АЛГЕБРА-3

ПРОХОРОВ
ЮРИЙ ГЕННАДЬЕВИЧ

—

МЕХМАТ МГУ

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

Алгебра

Семестр 3

Ю. Г. Прохоров

Последнее обновление: 25 января 2023 г.

Москва

2022

Оглавление

0 Вводная лекция **3**
- 0.1 Группы, подгруппы, теорема Лагранжа . . . 3
- 0.2 Теорема о гомоморфизме . . . 6
- 0.3 Прямые произведения групп . . . 11

1 Абелевы группы **16**
- 1.1 Свободные абелевы группы. . . . 16

2 Строение конечно порожденных абелевых групп **27**
- 2.1 Дискретные подгруппы в $\mathbb{R}^n$ . . . 30

3 Действия групп **32**
- 3.1 Действия групп . . . 32
- 3.2 Примеры действий . . . 33
- 3.3 p-группы. . . . 36
- 3.4 Теоремы Силова . . . 37

4 Разрешимые группы **42**
- 4.1 Коммутант . . . 42
- 4.2 Разрешимые группы . . . 43

5 Полупрямые произведения групп **47**

6 Простые группы **51**
- 6.1 Композиционный ряд группы . . . 51
- 6.2 Простота знакопеременных групп . . . 52
- 6.3 Простота проективных линейных групп . . . 54
- 6.4 Простота специальной ортогональной группы . . . 56

7 Кольца, идеалы, модули, гомоморфизмы **59**
- 7.1 Кольца . . . 59
- 7.2 Простота кольца матриц . . . 62
- 7.3 Модули над кольцами . . . 63

8 Коммутативные кольца **67**
- 8.1 Простые и максимальные идеалы. . . . 67
- 8.2 Кольца главных идеалов . . . 68
- 8.3 Модули над кольцами главных идеалов . . . 70

8.4 Китайская теорема об остатках 75

9 Поля. Расширения полей **79**
9.1 Простые поля 79
9.2 Расширения полей 80
9.3 Целые расширения колец 83

10 Расширения полей **86**
10.1 Присоединение к полю корня неприводимого многочлена 86
10.2 Поле разложения многочлена 87
10.3 Конструкция алгебраического замыкания поля 88

11 Конечные поля **91**
11.1 Отображение Фробениуса 91
11.2 Строение конечных полей 92
11.3 Автоморфизмы конечных полей 94
11.4 Группа обратимых элементов кольца вычетов 95

12 Алгебры над полем **98**
12.1 Определение алгебр 98
12.2 Конечномерные алгебры с делением 100
12.3 Конечные ассоциативные кольца с делением 101

13 Алгебра кватернионов **104**
13.1 Определение алгебры кватернионов 104
13.2 Алгебры с делением над $\mathbb{R}$. Теорема Фробениуса 105
13.3 Свойства алгебры кватернионов 106
13.4 Гомоморфизм $\mathrm{SU}_2 \to \mathrm{SO}_3$ 108

14 Сепарабельные расширения полей **112**
14.1 Сепарабельные расширения 112
14.2 Совершенные поля 115
14.3 Теорема о примитивном элементе 116

15 Нормальные расширения **119**
15.1 Продолжение автоморфизмов 119
15.2 Нормальные расширения полей 120
15.3 Автоморфизмы расширений 121
15.4 Расширения Галуа 121

16 Теория Галуа **125**
16.1 Основная теорема теории Галуа 125
16.2 Классические геометрические задачи 127
16.3 Разрешимость алгебраических уравнении в радикалах 131

17 Трансцендентные расширения полей **136**

Лекция 0

Вводная лекция

В этой лекции мы напомним некоторый материал первого семестра.

0.1 Группы, подгруппы, теорема Лагранжа

Определение. *Группой* называется непустое множество G с операцией

$$G \times G \longrightarrow G, \qquad (a, b) \longmapsto a \circ b,$$

удовлетворяющей следующим свойствам:

- $a \circ (b \circ c) = (a \circ b) \circ c$ для любых элементов a, b, $c \in G$ (закон ассоциативности);
- существует выделенный элемент $1 \in G$, называемый *единичным* (или *нейтральным*) такой, что $a \circ 1 = 1 \circ a = a$ для любого $a \in G$;
- для любого $a \in G$ существует элемент $a^{-1} \in G$ называемый *обратным* такой, что $a \circ a^{-1} = a^{-1} \circ a = 1$.

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

- $a \circ b = b \circ a$ для любых элементов a, $b \in G$.

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.

Приведем стандартные примеры групп. Эти обозначения будут использоваться на протяжении всего курса.

Примеры. (i) Если $\Bbbk$ – поле (например, $\Bbbk = \mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$), то множество всех ненулевых элементов $\Bbbk$ является группой по умножению, которую мы будем обозначать $\Bbbk^*$. Множество всех элементов $\Bbbk$ является группой по сложению. Эту группу мы будем обозначать $\Bbbk^+$.

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

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

(iv) 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

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

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

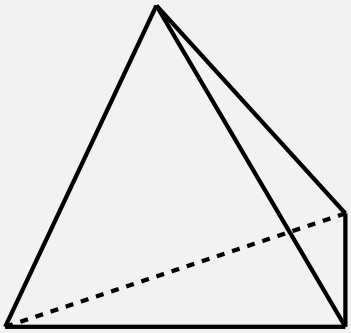
(vi) $\mathbb{Z}/n\mathbb{Z}$ – группа классов вычетов (с операцией сложения).

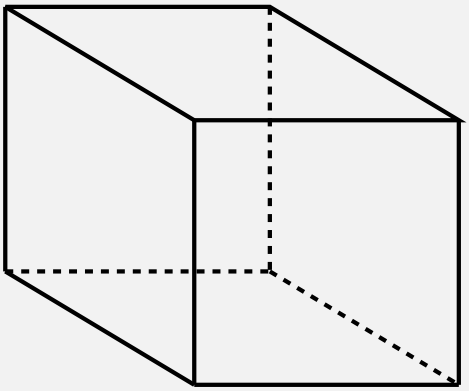
(vii) Отображение аффинного пространства $\mathbb{A}^n_{\Bbbk}$ в себя называется называется аффинным преобразованием, если образ любой прямой – прямая. Все аффинные преобразования $\mathbb{A}^n_{\Bbbk}$ образуют *группу аффинных преобразований* $\mathrm{Aff}_n(\Bbbk)$. Она содержит подгруппу параллельных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

(viii) Отображение евклидова пространства $\mathbb{E}^n$ в себя называется называется движением, если оно сохраняет расстояния. Все движения $\mathbb{E}^n$ образуют *группу движений* EAff_n, которая является подгруппой в $\mathrm{Aff}_n(\mathbb{R})$.

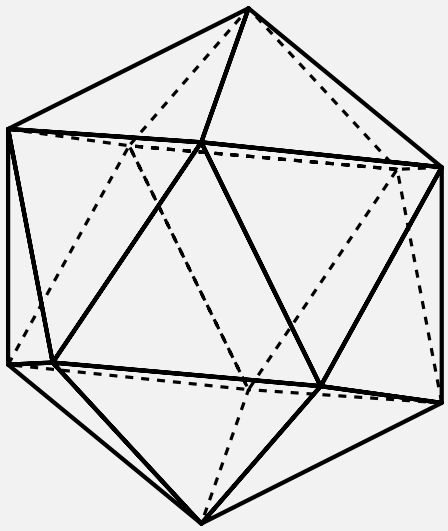
(ix) Все движения евклидова пространства $\mathbb{E}^2$, переводящие в себя правильный n-угольник Γ_n, образуют подгруппу $\mathrm{D}_n \subset \mathrm{EAff}_2$. Она называется *группой диэдра*.

(x) 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. (i) Симметрическая группа S_n порождается транспозициями.

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

(iii) 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.

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. *$gH = g'H$ тогда и только тогда, когда существует $h \in H$ такой, что $g' = gh$.*

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.*

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

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

(iii) *Все левые смежные классы равномощны.*

Аналогичные утверждения верны для правых смежных классов.

Доказательство. (i) очевидно, поскольку $g \in gH$.
(ii) 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.
(iii) Отображение $H \to gH$, $h \mapsto gh$ является биекцией. □

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

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

0.2 Теорема о гомоморфизме

0.2.1 Нормальные подгруппы

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

Замечание. На самом деле, в условиях выше верно равенство $gHg^{-1} = H$ (см. задачу 0.3).

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

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

(iii) $\mathrm{SL}_n(\Bbbk) \lhd \mathrm{GL}_n(\Bbbk)$.

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.

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

Предложение. *Следующие условия эквивалентны:*

(i) *$H \lhd G$;*

(ii) $gH = Hg$ *для любого элемента* $g \in G$.

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 $gH = Hg$ для любого элемента $g \in G$ 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. (i) $\mathrm{D}_n \rhd \mathrm{R}_n$, где R_n – подгруппа поворотов.

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

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

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

0.2.2 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

$$\exp : \mathbb{R}^+ \longrightarrow \mathbb{R}_{>0}, \qquad a \longmapsto \exp(a)$$

является изоморфизмом групп.

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 $\varphi(ab) = \varphi(a)\varphi(b)$ для любых элементов a, $b \in G$.

Примеры. (i) Тождественное отображение – автоморфизм.

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

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

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

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

Определение. Отображение

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

называется *внутренним автоморфизмом* группы.

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

Пример. $\mathrm{Aut}(\mathrm{S}_3) = \mathrm{Int}(\mathrm{S}_3) \simeq \mathrm{S}_3$.

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.

0.2.3 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.

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

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

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

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

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

(vi) 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:

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

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

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

(i) *Если $N_1 \lhd G_1$, то $\varphi^{-1}(N_1) \lhd G$.*

(ii) *Если гомоморфизм φ сюръективен и $N \lhd G$, то $\varphi(N) \lhd G_1$.*

Доказательство. Докажите самостоятельно. $\square$

0.2.5 Теорема о гомоморфизме групп

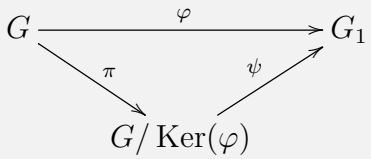
Теорема. *Пусть $\varphi : G \to G_1$ – гомоморфизм групп. Тогда*

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

(ii) *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 $H := \operatorname{Ker}(\varphi)$. 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. (i) $\mathrm{S}_n \,/\, \mathrm{A}_n \simeq \{\pm 1\}$;

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

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

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

Лемма (лемма о факторизации по сомножителям)**.** *Пусть $G_1, \ldots, G_n$ – группы, пусть $G := G_1 \times \cdots \times G_n$ и пусть $N_i \subset G_i$ – нормальные подгруппы. Положим*

$$N := N_1 \times \cdots \times N_n \subset G.$$

Тогда N – нормальная подгруппа в G и

$$G/N \simeq G_1/N_1 \times \cdots \times G_n/N_n.$$

Доказательство. Рассмотрим гомоморфизм

$$G = G_1 \times \cdots \times G_n \longrightarrow G_1/N_1 \times \cdots \times G_n/N_n.$$

Ясно, что он сюръективен, я его ядро равно $N_1 \times \cdots \times N_n = N$. Следовательно, N – нормальная подгруппа и $G/N \simeq G_1/N_1 \times \cdots \times G_n/N_n$. □

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!). □

0.3 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 $g_i g_j = g_j g_i$ для любых элементов $g_i \in G_i$, $g_j \in G_j$.

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

(ii) *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. (i) 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

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

(ii) Положим

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

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*

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

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

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

Доказательство. Докажем достаточность условий (i)– (iii). Пусть условия (i)– (iii) 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 (i)– (iii) предлагается проверить самостоятельно. □

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

(ii) 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

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

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

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

(v) 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 $\{\pm 1\}$.

(vi) 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.*

0.3.1 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 $(1, \ldots, g_i H_i, \ldots, 1)$ для любых $g_i \in G_i$ 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. □

Задачи

0.1. Докажите, что группа $\mathrm{GL}_n(\mathbb{C})$ не порождается элементами конечного порядка.

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

0.3. Докажите, что если H – нормальная подгруппа в группе G, то $gHg^{-1} = H$ для любого $g \in G$.

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

0.5. Докажите, что в абелевой группе элементы конечного порядка образуют подгруппу. Верно ли это для неабелевых групп?

0.6. Пусть $\boldsymbol{\mu}_\infty$ – подгруппа, состоящая из всех элементов конечного порядка в $\mathbb{C}^*$. Докажите, что $\boldsymbol{\mu}_\infty \simeq \mathbb{Q}/\mathbb{Z}$.

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

0.8. Пусть в группе A каждый неединичный элемент имеет порядок 2.

(a) Докажите, что A абелева.

(b) Пусть A конечна. Не пользуясь теоремой о строении абелевых групп (следующая лекция), докажите, что A разлагается в прямое произведение групп $\mathbb{Z}/2\mathbb{Z}$.

0.9. Найдите порядки группы движений

(a) тетраэдра,

(b) куба,

(c) икосаэдра.

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

0.11. Докажите, что группа $\mathbb{Q}^+$ не разлагается в нетривиальную прямую сумму.

0.12. Разложите группу $\mathbb{Q}^*$ в прямое произведение.

0.13. Когда группа диэдра D_n разлагается в нетривиальное прямое произведение?

0.14. Докажите, что 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.

0.15. Пусть H – подгруппа конечного индекса в группе G. Докажите, что существует подгруппа $N \subset H$, имеющая конечный индекс, и нормальная в G.

0.16. Докажите, что $\mathrm{Aut}(\mathrm{S}_3) \simeq \mathrm{S}_3$ и $\mathrm{Aut}(\mathrm{S}_4) \simeq \mathrm{S}_4$.

0.17. Докажите, что в симметрической группе S_n при $n \neq 6$ все автоморфизмы – внутренние и $\mathrm{Aut}(\mathrm{S}_n) \simeq \mathrm{S}_n$.

Лекция 1

Абелевы группы

Все абелевы группы будут рассматриваться с аддитивной операцией (операцией сложения). для удобства читателя элементы абелевой группы мы будем обозначать жирным шрифтом: $\mathbf{a}$, $\mathbf{b}$, $\mathbf{e}$ и т. д. (в отличие от целых чисел, которые мы будем обозначать обычным шрифтом). В аддитивной абелевой группе определено умножение на целые числа: для $\mathbf{a} \in A$, $n \in \mathbb{Z}$ положим

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

Эта операция удовлетворяет следующим свойствам:

- $(nm)\mathbf{a} = n(m\mathbf{a})$ для любых целых n, $m \in \mathbb{Z}$ для любого элемента $\mathbf{a} \in A$;
- $(n+m)\mathbf{a} = n\mathbf{a} + m\mathbf{a}$ для любых целых n, $m \in \mathbb{Z}$ для любого элемента $\mathbf{a} \in A$;
- $n(\mathbf{a} + \mathbf{b}) = n\mathbf{a} + n\mathbf{b}$ для любого целого $n \in \mathbb{Z}$ для любых элементов $\mathbf{a}$, $\mathbf{b} \in A$;
- $1\mathbf{a} = \mathbf{a}$ для любого элемента $\mathbf{a} \in A$.

Заметим, что эти свойства совпадают с аксиомами в определении векторного пространства. (За исключением того, что $\mathbb{Z}$ не является полем и поэтому равенство $n\mathbf{a} = 0$ не влечет $\mathbf{a} = 0$.) Таким образом, мы можем рассматривать целочисленные линейные комбинации элементов $\mathbf{a}_1, \ldots, \mathbf{a}_r \in A$

$$n_1\mathbf{a}_1 + \cdots + n_r\mathbf{a}_r, \qquad n_i \in \mathbb{Z}.$$

Абелева группа A *порождается* элементами $\mathbf{a}_1, \ldots, \mathbf{a}_r \in A$, если любой элемент $\mathbf{a} \in A$ представляется в виде целочисленной линейной комбинации элементов $\mathbf{a}_1, \ldots, \mathbf{a}_r$. В этом случае (т.е. если существует конечный набор порождающих) группа называется *конечно порожденной*.

1.1 Свободные абелевы группы.

Определение. Элементы $\mathbf{a}_1, \ldots, \mathbf{a}_r$ абелевой группы A называются *линейно зависимыми*, если некоторая их нетривиальная целочисленная линейная комбинация равна нулю. Набор элементов $\mathbf{e}_1, \ldots, \mathbf{e}_r$ называется *базисом* абелевой группы A, если выполнены два условия

- $\mathbf{e}_1, \ldots, \mathbf{e}_r$ порождают A;

- $\mathbf{e}_1, \ldots, \mathbf{e}_r$ линейно независимы.

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

Замечание. Несложно видеть, что элементы $\mathbf{e}_1, \ldots, \mathbf{e}_r \in A$ образуют базис тогда и только тогда, когда любой элемент $\mathbf{a} \in A$ *однозначно* представляется в виде целочисленной линейной комбинации

$$\mathbf{a} = n_1\mathbf{e}_1 + \cdots + n_r\mathbf{e}_r, \quad n_i \in \mathbb{Z}.$$

Примеры.

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

$$\mathbf{e}_i := (0, 0, \ldots, \underset{\substack{\uparrow \\ i}}{1}, \ldots, 0)$$

  и поэтому она свободна.

- Если в группе есть нетривиальный элемент конечного порядка, то она не является свободной.

- Группа $\mathbb{Q}^+$ не является свободной (см. упражнение 0.11).

Замечание. Любая свободная конечно порожденная абелева группа F изоморфна $\mathbb{Z}^r$ для некоторого r. Действительно, если $\mathbf{e}_1, \ldots, \mathbf{e}_r$ – базис F, то отображение

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

является изоморфизмом.

Замечание.

- Мы рассматриваем только конечно порожденные свободные абелевы группы, т.е. свободная абелева группы по определению имеет *конечный* базис.

- Понятие свободной абелевы группы отличается от понятия *свободной группы.*

Предложение. *Пусть F – свободная конечно порожденная абелева группа с базисом $\mathbf{e}_1, \ldots, \mathbf{e}_r$.*

(i) *Если элементы $\mathbf{b}_1, \ldots, \mathbf{b}_m \in F$ линейно независимы, то $m \leq r$.*

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

Доказательство. (ii) следует из (i). Докажем (i). Пусть $F_{\mathbb{Q}}$ – векторное пространство над $\mathbb{Q}$ с тем же базисом $\mathbf{e}_1, \ldots, \mathbf{e}_r$. Определим отображение

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

Ясно что это инъективный гомоморфизм абелевых групп. Поэтому если элементы $\mathbf{b}_1, \ldots, \mathbf{b}_m \in F$ линейно зависимы в F, то и их образы в $F_{\mathbb{Q}}$ также линейно зависимы. Наоборот, если $\mathbf{b}_1, \ldots, \mathbf{b}_m \in F$ и их образы в $F_{\mathbb{Q}}$ линейно зависимы, то, домножая линейную комбинацию на знаменатели коэффициентов, получим, что и сами $\mathbf{b}_1, \ldots, \mathbf{b}_m$ 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 $\mathrm{rk}(F)$.

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 $\mathrm{rk}(F) = 1$, 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 $\mathrm{rk}(F) = r$. Пусть $\mathbf{f}_1, \ldots, \mathbf{f}_r$ – базис F. Рассмотрим подгруппы $F' := \langle \mathbf{f}_1 \rangle$ и $F'' := \langle \mathbf{f}_2, \ldots, \mathbf{f}_r \rangle$ – свободные конечно порожденные абелевы группы ранга 1 и $r-1$, соответственно. Далее, рассмотрим проекцию

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

Ясно, что π – сюръективный гомоморфизм и $\mathrm{Ker}(\pi) = F'$. Поэтому множество $E'' = \pi(E)$ является подгруппой в F''. По предположению индукции E'' – свободная конечно порожденная абелева группа. Пусть $\mathbf{e}''_1, \ldots, \mathbf{e}''_m$ – базис E'' и пусть $\mathbf{e}_1, \ldots, \mathbf{e}_m \in E$ – элементы такие, что $\pi(\mathbf{e}_i) = \mathbf{e}''_i$.

Мы можем считать, что $E' \neq \{0\}$ (иначе $E \simeq E''$). Положим $E' := F' \cap E = \mathrm{Ker}(\pi) \cap E$. Ясно, что E' – циклическая группа (поскольку это подгруппа циклической группы $F' = \langle \mathbf{f}_1 \rangle$). Пусть $\mathbf{e}_0 \in E'$ – порождающий элемент. По теореме о гомоморфизме $E'' \simeq E/E'$.

Мы утверждаем, что $\mathbf{e}_0$, $\mathbf{e}_1$,..., $\mathbf{e}_m$ – базис E. Действительно, пусть $\mathbf{x} \in E$. Запишем

$$\pi(\mathbf{x}) = x_1\mathbf{e}''_1 + \cdots + x_m\mathbf{e}''_m$$

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

$$\mathbf{y} := x_1\mathbf{e}_1 + \cdots + x_m\mathbf{e}_m \in E.$$

Тогда $\pi(\mathbf{x}-\mathbf{y}) = 0$. Отсюда $\mathbf{x}-\mathbf{y} \in \mathrm{Ker}(\pi) \cap E = E'$. Следовательно, $\mathbf{x}-\mathbf{y} = x_0\mathbf{e}_0$ для некоторого $x_0 \in \mathbb{Z}$. Таким образом,

$$\mathbf{x} = x_0\mathbf{e}_0 + \mathbf{y} = x_0\mathbf{e}_0 + x_1\mathbf{e}_1 + \cdots + x_m\mathbf{e}_m,$$

т.е. элементы $\mathbf{e}_1$,..., $\mathbf{e}_m$ порождают E.

Предположим, что $\mathbf{e}_0, \ldots, \mathbf{e}_m$ линейно зависимы, т. е.

$$0 = x_0\mathbf{e}_0 + x_1\mathbf{e}_1 + \cdots + x_m\mathbf{e}_m$$

для $x_i \in \mathbb{Z}$. Тогда

$$0 = \pi(0) = \pi(x_0\mathbf{e}_0 + \cdots + x_m\mathbf{e}_m) = x_1\mathbf{e}''_1 + \cdots + x_m\mathbf{e}''_m.$$

С другой стороны, $\mathbf{e}_1$,..., $\mathbf{e}_m$ – базис E''. Следовательно, $x_i = 0 \quad \forall i = 1, \ldots, m$. Отсюда $x_0\mathbf{e}_0 = 0$ и $x_0 = 0$ поскольку $\mathbf{e}_0 \neq 0$ (и F – свободная абелева группа). $\square$

1.1.1 Универсальное свойство свободных абелевых групп.

Лемма. *Пусть A – конечно порожденная абелева группа и пусть $\mathbf{a}_1, \ldots, \mathbf{a}_r$ – некоторое множество ее порождающих. Тогда существует свободная абелева группа F ранга r с базисом $\mathbf{f}_1, \ldots, \mathbf{f}_r$ и сюръективный гомоморфизм $\varphi : F \to A$ такой, что*

$$\varphi(\mathbf{f}_i) = \mathbf{a}_i \qquad \forall i.$$

Доказательство. Положим

$$\varphi\left(\sum n_i \mathbf{f}_i\right) = \sum n_i \mathbf{a}_i.$$

Это отображение корректно определено, поскольку любой элемент $\mathbf{f} \in F$ однозначно записывается в виде $\mathbf{f} = \sum n_i \mathbf{f}_i$. Свойство гомоморфизма легко проверяется. Так как $\mathbf{a}_1, \ldots, \mathbf{a}_r$ 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).*

1.1.2 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 преобразований:

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

(ii) 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 (строк) может быть представлена как композиция целочисленных элементарных преобразований столбцов (строк).

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. Очевидно, что мы можем считать, что $M \neq 0$.

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 $\lambda_{i,1}' = 0 \quad \forall i > 1$. 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

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

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* $\mathbf{f}_1, \ldots, \mathbf{f}_r$ *– ее базис. Пусть* $M = (\lambda_{i,j})$ *– целочисленная* $r \times r$*-матрица. Положим*

$$\begin{array}{rcl} \mathbf{f}_1' & = & \lambda_{1,1}\mathbf{f}_1 + \cdots + \lambda_{r,1}\mathbf{f}_r, \\ \mathbf{f}_2' & = & \lambda_{1,2}\mathbf{f}_1 + \cdots + \lambda_{r,2}\mathbf{f}_r, \\ \cdots & \cdots & \cdots \\ \mathbf{f}_r' & = & \lambda_{1,r}\mathbf{f}_1 + \cdots + \lambda_{r,r}\mathbf{f}_r. \end{array}$$

т. е. $(\mathbf{f}_1', \ldots, \mathbf{f}_r') = (\mathbf{f}_1, \ldots, \mathbf{f}_r) \cdot M$*. Тогда элементы* $\mathbf{f}_1', \ldots, \mathbf{f}_r'$ *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 целочисленная и мы имеем $(\mathbf{f}_1, \ldots, \mathbf{f}_r) = (\mathbf{f}'_1, \ldots, \mathbf{f}'_r) \cdot M^{-1}$, т. е.

$$\begin{array}{rcl} \mathbf{f}_1 & = & \mu_{1,1}\mathbf{f}'_1 + \cdots + \mu_{r,1}\mathbf{f}'_r, \\ \mathbf{f}_2 & = & \mu_{1,2}\mathbf{f}'_1 + \cdots + \mu_{r,2}\mathbf{f}'_r, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ \mathbf{f}_r & = & \mu_{1,r}\mathbf{f}'_1 + \cdots + \mu_{r,r}\mathbf{f}'_r. \end{array} \qquad (*)$$

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

1.1.3 Теорема о согласованных базисах

Теорема. *Пусть F – свободная абелева группа и пусть $E \subset F$ – ее подгруппа. Тогда существуют базисы $\mathbf{f}_1, \ldots, \mathbf{f}_r \in F$ и $\mathbf{e}_1, \ldots, \mathbf{e}_m \in E$ такие, что $\mathbf{e}_i = \mu_i \mathbf{f}_i$, $i = 1, \ldots, m$, $\mu_i \in \mathbb{Z}$.*

Доказательство. Выберем любые базисы

$$\mathbf{a}_1, \ldots, \mathbf{a}_r \in F, \qquad \mathbf{b}_1, \ldots, \mathbf{b}_m \in E$$

и выразим $\mathbf{b}_i$ через $\mathbf{a}_j$:

$$\mathbf{b}_i = \sum_{j=1}^{r} \lambda_{j,i}\mathbf{a}_j, \quad \lambda_{j,i} \in \mathbb{Z}, \quad i = 1, \ldots, m.$$

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

$$(\mathbf{b}_1, \ldots, \mathbf{b}_m) = (\mathbf{a}_1, \ldots, \mathbf{a}_r) \cdot M.$$

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

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

Выберем новые базисы следующим образом

$$(\mathbf{f}_1, \ldots, \mathbf{f}_r) = (\mathbf{a}_1, \ldots, \mathbf{a}_r) \cdot T^{-1}, \quad (\mathbf{e}_1, \ldots, \mathbf{e}_m) = (\mathbf{b}_1, \ldots, \mathbf{b}_m) \cdot S.$$

Тогда

$$(\mathbf{f}_1, \ldots, \mathbf{f}_r) \cdot M' = (\mathbf{a}_1, \ldots, \mathbf{a}_r) \cdot T^{-1}TMS = (\mathbf{b}_1, \ldots, \mathbf{b}_m) \cdot S = (\mathbf{e}_1, \ldots, \mathbf{e}_m).$$

Это доказывает утверждение. □

Теорема (теорема о строении конечно порожденных абелевых групп)**.** *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 порожденности группы. Например, группа $\mathbb{Q}^+$ не может быть разложена в нетривиальную прямую сумму (см. задачу 0.11).

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 $\mathbf{f}_1, \dots, \mathbf{f}_r \in F$ и $\mathbf{e}_1, \dots, \mathbf{e}_m \in E$ такие, что $\mathbf{e}_i = \mu_i \mathbf{f}_i$, $i = 1, \dots, m$. Положим $F_i := \langle \mathbf{f}_i \rangle$ и $E_i := \langle \mathbf{e}_i \rangle$ при $i = 1, \dots, m$ и $E_i := \{0\}$ при $i = m, \dots, r$. Напомним лемму о факторизации по сомножителям (в аддитивной форме).

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

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

Тогда

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

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

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

Доказательство. Если $\mathbf{a}$, $\mathbf{b} \in \operatorname{Tor}(A)$, то существуют n, $m \in \mathbb{Z} \setminus \{0\}$ такие, что $n\mathbf{a} = 0$ и $m\mathbf{b} = 0$. Тогда $nm(\mathbf{a} - \mathbf{b}) = 0$, т. е. $\mathbf{a} - \mathbf{b} \in \operatorname{Tor}(A)$. Следовательно, $\operatorname{Tor}(A)$ – подгруппа. Обозначим через

$$\pi : A \to A/\operatorname{Tor}(A)$$

канонический гомоморфизм. Предположим, что $\pi(\mathbf{a})$ – элемент конечного порядка. Тогда $\pi(n\mathbf{a}) = n\pi(\mathbf{a}) = 0$ для некоторого $n \in \mathbb{Z}\setminus\{0\}$. Следовательно, $n\mathbf{a} \in \operatorname{Ker}(\pi) = \operatorname{Tor}(A)$. Поэтому существует $m \in \mathbb{Z} \setminus \{0\}$ такое, что $mn\mathbf{a} = 0$, т. е. $\mathbf{a} \in \operatorname{Tor}(A) = \operatorname{Ker}(\pi)$ и тогда $\pi(\mathbf{a}) = 0$. □

Пример. Пусть $\Bbbk$ – поле.

(i) Тогда $\operatorname{Tor}(\Bbbk^*)$ – подгруппа всех корней из 1.

(ii) Подгруппа $\operatorname{Tor}(\Bbbk^+)$ нетривиальна тогда и только тогда, когда $\operatorname{char}(\Bbbk) \neq 0$ и в этом случае $\operatorname{Tor}(\Bbbk^+) = \Bbbk^+$.

Аналогично доказывается следующее утверждение.

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

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

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

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

$$A = \Big(\bigoplus_{p,i} A_{p,i}\Big) \bigoplus \Big(\bigoplus_j A_{\infty,j}\Big),$$

где $A_{p,i}$ – p-примарные циклические группы (p – простое), а $A_{\infty,j}$ – 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

$$\bigoplus_{p,i} A_{p,i} = \mathrm{Tor}(A)$$

определена однозначно. Поэтому определена однозначно и свободная подгруппа подгруппа

$$\bigoplus_j A_{\infty,j} \simeq A/\,\mathrm{Tor}(A),$$

а также количество слагаемых в $\oplus_j A_{\infty,j}$, равное ее рангу.

Далее, рассмотрим подгруппы

$$\bigoplus_i A_{p,i} \subset \mathrm{Tor}_{(p)}(A).$$

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 имеет место равенство

$$\bigoplus_i A_{p,i} = \mathrm{Tor}_{(p)}(A).$$

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

$$\varphi : B \longrightarrow B, \qquad \mathbf{b} \longmapsto p\mathbf{b}.$$

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 $\mathbf{x} \in K \subset B$ существует единственное разложение

$$\mathbf{x} = \mathbf{x}_1 + \cdots \mathbf{x}_n,$$

где $\mathbf{x}_i \in B_i$. Так как

$$0 = p\mathbf{x} = p\mathbf{x}_1 + \cdots + p\mathbf{x}_n$$

и последнее разложение также единственно, то $p\mathbf{x}_i = 0$ для всех i, т. е. $\mathbf{x}_i \in K_i \cap B_i$. 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

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

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 примеры!)

Определение. 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.

Определение. *Показателем* (или *экспонентой*) конечной абелевой группы A называется число

$$\exp(A) := \min\{m \in \mathbb{N} \mid ma = 0 \quad \forall a \in A\}.$$

Замечание. Несложно видеть, что показатель $\exp(A)$ делится на порядок любого элемента группы. Более того, он равен наименьшему общему кратному порядков всех элементов группы:

$$\exp(A) = \text{НОК}\ \big\{\ |a|\ \mid\ a \in A\big\}.$$

Теорема. *Пусть A – конечная абелева группа.*

(i) *Экспонента A равна наименьшему общему кратному её элементарных делителей.*

(ii) *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 $A = \oplus_{p,i} A_{p,i}$ – разложение в сумму примарных циклических подгрупп. 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 $\mathbf{a}_p$ – порождающий элемент группы $A_{p,1}$. Положим $\mathbf{a} := \sum_p \mathbf{a}_p$. Тогда $n = \prod_p p^{k_p}$ и

$$|\mathbf{a}| = \text{НОК } \{|\mathbf{a}_i|\} = \text{НОК } \{p^{k_p}\} = n$$

поскольку в абелевой группе порядок суммы элементов взаимно простых порядков равен произведению их порядков (см. лемму ниже). □

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

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

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

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

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

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

Задачи

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

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

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

1.4. Докажите, что циклическая группа G порядка n содержит циклическую подгруппу порядка m тогда и только тогда, когда m делит n и в этом случае подгруппа порядка m в G единственна.

1.5. Докажите, что конечная абелева группа A является циклической тогда и только тогда, когда для каждого простого числа p, делящего $|A|$, в A имеется ровно $p-1$ элемент порядка p.

1.6. Сколько элементов порядка 6 имеется в группе $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$? Сколько элементов порядка 4 имеется в группе $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$?

1.7. Изоморфны ли группы: $\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/36\mathbb{Z}$ и $\mathbb{Z}/12\mathbb{Z}\oplus\mathbb{Z}/18\mathbb{Z}$; $\mathbb{Z}/6\oplus\mathbb{Z}/36$ и $\mathbb{Z}/9\oplus\mathbb{Z}/24$; $\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ и $\mathbb{Z}/60\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$?

1.8. Сколько существует попарно неизоморфных абелевых групп порядка 100?

1.9. Пусть A_1 и A_2 – конечно порожденные абелевы группы такие, что существует абелева группа A такая, что $A_1 \oplus A \simeq A_2 \oplus A$. Следует ли отсюда, что $A_1 \simeq A_2$? Верно ли это при условии, что A конечно порождена?

1.10. Пусть A – абелева группа, в которой каждый ненулевой элемент имеет порядок p (p – простое). Докажите, что на A можно ввести структуру векторного пространства над полем $\mathbb{F}_p$ из p элементов. Выведите отсюда, что A разлагается в прямое произведение групп $\mathbb{F}_p^+$.

Лекция 2

Строение конечно порожденных абелевых групп

Дадим другое доказательство существования разложения в теореме о строении конечно порожденных абелевых групп.

Лемма. *Пусть A – конечно порожденная абелева группа. Если в группе A нет элементов конечного порядка, то она является свободной абелевой.*

Доказательство. Пусть $A = \langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$. Проведем доказательство индукцией по n. База индукции $n = 1$ очевидна. Предположим, что утверждение верно для всех абелевых групп, порожденных менее чем n элементами.

Докажем вспомогательное утверждение.

Утверждение. *Существует элемент $\mathbf{b} \in A$, $\mathbf{b} \neq 0$ такой, что множество*

$$A_{\mathbf{b}} := \{x \in A \mid \exists l_1,\, l_2 \in \mathbb{Z},\, l_1 \neq 0,\, l_1 x = l_2 \mathbf{b}\}$$

является циклической подгруппой в A и факторгруппа $A/A_{\mathbf{b}}$ порождается меньшим количеством элементов.

Доказательство утверждения. Пусть $\mathbf{a}_1, \ldots, \mathbf{a}_n$ – порождающие элементы группы A. Если если они линейно независимы, то группа A – свободная абелева и они образуют базис в A. В этом случае положим $\mathbf{b} := \mathbf{a}_i$ для любого i и тогда $A_{\mathbf{b}} = \langle \mathbf{b} \rangle$ – циклическая группа и факторгруппа $A/A_{\mathbf{b}}$ порождается образами элементов $\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}, \mathbf{a}_{i+1}, \ldots, \mathbf{a}_n$.

Далее предположим, что $\mathbf{a}_1, \ldots, \mathbf{a}_n$ линейно зависимы. Значит, мы можем считать, что

$$k\mathbf{a}_1 = \sum_{i=2}^{n} k_i \mathbf{a}_i, \qquad (*)$$

где $k\mathbf{a}_1 \neq 0$. Положим $\mathbf{b} := k\mathbf{a}_1$ и $A' := \langle \mathbf{a}_2, \ldots, \mathbf{a}_n \rangle$. По предположению индукции A' – свободная абелева группа. Из $(*)$ следует, что $\mathbf{b} \in A'$ и $A' \supset kA$. Пусть также

$$A'_{\mathbf{b}} := \{x \in A' \mid \exists l_1,\, l_2 \in \mathbb{Z},\, l_1 \neq 0,\, l_1 x = l_2 \mathbf{b}\}.$$

Так как $A \supset A_{\mathbf{b}}$, то $kA \supset kA_{\mathbf{b}}$. Таким образом,

$$A_{\mathbf{b}} \supset A'_{\mathbf{b}} = A_{\mathbf{b}} \cap A' \supset kA_{\mathbf{b}} \cap kA = kA_{\mathbf{b}}.$$

С другой стороны, отображение

$$\varphi : A \longrightarrow A, \qquad x \longmapsto kx$$

является инъективным гомоморфизмом групп. Так как A' – свободная абелева группа, то группа $A'_{\mathbf{b}}$ является циклической. Следовательно, таковой является и группа $A_{\mathbf{b}} \simeq \varphi(A_{\mathbf{b}}) = kA_{\mathbf{b}} \subset A'_{\mathbf{b}}$. При этом факторгруппа $A/A_{\mathbf{b}}$ порождается образами элементов $\mathbf{a}_2, \ldots, \mathbf{a}_n$. □

Продолжим доказательство леммы. Возьмем элемент $\mathbf{b} \in A$ такой, как в утверждении. Тогда факторгруппа $A/A_{\mathbf{b}}$ не имеет элементов конечного порядка и порождается меньшим количеством элементов. Пусть $\mathbf{e}_1$ – порождающий элемент циклической группы $A_{\mathbf{b}}$. По предположению индукции $A/A_{\mathbf{b}}$ – свободная абелева группа. Пусть $\bar{\mathbf{e}}_2, \ldots, \bar{\mathbf{e}}_r$ – ее базис, пусть

$$\varphi : A \to A/A_{\mathbf{b}}$$

– гомоморфизм факторизации и пусть $\mathbf{e}_2, \ldots, \mathbf{e}_r \in A$ – любые элементы такие, что $\varphi(\mathbf{e}_i) = \bar{\mathbf{e}}_i$. Мы утверждаем, что элементы $\mathbf{e}_1, \ldots, \mathbf{e}_r$ порождают A. Действительно, для любого $\mathbf{x} \in A$ имеем $\varphi(\mathbf{x}) = \sum_{i=2}^r k_i \bar{\mathbf{e}}_i$ для некоторых $k_i \in \mathbb{Z}$. Тогда $\varphi(\mathbf{x} - \sum_{i=2}^r k_i \mathbf{e}_i) = 0$. Следовательно, $\mathbf{x} - \sum_{i=2}^r k_i \mathbf{e}_i \in \operatorname{Ker}(\varphi) = A_{\mathbf{b}}$. Это означает, что $\mathbf{x} - \sum_{i=2}^r k_i \mathbf{e}_i = k_1 \mathbf{e}_1$ для некоторого $k_1 \in \mathbb{Z}$. Таким образом,

$$\mathbf{x} = \sum_{i=1}^r k_i \mathbf{e}_i.$$

Это разложение единственно. Действительно, иначе

$$\mathbf{x} = \sum_{i=1}^r k_i \mathbf{e}_i = \sum_{i=1}^r k'_i \mathbf{e}_i. \tag{†}$$

и тогда

$$0 = \varphi(\mathbf{x} - \mathbf{x}) = \varphi\left(\sum_{i=1}^r (k_i - k'_i)\mathbf{e}_i\right) = \sum_{i=2}^r (k_i - k'_i)\bar{\mathbf{e}}_i.$$

Поскольку $\bar{\mathbf{e}}_2, \ldots, \bar{\mathbf{e}}_r$ – базис $A/A_{\mathbf{b}}$, то $k_i = k'_i$ для $i = 2, \ldots, r$. Из (†) следует, что $k_1 = k'_1$. Таким образом, $\mathbf{e}_1, \ldots, \mathbf{e}_r$ – базис A и поэтому группа A является свободной абелевой. □

Лемма. *Пусть A – конечно порожденная абелева группа. Существует свободная абелева подгруппа $F \subset A$ такая, что имеет место разложение*

$$A = \operatorname{Tor}(A) \oplus F.$$

Доказательство. Как и в предыдущей лемме рассмотрим гомоморфизм факторизации

$$A \longrightarrow A/\operatorname{Tor}(A).$$

Факторгруппа $A/\operatorname{Tor}(A)$ конечно порождена и не содержит элементов конечного порядка. Следовательно, она свободна и существует базис $\bar{\mathbf{e}}_1, \ldots, \bar{\mathbf{e}}_r \in A/\operatorname{Tor}(A)$. Пусть $\mathbf{e}_1, \ldots, \mathbf{e}_r \in A$ – любые элементы такие, что $\varphi(\mathbf{e}_i) = \bar{\mathbf{e}}_i$. Для любого $\mathbf{x} \in A$ имеем $\varphi(\mathbf{x}) = \sum_{i=1}^r k_i \bar{\mathbf{e}}_i$ для некоторых $k_i \in \mathbb{Z}$. Тогда $\varphi(\mathbf{x} - \sum_{i=1}^r k_i \mathbf{e}_i) = 0$. Следовательно,

$$\mathbf{x} - \sum_{i=1}^r k_i \mathbf{e}_i \in \operatorname{Ker}(\varphi) = \operatorname{Tor}(A).$$

Таким образом, существует элемент $\mathbf{y} \in \mathrm{Tor}(A)$ такой, что

$$\mathbf{x} = \mathbf{y} + \sum_{i=1}^{r} k_i \mathbf{e}_i.$$

Это разложение единственно. Действительно, иначе

$$\mathbf{x} = \mathbf{y} + \sum_{i=1}^{r} k_i \mathbf{e}_i = \mathbf{y}' + \sum_{i=1}^{r} k_i' \mathbf{e}_i. \qquad (\ddagger)$$

и тогда

$$0 = \varphi(\mathbf{x} - \mathbf{x}) = \varphi\left(\mathbf{y} - \mathbf{y}' + \sum_{i=1}^{r} (k_i - k_i')\mathbf{e}_i\right) = \sum_{i=1}^{r} (k_i - k_i')\bar{\mathbf{e}}_i.$$

Поскольку $\bar{\mathbf{e}}_1, \ldots, \bar{\mathbf{e}}_r$ – базис $A/\mathrm{Tor}(A)$, то $k_i = k_i'$ для $i = 1, \ldots, r$. Тогда из $(\ddagger)$ следует, что $\mathbf{y} = \mathbf{y}'$. Положим $F := \langle \mathbf{e}_1, \ldots, \bar{\mathbf{e}}_r \rangle$. Тогда $\mathbf{e}_1, \ldots, \mathbf{e}_r$ – базис F, группа F является свободной абелевой и $A = \mathrm{Tor}(A) \oplus F$. □

Следствие. *Если A – конечно порожденная абелева группа, то $\mathrm{Tor}(A)$ – конечная подгруппа.*

Лемма. *Для любой конечной абелевой группы A имеет место разложение*

$$A = \bigoplus_{p} \mathrm{Tor}_p(A).$$

Доказательство. Пусть $|A| = n$. Разложим n в произведение простых множителей $n = p_1^{k_1} \cdots p_m^{k_m}$. Проведем доказательство индукцией по m. База индукции $m = 1$ очевидна. Предположим, что утверждение верно для всех абелевых групп, у которых разложение в произведение степеней простых чисел имеет меньше чем m сомножителей. Представим n в виде $n = n_1 n_2$, где НОД $(n_1, n_2) = 1$ и $n_i > 1$. Тогда $1 = n_1 u_1 + n_2 u_2$ для некоторых целых u_1, u_2. Положим $A_1 := n_1 A$ и $A_2 := n_2 A$. Тогда $A_1 \cap A_2 = \{0\}$. Действительно, если $\mathbf{a} \in A_1 \cap A_2$, то $\mathbf{a} = n_1 \mathbf{a}' = n_2 \mathbf{a}''$ для некоторых $\mathbf{a}', \mathbf{a}'' \in A$. Так как $n_2 \mathbf{a} = n_1 n_2 \mathbf{a}' = n\mathbf{a}' = 0$, то по теореме Лагранжа порядок $\mathbf{a}$ делит n_2. Аналогично получаем, что порядок $\mathbf{a}$ делит n_1. Так как НОД $(n_1, n_2) = 1$, то $\mathbf{a} = 0$. Наконец, для любого элемента $\mathbf{a} \in A$ имеем $\mathbf{a} = (n_1 u_1 + n_2 u_2)\mathbf{a} = u_1 \mathbf{a}_1 + u_2 \mathbf{a}_2$, где $\mathbf{a}_i := n_i \mathbf{a} \in A_i$. По предположению индукции A_1 и A_2 раскладываются в суммы своих подгрупп $\mathrm{Tor}_p(A_i)$. Лемма доказана. □

Лемма. *Для любой конечной абелевой p-группы A имеет место разложение*

$$A = \bigoplus_{i=2}^{n} A_i$$

где A_i – (примарные) циклические группы.

