perm}}(\sigma)$ и $\mathrm{sgn}(\sigma) \cdot \rho'_{\mathrm{perm}}(\sigma)$ различны для нечетных подстановок σ. Отметим, что $\mathrm{sgn}(\sigma) \cdot \rho'_{\mathrm{perm}}(\sigma)$ – представление возникающее из изоморфизма между S_4 и группой собственных движений куба. Наконец, поскольку сумма квадратов степеней неприводимых представлений конечной группы равна ее порядку, то оставшееся неприводимое представление двумерно. Оно является композицией

$$\phi_2 : \mathrm{S}_4 \xrightarrow{\pi} \mathrm{S}_4 \,/\, \mathrm{V}_4 \simeq \mathrm{S}_3 \xrightarrow{\rho'_{\mathrm{perm}}} \mathrm{GL}_2(\mathbb{C}).$$

Таблица характеров выглядит следующим образом:

	(1)	$\{(i,j)(k,l)\}$	$\{(i,j,k)\}$	$\{(i,j)\}$	$\{(i,j,k,l)\}$
1	1	1	1	1	1
sgn	1	1	1	-1	-1
ϕ_2	2	2	-1	0	0
ρ'_{perm}	3	-1	0	1	-1
$\mathrm{sgn} \cdot \rho'_{\mathrm{perm}}$	3	-1	0	-1	1

Задача. Опишите все неприводимые комплексные представления группы диэдра D_n.