Доказательство. Пусть $|A| = p^m$. Проведем доказательство индукцией по m. База индукции $m = 1$ очевидна. Предположим, что утверждение верно для всех абелевых p-групп порядков меньших чем p^m. Возьмем элемент $\mathbf{a}_1 \in A$ максимального порядка. Пусть $|\mathbf{a}_1| = p^{m_1}$. Рассмотрим факторгруппу $\bar{A} := A/\langle \mathbf{a}_1 \rangle$ и гомоморфизм факторизации

$$\varphi : A \longrightarrow \bar{A}.$$

Группа $\bar{A}$ имеет порядок $p^{m-m_1} < p^m$. По предположению индукции имеет место разложение

$$\bar{A} = \bigoplus_{i=2}^{n} \bar{A}_i$$

где $\bar{A}_i$ – циклические группы. Пусть $\bar{\mathbf{a}}_i$ – порождающий элемент $\bar{A}_i$ и пусть $m_i := |\bar{A}_i|$, $i = 2, \ldots, n$. Существуют элементы $\mathbf{b}_2, \ldots, \mathbf{b}_n \in A$ такие, что $\varphi(\mathbf{b}_i) = \bar{\mathbf{a}}_i$. Тогда

$$\varphi(p^{m_i}\mathbf{b}_i) = p^{m_i}\bar{\mathbf{a}}_i = 0.$$

Следовательно, $p^{m_i}\mathbf{b}_i \in \mathrm{Ker}(\varphi) = \langle \mathbf{a}_1 \rangle$. Таким образом,

$$p^{m_i}\mathbf{b}_i = s_i\mathbf{a}_1 \quad \text{для некоторых } s_i \in \mathbb{Z}.$$

Согласно нашему выбору $\mathbf{a}_1$ порядки всех элементов группы A делят p^{m_1}. Отсюда

$$0 = p^{m_1}\mathbf{b}_i = p^{m_1-m_i}p^{m_i}\mathbf{b}_i = p^{m_1-m_i}s_i\mathbf{a}_1.$$

Следовательно, число $p^{m_1-m_i}s_i$ делится на порядок p^{m_1} элемента $\mathbf{a}_1$. Тогда s_i делится на p^{m_i}, т.е. мы можем записать

$$s_i = p^{m_i}q_i, \qquad q_i \in \mathbb{Z}.$$

Положим

$$\mathbf{a}_i := \mathbf{b}_i - q_i\mathbf{a}_1, \qquad i = 2, \ldots, n.$$

Тогда

$$p^{m_i}\mathbf{a}_i = p^{m_i}(\mathbf{b}_i - q_i\mathbf{a}_1) = p^{m_i}\mathbf{b}_i - p^{m_i}q_i\mathbf{a}_1 = s_i\mathbf{a}_1 - s_i\mathbf{a}_1 = 0. \qquad \square$$

2.1 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 $\mathbf{a}, \mathbf{b} \in A$ мы имеем $\|\mathbf{a} - \mathbf{b}\| \geq \delta$.*

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 $\|\mathbf{a} - \mathbf{b}\| < \delta$, то $0 \neq \mathbf{a} - \mathbf{b} \in U_\delta \cap A$. Противоречие. $\square$

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 $\mathbf{x} \in K$ пусть $U_\mathbf{x}$ – открытый шар радиуса $< \delta/2$ с центром в $\mathbf{x}$. Эти шары покрывают K. Из этого покрытия можно выбрать конечное подпокрытие $U_{\mathbf{x}_i}$, т.е. $K = \cup_i U_{\mathbf{x}_i}$. По конструкции каждый шар $U_{\mathbf{x}_i}$ содержит не более одного элемента A.

$\square$

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 $\mathbf{e}_1, \ldots, \mathbf{e}_m \in A$ – максимальная линейно независимая над $\mathbb{R}$ система. Положим

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

Поскольку множество K замкнуто и ограничено, то оно компактно. Следовательно, пересечение $K \cap A$ конечно. Тогда группа A порождается элементами $\mathbf{e}_1, \ldots, \mathbf{e}_m$ и конечным множеством $K \cap A$. Действительно, любой элемент $\mathbf{a} \in A$ можно записать в виде

$$\mathbf{a} = \sum \beta_i \mathbf{e}_i, \quad \beta_i \in \mathbb{R}.$$

Тогда

$$\mathbf{a} = \sum [\beta_i] \mathbf{e}_i + \sum \{\beta_i\} \mathbf{e}_i, \quad \sum \{\beta_i\} \mathbf{e}_i \in K \cap A. \qquad \square$$

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

Теорема. *Пусть $A \subset \mathbb{R}^n$ – дискретная подгруппа и пусть $\mathbf{e}_1, \ldots, \mathbf{e}_m$ – ее базис. Тогда $\mathbf{e}_1, \ldots, \mathbf{e}_m$ линейно независимы над $\mathbb{R}$.*

Доказательство. Предположим, что

$$\mathbf{e}_1 = \sum_{i=2}^{m} \alpha_i \mathbf{e}_i, \quad \alpha_i \in \mathbb{R}.$$

Рассмотрим множество

$$K := \left\{ \sum \beta_2 \mathbf{e}_2 + \cdots + \beta_m \mathbf{e}_m \mid 0 \leq \beta_i \leq 1 \right\}.$$

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

$$t\mathbf{e}_1 = \sum_{i=2}^{m} [t\alpha_i] \mathbf{e}_i + \sum_{i=2}^{m} \{t\alpha_i\} \mathbf{e}_i$$

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

$$t_1\mathbf{e}_1 - t_2\mathbf{e}_1 = \sum_{i=2}^{m} ([t_1\alpha_i] - [t_2\alpha_i]) \mathbf{e}_i \in \langle \mathbf{e}_2, \ldots, \mathbf{e}_m \rangle.$$

Противоречие. $\square$

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

Лекция 3

Действия групп

3.1 Действия групп

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

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

такое, что выполняются следующие два свойства:

- $(g_1 g_2) * x = g_1 * (g_2 * x)$ для любых элементов g_1, $g_2 \in G$ и для любого элемента $x \in \Omega$
- $1 * x = x$ для любого элемента $x \in \Omega$.

Замечание. Пусть задано действие $G \curvearrowright \Omega$. Для каждого элемента $g \in G$ определим отображение

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

По определению для любых элементов g_1, $g_2 \in G$, для любого элемента $x \in \Omega$ 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 $G \curvearrowright \Omega$ по правилу $g * x = \Psi(g)(x)$. (Проверьте!).

Ядром эффективности действия $G \curvearrowright \Omega$ называется подгруппа

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

Ясно, что ядро эффективности совпадает с ядром гомоморфизма $\Psi : G \to \mathrm{S}_\Omega$. Действие называется *эффективным*, если его ядро эффективности тривиально.

Определение. Пусть $G \curvearrowright \Omega$ – 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 $G \curvearrowright \Omega$ – действие группы G.*

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

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

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

Доказательство. (i) $y \in \mathrm{Orb}(x)$ тогда и только тогда, когда существует $g_0 \in G$ такой, что $y = g_0 * x \Longrightarrow$ для любого элемента $g \in G \quad g * y = (gg_0) * x \in \mathrm{Orb}(x)$. Следовательно, $\mathrm{Orb}(y) \subset \mathrm{Orb}(x)$. Аналогично, для любого элемента $g \in G \quad g * x = (gg_0^{-1}) * x \in \mathrm{Orb}(y)$ и поэтому имеет место обратное включение.

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

Утверждение (iii) следует из (ii) поскольку $x \in \mathrm{Orb}(x)$. □

3.2 Примеры действий

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

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

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

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

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

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

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

(vii) С каждым действием $G \curvearrowright \Omega$ связаны несколько других действий.

(a) Действие на множестве всех подмножеств $G \curvearrowright 2^\Omega$, где для $X \subset \Omega$ полагаем $g * X := \{g * x \mid x \in X\}$.

(b) Действие на декартовом произведении $G \curvearrowright \Omega \times \cdots \times \Omega$ по правилу $g * (x_1, \ldots, x_n) := (g * x_1, \ldots, g * x_n)$.

(c) Пусть $G \curvearrowright \Omega$ – действие группы G и пусть $H \subset G$ – подгруппа. Тогда имеется естественное действие $H \curvearrowright \Omega$ – *ограничение* действия $G \curvearrowright \Omega$.

Определение. Пусть $G \curvearrowright \Omega$ – 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 $H \curvearrowright G$ *левыми сдвигами* или *левое регулярное* действие:

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

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

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

Пример. Для любой группы G имеется действие $G \curvearrowright G$ 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

$$\mathrm{S}_4 \longrightarrow \mathrm{S}_\Omega \simeq \mathrm{S}_3,$$

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, $N_G(H) = G$ тогда и только тогда, когда $H \lhd G$. 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:

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

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.*

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

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

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

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

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

Отображение сюръективно по определению орбиты. Проверим его инъективность. Пусть $\phi(g'\,\mathrm{St}(x)) = \phi(g\,\mathrm{St}(x))$. Тогда имеем последовательно

$$g * x = g' * x, \quad (g^{-1}g') * x = x, \quad g^{-1}g' \in \mathrm{St}(x) \quad \text{и} \quad g\,\mathrm{St}(x) = g'\,\mathrm{St}(x). \qquad \square$$

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

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

Следствие.

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

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

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

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 T движений тетраэдра 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 O собственных движений куба. 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 $O \simeq \mathrm{S}_4 \to \mathrm{S}_3$.

Пример. Проективная линейная группа $\mathrm{PGL}_n(\Bbbk)$ естественным образом действует на проективном пространстве $\mathbb{P}^{n-1}$. Если $\Bbbk = \mathbb{F}_q$ – конечное поле, содержащее q элементов, то проективное пространство $\mathbb{P}^{n-1}$ над $\Bbbk$ содержит ровно $(q^n-1)(q-1)$ элементов. Следовательно, в этом случае действие $\mathrm{PGL}_n(\Bbbk) \curvearrowright \mathbb{P}^{n-1}$ индуцирует вложение $\mathrm{PGL}_n(\Bbbk) \hookrightarrow \mathrm{S}_{(q^n-1)(q-1)}$.

3.3 p-группы.

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

Теорема. *Центр p-группы нетривиален.*

Доказательство. Рассмотрим действие $G \curvearrowright G$ сопряжениями:

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

Тогда одноэлементные орбиты – это в точности элементы центра группы. Поэтому имеется 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 содержит нетривиальную нормальную подгруппу.*

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 группа $G/Z(G)$ – 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. □

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

Пример. Группа верхних унитреугольных 3×3-матриц над полем $\mathbb{F}_p$ из p элементов

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

имеет порядок p^3 и не является абелевой.

3.4 Теоремы Силова

Теорема (первая теорема Силова)**.** *Пусть G – конечная группа, порядок которой делится на p^k, где p – простое. Тогда в G существует подгруппа порядка p^k.*

Доказательство. Пусть $|G| = n = p^k m$. Докажем теорему индукцией по n. База индукции очевидна. Предположим, что теорема верна для всех групп порядков $n' < n$. Рассмотрим действие $G \curvearrowright G$ 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:

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

Отсюда

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

Имеются две возможности:

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

  $$p^k m = n = |Z(x)| \cdot |\operatorname{Orb}(x)|,$$

  то $|Z(x)| \equiv 0 \mod p^k$ и $|Z(x)| < n$. По предположению индукции в $Z(x)$ существует подгруппа порядка p^k.

- Для всех $x \in G \setminus Z(G)$ имеем $|\operatorname{Orb}(x)| \equiv 0 \mod p$. Тогда $|Z(G)| \equiv 0 \mod p$ 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.*

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

(ii) Пусть $\Bbbk = \mathbb{F}_p$ – 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

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

является силовской.

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

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

(ii) *Все силовские подгруппы сопряжены.*

Доказательство. Запишем $|G| = p^k m$, где НОД $(m, p) = 1$. Пусть $G_p \subset G$ – силовская p-подгруппа и пусть $H \subset G$ – любая p-подгруппа. 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 $H \curvearrowright G/G_p$. Число элементов любой орбиты делит порядок группы H и поэтому имеет вид p^k, $k \geq 0$. Поэтому

$$|G/G_p| = \sum_{xG_p \in G/G_p} |\,\mathrm{Orb}(xG_p)|$$

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

$$H \subset yG_py^{-1}, \tag{$*$}$$

что доказывает (i).

Для доказательства (ii) предположим, что G_p^o – другая силовская p-подгруппа. Полагая $H = G_p^o$ в $(*)$ получим утверждение (ii). □

Следствие. *Число s_p силовских p-подгрупп равно индексу нормализатора одной из них:*

$$s_p = [G : N(G_p)].$$

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

Теорема (третья теорема Силова)**.** *Число s_p силовских p-подгрупп сравнимо с 1 по модулю p;*

$$s_p \equiv 1 \mod p.$$

Доказательство. Пусть Ω – множество всех силовских p-подгрупп. Рассмотрим действие $G \curvearrowright \Omega$ сопряжениями. По второй теореме Силова это действие транзитивно. Зафиксируем одну силовскую подгруппу $G_p \in \Omega$ и рассмотрим ограничение действия $G \curvearrowright \Omega$ на подгруппу G_p. Это действие необязательно транзитивно. Пусть $\Omega = \cup\Omega_i$ – разложение в непересекающееся объединение орбит. Имеем $|\Omega_i| = p^{k_i}$, $k_i \geq 0$. Значит

$$s_p = |\Omega| = \sum |\Omega_i| = \sum p^{k_i}.$$

Орбита $\mathrm{Orb}(G_p) = \{G_p\}$ состоит из одного элемента. Предположим, что существует другая одноэлементная орбита

$$\Omega_i = \{G_p'\},$$

где $G_p' \in \Omega$, $G_p \neq G_p'$. Тогда $gG_p'g^{-1} = G_p'$ для любого элемента $g \in G_p$. 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 p-подгруппа в $N(G_p)$). Следовательно, существует единственная одноэлементная орбита $\mathrm{Orb}(G_p) = \{G_p\}$. Отсюда $|\Omega| \equiv 1 \mod p$. □

В качестве применения теорем Силова мы приведем следующий результат, описывающий свойства групп порядка pq, где p и q – простые числа. Напомним, что в случае $p = q$ группа является абелевой. Поэтому мы можем считать, что $p > q$.

Теорема. *Пусть G – группа порядка pq, где p и q – простые числа и $p > q$.*

(i) *Силовская p-подгруппа является нормальной в G.*

(ii) *Если $p \not\equiv 1 \mod q$, то и силовская q-подгруппа является нормальной в G.*

Доказательство. (i) Пусть G_p – силовская p-подгруппа и пусть s_p – число силовских p-подгрупп. По второй теореме Силова

$$s_p = [G : N(G_p)],$$

где $N(G_p)$ – нормализатор G_p в G. 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 $s_p = q$. С другой стороны, $s_p \equiv 1 \mod p$ по третьей теореме Силова. Это противоречит нашему предположению $p > q$.

(ii) Как и выше $s_q = [G : N(G_q)] = p$ или 1. С другой стороны, $s_q \neq p$ поскольку $s_q \equiv 1 \mod q$. □

Замечание. Условие $p \not\equiv 1 \mod q$ в утверждении (ii) необходимо. Действительно, в группе диэдра D_{2p} силовская 2-подгруппа не является нормальной.

Задачи

3.1. Используя действия на множестве вершин, дайте другое вычисление порядков групп движений тетраэдра и куба (задача 0.9).

3.2. Докажите, что группа собственных движений икосаэдра изоморфна A_5.

3.3. Докажите, что $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathrm{S}_3$ и $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathrm{S}_4$. *Указание.* Рассмотрите действие $\mathrm{PGL}_2(\mathbb{F}_q) \curvearrowright \mathbb{P}^1_{\mathbb{F}_q}$.

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

3.5. 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 $H \curvearrowright G/H$.

3.6. Пусть G – группа порядка p^3. Докажите, что любая подгруппа порядка p^2 в G нормальна. Верно ли это для подгрупп порядка p?

3.7. Пусть p-группа G действует на конечном множестве M. Обозначим через $M^G \subset M$ множество неподвижных элементов. Докажите, что число элементов в M сравнимо с числом элементов в M^G по модулю p.

3.8. Докажите, что в p-группе любая нормальная подгруппа нетривиально пересекается с центром.

3.9. Пусть G – p-группа и пусть Z – ее центр. Предположим, что Z имеет порядок p. Докажите, что Z содержится в любой нетривиальной нормальной подгруппе.

3.10. Пусть G – p-группа. Докажите, что для любого l такого, что $p^l \leq |G|$ существует нормальная подгруппа N в G порядка p^l.

3.11. Содержит ли S_4 подгруппу, изоморфную группе кватернионов?

3.12. Содержит ли S_5 подгруппу, изоморфную группе кватернионов?

3.13. Содержит ли S_6 подгруппу, изоморфную группе кватернионов?

3.14. Раскладывается ли силовская 2-подгруппа в S_6 в прямое произведение?

3.15. Найдите центр силовской 2-подгруппы в S_6.

3.16. Найдите коммутант силовской 2-подгруппы в S_6.

3.17. Сколько имеется силовских 2-подгрупп в S_6?

3.18. Докажите, что силовская 2-подгруппа в S_6 является централизатором некоторого элемента порядка 2.

3.19. Докажите, что каждая подгруппа порядка 48 в S_6 содержит ровно три силовские 2-подгруппы.

3.20. Докажите, что все подгруппы порядка 48 в S_6 сопряжены.

3.21. Докажите, что нормализатор подгруппы порядка 48 в S_6 совпадает с этой подгруппой.

3.22. Описать все силовские подгруппы и их нормализаторы в $\mathfrak{A}_5$.

3.23. Описать все силовские подгруппы и их нормализаторы в $\mathfrak{S}_5$.

3.24. Описать силовские p-подгруппы в группе S_{p^2} (p – простое).

3.25. Докажите, что группа порядка pq^2, где p и q – простые числа, не может быть простой.*

3.26. Докажите, что группа порядка pq^3, где p и q – простые числа, не может быть простой.

3.27. Докажите, что группа порядка pq^k, где p и q – простые числа, не может быть простой.

3.28. Докажите, что группа порядка pqr, где p, q и r – простые числа, не может быть простой.

3.29. Докажите, что группа любого из следующих порядков не может быть простой

(a) $36 = 2^2 \cdot 3^2$, $48 = 2^4 \cdot 3$, $96 = 2^5 \cdot 3$, $100 = 2^2 \cdot 5^2$, $108 = 2^2 \cdot 3^3$,

(b) $80 = 2^4 \cdot 5$, $160 = 2^5 \cdot 5$, $112 = 2^4 \cdot 7$,

(c) $72 = 2^3 \cdot 3^2$, $84 = 2^2 \cdot 3 \cdot 7$, $156 = 2^2 \cdot 3 \cdot 13$, $140 = 2^2 \cdot 5 \cdot 7$,

(d) $132 = 2^2 \cdot 3 \cdot 11$,

(e) $126 = 2 \cdot 3^2 \cdot 7$, $150 = 2 \cdot 3 \cdot 5^2$.

3.30. Докажите, что группа порядка 144 не может быть простой.

3.31. Докажите, что группа порядка 120 не может быть простой.

3.32. Докажите, что группа порядка 90 не может быть простой.

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

Лекция 4

Разрешимые группы

4.1 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 $[a, b]^{-1} = [b, a] \in [G, G]$. □

Пример. Группа G абелева тогда и только тогда, когда $[G, G] = \{1\}$.

Теорема. (i) *Пусть $\varphi : G \to G_1$ – гомоморфизм групп. Тогда $\varphi([G, G]) = [\varphi(G), \varphi(G)]$.*

(ii) *Коммутант переходит в себя при всех автоморфизмах группы:*

$$\varphi([G, G]) = [G, G]$$

для любого автоморфизма $\varphi \in \mathrm{Aut}(G)$.

(iii) $[G, G] \lhd G$.

(iv) *Факторгруппа $G/[G, G]$ абелева.*

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

Процесс факторизации по коммутанту называется *абелианизацией* группы.

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

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

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

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

(ii) следует из (i), а (iii) следует из (ii). Утверждение (iv) является частным случаем (v). Докажем (v). Пусть $\pi : G \to G/N$ – естественный гомоморфизм. Тогда согласно (i) имеем $\pi([G, G]) = [G/N, G/N]$. Поэтому G/N – абелева тогда и только тогда, когда $\pi([G, G]) = \{1\}$ тогда и только тогда, когда $[G, G] \subset N$. □

Пример. Пусть G – группа порядка pq, где p и q – простые числа и $p \geq q$. Если она абелева, то $[G, G] = \{1\}$. Это не выполнено только если $q \equiv 0 \mod p$. Пусть G не является абелевой. Мы показали в предыдущей лекции, что $q \equiv 0 \mod p$ и силовская p-подгруппа G_p нормальна в G. Так как факторгруппа G/G_p циклическая, то $[G, G] \subset G_p$. Отсюда следует, что $[G, G] = G_p$.

Пример. Вычислим коммутант группы диэдра D_n. Напомним, что D_n порождается элементами r и s, где r – поворот на угол $2\pi/n$, а s – симметрия относительно оси, проходящей через центр и одну из вершин. Имеются соотношения

$$r^n = s^2 = 1, \quad \text{и} \quad srs^{-1} = r^{-1}.$$

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.

4.2 Разрешимые группы

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

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

Определение. Группа называется *разрешимой*, если $G^{(n)} = \{1\}$ для некоторого n.

Абелева группа всегда разрешима поскольку для нее $G' = \{1\}$. Заметим также, что подгруппа H разрешимой группы G всегда разрешима так как $H^{(n)} \subset G^{(n)}$.

Пример (разрешимость групп порядка pq)**.** Группа порядка pq, где p и q – простые числа разрешима. Действительно, мы показали ранее, что коммутант $[G, G]$ или тривиален, или совпадает с силовской p-подгруппой (если $p > q$ и $p \equiv 1 \mod q$). Во втором случае $G'' = \{1\}$.

Замечание.

Теорема. *Пусть G – группа и пусть $N \lhd G$. Тогда группа G разрешима тогда и только тогда, когда разрешимы группы N и G/N.*

Пример. Из результата предыдущей лекции о p-группах следует, что любая p-группа разрешима.

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. Поскольку подгруппа разрешимой группы разрешима, то для некоторого n имеем

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

Поэтому разрешимы N и G/N.

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

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

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

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

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

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

гомоморфизма ψ являются абелевыми группами, то и группа K_n разрешима. $\square$

Теорема. *При $n \geq 5$ знакопеременная группа A_n не является разрешимой. Более того,*

$$[\mathrm{A}_n, \mathrm{A}_n] = \mathrm{A}_n\,.$$

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

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

Отсюда видно, что $[\mathrm{A}_n, \mathrm{A}_n]$ содержит все тройные циклы. Теперь утверждение легко выводится из следующей леммы. $\square$

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. □

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

$$[\mathrm{SL}_n(\Bbbk),\, \mathrm{SL}_n(\Bbbk)] = \mathrm{SL}_n(\Bbbk).$$

Замечание. На самом деле, можно доказать более сильное утверждение: если $[\mathrm{SL}_n(\Bbbk),\, \mathrm{SL}_n(\Bbbk)] \neq \mathrm{SL}_n(\Bbbk)$, 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, $[\mathrm{SL}_n(\Bbbk),\, \mathrm{SL}_n(\Bbbk)]$ 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 $\mathbf{a}_1, \ldots, \mathbf{a}_n$ – строки матрицы. Если $a_{2,1} = 0$, то преобразованием вида $\mathbf{a}'_2 = \mathbf{a}_2 + \mathbf{a}_i$ для некоторого i мы добьёмся того, что $a'_{2,1} \neq 0$. Далее преобразованием вида $\mathbf{a}'_1 = \mathbf{a}_1 + \lambda\mathbf{a}_2$ добьёмся того, что $a'_{1,1} = 1$. Наконец, преобразованиями вида $\mathbf{a}'_i = \mathbf{a}_i + \lambda\mathbf{a}_1$, $i > 1$ 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. □

Задачи

4.1. Докажите, что коммутант произведения двух групп совпадает с произведением их коммутантов.

4.2. Пусть G – группа всех движений трехмерного куба. Разложите факторгруппу G/G' в прямое произведение примарных циклических.

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

4.4. Вычислите коммутант группы A_4.

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

4.6. Пусть $\mathbb{F}_q$ – конечное поле из q элементов, $q > 2$. Докажите, что группа $\mathrm{PSL}_2(\mathbb{F}_q)$ действует на $\mathbb{P}^1$ только четными подстановками (и, таким образом, имеется инъективный гомоморфизм $\mathrm{PSL}_2(\mathbb{F}_q) \hookrightarrow \mathrm{A}_{q+1}$).

4.7. Докажите, что группы D_n и S_4 разрешимы.

4.8. Вычислите коммутант группы S_n.

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

4.10. Пусть p_1, p_2 и p_3 – различные простые числа. Докажите, что группа порядка $p_1p_2p_3$ разрешима.

4.11. Пусть p – нечетное простое число и пусть G – p-группа такая, что любая подгруппа в ней нормальна. Докажите, что G абелева. Верно ли это для $p = 2$? *Указание.* Сведите утверждение к случаю, когда $[G, G]$ – циклическая группа порядка p, содержащаяся в любой подгруппе (в частности, все подгруппы в G – циклические). Далее сведите утверждение к случаю, когда G порождается двумя элементами a, b и тогда $c := [a, b]$ порождает $[G, G]$, $a^p \in Z(G)$ и $b^p \in Z(G)$. Пусть $Z(G) = \langle g \rangle$. Тогда $a^p = g^m$, $b^p = g^k$. Положим $a' = ab$. Имеем $ab = cba$. Отсюда $a'^p = (ab)^p = abab \cdots ab = b^p a^p c^{1+\cdots+p} = b^p a^p c^{p(p-1)/2} = b^p a^p = a^p b^p = g^{m+k}$. Таким образом, заменяя пару порождающих a, b на $a' = ab$, b мы пару чисел (m, k) заменим на $(m' = m + k, k)$. Очевидно также, что заменяя a, b на $a' = a^{-1}$, b мы пару чисел (m, k) заменим на $(m' = -m, k)$. Применяя такие преобразования, мы можем уменьшать $\max(|m|, |k|)$ и добиться того, что $m = 1$, т.е. $a^p = 1$. Но тогда $G = \langle a \rangle \times Z(G)$.

Лекция 5

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

- $G = \langle G_1, G_2 \rangle$,
- $G_1 \cap G_2 = \{1\}$,
- $G_1 \lhd G$.

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

Примеры.
- 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.
- $\mathrm{S}_n = \mathrm{A}_n \rtimes \langle (i, j) \rangle$.
- $\mathrm{Aff}_n(\Bbbk) = \mathrm{TranAff}_n(\Bbbk) \rtimes \mathrm{GL}_n(\Bbbk)$, где $\mathrm{GL}_n(\Bbbk)$ отождествляется с подгруппой аффинных преобразований с (фиксированной) неподвижной точкой.

Пусть $G = G_1 \rtimes G_2$. Для элемента $g \in G$ через φ_g мы обозначим соответствующий внутренний автоморфизм. Так как подгруппа G_1 нормальна в G, то $\varphi_g(G_1) = G_1$. Следовательно, ограничение φ_g на G_1 – автоморфизм G_1 (необязательно внутренний). Мы его также обозначим через φ_g. Таким образом, определено отображение

$$\Phi : G \longrightarrow \mathrm{Aut}(G_1), \qquad g \longmapsto \varphi_g.$$

Оно является гомоморфизмом групп. Действительно,

$$\varphi_{g'g''}(a) = (g'g'')a(g'g'')^{-1} = g'(g''ag''^{-1})g'^{-1} = \varphi_{g'}(\varphi_{g''}(a)).$$

Следовательно, $\varphi_{g'g''} = \varphi_{g'} \circ \varphi_{g''}$.

Предложение. *Пусть* $G = G_1 \rtimes G_2$.

(i) *Для любого элемента* $g \in G$ *имеет место единственное разложение* $g = g_1 g_2$, $g_i \in G_i$.

(ii) *Если подгруппы* G_1 *и* G_2 *конечны, то* $|G| = |G_1| \cdot |G_2|$.

(iii) *Для g_i, $g_i' \in G_i$ умножение элементов g_1g_2 и $g_1'g_2'$ может быть выполнено по правилу*

$$(g_1g_2)\cdot(g_1'g_2') = \big(g_1\varphi_{g_2}(g_1')\big)(g_2g_2'), \qquad (*)$$

Доказательство. Заметим, что для $a_i \in G_i$ имеем

$$a_2a_1 = a_2a_1a_2^{-1}a_2 = \varphi_{a_2}(a_1)a_2, \qquad (\dagger)$$

где $\varphi_{a_2}(a_1) \in G_1$. Пользуясь этой формулой можно любое произведение

$$g = b_1^{(1)}b_2^{(1)}b_1^{(2)}b_2^{(2)}\cdots b_1^{(n)}b_2^{(n)}, \qquad b_i^{(j)} \in G_i.$$

привести к виду

$$g = g_1g_2, \qquad g_i \in G_i.$$

Отсюда следует существование разложения в (i). Для доказательства единственности предположим, что $g_1g_2 = g_1'g_2'$, где g_i, $g_i' \in G_i$. Тогда то

$$G_2 \ni g_2g_2'^{-1} = g_1^{-1}g_1' \in G_1$$

Так как $G_1 \cap G_2 = \{1\}$, то $g_2g_2'^{-1} = g_1^{-1}g_1' = 1$, $g_1 = g_1'$ и $g_2 = g_2'$.

Утверждение (ii) непосредственно следует из (i). Для доказательства (iii) пользуясь (†) запишем

$$(g_1g_2)\cdot(g_1'g_2') = \big(g_1(g_2g_1'g_2^{-1})\big)(g_2g_2') = \big(g_1\varphi_{g_2}(g_1')\big)(g_2g_2'). \qquad \square$$

Формула $(*)$ подводит нас к следующему определению.

Определение (внешнее определение)**.** Пусть даны две группы G_1 и G_2 и задан гомоморфизм $\Phi : G_2 \to \mathrm{Aut}(G_1)$. Для $g_2 \in G_2$ положим $\varphi_{g_2} := \Phi(G_2)$. Пусть $G := G_1 \underset{\text{inn}}{\rtimes} G_2$ – декартово произведение G_1 и G_2 (как множеств). Определим умножение на G по правилу:

$$(g_1,\, g_2)\cdot(g_1',\, g_2') = (g_1\varphi_{g_2}(g_1'),\, g_2g_2').$$

Имеются естественные инъективные отображения

$$\begin{aligned} G_1 &\hookrightarrow G, \qquad g_1 \longmapsto (g_1,\, 1),\\ G_2 &\hookrightarrow G, \qquad g_1 \longmapsto (1,\, g_2). \end{aligned}$$

Мы отождествим G_1 и G_2 с их образами при этих отображениях.

Предложение. (i) *Определенное выше умножение определяет группу $G_1 \underset{\text{inn}}{\rtimes} G_2$.*

(ii) *Группа $G_1 \underset{\text{inn}}{\rtimes} G_2$ является полупрямым произведением своих подгрупп G_1 и G_2.*

Доказательство. (i) Проверим ассоциативность. Учитывая (†), мы можем записать

$$\begin{aligned} a := (g_1,\, g_2)\cdot\big((g_1',\, g_2')\cdot(g_1'',\, g_2'')\big) &= (g_1,\, g_2)\cdot\big(g_1'\varphi_{g_2'}(g_1''),\, g_2'g_2''\big) = \big(g_1\varphi_{g_2}(g_1'\varphi_{g_2'}(g_1'')),\, g_1g_2'g_2''\big),\\ b := \big((g_1,\, g_2)\cdot(g_1',\, g_2')\big)\cdot(g_1'',\, g_2'') &= \big(g_1\varphi_{g_2}(g_1'),\, g_2g_2'\big)\cdot(g_1'',\, g_2'') = \big(g_1\varphi_{g_2}(g_1')\varphi_{g_2g_2'}(g_1''),\, g_1g_2'g_2''\big). \end{aligned}$$

Так как

$$g_1\varphi_{g_2}(g_1'\varphi_{g_2'}(g_1'')) = g_1\varphi_{g_2}(g_1')\varphi_{g_2}(\varphi_{g_2'}(g_1'')) = g_1\varphi_{g_2}(g_1')\varphi_{g_2g_2'}(g_1''),$$

то $a = b$. Единицей в нашей группе является $(1, 1)$:

$$(g_1,\, g_2) \cdot (1,\, 1) = (g_1\varphi_{g_2}(1),\, g_2) = (g_1,\, g_2),$$

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

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

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

Следовательно, $G_1 \underset{\text{inn}}{\rtimes} G_2$ – группа.

(ii) Ясно, что $G_1 \cap G_2 = \{(1,\, 1)\}$. Более того, для любого $g = (g_1,\, g_2) \in G$ имеет место однозначное разложение в произведение элементов групп G_i:

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

Наконец, для $(g_1',\, 1) \in G_1$ и $g = (g_1,\, g_2) \in G$ имеем

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

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. $\Phi(G_2) = \{1\}$.

Пример. Пусть p и q – простые числа такие, что p Несложно видеть, что

$$\mathrm{Aut}(\boldsymbol{\mu}_q) \simeq \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^*.$$

где последняя группа – то группа обратимых элементов в кольце $\mathbb{Z}/q\mathbb{Z}$. Она имеет порядок $q-1$. По теореме Лагранжа и первой теореме Силова $\mathrm{Aut}(\boldsymbol{\mu}_q)$ содержит подгруппу порядка p тогда и только тогда, когда $q \equiv 1 \mod p$. Следовательно, при $q \equiv 1 \mod p$ существует нетривиальный гомоморфизм $\boldsymbol{\mu}_p \to \mathrm{Aut}(\boldsymbol{\mu}_q)$ и он задает полупрямое произведение $\boldsymbol{\mu}_p \ltimes \boldsymbol{\mu}_q$, являющееся неабелевой группой порядка pq.

Задачи

5.1. Докажите, что группа S_4 разлагается в полупрямое произведение двумя существенно разными способами.

5.2. Представьте в виде нетривиального полупрямого произведения группу верхнетреугольных матриц.

5.3. Докажите существование неабелевой группы порядка p^3, используя полупрямое произведение $\mathbb{F}_p^2$ с силовской p-подгруппой в $\mathrm{GL}_2(\mathbb{F}_p)$.

5.4. Пусть p и q – различные простые числа. Когда существует неабелева группа порядка pq^2? Дайте полный ответ. *Решение.* Если $p \equiv 1 \mod q$ или $q^2 \equiv 1 \mod p$, то существует нетривиальное полупрямое произведение $\boldsymbol{\mu}_p \rtimes \boldsymbol{\mu}_q$ или $\boldsymbol{\mu}_p \ltimes (\boldsymbol{\mu}_q \times \boldsymbol{\mu}_q)$. Если же оба эти условия не выполняются, то группа должна быть прямым произведением своих силовских подгрупп (см. задачу 3.25).

5.5. Пусть p и q – различные простые числа. Когда существует неабелева группа порядка p^2q^2?

5.6. Пусть p_1, p_2, p_3 – различные простые числа. Когда существует неабелева группа порядка $p_1p_2p_3$? Дайте полный ответ. *Решение.* Если $p_i \equiv 1 \mod p_j$ при $i \neq j$, то существует нетривиальное полупрямое произведение $\boldsymbol{\mu}_{p_i} \rtimes \boldsymbol{\mu}_{p_j}$. Если же все эти условия не выполняются, то по крайней мере одна из силовских подгрупп будет нормальной и действие на ней всей группы сопряжениями будет тривиальным (см. задачу 3.28).

Лекция 6

Простые группы

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

6.1 Композиционный ряд группы

Предложение. *Пусть G – конечная группа. Тогда существует последовательность подгрупп*

$$\{1\} = G_0 \subsetneqq G_1 \subsetneqq \cdots \subsetneqq G_n = G$$

такая, что

- *каждая нормальна G_i в G_{i+1},*
- *факторгруппа G_{i+1}/G_i проста для всех i.*

Такая последовательность называется *композиционным рядом* группы G. Таким образом, композиционный ряд – это цепочка нормальных друг в друге подгрупп, которую нельзя "уплотнить".

Доказательство. Индукция по порядку группы. База индукции очевидна. Мы можем считать, что G не является простой, т.е. в G существует нетривиальная нормальная подгруппа N. Тогда факторгруппа $\bar{G} := G/N$ имеет меньший порядок и по предположению индукции для $\bar{G}$ существует композиционный ряд

$$\{1\} = \bar{G}_0 \subsetneqq \bar{G}_1 \subsetneqq \cdots \subsetneqq \bar{G}_m = \bar{G}.$$

Пусть $\varphi : G \to G/N$ – гомоморфизм факторизации. Положим $G_{n-1} := \varphi^{-1}(\bar{G}_{m-1})$. Тогда гомоморфизм $G \to \bar{G}/\bar{G}_{m-1}$ сюръективен и его ядро совпадает с G_{n-1}. Следовательно,

$$G/G_{n-1} \simeq \bar{G}/\bar{G}_{m-1}.$$

Эта группа является простой, а для G_{n-1} композиционный ряд существует по предположению индукции. □

Замечание. Конечная группа G является разрешимой тогда и только тогда, когда ее (любой) композиционный ряд имеет только абелевы факторгруппы G_{i+1}/G_i.

Далее мы рассмотрим некоторые серии простых неабелевых групп.

6.2 Простота знакопеременных групп

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

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

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. □

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 2, то по первой теореме Силова в H_1 существует элемент σ порядка 2. Пусть $\sigma = \sigma_1 \cdots \sigma_k$ – разложение в произведение независимых транспозиций. Тогда

$$H_1 \ni \sigma = \sigma_1\sigma\sigma_1^{-1} \in \sigma_1 H_1 \sigma_1^{-1} = H_2$$

Последнее противоречие доказывает теорему. □

6.3 Простота проективных линейных групп

Напомним, что проективная линейная группа – это факторгруппа

$$\mathrm{PGL}_n(\Bbbk) := \mathrm{GL}_n(\Bbbk)/\{\lambda E \mid \lambda \in \Bbbk^*\},$$

а специальная проективная линейная группа $\mathrm{PSL}_n(\Bbbk)$ – это образ $\mathrm{SL}_n(\Bbbk)$ в $\mathrm{PGL}_n(\Bbbk)$.

Теорема. *При $n \geq 2$ группа $\mathrm{PSL}_n(\Bbbk)$ проста за исключением двух случаев:*

$$\mathrm{PSL}_2(\mathbb{F}_2) \quad \text{и} \quad \mathrm{PSL}_2(\mathbb{F}_3),$$

где $\mathbb{F}_q$ – поле из q элементов.

Мы докажем эту теорему только для случая $n = 2$. Доказательство основывается на следующем предложении.

Предложение. *Пусть поле $\Bbbk$ содержит не менее четырех элементов и пусть $N \lhd \mathrm{SL}_2(\Bbbk)$ нетривиальная нормальная подгруппа, содержащая $-E$. Тогда $N = \{\pm E\}$.*

Сначала докажем лемму.

Лемма (разложение Брюа)**.** *Положим*

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad b_{\lambda,\mu} := \begin{pmatrix} \lambda & \mu \\ 0 & \lambda^{-1} \end{pmatrix}, \qquad B := \left\{ b_{\lambda,\mu} \mid \lambda \in \Bbbk^*, \quad \mu \in \Bbbk \right\}.$$

Тогда

$$\mathrm{SL}_2(\Bbbk) = B \cup BwB, \qquad B \cap BwB = \varnothing.$$

Доказательство. Пусть $\mathbf{e}_1$, $\mathbf{e}_2$ – стандартный базис в пространстве столбцов. Ясно, что

$$\begin{aligned} b_{\lambda,\mu}\,\mathbf{e}_1 &= \lambda \mathbf{e}_1 = \begin{pmatrix} \lambda \\ 0 \end{pmatrix}, \\ b_{\lambda,\mu}\,w\,\mathbf{e}_1 &= -b_{\lambda,\mu}\,\mathbf{e}_2 = \begin{pmatrix} \mu \\ \lambda^{-1} \end{pmatrix}. \end{aligned} \tag{$*$}$$

Пусть $g \in \mathrm{SL}_2(\Bbbk)$ – произвольный элемент. Рассмотрим вектор

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} := g\,\mathbf{e}_1.$$

Предположим, что $x_2 = 0$. Тогда $x_1 \neq 0$. Согласно $(*)$, существует элемент $b \in B$ такой, что $b\,\mathbf{e}_1 = \mathbf{x} = g\,\mathbf{e}_1$. Тогда $\mathbf{e}_1$ – собственный вектор для $g^{-1}b$ и, значит, $g^{-1}b \in B$. Следовательно, $g \in B$.

Пусть $x_2 \neq 0$. Тогда $b\,w\,\mathbf{e}_1 = \mathbf{x} = g\,\mathbf{e}_1$ для некоторого $b \in B$. Отсюда следует, что $\mathbf{e}_1$ – собственный вектор для $g^{-1}bw$ и, значит, $g^{-1}bw \in B$. Следовательно, $g \in BwB$. Таким образом, мы показали, что $\mathrm{SL}_2(\Bbbk) = B \cup BwB$.

Наконец, если $g \in B \cap BwB$, то $g = b'wb'' \in B$ для некоторых $b', b'' \in B$. Но тогда $w = b'^{-1}gb''^{-1} \in B$. Противоречие. $\square$

Доказательство предложения. Из разложения Брюа следует, что B не содержится в другой подгруппе, отличной от $\mathrm{SL}_2(\Bbbk)$. Действительно, если H – подгруппа такая, что $B \subsetneqq H \subsetneqq \mathrm{SL}_2(\Bbbk)$, то для $h \in H \setminus B$ мы имеем $h \in BwB$, т.е. $h = b'wb''$ для некоторых $b', b'' \in B$. Но тогда $w = b'^{-1}hb''^{-1} \in H$. Следовательно, $H = \mathrm{SL}_2(\Bbbk)$. Противоречие.

Далее, пусть $N \lhd \mathrm{SL}_2(\Bbbk)$, $N \supset \{\pm 1\}$. Тогда NB – подгруппа в $\mathrm{SL}_2(\Bbbk)$. Согласно сказанному выше, $NB = B$ или $NB = \mathrm{SL}_2(\Bbbk)$.

Во первом случае имеем $N \subset B$. Но тогда $\mathbf{e_1}$ – собственный вектор для любого элемента $h \in N$, т.е. $h\mathbf{e_1} = \lambda_h \mathbf{e_1}$, $\lambda_h \in \Bbbk$ и для любого $g \in \mathrm{SL}_2(\Bbbk)$ имеем

$$h(g\mathbf{e_1}) = g(g^{-1}hg)\mathbf{e_1} = gh'\mathbf{e_1} = \lambda_{h'} g\mathbf{e_1},$$

где $h' := g^{-1}hg) \in N$. Таким образом, $g\mathbf{e_1}$ – также собственный вектор для h. Так как $g\mathbf{e_1}$ может быть любым ненулевым вектором, то h – скалярная матрица. Противоречие.

Во втором случае $w = hb$ для некоторых $h \in N$ и $b \in B$. Положим

$$U := \{b_{1,\mu} \mid \mu \in \Bbbk\} = \left\{ \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \;\middle|\; \mu \in \Bbbk \right\}, \qquad U^{\mathrm{t}} := \left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} \;\middle|\; \mu \in \Bbbk \right\}.$$

Так как N нормальна в $\mathrm{SL}_2(\Bbbk)$, то для любого $u \in U$ имеем

$$huh^{-1} = h(uh^{-1}u^{-1})u \in NU$$

Следовательно,

$$U^{\mathrm{t}} = wUw^{-1} = hbUb^{-1}h^{-1} = hUh^{-1} \subset NU.$$

Так как U^{t} и U порождают $\mathrm{SL}_2(\Bbbk)$, то $NU = \mathrm{SL}_2(\Bbbk)$. Тогда группа

$$\mathrm{SL}_2(\Bbbk)/N = NU/N \simeq U/U \cap N$$

является абелевой. Значит $N \supset [\mathrm{SL}_2(\Bbbk), \mathrm{SL}_2(\Bbbk)] = \mathrm{SL}_2(\Bbbk)$. □

Доказательство теоремы. Пусть $N \lhd \mathrm{PSL}_2(\Bbbk)$ нетривиальная нормальная подгруппа, пусть $\pi : \mathrm{SL}_2(\Bbbk) \to \mathrm{PSL}_2(\Bbbk)$ – естественный гомоморфизм и пусть $\tilde{N} := \pi^{-1}(N)$. Тогда $\tilde{N} \lhd \mathrm{SL}_2(\Bbbk)$, $\tilde{N} \neq \mathrm{SL}_2(\Bbbk)$ и $\tilde{N} \neq \{\pm 1\}$. Это противоречит предложению. □

Замечание. Имеют место изоморфизмы:

- $\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathrm{S}_3$ (см. задачу 3.3),
- $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathrm{A}_4$ (см. задачу 3.3),
- $\mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathrm{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$ (см. задачи 3.4 и 6.7),
- $\mathrm{PSL}_2(\mathbb{F}_9) \simeq \mathrm{A}_6$.

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

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

6.4 Простота специальной ортогональной группы

Напомним, что ортогональная группа $\mathrm{SO}_n(\mathbb{R})$ – это группа всех ортогональных операторов с определителем 1 в n-мерном вещественном пространстве. При $n = 2$ эта группа абелева:

$$\mathrm{SO}_n(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \;\middle|\; \alpha \in \mathbb{R} \right\} \simeq \mathbb{R}/2\pi\mathbb{R}.$$

При $n > 2$ центр группы $\mathrm{SO}_n(\mathbb{R})$ тривиален, если n нечетно и порождается скалярной матрицей $-E$, если n четно (см. задачу 6.8).

Далее мы докажем простоту специальной ортогональной группы $\mathrm{SO}_3(\mathbb{R})$. Напомним, что любой ортогональный оператор с определителем 1 в трехмерном пространстве в некотором базисе может быть записан матрицей

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}$$

т.е. он является поворотом вокруг некоторой прямой. Поворот вокруг прямой l на угол α мы будем обозначать $r_{l,\alpha}$.

Теорема. *Группа* $\mathrm{SO}_3(\mathbb{R})$ *проста.*

Предположим, что группа $\mathrm{SO}_3(\mathbb{R})$ не является простой и пусть N – ее нормальная подгруппа, отличная от единичной. Пусть $r_{l,\alpha}$ – неединичный элемент (поворот на угол $\alpha \not\equiv 0 \mod 2\pi$).

Лемма. *Для любых двух элементов* r, $r' = r_{l,\alpha} \in \mathrm{SO}_3(\mathbb{R})$ *верно равенство*

$$r\, r_{l,\alpha}\, r^{-1} = r_{r(l),\alpha}.$$

Следствие. *Если нормальная подгруппа* $N \lhd \mathrm{SO}_3(\mathbb{R})$ *содержит поворот на угол* α*, то она содержит и все повороты на этот угол.*

Лемма. *Для любых двух элементов* $r = r_{l,\pi}$, $r' = r_{l',\pi} \in \mathrm{SO}_3(\mathbb{R})$, $l \neq l''$ *верно равенство*

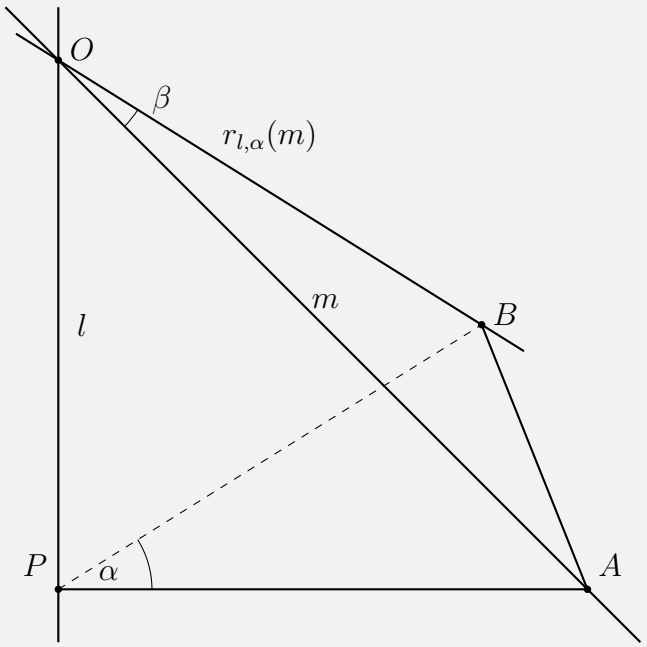
$$r_{l,\pi}\, r_{l',\pi} = r_{l'',2\beta},$$

где l'' *– прямая, перпендикулярная* l *и* l'*, а* β *– угол между* l *и* l'*.*

Следствие. *Если нормальная подгруппа* $N \lhd \mathrm{SO}_3(\mathbb{R})$ *содержит поворот на угол* π*, то* $N = \mathrm{SO}_3(\mathbb{R})$*.*

Лемма. *Для любого поворота* $r_{l,\alpha}$, $0 < \alpha < \pi$ *и для любого* $0 < \beta < \alpha$ *существует прямая* m *такая, что угол* β *между* m *и* $r_{l,\alpha}(m)$ *равен* β*.*

Доказательство. Проведем плоскость Π, не проходящую через начало координат и перпендикулярную l. Положим $P := \Pi \cap l$ и $h := OP$. Для любого $p > 0$ мы можем взять в плоскости Π точку A, отстоящую от P на расстояние p. Пусть $B := r_{l,\alpha}(A)$ и пусть m – прямая, соединяющая точки O и A. Тогда $r_{l,\alpha}(m)$ будет прямой, соединяющей точки O и B. Положим $OA = a$. Ясно, что треугольники OPA и OPB прямоугольны и равны.



Применим теорему косинусов в равнобедренных треугольниках OAB и PAB:

$$2a^2 - 2a^2\cos\beta = 2p^2 - 2p^2\cos\alpha, \qquad a^2 = p^2\,\frac{1-\cos\alpha}{1-\cos\beta}.$$

Теперь применим теорему Пифагора в треугольнике OPA:

$$h^2 + p^2 = a^2.$$

Отсюда

$$h^2 + p^2 = p^2\,\frac{1-\cos\alpha}{1-\cos\beta}, \qquad p^2 = h^2\,\frac{1-\cos\beta}{\cos\beta-\cos\alpha}.$$

Для $0 < \beta < \alpha$ правая часть последнего выражения положительна. Следовательно, для $0 < \beta < \alpha$ мы можем найти h такое, что угол между m и $r_{l,\alpha}(m)$ равен β. □

Следствие. *Если нормальная подгруппа $N \lhd \mathrm{SO}_3(\mathbb{R})$ содержит нетривиальный поворот на угол α, то она содержит и все повороты на углы γ для $0 < \gamma < 2\alpha$.*

Доказательство. Согласно последнему следствию мы можем считать, что $0 < \alpha < \pi$. Пусть $r := r_{l,\alpha}$. Для любых прямых l и m имеем $r_{m,\pi}\, r^{-1}\, r_{m,\pi} \in N$. Следовательно,

$$r_{r(m),\pi}\, r_{m,\pi} = (r\, r_{m,\pi}\, r^{-1})\, r_{m,\pi} = r\,(r_{m,\pi}\, r^{-1}\, r_{m,\pi}) \in N.$$

Таким образом, N содержит повороты на углы 2γ, где γ – угол между прямыми m и $r(m)$. По предыдущей лемме γ может принимать все значения $0 < \gamma < \alpha$. □

Окончание доказательства теоремы. Согласно последнему следствию мы можем считать, что подгруппа $N \lhd \mathrm{SO}_3(\mathbb{R})$ содержит и все повороты $r_{l,\gamma}$ на углы γ для $0 < \gamma < 2\alpha$. Беря их кратности, мы получим, что N содержит повороты на любые углы. □

Известно, что группа $\mathrm{SO}_n(\mathbb{R})$ является простой для любого нечетного $n \geq 3$, а группа $\mathrm{SO}_n(\mathbb{R})/\{\pm E\}$ является простой для любого четного $n \geq 6$. Отметим, однако, что группа $\mathrm{SO}_4(\mathbb{R})/\{\pm E\}$ простой не является.

Задачи

6.1. 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.

6.2. Опишите классы сопряженных элементов в A_6.

6.3. Докажите, что $\mathrm{PSL}_n(\Bbbk)$ – нормальная подгруппа в $\mathrm{PGL}_n(\Bbbk)$ для любого поля $\Bbbk$. Если поле $\Bbbk$ конечно, то чему равен индекс $[\mathrm{PGL}_n(\Bbbk) : \mathrm{PSL}_n(\Bbbk)]$?

6.4. Докажите, что группа $\mathrm{SL}_n(\mathbb{C})$ порождается элементами конечного порядка.

6.5. Пусть $\mathbb{F}_q$ – поле из q элементов, где q – четное, $q > 2$. Докажите, что группа $\mathrm{PGL}_2(\mathbb{F}_q)$ действует на $\mathbb{P}^1$ только четными подстановками (и, таким образом, имеется инъективный гомоморфизм $\mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow \mathrm{A}_{q+1}$, ср. с задачей 4.6).

6.6. Пусть $\mathbb{F}_q$ – поле из q элементов, где q – нечетное. Докажите, что группа $\mathrm{PGL}_2(\Bbbk)$ не может действовать на $\mathbb{P}^1$ только четными подстановками (ср. с задачами и 4.6 и 6.5).

6.7. Докажите, что простая группа порядка 60 изоморфна $\mathfrak{A}_5$.

6.8. Докажите, что центр группы $\mathrm{SO}_n(\mathbb{R})$, $n \geq 3$ тривиален, если n нечетно и порождается скалярной матрицей $-E$ при четном n.

Лекция 7

Кольца, идеалы, модули, гомоморфизмы

7.1 Кольца

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

- R является абелевой группой относительно сложения;
- $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad$ для любых элементов a, b, $c \in R$.

Кольцо называется *ассоциативным*, если выполнено свойство

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

Кольцо называется *коммутативным*, если выполнено свойство

$$a \cdot b\cdot = b \cdot a \qquad \forall a,\, b \in R.$$

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

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

(если такой существует). Заметим, что единица единственна, если она существует.

Центром кольца R называется множество

$$Z(R) := \{a \in R \mid a \cdot x = x \cdot a \quad \forall x \in R\},$$

т.е. это множество элементов, которые коммутируют со всеми элементами R. Ясно, что $Z(R)$ является подкольцом в R.

Примеры. (i) Стандартными примерами коммутативных ассоциативных колец с единицей являются кольцо целых чисел $\mathbb{Z}$, кольца вычетов $\mathbb{Z}/n\mathbb{Z}$ и кольца многочленов $R[x]$ (над коммутативным ассоциативным кольцом с единицей). Целые четные числа образуют коммутативное ассоциативное кольцо без единицы.

(ii) 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.

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

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

$$[a, b] = a \cdot b - b \cdot a.$$

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

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

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

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

Определение. Подмножество $R_0 \subset R$ кольца R называется *подкольцом*, если R_0 является кольцом с теми же операциями сложения и умножения.

Ясно, что $R_0 \subset R$ является подкольцом, если для любых элементов для любых элементов $a,\, b \in R_0$ их сумма $a + b$, разность $a - b$ и произведение $a \cdot b$ лежат в R_0.

Определение. *Делителями нуля* в кольце R называются элементы $a,\, b \in R$ такие, что $a \cdot b = 0$, 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 $\mathbb{Z}/n\mathbb{Z}$ – это ненулевые классы вычетов, имеющие общий делитель с n.

Определение. Если R – кольцо с единицей, то элемент $a \in R$ называется *обратимым*, если существует $a^{-1} \in R$ такой, что $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

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 ассоциативное кольцо R является *кольцом с делением*, если в R имеется единица и любой ненулевой элемент является обратимым, т. е. $R^* = R \setminus \{0\}$. Ассоциативное кольцо с делением также называется *телом*. Таким образом, *поле* – это коммутативное тело.

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

Если для подгруппы $\mathfrak{I} \subset R$ выполнено только одно включение $a\mathfrak{I} \subset \mathfrak{I}$ (соответственно, $\mathfrak{I}a \subset \mathfrak{I}$) для любого $a \in R$, то $\mathfrak{I}$ называется *левым* (соответственно, *правым идеалом*).

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

(ii) Четные числа – идеал в кольце $\mathbb{Z}$.

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

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

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

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

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

Замечание. Если $\mathfrak{I}_1$ и $\mathfrak{I}_2$ – идеалы кольца R, то их сумма $\mathfrak{I}_1 + \mathfrak{I}_2 := \{x_1 + x_2 \mid x_1 \in \mathfrak{I}_1,\ x_2 \in \mathfrak{I}_2\}$ является идеалом в R. Пересечение $\mathfrak{I}_1 \cap \mathfrak{I}_2$ идеалов – также идеал. Однако, объединение идеалов, в общем случае, идеалом не является.

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

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

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*.

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

Определение. *Гомоморфизмом колец* называется отображение

$$\varphi : R \longrightarrow R_1$$

такое, что

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ и } \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \text{для любых элементов } a,\ b \in R.$$

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).

Ядром гомоморфизма $\varphi : R \to R_1$ называется подмножество

$$\mathrm{Ker}(\varphi) := \{a \in R \mid \varphi(a) = 0\}.$$

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

(ii) 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.

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

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

является гомоморфизмом.

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

$$a' \cdot b' - a \cdot b = a \cdot d + c \cdot b + c \cdot d \in \mathfrak{I}$$

и поэтому $a' \cdot b' + \mathfrak{I} = a \cdot b + \mathfrak{I}$. Кольцо $R/\mathfrak{I}$ называется *факторкольцом*.

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

(i) $\mathfrak{I} := \mathrm{Ker}(\varphi)$ – *идеал в* R, $\varphi(R)$ – *подкольцо в* R_1.

(ii) *Имеется естественный изоморфизм колец* $\varphi(R) \simeq R/\mathfrak{I}$.

Доказательство. Воспользуемся теоремой о гомоморфизме групп. Из нее следует, что $\mathfrak{I}$ – подгруппа аддитивной группы R, $\varphi(R)$ – подгруппа аддитивной группы R_1 и имеется естественный изоморфизм групп

$$\psi : R/\mathfrak{I} \longrightarrow \varphi(R), \qquad \psi(a + \mathfrak{I}) = \varphi(a).$$

Ясно, что для любых $a \in R$, $x \in \mathfrak{I}$ выполнено $\varphi(a \cdot x) = a \cdot \varphi(x) = 0$ и $\varphi(x \cdot a) = \varphi(x) \cdot a = 0$, т.е. $a \cdot x \in \mathfrak{I}$ и $x \cdot a \in \mathfrak{I}$. Значит, $\mathfrak{I}$ – идеал. Аналогично, для любых a, $b \in \varphi(R)$ существуют элементы $\tilde{a}$, $\tilde{b} \in R$ такие, что $\varphi(\tilde{a}) = a$, $\varphi(\tilde{b}) = b$. Отсюда

$$a \cdot b = \varphi(\tilde{a}) \cdot \varphi(\tilde{b}) = \varphi(\tilde{a} \cdot \tilde{b}) \in \varphi(M).$$

Значит, $\varphi(M)$ – подкольцо.

Остается доказать, что ψ – гомоморфизм колец:

$$\psi((a + \mathfrak{I}) \cdot (b + \mathfrak{I})) = \psi(a \cdot b + \mathfrak{I}) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \psi(a + \mathfrak{I}) \cdot \psi(b + \mathfrak{I}). \qquad \square$$

7.2 Простота кольца матриц

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

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

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

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

Проверим, что $\mathfrak{I}_R$ – идеал в R:

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

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

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

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

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

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

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

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

7.3 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 $R \times M \to M$, $(a, \mathbf{x}) \mapsto a\mathbf{x}$ умножения элементов M на элементы R, удовлетворяющая аксиомам векторного пространства:

- $a(\mathbf{x} + \mathbf{y}) = a\mathbf{x} + a\mathbf{y}$ для любого элемента $a \in R$, для любых элементов $\mathbf{x}$, $\mathbf{y} \in M$;
- $(a + b)\mathbf{x} = a\mathbf{x} + b\mathbf{x}$ для любых элементов a, $b \in R$, для любого элемента $\mathbf{x} \in M$;
- $(ab)\mathbf{x} = a(b\mathbf{x})$ для любых элементов a, $b \in R$, для любого элемента $\mathbf{x} \in M$;
- $1\,\mathbf{x} = \mathbf{x}$ для любого элемента $\mathbf{x} \in M$.

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

(ii) Кольцо R является модулем над собой.

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

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

(v) 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

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

(vi) 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.

(vii) 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

$$a\mathbf{x} = \phi(a)\mathbf{x} \qquad a \in R, \quad \mathbf{x} \in M_1.$$

В частности, для любого идеала $\mathfrak{I} \subset R$ факторкольцо $R/\mathfrak{I}$ 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).

Определение. Подмножество $M_0 \subset M$ R-модуля M называется *подмодулем*, если M_0 является модулем с теми же операциями сложения и умножения на элементы R.

Ясно, что $M_0 \subset M$ является подмодулем, если для любых элементов для любых элементов $\mathbf{x}$, $\mathbf{y} \in M_0$ их сумма $\mathbf{x} + \mathbf{y}$ лежит в M_0 и для любых элементов $a \in R$, $\mathbf{x} \in M_0$ произведение $a\mathbf{x}$ также лежит в M_0.

Определение. *Гомоморфизмом R-модулей* называется отображение $\varphi : M \to N$ такое, что $\varphi(\mathbf{x} + \mathbf{y}) = \varphi(\mathbf{x}) + \varphi(\mathbf{y})$ для любых элементов $\mathbf{x}$, $\mathbf{y} \in M$ и $\varphi(a\mathbf{x}) = a\varphi(\mathbf{x})$ для любых элементов $a \in R$, $\mathbf{x} \in M$.

Ядром гомоморфизма $\varphi : M \to N$ R-модулей называется подмножество

$$\mathrm{Ker}(\varphi) := \{\mathbf{x} \in M \mid \varphi(\mathbf{x}) = 0\}.$$

Определение. Пусть M_0 – подмодуль R-модуля M. На факторгруппе M/M_0 аддитивной группы определим умножение на элементы R по правилу

$$a(\mathbf{x} + M_0) = a\mathbf{x} + M_0.$$

Несложно проверить, что это определение не зависит от вида записи смежного класса $\mathbf{x} + M_0$.

Действительно, пусть $\mathbf{x} + M_0 = \mathbf{x}' + M_0$. Тогда $\mathbf{x}' = \mathbf{x} + \mathbf{u}$ для некоторого $\mathbf{u} \in M_0$. Отсюда

$$a(\mathbf{x}' + M_0) = a\mathbf{x}' + M_0 = a(\mathbf{x} + \mathbf{u}) + M_0 = (a\mathbf{x} + a\mathbf{u}) + M_0 = (a\mathbf{x} + M_0) + (a\mathbf{u} + M_0).$$

Так как $a\mathbf{u} \in M_0$, то $a\mathbf{u} + M_0 = M_0$ и поэтому

$$a(\mathbf{x}' + M_0) = a(\mathbf{x} + M_0).$$

Модуль M/M_0 называется *фактормодулем*.

Для модулей также имеет место теорема о гомоморфизме.

Теорема (теорема о гомоморфизме модулей)**.** *Пусть $\varphi : M \to N$ – гомоморфизм R-модулей. Тогда*

(i) $\operatorname{Ker}(\varphi)$ – *подмодуль в M, $\varphi(M)$ – подмодуль в N.*

(ii) *Имеется естественный изоморфизм $\varphi(M) \simeq M/\operatorname{Ker}(\varphi)$.*

Доказательство. Положим $M_0 := \operatorname{Ker}(\varphi)$. Воспользуемся теоремой о гомоморфизме групп. Из нее следует, что M_0 – подгруппа аддитивной группы M, $\varphi(M)$ – подгруппа аддитивной группы N и имеется естественный изоморфизм групп

$$\psi : M/M_0 \longrightarrow \varphi(M), \qquad \psi(\mathbf{x} + M_0) = \varphi(\mathbf{x}).$$

Ясно, что для любых $a \in R$, $\mathbf{x} \in M_0$ выполнено $\varphi(a\mathbf{x}) = a\varphi(\mathbf{x}) = 0$, т.е. $a\mathbf{x} \in M_0$. Значит, M_0 – подмодуль. Аналогично, для любых $a \in R$, $\mathbf{y} \in \varphi(M)$ существует элемент $\mathbf{x} \in M$ такой, что $\varphi(\mathbf{x}) = \mathbf{y}$. Отсюда

$$a\mathbf{y} = a\varphi(\mathbf{x}) = \varphi(a\mathbf{x}) \in \varphi(M).$$

Значит, $\varphi(M)$ – также подмодуль.

Остается доказать, что ψ – гомоморфизм колец:

$$\psi\big((\mathbf{x} + M_0)(\mathbf{y} + M_0)\big) = \psi(\mathbf{xy} + M_0) = \varphi(\mathbf{xy}) = \varphi(\mathbf{x})\varphi(\mathbf{y}) = \psi(\mathbf{x} + M_0)\psi(\mathbf{y} + M_0). \qquad \square$$

Определение. Пусть M – R-модуль и пусть $M_1, \ldots, M_n$ – его подмодули. Говорят, что M является *прямой суммой* этих подмодулей, если любой элемент $\mathbf{x} \in M$ однозначно представляется в виде

$$\mathbf{x} = \mathbf{x}_1 + \cdots + \mathbf{x}_n, \qquad \mathbf{x}_i \in M_i.$$

* * *

Пусть M – модуль над ассоциативным кольцом R с единицей.

Определение. Элементы $\mathbf{x}_1, \ldots, \mathbf{x}_r \in M$ называются *линейно зависимыми*, если некоторая их нетривиальная целочисленная линейная комбинация

$$a_1\mathbf{x}_1 + \cdots + a_r\mathbf{x}_r$$

с коэффициентами $a_i \in R$ равна нулю. Набор элементов $\mathbf{e}_1, \ldots, \mathbf{e}_r$ называется *базисом* модуля M, если выполнены два условия

- $\mathbf{e}_1, \ldots, \mathbf{e}_r$ порождают M;
- $\mathbf{e}_1, \ldots, \mathbf{e}_r$ линейно независимы.

Модуль M, обладающий базисом, называется *свободным*. Число элементов базиса называется *рангом* M и обозначается $\operatorname{rk}(M)$. *

Замечание. Несложно видеть, что элементы $\mathbf{e}_1, \ldots, \mathbf{e}_r \in M$ образуют базис тогда и только тогда, когда любой элемент $\mathbf{x} \in M$ *однозначно* представляется в виде целочисленной линейной комбинации

$$\mathbf{x} = a_1\mathbf{e}_1 + \cdots + a_r\mathbf{e}_r, \quad a_i \in R.$$

*Мы рассматриваем только конечно пороженные модули

Задачи

7.1. Докажите, что для любой абелевой группы A имеет место изоморфизм $\mathrm{Aut}(A) \simeq \mathrm{End}(A)^*$.

7.2. Найдите кольцо эндоморфизмов $\mathrm{End}(A)$ циклической группы $A = \mathbb{Z}/n\mathbb{Z}$ и свободной абелевой группы $A = \mathbb{Z}^n$.

7.3. Докажите, что $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, где в левой части $\mathbb{Z}/n\mathbb{Z}$ рассматривается как группа, а в правой части – как кольцо.

7.4. Пусть p – простое число и пусть $R \subset \mathbb{Q}$ – подкольцо, состоящее из элементов n/m, где m не делится на p. Какие в этом кольце есть простые идеалы?

7.5. Докажите, что любой автоморфизм кольцо многочленов $\Bbbk[t]$ над полем задается формулой $\varphi : t \longmapsto at + b$, $a \in \Bbbk^*$, $b \in \Bbbk$.

7.6. Пусть R – ассоциативное кольцо с единицей, без делителей нуля. Докажите, что в R каждый элемент, имеющий односторонний обратный, имеет и двусторонний обратный.

7.7. Пусть R – ассоциативное кольцо из конечного числа элементов. Докажите, что

(a) если R не имеет делителей нуля, то оно имеет единицу и все его ненулевые элементы обратимы;

(b) если R имеет единицу, то каждый элемент $a \in R$, имеющий односторонний обратный, имеет и двусторонний обратный;

(c) если R имеет единицу, то всякий левый делитель нуля является правым делителем нуля.

7.8. Пусть R – ассоциативное кольцо с единицей. Докажите, что

(a) если произведения ab и ba элементов $a, b \in R$ обратимы, то и элементы a и b также обратимы;

(b) если R не имеет делителей нуля и произведение ab обратимо, то a и b обратимы;

(c) если обратим элемент $1 + ab$, то обратим и элемент $1 + ba$.

7.9. Найдите все (с точностью до изоморфизма) коммутативные двумерные алгебры а) над $\mathbb{C}$; а) над $\mathbb{R}$.

7.10. Докажите, что $\mathbb{R}^3$ как кольцо с векторным умножением является простым.

7.11. Докажите, что в кольце матриц $\mathrm{Mat}_n(\Bbbk)$ над полем любой левый идеал имеет вид

$$\mathfrak{I}_B := \{A \in \mathrm{Mat}_n(\Bbbk) \mid AB = 0\},$$

где B – некоторая фиксированная матрица.

Лекция 8

Коммутативные кольца

8.1 Простые и максимальные идеалы.

Идеал $\mathfrak{P}$ кольца R называется *простым*, если из того, что $ab \in \mathfrak{P}$ следует или $a \in \mathfrak{P}$ или $b \in \mathfrak{P}$. Идеал $\mathfrak{M} \subset R$ называется *максимальным*, если любой идеал, содержащий $\mathfrak{M}$ или совпадает с $\mathfrak{M}$, или является единичным.

Предложение. *Пусть R – коммутативное ассоциативное кольцо с единицей $1 \neq 0$ и пусть $\mathfrak{I} \subset R$ – любой идеал.*

(i) *Если $\mathfrak{I}$ максимальный, то он прост.*

(ii) *Факторкольцо $R/\mathfrak{I}$ не имеет делителей нуля тогда и только тогда, когда $\mathfrak{I}$ простой.*

(iii) *Факторкольцо $R/\mathfrak{I}$ является полем тогда и только тогда, когда $\mathfrak{I}$ максимальный.*

Доказательство. (i) Пусть $ab \in \mathfrak{I}$. Предположим, что $a \notin \mathfrak{I}$. Рассмотрим идеал $\tilde{\mathfrak{I}}$, порожденный $\mathfrak{I}$ и элементом a. Он состоит из элементов вида $x + ar$, где $x \in \mathfrak{I}$, $r \in R$. Так как $a \notin \mathfrak{I}$, то $\tilde{\mathfrak{I}} \neq \mathfrak{I}$. Так как $\mathfrak{I}$ максимальный, то $\tilde{\mathfrak{I}} = R$. В частности, $1 \in \tilde{\mathfrak{I}}$. Значит для некоторых $x \in \mathfrak{I}$, $r \in R$ мы можем записать $1 = x + ar$. Отсюда $b = bx + abr \in \mathfrak{I}$. Следовательно, $\mathfrak{I}$ – простой идеал.

Далее рассмотрим канонический гомоморфизм $\varphi : R \to R/\mathfrak{I}$.

(ii) Пусть факторкольцо $R/\mathfrak{I}$ не имеет делителей нуля и пусть $ab \in \mathfrak{I}$, где $a \notin \mathfrak{I}$. Тогда

$$\varphi(a)\varphi(b) = \varphi(ab) = 0.$$

Так как $a \notin \mathfrak{I}$, то $\varphi(a) \neq 0$. Так как $R/\mathfrak{I}$ не имеет делителей нуля, то $\varphi(b) = 0$. Значит, $b \in \mathfrak{I}$ и, следовательно, $\mathfrak{I}$ – простой идеал.

Пусть идеал $\mathfrak{I}$ прост и пусть $xy = 0$ для некоторых x, $y \in R/\mathfrak{I}$, причем $x \neq 0$. Существуют элементы $\tilde{x}$, $\tilde{y} \in R$ такие, что $\varphi(\tilde{x}) = x$, $\varphi(\tilde{y}) = y$. Тогда $\varphi(\tilde{x}\tilde{y}) = xy = 0$. Отсюда $\tilde{x}\tilde{y} \in \mathfrak{I}$. Так как $\varphi(\tilde{x}) = x \neq 0$, то $\tilde{x} \notin \mathfrak{I}$. Так как идеал $\mathfrak{I}$ прост, то $\tilde{y} \in \mathfrak{I}$. Значит, $y = \varphi(\tilde{y}) = 0$.

(iii) Пусть факторкольцо $R/\mathfrak{I}$ является полем. Предположим, что существует идеал $\tilde{\mathfrak{I}}$ такой, что $\mathfrak{I} \subsetneqq \tilde{\mathfrak{I}} \neq R$. Возьмем любой элемент $a \in \tilde{\mathfrak{I}} \setminus \mathfrak{I}$. Тогда элемент $\bar{a} := \varphi(a)$ обратим. Следовательно, существует $\bar{b} \in R/\mathfrak{I}$ такой, что $\bar{b}\bar{a} = 1$. Пусть $b \in R$ – любой прообраз $\bar{b}$. Тогда $ba = 1 + x$ для некоторого $x \in \mathfrak{I}$. Следовательно, $1 = ba - x \in \tilde{\mathfrak{I}}$, т.е. $\tilde{\mathfrak{I}} = R$. Противоречие.

Наконец, пусть $\mathfrak{I}$ – максимальный идеал. Возьмем любой ненулевой элемент $x \in R/\mathfrak{I}$. Пусть $\tilde{x} \in R$ – его прообраз. Тогда $\tilde{x} \notin \mathfrak{I}$. Рассмотрим идеал $\tilde{\mathfrak{I}} \subset R$, порожденный $\mathfrak{I}$ и $\tilde{x}$. Так как $\tilde{x} \notin \mathfrak{I}$,

то $\tilde{\mathfrak{I}} \neq \mathfrak{I}$. Так как $\mathfrak{I}$ – максимальный идеал, то $\tilde{\mathfrak{I}} = R$. В частности, $1 \in \tilde{\mathfrak{I}}$. Следовательно, для некоторых $z \in \mathfrak{I}$, $r \in R$ мы можем записать $1 = z + \tilde{x}r$. Отсюда

$$1 = \varphi(z) + \varphi(\tilde{x}r) = x\varphi(r),$$

т.е. элемент x обратим. □

Теорема. *Пусть R – целостное кольцо и пусть $\mathfrak{I} \subset R$ – любой идеал. Тогда существует максимальный идеал, содержащий $\mathfrak{I}$.*

Доказательство. Воспользуемся леммой Цорна. Следует проверить выполнение условий. Пусть Σ – множество всех неединичных идеалов в R, содержащих $\mathfrak{I}$. На Σ есть частичный порядок – по включению. Пусть $C \subset \Sigma$ – цепь, т.е. множество идеалов $\mathfrak{I}_\alpha$ таких, что для любых $\mathfrak{I}_\alpha$, $\mathfrak{I}_\beta \in C$ выполнено $\mathfrak{I}_\alpha \subset \mathfrak{I}_\beta$ или $\mathfrak{I}_\alpha \supset \mathfrak{I}_\beta$. Тогда

$$\tilde{\mathfrak{I}} := \bigcup_{\mathfrak{I}_\alpha \in C} \mathfrak{I}_\alpha$$

является верхней гранью для C. Действительно, если a, $b \in \tilde{\mathfrak{I}}$, то a, $b \in \mathfrak{I}_\alpha$ для некоторого $\mathfrak{I}_\alpha$, а значит $a \pm b \in \mathfrak{I}_\alpha \subset \tilde{\mathfrak{I}}$. Аналогично, если $a \in \tilde{\mathfrak{I}}$ и $b \in R$, то $a \in \mathfrak{I}_\alpha$ для некоторого $\mathfrak{I}_\alpha$, а значит $ab \in \mathfrak{I}_\alpha \subset \tilde{\mathfrak{I}}$. Следовательно, $\tilde{\mathfrak{I}}$ – идеал. Он содержит все идеалы $\mathfrak{I}_\alpha \in C$, значит $\tilde{\mathfrak{I}}$ является верхней гранью.

Таким образом, условия леммы Цорна выполнены и поэтому существует максимальный элемент $\mathfrak{I}_{\max} \in \Sigma$. Ясно, что он является максимальным идеалом в R. □

8.2 Кольца главных идеалов

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

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

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

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

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

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

Далее на протяжении настоящего параграфа мы предположим, что R – коммутативное ассоциативное кольцо с единицей без делителей нуля. Такое кольцо называется *целостным* или *областью целостности*. В целостном кольце можно определить понятие делимости: для a, $b \in R$ будем говорить, что a делит b и писать $a \mid b$, 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 $a \mid b$ тогда и только тогда, когда $b \in (a)$. Элементы a, $b \in R$ являются ассоциированными тогда и только тогда, когда $(a) = (b)$.

Элемент $a \in R \setminus \{0\}$ называется *неразложимым* или *простым*, если он делится только на обратимые и ассоциированные с ним элементы. Целостное кольцо называется *факториальным*, если в нем выполнена основная теорема арифметики: любой элемент $a \in R \setminus \{0\}$ разлагается в произведение простых и это разложение единственно с точностью до порядка и ассоциированности.

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

Замечание. Обратное утверждение не верно: кольцо $\Bbbk[t_1, \dots, t_n]$ от нескольких переменных над полем факториально, но не является кольцом главных идеалов. То же самое верно для кольца $\mathbb{Z}[t_1, \dots, t_n]$ многочленов с целыми коэффициентами.

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

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

Если эта последовательность обрывается, то последний ее элемент a_n должен быть простым делителем всех a_{n-1},..., 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 $\mathfrak{I} := \cup(a_k)$. Легко поверить, что $\mathfrak{I}$ – идеал и $\mathfrak{I} \neq (1)$. По нашему предположению $\mathfrak{I} = (b)$ 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 – простой делитель a_{k-1} и $a_k = a_{k-1}/p_k$. Таким образом, имеем

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

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. □

Лемма. *В условиях теоремы если простой 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 $b = abuc^{-1} + pbvc^{-1}$. □

Определение. Целостное кольцо R называется *евклидовым*, если существует отображение (евклидова норма)

$$\nu : R \setminus \{0\} \to \mathbb{N}$$

такое, что

- $\nu(ab) \geq \nu(a)$, для любых элементов a, $b \in R \setminus \{0\}$;
- (деление с остатком) для любых элементов a, $b \in R \setminus \{0\}$ существуют q, $r \in R$ такие, что $a = bq + r$, 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 $\nu(f) = \deg f$.

Теорема. *Евклидово кольцо является кольцом главных идеалов.*

Доказательство. Аналогично доказательству того, что $\Bbbk[t]$ – кольцо главных идеалов. Пусть $\mathfrak{I}$ – ненулевой идеал. Выберем $a \in \mathfrak{I} \setminus \{0\}$ с наименьшим значением $\nu(a)$. Для любого другого элемента $b \in \mathfrak{I} \setminus \{0\}$ 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.*

8.3 Модули над кольцами главных идеалов

Пусть R – (целостное) кольцо главных идеалов. Теория (конечно порожденных) модулей над таким кольцом полностью аналогична теории конечно порожденных абелевых групп. Мы воспроизведем здесь эту теорию, несмотря на то, что она не принесет ничего нового.

Для начала мы напомним основные определения. Некоторые из них уже формулировались для случая модулей над произвольными ассоциативными кольцами. В основном, эти определения похожи на соответствующие им определения для абелевых групп, однако терминология иногда отличается.

Пусть R – целостное кольцо и пусть M – модуль над R. Говорят, что M *порождается* элементами $\mathbf{a}_i \in M$, если любой элемент $\mathbf{a} \in M$ представляется в виде линейной комбинации $\mathbf{a} = \sum \lambda_i \mathbf{a}_i$, $\lambda_i \in R$. Модуль M называется *конечно порожденным*, если у него существует система порождающих из конечного числа элементов.

Элементы $\mathbf{a}_1, \ldots, \mathbf{a}_r \in M$ называются *линейно зависимыми*, если некоторая их нетривиальная линейная комбинация

$$\lambda_1\mathbf{a}_1 + \lambda_2\mathbf{a}_2 + \cdots + \lambda_r\mathbf{a}_r, \qquad \lambda_i \in R$$

равна нулю. Набор элементов $\mathbf{a}_1, \ldots, \mathbf{a}_r$ называется *базисом* модуля M, если выполнены два условия

- $\mathbf{a}_1, \ldots, \mathbf{a}_r$ порождают M;
- $\mathbf{a}_1, \ldots, \mathbf{a}_r$ линейно независимы.

Модуль, обладающий базисом, называется *свободным*.

Модуль, порожденный одним элементом, называется *циклическим*. Свободный циклический модуль изоморфен кольцу R (рассматриваемым как модуль над собой). Для любого идеала $\mathfrak{I} \subset R$ факторкольцо $R/\mathfrak{I}$ является циклическим модулем над R. Наоборот, пусть M – циклический модуль и пусть $\mathbf{a} \in M$ – порождающий элемент. Рассмотрим отображение

$$\varphi : R \longrightarrow M, \qquad \lambda \longmapsto \lambda\mathbf{a}.$$

Ясно, что это сюръективный гомоморфизм модулей. По теореме о гомоморфизме $M \simeq R/\mathfrak{I}$, где $\mathfrak{I} := \operatorname{Ker}(\varphi)$.

Если для элемента $\mathbf{a} \in M$ существует ненулевой элемент $\lambda \in R$ такой, что $\lambda\mathbf{a} = 0$, то $\mathbf{a}$ называется *периодическим* (или *элементом кручения*). Для элемента кручения $\mathbf{a} \in M$ множество

$$\mathfrak{I} = \{\lambda \in R \mid \lambda\mathbf{a} = 0\}$$

является идеалом в R.

Пусть теперь R – кольцо главных идеалов. Тогда идеал $\mathfrak{I}$ является главным, т.е. $\mathfrak{I} = (m)$ для некоторого $m \in R$. В этом случае m называется *периодом* элемента $\mathbf{a}$. Ясно, что период определен с точностью до умножения на обратимый элемент. Все периодические элементы в M образуют подмодуль $\operatorname{Tor}(M) \subset M$, который называется *подмодулем кручения*. Таким образом,

$$\operatorname{Tor}(M) := \{\mathbf{a} \in M \mid \exists \lambda \in R,\ \lambda \neq 0 \quad \lambda\mathbf{a} = 0\}.$$

Несложно видеть, что фактормодуль $M/\operatorname{Tor}(M)$ не имеет кручения.

Пусть $p \in R$ – простой элемент. Положим

$$\operatorname{Tor}_{(p)}(M) := \{\mathbf{a} \in M \mid \exists k \in \mathbb{N} \quad p^k\mathbf{a} = 0\}.$$

Тогда $\operatorname{Tor}_{(p)}(M)$ – подмодуль и фактормодуль $M/\operatorname{Tor}_{(p)}(M)$ не имеет нетривиальных элементов периода p^k. Подмодуль $\operatorname{Tor}_{(p)}(M)$ называется *p-периодической частью* модуля M.

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 – простой 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.

Лемма. *Пусть M – конечно порожденный модуль над R. Если $\operatorname{Tor}(M) = 0$, то M является свободным.*

Доказательство. Пусть $M = \langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$. Проведем доказательство индукцией по n. База индукции $n = 1$ очевидна. Предположим, что утверждение верно для всех модулей, порожденных менее чем n элементами.

Докажем вспомогательное утверждение.

Утверждение. *Существует элемент $\mathbf{b} \in M$ такой, что множество*

$$M_{\mathbf{b}} := \{\mathbf{x} \in M \mid \exists l_1,\, l_2 \in \mathbb{Z},\, l_1 \neq 0,\, l_1\mathbf{x} = l_2\mathbf{b}\}$$

является ненулевым циклическим подмодулем в M и фактормодуль $M/M_{\mathbf{b}}$ порождается меньшим количеством элементов.

Доказательство утверждения. Пусть $\mathbf{a}_1, \ldots, \mathbf{a}_n$ – порождающие элементы модуля M. Если если они линейно независимы, то модуль M свободен и они образуют базис в M. В этом случае положим $\mathbf{b} := \mathbf{a}_i$ для любого i и тогда $M_{\mathbf{b}} = \langle \mathbf{b} \rangle$ – циклический модуль и фактормодуль $M/M_{\mathbf{b}}$ порождается образами элементов $\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}, \mathbf{a}_{i+1}, \ldots, \mathbf{a}_n$.

Далее предположим, что $\mathbf{a}_1, \ldots, \mathbf{a}_n$ линейно зависимы. Значит, мы можем считать, что

$$\lambda\mathbf{a}_1 = \sum_{i=2}^{n} \lambda_i \mathbf{a}_i, \qquad (*)$$

где $\lambda\mathbf{a}_1 \neq 0$. Положим $\mathbf{b} := \lambda\mathbf{a}_1$ и $M' := \langle \mathbf{a}_2, \ldots, \mathbf{a}_n \rangle$. Из $(*)$ следует, что $\mathbf{b} \in M'$. Пусть также

$$M'_{\mathbf{b}} := \{\mathbf{x} \in M' \mid \exists l_1,\, l_2 \in \mathbb{Z},\, l_1 \neq 0,\, l_1\mathbf{x} = l_2\mathbf{b}\}.$$

Так как $M' \supset \lambda M$ (снова по формуле $(*)$), то

$$M_{\mathbf{b}} \supset M'_{\mathbf{b}} = M_{\mathbf{b}} \cap M' \supset \lambda M_{\mathbf{b}} \cap \lambda M = \lambda M_{\mathbf{b}}.$$

С другой стороны, поскольку $\mathrm{Tor}(M) = 0$, то отображение

$$\varphi : M \longrightarrow M, \qquad \mathbf{x} \longmapsto \lambda\mathbf{x}$$

является инъективным гомоморфизмом модулей. По предположению индукции модуль $M'_{\mathbf{b}}$ является циклическим. Следовательно, таковым является и модуль

$$M_{\mathbf{b}} \simeq \varphi(M_{\mathbf{b}}) = \lambda M_{\mathbf{b}} \subset M'_{\mathbf{b}}.$$

При этом фактормодуль $M/M_{\mathbf{b}}$ порождается образами элементов $\mathbf{a}_2, \ldots, \mathbf{a}_n$. □

Продолжим доказательство леммы. Возьмем элемент $\mathbf{b} \in M$ такой, как в утверждении. Тогда фактормодуль $M/M_{\mathbf{b}}$ не имеет элементов конечного порядка и порождается меньшим количеством элементов. Пусть $\mathbf{e}_1$ – порождающий элемент циклического модуля $M_{\mathbf{b}}$. По предположению индукции $M/M_{\mathbf{b}}$ – свободный модуль над R. Пусть $\bar{\mathbf{e}}_2, \ldots, \bar{\mathbf{e}}_r$ – его базис, пусть

$$\varphi : M \to M/M_{\mathbf{b}}$$

– гомоморфизм факторизации и пусть $\mathbf{e}_2, \ldots, \mathbf{e}_r \in M$ – любые элементы такие, что $\varphi(\mathbf{e}_i) = \bar{\mathbf{e}}_i$. Мы утверждаем, что элементы $\mathbf{e}_1, \ldots, \mathbf{e}_r$ порождают M. Действительно, для любого $\mathbf{x} \in M$ имеем $\varphi(\mathbf{x}) = \sum_{i=2}^{r} \lambda_i \bar{\mathbf{e}}_i$ для некоторых $\lambda_i \in \mathbb{Z}$. Тогда

$$\varphi(\mathbf{x} - \sum_{i=2}^{r} \lambda_i \mathbf{e}_i) = 0.$$

Следовательно, $\mathbf{x} - \sum_{i=2}^{r} \lambda_i \mathbf{e}_i \in \operatorname{Ker}(\varphi) = M_{\mathbf{b}}$. Это означает, что $\mathbf{x} - \sum_{i=2}^{r} \lambda_i \mathbf{e}_i = \lambda_1 \mathbf{e}_1$ для некоторого $\lambda_1 \in \mathbb{Z}$. Таким образом,

$$\mathbf{x} = \sum_{i=1}^{r} \lambda_i \mathbf{e}_i.$$

Это разложение единственно. Действительно, иначе

$$\mathbf{x} = \sum_{i=1}^{r} \lambda_i \mathbf{e}_i = \sum_{i=1}^{r} \lambda_i' \mathbf{e}_i. \qquad (\dagger)$$

и тогда

$$0 = \varphi(\mathbf{x} - \mathbf{x}) = \varphi\left(\sum_{i=1}^{r} (\lambda_i - \lambda_i') \mathbf{e}_i\right) = \sum_{i=2}^{r} (\lambda_i - \lambda_i') \bar{\mathbf{e}}_i.$$

Поскольку $\bar{\mathbf{e}}_2, \ldots, \bar{\mathbf{e}}_r$ – базис $M/M_{\mathbf{b}}$, то $\lambda_i = \lambda_i'$ для $i = 2, \ldots, r$. Из $(\dagger)$ следует, что $\lambda_1 = \lambda_1'$. Таким образом, $\mathbf{e}_1, \ldots, \mathbf{e}_r$ – базис M и поэтому модуль M является свободным. □

Лемма. *Пусть M – конечно порожденный модуль над R. Существует свободный подмодуль $F \subset M$ такой, что имеет место разложение*

$$M = \operatorname{Tor}(M) \oplus F.$$

Доказательство. Как и в предыдущей лемме рассмотрим гомоморфизм факторизации

$$M \longrightarrow M/\operatorname{Tor}(M).$$

Фактормодуль $M/\operatorname{Tor}(M)$ конечно порожден и не содержит элементов кручения. Следовательно, он свободен и существует базис $\bar{\mathbf{e}}_1, \ldots, \bar{\mathbf{e}}_r \in M/\operatorname{Tor}(M)$. Пусть $\mathbf{e}_1, \ldots, \mathbf{e}_r \in M$ – любые элементы такие, что $\varphi(\mathbf{e}_i) = \bar{\mathbf{e}}_i$. Для любого $\mathbf{x} \in M$ имеем $\varphi(\mathbf{x}) = \sum_{i=1}^{r} \lambda_i \bar{\mathbf{e}}_i$ для некоторых $\lambda_i \in R$. Тогда $\varphi(\mathbf{x} - \sum_{i=1}^{r} \lambda_i \mathbf{e}_i) = 0$. Следовательно,

$$\mathbf{x} - \sum_{i=1}^{r} \lambda_i \mathbf{e}_i \in \operatorname{Ker}(\varphi) = \operatorname{Tor}(M).$$

Таким образом, существует элемент $\mathbf{y} \in \operatorname{Tor}(M)$ такой, что

$$\mathbf{x} = \mathbf{y} + \sum_{i=1}^{r} \lambda_i \mathbf{e}_i.$$

Это разложение единственно. Действительно, иначе

$$\mathbf{x} = \mathbf{y} + \sum_{i=1}^{r} \lambda_i \mathbf{e}_i = \mathbf{y}' + \sum_{i=1}^{r} \lambda_i' \mathbf{e}_i. \qquad (\ddagger)$$

и тогда

$$0 = \varphi(\mathbf{x} - \mathbf{x}) = \varphi\left(\mathbf{y} - \mathbf{y}' + \sum_{i=1}^{r} (\lambda_i - \lambda_i') \mathbf{e}_i\right) = \sum_{i=1}^{r} (\lambda_i - \lambda_i') \bar{\mathbf{e}}_i.$$

Поскольку $\bar{\mathbf{e}}_1, \ldots, \bar{\mathbf{e}}_r$ – базис $M/\operatorname{Tor}(M)$, то $\lambda_i = \lambda_i'$ для $i = 1, \ldots, r$. Тогда из $(\ddagger)$ следует, что $\mathbf{y} = \mathbf{y}'$. Положим $F := \langle \mathbf{e}_1, \ldots, \bar{\mathbf{e}}_r \rangle$. Тогда $\mathbf{e}_1, \ldots, \mathbf{e}_r$ – базис F, модуль F является свободным и $M = \operatorname{Tor}(M) \oplus F$. □

Лемма. *Для любого конечно порожденного периодического модуля M имеет место разложение*

$$M = \bigoplus_p \mathrm{Tor}_p(M).$$

где суммирование ведется по всем простым элементам кольца R.

Доказательство. Так как модуль M – периодический и конечно порожден, то существует ненулевой элемент $n \in R$ такой, что $nM = 0$. Разложим n в произведение простых множителей $n = p_1^{k_1} \cdots p_m^{k_m}$. Проведем доказательство индукцией по m. База индукции $m = 1$ очевидна. Предположим, что утверждение верно для всех модулей, у которых разложение в произведение степеней простых элементов имеет меньше чем m сомножителей. Представим n в виде $n = n_1 n_2$, где НОД $(n_1, n_2) = 1$ и n_i не являются обратимыми. Тогда $1 = n_1 u_1 + n_2 u_2$ для некоторых u_1, $u_2 \in R$. Положим $M_1 := n_1 M$ и $M_2 := n_2 M$. Тогда $M_1 \cap M_2 = \{0\}$. Действительно, если $\mathbf{a} \in M_1 \cap M_2$, то $\mathbf{a} = n_1 \mathbf{a}' = n_2 \mathbf{a}''$ для некоторых $\mathbf{a}', \mathbf{a}'' \in M$. Так как

$$n_2 \mathbf{a} = n_1 n_2 \mathbf{a}' = n \mathbf{a}' = 0,$$

то период $\mathbf{a}$ делит n_2. Аналогично получаем, что период $\mathbf{a}$ делит n_1. Так как НОД $(n_1, n_2) = 1$, то $\mathbf{a} = 0$. Наконец, для любого элемента $\mathbf{a} \in M$ имеем

$$\mathbf{a} = (n_1 u_1 + n_2 u_2)\mathbf{a} = u_1 \mathbf{a}_1 + u_2 \mathbf{a}_2,$$

где $\mathbf{a}_i := n_i \mathbf{a} \in M_i$. По предположению индукции M_1 и M_2 раскладываются в суммы своих подмодулей $\mathrm{Tor}_p(M_i)$. Лемма доказана. □

Лемма. *Для любого конечно порожденного p-периодического модуля M имеет место разложение*

$$M = \bigoplus_{i=2}^{n} M_i$$

где M_i – (примарные) циклические модули.

Доказательство. Так как модуль M p-периодический и конечно порожден, то $p^m M = 0$ для некоторого $m \in \mathbb{N}$. Проведем доказательство индукцией по m. База индукции $m = 1$ очевидна. Предположим, что утверждение верно для всех p-периодических модулей N таких, что $p^{m-1} N = 0$. Возьмем элемент $\mathbf{a}_1 \in M$ максимального периода p^{m_1}. Рассмотрим фактормодуль $\bar{M} := M/\langle \mathbf{a}_1 \rangle$ и гомоморфизм факторизации

$$\varphi : M \longrightarrow \bar{M}.$$

Модуль $\bar{M}$ аннулируется элементом $p^{m-m_1} < p^m$. По предположению индукции имеет место разложение

$$\bar{M} = \bigoplus_{i=2}^{n} \bar{M}_i$$

где $\bar{M}_i$ – циклические модули. Пусть $\bar{\mathbf{a}}_i$ – порождающий элемент $\bar{M}_i$ и пусть $m_i := |\bar{M}_i|$, $i = 2, \ldots, n$. Существуют элементы $\mathbf{b}_2, \ldots, \mathbf{b}_n \in M$ такие, что $\varphi(\mathbf{b}_i) = \bar{\mathbf{a}}_i$. Тогда

$$\varphi(p^{m_i} \mathbf{b}_i) = p^{m_i} \bar{\mathbf{a}}_i = 0.$$

Следовательно, $p^{m_i}\mathbf{b}_i \in \mathrm{Ker}(\varphi) = \langle \mathbf{a}_1 \rangle$. Таким образом,

$$p^{m_i}\mathbf{b}_i = s_i\mathbf{a}_1 \quad \text{для некоторых } s_i \in \mathbb{Z}.$$

Согласно нашему выбору $\mathbf{a}_1$ периоды всех элементов модуля M делят p^{m_1}. Отсюда

$$0 = p^{m_1}\mathbf{b}_i = p^{m_1-m_i}p^{m_i}\mathbf{b}_i = p^{m_1-m_i}s_i\mathbf{a}_1.$$

Следовательно, число $p^{m_1-m_i}s_i$ делится на период p^{m_1} элемента $\mathbf{a}_1$. Тогда s_i делится на p^{m_i}, т.е. мы можем записать

$$s_i = p^{m_i}q_i, \qquad q_i \in \mathbb{Z}.$$

Положим

$$\mathbf{a}_i := \mathbf{b}_i - q_i\mathbf{a}_1, \qquad i = 2, \ldots, n.$$

Тогда

$$p^{m_i}\mathbf{a}_i = p^{m_i}(\mathbf{b}_i - q_i\mathbf{a}_1) = p^{m_i}\mathbf{b}_i - p^{m_i}q_i\mathbf{a}_1 = s_i\mathbf{a}_1 - s_i\mathbf{a}_1 = 0. \qquad \square$$

8.4 Китайская теорема об остатках

Теорема. *Пусть R – коммутативное ассоциативное кольцо с единицей и пусть $\mathfrak{I}_1, \ldots, \mathfrak{I}_n$ – идеалы в R такие, что $\mathfrak{I}_k + \mathfrak{I}_l = R$ для всех $k \neq l$. Тогда для любого набора элементов $a_1, \ldots, a_n \in R$ существует элемент $a \in R$ такой, что*

$$a \equiv a_k \mod \mathfrak{I}_k.$$

Доказательство. Индукция по n. База индукции $n = 2$ очевидна: в этом случае $1 = b_1 + b_2$ для некоторых $b_1 \in \mathfrak{I}_1$, $b_2 \in \mathfrak{I}_2$. Следовательно, мы можем положить $a := a_2b_1 + a_1b_2$.

Предположим, что утверждение верно для наборов из $n-1$ идеалов. Значит, мы можем найти $a' \in R$ такой, что

$$a' \equiv a_j \mod \mathfrak{I}_j, \quad j = 1, \ldots, n-1.$$

Для $j < n$ мы можем записать

$$1 = b_j + c_j, \quad b_j \in \mathfrak{I}_n, \quad c_j \in \mathfrak{I}_j.$$

Тогда

$$1 = \prod_{j=1}^{n-1}(b_j + c_j) \in \mathfrak{I}_n + \tilde{\mathfrak{I}}, \qquad \text{где } \tilde{\mathfrak{I}} := \mathfrak{I}_1 \cdots \mathfrak{I}_{n-1}.$$

Следовательно, $\mathfrak{I}_n + \tilde{\mathfrak{I}} = R$. Так как теорема верна для $n = 2$, то существует элемент $a \in R$ такой, что

$$a \equiv a_n \mod \mathfrak{I}_n, \qquad a \equiv a' \mod \tilde{\mathfrak{I}}.$$

Так как $\mathfrak{I}_j \supset \tilde{\mathfrak{I}}$ при $j = 1, \ldots, n-1$, то

$$a \equiv a' \equiv a_j \mod \mathfrak{I}_j \quad \text{при } j = 1, \ldots n-1. \qquad \square$$

Доказательство. Индукция по n. База индукции $n = 2$ очевидна: в этом случае $1 = b_1 + b_2$ для некоторых $b_1 \in \mathfrak{I}_1$, $b_2 \in \mathfrak{I}_2$. Следовательно, мы можем положить $a := a_2 b_1 + a_1 b_2$.

Для $j < n$ мы можем записать

$$1 = b_j + c_j, \quad b_j \in \mathfrak{I}_n, \quad c_j \in \mathfrak{I}_j.$$

Тогда

$$1 = \prod_{j=1}^{n-1}(b_j + c_j) \in \mathfrak{I}_n + \tilde{\mathfrak{I}}, \qquad \text{где } \tilde{\mathfrak{I}} := \mathfrak{I}_1 \cdots \mathfrak{I}_{n-1}.$$

Следовательно, $\mathfrak{I}_n + \tilde{\mathfrak{I}} = R$. Так как теорема верна для $n = 2$, то существует элемент $d_n \in R$ такой, что

$$d_n \equiv 1 \mod \mathfrak{I}_n, \qquad d_n \equiv 0 \mod \tilde{\mathfrak{I}}.$$

Так как $\mathfrak{I}_j \supset \tilde{\mathfrak{I}}$ при $j = 1, \ldots, n-1$, то

$$d_n \equiv 0 \mod \mathfrak{I}_j \quad \text{при } j = 1, \ldots n-1$$

Предположим, что утверждение верно для наборов из $n-1$ идеалов. Тогда для любого $1 \le j \le n-1$ существует элемент $d'_j \in R$ такой, что

$$d'_j \equiv 1 \mod \mathfrak{I}_j, \qquad d'_j \equiv 0 \mod \mathfrak{I}_k \quad \text{при} \quad k = 1, \ldots, n-1, \quad k \ne j.$$

Применим еще раз теорему к идеалам $\tilde{\mathfrak{I}}$ и $\mathfrak{I}_n$: для любого $1 \le j \le n-1$ существует элемент $d_j \in R$ такой, что

$$d_j \equiv d'_j \mod \tilde{\mathfrak{I}}, \qquad d_j \equiv 0 \mod \mathfrak{I}_n.$$

Следовательно,

$$d_j \equiv 1 \mod \mathfrak{I}_j, \qquad d_j \equiv 0 \mod \mathfrak{I}_k \quad \text{при} \quad k = 1, \ldots, n, \quad k \ne j.$$

Положим

$$a := a_1 d_1 + \cdots + a_n d_n.$$

Тогда

$$a \equiv a_1 \cdot 0 + \cdots + a_{n-1} \cdot 0 + a_n \cdot 1 \equiv a_n \mod \mathfrak{I}_n,$$
$$a \equiv a_1 \cdot 0 + \cdots + a_j \cdot 1 + \cdots + a_n \cdot 0 \equiv a_j \mod \mathfrak{I}_j. \qquad \square$$

Следствие. *Пусть R – коммутативное ассоциативное кольцо с единицей и пусть $\mathfrak{I}_1, \ldots, \mathfrak{I}_n$ – идеалы в R такие, что $\mathfrak{I}_k + \mathfrak{I}_l = R$ для всех $k \ne l$. Тогда для естественного гомоморфизма*

$$\varphi : R \longrightarrow \prod_{k=1}^{n} R/\mathfrak{I}_k$$

имеют место следующие утверждения:

(i) *φ сюръективен,*

(ii) $\mathrm{Ker}(\varphi) = \cap_{k=1}^{n} \mathfrak{I}_k$,

(iii) $R/\cap_{k=1}^{n} \mathfrak{I}_k \simeq \prod_{k=1}^{n} R/\mathfrak{I}_k$.

Следствие. *Пусть $m_1, \ldots, m_n$ – попарно взаимно простые целые числа. Тогда для любого набора чисел $a_1, \ldots, a_n \in \mathbb{Z}$ существует $a \in \mathbb{Z}$ такое, что*

$$a \equiv a_i \mod m_i.$$

Следствие. *Пусть целое число m следующим образом раскладывается в произведение простых множителей:*

$$m = p_1^{k_1} \ldots p_n^{k_n},$$

где все p_i различны. Тогда

$$\mathbb{Z}/m\mathbb{Z} \simeq \prod_{i=1}^{n} \mathbb{Z}/p_i^{k_i}\mathbb{Z},$$

$$(\mathbb{Z}/m\mathbb{Z})^* \simeq \prod_{i=1}^{n} (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*.$$

Задачи

Пусть R – коммутативное ассоциативное кольцо с единицей.

8.1. Напомним, что элемент $a \in R$ называется *нильпотентным*, если $a^n = 0$ для некоторого n. Докажите, что если a нильпотент, то элемент $1 + a$ обратим.

8.2. Докажите, что все нильпотентные элементы R образуют идеал $\mathfrak{N}$, который содержится в пересечении всех простых идеалов. Он называется *нильрадикалом* кольца R. Докажите, что факторкольцо $R/\mathfrak{N}$ не содержит нильпотентов. *

8.3. Докажите, что многочлен $f \in R[t]$, $f = a^n t^n + \cdots + a_1 t + a_0$ является обратимым элементом тогда и только тогда, когда младший коэффициент a_0 обратим, остальные коэффициенты $a_1, \ldots, a_n$ являются нильпотентами.

8.4. *Радикалом Джекобсона* кольца R называется пересечение всех его максимальных идеалов. Докажите, что элемент $a \in R$ принадлежит радикалу Джекобсона тогда и только тогда, когда элемент $1 - ax$ обратим для любого $x \in R$.

8.5. Докажите, что в кольце главных идеалов каждый ненулевой простой идеал является максимальным.

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

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

*На самом деле нильрадикал *совпадает* с пересечением всех простых идеалов. Попробуйте это доказать.

8.8. Докажите, что кольцо
$$\mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} \in \mathbb{C} \mid a,\, b \in \mathbb{Z}\}$$
не является факториальным.

8.9. Докажите, что кольцо
$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \in \mathbb{C} \mid a,\, b \in \mathbb{Z}\}$$
не является факториальным.

8.10. Докажите, что кольцо целых гауссовых чисел
$$\mathbb{Z}[\boldsymbol{i}] := \{a + \boldsymbol{i}b \in \mathbb{C} \mid a,\, b \in \mathbb{Z}\}$$
является евклидовым. *Указание.* Рассмотрите норму $\nu(z) := z\bar{z} = |z|^2$.

8.11. Докажите, что кольцо
$$\mathbb{Z}[\zeta] = \{a + b\zeta + c\zeta^2 \mid a,\, b,\, c \in \mathbb{Z}\},$$
где $\zeta = \zeta_3$ – первообразный корень степени 3 из 1, является евклидовым. *Указание.* Воспользуйтесь указаниями предыдущей задачи.

8.12. Докажите, что кольцо
$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a,\, b \in \mathbb{Z}\}$$
является евклидовым.

8.13. Пусть $f\colon R \to R'$ – сюръективный гомоморфизм колец. Докажите, что если R – кольцо главных идеалов, то таковым же является и R'. Верно ли обратное?

8.14. Докажите, что кольцо функций дифференцируемых в точке не является кольцом главных идеалов. Опишите максимальные идеалы в этом кольце.

8.15. Пусть $\Bbbk$ поле алгебраически замкнуто и $\operatorname{char}\Bbbk \neq 2$. Рассмотрим факторкольцо
$$R := \Bbbk[x, y]/(y^2 - x^3 + x).$$
Докажите, что в R нет делителей нуля. Докажите, что обратимые элементы кольца R – в точности ненулевые элементы $\Bbbk$. Докажите, что кольцо R не является факториальным.

8.16. Пусть R – факториальное кольцо. Докажите, что

(a) каждый простой элемент $p \in R$ порождает простой идеал $(p) \subset R$;

(b) каждый простой идеал $\mathfrak{P} \subset R$ содержит простой элемент;

(c) каждый главный простой идеал $(p) \subset R$ порождается простым элементом;

(d) если простой идеал $\mathfrak{P} \subset R$ не содержит простых идеалов, отличных от $\mathfrak{P}$ и (0), то он – главный.

Лекция 9

Поля. Расширения полей

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 $[\mathbb{K} : \Bbbk]$.

9.1 Простые поля

Пусть $\Bbbk$ – произвольное поле. Обозначим через M множество всех $m \in \mathbb{N}$ таких, что

$$\underbrace{1 + \cdots + 1}_{m} = 0.$$

Характеристикой $\operatorname{char}(\Bbbk)$ поля $\Bbbk$ называется число

$$\operatorname{char}(\Bbbk) = \begin{cases} \min M, & \text{если } M \neq \varnothing, \\ 0, & \text{если } M = \varnothing. \end{cases} \qquad (*)$$

Таким образом, $\operatorname{char}(\Bbbk)$ – 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

$$\phi\colon \mathbb{Z} \longrightarrow \Bbbk, \qquad \phi(n) = n \cdot 1 \qquad (\dagger)$$

является гомоморфизмом колец. Непосредственно из определения характеристики получаем следующее

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

Доказательство. Если $\operatorname{char}(\Bbbk) = 0$, то $\phi(m) = m \cdot 1 \neq 0$ для любого $m \in \mathbb{Z}$. Следовательно, $\operatorname{Ker}(\phi) = (0)$. Предположим, что $\operatorname{char}(\Bbbk) = n > 0$. 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, $\operatorname{Ker}(\phi) \supset (n)$. Обратно, пусть $m \in \operatorname{Ker}(\phi)$. Тогда $m \cdot 1 = 0$ и поэтому m делится на n, т.е. $m \in (n)$. Следовательно, имеется обратное включение $\operatorname{Ker}(\phi) \subset (n)$. $\square$

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 $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$. Если n не является простым, то $\mathbb{Z}/n\mathbb{Z} \simeq \phi(\mathbb{Z})$ 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 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ по простому модулю p. Верно и обратное:

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

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

Теперь рассмотрим случай $\mathrm{char}(\Bbbk) = 0$. 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:

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

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. □

9.2 Расширения полей

Пусть $\mathbb{K}/\Bbbk$ – любое расширение полей. Для элементов $\theta_1, \ldots, \theta_n \in \mathbb{K}$ обозначим через $\Bbbk[\theta_1, \ldots, \theta_n]$ (соответственно, через $\Bbbk(\theta_1, \ldots, \theta_n)$) – наименьшее подкольцо (соответственно подполе) в $\mathbb{K}$, содержащее $\Bbbk$ и все $\theta_1, \ldots, \theta_n$. Ясно, что

$$\Bbbk[\theta_1, \ldots, \theta_n] = \left\{\sum \alpha_{k_1,\ldots,k_n} \theta_1^{k_1} \cdots \theta_n^{k_n} \mid \alpha_{k_1,\ldots,k_n} \in \Bbbk,\ k_j \geq 0\right\},$$

$$\Bbbk(\theta_1, \ldots, \theta_n) = \left\{\tfrac{\beta}{\gamma} \mid \beta, \gamma \in \Bbbk[\theta_1, \ldots, \theta_n], \quad \gamma \neq 0\right\}.$$

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

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.*

Пример. Пусть $\mathbb{K}/\mathbb{R}$ – алгебраическое расширение. Тогда $\mathbb{K} = \mathbb{R}$ или $\mathbb{K} \simeq \mathbb{C}$ (как поле над $\mathbb{R}$).

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.

Предложение. *Пусть $\mathbb{K}/\Bbbk$ – любое расширение полей. Следующие условия эквивалентны.*

(i) *элемент $\theta \in \mathbb{K}$ является алгебраическим над $\Bbbk$;*

(ii) *кольцо $\Bbbk[\theta]$, как векторное пространство над $\Bbbk$, конечномерно;*

(iii) *кольцо $\Bbbk[\theta]$ является полем;*

(iv) *поле $\Bbbk(\theta)$, как векторное пространство над $\Bbbk$, конечномерно.*

Доказательство. (i)$\Longrightarrow$(ii) 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 старший коэффициент f равен 1, т.е.

$$f = t^n + \lambda_{n-1}t^{n-1} + \cdots \lambda_1 t + \lambda_0.$$

Тогда

$$\theta^n = -\lambda_{n-1}\theta^{n-1} - \cdots \lambda_1\theta - \lambda_0$$

и мы можем (по индукции) выразить все степени θ как линейные комбинации $1, \theta, \ldots, \theta^{n-1}$ с коэффициентами в $\Bbbk$. Таким образом, $\Bbbk[\theta]$ как векторное пространство над $\Bbbk$ порождается конечным числом элементов.

(ii)$\Longrightarrow$(iii) Достаточно показать, что любой ненулевой элемент $b \in \Bbbk[\theta]$ имеет обратный. Рассмотрим $\Bbbk[\theta]$ как векторное пространство над $\Bbbk$ и пусть

$$\mathscr{A}_b : \Bbbk[\theta] \to \Bbbk[\theta]$$

– линейный оператор

$$\mathscr{A}_b : \alpha \longmapsto b\alpha.$$

Так как в $\Bbbk[\theta]$ нет делителей 0, то этот оператор инъективен. Так как $\Bbbk[\theta]$ конечномерно, то он и сюръективен. Значит, существует элемент $b^{-1} \in \Bbbk[\theta]$ такой, что $\mathscr{A}_b(b^{-1}) = b\,b^{-1} = 1$.

(iii)$\Longrightarrow$(iv) Мы можем записать $\theta^{-1} = \sum_{k=0}^{n} \lambda_k \theta^k$. Отсюда

$$\theta^{n+1} = -\frac{1}{\lambda_n}\sum_{k=1}^{n} \lambda_k \theta^k + \frac{1}{\lambda_n}.$$

Как и выше,мы можем (по индукции) выразить все степени θ как линейные комбинации $1, \theta, \ldots, \theta^{n1}$ с коэффициентами в $\Bbbk$. Таким образом, $\Bbbk[\theta] = \Bbbk(\theta)$ как векторное пространство над $\Bbbk$ порождается конечным числом элементов.

(iv)$\Longrightarrow$(i) Пусть $n := \dim_{\Bbbk} \Bbbk(\theta) < \infty$. Тогда элементы $1, \theta, \theta^2, \ldots, \theta^n$ линейно зависимы над $\Bbbk$ для некоторого n. Следовательно, $\sum_{i=0}^{n} \lambda_i \theta^i = 0$ для некоторых $\lambda_i \in \Bbbk$, т.е. $f(\theta) = 0$, где

$$f = \sum_{i=0}^{n} \lambda_i t^i. \qquad \square$$

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 $\mathbb{L}/\mathbb{K}$ и

$$\sum_{i} \lambda_{i,j} a_i \in \mathbb{K},$$

то $\sum_i \lambda_{i,j} a_i = 0 \quad$ для любого элемента 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 $\Bbbk$. $\square$

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 $\alpha, \beta \in \mathbb{K}$ 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. $\square$

Определение. Пусть $\mathbb{K}/\Bbbk$ – любое расширение полей и пусть $\theta \in \mathbb{K}$ – алгебраический над $\Bbbk$ элемент. Ненулевой многочлен $\mu_\theta^\Bbbk(t) \in \Bbbk[t]$ минимальной степени, для которого θ является корнем, называется *минимальным многочленом* элемента θ над $\Bbbk$. Если это не приводит к путанице, вместо $\mu_\theta^\Bbbk(t)$ мы будем писать просто μ_θ или даже μ.

Предположим, что расширение $\mathbb{K}/\Bbbk$ конечно. Тогда отображение $\mathscr{A}_\theta\colon \mathbb{K} \to \mathbb{K}$, заданное формулой $\mathscr{A}_\theta(\beta) = \theta\beta$, является линейным оператором в конечномерном пространстве. Многочлен μ_θ совпадает с минимальным многочленом этого линейного оператора.

Предложение. *Пусть $\mathbb{K}/\Bbbk$ – расширение полей и пусть $\theta \in \mathbb{K}$ – алгебраический над $\Bbbk$ элемент.*

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

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

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

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

Тогда

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

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

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

9.3 Целые расширения колец

Определение. Пусть Q – коммутативное ассоциативное кольцо с единицей и пусть R – его подкольцо (содержащее единицу). Элемент $\theta \in Q$ называется *целым* над R, если существует многочлен $f \in R[t]$ со старшим коэффициентом 1:

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0, \qquad a_i \in R \tag{‡}$$

такой, что $f(\theta) = 0$. Кольцо Q называется *целым* над R, если каждый элемент $\theta \in Q$ является целым над R.

Определение. Пусть Q – коммутативное ассоциативное кольцо с единицей и пусть R – его подкольцо (содержащее единицу). Говорят, что R *целозамкнуто в* Q, если каждый элемент $a \in Q$ цел над R. Кольцо R называется *целозамкнутым*, если оно целозамкнуто в своем поле частных $\mathbb{K}$.

Пример. Кольцо целых чисел $\mathbb{Z}$ является целозамкнутым. Действительно, любой рациональный корень многочлен вида (‡) является целым.

Предложение. *Пусть Q – коммутативное ассоциативное кольцо с единицей и пусть R – его подкольцо (содержащее единицу). Предположим, что Q конечно порождено как R-модуль. Тогда R целозамкнуто в Q.*

Доказательство. Возьмем любой элемент $a \in Q$. Пусть $\mathbf{e}_1, \ldots, \mathbf{e}_n$ – элементы, порождающие Q как R-модуль. Тогда мы можем записать

$$a\mathbf{e}_j = \sum_{i=1}^{n} \lambda_{i,j}\mathbf{e}_i$$

для некоторых $\lambda_{i,j} \in R$. Эти равенства можно переписать в матричном виде:

$$(\mathbf{e}_1, \ldots, \mathbf{e}_n) \cdot A = (0, \ldots, 0),$$

где

$$A := \begin{pmatrix} \lambda_{1,1} - a & \lambda_{1,2} & \ldots & \lambda_{1,n} \\ \lambda_{2,1} & \lambda_{2,2} - a & \ldots & \lambda_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_{n,1} & \lambda_{n,2} & \ldots & \lambda_{n,n} - a \end{pmatrix}$$

Домножим обе части на присоединенную матрицу

$$(\mathbf{e}_1, \ldots, \mathbf{e}_n) \cdot A \cdot \hat{A} = (\mathbf{e}_1, \ldots, \mathbf{e}_n) \cdot \det(A)E = (\det(A)\mathbf{e}_1, \ldots, \det(A)\mathbf{e}_n) = (0, \ldots, 0).$$

Получим, что $\det(A)\mathbf{e}_i = 0$ для всех $\mathbf{e}_i$. Но это означает, что $\det(A)\, x = 0$ для любого элемента $x \in Q$. В частности, $\det(A)\, 1 = \det(A) = 0$. Таким образом, a является корнем характеристического многочлена

$$\chi(t) := \det \begin{pmatrix} \lambda_{1,1} - t & \lambda_{1,2} & \ldots & \lambda_{1,n} \\ \lambda_{2,1} & \lambda_{2,2} - a & \ldots & \lambda_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_{n,1} & \lambda_{n,2} & \ldots & \lambda_{n,n} - t \end{pmatrix}$$

□

Следствие. *Пусть S – коммутативное ассоциативное кольцо с единицей и пусть R – его подкольцо (содержащее единицу). Для любого элемента $a \in S$ следующие условия эквивалентны:*

(i) *элемент a цел над R;*

(ii) *кольцо $R[a]$ конечно порождено как R-модуль.*

Доказательство. (i) $\Longrightarrow$ (ii) Предположим, что a цел над R, т.е. $a^n + b_{n-1}a^{n-1} + \cdots + b_1 a + b_0 = 0$ для некоторых $b_i \in R$. Ясно, что $R[a]$ как R-модуль порождается элементами a^m. Так как при $m > n$ мы можем выразить

$$a^m = -b_{n-1}a^{m-1} - \cdots - b_1 a^{m-n+1} - b_0 a^{m-n},$$

то мы можем ограничиться только конечным числом элементов a^m.

Импликация (ii) $\Longrightarrow$ (i) непосредственно следует из предложения, примененного к $Q = R[a]$. □

Следствие. *Пусть S – коммутативное ассоциативное кольцо с единицей и пусть R – его подкольцо (содержащее единицу). Все элементы S целые над R образуют подкольцо $\bar{R} \subset S$.*

Доказательство. Достаточно показать, что множество $\bar{R}$ вместе с любыми двумя элементами a, b содержит их разность и произведение, а для этого достаточно показать, что подкольцо $R[a,b]$ конечно порождено как R-модуль. Так как a цел над R, то подкольцо $R[a]$ конечно порождено как R-модуль. Так как b цел над R, то он цел над $R[a]$ и поэтому подкольцо $R[a,b] = R[a][b]$ конечно порождено как $R[a]$-модуль. Пусть элементы $a_1, \ldots, a_n$ порождают $R[a]$ над R, а элементы $b_1, \ldots, b_m$ порождают $R[a,b]$ над $R[a]$. Тогда всевозможные произведения $a_1b_1, a_1b_2, \ldots, a_nb_m$ порождают $R[a,b]$ над R. □

Теорема. *Факториальное кольцо целозамкнуто.*

Доказательство. Пусть $\alpha/\beta \in \mathbb{K}$ целый над R элемент, где α, $\beta \in R$, $\beta \neq 0$. Мы можем считать, что дробь α/β несократима. Тогда

$$\left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \cdots + a_1\frac{\alpha}{\beta} + a_0 = 0.$$

Отсюда

$$\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n = 0.$$

Несложно видеть, что β делит α^n. По нашему предположению о несократимости дроби β является обратимым, т.е. $\alpha/\beta \in R$. □

Задачи

9.1. Докажите, что кольцо целых гауссовых чисел $\mathbb{Z}[\boldsymbol{i}] = \{a + \boldsymbol{i}b \mid a, b \in \mathbb{Z}\}$ является целозамкнутым.

9.2. Докажите, что кольцо $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ является целозамкнутым.

9.3. Пусть $R \subset Q \subset P$ – кольца (с общей единицей) такие, что Q цело над R, а P цело над Q. Докажите, что P цело над R.

9.4. Докажите, что кольцо $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ не является целозамкнутым и его целым замыканием является кольцо

$$\mathbb{Z}[\zeta] = \{a + b\zeta + c\zeta^2 \mid a, b, c \in \mathbb{Z}\},$$

где $\zeta = \zeta_3$ – первообразный корень степени 3 из 1.

9.5. Докажите, что кольцо R

$$R := \Bbbk[x,y]/(y^2 - x^3 + x).$$

не является целозамкнутым. Найдите его целое замыкание.

Лекция 10

Расширения полей

10.1 Присоединение к полю корня неприводимого многочлена

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

(i) *Следующие три условия эквивалентны:*

  (a) *многочлен f неприводим,*

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

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

(ii) *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. (i) Докажем (i)(a) $\Longrightarrow$ (i)(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 (i)(b) $\Longrightarrow$ (i)(c) очевидна. Для доказательства (i)(c) $\Longrightarrow$ (i)(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.

(ii) 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 (ii) образ $\theta := \pi(t)$ является корнем многочлена f. Степень расширения $[\Bbbk[t]/(f) : \Bbbk]$ равна степени многочлена f.

10.2 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:

$$f = c\prod_{i=1}^{n}(t - \alpha_i),$$

где $c \in \Bbbk$, а $\alpha_i \in \mathbb{K}$ и элементы α_i порождают $\mathbb{K}$ над $\Bbbk$, т.е. $\mathbb{K} = \Bbbk(\alpha_1, \ldots, \alpha_n)$.

Таким образом, поле разложения многочлена $f \in \Bbbk[t]$ – это минимальное поле, содержащее $\Bbbk$, в котором f в котором f разлагается на линейные множители.

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 $\mathbb{K}_1/\Bbbk$, где $\mathbb{K}_1 = \Bbbk[t]/(f_1)$. 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 $\mathbb{K}^\sharp_{l-1} := \varphi_{l-1}(\mathbb{K}_{l-1})$. Пусть $f_l^\sharp \in \mathbb{K}^\sharp_{l-1}[t]$ – многочлен, полученный применением φ_{l-1} ко всем коэффициентам f_l. Этот многочлен неприводим над $\mathbb{K}^\sharp_{l-1}$ и имеет корень $\theta_l^\sharp \in \mathbb{K}^\sharp$. Тогда

$$\mathbb{K}_l = \mathbb{K}_{l-1}(\theta_l) \simeq \mathbb{K}_{l-1}[t]/(f_l) \simeq \mathbb{K}^\sharp_{l-1}[t]/(f_l^\sharp) \simeq \mathbb{K}^\sharp_{l-1}(\theta_l^\sharp).$$

Следовательно, существует изоморфизм

$$\varphi_l : \mathbb{K}_l \longrightarrow \mathbb{K}^\sharp_{l-1}(\theta_l^\sharp) \subset \mathbb{K}^\sharp.$$

На последнем шаге мы получим изоморфизм

$$\varphi = \varphi_l : \mathbb{K}_m = \mathbb{K} \longrightarrow \mathbb{K}^\sharp_m \subset \mathbb{K}^\sharp.$$

Так как $f^\sharp$ разлагается в $\mathbb{K}^\sharp_m$ на линейные множители, то $\mathbb{K}^\sharp_m = \mathbb{K}^\sharp$. □

Замечание. Пусть $f \in \Bbbk[t]$ – многочлен положительной степени и пусть $\mathbb{K}$ – его поле разложения f над $\Bbbk$. Мы считаем, что f неприводим. 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 θ_2, $\theta_3 \in \Bbbk(\theta_1)$, т.е. $\Bbbk(\theta_1) = \mathbb{K}$. Следовательно, $[\mathbb{K} : \Bbbk] = 3$.

Пусть $\sqrt{D} \notin \Bbbk$. Предположим, что $[\mathbb{K} : \Bbbk] = 3$. Тогда $\Bbbk(\theta_1) = \mathbb{K}$. Следовательно, θ_2, $\theta_3 \in \Bbbk(\theta_1)$ и поэтому $\sqrt{D} \in \Bbbk(\theta_1)$. Таким образом, мы имеем башню полей

$$\Bbbk \subset \Bbbk(\sqrt{D}) \subset \Bbbk(\theta_1).$$

По теореме о башне полей

$$[\Bbbk(\theta_1) : \Bbbk] = [\Bbbk(\theta_1) : \Bbbk(\sqrt{D})] \cdot [\Bbbk(\sqrt{D}) : \Bbbk].$$

Так как $[\Bbbk(\theta_1) : \Bbbk] = 3$ и $[\Bbbk(\sqrt{D}) : \Bbbk] = 2$, то мы получаем противоречие.

10.3 Конструкция алгебраического замыкания поля

Теорема. *Для любого поля $\Bbbk$ существует алгебраическое расширение $\bar{\Bbbk}/\Bbbk$ такое, что поле $\bar{\Bbbk}$ алгебраически замкнуто.*

Сначала докажем следующую лемму.

Лемма. *Для любого поля $\Bbbk$ существует расширение $\mathbb{L}/\Bbbk$ такое, что поле $\mathbb{L}$ алгебраически замкнуто.*

Доказательство. Пусть Σ – множество всех неприводимых многочленов над $\Bbbk$ со старшим коэффициентом 1. Каждому многочлену $f \in \Sigma$ сопоставим независимую переменную t_f. Рассмотрим кольцо многочленов от всех этих переменных

$$R := \Bbbk\left[\{t_f \mid f \in \Sigma\}\right]$$

и идеал $\mathfrak{I} \subset R$, порожденный многочленами $f(t_f)$ для всех $f \in \Sigma$. Мы утверждаем, что идеал $\mathfrak{I}$ не является единичным. Действительно, иначе для некоторых $f_1, \ldots, f_n \in \Sigma$ и некоторых $g_1, \ldots, g_n \in R$ выполнялось бы равенство

$$\sum_{i=1}^{n} g_i\, f_i(t_{f_i}) = 1.$$

Рассмотрим расширение $\mathbb{K}/\Bbbk$ такое, что все многочлены $f_1, \ldots, f_n$ имеют корни в $\mathbb{K}$. Пусть $\theta_i \in \mathbb{K}$ – корень f_i. Подставим в наше соотношение $t_{f_1} = \theta_1, \ldots, t_{f_n} = \theta_n$. Тогда левая часть занулится, что невозможно. Следовательно, $\mathfrak{I}$ содержится в максимальном идеале $\mathfrak{M}$. Факторкольцо

$$\Bbbk_1 := R/\mathfrak{M}$$

является полем. Так как $\mathfrak{M}$ содержит все многочлены $f(t_f)$, то в $\Bbbk_1$ каждый из этих многочленов имеет корень – образ t_f. Мы построили поле $\Bbbk_1$, в котором каждый многочлен с коэффициентами из $\Bbbk$ имеет корень. Применим нашу конструкцию к $\Bbbk_1$. Получим поле $\Bbbk_2$, в котором каждый многочлен с коэффициентами из $\Bbbk_1$ имеет корень. Продолжая процесс, получим вложенную цепочку полей

$$\Bbbk \subset \Bbbk_1 \subset \Bbbk_2 \subset \cdots \subset \Bbbk_n \subset \cdots$$

Такую, что каждый многочлен с коэффициентами из $\Bbbk_n$ имеет корень в $\Bbbk_{n+1}$. Положим

$$\mathbb{L} := \bigcup_{i=1}^{\infty} \Bbbk_i.$$

Тогда $\mathbb{L}$ – поле. Более того, каждый многочлен $f \in \Bbbk_n[t]$ для любого n имеет корень в $\mathbb{L}$. Поскольку каждый многочлен $f \in \mathbb{L}[t]$ лежит в некотором $\Bbbk_n[t]$, то он также имеет корень в $\mathbb{L}$. Следовательно, поле $\mathbb{L}$ алгебраически замкнуто. □

Доказательство теоремы. Пусть $\bar{\Bbbk} \subset \mathbb{L}$ – множество всех алгебраических элементов над $\Bbbk$. Тогда $\bar{\Bbbk}$ снова поле. Пусть $f \in \bar{\Bbbk}[t]$ – неприводимый многочлен. Так как $\mathbb{L}$ алгебраически замкнуто, то f имеет корень $\theta \in \mathbb{L}$. Элемент θ алгебраичен над $\bar{\Bbbk}$, а поле $\bar{\Bbbk}$ является алгебраическим расширением поля $\Bbbk$. Значит, θ алгебраичен над $\Bbbk$ и по конструкции $\theta \in \Bbbk$. □

Задачи

10.1. Вычислите степень поля разложения многочлена $t^3 - 2$ над $\mathbb{Q}$.

10.2. Пусть $\mathbb{Q}_1 \subset \mathbb{C}$ – подполе, полученное присоединением корней всех неприводимых многочленов над $\mathbb{Q}$. Докажите, что поле $\mathbb{Q}_1$ алгебраически замкнуто.

10.3. Пусть $\Bbbk$ – поле и пусть $\bar{\Bbbk}$ – его алгебраическое замыкание. Докажите, что для любого элемента $\theta \in \bar{\Bbbk} \setminus \Bbbk$ существует максимальное подполе $\mathbb{K} \subset \bar{\Bbbk}$, не содержащее θ. *Указание.* Воспользуйтесь леммой Цорна.

Лекция 11

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 $\mathbb{F}_p$.

11.1 Отображение Фробениуса

Пусть $\Bbbk$ – поле характеристики $p > 0$. Рассмотрим отображение

$$\phi : \Bbbk \longrightarrow \Bbbk, \qquad a \longmapsto a^p.$$

Это отображение называется *отображением Фробениуса* . Его образ мы обозначим через $\Bbbk^p$:

$$\Bbbk^p := \phi(\Bbbk) = \{a^p \mid a \in \Bbbk\}.$$

Предложение. (i) *Отображение является тождественным на простом подполе* $\Bbbk_0 \simeq \mathbb{F}_p$.

(ii) $\Bbbk^p$ *является подполем в* $\Bbbk$.

(iii) ϕ *является изоморфизмом между* $\Bbbk$ *и* $\Bbbk^p$.

(iv) *Если поле* $\Bbbk$ *конечно, то* $\Bbbk^p = \Bbbk$.

Доказательство. Первое утверждение очевидно, поскольку, $\phi(1) = 1$ и $\phi(n \cdot 1) = n\phi(1) = n \cdot 1$ для любого целого n.

Для доказательства (ii) запишем

$$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$$

и

$$\phi(a + b) = (a + b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}.$$

В последней сумме биномиальные коэффициенты $\binom{p}{k} = \frac{p!}{(p-k)!k!}$ рассматриваются как целые числа. Так как все они делятся на p, то

$$\phi(a + b) = (a + b)^p = a^p + b^p = \phi(a) + \phi(b).$$

Из этого следует, что $\phi : \Bbbk \to \Bbbk$ – гомоморфизм колец. Так как ядро этого гомоморфизма тривиально, то ϕ является изоморфизмом между $\Bbbk$ и $\phi(\Bbbk)$. В частности, $\phi(\Bbbk)$ – поле. Это доказывает (ii) и (iii). Утверждение (iv) следует из того, что в случае конечного поля $\Bbbk^p$ содержит столько же элементов, что и $\Bbbk$. □

Таким образом, если $\Bbbk^p = \Bbbk$, то отображение ϕ является автоморфизмом поля $\Bbbk$. Он называется *автоморфизмом Фробениуса.*

11.2 Строение конечных полей

Теорема (Первая теорема о строении конечных полей)**.** *Пусть $\Bbbk$ – конечное поле характеристики $p > 0$ и пусть $\Bbbk_0$ – его простое подполе. Тогда*

(i) *число элементов $\Bbbk$ равно p^m, где $m = [\Bbbk : \Bbbk_0]$,*

(ii) *$\Bbbk$ 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 $(x_1, \dots, x_m)$ (в фиксированном базисе), а в нашем случае для каждой координаты x_i имеется ровно p возможностей, так как $x_i \in \Bbbk_0 \simeq \mathbb{F}_p$.

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 $\mathbb{F}_p$ 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 $\mathbb{F}_p$ конечно (поскольку является конечномерным пространством над $\mathbb{F}_p$), а значит состоит из p^l элементов. Рассмотрим подмножество $M \subset \mathbb{K}$, состоящее из всех корней $t^q - t$. Заметим, что $a^q = a^{p^m} = \phi^m(a)$, где $\phi : \mathbb{K} \to \mathbb{K}$ – автоморфизм Фробениуса. Таким образом,

$$M = \{a \in \mathbb{K} \mid \phi^m(a) = a\}$$

– множество неподвижных элементов ϕ^m. Это множество замкнуто относительно операций:

$$a, b \in M \quad \Longrightarrow \quad \phi^m(a) = a,\ \phi^m(b) = b \quad \Longrightarrow \quad \phi^m(a \pm b) = \phi^m(a) \pm \phi^m(b) = a \pm b \in M$$

(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 $\theta \in \mathbb{K}$, который порождает $\mathbb{K}$ над $\Bbbk$ (т. е., $\mathbb{K} = \Bbbk(\theta)$).*

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, НОД $(f, t^{q^d} - t) \neq 1$. 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

$$\text{НОД } (f, t^{q^d} - t) = f.$$

Отсюда получается первое утверждение.

Для доказательства второго рассмотрим порождающий элемент θ поля $\mathbb{F}_{q^d}$ над $\mathbb{F}_q$. Пусть $\mu_\theta \in \mathbb{F}_q[t]$ – минимальный многочлен для θ. Тогда μ_θ неприводим и $\deg \mu_\theta = [\mathbb{F}_{q^d} : \mathbb{F}_q] = d$. Это доказывает следствие. □

Пример. Построим поле $\mathbb{F}_8$ из 8 элементов. Любой элемент из $\mathbb{F}_8$ может быть записан как линейная комбинация $\alpha_0 + \alpha_1\theta + \alpha_2\theta^2$, $\alpha_i \in \mathbb{F}_2$. Для составления таблицы умножения мы должны найти минимальный многочлен $\mu = \mu_\theta$ 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 $\theta^3 = -\theta - 1 = \theta + 1$. Обе возможности приводят к изоморфным полям.

11.3 Автоморфизмы конечных полей

Теорема. *Пусть $\mathbb{F}_q$ – конечное поле, $q = p^n$.*

(i) *Группа автоморфизмов $\mathrm{Aut}(\mathbb{F}_q)$ поля $\mathbb{F}_q$ является циклической порядка n и порождается автоморфизмом Фробениуса ϕ.*

(ii) *Пусть $G \subset \mathrm{Aut}(\mathbb{F}_q)$ – подгруппа порядка m. Множество*

$$\mathbb{K} := \{a \in \mathbb{F}_q \mid \psi(a) = a \qquad \forall \psi \in G\} \tag{$*$}$$

Является подполем в $\mathbb{F}_q$ и $\mathbb{K} \simeq \mathbb{F}_{p^{n-m}}$.

(iii) *Пусть $\mathbb{F}_{p^d}$ – подполе поля $\mathbb{F}_q$. Множество*

$$\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_{p^d}) := \{\psi \in \mathrm{Aut}(\mathbb{F}_q) \mid \psi(a) = a, \quad \forall a \in \mathbb{F}_{p^d}\} \tag{$\dagger$}$$

является подгруппой в $\mathrm{Aut}(\mathbb{F}_q)$ и порождается элементом ϕ^d.

Доказательство. (i) Поле $\mathrm{Aut}(\mathbb{F}_q)$ порождается над $\mathbb{F}_p$ одним элементом: $\mathrm{Aut}(\mathbb{F}_q) = \mathbb{F}_p[\theta]$. Пусть $\mu(t) = \mu_\theta(t)$ – минимальный многочлен этого элемента. Любой автоморфизм $\psi \in \mathrm{Aut}(\mathbb{F}_q)$ является тождественным на $\mathbb{F}_p \subset \mathbb{F}_q$ и однозначно задается образом θ. С другой стороны, ϕ корни многочлена $\mu \in \mathbb{F}_p$ переводит в корни. Так как $\deg(\mu) = n$, то для $\psi(\theta)$ имеется не более n возможностей. Таким образом, $|\mathrm{Aut}(\mathbb{F}_q)| \leq n$.

Далее, пусть m – порядок элемента ϕ в группе $\mathrm{Aut}(\mathbb{F}_q)$. Так как $a = a^{p^n} = \phi^n(a)$ для любого $a \in \mathbb{F}_q$, то m делит n. Далее, ϕ^m – тождественный автоморфизм, т.е. $\phi^m(a) = a$ для любого $a \in \mathbb{F}_q$. Это эквивалентно равенству $a^{p^m} - a = 0$. Иначе говоря, каждый элемент $\mathbb{F}_q$ является корнем многочлена $t^{p^m} - t$. Отсюда получаем, что $m \geq n$. Таким образом, порядок элемента ϕ в группе $\mathrm{Aut}(\mathbb{F}_{p^n})$ равен n и $\mathrm{Aut}(\mathbb{F}_{p^n})$ порождается этим элементом.

(ii) Непосредственно из $(*)$ следует, что множество $\mathbb{K}$ замкнуто относительно взятия сумм, разностей, произведений и частных. Значит, оно является подполем. Так как G является подгруппой в циклической группе $\mathrm{Aut}(\mathbb{F}_q)$, то она является циклической группой и порождается элементом ϕ^{n-m}. Тогда все все элементы поля $\mathbb{K}$ являются корнями многочлена $t^{p^{n-m}} - t$. Многочлен $t^{p^n} - t$ делится на многочлен $t^{p^{n-m}} - t$. Значит, $t^{p^{n-m}} - t$ разлагается на линейные множители в $\mathbb{F}_q$ и поэтому $\mathbb{K}$ – поле разложения многочлена $t^{p^{n-m}} - t$ над $\mathbb{F}_p$. Согласно структурной теории конечных полей $\mathbb{K} = \mathbb{F}_{p^{n-m}}$.

(iii) Непосредственно из $(\dagger)$ следует, что множество $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_{p^d})$ замкнуто относительно произведения и взятия обратных. Значит, оно является подгруппой в циклической группе $\mathrm{Aut}(\mathbb{F}_q)$,

а потому тоже является циклической группой. Так как все элементы поля $\mathbb{F}_d$ являются корнями многочлена $t^d - t$, то $\phi^d(a) = a^{p^d} = a$ для любого $a \in \mathbb{F}_d$. Поэтому $\phi^d \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_{p^d})$. Если же $\phi^k \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_{p^d})$ для некоторого k, то $\phi^k(a) = a^{p^k} = a$ для любого $a \in \mathbb{F}_d$. Значит, все элементы поля $\mathbb{F}_d$ являются корнями многочлена $t^{p^k} - t$. Но тогда $t^{p^k} - t$ делится на $t^{p^d} - t$. Отсюда k делится на d. Значит, ϕ^d порождает $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_{p^d})$. □

11.4 Группа обратимых элементов кольца вычетов

Теорема. (i) *Если p – нечетное простое число, то $(\mathbb{Z}/p^m\mathbb{Z})^*$ – циклическая группа.*

(ii) *При $m \geq 3$ группа $(\mathbb{Z}/2^m\mathbb{Z})^*$ является прямым произведением циклических групп порядков 2^{m-2} и 2.*

Доказательство. (i) Напомним, что порядок группы $(\mathbb{Z}/p^m\mathbb{Z})^*$ равен $(p-1)p^{m-1}$. Согласно третьей теореме о строении конечных полей утверждение верно для $m = 1$, т.е. существует $a \in \mathbb{Z} \setminus p\mathbb{Z}$ такое, что его образ в группе $\mathbb{Z}/p\mathbb{Z}$ имеет порядок $p-1$. Будем искать образующий элемент группы $(\mathbb{Z}/p^m\mathbb{Z})^*$ в виде $a + pt$ для подходящего $t \in \mathbb{Z}$. Для этого запишем

$$(a+pt)^{p-1} = 1 + pu, \quad u \in \mathbb{Z}. \tag{‡}$$

Потребуем, чтобы выполнялось условие $u \not\equiv 0 \mod p$. Так как $a^{p-1} \equiv 0 \mod p$, то существует $k \in \mathbb{Z}$ такое, что

$$\begin{aligned} a^{p-1} &= 1 + pk \\ (a+pt)^{p-1} &= 1 + p(k + a^{p-2}t + pr), \qquad r \in \mathbb{Z}. \end{aligned}$$

Тогда $u = k + a^{p-2}t + pr$. Так как НОД $(p, a) = 1$, то можно взять t так, что $u \not\equiv 0 \mod p$.

Пусть n – порядок образа построенного элемента $a+pt$ в группе $(\mathbb{Z}/p^m\mathbb{Z})^*$. Имеем $(a+pt)^n \equiv 1 \mod p^m$. В частности, $a^n \equiv 1 \mod p$. Так как образ a в группе $\mathbb{Z}/p\mathbb{Z}$ имеет порядок $p-1$, то $n \equiv 0 \mod p-1$. По теореме Лагранжа n делит $(p-1)p^{m-1}$. Значит n имеет вид $n = p^l(p-1)$.

Из (‡) последовательно получаем

$$\begin{array}{rcll} (a+pt)^{p-1} &=& 1+pu, & u \not\equiv 0 \mod p, \\ (a+pt)^{p(p-1)} &=& (1+pu)^p = 1 + p^2u_1, & u_1 \not\equiv 0 \mod p, \\ (a+pt)^{p^2(p-1)} &=& (1+p^2u_1)^p = 1+p^3u_2, & u_2 \not\equiv 0 \mod p, \\ \multicolumn{4}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\ (a+pt)^{p^{m-2}(p-1)} &=& (1+p^{m-2}u_{m-3})^p = 1 + p^{m-1}u_{m-2}, & u_{m-2} \not\equiv 0 \mod p. \end{array}$$

Значит, l не равно $m-2$. Таким образом, $l = m-1$ и $n = p^{m-1}(p-1)$.

(ii) Индукцией по m докажем, что

$$5^{2^{m-3}} \equiv 1 + 2^{m-1} \mod 2^m.$$

Базой индукции является случай $m = 3$ и он тривиален. Пусть сравнение верно для m. Тогда

$$5^{2^{m-2}} = \left(5^{2^{m-3}}\right)^2 = (1 + 2^{m-1} + 2^m k)^2 \equiv 1 + 2^{m-2} \mod 2^{m+1}.$$

Значит, шаг индукции работает и сравнение верно для всех m. Отсюда получаем, что

$$5^{2^{m-3}} \not\equiv 1 \mod 2^m \quad \text{и} \quad 5^{2^{m-2}} \equiv 1 \mod 2^m,$$

т.е. порядок образа 5 в группе $(\mathbb{Z}/2^m\mathbb{Z})^*$ равен 2^{m-2}.

Ясно, что порядок образа -1 в группе $(\mathbb{Z}/2^m\mathbb{Z})^*$ равен 2. Если бы образ -1 лежал в подгруппе, порожденной образом 5, то выполнялось бы сравнение

$$-1 \equiv 5^k \mod 2^m.$$

Но тогда $-1 \equiv 5^k \equiv 1 \mod 4$. Противоречие. Значит, $(\mathbb{Z}/2^m\mathbb{Z})^*$ является прямым произведением подгрупп, порожденных образами 5 и -1. □

Следствие. *Для нечетного простого p группа автоморфизмов (аддитивной) группы $\mathbb{Z}/p^m\mathbb{Z}$ является циклической порядка $p^m - p^{m-1}$.*

Доказательство. Следует из того, что $\mathrm{Aut}(\mathbb{Z}/p^m\mathbb{Z}) \simeq (\mathbb{Z}/p^m\mathbb{Z})^*$. □

Задачи

11.1. Докажите, что неприводимый многочлен $f \in \mathbb{F}_q$ делит $t^{q^e} - t$ тогда и только тогда, когда $\deg(f)$ делит e,

11.2. Пусть $\Bbbk$ – поле. Могут ли быть изоморфны мультипликативная и аддитивная группы $\Bbbk$?

11.3. Пусть $\Bbbk$ – поле. Пусть $\Bbbk^+$ и $\Bbbk^*$ – его мультипликативная и аддитивная группы, соответственно.

(a) Когда $\Bbbk^*$ – циклическая?

(b) Когда $\Bbbk^+$ – циклическая?

11.4. Когда аддитивная группа поля $\Bbbk$ конечно порождена?

11.5. Докажите, что мультипликативная группа поля $\Bbbk$ конечно порождена тогда и только тогда, когда поле конечно.

11.6. Докажите, что множество неподвижных точек

$$\{a \in \Bbbk \mid \phi(a) = a\}$$

отображения Фробениуса совпадает с простым подполем $\Bbbk_0 \subset \Bbbk$. Что представляет собой множество неподвижных точек отображения ϕ^k?

11.7. Как устроены группы $(\mathbb{Z}/n\mathbb{Z})^*$ при $n = 2p^m$ и $4p^m$, p – нечетное простое?

11.8. Найдите все неприводимые многочлены степени 2 над полем $\mathbb{F}_3$.

11.9. Найдите число неприводимых многочленов степеней 2 и 3 над полем $\mathbb{F}_9$.

11.10. Докажите, что при $a \neq 1$ многочлен $t^q + at + b$ имеет в $\mathbb{F}_q$ корень.

11.11. Пусть $\tilde{\mathbb{F}}$ – бесконечное алгебраическое расширение поля $\mathbb{F}_q$. Верно ли, что $\tilde{\mathbb{F}}$ алгебраически замкнуто?

11.12. Докажите, что алгебраическое замыкание поля $\mathbb{F}_q$ может быть построено как объединение башни полей

$$\mathbb{F}_q \subset \mathbb{F}_{q^{2!}} \subset \mathbb{F}_{q^{3!}} \subset \cdots \subset \mathbb{F}_{q^{e!}} \subset \mathbb{F}_{q^{(e+1)!}} \subset \cdots$$

11.13. Докажите, что при четном q все элементы поля $\mathbb{F}_q$ являются квадратами, а при нечетном q квадраты в $\mathbb{F}_q^*$ образуют подгруппу индекса 2.

11.14. Докажите, что над полем $\mathbb{F}_q$, $q = p^n$ многочлен $t^p - a$ или является неприводимым или полностью раскладывается на линейные множители (как?).

Лекция 12

Алгебры над полем

12.1 Определение алгебр

Определение. Пусть A – векторное пространство над полем $\Bbbk$. Говорят, что A является *алгеброй* над $\Bbbk$ если A является кольцом и умножение в кольце связано с умножением на скаляры следующим образом:

$$\lambda(\mathbf{a}\cdot\mathbf{b}) = (\lambda\mathbf{a})\cdot\mathbf{b} = \mathbf{a}\cdot(\lambda\mathbf{b}) \qquad \forall \mathbf{a},\, \mathbf{b}\in A, \quad \forall\lambda\in\Bbbk.$$

Обобщением этого понятия является *алгебра над кольцом*.

Алгебра называется *ассоциативной* (*коммутативной*, *без делителей нуля* и т.д.) если таковым является соответствующее кольцо. Говорят, что A – *алгебра с делением*, если A – алгебра, в которой существует единица и любой ненулевой элемент обратим: для любого $\mathbf{a}\in A$, $\mathbf{a}\neq 0$ существует $\mathbf{a}^{-1}\in A$ такой, что $\mathbf{a}\cdot\mathbf{a}^{-1} = \mathbf{a}^{-1}\cdot\mathbf{a} = 1$. В этом случае множество $A^* := A\setminus\{0\}$ является (необязательно абелевой) группой по умножению.

Приведем примеры алгебр над полем. Начнем со стандартных примеров, обсуждавшихся ранее.

Примеры. (i) Пусть A – векторное пространство над полем $\Bbbk$. Оно является алгеброй над $\Bbbk$ с нулевым умножением: $\mathbf{a}\cdot\mathbf{b} = 0$ для любых элементов $\mathbf{a}$, $\mathbf{b}\in\Bbbk$.

(ii) Если $\mathbb{K}/\Bbbk$ – расширение полей, то $\mathbb{K}$ – алгебра над $\Bbbk$. В частности, $\mathbb{C}$ – (коммутативная и ассоциативная) алгебра с делением над $\mathbb{R}$.

(iii) Все квадратные $n\times n$-матрицы над полем $\Bbbk$ образуют ассоциативную алгебру $\mathrm{Mat}_n(\Bbbk)$ с единицей над $\Bbbk$.

(iv) Алгебра многочленов $\Bbbk[t_1,\ldots,t_n]$ – ассоциативная коммутативная алгебра с единицей.

Любая конечномерная алгебра может быть задана следующим способом.

Пример. Пусть A – конечномерная алгебра над $\Bbbk$ с базисом $\mathbf{e}_1,\ldots,\mathbf{e}_n$. Тогда умножение в A однозначно определяется произведениями элементов $\mathbf{e}_i\mathbf{e}_j$. Действительно, для $\mathbf{a} = \sum_i \lambda^i\mathbf{e}_i \in A$ и $\mathbf{b} = \sum_j \mu^j\mathbf{e}_j \in A$ имеем (мы используем тензорные обозначения)

$$\mathbf{a}\cdot\mathbf{b} = \Big(\sum_i \lambda^i\mathbf{e}_i\Big)\cdot\Big(\sum_j \mu^j\mathbf{e}_j\Big) = \sum_{i,j}\lambda^i\mu^j\mathbf{e}_i\cdot\mathbf{e}_j.$$

С другой стороны, мы можем разложить элементы $\mathbf{e}_i \cdot \mathbf{e}_j$ по базису

$$\mathbf{e}_i \cdot \mathbf{e}_j = \sum_k \theta_{i,j}^k \mathbf{e}_k.$$

Скаляры $\theta_{i,j}^k$ односначно задают алгебру A. Они называются *структурными константами* алгебры.

Приведем больше стандартных примеров алгебр.

Примеры. (i) Над полем $\mathbb{R}$ (соответственно, $\mathbb{C}$) можно определить алгебру $\mathbb{R}\{t\}$ (соответственно, $\mathbb{C}\{t\}$) сходящихся (например в 0), степенных рядов. Над любым полем определена алгебра *формальных степенных рядов* $\Bbbk[[t]]$.

(ii) Все непрерывные (соответственно, дифференцируемые) функции на интервале образуют ассоциативную коммутативную алгебру $\mathscr{C}(a,b)$ (соответственно, $\mathscr{D}(a,b)$) над $\mathbb{R}$ с единицей.

(iii) Трехмерное векторное пространство $\mathbb{R}^3$ с операцией векторного умножения является неассоциативной алгеброй.

(iv) С каждым векторным пространством над полем $\Bbbk$ связаны три ассоциативные алгебры: *тензорная* $\mathrm{T}^\bullet(V)$, *внешняя* $\bigwedge^\bullet(V)$ и *симметрическая* $\mathrm{S}^\bullet(V)$.

(v) Пусть G – группа (для простоты предположим, что G – конечная) и пусть A – векторное пространство над $\Bbbk$ с базисом $\mathbf{e}_g$, $g \in G$. Определим умножение элементов базиса следующим образом: $\mathbf{e}_g \cdot \mathbf{e}_h = \mathbf{e}_{gh}$. По линейности это умножение продолжается на все A. Мы получим ассоциативную алгебру с единицей. Она называется *групповой алгеброй* G и обозначается $\Bbbk[G]$.

Определение. *Гомоморфизм алгебр* (над одним и тем же полем $\Bbbk$) – это гомоморфизм колец, который является $\Bbbk$-линейным отображением. Аналогично определяются понятия изоморфизма и автоморфизма алгебр.

Пусть A, A_1 – алгебры над полем $\Bbbk$, пусть $\varphi : A \to A_1$ – $\Bbbk$-линейное отображение (как векторных пространств) и пусть $\mathbf{e}_1, \dots, \mathbf{e}_n$ – базис A. Отображение φ является гомоморфизмом алгебр тогда и только тогда, когда

$$\varphi(\mathbf{e}_i \cdot \mathbf{e}_j) = \varphi(\mathbf{e}_i) \cdot \varphi(\mathbf{e}_j) \qquad \forall i,\, j.$$

Примеры. (i) Рассмотрим групповую алгебру $\Bbbk[G]$ конечной группы G. Отображение

$$\Bbbk[G] \longrightarrow \Bbbk, \qquad \sum \alpha_g \mathbf{e}_g \longmapsto \sum \alpha_g$$

является гомоморфизмом алгебр.

(ii) Если A – алгебра с единицей, то отображение

$$\Bbbk \longmapsto A, \qquad \alpha \longmapsto \alpha \cdot 1$$

является (инъективным) гомоморфизмом алгебр.

Определение. *Идеал в алгебре* – это идеал в кольце, который является векторным подпространством. Если $\mathfrak{I} \subset A$ – идеал в $\Bbbk$-алгебре, то на факторкольце $A/\mathfrak{I}$ можно ввести умножение на скаляры формулой

$$\alpha(\mathbf{x} + \mathfrak{I}) = \alpha\mathbf{x} + \mathfrak{I} \qquad \alpha \in \Bbbk, \qquad \mathbf{x} \in A.$$

Несложно проверить, что это определение корректно. Получившаяся алгебра называется *факторалгеброй.*

Примеры. (i) В групповой алгебре $\Bbbk[G]$ конечной группы G подмножество

$$\mathfrak{I} := \Big\{ \sum \alpha_g \mathbf{e}_g \quad \Big| \quad \sum \alpha_g = 0 \Big\}$$

является идеалом. Факторалгебра $\Bbbk[G]/\mathfrak{I}$ изоморфна $\Bbbk$.

(ii) 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 $\varphi : A \to A_1$ – гомоморфизм алгебр над полем $\Bbbk$. Тогда*

(i) $\mathrm{Ker}(\varphi)$ *– идеал в алгебре A;*

(ii) *имеется естественный изоморфизм $\varphi(A) \simeq A/\mathfrak{I}$.*

12.2 Конечномерные алгебры с делением

Лемма. *Пусть A – конечномерная ассоциативная алгебра с единицей над полем $\Bbbk$. Если в A нет делителей нуля, то A – алгебра с делением.*

Доказательство. Пусть $\mathbf{a} \in A$, $\mathbf{a} \neq 0$. Рассмотрим отображение

$$\varphi : A \longrightarrow A, \qquad \mathbf{x} \longmapsto \mathbf{a} \cdot \mathbf{x}.$$

Ясно, что это отображение является линейным оператором. Поскольку в A нет делителей нуля, то φ невырожден. В частности, он сюръективен. Положим $\mathbf{a}^{-1} = \varphi(1)$. □

Лемма. *Центр $Z(A)$ ассоциативного кольца с делением A является полем и A является алгеброй над $Z(A)$.*

Доказательство. Ясно, что $Z(A)$ – коммутативное подкольцо с делением в A, т.е. $Z(A)$ – поле. Тогда A является также векторным пространством над $Z(A)$, а поскольку A ассоциативно, то A – алгебра над $Z(A)$. □

Лемма. *Пусть A – конечномерная ассоциативная алгебра с делением над алгебраически замкнутым полем $\Bbbk$. Тогда $A \simeq \Bbbk$.*

Доказательство. Пусть элемент $\mathbf{a} \in A$ не имеет вида $\mathbf{a} = \lambda\,\mathbf{1}$, $\lambda \in \Bbbk$. Как и выше, рассмотрим оператор

$$\varphi : A \longrightarrow A, \qquad \mathbf{x} \longmapsto \mathbf{a} \cdot \mathbf{x}.$$

Над алгебраически замкнутым полем он имеет собственный вектор:

$$\exists \mathbf{x} \in A,\ \exists \lambda \in \Bbbk \quad \varphi(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} = \lambda \mathbf{x}.$$

Но тогда $(\mathbf{a} - \lambda\,\mathbf{1}) \cdot \mathbf{x} = 0$ и $\mathbf{a} = \lambda\,\mathbf{1}$. Противоречие. □

12.3 Конечные ассоциативные кольца с делением

Теорема. *Конечное ассоциативное с единицей без делителей нуля является полем.*

Доказательство. Пусть A – конечное ассоциативное с единицей без делителей нуля. Зафиксируем элемент $\mathbf{a} \in A$, $\mathbf{a} \neq 0$ и рассмотрим отображение

$$\varphi : A \longrightarrow A, \qquad \mathbf{x} \longmapsto \mathbf{a} \cdot \mathbf{x}.$$

Так как в A нет делителей нуля, то это отображение инъективно. Так как A конечно, то оно сюръективно. Значит у $\mathbf{a}$ существует обратный элемент $\mathbf{a}^{-1} = \varphi^{-1}(1)$. Следовательно, A – кольцо с делением. Его центр $\Bbbk := Z(A)$ является конечным полем, а A является алгеброй над $\Bbbk$. Достаточно доказать, что $A = \Bbbk$. Предположим противное, т.е. $A \neq \Bbbk$. Пусть $n := \dim_{\Bbbk} A$. Тогда $|A| = q^n$, $n > 1$. Для $\mathbf{a} \in A$ положим

$$C(\mathbf{a}) := \{\mathbf{x} \mid \mathbf{a} \cdot \mathbf{x} = \mathbf{x} \cdot \mathbf{a}\}.$$

Тогда $C(\mathbf{a})$ – подалгебра с делением в A. Поэтому

$$|C(\mathbf{a})| = q^{d(\mathbf{a})}$$

для некоторого $d(\mathbf{a})$. Заметим также, что A можно рассматривать как свободный модуль над $C(\mathbf{a})$. Поэтому

$$|A| = |C(\mathbf{a})|^{r(\mathbf{a})} = q^{d(\mathbf{a})r(\mathbf{a})} = q^n, \quad \text{где } r(\mathbf{a}) := \operatorname{rk}_{C(\mathbf{a})} A$$

(см. следвсвие ниже). Отсюда

$$n = d(\mathbf{a})r(\mathbf{a}).$$

С другой стороны, $\Bbbk^* = \Bbbk \setminus \{0\}$ – центр мультипликативной группы $A^* = A \setminus \{0\}$. Рассмотрим действие A^* на себе сопряжениями. Класс сопряженности элемента $\mathbf{a} \in A^*$ содержит ровно

$$\frac{|A^*|}{|C(\mathbf{a})^*|} = \frac{q^n - 1}{q^{d(\mathbf{a})} - 1}$$

элементов. При этом $|A^*|/|C(\mathbf{a})^*| = 1$ тогда и только тогда, когда $\mathbf{a} \in \Bbbk^*$. Следовательно,

$$|A^*| = q^n - 1 = q - 1 + \sum_{\mathbf{a}} \frac{q^n - 1}{q^{d(\mathbf{a})} - 1}, \qquad (*)$$

где сумма берется по всем представителям $\mathbf{a}$ классов сопряженности, содержащих более одного элемента. Иначе говоря, сумма берется по некоторым делителям $d(\mathbf{a})$ числа n таким, что $d(\mathbf{a}) <$

n. Докажем, что равенство $(*)$ невозможно. Рассмотрим круговой многочлен $\Phi_n(t)$. Напомним, что по определению

$$\Phi_n(t) = \prod_{\varepsilon \in \boldsymbol{\mu}'_n} (t - \varepsilon) \qquad (\dagger)$$

(произведение берется по множеству $\boldsymbol{\mu}'_n := \boldsymbol{\mu}_n \setminus \cup_{m<n} \boldsymbol{\mu}_m$ всех первобра́зных (примитивных) корней степени n из 1). Круговые многочлены удовлетворяют равенству

$$t^n - 1 = \prod_{d|n} \Phi_d(t).$$

По лемме Гаусса все они имеют целые коэффициенты. В частности, $\Phi_n(t)$ делит $t^n - 1$ в кольце $\mathbb{Z}[t]$. Значит, целое число $\Phi_n(q)$ делит $q^n - 1$. С другой стороны,

$$t^n - 1 = \prod_{e|d} \Phi_e(t) \prod_{e|n,\ e\nmid d} \Phi_e(t) = (t^d - 1) \prod_{e|n,\ e\nmid d} \Phi_e(t) = (t^d - 1)\Phi_n(t) \prod_{e|n,\ e\nmid d,\ e<n} \Phi_e(t).$$

Подставляя в это равенство $t = q$, получим, что $\Phi_n(q)$ делит $(q^n-1)/(q^d-1)$ для любого делителя d числа n такого, что $d < n$. Из равенства $(*)$ получаем, что $\Phi_n(q)$ делит $q-1$. С другой стороны, из $(\dagger)$ следует, что

$$|\Phi_n(q)| = \prod_{\varepsilon \in \boldsymbol{\mu}'_n} |q - \varepsilon| > q - 1.$$

Следовательно, $\Phi_n(q)$ не может делить $q - 1$. Противоречие. □

Следующий факт является незначительным обобщением теоремы о существования базиса для векторных пространств над полем.

Лемма. *Пусть R – ассоциативное кольцо с делением. Тогда любой конечно порожденный модуль над R является свободным.*

Доказательство. Пусть M – конечно порожденный модуль над R и пусть $\mathbf{x}_1, \ldots, \mathbf{x}_n$ – система порождающих. Мы можем считать, что не все они равны нулю (иначе $M = 0$). Так как R – кольцо с делением, то система из одного ненулевого вектора линейно независима. Выберем в $\mathbf{x}_1, \ldots, \mathbf{x}_n$ максимальную линейно независимую подсистему $\mathbf{x}_{i_1}, \ldots, \mathbf{x}_{i_r}$. Докажем, что $\mathbf{x}_{i_1}, \ldots, \mathbf{x}_{i_r}$ – базис. Действительно, для любого $\mathbf{x}_j$ система $\mathbf{x}_j, \mathbf{x}_{i_1}, \ldots, \mathbf{x}_{i_r}$ линейно зависима по предположению. Значит

$$\lambda_j \mathbf{x}_j + \lambda_{j,i_1} \mathbf{x}_{i_1} + \cdots + \lambda_{j,i_r} \mathbf{x}_{i_r} = 0$$

для некоторых $\lambda_j, \lambda_{j,i_1}, \ldots, \lambda_{j,i_r} \in R$, причем $\lambda_j \neq 0$ (иначе $\mathbf{x}_{i_1}, \ldots, \mathbf{x}_{i_r}$ будут линейно зависимыми). Так как R – кольцо с делением, то мы можем выразить $\mathbf{x}_j$:

$$\mathbf{x}_j = \mu_{j,i_1} \mathbf{x}_{i_1} + \cdots + \mu_{j,i_r} \mathbf{x}_{i_r} = \sum_{k=1}^{r} \mu_{j,i_k} \mathbf{x}_{i_k} \qquad \mu_{j,i_k} \in R.$$

С другой стороны, любой элемент $\mathbf{x} \in M$ можно выразить через $\mathbf{x}_1, \ldots, \mathbf{x}_n$:

$$\mathbf{x} = \sum_{j=1}^{n} \delta_j \mathbf{x}_j.$$

Подставляя, получим

$$\mathbf{x} = \sum_{j=1}^{n} \delta_j \left(\sum_{k=1}^{r} \mu_{j,i_k} \mathbf{x}_{i_k} \right) = \sum_{k=1}^{r} \left(\sum_{j=1}^{n} \delta_j \mu_{j,i_k} \right) \mathbf{x}_{i_k}.$$

Значит, $\mathbf{x}_{i_1}, \ldots, \mathbf{x}_{i_r}$ – базис. □

Следствие. *Пусть R – конечное ассоциативное кольцо с делением и пусть M (свободный) конечно порожденный R-модуль ранга r. Тогда число элементов в M вычисляется по формуле*

$$|M| = |R|^r.$$

Задачи

12.1. Пусть A – двумерная ассоциативная алгебра с единицей. Докажите, что коммутативна.

12.2. Какие условия нужно наложить на сттруктурные констант алгебры для того, чтобы она была ассоциативна?

12.3. Пусть A – конечномерная ассоциативная алгебра. Докажите, что если в A нет делителей нуля, то A – алгебра с единицей. *Указание.* Во-первых покажите, что для любых $\mathbf{b} \in A$, $\mathbf{a} \in A \setminus \{0\}$ уравнения $\mathbf{b} = \mathbf{x} \cdot \mathbf{a}$ и $\mathbf{b} = \mathbf{a} \cdot \mathbf{x}$ имеют единственные решения. Поэтому для $\mathbf{a} \in A \setminus \{0\}$ существует $\mathbf{1} \in A$ такой, что $\mathbf{a}\,\mathbf{1} = \mathbf{a}$. Отсюда $\mathbf{b} \cdot \mathbf{1} = \mathbf{x} \cdot \mathbf{a} \cdot \mathbf{1} = \mathbf{x} \cdot \mathbf{a} = \mathbf{b}$, т.е. $\mathbf{1}$ – правая единица. Покажите аналогично, что существует левая единица $\mathbf{1}'$ и тогда $\mathbf{1}' = \mathbf{1}$.

12.4. Пусть A – ассоциативная алгебра размерности n с единицей. Пусть $\mathbf{a} \in A$ – нильпотентный элемент, т.е. $\mathbf{a}^m = 0$ для некоторого $m \in \mathbb{N}$. Докажите, что тогда $\mathbf{a}^n = 0$.

12.5. Докажите, что групповая алгебра обязательно имеет делители нуля.

12.6. Пусть A – одна из абелевых групп $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Найдите все идеалы в групповой алгебре $\mathbb{C}[A]$.

12.7. Является ли алгебра матриц $\mathrm{Mat}_n(\Bbbk)$ групповой алгеброй для некоторой группы?

12.8. Докажите, что алгебра $\Bbbk[[t]]$ формальных степенных рядов не содержит делителей нуля.

12.9. Докажите, что в алгебре $\Bbbk[[t]]$ формальных степенных рядов элемент $f = a_0 + a_1 t + a_2 t^2 + \cdots$ обратим тогда и только тогда, когда $a_0 \neq 0$. Выведите отсюда, что поле частных алгебры $\Bbbk[[t]]$ – это поле формальных рядов Лорана

$$\Bbbk((t)) := \left\{ f = \sum_{i=N}^{+\infty} a_i t^i \;\middle|\; a_i \in \Bbbk, \quad \text{константа } N \text{ не фиксируется} \right\}.$$

12.10. Опишите центр групповой алгебры конечной группы.

12.11. Пусть A – конечномерная ассоциативная алгебра с делением и пусть A' – ее подалгебра Докажите, что размерность $\dim(A')$ делит $\dim(A)$.

Лекция 13

Алгебра кватернионов

13.1 Определение алгебры 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 построена Р. 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

$$\mathbb{H} \longrightarrow \mathbb{H}, \quad \mathbf{x} = \alpha\,\mathbf{1} + \beta\,\mathbf{i} + \gamma\,\mathbf{j} + \delta\,\mathbf{k} \longmapsto \overline{\mathbf{x}} := \alpha\,\mathbf{1} - \beta\,\mathbf{i} - \gamma\,\mathbf{j} - \delta\,\mathbf{k},$$

которое мы назовем *сопряжением*. Несложно проверить, что

$$\overline{\lambda\mathbf{x}} = \lambda\overline{\mathbf{x}}, \quad \overline{\mathbf{x}+\mathbf{y}} = \overline{\mathbf{x}} + \overline{\mathbf{y}}, \quad \overline{\mathbf{x}\cdot\mathbf{y}} = \overline{\mathbf{y}}\cdot\overline{\mathbf{x}}, \quad \forall \mathbf{x},\, \mathbf{y} \in \mathbb{H},\ \forall \lambda \in \mathbb{R}.$$

Действительно, эти свойства достаточно проверить на базисных элементах, а последнее – простой перебор возможностей. Таким образом, сопряжение является *антиавтоморфизмом* алгебры. Для кватерниона

$$\mathbf{x} = \alpha\,\mathbf{1} + \beta\,\mathbf{i} + \gamma\,\mathbf{j} + \delta\,\mathbf{k} \in \mathbb{H}$$

определим его *норму*

$$\|\mathbf{x}\| := \mathbf{x}\cdot\overline{\mathbf{x}} = \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

Тогда

$$\|\mathbf{x}\cdot\mathbf{y}\| = \mathbf{x}\cdot\mathbf{y}\cdot\overline{\mathbf{x}\cdot\mathbf{y}} = \mathbf{x}\cdot\mathbf{y}\cdot\overline{\mathbf{y}}\cdot\overline{\mathbf{x}} = \mathbf{x}\cdot\|\mathbf{y}\|\cdot\overline{\mathbf{x}} = \|\mathbf{x}\|\cdot\|\mathbf{y}\|.$$

Теперь несложно предъявить обратный элемент: если $\mathbf{x} \neq 0$, то

$$\mathbf{x}^{-1} = \frac{1}{\|\mathbf{x}\|}\bar{\mathbf{x}}.$$

□

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 $\mathbf{x} \in \mathbb{H}$ однозначно записывается в виде

$$\mathbf{x} = \mathbf{z}_1 + \mathbf{z}_2\,\mathbf{j}, \qquad \mathbf{z}_1,\, \mathbf{z}_2 \in \mathbb{C}.$$

Однако, $\mathbb{H}$ не является $\mathbb{C}$-алгеброй:

$$\mathbf{j}\cdot\mathbf{z} = \bar{\mathbf{z}}\cdot\mathbf{j} \qquad \forall \mathbf{z} \in \langle \mathbf{1},\, \mathbf{i}\rangle = \mathbb{C}.$$

13.2 Алгебры с делением над $\mathbb{R}$. Теорема Фробениуса

Теорема (теорема Фробениуса)**.** *Пусть A – конечномерная ассоциативная алгебра с делением над полем $\mathbb{R}$. Тогда $A \simeq \mathbb{R}$, $\mathbb{C}$ или $\mathbb{H}$.*

Лемма (коммутативный случай)**.** *Пусть A – конечномерная ассоциативная коммутативная алгебра с делением над полем $\mathbb{R}$. Тогда $A \simeq \mathbb{R}$ или $\mathbb{C}$.*

Доказательство. Отождествим $\mathbb{R}$ с подалгеброй A при помощи отображения $\lambda \mapsto \lambda\,\mathbf{1}$. Пусть $A \neq \mathbb{R}$ и пусть $\mathbf{a} \in A \setminus \mathbb{R}$. Пусть A_1 – подалгебра, порожденная $\mathbf{a}$ и $\mathbf{1}$. Она коммутативна и без делителей нуля. Следовательно, A_1 – поле. Минимальный многочлен $\mu(t)$ элемента $\mathbf{a}$ неприводим над $\mathbb{R}$, т.е. $A_1/\mathbb{R}$ – квадратичное расширение. Тогда $A_1 \simeq \mathbb{C}$. Так как A коммутативна, то A является алгеброй над $A_1 \simeq \mathbb{C}$. Поскольку поле $\mathbb{C}$ алгебраически замкнуто, то $A \simeq \mathbb{C}$. □

Доказательство теоремы. Как и выше, отождествим $\mathbb{R}$ с подалгеброй A при помощи отображения $\lambda \mapsto \lambda\,\mathbf{1}$. Пусть $Z \subset A$ – *центр алгебры*, т.е. множество элементов, коммутирующих со всеми элементами A. 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, A является алгеброй над $Z \simeq \mathbb{C}$ и поле $\mathbb{C}$ алгебраически замкнуто. Поэтому $A \simeq \mathbb{C}$.

Далее мы всюду предполагаем, что $Z = \mathbb{R}$ и $A \neq Z$. Возьмем любой элемент $\mathbf{a} \in A \setminus Z$. Пусть A_1 – подалгебра, порожденная $\mathbf{a}$ и Z. Она коммутативна и без делителей нуля. Следовательно, $A_1 \simeq \mathbb{C}$ и поэтому существует элемент $\mathbf{i} \in A_1$ такой, что $\mathbf{i}^2 = -\,\mathbf{1}$. Рассмотрим отображение

$$\varphi : A \longrightarrow A, \quad \mathbf{x} \longmapsto \mathbf{i}\cdot\mathbf{x}\cdot\mathbf{i}^{-1} = -\,\mathbf{i}\cdot\mathbf{x}\cdot\mathbf{i}\,.$$

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 A, как векторное пространство над $\mathbb{R}$, разлагается в прямую сумму $A = A_+ \oplus A_-$ собственных подпространств собственными значениями ± 1. Элементы A_+ коммутируют с $\mathbf{i}$, а, следовательно, и со всей подалгеброй $A_1 \simeq \mathbb{C}$. Следовательно, A_+ – ассоциативная алгебра с делением над $\mathbb{C}$ и поэтому $A_+ = A_1$.

Элементы A_- антикоммутируют с $\mathbf{i}$:

$$\mathbf{i}\cdot\mathbf{b} = -\mathbf{b}\cdot\mathbf{i} \quad \forall \mathbf{b} \in A_-.$$

Возьмем любой элемент $0 \neq \mathbf{b} \in A_-$ и рассмотрим оператор

$$\psi : A \longrightarrow A, \quad \mathbf{x} \longmapsto \mathbf{b}\cdot\mathbf{x}.$$

Так как A – алгебра с делением, то ψ невырожден. Более того, ψ переставляет подпространства A_+ и A_-. Действительно,

$$\mathbf{x} \in A_+ \iff \mathbf{x}\cdot\mathbf{i} = \mathbf{i}\cdot\mathbf{x} \iff (\mathbf{b}\cdot\mathbf{x})\cdot\mathbf{i} = \mathbf{b}\cdot\mathbf{i}\cdot\mathbf{x} = -\,\mathbf{i}\cdot(\mathbf{b}\cdot\mathbf{x}) \iff \mathbf{b}\cdot\mathbf{x} \in A_-.$$

и аналогично

$$\mathbf{x} \in A_- \qquad \Longleftrightarrow \qquad \mathbf{b}\cdot\mathbf{x} \in A_+.$$

В частности,

$$\dim A_- = \dim A_+ = 2, \qquad \dim A = 4.$$

Далее,

$$\varphi(\mathbf{b}^2) = \varphi(\mathbf{b})^2 = (-\mathbf{b})^2 = \mathbf{b}^2.$$

Следовательно, $\mathbf{b}^2 \in A_+$. Таким образом, $\mathbf{b}^2$ коммутирует с элементами $\mathbf{1}$, $\mathbf{i}$, $\mathbf{b}$ и $\mathbf{b}\cdot\mathbf{i}$, составляющих базис A. Поэтому $c := \mathbf{b}^2 \in Z = \mathbb{R}$. 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

$$\mathbf{j} := \frac{\mathbf{b}}{\sqrt{-c}}, \qquad \mathbf{k} := \mathbf{i}\cdot\mathbf{j}\,.$$

Несложно проверить, что для базисных элементов $\mathbf{1}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ в алгебре A выполняются те же соотношения, что и для соответствующих базисных элементов в $\mathbb{H}$. □

13.3 Свойства алгебры кватернионов

Отождествим подалгебру, порожденную элементами $\mathbf{1}$ и $\mathbf{i}$ с полем комплексных чисел $\mathbb{C}$. Тогда $\mathbb{H}$ является $\mathbb{C}$-векторным пространством с базисом $\mathbf{1}$, $\mathbf{j}$. Рассмотрим отображение

$$\delta : \mathbb{H} \longrightarrow \mathrm{Mat}_2(\mathbb{C}), \qquad \mathbf{x} = \mathbf{z}_1 + \mathbf{z}_2\cdot\mathbf{j} \longmapsto \begin{pmatrix} \mathbf{z}_1 & \mathbf{z}_2 \\ -\bar{\mathbf{z}}_2 & \bar{\mathbf{z}}_1 \end{pmatrix}$$

Очевидно, что оно инъективно и является $\mathbb{R}$-линейным отображением векторных пространств. Оно также сохраняет произведение:

$$\begin{aligned}\delta\big((\mathbf{z}_1 + \mathbf{z}_2\,\mathbf{j})\cdot(\mathbf{z}_1' + \mathbf{z}_2'\,\mathbf{j})\big) &= \delta(\mathbf{z}_1\cdot\mathbf{z}_1' + \mathbf{z}_1\cdot\mathbf{z}_2'\cdot\mathbf{j} + \mathbf{z}_2\cdot\mathbf{j}\cdot\mathbf{z}_1' + \mathbf{z}_2\cdot\mathbf{j}\cdot\mathbf{z}_2'\cdot\mathbf{j}) = \\ &= \delta\left(\mathbf{z}_1\cdot\mathbf{z}_1' + \mathbf{z}_1\cdot\mathbf{z}_2'\cdot\mathbf{j} + \mathbf{z}_2\cdot\overline{\mathbf{z}_1'}\cdot\mathbf{j} - \mathbf{z}_2\cdot\overline{\mathbf{z}_2'}\right) = \delta\big(\mathbf{z}_1 + \mathbf{z}_2\,\mathbf{j}\,\big)\cdot\delta\big(\mathbf{z}_1' + \mathbf{z}_2'\,\mathbf{j}\,\big)\end{aligned}$$

Таким образом, δ является инъективным гомоморфизмом $\mathbb{R}$-алгебр. Образ $\delta(\mathbb{H})$ порождается, как векторное пространство над $\mathbb{R}$, матрицами

$$\delta(\mathbf{1}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \delta(\mathbf{i}) = \begin{pmatrix} \boldsymbol{i} & 0 \\ 0 & -\boldsymbol{i} \end{pmatrix}, \quad \delta(\mathbf{j}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \delta(\mathbf{k}) = \begin{pmatrix} 0 & \boldsymbol{i} \\ \boldsymbol{i} & 0 \end{pmatrix}.$$

Легко проверить, что

$$\|\mathbf{x}\| = \det\delta(\mathbf{x}).$$

Предложение. (i) *Соотношение*

$$(\mathbf{x},\,\mathbf{y}) = \frac{1}{2}(\mathbf{x}\bar{\mathbf{y}} + \mathbf{y}\bar{\mathbf{x}}) = \frac{1}{2}(\mathbf{x}\bar{\mathbf{y}} + \overline{\mathbf{x}\bar{\mathbf{y}}}) \in \mathbb{R}.$$

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.

(ii) *Аналогично,*

$$\langle \mathbf{x},\,\mathbf{y}\rangle = \frac{1}{2}(\mathbf{x}\mathbf{y} + \bar{\mathbf{y}}\bar{\mathbf{x}}) = \frac{1}{2}(\mathbf{x}\mathbf{y} + \overline{\mathbf{x}\mathbf{y}}) \in \mathbb{R}$$

– симметрическая $\mathbb{R}$-билинейная форма сигнатуры $(1,3)$.

(iii) *Соотношение*

$$\mathbf{x}\times\mathbf{y} = -\frac{1}{2}(\mathbf{x}\bar{\mathbf{y}} - \mathbf{y}\bar{\mathbf{x}}).$$

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

$$\mathbf{x}\times\mathbf{y} = \frac{1}{2}(\mathbf{x}\mathbf{y} - \mathbf{y}\mathbf{x}), \qquad \mathbf{x}\times\mathbf{y} = -\mathbf{y}\times\mathbf{x}$$

и совпадает со стандартным векторным умножением на $\mathbb{R}^3$.

Доказательство. Все утверждения доказываются непосредственной проверкой. Проверим, например, (ii). Для этого запишем элементы $\mathbf{x},\,\mathbf{y}\in\mathbb{H}$ в виде $\mathbf{x} = \mathbf{x}_0 + \mathbf{x}'$ и $\mathbf{y} = \mathbf{y}_0 + \mathbf{y}'$, где $\mathbf{x}_0,\,\mathbf{y}_0 \in \langle\mathbf{1}\rangle$, а $\mathbf{x}',\,\mathbf{y}'\in\mathbb{E}$. Тогда

$$\begin{aligned}2\langle \mathbf{x},\,\mathbf{y}\rangle = (\mathbf{x}_0+\mathbf{x}')(\mathbf{y}_0+\mathbf{y}') + (\mathbf{y}_0-\mathbf{y}')(\mathbf{x}_0-\mathbf{x}') = \mathbf{x}_0\mathbf{y}_0 + \mathbf{x}_0\mathbf{y}' + \\ + \mathbf{y}_0\mathbf{x}' + \mathbf{x}'\mathbf{y}' + \mathbf{x}_0\mathbf{y}_0 - \mathbf{x}_0\mathbf{y}' - \mathbf{y}_0\mathbf{x}' + \mathbf{y}'\mathbf{x}' = 2\mathbf{x}_0\mathbf{y}_0 + \mathbf{x}'\mathbf{y}' + \mathbf{y}'\mathbf{x}'.\end{aligned}$$

(Мы воспользовались тем, что $\mathbf{x}_0$ и $\mathbf{y}_0$ коммутируют со всеми элементами $\mathbb{H}$.) Запишем далее

$$\mathbf{x}' = x_1\,\mathbf{i} + x_2\,\mathbf{j} + x_3\,\mathbf{k}, \qquad \mathbf{y}' = y_1\,\mathbf{i} + y_2\,\mathbf{j} + y_3\,\mathbf{k}, \qquad x_i,\,y_i\in\mathbb{R}.$$

Тогда

$$\mathbf{x}'\mathbf{y}' + \mathbf{y}'\mathbf{x}' = -2x_1y_1 - 2x_2y_2 - 2x_3y_3.$$

Следовательно,

$$\langle \mathbf{x},\,\mathbf{y}\rangle = \mathbf{x}_0\mathbf{y}_0 - x_1y_1 - x_2y_2 - x_3y_3.$$

Отсюда немедленно получаем (ii). □

13.4 Гомоморфизм $\mathrm{SU}_2 \to \mathrm{SO}_3$

Рассмотрим подгруппу $U \subset \mathbb{H}^*$ мультипликативной группы алгебры кватернионов, состоящую из кватернионов нормы 1:

$$U := \{\mathbf{u} \in \mathbb{H} \mid \|\mathbf{u}\| = 1\}.$$

Лемма. *Построенный выше инъективный гомоморфизм $\mathbb{R}$-алгебр*

$$\delta : \mathbb{H} \longrightarrow \mathrm{Mat}_2(\mathbb{C}), \qquad \mathbf{x} = \mathbf{z}_1 + \mathbf{z}_2\,\mathbf{j} \longmapsto \begin{pmatrix} \mathbf{z}_1 & \mathbf{z}_2 \\ -\bar{\mathbf{z}}_2 & \bar{\mathbf{z}}_1 \end{pmatrix}$$

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

$$C = \begin{pmatrix} \mathbf{z}_1 & \mathbf{z}_2 \\ -\bar{\mathbf{z}}_2 & \bar{\mathbf{z}}_1 \end{pmatrix}, \qquad |\mathbf{z}_1|^2 + |\mathbf{z}_2|^2 = 1.$$

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 $\mathbf{u} \in U$ рассмотрим $\mathbb{R}$-линейный оператор

$$\varphi_{\mathbf{u}} : \mathbb{H} \longrightarrow \mathbb{H}, \qquad \mathbf{x} \longmapsto \mathbf{u}\mathbf{x}\mathbf{u}^{-1} = \mathbf{u}\mathbf{x}\bar{\mathbf{u}}.$$

Лемма. *Оператор $\varphi_{\mathbf{u}}$ является ортогональным относительно скалярного произведения*

$$(\mathbf{x}, \mathbf{y}) = \frac{1}{2}(\mathbf{x}\bar{\mathbf{y}} + \mathbf{y}\bar{\mathbf{x}}).$$

Трехмерное подпространство

$$\mathbb{E} := \langle \mathbf{i}, \mathbf{j}, \mathbf{k} \rangle = \langle \mathbf{1} \rangle^{\perp}$$

чисто мнимых кватернионов является инвариантным для $\varphi_{\mathbf{u}}$.

Доказательство. Проверим, что $\varphi_{\mathbf{u}}$ сохраняет билинейную форму $(\ ,\ )$:

$$(\varphi_{\mathbf{u}}(\mathbf{x}), \varphi_{\mathbf{u}}(\mathbf{y})) = \frac{1}{2}(\mathbf{u}\mathbf{x}\bar{\mathbf{u}}\overline{\mathbf{u}\mathbf{y}\bar{\mathbf{u}}} + \mathbf{u}\mathbf{y}\bar{\mathbf{u}}\overline{\mathbf{u}\mathbf{x}\bar{\mathbf{u}}}) =$$

$$= \frac{1}{2}(\mathbf{u}\mathbf{x}\bar{\mathbf{y}}\bar{\mathbf{u}} + \mathbf{u}\mathbf{y}\bar{\mathbf{x}}\bar{\mathbf{u}}) = \frac{1}{2}\mathbf{u}(\mathbf{x}\bar{\mathbf{y}} + \mathbf{y}\bar{\mathbf{x}})\bar{\mathbf{u}} = \frac{1}{2}(\mathbf{x}\bar{\mathbf{y}} + \mathbf{y}\bar{\mathbf{x}})\mathbf{u}\bar{\mathbf{u}} = (\mathbf{x}, \mathbf{y}).$$

Так как $\varphi_{\mathbf{u}}(\mathbf{1}) = \mathbf{1}$, то $\mathbb{E} = \langle \mathbf{1} \rangle^{\perp}$ является инвариантным. □

Таким образом, каждому кватерниону $\mathbf{u} \in U$ мы можем сопоставить ортогональный оператор $\varphi_{\mathbf{u}}|_{\mathbb{E}}$ в трехмерном евклидовом пространстве $\mathbb{E}$. Так как $\varphi_{\mathbf{u}} \circ \varphi_{\mathbf{v}} = \varphi_{\mathbf{uv}}$, то это соответствие

$$\Psi : U \longrightarrow \mathrm{O}(\mathbb{E}) = \mathrm{O}_3(\mathbb{R}), \qquad \mathbf{u} \longmapsto \varphi_{\mathbf{u}}|_{\mathbb{E}}$$

является гомоморфизмом групп.

Теорема. *Построенный выше гомоморфизм* Ψ *индуцирует сюръективный гомоморфизм*

$$\mathrm{SU}_2 \longrightarrow \mathrm{SO}_3(\mathbb{R})$$

с ядром $\{\pm E\}$.

Доказательство. Отображение

$$\Psi : U \longrightarrow \mathrm{O}_3(\mathbb{R}) \subset \mathrm{Mat}_3(\mathbb{R})$$

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 $\Psi(U) \subset \mathrm{SO}_3(\mathbb{R})$.

Ясно, что ядро гомоморфизма Ψ состоит из кватернионов $\mathbf{u} \in U$ таких, что $\mathbf{ux} = \mathbf{xu}$ для любого $\mathbf{x} \in \mathbb{H}$. Такой кватернион $\mathbf{u}$ должен лежать в пересечении центра алгебры $\mathbb{H}$ с группой U, т.е. $\mathbf{u} \pm \mathbf{1}$. Таким образом,

$$\mathrm{Ker}(\Psi) = \{\pm \mathbf{1}\}.$$

Осталось доказать сюръективность Ψ. Для элемента

$$\mathbf{z} = \mathbf{z}_\theta := \cos(\theta/2) + \mathbf{i}\sin(\theta/2) \in U$$

имеем

$$\begin{aligned}
\varphi_{\mathbf{z}}(\mathbf{i}) &= \mathbf{i} \\
\varphi_{\mathbf{z}}(\mathbf{j}) &= \mathbf{z}\,\mathbf{j}\,\bar{\mathbf{z}} = \mathbf{z}^2\,\mathbf{j} = (\cos\theta)\,\mathbf{j} + (\sin\theta)\,\mathbf{k}, \\
\varphi_{\mathbf{z}}(\mathbf{k}) &= \mathbf{z}\,\mathbf{k}\,\bar{\mathbf{z}} = \mathbf{z}^2\,\mathbf{k} = -(\sin\theta)\,\mathbf{j} + (\cos\theta)\,\mathbf{k}\,.
\end{aligned}$$

Таким образом, $\Psi(U)$ содержит элемент

$$\Psi(\mathbf{z}_\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

– поворот на произвольный угол θ вокруг $\mathbf{i}$. Аналогично, для

$$\mathbf{u} = \mathbf{u}_{\theta'} := \cos(\theta'/2) + \mathbf{j}\sin(\theta'/2) \in U$$

имеем

$$\begin{aligned}
\varphi_{\mathbf{u}}(\mathbf{j}) &= \mathbf{j}, \\
\varphi_{\mathbf{u}}(\mathbf{i}) &= \mathbf{u}\,\mathbf{i}\,\bar{\mathbf{u}} = \mathbf{u}^2\,\mathbf{i} = (\cos\theta')\,\mathbf{i} - (\sin\theta')\,\mathbf{k}, \\
\varphi_{\mathbf{u}}(\mathbf{k}) &= \mathbf{u}\,\mathbf{k}\,\bar{\mathbf{u}} = \mathbf{u}^2\,\mathbf{k} = (\sin\theta')\,\mathbf{i} + (\cos\theta')\,\mathbf{k}\,.
\end{aligned}$$

Таким образом, $\Psi(U)$ содержит элемент

$$\Psi(\mathbf{u}_{\theta'}) = \begin{pmatrix} \cos\theta' & 0 & \sin\theta' \\ 0 & 1 & 0 \\ -\sin\theta' & 0 & \cos\theta' \end{pmatrix}$$

– поворот на произвольный угол $-\theta'$ вокруг $\mathbf{j}$. Рассмотрим любой вектор $\mathbf{v} \in \mathbb{E}$ единичной длины. Поворотом вокруг вокруг $\mathbf{i}$ мы можем $\mathbf{v}$ перевести в вектор плоскости $\langle \mathbf{i}, \mathbf{k} \rangle$:

$$\Psi(\mathbf{z}_\theta)(\mathbf{e}_1) = \mathbf{e}_1' \in \langle \mathbf{i}, \mathbf{k} \rangle.$$

Так как $\|\mathbf{v}\| = 1 = \|\,\mathbf{i}\,\|$, то поворотом вокруг вокруг $\mathbf{j}$ мы можем $\mathbf{v}$ перевести в $\mathbf{i}$. Таким образом, существует элемент $\varphi \in \Psi(U)$, являющийся композицией $\Psi(\mathbf{z}_\theta)$ и $\Psi(\mathbf{u}_{\theta'})$, такой, что $\varphi(\mathbf{v}) = \mathbf{i}$. Тогда произведение $\varphi^{-1}\Psi(\mathbf{z}_\theta)\varphi$ является поворотом вокруг $\varphi^{-1}(\mathbf{i}) = \mathbf{v}$ на угол θ. Таким образом, $\Psi(U)$ содержит все повороты. Следовательно, гомоморфизм Ψ сюръективен. □

Теорема. *Существует сюръективный гомоморфизм*

$$\mathrm{SU}_2 \times \mathrm{SU}_2 \longrightarrow \mathrm{SO}_4(\mathbb{R})$$

с ядром $\{\pm(E, E)\}$.

Доказательство. Как и в доказательстве предыдущей теоремы отождествим SU_2 с группой U кватернионов единичной длины и рассмотрим действие

$$U \times U \curvearrowright \mathbb{H}, \qquad (\mathbf{u}_1, \mathbf{u}_2) * \mathbf{x} = \mathbf{u}_1\mathbf{x}\mathbf{u}_2^{-1}.$$

сопоставляющее паре кватернионов $(\mathbf{u}_1, \mathbf{u}_2)$ линейный оператор $\varphi_{\mathbf{u}_1,\mathbf{u}_2} \in \mathrm{GL}(\mathbb{H})$. Легко видеть, что этот оператор является ортогональным для скалярного произведения $(\mathbf{x}, \mathbf{y})$. Более того, соображения непрерывности позволяют заключить, что его определитель равен 1. Таким образом, $\varphi_{\mathbf{u}_1,\mathbf{u}_2} \in \mathrm{SO}_4(\mathbb{R})$. Получаем гомоморфизм

$$\Phi : U \times U \longrightarrow \mathrm{SO}_4(\mathbb{R}).$$

Его ядро состоит из пар $(\mathbf{u}_1, \mathbf{u}_2)$ таких, что $\mathbf{u}_1\mathbf{x} = \mathbf{x}\mathbf{u}_2$ для любого $\mathbf{x} \in \mathbb{H}$. Полагая здесь $\mathbf{x} = \mathbf{1}$, получим $\mathbf{u}_1 = \mathbf{u}_2$. Тогда равенство $\mathbf{u}_1\mathbf{x} = \mathbf{x}\mathbf{u}_1$ означает, что $\mathbf{u}_1 = \mathbf{u}_2$ лежит в пересечении центра алгебры $\mathbb{H}$ с группой U, т.е. $\mathbf{u}_1 = \mathbf{u}_2 = \pm\mathbf{1}$.

Осталось доказать сюръективность Φ. Согласно предыдущей теореме образ при гомоморфизме Φ подгруппы $U \subset U \times U$, диагонально вложенной в $U \times U$, совпадает с подгруппой $\mathrm{SO}_3(\mathbb{R}) \subset \mathrm{SO}_4(\mathbb{R})$, состоящей из операторов фиксирующих вектор $\mathbf{1}$. Пусть теперь $\varphi \in \mathrm{SO}_4(\mathbb{R})$ – произвольный элемент и пусть $\mathbf{u} := \varphi(\mathbf{1})$. Тогда $\mathbf{u} \in U$. Зададим оператор ψ формулой $\psi(\mathbf{x}) = \mathbf{u}^{-1}\varphi(\mathbf{x})$. Тогда $\psi = \varphi_{\mathbf{u}^{-1},1} \circ \varphi$. Следовательно, $\psi \in \mathrm{SO}_4(\mathbb{R})$. Ясно, что $\psi(\mathbf{1}) = \mathbf{1}$. Значит,$\psi = \varphi_{\mathbf{u}',\mathbf{u}'}$ для некоторого $\mathbf{u}' \in U$. Получаем $\psi(\mathbf{x}) = \mathbf{u}^{-1}\varphi(\mathbf{x}) = \varphi_{\mathbf{u}',\mathbf{u}'}$, $\varphi(\mathbf{x}) = \mathbf{u}\varphi_{\mathbf{u}',\mathbf{u}'}(\mathbf{x}) = \varphi_{\mathbf{u}\mathbf{u}',\mathbf{u}'}(\mathbf{x})$. Таким образом, $\varphi = \varphi_{\mathbf{u}\mathbf{u}',\mathbf{u}'} \in \Phi(U \times U)$. □

Задачи

13.1. Найдите все решения уравнения $\mathbf{x}^2 = -\mathbf{1}$ в алгебре $\mathbb{H}$.

13.2. Является ли алгебра кватернионов $\mathbb{H}$ групповой алгеброй для некоторой группы?

13.3. Докажите, что любая подалгебра в алгебре кватернионов $\mathbb{H}$ коммутативна.

13.4. Пусть $\Bbbk$ – произвольное поле характеристики $\neq 2$. 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

$$\mathbf{i}^2 = \alpha\,\mathbf{1} \quad \mathbf{j}^2 = \beta\,\mathbf{1}, \quad \mathbf{k} = \mathbf{i}\cdot\mathbf{j} = -\mathbf{j}\cdot\mathbf{i}\,.$$

При каком условии на α и β построенная алгебра $\mathbb{H}_{\alpha,\beta}$ будет алгеброй с делением?

13.5. Опишите алгебру $\mathbb{H}_{\alpha,\beta}$ в случае $\operatorname{char}(\Bbbk) = 2$.

13.6. Докажите, что алгебра $\mathbb{H}_{\alpha,\beta}$ является простой.

13.7. Пусть алгебра $\mathbb{H}_{\alpha,\beta}$ не является алгеброй с делением.

(a) Докажите, что если $V \subset \mathbb{H}_{\alpha,\beta}$ векторное подпространство такое, что $\|\mathbf{x}\| = 0$ для любого $\mathbf{x} \in V$, то $\dim V \leq 2$.

(b) Докажите, что любой нетривиальный левый (правый) идеал в $\mathbb{H}_{\alpha,\beta}$ двумерен, как векторное подпространство над $\Bbbk$.

(c) Докажите, что алгебра $\mathbb{H}_{\alpha,\beta}$ изоморфна матричной алгебре $\mathrm{Mat}_2(\Bbbk)$.

Докажите, что если алгебра $\mathbb{H}_{\alpha,\beta}$ является

13.8. Пусть A – конечномерная (необязательно ассоциативная) алгебра с делением над $\mathbb{R}$. Докажите, что размерность A четна.

13.9. Пусть $a \in \mathrm{SU}_2$ – элемент конечного четного порядка n. Докажите, что его образ при гомоморфизме $\mathrm{SU}_2 \to \mathrm{SO}_3(\mathbb{R})$ имеет порядок $n/2$.

13.10. Пусть $G \subset \mathrm{SO}_3(\mathbb{R})$ – конечная группа четного порядка n. Докажите, что ее прообраз при гомоморфизме $\mathrm{SU}_2 \to \mathrm{SO}_3(\mathbb{R})$ является подгруппой $\tilde{G} \subset \mathrm{SU}_2$ такой, что $\tilde{G}/\{\pm 1\} \simeq G$, но $\tilde{G} \not\simeq G \times \{\pm 1\}$.

Лекция 14

Сепарабельные расширения полей

14.1 Сепарабельные расширения

Определение. Неприводимый многочлен $f \in \Bbbk[t]$ называется *сепарабельным* над $\Bbbk$, если $f' \neq 0$. Любой многочлен $f \in \Bbbk[t]$ называется сепарабельным, если таковыми являются все его неприводимые множители. Пусть $\mathbb{K}/\Bbbk$ – расширение полей. Алгебраический элемент $\theta \in \mathbb{K}$ называется сепарабельным над $\Bbbk$, если таковым является его минимальный многочлен $\mu(t)$. Расширение полей $\mathbb{K}/\Bbbk$ называется сепарабельным, если оно алгебраично и все элементы $\theta \in \mathbb{K}$ сепарабельны над $\Bbbk$.

Отметим, что для приводимого многочлена $f \in \Bbbk[t]$ сепарабельность не эквивалентна тому, что $f' \neq 0$. Действительно, если f_1 – неприводимый сепарабельный многочлен над полем характеристики $p > 0$, то по нашему определению многочлен $f = f_1^p$ является сепарабельным, однако $f' = pf^{p-1}f' = 0$. Наоборот, если f_1 и f_2 – неприводимые многочлены такие, что f_1 сепарабелен, а f_2 несепарабелен, то и $f = f_1 f_2$ не является сепарабельным. Однако, $f' = f_1' f_2 + f_1 f_2' = f_1' f_2 \neq 0$.

Сепарабельные расширения важны, поскольку они обладают следующим свойством:

Предложение. *Если неприводимый многочлен $f \in \Bbbk[t]$ сепарабелен, то он не имеет кратных корней в любом расширении.*

Доказательство. Для того чтобы f обладал кратными корнями в $\mathbb{K} \supset \Bbbk$ необходимо, чтобы наибольший общий делитель НОД (f, f') многочленов f и f' был отличен от константы. С другой стороны, НОД (f, f') вычисляется при помощи алгоритма Евклида и поэтому НОД (f, f') – элемент $\Bbbk[t]$. Если многочлен f неприводим, то ни с каким многочленом меньшей степени: f не может иметь непостоянных общих множителей, следовательно, должно иметь место равенство $f' = 0$. □

Следствие. *Пусть $\mathbb{L}/\Bbbk$ и $\mathbb{K}/\mathbb{L}$ – алгебраические расширения полей. Если элемент $\theta \in \mathbb{K}$ сепарабелен над $\Bbbk$, то он сепарабелен над $\mathbb{L}$.*

Доказательство. Пусть $\mu^{\Bbbk}(t)$ и $\mu^{\mathbb{L}}(t)$ – минимальные многочлены элемента θ над $\Bbbk$ и $\mathbb{L}$, соответственно. Так как $\mu^{\Bbbk}(\theta) = 0$, то $\mu^{\mathbb{L}}(t)$ делит $\mu^{\Bbbk}(t)$. □

Предложение. *Над полем характеристики 0 любой многочлен является сепарабельным. Над полем характеристики $p > 0$ неприводимый многочлен f не является сепарабельным тогда и только тогда, когда $f(t) = g(t^p)$ для некоторого многочлена g.*

Доказательство. Пусть $f \in \Bbbk[t]$ – неприводимый несепарабельный многочлен. Тогда $f' = 0$. Запишем

$$\begin{aligned} f &= a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n, \\ f' &= a_1 + 2a_2 t + \cdots + n a_n t^{n-1}. \end{aligned}$$

Откуда получаем $k a_k = 0$ для всех $k > 0$. В случае характеристики нуль отсюда следует, что $a_k = 0$ для всех $k = 1, \ldots, n$. Следовательно, $f(t) = a_0$ – константа.

В случае же характеристики $p > 0$ для каждого $k = 1, \ldots, n$ мы имеем одно из двух:

$$a_k = 0 \quad \text{или} \quad k \equiv 0 \mod p.$$

Таким образом, чтобы многочлен f обладал кратными корнями, все его слагаемые должны обращаться в нуль, за исключением тех слагаемых, для которых $k \equiv 0 \mod p$, т. е. f должен иметь вид $f = a_0 + a_p t^p + a_{2p} t^{2p} + \ldots$. □

Пример. Пусть поле характеристики $p > 0$ и пусть $a \in \Bbbk$. Тогда любой неприводимый множитель f степени $l > 1$ многочлена $t^{p^e} - a$ не является сепарабельным. Действительно, пусть $\mathbb{K} \supset \Bbbk$ – поле разложения для $t^{p^e} - a$ и пусть $\theta \in \mathbb{K}$ – любой корень f. Тогда $\theta^{p^e} = a$ и поэтому $t^{p^e} - a = (t - \theta)^{p^e}$. Таким образом, f имеет вид $f = (t - \theta)^{p^l}$ и поэтому не является сепарабельным.

Определение. Пусть $\Bbbk$ – поле характеристики $p > 0$ и пусть $\mathbb{K}/\Bbbk$– любое расширение. Элемент $\theta \in \mathbb{K}$ называется *чисто несепарабельным* над $\Bbbk$, если $\theta^{p^e} \in \Bbbk$ для некоторого e. Расширение $\mathbb{K}/\Bbbk$ называется чисто несепарабельным, если все элементы $\theta \in \mathbb{K}$ чисто несепарабельны над $\Bbbk$.

Предложение. *Пусть $\Bbbk$ – поле характеристики $p > 0$ и пусть $\mathbb{K}/\Bbbk$ – любое расширение. Элемент $\theta \in \mathbb{K}$ является одновременно сепарабельным и чисто несепарабельным тогда и только тогда, когда $\theta \in \Bbbk$.*

Доказательство. Действительно, θ является корнем многочлена $t^{p^e} - a$ для некоторых $a \in \Bbbk$ и $e \in \mathbb{N}$. Поэтому минимальный многочлен $\mu(t)$ элемента θ делит $t^{p^e} - a$. Согласно последнему примеру многочлен $\mu(t)$ должен быть линейным. □

Теорема. *Пусть $\mathbb{K}/\Bbbk$ – алгебраическое расширение полей и пусть $\mathbb{K}^{\mathrm{sep}} \subset \mathbb{K}$ – подмножество всех сепарабельных над $\Bbbk$ элементов. Тогда*

(i) *$\mathbb{K}^{\mathrm{sep}}$ – поле;*

(ii) *расширение $\mathbb{K}/\mathbb{K}^{\mathrm{sep}}$ чисто несепарабельно.*

Определение. Поле $\mathbb{K}^{\mathrm{sep}}$, построенное в теореме называется *сепарабельным замыканием* поля $\Bbbk$ в $\mathbb{K}$.

Доказательство. Сначала мы докажем утверждение в случае, когда расширение $\mathbb{K}/\Bbbk$ конечно.

Шаг 1. Для $e \in \mathbb{N}$ обозначим

$$\Bbbk\mathbb{K}^{p^e} := \left\{ \sum \alpha_i \beta_i^{p^e} \mid \alpha_i \in \Bbbk, \quad \beta_i \in \mathbb{K} \right\}.$$

Утверждается, что $\Bbbk\mathbb{K}^{p^e}$ – поле. Действительно, очевидно, что $\Bbbk\mathbb{K}^{p^e}$ является конечномерной $\Bbbk$-подалгеброй в $\mathbb{K}$. Так как она не имеет делителей нуля, то она является полем.

Шаг 2. Согласно шагу 1 существует цепочка вложенных полей

$$\Bbbk\mathbb{K} = \mathbb{K} \supset \Bbbk\mathbb{K}^p \supset \Bbbk\mathbb{K}^{p^2} \supset \cdots \supset \Bbbk\mathbb{K}^{p^l} \supset \cdots .$$

Рассматривая эти поля как векторные пространства над $\Bbbk$, мы видим, что цепочка стабилизируется: существует $e \in \mathbb{N}$ такое, что $\Bbbk\mathbb{K}^{p^l} = \Bbbk\mathbb{K}^{p^e}$ для всех $l \geq e$. Положим

$$\mathbb{L} := \Bbbk\mathbb{K}^{p^e} = \bigcap_{l=0}^{e} \Bbbk\mathbb{K}^{p^l} = \bigcap_{l=0}^{\infty} \Bbbk\mathbb{K}^{p^l}.$$

Согласно сказанному выше, $\mathbb{L}$ – поле. Мы покажем, что $\mathbb{K}^{\mathrm{sep}} = \mathbb{L}$.

Шаг 3. Возьмем любой элемент $\theta \in \mathbb{K} \setminus \mathbb{L}$. Тогда

$$\theta^{p^e} \in \mathbb{K}^{p^e} \subset \Bbbk\mathbb{K}^{p^e} = \mathbb{L}.$$

Поэтому θ чисто несепарабелен над $\mathbb{L}$ и $\mathbb{K}/\mathbb{L}$ – чисто несепарабельное расширение. Предположим, что θ сепарабелен над $\Bbbk$. Тогда он сепарабелен над $\mathbb{L}$. Следовательно, θ содержится в $\mathbb{L}$. Противоречие.

Таким образом, поле $\mathbb{L}$ содержит все сепарабельные над элементы, т.е. $\mathbb{L} \supset \mathbb{K}^{\mathrm{sep}}$. Остается доказать, что все элементы $\mathbb{L}$ сепарабельны, т.е. $\mathbb{L} \subset \mathbb{K}^{\mathrm{sep}}$

Шаг 4. Мы утверждаем, что $\Bbbk\mathbb{L}^p = \mathbb{L}$. Действительно, включение $\Bbbk\mathbb{L}^p \subset \mathbb{L}$ очевидно. С другой стороны, пусть $\theta \in \mathbb{L}$. Тогда

$$\theta \in \Bbbk\mathbb{K}^{p^e} = \Bbbk\mathbb{K}^{p^{e+1}} = \Bbbk\mathbb{K}^{p^{e+2}} = \cdots$$

и поэтому θ представляется в виде

$$\theta = \sum_i \alpha_i \beta_i^{p^{e+1}} = \sum_i \alpha_i \big(\beta_i^{p^e}\big)^p, \qquad \alpha_i \in \Bbbk, \quad \beta_i \in \mathbb{K}.$$

Здесь $\beta_i^{p^e} \in \Bbbk\mathbb{K}^{p^e} = \mathbb{L}$. Следовательно, $\theta \in \Bbbk\mathbb{L}^p$.

Шаг 5. Для любых линейно независимых над $\Bbbk$ элементов

$$\omega_1, \ldots, \omega_r \in \mathbb{L}$$

элементы

$$\omega_1^p, \ldots, \omega_r^p$$

также линейно независимы над $\Bbbk$. Действительно, мы дополним $\omega_1, \ldots, \omega_r \in \mathbb{L}$ до базиса $\omega_1, \ldots, \omega_n$ пространства $\mathbb{L}$ над $\Bbbk$. Так как $\mathbb{L} = \Bbbk\mathbb{L}^p$, то любой элемент $\theta \in \mathbb{L}$ представляется в виде

$$\theta = \sum_i \alpha_i \beta_i^p,$$

где $\alpha_i \in \Bbbk$, $\beta_i \in \mathbb{L}$. Далее $\beta_i = \sum_{j=1}^n \lambda_{i,j}\omega_j$ где $\in \lambda_{i,j}$. Отсюда получаем

$$\theta = \sum_i \alpha_i \Big(\sum_j \lambda_{i,j}\, \omega_j \Big)^p = \sum_{i,j} \alpha_i \lambda_{i,j}^p\, \omega_j^p$$

Следовательно, $\omega_1^p, \ldots, \omega_n^p$ – также базис $\mathbb{L}$ над $\Bbbk$.

Шаг 6. Предположим, что элемент $\theta \in \mathbb{L}$ не является сепарабельным над $\Bbbk$. Тогда его минимальный многочлен представляется в виде $\mu(t) = g(t^p)$ для некоторого многочлена $g(y)$. Пусть $d := \deg g(y)$. Тогда $\deg \mu(t) = pd > d$ и элементы $1, \theta, \theta^2, \ldots, \theta^{d-1}$ линейно независимы над $\Bbbk$. Согласно предыдущему шагу элементы $1, \theta^p, \theta^{2p}, \ldots, \theta^{(d-1)p}$ также линейно независимы над $\Bbbk$. Это противоречит тому, что $\mu(\theta) = 0$. Противоречие показывает, что $\mathbb{L} \subset \mathbb{K}^{\mathrm{sep}}$ и заканчивает доказательство теоремы в случае, когда расширение $\mathbb{K}/\Bbbk$ конечно.

Шаг 7. Пусть теперь $\mathbb{K}/\Bbbk$ – произвольное (необязательно конечное) алгебраическое расширение. Докажем, что $\mathbb{K}^{\mathrm{sep}}$ – поле. Для этого достаточно доказать, что для любых двух сепарабельных над $\Bbbk$ элементов a, $b \in \mathbb{K}$ имеет место включение $\Bbbk(a, b) \subset \mathbb{K}^{\mathrm{sep}}$. Для этого заметим, что $\Bbbk(a, b)/\Bbbk$ – конечное расширение и, согласно доказанному выше, $\Bbbk(a, b) \subset \Bbbk(a, b)^{\mathrm{sep}} \subset \mathbb{K}^{\mathrm{sep}}$. Это доказывает (i). Для доказательства (ii) возьмем любой элемент $\theta \in \mathbb{K} \setminus \mathbb{K}^{\mathrm{sep}}$. Пусть $\mu(t)$ – его минимальный многочлен над $\Bbbk$. Его можно представить в виде $\mu(t) = f(t^{p^e})$ для некоторого неприводимого над $\Bbbk$ многочлена f. Мы можем считать, что e выбрано максимально возможным и тогда многочлен f сепарабелен над $\Bbbk$. Так как θ^{p^e} – его корень, то $\theta^{p^e} \in \mathbb{K}^{\mathrm{sep}}$. Значит, θ чисто несепарабелен над $\mathbb{K}^{\mathrm{sep}}$. □

14.2 Совершенные поля

Определение. Поле называется *совершенным* если $\operatorname{char} \Bbbk = 0$ или $\operatorname{char} \Bbbk = p > 0$ и $\Bbbk^p = \Bbbk$.

Иначе говоря, поле $\Bbbk$ характеристики $p > 0$ является совершенным тогда и только тогда, когда оно вместе с каждым элементом $a \in \Bbbk$ содержит и корень p-й степени из него: существует $\alpha \in \Bbbk$ такой, что $\alpha^p = a$. Этот корень должен быть единственным (т.е. он – кратный). Действительно, иначе $\alpha^p = a = \beta^p$. Но тогда $0 = \alpha^p - \beta^p = (\alpha - \beta)^p$ и $\alpha = \beta$. Таким образом, в совершенном поле характеристики p уравнение $t^p - a = 0$ имеет единственное решение.

Предложение. *Над совершенным полем $\Bbbk$ любой многочлен является сепарабельным.*

Доказательство. Пусть $f \in \Bbbk[t]$ – неприводимый несепарабельный многочлен. Тогда f может быть записан в виде

$$f(t) = \sum_k a_{pk} t^{pk} = \sum_k \left(\sqrt[p]{a_{pk}}\, t^k\right)^p = \Big(\sum_k \sqrt[p]{a_{pk}}\, t^k\Big)^p.$$

Это противоречит неприводимости f. □

Следствие. *Любое алгебраическое расширение совершенного пол является сепарабельным.*

На самом деле, верно и обратное (см.задачу 14.9).

Замечания. (i) Ясно, что алгебраически замкнутое поле совершенно.

(ii) Поле характеристики $p > 0$ является совершенным тогда и только тогда, когда отображение Фробениуса

$$\phi : \Bbbk \longrightarrow \Bbbk$$

сюръективно. Так как отображение Фробениуса всегда инъективно, то в совершенном поле характеристики $p > 0$ отображение Фробениуса является *автоморфизмом*.

Предложение. *Любое конечное поле совершенно.*

Доказательство. Инъективное отображение $\phi : \Bbbk \to \Bbbk$ конечного множества в себя должно быть сюръективным. □

Пример. Пусть $\Bbbk$ любое поле характеристики $p > 0$ и пусть $\mathbb{K} = \Bbbk(x)$ – поле рациональных дробей над $\Bbbk$. Так как уравнение $t^p - x = 0$ не имеет корней в $\mathbb{K}$, то поле $\mathbb{K}$ не является совершенным.

Предложение. *Пусть $\Bbbk$ – совершенное поле и пусть $\mathbb{K}$ – его алгебраическое расширение. Тогда поле $\mathbb{K}$ также совершенно.*

Доказательство. Сначала предположим, что расширение $\mathbb{K}/\Bbbk$ конечно. Ясно, что мы можем считать, что $\operatorname{char}\Bbbk = p > 0$. Так как $\Bbbk^p = \Bbbk$, то мы имеем включения $\Bbbk \subset \mathbb{K}^p \subset \mathbb{K}$. Рассмотрим $\mathbb{K}$ и $\mathbb{K}^p$ как векторные пространства над $\Bbbk$. Пусть $\theta_1, \dots, \theta_n$ – базис $\mathbb{K}$. Тогда элементы $\theta_1^p, \dots, \theta_n^p$ – линейно независимы в $\mathbb{K}^p$ над $\Bbbk$. Действительно, предположим, что $\sum \lambda_i \theta_i^p$ для некоторых $\lambda_i \in \Bbbk$. Отсюда

$$0 = \sum \lambda_i \theta_i^p = \sum \left(\sqrt[p]{\lambda_i}\theta_i\right)^p = \left(\sum \sqrt[p]{\lambda_i}\theta_i\right)^p.$$

Это дает нам $\sum \sqrt[p]{\lambda_i}\theta_i = 0$, а так как элементы $\theta_1, \dots, \theta_n$ линейно независимы, то $\lambda_i = 0$ для всех i. Поэтому $\dim \mathbb{K}^p = \dim \mathbb{K}$ и, следовательно, $\mathbb{K}^p = \mathbb{K}$.

Пусть теперь расширение $\mathbb{K}/$ не является конечным. Предположим, что уравнение $t^p - a = 0$ не имеет решений для некоторого $a \in \mathbb{K}$. Расширение $\mathbb{K}(a)/\Bbbk$ конечно и по доказанному выше $\sqrt[p]{a} \in \mathbb{K}(a)$. Противоречие. □

14.3 Теорема о примитивном элементе

Теорема. *Пусть $\mathbb{K}/\Bbbk$ – конечное сепарабельное расширение полей. Тогда существует элемент $\theta \in \mathbb{K}$ такой, что $\mathbb{K} = \Bbbk(\theta)$.*

Доказательство. Если поле $\mathbb{K}$ конечно, то его мультипликативная группа – циклическая. В частности, $\mathbb{K}$ порождается одним элементом в этом случае. Далее предположим, что $\mathbb{K}$ бесконечно.

Ясно, что достаточно доказать утверждение в случае, когда $\mathbb{K}$ порождается над $\Bbbk$ двумя элементами, т.е. $\mathbb{K} = \Bbbk(a, b)$ для некоторых a, b. Пусть $\mu_a(t)$ – минимальный многочлен элемента a (над $\Bbbk$), а $\mu_b(t)$ – минимальный многочлен элемента b. Напомним, что минимальные многочлены неприводимы (над $\Bbbk$). Пусть $\bar{\mathbb{K}}$ – алгебраическое замыкание поля $\mathbb{K}$. Тогда $\mu_a(t)$ и $\mu_b(t)$ разлагаются в $\bar{\mathbb{K}}$ на линейные множители:

$$\mu_a(t) = \prod_{i=1}^{n}(t - a_i), \qquad \mu_b(t) = \prod_{j=1}^{m}(t - b_j).$$

Мы считаем, что $a_1 = a$ и $b_1 = b$. Так как элементы a и b сепарабельны над $\Bbbk$, то все корни $a_1, \dots, a_n$ и $b_1, \dots, b_m$ различны. Возьмем элемент $c \in \Bbbk$ такой, что $a_i + cb_j \neq a + cb$ для всех i, j, $j \neq 1$ (это возможно поскольку наше поле бесконечно по предположению). Положим $\theta := a + cb$. Докажем, что $\Bbbk(a, b) = \Bbbk(\theta)$. Действительно, b является общим корнем многочленов

$$\mu_b(t), \qquad g(t) := \mu_a(\theta - ct) \in \Bbbk(\theta)[t].$$

Так как $\theta = a + cb \neq a_i + cb_j$ при $j \neq 1$, то $\theta - cb_j \neq a_i$ и поэтому многочлены μ_b и g не имеют других общих корней в $\bar{\mathbb{K}}$. Значит

$$\text{НОД}\ (\mu_b,\ g) = t - b.$$

Поэтому $b \in \Bbbk(\theta)$. Но тогда $a = \theta - cb \in \Bbbk(\theta)$. Следовательно, $\Bbbk(a, b) = \Bbbk(\theta)$. □

Задачи

14.1. Пусть $\Bbbk$ – любое поле. Докажите, что поле разложения многочлена $t^n - 1$ всегда сепарабельно над $\Bbbk$.

14.2. Пусть $\mathbb{K}/\Bbbk$ – алгебраическое расширение полей. Докажите, что все чисто несепарабельные элементы в $\mathbb{K}$ над $\Bbbk$ образуют подполе. Образуют ли подполе все несепарабельные элементы?

14.3. Пусть $\mathbb{K}/\mathbb{L}$ и $\mathbb{L}/\Bbbk$ – сепарабельные расширения. Докажите, что расширение $\mathbb{K}/\Bbbk$ сепарабельно.

14.4. Пусть $\mathbb{K}/\mathbb{L}$ и $\mathbb{L}/\Bbbk$ – чисто несепарабельные расширения. Докажите, что расширение $\mathbb{K}/\Bbbk$ чисто несепарабельно.

14.5. Пусть $\mathbb{K}/\Bbbk$ – расширение полей характеристики $p > 0$ и пусть $\theta \in \mathbb{K}$ алгебраический над элемент. Докажите, что элемент θ^{p^e} сепарабелен над $\Bbbk$ для некоторого e.

14.6. Пусть $\Bbbk$ – поле характеристики $p > 0$ и пусть $f \in \Bbbk[t]$ – неприводимый многочлен. Докажите, что все корни f имеют одну и ту же кратность p^e для некоторого e.

14.7. Докажите, что если $a \in \Bbbk$, $a \notin \Bbbk^p$, то многочлен $t^{p^e} - a$ неприводим в $\Bbbk[t]$ ($\operatorname{char} \Bbbk = p > 0$).

14.8. Если $\mathbb{K}/\Bbbk$ – конечное чисто несепарабельное расширение поля $\Bbbk$, то степень $\mathbb{K}/\Bbbk$ является степенью числа p, $p = \operatorname{char} \Bbbk$. Докажите.

14.9. Докажите, что если любое алгебраическое расширение поля $\Bbbk$ является сепарабельным, то $\Bbbk$ совершенно.

14.10. Пусть $\Bbbk$ – поле характеристики $p > 0$. Докажите, что следующие условия эквивалентны:

- θ сепарабелен над $\Bbbk$;
- $\Bbbk(\theta) = \Bbbk(\theta^p)$;
- $\Bbbk(\theta)$ – сепарабельное расширение поля $\Bbbk$.

14.11. Пусть $\Bbbk(x_1, x_2)$ – поле рациональных функций над полем $\Bbbk$ характеристики $p > 0$. Докажите, что расширение $\Bbbk(x_1, x_2)/\Bbbk(x_1^p, x_2^p)$ не порождается одним элементом. *Указание.* Расширение $\Bbbk(x_1, x_2)/\Bbbk(x_1^p, x_2^p)$ имеет степень p^2. С другой стороны, если $\Bbbk(x_1, x_2) = \Bbbk(z)$, то $\Bbbk(x_1^p, x_2^p) = \Bbbk(z^p)$.

14.12. Пусть $\mathbb{K} = \Bbbk(\theta)/\Bbbk$ – конечное расширение полей, порожденное одним элементом. Докажите, что существует только конечное число промежуточных полей $\mathbb{K} \supset \mathbb{L} \supset \Bbbk$. *Указание.* Рассмотрите отображение $\mathbb{L} \longmapsto \mu^{\mathbb{L}}(t)$, отображающее промежуточное поле $\mathbb{L}$ в минимальный многочлен θ над $\mathbb{L}$, и докажите, что оно инъективно.

14.13. Является ли любой примитивный элемент расширения конечных полей $\mathbb{F}_{q^e}/\mathbb{F}_q$ образующей мультипликативной группы $\mathbb{F}_{q^e}^*$?

14.14. Пусть p и q – различные простые числа. Найдите примитивный элемент расширения $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ над $\mathbb{Q}$.

Лекция 15

Нормальные расширения

15.1 Продолжение автоморфизмов

Предложение. *Пусть $\mathbb{K}/\Bbbk$ – алгебраическое расширение полей и пусть $\varphi : \mathbb{K} \to \mathbb{K}$ – гомоморфизм алгебр над $\Bbbk$, то φ – автоморфизм.*

Доказательство. Так как $\mathbb{K}$ – поле, то ядро гомоморфизма φ тривиально. Поэтому достаточно проверить, что φ сюръективен. Пусть $\theta \in \mathbb{K} \setminus \Bbbk$ и пусть μ – минимальный многочлен θ. Пусть $\theta_1 = \theta, \ldots, \theta_r$ все корни μ в $\mathbb{K}$. Положим $\mathbb{L} := \Bbbk(\theta_1, \ldots, \theta_r)$. Тогда $\mathbb{L}$ является конечномерным векторным пространством над $\Bbbk$ и $\varphi(\theta_i) = \theta_j$ для некоторого j. Отсюда $\varphi(\mathbb{L}) \subset \mathbb{L}$. Таким образом, $\varphi_{\mathbb{L}}$ является инъективным линейным оператором в конечномерном векторном пространстве $\mathbb{K}$ над $\Bbbk$. Следовательно, он сюръективен. Значит, для любого θ существует θ' такой, что $\varphi(\theta') = \theta$. □

Замечание. В предложении условие "φ – *гомоморфизм над* $\Bbbk$" существенно. Например, отображение Фробениуса является инъективным гомоморфизмом поля в себя, но может не быть сюръективным.

Предложение. *Пусть $\mathbb{L}$ – алгебраически замкнутое поле, пусть $\Bbbk$ – любое поле и пусть $\sigma : \Bbbk \to \mathbb{L}$ – (инъективный) гомоморфизм полей. Тогда для любого алгебраического расширения $\mathbb{K}/\Bbbk$ существует гомоморфизм $\sigma_{\mathbb{K}}$, продолжающий σ, т.е. такой, что $\sigma_{\mathbb{K}}|_{\Bbbk} = \sigma$.*

Доказательство. Воспользуемся леммой Цорна. Пусть S – множество пар $(\mathbb{K}_\alpha, \sigma_\alpha)$, состоящих из промежуточного поля в $\mathbb{K} \supset \mathbb{K}_\alpha \supset \Bbbk$ и гомоморфизма $\sigma_\alpha : \mathbb{K}_\alpha \hookrightarrow \mathbb{L}$ таких, что $\sigma_\alpha|_{\Bbbk} = \sigma$. Введем на S частичный порядок:

$$(\mathbb{K}_\alpha, \sigma_\alpha) \leq (\mathbb{K}_\beta, \sigma_\beta) \quad \text{если} \quad \mathbb{K}_\alpha \subset \mathbb{K}_\beta \quad \text{и} \quad \sigma_\beta|_{\mathbb{K}_\alpha} = \sigma_\alpha.$$

Следует проверить выполнение условий леммы Цорна. Пусть дана цепочка $I \subset S$, множество пар $(\mathbb{K}_\alpha, \sigma_\alpha)$ таких, что

$$(\mathbb{K}_\alpha, \sigma_\alpha) \leq (\mathbb{K}_\beta, \sigma_\beta) \quad \text{или} \quad (\mathbb{K}_\alpha, \sigma_\alpha) \geq (\mathbb{K}_\beta, \sigma_\beta), \qquad \forall (\mathbb{K}_\alpha, \sigma_\alpha), (\mathbb{K}_\beta, \sigma_\beta) \in I.$$

Положим

$$\mathbb{K}^\bullet := \bigcup_{(\mathbb{K}_\alpha, \sigma_\alpha) \in I} \mathbb{K}_\alpha.$$

Тогда можно определить гомоморфизм $\sigma^\bullet : \mathbb{K}^\bullet \hookrightarrow \mathbb{L}$:

$$\sigma^\bullet(a) = \sigma_\alpha(a), \quad \text{если} \quad a \in \mathbb{K}_\alpha.$$

Легко видеть, что $\sigma^\bullet$ корректно определен и является вложением полей.

Таким образом, $\mathbb{K}^\bullet_\alpha \in S$, т.е. условия леммы Цорна выполнены и поэтому существует максимальное промежуточное поле $\Bbbk \subset \mathbb{K}' \subset \mathbb{K}$, на которое гомоморфизм σ продолжается, т.е. имеется гомоморфизм $\sigma' : \mathbb{K}' \to \mathbb{L}$ такой, что $\sigma'|_\Bbbk = \sigma$. Предположим, что $\mathbb{K}' \neq \mathbb{K}$. Возьмем любой элемент $\theta \in \mathbb{K} \setminus \mathbb{K}'$. Обозначим через $\Bbbk_\mathbb{L}$ подполе $\sigma'(\Bbbk) = \sigma(\Bbbk)$ в $\mathbb{L}$. Пусть

$$\mu = t^n + a_{n-1}t^{n-1} + \cdots + a_0$$

– минимальный многочлен θ над $\Bbbk$ и пусть

$$\mu^\sigma = t^n + \sigma(a_{n-1})t^{n-1} + \cdots + \sigma(a_0)$$

– соответствующий ему многочлен над $\Bbbk_\mathbb{L}$. Пусть θ^σ – любой корень μ^σ в $\mathbb{L}$. Так как многочлен μ^σ неприводим в $\Bbbk_\mathbb{L}[t]$, то имеется изоморфизм полей $\Bbbk_\mathbb{L}(\theta^\sigma) \simeq \Bbbk_\mathbb{L}[t]/(\mu^\sigma)$. С другой стороны, $\Bbbk(\theta) \simeq \Bbbk[t]/(\mu)$. Следовательно, $\Bbbk_\mathbb{L}(\theta) \simeq \Bbbk(\theta)$. Таким образом, имеется гомоморфизи полей

$$\Bbbk(\theta) \xrightarrow{\simeq} \Bbbk_\mathbb{L}(\theta) \hookrightarrow \mathbb{L},$$

продолжающий σ', т.е. $(\mathbb{K}', \sigma')$ не является максимальным элементом. Противоречие. □

Из последнего предложение непосредственно получается следующее.

Следствие. *Пусть $\bar{\Bbbk}$ – алгебраическое замыкание поля $\Bbbk$ и пусть $\Bbbk \subset \mathbb{K}_1 \subset \bar{\Bbbk}$ и $\Bbbk \subset \mathbb{K}_2 \subset \bar{\Bbbk}$ – два промежуточных поля. Тогда любой изоморфизм $\mathbb{K}_1 \to \mathbb{K}_2$ над $\Bbbk$ продолжается до автоморфизма поля $\bar{\Bbbk}$.*

Следствие. *Пусть $\bar{\Bbbk}$ – алгебраическое замыкание поля $\Bbbk$ и пусть $\Bbbk \subset \mathbb{K} \subset \bar{\Bbbk}$ – промежуточное поле. Тогда любой автоморфизм $\mathbb{K} \to \mathbb{K}$ над $\Bbbk$ продолжается до автоморфизма поля $\bar{\Bbbk}$.*

15.2 Нормальные расширения полей

Определение. Алгебраическое расширение полей $\mathbb{K}/\Bbbk$ называется *нормальным*, если любой неприводимый над $\Bbbk$ многочлен, который имеет корень в $\mathbb{K}$, полностью разлагается на множители в $\mathbb{K}$.

Предложение. *Поле разложения любого многочлена $f \in \Bbbk[t]$ является нормальным расширением над $\Bbbk$.*

Доказательство. Пусть $\mathbb{K}$ – поле разложения многочлена $f \in \Bbbk[t]$ и пусть $g \in \Bbbk[t]$ – неприводимый многочлен, имеющий корень θ в $\mathbb{K}$. Мы можем считать, что $\mathbb{K}$ содержится в алгебраическом замыкании $\bar{\Bbbk}$ поля $\Bbbk$. Пусть $\theta' \in \bar{\Bbbk}$ – другой корень многочлена g. Мы предположим, что $\theta' \notin \mathbb{K}$. Имеются изоморфизмы полей

$$\Bbbk(\theta') \simeq \Bbbk[t]/(g) \simeq \Bbbk(\theta).$$

Композиция $\Bbbk(\theta') \longrightarrow \Bbbk(\theta)$ продолжается до автоморфизма $\varphi : \bar{\Bbbk} \to \bar{\Bbbk}$. Тогда φ сохраняет множество корней многочлена f, а значит и поле $\mathbb{K}$. Таким образом, $\theta' \in \mathbb{K}$. □

15.3 Автоморфизмы расширений

Пусть $\mathbb{K}/\Bbbk$ – расширение полей. Через $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ мы обозначим подгруппу в $\mathrm{Aut}(\mathbb{K})$, состоящую из тех автоморфизмов, которые тривиальны на $\Bbbk$:

$$\mathrm{Aut}(\mathbb{K}/\Bbbk) := \{g \in \mathrm{Aut}(\mathbb{K}) \mid g(a) = a \quad \forall a \in \Bbbk\}.$$

Элементы группы $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ называются автоморфизмами поля $\mathbb{K}$ над $\Bbbk$.

Теорема. *Пусть $\mathbb{K}/\Bbbk$ – конечное расширение полей. Тогда*

$$|\mathrm{Aut}(\mathbb{K}/\Bbbk)| \leq [\mathbb{K} : \Bbbk]. \qquad (*)$$

Доказательство. Докажем утверждение индукцией по степени расширения. База индукции $[\mathbb{K} : \Bbbk] = 1$ очевидна. Предположим, что утверждение верно для всех расширений степени $< [\mathbb{K} : \Bbbk]$. Возьмем произвольный элемент $\theta \in \mathbb{K} \setminus \Bbbk$. Пусть $\mu(t)$ – его минимальный многочлен и пусть

$$\theta_1 = \theta, \theta_2, \ldots, \theta_r$$

– все корни $\mu(t)$ в $\mathbb{K}$. Напомним, что $[\Bbbk(\theta) : \Bbbk] = \deg(\mu)$. Ясно, что группа $\mathrm{Aut}(\mathbb{K}/\Bbbk(\theta))$ естественно вкладывается в $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ и совпадает в ней со стабилизатором элемента θ. Любой элемент группы $g \in \mathrm{Aut}(\mathbb{K}/\Bbbk)$ многочлен μ переводит в себя. Следовательно, g переставляет корни μ:

$$g(\theta_i) = \theta_j.$$

Следовательно, индекс подгруппы $\mathrm{Aut}(\mathbb{K}/\Bbbk(\theta))$ в группе $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ равен числу элементов орбиты элемента θ. Таким образом,

$$[\mathrm{Aut}(\mathbb{K}/\Bbbk) : \mathrm{Aut}(\mathbb{K}/\Bbbk(\theta))] \leq r \leq \deg(\mu) = [\Bbbk(\theta)) : \Bbbk].$$

С другой стороны, по предположению индукции

$$|\mathrm{Aut}(\mathbb{K}/\Bbbk(\theta)| \leq [\mathbb{K} : \Bbbk(\theta)].$$

Применяя теорему о башне полей, получим

$$|\mathrm{Aut}(\mathbb{K}/\Bbbk)| = |\mathrm{Aut}(\mathbb{K}/\Bbbk(\theta))| \cdot [\mathrm{Aut}(\mathbb{K}/\Bbbk) : \mathrm{Aut}(\mathbb{K}/\Bbbk(\theta))] \leq [\mathbb{K} : \Bbbk(\theta)] \cdot [\Bbbk(\theta) : \Bbbk] = [\mathbb{K} : \Bbbk]. \qquad \square$$

15.4 Расширения Галуа

Определение. Конечное расширение полей $\mathbb{K}/\Bbbk$ называется *расширением Галуа*, если в неравенстве $(*)$ достигается равенство, т.е.

$$|\mathrm{Aut}(\mathbb{K}/\Bbbk)| = [\mathbb{K} : \Bbbk].$$

Пример. Пусть $\mathbb{K}/\Bbbk$ – расширение полей степени 2. Мы считаем, что $\mathrm{char}(\Bbbk) \neq 2$. Возьмем любой элемент $\alpha \in \mathbb{K} \setminus \Bbbk$. Тогда минимальный многочлен элемента α можно записать в виде $\mu_\alpha = t^2 + 2px + q$, $p,\ q \in \Bbbk$. Разность $\theta := \alpha + p$ имеет минимальный многочлен $\mu_\theta = t^2 - d$, где $d = p^2 - q$. Так как $[\mathbb{K} : \Bbbk] = 2$, то $\Bbbk(\theta) = \Bbbk(\alpha) = \mathbb{K}$. Таким образом, любой элемент поля $\mathbb{K}$ может быть записан в виде $\lambda_1 + \lambda_2\theta$, λ_1, $\lambda_2 \in \Bbbk$. Отображение

$$\sigma : \lambda_1 + \lambda_2\theta \longmapsto \lambda_1 - \lambda_2\theta$$

является автоморфизмом $\mathbb{K}$ над $\Bbbk$. По теореме $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ – группа порядка 2, порожденная элементом σ. Таким образом, $\mathbb{K}/\Bbbk$ – расширение Галуа. Отметим, что утверждение перестает быть верным, если $\mathrm{char}(\Bbbk) = 2$.

Пример. Пусть расширение $\mathbb{K}/\Bbbk$ чисто несепарабельно. Тогда любой элемент $\theta \in \mathbb{K}\setminus\Bbbk$ является (единственным!) корнем многочлена $t^{p^e} - a$ для некоторых $a \in \Bbbk$ и $e \in \mathbb{N}$. Любой автоморфизм $g \in \mathrm{Aut}(\mathbb{K}/\Bbbk)$ переставляет корни многочлена. Значит он действует тривиально. Таким образом, $\mathrm{Aut}(\mathbb{K}/\Bbbk) = \{1\}$ и $\mathbb{K}/\Bbbk$ не может быть расширением Галуа.

Предложение. *Пусть $\mathbb{K}/\Bbbk$ – расширение Галуа.*

(i) *Для любого промежуточного поля $\mathbb{K} \supset \mathbb{L} \supset \Bbbk$ расширение $\mathbb{K}/\mathbb{L}$ также является расширением Галуа.*

(ii) *Если элемент θ инвариантен относительно всех элементов $\mathrm{Aut}(\mathbb{K}/\Bbbk)$, то $\theta \in \Bbbk$.*

Замечание. В условиях предложения не верно, что $\mathbb{L}/\Bbbk$ является расширением Галуа.

Доказательство. Положим $G = \mathrm{Aut}(\mathbb{K}/\Bbbk)$. Возьмем элемент $\theta \in \mathbb{K} \setminus \Bbbk$. Пусть $\mu(t)$ – минимальный многочлен θ над $\Bbbk$ и пусть

$$\theta_1 = \theta, \theta_2, \ldots, \theta_r$$

– все корни $\mu(t)$ в $\mathbb{K}$. Напомним, что

$$[\Bbbk(\theta) : \Bbbk] = \deg(\mu).$$

Любой элемент группы $g \in G$ многочлен μ переводит в себя. Следовательно, g переставляет корни μ:

$$g(\theta_i) = \theta_j.$$

Пусть $G_\theta \subset G$ – стабилизатор элемента θ в G. Тогда $\mathrm{Aut}(\mathbb{K}/\Bbbk(\theta)) = G_\theta$. Индекс подгруппы G_θ в группе G числу элементов орбиты элемента θ. Таким образом,

$$[G : G_\theta] \leq r \leq [\Bbbk(\theta)) : \Bbbk].$$

Применяя теорему о башне полей получим

$$[\mathbb{K} : \Bbbk(\theta)] \cdot [\Bbbk(\theta)) : \Bbbk] = [\mathbb{K} : \Bbbk] = |G| = |G_\theta| \cdot [G : G_\theta] \leq |G_\theta| \cdot [\Bbbk(\theta)) : \Bbbk].$$

Таким образом, $[\mathbb{K} : \Bbbk(\theta)] \leq |G_\theta|$. С другой стороны, по последней теореме всегда имеется обратное неравенство. Отсюда $[\mathbb{K} : \Bbbk(\theta)] = |G_\theta|$ для любого элемента $\theta \in \mathbb{K}\setminus\Bbbk$, т.е. $\mathbb{K}/\mathbb{L}$ является расширением Галуа для любого подполя вида $\mathbb{L} = \Bbbk(\theta)$. Так как любое промежуточное поле $\mathbb{K} \supset \mathbb{L} \supset \Bbbk$ получается из $\Bbbk$ последовательным присоединением корней неприводимых многочленов, то $\mathbb{K}/\mathbb{L}$ является расширением Галуа и для любого промежуточного поля $\mathbb{K} \supset \mathbb{L} \supset \Bbbk$. Это доказывает (i).

Для доказательства (ii) заметим, что $\mathbb{K}/\Bbbk(\theta)$ – расширение Галуа согласно пункту (i). Отсюда

$$[\mathbb{K} : \Bbbk(\theta)] = \mathrm{Aut}(\mathbb{K} : \Bbbk(\theta)) = \mathrm{Aut}(\mathbb{K} : \Bbbk) = [\mathbb{K} : \Bbbk],$$

где среднее равенство выполняется поскольку элемент θ инвариантен. Следовательно, $\Bbbk(\theta) = \Bbbk$ и $\theta \in \Bbbk$ □

Теорема. *Конечное расширение полей $\mathbb{K}/\Bbbk$ является расширением Галуа тогда и только тогда, когда оно нормально и сепарабельно.*

Доказательство. Пусть $n := [\mathbb{K} : \Bbbk]$. Предположим, что $\mathbb{K}/\Bbbk$ расширение Галуа, т.е. $|\operatorname{Aut}(\mathbb{K}/\Bbbk)| = n$. Докажем, что $\mathbb{K}/\Bbbk$ нормально. Пусть f – неприводимый многочлен над $\Bbbk$ и пусть $\theta = \theta_1$ – его корень в $\mathbb{K}$. Пусть $\theta_2, \ldots, \theta_r$ – все остальные корни f в $\mathbb{K}$. Коэффициенты многочлена

$$f_1 := \prod (t - \theta_i)$$

– (с точностью до знака) элементарные симметрические функции от $\theta_1, \ldots, \theta_r$. Они инвариантны относительно перестановок корней, следовательно, они инвариантны относительно группы $\operatorname{Aut}(\mathbb{K}/\Bbbk)$. Согласно пункту (ii) последнего предложения коэффициенты f_1 лежат в $\Bbbk$. Так как f_1 делит f, то отсюда получается, что f_1 и f пропорциональны, т.е. f разлагается на линейные множители в $\mathbb{K}$.

Докажем, что $\mathbb{K}/\Bbbk$ сепарабельно. Предположим противное. Пусть $\mathbb{K}^{\mathrm{sep}}$ – сепарабельное замыкание $\Bbbk$ в $\mathbb{K}$. Тогда $\mathbb{K}/\mathbb{K}^{\mathrm{sep}}$ – расширение Галуа согласно пункту (i) последнего предложения. Значит $|\operatorname{Aut}(\mathbb{K}/\mathbb{K}^{\mathrm{sep}})| = [\mathbb{K} : \mathbb{K}^{\mathrm{sep}}]$. С другой стороны, $\mathbb{K}/\mathbb{K}^{\mathrm{sep}}$ – чисто несепарабельное расширение и как отмечалось выше группа $\operatorname{Aut}(\mathbb{K}/\mathbb{K}^{\mathrm{sep}})$ тривиальна. Противоречие.

Предположим, что $\mathbb{K}/\Bbbk$ нормально и сепарабельно. По теореме о примитивном элементе существует элемент $\theta \in \mathbb{K}/\Bbbk$ такой, что $\mathbb{K} = \Bbbk(\theta)$. Пусть $\mu(t)$ – минимальный многочлен θ. Тогда $\deg \mu = n$. Так как расширение $\mathbb{K}/\Bbbk$ нормально и сепарабельно, то μ имеет ровно n корней $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ в $\mathbb{K}$ (и все они различны). Имеют место изоморфизмы

$$\begin{array}{ccc} \mathbb{K} = \Bbbk(\theta) & \xrightarrow{\quad\psi_i\quad} & \Bbbk(\theta_i) = \mathbb{K} \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\varphi_i} & \\ & \Bbbk[t]/(\mu) & \end{array}$$

Так, что $\varphi_i \circ \psi_i = \varphi$ и $\varphi(\theta) = \varphi_i(\theta_i) = t$. Получаем n автоморфизмов ψ_i. Поскольку $\psi_i(\theta) = \theta_i$, то все они различны. С другой стороны, $|\operatorname{Aut}(\mathbb{K}/\Bbbk)| \leq n$. Теорема доказана. □

Если $\mathbb{K}/\Bbbk$ – расширение Галуа, то группа $\operatorname{Aut}(\mathbb{K}/\Bbbk)$ называется *группой Галуа* этого расширения. Она обозначается также $\operatorname{Gal}(\mathbb{K}/\Bbbk)$. Если f – многочлен над $\Bbbk$, то его группа Галуа – это группа Галуа поля разложения f над $\Bbbk$. Она обозначается $\operatorname{Gal}(f)$.

Замечание. Пусть $f \in \Bbbk[t]$ – неприводимый сепарабельный многочлен степени n и пусть $\mathbb{K}/\Bbbk$ – его поле разложения. Тогда $\mathbb{K}/\Bbbk$ – расширение Галуа. Многочлен f имеет в $\mathbb{K}$ ровно n корней

$$\theta_1, \theta_2, \ldots, \theta_n.$$

Любой автоморфизм $\sigma \in \operatorname{Aut}(\mathbb{K}/\Bbbk)$ корни многочлена с коэффициентами в $\Bbbk$ переводит в корни. Следовательно, он переставляет элементы $\theta_1, \theta_2, \ldots, \theta_n$. Значит, имеется гомоморфизм

$$\Psi : \operatorname{Aut}(\mathbb{K}/\Bbbk) \longrightarrow \mathrm{S}_n$$

в группу перестановок корней. Так как $\mathbb{K} = \Bbbk(\theta_1, \theta_2, \ldots, \theta_n)$, то любой автоморфизм $\sigma \in \operatorname{Aut}(\mathbb{K}/\Bbbk)$ однозначно определяется образами элементов θ_i. Следовательно, Ψ инъективен.

Таким образом, группа Галуа расширения степени n изоморфна подгруппе симметрической группы S_n. Более того, действие $\operatorname{Aut}(\mathbb{K}/\Bbbk)$ на множестве $\{\theta_1, \theta_2, \ldots, \theta_n\}$ транзитивно. Действительно, иначе существует орбита $\{\theta_{i_1}, \ldots, \theta_{i_r}\}$, где $r < n$, и тогда

$$f_1 := (t - \theta_{i_1})(t - \theta_{i_1}) \cdots (t - \theta_{i_r})$$

– многочлен, коэффициенты которого инвариантны относительно всех автоморфизмов $\sigma \in \mathrm{Aut}(\mathbb{K}/\Bbbk)$. Таким образом, многочлен f_1 лежит в $\Bbbk[t]$ и является делителем f. Это противоречит неприводимости f.

Для малых значений n с точностью до сопряженности в S_n для группы Галуа имеются следующие возможности (для краткости положим $G := \mathrm{Aut}(\mathbb{K}/\Bbbk)$):

- $n = 2$, $G = \mathrm{S}_2$;
- $n = 3$, $G = \mathrm{S}_3$ или A_3;
- $n = 4$, $G = \mathrm{S}_4$, A_4, V_4, $\langle (1,2,3,4) \rangle$ (циклическая группа порядка 4) или $\mathrm{D}_4 = \langle \mathrm{V}_4,\ (1,2,3,4) \rangle$.

Отметим, однако, что расширение Галуа $\mathbb{K}/\Bbbk$ не задает однозначно многочлен (и даже его степень), для которого оно является полем разложения. Поэтому говорить о вложении $\mathrm{Aut}(\mathbb{K}/\Bbbk) \hookrightarrow \mathrm{S}_n$ можно говорить только если многочлен f фиксирован.

Задачи

15.1. Докажите, что расширение $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ не является нормальным. Таким образом, башня нормальных расширений необязательно нормальна. Найдите примитивный элемент этого расширения.

15.2. Докажите, что расширение $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ не является нормальным. Найдите примитивный элемент этого расширения.

15.3. Докажите, что для чисто несепарабельного расширения $\mathbb{K}/\Bbbk$ группа $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ тривиальна.

15.4. Пусть $\mathbb{K}$ – поле и пусть G – конечная группа его автоморфизмов. Докажите, что расширение $\mathbb{K}/\mathbb{K}^G$, где

$$\mathbb{K}^G := \{a \in \mathbb{K} \mid \sigma(a) = a,\ \forall \sigma \in G\},$$

является нормальным. В частности, если $\mathrm{char}(\mathbb{K}) = 0$, то $\mathbb{K}/\mathbb{K}^G$ – расширение Галуа и $[\mathbb{K} : \mathbb{K}^G] = |G|$.*

*На самом деле можно показать, что расширение $\mathbb{K}/\mathbb{K}^G$ сепарабельно, поэтому предположение о характеристике здесь излишне.

Лекция 16

Теория Галуа

16.1 Основная теорема теории Галуа

Теорема (Основная теорема теории Галуа)**.** *Пусть* $\mathbb{K}/\Bbbk$ *– конечное расширение Галуа. Каждому промежуточному полю* $\mathbb{K} \supset \mathbb{L} \supset \Bbbk$ *сопоставим подгруппу в* $\mathrm{Aut}(\mathbb{K}/\Bbbk)$*.*

$$\mathrm{Aut}(\mathbb{K}/\mathbb{L}) = \{\sigma \in \mathrm{Aut}(\mathbb{K}/\Bbbk) \mid \sigma(a) = a \quad \forall a \in \mathbb{L}\},$$

а каждой подгруппе $H \subset \mathrm{Aut}(\mathbb{K}/\Bbbk)$ *сопоставим промежуточное поле*

$$\mathbb{K}^H := \{a \in \mathbb{K} \mid \tau(a) = a \quad \forall \tau \in H\}.$$

(i) *Отображения*

$$\mathbb{L} \longmapsto \mathrm{Aut}(\mathbb{K}/\mathbb{L}) \quad \textit{и} \quad H \longmapsto \mathbb{K}^H$$

взаимно обратны и устанавливают биекцию между множеством подполей поля $\mathbb{K}$*, содержащих* $\Bbbk$*, и множеством подгрупп в* $\mathrm{Aut}(\mathbb{K}/\Bbbk)$*.*

(ii) $[\mathbb{K} : \mathbb{K}^H] = |H|$ *и* $[\mathbb{K}^H : \Bbbk] = [\mathrm{Aut}(\mathbb{K}/\Bbbk) : H]$*.*

(iii) *Расширение* $\mathbb{K}^H/\Bbbk$ *является нормальным (т.е. расширением Галуа) тогда и только тогда, когда* H *– нормальная подгруппа в* $\mathrm{Aut}(\mathbb{K}/\Bbbk)$*. В этом случае,*

$$\mathrm{Aut}(\mathbb{K}^H/\Bbbk) \simeq \mathrm{Aut}(\mathbb{K}/\Bbbk)/H.$$

Доказательство. (i) Пусть задано промежуточное поле $\mathbb{L}$. Положим

$$G := \mathrm{Aut}(\mathbb{K}/\Bbbk), \qquad H := \mathrm{Aut}(\mathbb{K}/\mathbb{L}) \quad \text{и} \quad \mathbb{L}' := \mathbb{K}^H.$$

Ясно, что

$$\mathbb{L}' \supset \mathbb{L} \quad \text{и} \quad \mathrm{Aut}(\mathbb{K}/\mathbb{L}') \supset H.$$

Расширение $\mathbb{K}/\mathbb{L}$ является расширением Галуа. Поэтому $|H| = [\mathbb{K} : \mathbb{L}]$. Применяя теорему о башне полей, получим

$$|\mathrm{Aut}(\mathbb{K}/\mathbb{L}')| \geq |H| = [\mathbb{K} : \mathbb{L}] = [\mathbb{K} : \mathbb{L}'] \cdot [\mathbb{L}' : \mathbb{L}] \geq [\mathbb{K} : \mathbb{L}'].$$

С другой стороны, $|\mathrm{Aut}(\mathbb{K}/\mathbb{L}')| \leq [\mathbb{K} : \mathbb{L}']$. Значит, все неравенства выше являются равенствами, $[\mathbb{K} : \mathbb{L}] = [\mathbb{K} : \mathbb{L}']$ и поэтому $\mathbb{L}' = \mathbb{L}$. Таким образом, $\mathbb{K}^H = \mathbb{L}$.

Наоборот, пусть задана подгруппа $H \subset G$. Обозначим $H' := \mathrm{Aut}(\mathbb{K}/\mathbb{K}^H)$. Тогда

$$H' \supset H \quad \text{и} \quad \mathbb{K}^{H'} \subset \mathbb{K}^H.$$

С другой стороны, $\mathbb{K}/\mathbb{K}^H$ является расширением Галуа степени $m := |H'|$. По теореме о примитивном элементе $\mathbb{K} = \mathbb{K}^H(\theta_1)$. Пусть μ – минимальный многочлен θ_1 над $\mathbb{K}^H$ и пусть $\theta_1, \dots, \theta_m$ – его корни в $\mathbb{K}$. Пусть $\{\theta_{i_1}, \dots, \theta_{i_r}\}$ – некоторая орбита группы H. Тогда

$$f := (t - \theta_{i_1})(t - \theta_{i_1}) \cdots (t - \theta_{i_r})$$

– многочлен, коэффициенты которого инвариантны относительно всех автоморфизмов $\sigma \in H$. Таким образом, многочлен f лежит в $\mathbb{K}^H[t]$ и является делителем μ. Это возможно только если $\mu = f$, т.е. действие H на множестве $\{\theta_1, \dots, \theta_m\}$ транзитивно. Но тогда $|H| \geq m$. С другой стороны, $|H| \leq |H'| = m$. Значит, $H = H' = \mathrm{Aut}\left(\mathbb{K}/\mathbb{K}^H\right)$. Это доказывает (i).

(ii). Равенство $[\mathbb{K} : \mathbb{K}^H] = |H|$ следует из того, что $\mathbb{K}/\mathbb{K}^H$ – расширение Галуа и того, что $H = \mathrm{Aut}(\mathbb{K}/\mathbb{K}^H)$. Для доказательства второго равенства заметим, что по теореме о башне полей

$$\left[\mathbb{K} : \mathbb{K}^H\right] \cdot \left[\mathbb{K}^H : \Bbbk\right] = [\mathbb{K} : \Bbbk] = \mathrm{Aut}(\mathbb{K}/\Bbbk).$$

Значит,

$$[\mathbb{K}^H : \Bbbk] = \frac{|\,\mathrm{Aut}(\mathbb{K}/\Bbbk)|}{[\mathbb{K} : \mathbb{K}^H]} = \frac{|\,\mathrm{Aut}(\mathbb{K}/\Bbbk)|}{|H|}.$$

Для доказательства (iii) рассмотрим произвольную подгруппу $H \subset G$. Пусть $n := [G : H]$. Тогда $[\mathbb{K}^H : \Bbbk] = n$ согласно пункту (ii). По теореме о примитивном элементе поле $\mathbb{K}^H$ порождено над $\Bbbk$ одним элементом: $\mathbb{K}^H = \Bbbk(\theta)$. Пусть $\mu \in \Bbbk[t]$ – минимальный многочлен элемента θ над $\Bbbk$. Так как расширение $\mathbb{K}/\Bbbk$ нормально и сепарабельно, то μ имеет в $\mathbb{K}$ ровно $n = \deg(\mu)$ корней

$$\theta_1 = \theta,\ \theta_2, \dots, \theta_n.$$

Таким образом, для каждого θ_i существует автоморфизм $\sigma_i \in G$ такой, что $\theta_i = \sigma_i(\theta)$.

Предположим, что подгруппа H нормальна в G. Тогда для любого $\tau \in H$ имеем

$$\tau(\theta_i) = \tau \circ \sigma_i(\theta) = \sigma_i \circ \sigma_i^{-1} \circ \tau \circ \sigma_i(\theta) = \sigma_i(\theta) = \theta_i$$

(поскольку $\sigma_i^{-1} \circ \tau \circ \sigma_i \in H$ и $\theta \in \mathbb{K}^H$). Это показывает, что $\theta_i \in \mathbb{K}^H$. Следовательно, поле $\mathbb{K}^H$ является полем разложения многочлена μ, а потому $\mathbb{K}^H/\Bbbk$ – нормальное расширение.

Предположим, что расширение $\mathbb{K}^H/\Bbbk$ нормально. Тогда $\mathbb{K}^H$ содержит все корни многочлена μ, т.е. $\theta_i \in \mathbb{K}^H$. Как и выше для любого $\tau \in H$ получаем

$$\sigma_i^{-1} \circ \tau \circ \sigma_i(\theta) = \sigma_i^{-1} \circ \tau(\theta_i) = \sigma_i^{-1}(\theta_i) = \theta.$$

Это означает, что $\sigma_i^{-1} \circ \tau \circ \sigma_i$ тождественно действует на $\mathbb{K}^H = \Bbbk(\theta)$, т.е. $\sigma_i^{-1} \circ \tau \circ \sigma_i \in H$. Таким образом, $H \lhd \mathrm{Aut}(\mathbb{K}/\Bbbk)$.

Наконец, всегда имеется гомоморфизм-ограничение

$$\Psi : \mathrm{Aut}(\mathbb{K}/\Bbbk) \longrightarrow \mathrm{Aut}(\mathbb{K}^H/\Bbbk)$$

Его ядро, очевидно, содержит H. В нашем случае имеем

$$|\,\mathrm{Aut}(\mathbb{K}^H/\Bbbk)| = [\mathbb{K}^H : \Bbbk] = \frac{[\mathbb{K} : \Bbbk]}{[\mathbb{K} : \mathbb{K}^H]} = \frac{\mathrm{Aut}(\mathbb{K}/\Bbbk)}{H}$$

Следовательно, гомоморфизм Ψ сюръективен, $\mathrm{Ker}(\Psi) = H$ и $\mathrm{Aut}(\mathbb{K}^H/\Bbbk) \simeq \mathrm{Aut}(\mathbb{K}/\Bbbk)/H$. $\square$

16.2 Классические геометрические задачи

Для простоты, ниже мы предположим, что характеристика всех рассматриваемых полей полей равна 0 (или, по крайней мере, отлична от 2).

Определение. Поле $\mathbb{K}$ называется *квадратично замкнутым*, если любой многочлен $f \in \mathbb{K}[t]$ степени 2 имеет корень, в $\mathbb{K}$. Пусть $\Bbbk$ – поле и пусть $\bar{\Bbbk}$ – его алгебраическое замыкание. Квадратичным замыканием $\Bbbk$ в $\bar{\Bbbk}$ называется наименьшее квадратично замкнутое подполе $\Bbbk^{\mathrm{qua}} \subset \bar{\Bbbk}$, содержащее $\Bbbk$.

Теорема. *Квадратичное замыкание $\Bbbk$ в $\bar{\Bbbk}$ существует и единственно.*

Доказательство. Пусть $\mathbb{K}_1$ – подполе в $\bar{\Bbbk}$, полученное присоединением корней всех многочленов степени 2 над $\Bbbk$ (это пересечение всех подполей в $\bar{\Bbbk}$, содержащих $\Bbbk$ и корни всех многочленов степени 2). Далее, пусть $\mathbb{K}_2$ – подполе в $\bar{\Bbbk}$, полученное присоединением корней всех многочленов степени 2 над $\mathbb{K}_1$. Продолжая по индукции, получим цепочку подполей в $\bar{\Bbbk}$

$$\Bbbk \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_i \subset \mathbb{K}_{i+1} \subset \cdots, \qquad (*)$$

где $\mathbb{K}_{i+1}$ – подполе в $\bar{\Bbbk}$, полученное присоединением корней всех многочленов степени 2 над $\mathbb{K}_i$. Тогда $\Bbbk^{\mathrm{qua}} = \cup \mathbb{K}_i$. □

Замечание. Для любого подполя $\mathbb{K} \subset \Bbbk^{\mathrm{qua}}$ такого, что $[\mathbb{K} : \Bbbk] < \infty$ существует конечная цепочка квадратичных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_n,$$

такая, что $[\mathbb{L}_i : \mathbb{L}_{i-1}] = 2$ и $\mathbb{K} \subset \mathbb{L}_n$.

Доказательство. Поле $\mathbb{K}$ лежит в некотором поле $\mathbb{K}_n$ в башне $(*)$. Докажем утверждение индукцией по n. Так как $[\mathbb{K} : \Bbbk] < \infty$, то $\mathbb{K} = \Bbbk(\theta_1, \ldots, \theta_m)$ для некоторых $\theta_1, \ldots, \theta_m \in \mathbb{K} \subset \mathbb{K}_n$. Значит, существуют многочлены $t^2 + a_i t + b_i \in \mathbb{K}_{n-1}[t]$ для которых $\theta_1, \ldots, \theta_m$ – корни. По предположению индукции для поля

$$\mathbb{K}' := \Bbbk(a_1, \ldots, a_m, b_1, \ldots, b_m)$$

существует башня

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_s,$$

такая, что $[\mathbb{L}_i : \mathbb{L}_{i-1}] = 2$ и $\mathbb{K}' \subset \mathbb{L}_s$. Мы можем ее продолжить

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_s \subset \mathbb{L}_{s+1} \subset \cdots \subset \mathbb{L}_{s+m}$$

где $\mathbb{L}_{i+1} = \mathbb{L}_i(\theta_i)$ при $i > s$. Ясно, что все расширения $\mathbb{L}_{i+1}/\mathbb{L}_i$ квадратичны и

$$\mathbb{K} = \Bbbk(\theta_1, \ldots, \theta_m) \subset \mathbb{L}_{s+m}.$$ □

Теорема. *Пусть $f \in \Bbbk[t]$ – неприводимый многочлен и пусть $\mathbb{K} \subset \bar{\Bbbk}$ – его поле разложения. Включение $\mathbb{K} \subset \Bbbk^{\mathrm{qua}}$ имеет место тогда и только тогда, когда $[\mathbb{K} : \Bbbk] = 2^m$ для некоторого m.*

Доказательство. Пусть $\mathbb{K} \subset \Bbbk^{\mathrm{qua}}$. Согласно замечанию существует цепочка квадратичных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_n,$$

такая что $\mathbb{L}_n \supset \mathbb{K}$. По теореме о башне полей

$$[\mathbb{L}_n : \Bbbk] = [\mathbb{L}_n : \mathbb{L}_{n-1}] \cdot [\mathbb{L}_{n-1} : \mathbb{L}_{n-2}] \cdots [\mathbb{L}_1 : \mathbb{L}_0] = 2^n.$$

С другой стороны,

$$2^n = [\mathbb{L}_n : \Bbbk] = [\mathbb{L}_n : \mathbb{K}] \cdot [\mathbb{K} : \Bbbk].$$

Значит, $[\mathbb{K} : \Bbbk] = 2^m$.

Обратно, пусть $[\mathbb{K} : \Bbbk] = 2^m$. Тогда группа Галуа $G := \mathrm{Aut}(\mathbb{K}/\Bbbk)$ является 2-группой. Следовательно, она разрешима и имеется композиционный ряд

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = \{1\},$$

в котором все факторы имеют порядок 2. Согласно основной теореме теореме Галуа получаем цепочку квадратичных расширений

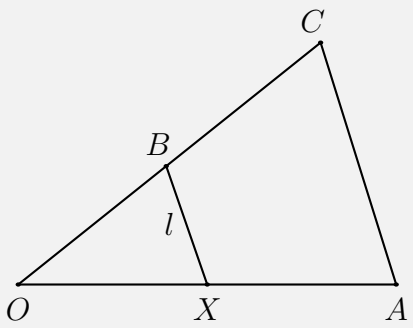
$$\Bbbk = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r = \mathbb{K},$$

где $\mathbb{K}_i = \mathbb{K}_{i+1}^{G_{i+1}}$. Значит, $\mathbb{K}$ содержится в квадратичном замыкании поля $\Bbbk$. □

Геометрическая задача на построение циркулем и линейкой может быть сформулирована следующим образом: даны отрезки длин 1, a_1, …, a_n, построить отрезок длины c.

Предложение. *Пусть даны отрезки длин* 1, a_1, …, a_n. *Отрезок длины* c *можно построить при помощи циркуля и линейки, исходя из* 1, a_1, …, a_n, *тогда и только тогда, когда* $c \in \mathbb{Q}(a_1, \ldots, a_n)^{\mathrm{qua}} \cap \mathbb{R}$.

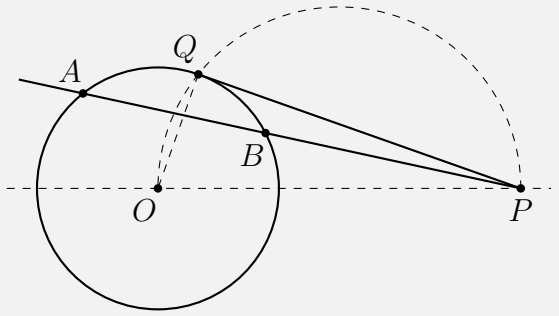
Доказательство. Пусть $\mathbb{K}$ – множество точек комплексной плоскости, которые можно построить при помощи циркуля и линейки, исходя из 1, a_1, …, $a_n \in \mathbb{R}$. Докажем, что $\mathbb{K}$ является полем. Действительно, пусть a, $b \in \mathbb{K}$. Очевидно, что $a \pm b \in \mathbb{K}$. Пусть a, $b \in \mathbb{K} \cap \mathbb{R}$. Для доказательства того, что $ab \in \mathbb{K}$ покажем, что уравнение $a/x = 1/b$ можно решить при помощи циркуля и линейки. Для этого построим треугольник OAC такой, что $OA = a$, $OC = 1$ (сторона AC – произвольная). На стороне OC отложим точку B так, что $OB = b$. Проведем через B прямую l, параллельную AC и пусть $X := OC \cap l$.



Тогда из подобия треугольников получаем

$$\frac{a}{x} = \frac{OA}{OX} = \frac{OC}{OB} = \frac{1}{b}.$$

Это показывает, что отрезок длины $x = ab$ может быть построен. Аналогично, для доказательства того, что $a/b \in \mathbb{K}$ нужно показать, что уравнение $a/x = b/1$ можно решить при помощи циркуля и линейки. Это делается таким же построением. Если же a, b – комплексные, то для их умножения (деления) нужно перемножить (поделить) их модули и сложить (вычесть) аргументы. Ясно, что это возможно. Таким образом, $\mathbb{K}$ – поле. Для доказательства того, что оно квадратично замкнуто, достаточно показать, что из $a \in \mathbb{K} \cap \mathbb{R}$ следует, что $\sqrt{a} \in \mathbb{K}$. Для этого на прямой от точки P в одну сторону отложим отрезки PB и PA длин 1 и a, соответственно. Проведем через A и B окружность с центром O.



Теперь через точку P проведем касательную PQ к этой окружности. Точка Q находится как точка пересечения нашей окружности с окружностью, у которой отрезок OP – диаметр. Тогда искомая величина $\sqrt{a}$ – это длина отрезка PQ: по основному свойству секущих

$$PQ^2 = PA \cdot PB = a.$$

Значит, мы всегда можем присоединять к $\mathbb{K}$ квадратные корни из любых его положительных элементов. Присоединяя к $\mathbb{K}$ также $\boldsymbol{i} = \sqrt{-1}$, получаем, что $\mathbb{K}$ квадратично замкнуто. С другой стороны, при помощи циркуля и линейки мы можем проводить и находить точки пересечения только линий второго порядка, т.е. мы можем решать только квадратичные уравнения. Следовательно, $\mathbb{K} = \mathbb{Q}(a_1, \ldots, a_n)^{\mathrm{qua}}$. □

Задача об удвоении куба: при помощи циркуля и линейки построить сторону куба, имеющего объем 2. Вопрос сводится к построению (при помощи циркуля и линейки) числа $\sqrt[3]{2}$. Иначе говоря, верно ли, что $\sqrt[3]{2} \in \mathbb{Q}^{\mathrm{qua}}$. Поскольку $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3 \neq 2^m$, то задача не имеет решения.

Трисекция угла: при помощи циркуля и линейки разделить угол на три равные части. Вопрос сводится к построению величины $\cos(\alpha/3)$ по $\cos(\alpha)$. Имеет место тригонометрическое тождество

$$\cos(\alpha) = 4\cos^3(\alpha/3) - 3\cos(\alpha/3).$$

Таким образом, требуемая величина $\cos(\alpha/3)$ является корнем многочлена

$$f = 4t^3 - 3t - u, \qquad u := \cos(\alpha).$$

Если речь идет об универсальном методы трисекции угла, не зависящем от величины угла α, то мы должны рассматривать $u = \cos(\alpha)$ как независимую переменную. Тогда многочлен f неприводим над $\mathbb{Q}(u)$, и задача неразрешима. Для конкретных углов (например, для прямого) задача, конечно, может быть разрешима. Критерием разрешимости является наличие у многочлена f корней в поле $\mathbb{Q}(u)$.

Построение правильного n-угольника: при помощи циркуля и линейки построить правильный n-угольник. Мы рассмотрим только случай простого $n = p$. Задача сводится к построению комплексного числа

$$\zeta_p := \cos(2\pi/p) + \boldsymbol{i}\sin(2\pi/p),$$

которое является корнем кругового многочлена

$$\Phi_p = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

Лемма. *Для простого p круговой многочлен $\Phi_p(t)$ неприводим над $\mathbb{Q}$.*[*]

Доказательство. Действительно, согласно лемме Гаусса достаточно доказать неприводимость над $\mathbb{Z}$. Сделаем замену переменной $z = t - 1$:

$$\Phi_p = \frac{t^p - 1}{t - 1} = \frac{(z+1)^p - 1}{z}.$$

Легко видеть, что все коэффициенты, кроме старшего, делятся на p и не делятся на p^2. Согласно критерию Эйзенштейна Φ_p неприводим. □

Следствие. $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg(\Phi_p) = p - 1$.

Таким образом, правильный p-угольник можно построить при помощи циркуля и линейки только если p имеет вид $2^m + 1$. Верно и обратное если простое число имеет вид $p = 2^m + 1$, то правильный p-угольник можно построить при помощи циркуля и линейки. Действительно, все корни многочлена Φ_p являются степенями ζ_p. Следовательно, $\mathbb{Q}(\zeta_p)$ – поле разложения для Φ_p, т.е. $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ – расширение Галуа с группой Галуа $G = \mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ порядка 2^m, т.е. G – 2-группа. Такая группа должна быть разрешима и поэтому существует композиционный ряд

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G \qquad (\dagger)$$

где G_{i+1}/G_i – циклическая группа порядка 2. Согласно основной теореме теории Галуа цепочке подгрупп (†) соответствует башня полей

$$\mathbb{Q}(\zeta_p) = \mathbb{K}_0 \supset \mathbb{K}_1 \supset \cdots \supset \mathbb{K}_m = \mathbb{Q}.$$

так, что $[\mathbb{K}_i : \mathbb{K}_{i+1}] = 2$ для всех i, т.е. все $\mathbb{K}_i/\mathbb{K}_{i+1}$ – квадратичные расширения. Следовательно, $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}^{\mathrm{qua}}$.

Простые числа вида $p = 2^m + 1$ называются *простыми числами Ферма*. В настоящее время известно лишь пять таких чисел: 3, 5, 17, 257, 65537.

Аналогичное рассуждение может быть проведено для n-угольника, где n необязательно простое. Как и выше, нужно воспользоваться неприводимостью кругового многочлена Φ_n (см. задачу 16.3).

[*]Утверждение верно и для произвольного кругового многочлена $\Phi_n(t)$, однако доказательство этого факта немного сложнее.

16.3 Разрешимость алгебраических уравнении в радикалах

Лемма. *Пусть характеристика* $\Bbbk$ *взаимно проста с* n*. Тогда группа Галуа многочлена* $t^n - 1$ *изоморфна* подгруппе *мультипликативной группы* $(\mathbb{Z}/n\mathbb{Z})^*$*. В частности, она абелева.*

Доказательство. Пусть $\mathbb{K}$ – поле разложения $t^n - 1$ и пусть $\boldsymbol{\mu}_n \subset \mathbb{K}$ – множество всех корней степени n из 1. Так как

$$(t^n - 1)' = nt^{n-1} \neq 0,$$

то многочлен $t^n - 1$ не имеет кратных корней в $\mathbb{K}$. Следовательно, $\mathbb{K}/\Bbbk$ – расширение Галуа и $\boldsymbol{\mu}_n$ – группа порядка n. Напомним, что эта группа должна быть циклической. Пусть $\zeta = \zeta_n \in \mathbb{K}$ – первообразный корень степени n из 1, т.е. порождающий $\boldsymbol{\mu}_n$. Тогда $\mathbb{K} = \Bbbk(\zeta)$. Следовательно, любой автоморфизм $\sigma \in \mathrm{Aut}(\mathbb{K}/\Bbbk)$ однозначно задается образом элемента ζ. При этом

$$\sigma(\zeta) = \zeta^{m(\sigma)},$$

где $m(\sigma)$ – натуральное число, зависящее от σ и определенное по модулю n. Таким образом, мы имеем отображение

$$m : \mathrm{Aut}(\mathbb{K}/\Bbbk) \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad \sigma \longmapsto m(\sigma)$$

Для σ_1, $\sigma_2 \in \mathrm{Aut}(\mathbb{K}/\Bbbk)$ имеем

$$\sigma_1(\sigma_2(\zeta)) = \sigma_1(\zeta^{m(\sigma_2)}) = \sigma_1(\zeta)^{m(\sigma_2)} = (\zeta^{m(\sigma_1)})^{m(\sigma_2)} = \zeta^{m(\sigma_1)m(\sigma_2)}.$$

Отсюда

$$m(\sigma_1 \circ \sigma_2) = m(\sigma_1)m(\sigma_2).$$

Следовательно, отображение m задает гомоморфизм групп

$$m : \mathrm{Aut}(\mathbb{K}/\Bbbk) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$

Его ядро состоит из автоморфизмов σ таких, что $m(\sigma) = 1$, т.е. $\sigma(\zeta) = \zeta$. Ясно, что оно тривиально. Следовательно, гомоморфизм m инъективен. □

Нормальное расширение полей называется *циклическим*, если циклична его группа Галуа. Циклические расширения допускают естественное описание:

Лемма. *Пусть поле* $\Bbbk$ *содержит* n *различных корней* $\zeta = \zeta_n$ *степени* n *из* 1*. Если* $\mathbb{K} = \Bbbk(\theta)$*, где* θ *– корень многочлена* $t^n - a$*, то* $\mathbb{K}/\Bbbk$ *– циклическое расширение*[†] *и* $[\mathbb{K} : \Bbbk]$ *делит* n*. Более того,* $\theta^r \in \Bbbk$*, где* $r := [\mathbb{K} : \Bbbk]$*.*

Доказательство. Пусть $\zeta = \zeta_n$ – первообразный корень степени n из 1. Любой корень многочлена $t^n - a$ приналежит $\mathbb{K}$ и имеет вид

$$\theta_k := \theta\,\zeta^k,$$

причем элементы $\theta_0, \theta_1, \ldots, \theta_{n-1}$ различны. Следовательно, $\mathbb{K}$ – поле разложения $t^n - a$, т.е. расширение $\mathbb{K}/\Bbbk$ нормально. Отсюда мы видим, что многочлен $t^n - a$ имеет ровно n корней в $\mathbb{K}$, следовательно, расширение $\mathbb{K}/\Bbbk$ также сепарабельно.

[†]На самом деле, верно и обратное: если $\mathbb{K}/\Bbbk$ – циклическое расширение, то $\mathbb{K} = \Bbbk(\theta)$ для $\theta^n \in \Bbbk$. Доказательство этой импликации немного более сложное и мы его здесь не приводим.

Любой автоморфизм $\sigma \in \mathrm{Aut}(\mathbb{K}/\Bbbk)$ корни многочлена $t^n - a$ переводит в корни. Так как $\mathbb{K} = \Bbbk(\theta)$, то σ однозначно задается образом элемента θ. При этом

$$\sigma(\theta) = \theta\,\zeta^{m(\sigma)}, \tag{‡}$$

где $m(\sigma)$ – натуральное число, зависящее от σ и определенное по модулю n. Таким образом, мы имеем отображение

$$m : \mathrm{Aut}(\mathbb{K}/\Bbbk) \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad \sigma \longmapsto m(\sigma).$$

Для σ_1, $\sigma_2 \in \mathrm{Aut}(\mathbb{K}/\Bbbk)$ имеем

$$\sigma_1(\sigma_2(\theta)) = \sigma_1(\theta\,\zeta^{m(\sigma_2)}) = \zeta^{m(\sigma_2)}\sigma_1(\theta) = \zeta^{m(\sigma_2)}\zeta^{m(\sigma_1)}\theta = \zeta^{m(\sigma_1)+m(\sigma_2)}\theta.$$

Следовательно, отображение m задает гомоморфизм групп

$$m : \mathrm{Aut}(\mathbb{K}/\Bbbk) \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

Его ядро состоит из автоморфизмов σ таких, что $m(\sigma) = 1$, т.е. $\sigma(\theta) = \theta$. Ясно, что оно тривиально. Таким образом, гомоморфизм m инъективен. Следовательно, его образ в $\mathbb{Z}/n\mathbb{Z}$ изоморфен $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ и поэтому $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ – циклическая группа. Ее порядок r равен степени расширения $\mathbb{K}/\Bbbk$, поскольку расширение нормально и сепарабельно.

Так как $\sigma^r = 1$ для любого $\sigma \in \mathrm{Aut}(\mathbb{K}/\Bbbk)$, то из (‡) получаем $\theta = \sigma^r(\theta) = \theta\,\zeta^{m(\sigma)r}$. Отсюда $\zeta^{m(\sigma)r} = 1$. Тогда получаем $\sigma^r(\theta^r) = (\theta\,\zeta^{m(\sigma)})^r = \theta^r$. Следовательно, $b := \theta^r \in \Bbbk$. Так как $[\mathbb{K} : \Bbbk] = r$, то отсюда следует, что минимальный многочлен элемента θ имеет вид $t^r - b$. Он должен делить многочлен $t^n - a$. Это возможно только если r делит n. □

Определение. Конечное расширение полей $\mathbb{K}/\Bbbk$ называется *радикальным*, если существует башня подполей

$$\Bbbk = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_{n-1} \subset \mathbb{K}_n = \mathbb{K}, \tag{§}$$

где

$$\mathbb{K}_i = \mathbb{K}_{i-1}(\theta_i), \qquad \theta_i^{r_i} \in \mathbb{K}_{i-1}.$$

Таким образом, $\theta_i = \sqrt[r_i]{a_i}$ для некоторого $a_i \in \mathbb{K}_{i-1}$. Говорят также, что алгебраическое уравнение $f(t) = 0$, $f \in \Bbbk[t]$ *разрешимо в радикалах*, если существует радикальное расширение, содержащее все корни многочлена f.

Заметим, что расширение $\mathbb{K}/\Bbbk$ не обязано быть нормальным. Этот недостаток легко исправляется расширением поля $\mathbb{K}$.

Лемма. *Каждое радикальное расширение $\mathbb{K}/\Bbbk$ содержится в некотором нормальном радикальном расширении $\mathbb{K}'/\Bbbk$.*

Доказательство. Доказательство проводим индукцией по высоте n башни (§). Пусть $n = 1$. Тогда $\mathbb{K} = \Bbbk(\theta)$, $\theta^r = a \in \Bbbk$. Пусть $\zeta = \zeta_r$ – первообразный корень степени r из 1. Тогда поле разложения $\Bbbk(\theta, \zeta)$ многочлена $t^r - a$ как раз и будет нормальным радикальным расширением.

Предположим, что утверждение верно для полей с башней (§) высоты $< n$. Тогда $\mathbb{K}_{n-1}$ содержится в нормальном радикальном расширении $\mathbb{L}_{n-1}/\Bbbk$ и $\mathbb{K} = \mathbb{K}_{n-1}(\theta)$, где $\theta^r = a \in \mathbb{K}_{n-1}$. Рассмотрим минимальный многочлен $\mu(t)$ элемента a над $\Bbbk$. По определению нормальности многочлен $\mu(t)$ над полем $\mathbb{L}_{n-1}$ распадается в произведение линейных множителей:

$$\mu(t) = (t - a_1)(t - a_2)\cdots(t - a_m), \qquad a_1 = a.$$

Пусть $\mathbb{M}$ – поле разложения над $\Bbbk$ многочлена $\mu(t^r)$. Ясно, что $\mathbb{M} = \Bbbk(\zeta, \theta_1, \ldots, \theta_m)$, где $\theta_i^r = a_i$, а $\zeta = \zeta_r$ – первообразный корень степени r из 1. Мы можем считать, что $\mathbb{M}$ и $\mathbb{L}$ содержатся в одном большом поле – алгебраическом замыкании $\bar{\mathbb{K}}$ поля $\mathbb{K}$. Пусть $\mathbb{K}' := \mathbb{L}_{n-1} \cdot \mathbb{M}$ – подполе в $\bar{\mathbb{K}}$, порожденное $\mathbb{L}_{n-1}$ и $\mathbb{M}$. Так как расширение $\mathbb{L}_{n-1}/\Bbbk$ нормально, то оно является полем разложения некоторого многочлена $h(t) \in \Bbbk[t]$. Тогда $\mathbb{K}'$ является полем разложения над $\Bbbk$ многочлена $\mu(t^r)h(t)$. Значит, $\mathbb{K}'/\Bbbk$ – нормальное расширение. С другой стороны, $\mathbb{K}' = \mathbb{L}(\zeta, \theta_1, \ldots, \theta_m)$. Поэтому расширение $\mathbb{K}'/\Bbbk$ радикально и $\mathbb{K}' \supset \mathbb{K}$. □

Лемма. *Группа Галуа* $\mathrm{Aut}(\mathbb{K}/\Bbbk)$ *нормального радикального расширения* $\mathbb{K}/\Bbbk$ *разрешима.*

Доказательство. По определению радикальности для расширения $\mathbb{K}/\Bbbk$ существует башня полей §. Однако, промежуточные расширения $\mathbb{K}_i/\mathbb{K}_{i-1}$ могут не быть нормальными. Для того, чтобы обойти эту трудность добавим к $\Bbbk$ соответствующий первообразный корень из 1.

Пусть $\zeta = \zeta_r$ – первообразный корень степени $r = r_1 r_2 \cdots r_n$ из 1. Поле $\mathbb{K}(\zeta)$ является полем разложения некоторого многочлена над $\Bbbk$. Действительно, по предположению расширение $\mathbb{K}/\Bbbk$ нормально. Поэтому $\mathbb{K}$ является полем разложения некоторого многочлена $h(t) \in \Bbbk$. Тогда $\mathbb{K}(\zeta)$ является полем разложения над $\Bbbk$ многочлена $h(t)(t^r - 1)$. Следовательно, расширение $\mathbb{K}(\zeta)/\Bbbk$ нормально. Рассмотрим башню

$$\Bbbk \subset \Bbbk(\zeta) \subset \mathbb{K}_1(\zeta) \subset \mathbb{K}_2(\zeta) \subset \cdots \subset \mathbb{K}_{n-1}(\zeta) \subset \mathbb{K}_n(\zeta) = \mathbb{K}(\zeta).$$

По предыдущим леммам группа $\mathrm{Aut}(\Bbbk(\zeta)/\Bbbk)$ абелева, а остальные последовательные расширения в башне являются циклическими. В силу соответствия Галуа группа $G := \mathrm{Aut}(\mathbb{K}(\zeta)/\Bbbk)$ обладает нормальным рядом

$$G \rhd G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd \{1\},$$

в котором факторгруппа G/G_0 абелева, а остальные последовательные факторгруппы G_i/G_{i+1} циклические. Следовательно, G разрешима. Расширение $\mathbb{K}/\Bbbk$ нормально. Следовательно, $H := \mathrm{Aut}(\mathbb{K}(\zeta)/\mathbb{K})$ – нормальная подгруппа в $G = \mathrm{Aut}(\mathbb{K}(\zeta)/\Bbbk)$. Тогда $\mathrm{Aut}(\mathbb{K}/\Bbbk) = G/H$ – также разрешимая группа. □

Теорема. *Если алгебраическое уравнение* $f(t) = 0$, $f \in \Bbbk[t]$ *разрешимо в радикалах, то его группа Галуа* $\mathrm{Gal}(f)$ *разрешима.*

Доказательство. Предположим, что все корни $\theta_1, \ldots, \theta_n$ многочлена $f(t)$ лежат в нормальном радикальном расширении $\mathbb{K}/\Bbbk$. Естественное включение

$$\Bbbk \subset \Bbbk(\theta_1, \ldots, \theta_n) \subset \mathbb{K}$$

означает, что группа

$$\mathrm{Gal}(f) = \mathrm{Aut}(\Bbbk(\theta_1, \ldots, \theta_n)/\Bbbk)$$

является факторгруппой разрешимой группы $\mathrm{Aut}(\mathbb{K}/\Bbbk)$. Поэтому она сама разрешима. □

При $n \leq 4$ симметрическая группа S_n разрешима. Поэтому алгебраические уравнения степени ≤ 4 разрешимы в радикалах. Это уже не верно при $n \geq 5$. Например, если группа Галуа многочлена f содержит знакопеременную группу A_n, $n \geq 5$, то уравнение $f(t) = 0$ неразрешимо в радикалах. Приведем конкретный пример многочлена с неразрешимой группой Галуа.

Лемма. *Пусть $f(t)$ – неприводимый многочлен простой степени p над $\mathbb{Q}$, причем ровно два его корня невещественны. Тогда* $\mathrm{Gal}(f) = \mathrm{S}_p$. *Следовательно, уравнение $f(t) = 0$ неразрешимо в радикалах при $p \geq 5$.*

Доказательство. Пусть $\mathbb{K}$ – поле разложения $\mathbb{K}$ над $\mathbb{Q}$. Так как $\deg(f) = p$, то $\mathrm{Gal}(f) \subset \mathrm{S}_p$. Так как степень расширения $[\mathbb{K} : \mathbb{Q}]$ делится на p, то и порядок $\mathrm{Gal}(f)$ делится на p. Значит, в $\mathrm{Gal}(f)$ содержится длинный цикл (как единственный элемент порядка p в группе S_p). Транспозиция там также содержится, так как комплексное сопряжение является автоморфизмом, сохраняющим этот многочлен, а при этом меняющим местами ровно два (невещественных) корня. Оставшаяся часть доказательства следует из следующей леммы. □

Лемма. *Пусть p – нечетное простое число. Если подгруппа $G \subset \mathrm{S}_p$ содержит цикл σ длины p и транспозицию τ, то $G = \mathrm{S}_p$.*

Доказательство. Пусть транспозиция имеет вид $\tau = (i_1, i_2)$. Ясно, что $\sigma^k(i_1) = i_2$ для некоторого $1 \leq k \leq p-1$. Заменяя σ на σ^k мы можем считать, что σ имеет вид $\sigma = (i_1, i_2, i_3, \ldots, i_p)$. Тогда группа G содержит транспозиции $\tau_k := \sigma^k \circ \tau \circ \sigma^{-k}$, где

$$\tau_k := \sigma^{k-1} \circ \tau \circ \sigma^{-(k-1)} = (\sigma^{k-1}(i_1), \sigma^{k-1}(i_2)) = (i_k, i_{k+1})$$

(нижние индексы рассматриваются по модулю p). Также группа G содержит цикл $\tau \circ \sigma \circ \tau^{-1}$, который получается из σ перестановкой между собой "соседних" элементов i_k и i_{k+1}. Ясно, что перестановкой между собой пар "соседних" элементов мы можем из σ получить любой цикл $\sigma' = (j_1, j_2, \ldots, j_p)$ длины p. Тогда G содержит и транспозиции

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

т.е. все транспозиции. Так как симметрическая группа порождается транспозициями, то $G = \mathrm{S}_p$. □

Мы можем также рассмотреть "общий" многочлен.

Пример. Пусть $\mathbb{K} = \Bbbk(x_1, \ldots, x_n)$ – поле рациональных дробей над $\Bbbk$ от переменных $x_1, \ldots, x_n$. Пусть $\mathbb{L} \subset \mathbb{K}$ – подполе симметрических рациональных дробей. По основной теореме о симметрических функциях $\mathbb{L}$ порождается элементарными симметрическими многочленами $\sigma_1, \ldots, \sigma_n$. Более того, каждый элемент из $\mathbb{L}$ однозначно выражается через $\sigma_1, \ldots, \sigma_n$ как рациональная функция. Это означает, что

$$\mathbb{L} = \Bbbk(\sigma_1, \ldots, \sigma_n).$$

Рассмотрим многочлен

$$f(t) = t^n - \sigma_1 t^{n-1} + \sigma_2 t^{n-2} + \cdots + (-1)^{n-1}\sigma_{n-1} t + (-1)^n \sigma_n \in \mathbb{L}[t].$$

Это "общий" многочлен над $\mathbb{L}$, любой многочлен, у которого коэффициенты – алгебраически независимые величины, может быть записан в таком виде. Легко видеть, что $x_1, \ldots, x_n$ – корни f. Так как $\mathbb{K} = \mathbb{L}(x_1, \ldots, x_n)$, то $\mathbb{K}$ – поле разложения для f над $\mathbb{L}$.

Симметрическая группа S_n действует на поле $\mathbb{K} = \Bbbk(x_1, \ldots, x_n)$ перестановками переменных так, что $\mathbb{L} = \mathbb{K}^{\mathrm{S}_n}$. Следовательно, $\mathrm{Aut}(\mathbb{K}/\mathbb{L}) \supset \mathrm{S}_n$ и $[\mathbb{K} : \mathbb{L}] \geq |\mathrm{S}_n| = n!$. С другой стороны, $\mathbb{K}$ является полем разложения многочлена $f(t) \in \mathbb{L}[t]$. Значит, $[\mathbb{K} : \mathbb{L}] \leq (\deg(f))! = n!$. Таким образом, $[\mathbb{K} : \mathbb{L}] = n!$ и

$$\mathrm{Gal}(f) = \mathrm{Aut}(\mathbb{K}/\mathbb{L}) = \mathrm{S}_n\,.$$

Задачи

16.1. Вычислите группы Галуа над $\mathbb{Q}$ многочленов t^3+t+1, $t^3-12t+8$, t^3-2t-2, t^4+3t^3-3t+3.

16.2. Пусть $q = p^n$ и $e \in \mathbb{N}$. Тогда $\mathbb{F}_q \subset \mathbb{F}_{q^e}$. Докажите, что $\mathrm{Aut}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ – циклическая группа порядка e, порожденная степенью автоморфизма Фробениуса ϕ^n. *Указание.* Используйте то, что группа $\mathbb{F}_{q^e}^*$ циклическая.

16.3. Принимая на веру факт, что круговой многочлен Φ_n неприводим, найдите критерий того, что правильный n-угольник (для произвольного n) может быть построен при помощи циркуля и линейки.

16.4. Докажите, что круговой многочлен $\Phi_{15}(t)$ неприводим. *Указание.* Используйте редукцию по модулю 2.

Лекция 17

Трансцендентные расширения полей

Базисы трансцендентности

Определение. Пусть $\mathbb{K}$ – расширение поля $\Bbbk$. Подмножество $M \subset \mathbb{K}$ называется *алгебраически независимым* над $\Bbbk$, если для любого многочлена $f(t_1, \ldots, t_m) \in \Bbbk[t_1, \ldots, t_m]$ из соотношения

$$f(\alpha_1, \ldots, \alpha_m) = 0, \qquad \alpha_i \in M, \quad \alpha_i \neq \alpha_j$$

следует, что $f(t_1, \ldots, t_m) = 0$. Подмножество $M \subset \mathbb{K}$ называется *базисом трансцендентности*, если

(i) M алгебраически независимо и

(ii) любое алгебраически независимое подмножество $M' \subset \mathbb{K}$, содержащее M, совпадает с M.

Замечание. Алгебраически независимое подмножество M является базисом трансцендентности $\mathbb{K}$ над $\Bbbk$ тогда и только тогда, когда поле $\mathbb{K}$ алгебраично над $\Bbbk(M)$.

Пример. Множество из одного элемента α алгебраически независимо тогда и только тогда, когда α трансцендентен (неалгебраичен) над $\Bbbk$.

Пример. Пусть $\mathbb{K} = \Bbbk(t_1, \ldots, t_n)$ – поле рациональных дробей от n переменных. Тогда элементы $t_1, \ldots, t_n$ алгебраически независимы над $\Bbbk$ и образуют базис. Верно и обратное: если $\mathbb{K} = \Bbbk(\vartheta_1, \ldots, \vartheta_n)$, где элементы $\vartheta_1, \ldots, \vartheta_n$ образуют базис трансцендентности, то $\mathbb{K}$ изоморфно (над $\Bbbk$) полю рациональных дробей от n переменных.

Определение. Расширение полей $\mathbb{K}/\Bbbk$ называется *чисто трансцендентным*, если существует базис трансцендентности, порождающий $\mathbb{K}$ над $\Bbbk$, т.е. $\mathbb{K} = \Bbbk(\vartheta_1, \ldots, \vartheta_n)$.

Замечание. Если расширение полей $\mathbb{K}/\Bbbk$ является *чисто трансцендентным*, то $\mathbb{K} \setminus \Bbbk$ не содержит алгебраических над $\Bbbk$ элементов. Обратное, вообще говоря, неверно. Долгое время в математике оставалась нерешенной *проблема Люрота*: верно ли что промежуточное подполе $\mathbb{L}$, $\mathbb{K} \supset \mathbb{L} \supset \Bbbk$ в чисто трансцендентном расширении $\mathbb{K}/\Bbbk$ является чисто трансцендентным над $\Bbbk$? Проблема имеет отрицательное решение.

Определение. Предположим, что расширение $\mathbb{K}/\Bbbk$ конечно порождено. Если M – алгебраически независимое подмножество в $\mathbb{K}$ и если мощность M является наибольшей среди мощностей всех таких подмножеств, то мы будем называть эту мощность *степенью трансцендентности* расширения $\mathbb{K}$ над $\Bbbk$ и обозначать $\operatorname{degtr}_{\Bbbk} \mathbb{K}$ или просто $\operatorname{degtr} \mathbb{K}$, если это не приводит к путанице.

Лемма. *Пусть $\mathbb{K}$ – расширение поля $\Bbbk$. Если множество M порождает $\mathbb{K}$ над $\Bbbk$ (т. е. $\mathbb{K} = \Bbbk(M)$) и S – подмножество в M, алгебраически независимое над $\Bbbk$, то существует базис трансцендентности E поля $\mathbb{K}$ над $\Bbbk$ такой, что $S \subset E \subset M$.*

Доказательство. Мы рассмотрим только случай, когда множество M конечно. Пусть $M = \{\alpha_1, \ldots, \alpha_n\}$. После подходящей перенумерации мы можем считать, что $S = \{\alpha_1, \ldots, \alpha_r\}$, где элементы $\alpha_1, \ldots, \alpha_r$ алгебраически независимы, а каждая система $\alpha_1, \ldots, \alpha_r, \alpha_j$ для $j = r + 1, \ldots, n$ алгебраически зависима. Тогда элементы $\alpha_{r+1}, \ldots, \alpha_n$ алгебраичны над $\Bbbk(\alpha_1, \ldots, \alpha_r)$, а поэтому алгебраично и расширение $\mathbb{K}/\Bbbk$. Это означает, что $\alpha_1, \ldots, \alpha_r$ – базис трансцендентности. □

Следствие. *Если поле $\mathbb{K}$ конечно порождено над $\Bbbk$, то в $\mathbb{K}$ существует базис трансцендентности из конечного числа элементов.*

Следствие. *Если поле $\mathbb{K}$ конечно порождено над $\Bbbk$, то существует промежуточное поле $\mathbb{K} \supset \mathbb{L} \supset \Bbbk$ такое, что расширение $\mathbb{L}/\Bbbk$ чисто трансцендентно, а расширение $\mathbb{K}/\mathbb{L}$ конечно (и алгебраично).*

Заметим, что понятия степени трансцендентности и алгебраической независимости очень похожи на понятия размерности и линейной независимости в линейной алгебре. Однако следует сказать, что пользоваться этой аналогией следует очень осторожно. Например, различные базисы трансцендентности в одном расширении не могут быть алгебраически выражены друг через друга.

Теорема. *Пусть $\mathbb{K}$ – расширение поля $\Bbbk$. Любые два базиса трансцендентности $\mathbb{K}$ над $\Bbbk$ имеют одинаковую мощность.*

Доказательство. Мы докажем утверждение только в случае, когда $\mathbb{K}$ конечно порождено над $\Bbbk$. Тогда существует по крайней мере один конечный базис трансцендентности, скажем $\alpha_1, \ldots, \alpha_n$. По лемме (ниже) любой другой базис трансцендентности также должен содержать n элементов. Это доказывает теорему. □

Лемма (об алгебраической зависимости)**.** *Пусть $\mathbb{K}$ – расширение поля $\Bbbk$ и пусть $\alpha_1, \ldots, \alpha_n$ – базис трансцендентности для $\mathbb{K}/\Bbbk$. Если $\beta_1, \ldots, \beta_m$ – элементы из $\mathbb{K}$, алгебраически независимые над $\Bbbk$, то $m \leq n$.*

Доказательство. Предположим, что $m \geq n$. Мы можем считать, что $\alpha_1, \ldots, \alpha_n$ – базис трансцендентности из минимального числа элементов. По предположению существует ненулевой многочлен $f(t_1, \ldots, t_{n+1})$ с коэффициентами в $\Bbbk$, такой, что $f(\alpha_1, \ldots, \alpha_n, \beta_1) = 0$. Кроме того, по предположению t_{n+1} встречается в f и некоторая переменная t_i, $1 \leq i \leq n$, скажем t_1, также встречается в f. Тогда элемент α_1 алгебраичен над $\Bbbk(\beta_1, \alpha_2, \ldots, \alpha_n)$. Поэтому над $\Bbbk(\beta_1, \alpha_2, \ldots, \alpha_n)$ алгебраичен и любой элемент из поля $\Bbbk(\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_n)$. Таким образом, имеется башня алгебраических расширений

$$\Bbbk(\beta_1, \alpha_2, \ldots, \alpha_n) \subset \Bbbk(\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{K}$$

Следовательно, расширение $\mathbb{K}/\Bbbk(\beta_1, \alpha_2, \ldots, \alpha_n)$ является алгебраическим. По предыдущей лемме можно выбрать базис трансцендентности поля $\Bbbk(\beta_1, \alpha_2, \ldots, \alpha_n)$ над $\Bbbk$, содержащийся в множестве $\{\beta_1, \alpha_2, \ldots, \alpha_n\}$. Согласно сказанному выше, он будет базисом трансцендентности для $\mathbb{K}/\Bbbk$, а по нашему предположению о минимальности этот базис совпадает с $\beta_1, \alpha_2, \ldots, \alpha_n$. Заменяя α_1 на β_1, мы можем считать, что $\alpha_1 = \beta_1$.

Далее по индукции мы сведем утверждение к случаю $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$. Действительно, пусть $\alpha_1 = \beta_1, \ldots, \alpha_r = \beta_r$ для некоторого $1 \leq r \leq n$. Как и выше, существует ненулевой многочлен $g(t_1, \ldots, t_{n+1})$ с коэффициентами в $\Bbbk$, для которого $g(\beta_{r+1}, \alpha_1, \ldots, \alpha_n) = 0$, причем β_{r+1} действительно встречается в g. Так как все β_i алгебраически независимы над $\Bbbk$, то некоторый элемент α_j $(j = r+1, \ldots, n)$ также встречается в g. После перенумерации мы можем считать, что $j = r+1$. Тогда α_{r+1} алгебраичен над

$$\Bbbk(\beta_{r+1}, \alpha_1, \ldots, \widehat{\alpha_{r+1}}, \ldots, \alpha_n).$$

Следовательно, над этим полем алгебраичен и любой элемент из $\mathbb{K}$. Выберем базис трансцендентности из элементов $\beta_{r+1}, \alpha_1, \ldots, \widehat{\alpha_{r+1}}, \ldots, \alpha_n$. По нашему предположению о минимальности базиса

$$\beta_{r+1}, \alpha_1, \ldots, \widehat{\alpha_{r+1}}, \ldots, \alpha_n$$

– базис трансцендентности для $\mathbb{K}/\Bbbk$. Заменяя α_{r+1} на β_{r+1}, мы можем считать, что $\alpha_{r+1} = \beta_{r+1}$. Таким образом, мы можем считать, что $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$. Если $m > n$, то элемент β_{n+1} должен быть алгебраическим над $\Bbbk(\alpha_1, \ldots, \alpha_n) = \Bbbk(\beta_1, \ldots, \beta_n)$, что противоречит нашим предположениям. □

Мы, таким образом, доказали следующее: либо степень трансцендентности конечна и равна мощности любого другого базиса трансцендентности, либо она бесконечна, и тогда всякий базис трансцендентности бесконечен.

Задачи

17.1. Докажите, что поле действительных чисел $\mathbb{R}$ имеет бесконечную степень трансцендентности над $\mathbb{Q}$.

17.2. Пусть $\mathbb{K} = \Bbbk(t)/\Bbbk$ – чисто трансцендентное расширение степени трансцендентности 1. Докажите, что дробно-линейное отображение $\Bbbk(t) \to \Bbbk(t)$, заданное формулой

$$t \longmapsto \frac{at+b}{ct+d}, \qquad a,\, b,\, c,\, d \in \Bbbk,$$

является автоморфизмом тогда и только тогда, когда $ad - bc \neq 0$.

17.3. Пусть $\mathbb{K}/\Bbbk$ – расширение полей такое, что *каждый* элемент $\mathbb{K}$ трансцендентен над $\Bbbk$. Верно ли, что расширение чисто трансцендентно?

17.4. Пусть $\mathbb{K}/\Bbbk$ – конечно порожденное расширение полей. Докажите, что любое промежуточное подполе $\mathbb{L}$ конечно порождено над $\Bbbk$.

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА