Дополнительные главы алгебры

2023 - 2024

Оглавление

Глава 1

Свободные группы

1.1 Свободные абелевы группы

Пусть G — абелева группа. Тогда для любых элементов $a_1, \ldots, a_n \in G$ и целых чисел $k_1, \ldots, k_n \in \mathbb{Z}$ корректна определена линейная комбинация $k_1a_1 + \ldots + k_na_n \in G$. Здесь мы по определению считаем $k_ia_i = \underbrace{a_i + \ldots + a_i}_{k_i}$. При этом, если $a = \sum_i k_ia_i$ и $b = \sum_i l_ia_i$, то $a + b = \sum_i (k_i + l_i)a_i$.

Определение 1. *Пусть X — подмножество группы G. Будем говорить, что X* ***независимо****, если для любого конечного подмножества $\{x_1, \ldots, x_n\} \subseteq X$ линейная комбинация $k_1x_1 + \ldots + k_nx_n$ равна нулю тогда и только тогда, когда $k_1 = \ldots = k_n = 0$.*

Определение 2. *Пусть X — некоторое множество и есть семейство групп $\{G_x\}_{x\in X}$. Тогда* ***прямым произведением групп*** *G_x называется декартово произведение $\prod_{x\in X} G_x$, где умножение производится покоординатно.*

Прямой суммой *называется подгруппа $\sum_{x\in X} G_x \subseteq \prod_{x\in X} G_x$, состоящая из всех финитных последовательностей, то есть из тех последовательностей, у которых только конечное число координат не равно нейтральному элементу.*

Определение 3. *Пусть G — группа и $\{H_i\}_{i\in I}$ — семейство подгрупп в G. Зафиксируем некоторый линейный порядок на множестве I. Тогда будем говорить, что G есть* ***(внутренняя) прямая сумма*** *подгрупп H_i, если отображение*

$$\sum_{i\in I} H_i \to G,\ (h_i)_{i\in I} \to \prod_{i\in I} g_i$$

является изоморфизмом. В этом случае мы будем писать $G = \sum_{i\in I} H_i$.

Замечание 1. *По теореме Цермело, на I всегда есть линейный порядок.*

Задача 1. *Докажите, что определение 3 не зависит от выбора порядка на I.*

Как обычно, если X — подмножество группы G, то через $\langle X\rangle$ мы обозначаем подгруппу в G, порожденную X. Если $X = \emptyset$, то мы считаем, что $\langle X\rangle = \{e\}$.

Утверждение 1. *Пусть G — абелева группа и X — подмножество G. Тогда X независимо тогда и только тогда, когда $\langle X\rangle = \sum_{x\in X}\langle x\rangle$ и порядок всех элементов из X равен бесконечности.*

Задача 2. *Докажите утверждение 1.*

Определение 4. ***Свободной абелевой группой*** *называется абелева группа F_a, в которой есть независимое подмножество $X \subseteq F_a$, такое что $F_a = \langle X \rangle$. В этом случае говорят, что X* ***базис*** *F_a.*

Замечание 2. *Из утверждения 1 следует, что если F_a — свободная абелева группа с базисом X, то $F_a \simeq \sum_{x \in X} \mathbb{Z}$.*

Теорема 1. *(Универсальное свойство свободной абелевой группы)*
Пусть F_a — свободная абелева группа с базисом X. Тогда для любой абелевой группы G и отображения $f : X \to G$, существует единственный гомоморфизм $\varphi : F_a \to G$, такой что $\varphi(x) = f(x)$ для всех $x \in X$.

Обратно, пусть дана абелева группа H и подмножество $X \subseteq H$. Пусть для любой абелевой группы G и отображения $f : X \to G$ существует единственный гомоморфизм $\varphi : H \to G$, такой что $\varphi(x) = f(x)$. Тогда H свободная абелева группа с базисом X.

Доказательство. Докажем сначала прямое утверждение. Любой элемент $g \in F_a$ единственным образом представляется в виде линейной комбинации $g = \sum_{x \in X} k_x x$, где $k_x \in \mathbb{Z}$. Тогда положим

$$\varphi(g) = \sum_{x \in X} k_x f(x).$$

Легко видеть, что φ — единственный гомоморфизм из F_a в G, такой что $\varphi(x) = f(x)$ для всех $x \in X$.

Докажем обратное утверждение. Пусть F_a — свободная абелева группа с базисом X. Рассмотрим тождественное отображение $\mathrm{id}_X : X \to X$. Тогда существует единственный гомоморфизм $\varphi : H \to F_a$, такой что $\varphi(x) = x$ для всех $x \in X$. Так как мы уже доказали, что группа F_a удовлетворяет универсальному свойству, то мы можем утверждать, что существует единственный гомоморфизм $\psi : F_a \to H$, такой что $\psi(x) = x$ для всех $x \in X$. Тогда композиция $\psi \circ \varphi$ является гомоморфизмом из H в H, который продолжает тождественное отображение $\mathrm{id}_X : X \to X$. Мы знаем, что тождественный гомоморфизм продолжает тождественное отображение. В силу единственности мы получаем, что $\psi \circ \varphi = \mathrm{id}_H$.

Аналогично, $\varphi \circ \psi$ — тождественное отображение на F_a. Поэтому φ изоморфизм и $H \simeq F_a$. Так как X базис F_a, то X и базис H.

□

Следствие 1. *Любая абелева группа является факторгруппой некоторой свободной абелевой группы.*

Доказательство. Рассмотрим множество $X_G = \{x_g | g \in G\}$. Пусть F_a свободная абелева группа с базисом X_G. Тогда отображение

$$f : X_g \to G,\ x_g \to g$$

единственным образом продолжается до гомоморфизма $\varphi : F_a \to G$. При этом φ — сюръективный гомоморфизм, так как f — сюръективно. По теореме о гомоморфизме $G \simeq F_a/\mathrm{Ker}\ \varphi$. □

Определение 5. *Говорят, что абелева группа G* ***задается порождающими X и соотношениями*** *Δ, если $G \simeq F_a/R$, где F_a — свободная абелева группа с базисом X, Δ — некоторое множество линейных комбинаций элементов из X и R — подгруппа в F_a, порожденная Δ. Пару (X, Δ) также называют* ***копредставлением*** *абелевой группы G. Также пишут $G = \langle X \mid \Delta \rangle_a$.*

Пример 1. *$\mathbb{Z}_6 = \langle x \mid 6x \rangle_a$. Действительно, в этом случае $F_a = \langle x \rangle \simeq \mathbb{Z}$ и $R = \langle 6x \rangle = 6\mathbb{Z}$ и $F_a/R \simeq \mathbb{Z}_6$.*

Пример 2. $\mathbb{Z}_6 = \langle x, y \mid 2x, 3y\rangle_a$. *Здесь* $F_a = \langle x\rangle \oplus \langle y\rangle \simeq \mathbb{Z} \oplus \mathbb{Z}$ *и* $R = \langle 2x\rangle \oplus \langle 3y\rangle = 2\mathbb{Z} \oplus 3\mathbb{Z}$ *и* $F_a/R \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

Задача 3. *Пусть* $X = \{x_i \mid i \in \mathbb{N}\}$. *Докажите, что* $\mathbb{Q} = \langle X \mid x_1 - 2x_2, x_2 - 3x_3, \ldots, x_{n-1} - nx_n, \ldots\rangle_a$.

Теорема 2. *Пусть* F_a *— свободная абелева группа с базисом* X *и* G_a *— свободная абелева группа с базисом* Y. *Тогда* F_a *изоморфна* G_a *тогда и только тогда, когда* $|X| = |Y|$.

Доказательство. Пусть $|X| = |Y|$. Тогда существует биекция $f : X \to Y$. Из универсального свойства следует, что существует гомоморфизм : $F_a \to G_a$, который продолжает f и существует гомоморфизм $\psi : G_a \to F_a$, который продолжает f^{-1}. Тогда композиция $\psi \circ \varphi$ продолжает тождественное отображение id_X и поэтому является тождественным гомоморфизмом id_{F_a}, а композиция $\varphi \circ \psi$ продолжает отображение id_{G_a} и является тождественным гомоморфизмом id_{G_a}. Следовательно, φ изоморфизм.

Теперь предположим, что F_a и G_a изоморфны. Для некоторого простого числа p рассмотрим подгруппу $pF_a = \{pg | g \in F_a\} \subseteq F_a$. Тогда факторгруппа F_a/pF_a является векторным пространством над полем $\mathbb{Z}_p$. Рассмотрим систему $\overline{X} = \{x + pF_a \mid x \in X\}$. Докажем, что $\overline{X}$ — базис F_a/pF_a.

Пусть $\sum_{x\in X} \overline{m_x}(x + pF_p) = 0$, $(\overline{m_x} \in \mathbb{Z}_p)$. Тогда $\sum_{x\in X} m_x x \in pF_a$. Так как $F_a \simeq \sum_{x\in X} \mathbb{Z}$, то отсюда следует, что все числа m_x делятся на p. Но тогда $\overline{m_x} = 0$. Следовательно, элементы $\overline{X}$ линейно независимы.

С другой стороны, для любого элемента g найдутся такие целые числа k_x, что $g = \sum_{x\in X} k_x x$. Но тогда $g + pF_p = \sum_{x\in X} \overline{k_x}(x + pF_a)$. Отсюда следует, что $\overline{X}$ порождает F_a/pF_a. Поэтому $|X| = |\overline{X}| = \dim_{\mathbb{Z}_p} F_a/pF_a$. Аналогично, $|Y| = \dim_{\mathbb{Z}_p} G_a/pG_a$. Так как $F_a \simeq G_a$, то векторные пространства F_a/pF_a и G_a/pG_a изоморфны, а следовательно $|X| = |Y|$.

□

Замечание 3. *В доказательстве выше мы воспользовались тем фактом, что у векторного пространства все базисы равномощны. В конечномерном случае это доказывается в курсе линейной алгебры. В бесконечномерном случае над конечным полем это упражнение на теорию множеств.*

Следствие 2. *Любые два базиса свободной абелевой группы равномощны.*

Определение 6. ***Рангом*** *свободной абелевой группы называется мощность ее базиса.*

Теорема 3. *(Проективное свойство свободной абелевой группы)*
Пусть $\beta : B \to C$ *— сюръективный гомоморфизм между абелевыми группами,* F_a *— свободная абелева группа и* $\alpha : F_a \to C$ *— гомоморфизм. Тогда существует гомоморфизм* $\gamma : F_a \to B$, *такой что* $\alpha = \beta \circ \gamma$.

Доказательство. Пусть X — базис F_a. Тогда для любого $x \in X$ существует $b_x \in B$, такой что $\beta(b_x) = \alpha(x)$. Имеем отображение

$$f : X \to B,\ x \to b_x.$$

Из универсального свойства следует, что существует гомоморфизм $\gamma : F_a \to B$, который продолжает f. Гомоморфизмы α и $\beta \circ \gamma$ продолжают отображение $f' : X \to C,\ x \to \alpha(x)$. Поэтому $\alpha = \beta \circ \gamma$. □

Следствие 3. *Пусть* G *— абелева группа,* $H \leq G$ *и* G/H *— свободная абелева группа. Тогда существует подгруппа* $K \leq G$, *такая что* $G = H \oplus K$.

Доказательство. Применим теорему 3. Положим $F_a = C = G/H, B = G$, в качестве α возьмем тождественное отображение, а в качестве β возьмем канонический гомоморфизм $\pi_H : g \to gH$. Тогда существует гомоморфизм $\gamma : G/H \to G$, такой что $\alpha = \beta \circ \gamma$. Возьмем в качестве $K = \operatorname{Im} \gamma$. Нетрудно убедиться, что $K \cap H = \{e\}$ и $G = K + H$. □

Теорема 4. *Пусть F_a — свободная абелева группа и $H \leq F_a$. Тогда H — свободная абелева группа и* $\operatorname{rk} H \leq \operatorname{rk} F_a$.

Доказательство. Пусть $\{x_i | i \in I\}$ — базис F_a. Согласно теореме Цермело на I есть линейный порядок $\leq$, такой что I является вполне упорядоченным множеством. Для всех $i \in I$ положим $F'_i = \langle x_j \mid j < i \rangle$ и $F_i = \langle x_j \mid j \leq i \rangle = F'_i \oplus \langle x_i \rangle$.

Положим $H'_i = H \cap F'_i$ и $H_i = H \cap F_i$. Заметим, что $F = \cup F_i,\ H = \cup H_i$. Имеем $H'_i = H \cap F'_i = H_i \cap F'_i$. Тогда

$$H_i/H'_i = H_i/(H_i \cap F'_i) \simeq (H_i + F'_i)/F'_i \leq F_i/F'_i \simeq \mathbb{Z}.$$

Здесь первый изоморфизм следует из второй теоремы о гомоморфизме. Второй изоморфизм из того, что $F_i = F'_i \oplus \langle x_i \rangle$.

Любая подгруппа $F_i/F'_i \simeq \mathbb{Z}$ либо тривиальна, либо изоморфна $\mathbb{Z}$. Поэтому H_i/H'_i либо тривиальная группа, либо изоморфна $\mathbb{Z}$. В первом случае $H_i = H'_i$. Во втором случае, по следствию 3 существует такое $h_i \in H_i$, что $H_i = H'_i \oplus \langle h_i \rangle$.

Для каждого $i \in I$ мы либо построили h_i, либо $H_i = H'_i$. Докажем, что множество всех h_i — базис H.

Так как $F_a = \cup_i F_i$, то для любого $h \in H$ существует $i \in I$, такое что $h \in F_i$. Положим

$$\mu(h) = \min\{i \in I \mid h \in F_i\}.$$

Пусть H^* — подгруппа в H, порожденная элементами h_i. Предположим, что $H^* \neq H$. Положим

$$j = \min\{\mu(h) \mid h \in H \text{ и } h \notin H^*\}.$$

Существует $h' \in H$, такой что $h' \notin H^*$ и $\mu(h') = j$. Так как $\mu(h') = j$ то $h' \in H \cap F_j = H_j$. Следовательно, $h' = a + mh_j$ для некоторого $a \in H'_j, m \in \mathbb{Z}$. (Здесь, если для данного j мы не строили соответствующее h_j, то мы берем $m = 0$). Тогда $a = h' - mh_j \in H$ и $a \notin H^*$. При этом $\mu(a) < j$, что противоречит выбору j. Следовательно, $H = H^*$.

Докажем, что множество $\{h_i\}$ независимо. Пусть

$$k_{i_1} h_{i_1} + \ldots + k_{i_n} h_{i_n} = 0,$$

где $i_1, \ldots, i_n \in I, i_1 < i_2 < \ldots < i_n$ и $k_{i_1}, \ldots, k_{i_n} \in \mathbb{Z}$. Тогда

$$k_{i_n} h_{i_n} \in \langle h_{i_n} \rangle \cap H'_{i_n}.$$

Последнее противоречит построению h_{i_n}.

Значит множество $\{h_i\}$ является базисом H, при этом мощность множества $\{h_i\}$ не превосходит мощность базиса F_a. □

Задача 4. *Докажите, что группа $(\mathbb{Q}_{>0}, \cdot)$ является свободной абелевой группой. Какой в ней базис?*

Задача 5. *Является ли группа $(\mathbb{Q}^*, \cdot)$ свободной? Является ли группа $(\mathbb{Q}, +)$ свободной?*

Задача 6. *Пусть $X = \{x_i \mid i \in \mathbb{N}\}$ и p — простое число. Рассмотрим группу $G = \langle X \mid px_1, x_1 - px_2, x_2 - px_3, \ldots, x_n - px_{n+1}, \ldots \rangle_a$. Докажите, что G изоморфна группе*

$$U_{p^\infty} = \{z \in \mathbb{C}^* \mid \exists k \in \mathbb{N}\ z^{p^k} = 1\}.$$

1.2 Свободные группы

Определение 7. *Пусть F — группа и $X \subseteq F$ — подмножество. Будем называть F* ***свободной группой с базисом*** *X, если для любой группы G и отображения $f : X \to G$ существует единственный гомоморфизм $\varphi : F \to G$, такой что $\varphi(x) = f(x)$ для всех $x \in X$.*

Сейчас мы построим свободную группу. Пусть $\mathcal{A}$ — некоторое множество и $X = \{x_\alpha\}_{\alpha\in\mathcal{A}}$ — алфавит. Для каждого символа x_α из алфавита X введем "обратный" элемент x_α^{-1} и обозначим через X^{-1} множество $\{x_\alpha^{-1}\}_{\alpha\in\mathcal{A}}$.

Словом будем обозначать последовательность элементов из $X \sqcup X^{-1}$:

$$x_1^{\epsilon_1} \dots x_n^{\epsilon_n},$$

где $\epsilon_i \in \{\pm\}$. Пустое слово будем обозначать 1 или $\emptyset$. Длиной слова называется длина соответствующей последовательности, то есть длина слова $x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ равна n. **Обратным словом** к слову $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ будем называть слово $w^{-1} = x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1}$.

Слово w называется **приведенным,** если в w нет подслов вида $x^\epsilon x^{-\epsilon}$. **Произведением слов** $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ и $u = y_1^{\delta_1} \dots y_m^{\delta_m}$ будем называть слово $wu = x_1^{\epsilon_1} \dots x_n^{\epsilon_n} y_1^{\delta_1} \dots y_m^{\delta_m}$. Легко видеть, что произведение ассоциативно. Однако множество слов относительно этой операции не является группой, так как ни у какого непустого слова нет обратного.

Пусть w и u приведенные слова. Обозначим через v слово максимальной длины, такое что $w = w_1 v,\ u = v^{-1} u_1$, где w_1, u_1 некоторые приведенные слова. **Произведением с сокращением** приведенных слов w и u называется слово $w_1 u_1$. Легко видеть, что $w_1 u_1$ также приведенное слово. Относительно произведения с сокращением уже все приведенные слова имеют обратные. Однако теперь неочевидно, что это произведение ассоциативно.

Введем на множестве всех слов отношение эквивалентности, порожденное отношениями

$$x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \sim x_1^{\epsilon_1} \dots x_i^{\epsilon_i} x^\epsilon x^{-\epsilon} x_{i+1}^{\epsilon_{i+1}} \dots x_n^{\epsilon_n}.$$

Утверждение 2. *Каждый класс эквивалентности содержит ровно одно приведенное слово.*

Доказательство. (Трюк Ван дер Вардена.) Обозначим через F множество всех приведенных слов. Для каждого $x \in X$ определим отображения

$$|x^\epsilon| : F \to F,\ |x^\epsilon|(x_1^{\epsilon_1} \dots x_n^{\epsilon_n}) = \begin{cases} x^\epsilon x_1^{\epsilon_1} \dots x_n^\epsilon, & x^\epsilon \neq x_1^{-\epsilon_1} \\ x_2^{\epsilon_2} \dots x_n^\epsilon, & x^\epsilon = x_1^{-\epsilon_1} \end{cases}.$$

Заметим, что $|x^\epsilon| \circ |x^{-\epsilon}| = |x^{-\epsilon}| \circ |x^\epsilon| = \mathrm{id}_F$. Поэтому $|x^\epsilon|$ биекция на множестве F.

Для произвольного (не обязательно приведенного) слова $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ определим отображение

$$|w| = |x_1^{\epsilon_1}| \circ \dots \circ |x_n^{\epsilon_n}|.$$

Легко видеть, что если $w \sim w_1$, то $|w| = |w_1|$. Если w и w_1 два приведенных эквивалентных слова, то $|w| = |w_1|$, но $|w|(1) = w$, а $|w_1|(1) = w_1$. □

Умножение слов конгруэнтно относительно заданного отношения эквивалентности, то есть, если $w \sim w_1, u \sim u_1$, то $wu \sim w_1 u_1$. Таким образом корректно определено умножение классов эквивалентности, которое также будет ассоциативно. Заметим, что результат умножения с сокращением двух приведенных слов w и u является единственным приведенным словом эквивалентным слову wu. Так как индуцированное умножение на классах эквивалентности ассоциативно, то умножение с сокращением тоже ассоциативно.

Следствие 4. *Множество F всех приведенных слов с операцией "умножение с сокращением" является группой.*

Замечание 4. *Про F можно думать как про множество приведенных слов с операцией "умножение с сокращением" , а можно думать как про множество классов эквивалентности с умножением индуцированным с обычного умножения слов.*

Теорема 5. *F — свободная группа с базисом X.*

Доказательство. Пусть G — группа и $f : X \to G$ — отображение. Положим $g_\alpha = f(x_\alpha)$. Тогда легко проверить, что отображение

$$\varphi : F \to G,\ \varphi(x_1^{\epsilon_1} \dots x_n^{\epsilon_n}) = g_1^{\epsilon_1} \dots g_n^{\epsilon_n}$$

единственный гомоморфизм, который продолжает f. □

Утверждение 3. *Любая группа — факторгруппа свободной группы.*

Доказательство. Такое же, как и в абелевом случае. □

Определение 8. *Пусть X — множество и Δ некоторое подмножество слов, составленное из элементов $X \sqcup X^{-1}$. Говорят, что группа G задана порождающими X и соотношениями Δ, если $G \simeq F/R$, где F группа приведенных слов, составленных из $X \sqcup X^{-1}$, а R — нормальное замыкание множества Δ в F. Обозначение: $G = \langle X|\Delta\rangle$. Пару $\langle X|\Delta\rangle$ также называют* ***копредставлением*** *группы G. Часто вместо $\langle X|w_1, \dots, w_s\rangle$ пишут $\langle X|w_1 = 1, \dots, w_s = 1\rangle$ или $\langle X|u_1 = v_1, \dots, u_s = v_s\rangle$, где $w_i = u_i v_i^{-1}$.*

Пример 3. $\mathbb{Z}_6 = \langle x \mid x^6 = 1\rangle$;

Пример 4. $\mathbb{Z}_6 = \langle x, y \mid x^3 = 1, y^2 = 1, xyx^{-1}y^{-1} = 1\rangle$;

Доказательство. Пусть $F = F(x, y)$ — группа приведенных слов на алфавите $X = \{x, y\}$. Рассмотрим отображение $f : X \to \mathbb{Z}_6,\ f(x) = \overline{2},\ f(y) = \overline{3}$. Тогда существует гомоморфизм $\varphi : F \to \mathbb{Z}_6$, продолжающий f. Ядро этого гомоморфизма содержит x^3, y^2 и $xyx^{-1}y^{-1}$. Поэтому $\mathrm{Ker}\ \varphi \supseteq R$. Имеем

$$F/\mathrm{Ker}\ \varphi \simeq \mathbb{Z}_6 \simeq (F/R)/(\mathrm{Ker}\ \varphi/R).$$

Каждый смежный класс из F/R равен смежному классу вида $x^a y^b R$, где $0 \le a \le 2,\ 0 \le b \le 1$. Поэтому $|F/R| \le 6$. Отсюда следует, что $R = \mathrm{Ker}\ \varphi$. □

Задача 7. *Докажите, что $D_n = \langle x, y \mid x^n = 1, y^2 = 1, yxy = x^{-1}\rangle$. Здесь x соответствует повороту на угол $\frac{2\pi}{n}$, а y соответствует любой симметрии.*

Задача 8. *Докажите, что $Q_8 = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1}\rangle$. Здесь x соответствует элементу i, y соответствует элементу j.*

Пример 5. *Свободная абелева группа F_a имеет копредставление $F_a = \langle X \mid xyx^{-1}y^{-1},\ \forall x, y \in X\rangle$.*

Пример 6. $S_n = \langle \sigma_1, \dots, \sigma_{n-1} \mid \sigma_i^2 = 1,\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ \sigma_i\sigma_j = \sigma_j\sigma_i,\ \text{при } |i-j| > 1\rangle$. *Здесь σ_i соответствует транспозиции $\sigma_i = (i, i+1)$.*

Пример 7. $A_n = \langle s_3, \dots, s_n \mid s_i^3 = 1,\ (s_i s_j)^2 = 1\rangle$. *Здесь s_i соответствует циклу $s_i = (12i)$.*

Определение 9. *Пусть $G_1 = \langle X_1 \mid \Delta_1\rangle$ и $G_2 = \langle X_2 \mid \Delta_2\rangle$. Определим* ***свободное произведение*** *групп G_1 и G_2 как группу*

$$G_1 * G_2 = \langle X_1 \sqcup X_2 \mid \Delta_1 \sqcup \Delta_2\rangle.$$

Замечание 5. *Вообще говоря, такое определение нуждается в доказательстве корректности. А именно нужно доказать, что $G_1 * G_2$ не зависит от выбора копредставлений G_1 и G_2. Однако мы здесь опустим доказательство корректности.*

Задача 9. *Докажите, что группа $\mathbb{Z}_2 * \mathbb{Z}_2$ бесконечна.*

Следующее предложение показывает, что, зная копредставление некоторой группы, удобно определять гомоморфизмы из этой группы.

Утверждение 4. *Пусть $G = \langle X \mid \Delta \rangle$ и H — некоторая группа. Рассмотрим отображение $f : X \to H$, такое что для любого $w \in \Delta$, $f(w) = e_H$. Тогда существует единственный гомоморфизм $\varphi : G \to H$, такой что $\varphi(xR) = f(x)$.*

Доказательство. Существует единственный гомоморфизм $\overline{\varphi} : F \to H$, такой что $\overline{\varphi}(x) = f(x)$. Тогда $\operatorname{Ker} \overline{\varphi}$ содержит Δ, а значит и R. Отсюда следует, что $\overline{\varphi}$ пропускается через $G = F/R$, то есть существует гомоморфизм $\varphi : F/R \to H$, такой что $\overline{\varphi} = \varphi \circ \pi_R$, где $\pi_R : F \to F/R$ гомоморфизм факторизации.

Если $\varphi' : G \to H$ другой гомоморфизм, такой что $\varphi'(xR) = f(x)$, то $\varphi' \circ \pi_R$ — еще один гомоморфизм из $F \to H$, который продолжает f. □

Лемма 1. *Пусть F — свободная группа с базисом X. Тогда F/F' — свободная абелева группа с базисом $X_\# = \{xF' \mid x \in X\}$.*

Замечание 6. *Заметим, что $xF' = yF'$ для элементов $x, y \in X$ тогда и только тогда, когда $x = y$. Действительно, рассмотрим произвольную абелеву группу A и рассмотрим произвольное отображение $f : X \to A$, при котором $f(x) \neq f(y)$. Тогда существует гомоморфизм $\varphi : F \to A$, который продолжает f. Но любой гомоморфизм из F в абелеву группу пропускается через F/F'. Поэтому $xF' \neq yF'$.*

Доказательство. (Леммы 1)

Рассмотрим абелеву группу A и отображение $f : X_\# \to A$. Определим отображение $\overline{f} : X \to A$ по правилу $\overline{f}(x) = f(xF')$. Тогда существует гомоморфизм $\varphi : F \to A$, который продолжает $\overline{f}$. Тогда φ пропускается через F/F', то есть существует гомоморфизм $\overline{\varphi} : F/F' \to A$, такой что $\varphi = \overline{\varphi} \circ \pi_{F'}$, где $\pi_{F'} : F \to F/F'$ гомоморфизм факторизации. При этом $\overline{\varphi}(xF') = \varphi(x) = \overline{f}(x) = f(xF')$. Поэтому $\overline{\varphi}$ продолжает отображение f.

Пусть есть другой гомоморфизм $\theta : F/F' \to A$, который продолжает отображение f. Но тогда $\theta \circ \pi_{F'}$ — гомоморфизм из F в A, который продолжает $\overline{f}$. Отсюда следует, что $\theta \circ \pi_{F'} = \overline{\varphi} \circ \pi_{F'}$. Так как $\pi_{F'}$ сюръективно, то $\theta = \overline{\varphi}$.

Мы доказали, что F/F' вместе с подмножеством $X_\#$ удовлетворяют универсальному свойству свободных абелевых групп. Поэтому F/F' свободная абелева группа, а $X_\#$ её базис.

□

Теорема 6. *Пусть F и G — свободные группы с базисами X и Y соответственно. Тогда $F \simeq G$ тогда и только тогда, когда $|X| = |Y|$.*

Доказательство. Пусть F и G изоморфны. Тогда $F/F' \simeq G/G'$. Пользуясь леммой 1 и теоремой 2 получаем, что $|X| = |X_\#| = |Y_\#| = |Y|$.

Если $|X| = |Y|$, то аналогично абелевому случаю доказываем, что $F \simeq G$.

□

Определение 10. ***Рангом*** *свободной группы F называется мощность базиса X.*

Следствие 5. *Любая свободная группа с базисом X изоморфна группе приведенных слов на алфавите X. В частности, свободная группа с базисом X порождается X.*

Теорема 7. *(Проективное свойство свободных групп)*
Пусть $\beta : B \to C$ — сюръективный гомоморфизм между группами, F — свободная группа и $\alpha : F \to C$ — гомоморфизм. Тогда существует гомоморфизм $\gamma : F \to B$, такой что $\alpha = \beta \circ \gamma$.

Доказательство. Доказательство аналогично доказательству абелевого случая. □

Следствие 6. *Пусть G — группа и H — нормальная подгруппа в G. Предположим, что факторгруппа G/H свободна. Тогда существует подгруппа K в G, такая что $G = H \leftthreetimes K$.*

Доказательство. Воспользуемся теоремой 7. Положим $F = C = G/H,\ B = G, \alpha = \mathrm{id}_{G/H},\ \beta = \pi_H$. Тогда существует гомоморфизм $\gamma : G/H \to G$, такой что $\mathrm{id}_{G/H} = \pi_H \circ \gamma$. Положим $K = \mathrm{Im}\ \gamma$. Легко видеть, что $K \cap H = \{e\}$ и $KH = G$. Поэтому $G = H \leftthreetimes K$. □

Задача 10. *Пусть F — свободная группа. Докажите, что существует автоморфизм $\varphi : F \to F$, такой что $\varphi^2 = \mathrm{id}_F$ и $\varphi(x) = x$, только если $x = e$.*

1.3 Комплексы. Теорема Титце

Определение 11. *Пусть V — множество и K — семейство непустых конечных подмножеств в V. Тогда K называется* комплексом, *если выполнены следующие свойства:*

1. *Если $v \in V$, то множество $\{v\} \in K$;*
2. *Если множество $s \in K$, то все подмножества s также принадлежат K.*

Множество V называется **множеством вершин** комплекса K и обозначается $\mathrm{Vert}(K)$. Подмножества $s \in K$ называются **симплексами.** Если $|s| = q + 1$, то говорят, что **размерность** s равна q. **Размерностью комплекса** K называется число

$$\dim K = \sup_{s \in K} \dim s.$$

Размерность комплекса может быть равна бесконечности.

Определение 12. *Последовательность вершин $\alpha = (v_0, v_1, \ldots, v_n),\ v_i \in V$ называется **путем** в K, если для любого i множество $\{v_i, v_{i+1}\}$ является симплексом. Мы всегда считаем, что $n \geq 1$.*

Вершина v_0 называется **началом** пути α и обозначается $o(\alpha)$, а вершина v_n называется **концом** пути α и обозначается $e(\alpha)$. Комплекс K называется **связным**, если для любых двух вершин $u, w \in V$ существует путь α в K, такой что $o(\alpha) = u$ и $e(\alpha) = w$.

Утверждение 5. *Любой комплекс K единственным образом представляется в виде $K = \sqcup K_i$, где K_i — связные комплексы.*

Доказательство. K_i — максимальные по включению связные подкомплексы в K. □

Подмножества K_i называются **компонентами связности** K.

Пусть есть два пути $\alpha = (v_0, \ldots, v_n)$ и $w = (w_0 = v_n, w_1, \ldots, w_n)$. Тогда определим их произведение следующим образом:

$$\alpha\beta = (v_0, \ldots, v_n, w_1, \ldots, w_n).$$

Введем на множестве всех путей в K отношение эквивалентности, порожденное отношениями

$$(v_0, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n) \sim (v_0, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n),$$

если $\{v_{i-1}, v_i, v_{i+1}\} \in K$. Класс эквивалентности пути α будем обозначать $[\alpha]$. Заметим, что если $\alpha \sim \alpha_1$ и $\beta \sim \beta_1$, то $\alpha\beta \sim \alpha_1\beta_1$. Поэтому корректно определено произведение классов эквивалентности $[\alpha][\beta] = [\alpha\beta]$.

Эквивалентные пути имеют одинаковые начала и концы. Поэтому можно определить начало и конец класса эквивалентности: $o([\alpha]) = o(\alpha),\ e([\alpha]) = e(\alpha)$.

Определение 13. ***Фундаментальной группой*** *комплекса K в точке w называется группа $\pi(K, w)$ — группа классов эквивалентности путей $[\alpha]$, для которых $o([\alpha]) = e([\alpha]) = w$.*

Легко убедиться, что $\pi(K, w)$ действительно группа, где $e = [(w, w)]$ и $[(v_0, \ldots, v_n)]^{-1} = [(v_n, \ldots, v_0)]$.

Теорема 8. *Пусть K_i — компонента связности комплекса K и $v, w \in \mathrm{Vert}(K_i)$. Тогда*

$$\pi(K, v) \simeq \pi(K, w) \simeq \pi(K_i, w) \simeq \pi(K_i, v).$$

Доказательство. Первый изоморфизм устанавливается отображением

$$[\alpha] \to [\gamma]^{-1}[\alpha][\gamma],$$

где γ — путь, соединяющий v и w. Второй изоморфизм следует из того, что любой путь в K с началом и концом в w содержится в K_i. Третий изоморфизм доказывается так же, как и первый. □

Определение 14. *Отображение $\varphi : K \to L$ называется* ***симплициальным****, если существует отображение $\overline{\varphi} : \mathrm{Vert}(K) \to \mathrm{Vert}(L)$, такое что $\varphi(\{v_0, \ldots, v_n\}) = \{\overline{\varphi}(v_0), \ldots, \overline{\varphi}(v_n)\}$, где $s = \{v_0, \ldots, v_n\}$ — симплекс в K. Заметим, что при этом $\{\overline{\varphi}(v_0), \ldots, \overline{\varphi}(v_n)\}$ симплекс в L.*

Далее мы будем все время отождествлять φ и $\overline{\varphi}$.

Теорема 9. *Пусть $\varphi : K \to L$ — симплициальное отображение между комплексами K и L. Тогда отображение*

$$\varphi : \pi(K, v) \to \pi(L, \varphi(v)),\ [\alpha] \to [\varphi(\alpha)]$$

корректно определено и является гомоморфизмом.

Доказательство. Тривиальная проверка. □

Пусть называется **приведенным**, если он не содержит подпутей вида (v, w, v) или (v, v). Однако тривиальный путь $\alpha = (v, v)$ мы будем считать приведенным. Каждый путь эквивалентен приведенному. **Цикл** — приведенный путь α, такой что $o(\alpha) = e(\alpha)$. **Дерево** — связный комплекс без нетривиальных циклов. Дерево имеет размерность 1 или 0. В последнем случае это просто точка. В дереве любые две вершины соединены единственным приведенным путем.

Связный комплекс K называется **односвязным**, если $\pi(K, v) = \{e\}$ для какой-то (любой) вершины $v \in \mathrm{Vert}(K)$. Дерево всегда односвязный комплекс.

Утверждение 6. *Пусть K — связный комплекс и T — максимальное по включению дерево в K. Тогда* $\mathrm{Vert}(K) = \mathrm{Vert}(T)$.

Доказательство. Предположим, что есть вершина $v \in \mathrm{Vert}(K) \setminus \mathrm{Vert}(T)$. Возьмем точку $w \in \mathrm{Vert}(T)$. Тогда есть пусть α в K, такой что $o(\alpha) = w$ и $e(\alpha) = v$. Пусть u — первая точка в α, которая не лежит в $\mathrm{Vert}(T)$. Легко проверить, что если мы добавим точку u в T вместе с ребром, соединяющим u с некоторой точкой из T, то получим дерево, содержащее T. □

Пусть K — связный комплекс и T — максимальное дерево в K. Определим группу $\mathcal{T}(K,T)$ с помощью копредставления. В качестве множества порождающих X возьмем все пути в K из двух вершин:

$$X = \{(v,w) \in K\}.$$

И рассмотрим соотношения Δ, которые бывают двух типов:

Тип а. $(v,w) = 1$, если $(v,w) \in T$.

Тип б. $(v,w)(w,u) = (v,u)$, если $\{v,w,u\}$ — симплекс в K.

Тогда по определению положим $\mathcal{T}(K,T) = \langle X|\Delta\rangle$.

Теорема 10. *(Теорема Титце) Пусть K — связный комплекс, T — максимальное дерево в K и $w \in \mathrm{Vert}(K)$. Тогда $\pi(K,w) \simeq \mathcal{T}(K,T)$.*

Доказательство. Так как T — максимальное дерево, то для любой вершины $v \in \mathrm{Vert}(T) = \mathrm{Vert}(K)$, существует единственный приведенный путь λ_v в T, такой что $o(\lambda_v) = w$ и $e(\lambda_v) = v$. Рассмотрим свободную группу F с базисом X и отображение

$$f : X \to \pi(K,w),\ (u,v) \to [\lambda_u(u,v)\lambda_v^{-1}].$$

Тогда существует гомоморфизм $\varphi : F \to \pi(K,w)$, который продолжает f. Пусть R — нормальное замыкание в F соотношений Δ. Тогда $\mathcal{T}(K,T) = F/R$.

Заметим, что $R \leq \mathrm{Ker}\ \varphi$. Действительно, если $(v,u) \in T$, то путь $\lambda_u(u,v)\lambda_v^{-1}$ содержится в T, а так как T односвязный комплекс, то $[\lambda_u(u,v)\lambda_v^{-1}] = [(w,w)] = e \in \pi(K,w)$. Поэтому $\varphi((u,v)) = f((u,v)) = e$. Следовательно, все соотношения типа а из Δ содержатся в $\mathrm{Ker}\ \varphi$.

Если же $\{v,u,p\} \in K$, то

$$\varphi((v,u)(u,p)) = f((v,u))f((u,p)) = [\lambda_v(v,u)\lambda_u^{-1}][\lambda_u(u,p)\lambda_p^{-1}] = [\lambda_v(v,u,p)\lambda_p^{-1}] =$$

$$= [\lambda_v(v,p)\lambda_p^{-1}] = f((v,p)) = \varphi((v,p)).$$

Здесь первое равенство следует из того, что гомоморфизм φ продолжает отображение f, четвертое равенство следует из определения эквивалентных путей, остальные равенства тривиальные. Отсюда следует, что $\varphi((v,u)(u,p)(v,p)^{-1}) = e$, поэтому соотношения типа б также содержатся в $\mathrm{Ker}\ \varphi$. Следовательно, $\mathrm{Ker}\ \varphi$ содержит R.

Тогда гомоморфизм φ можно пропустить через факторгруппу F/R, то есть существует гомоморфизм $\overline{\varphi} : F/R \to \pi(K,w)$, такой что $\varphi = \overline{\varphi} \circ \pi_R$, где $\pi_R : F \to F/R$ — канонический гомоморфизм факторизации.

Докажем, что $\overline{\varphi}$ — изоморфизм. Рассмотрим отображение

$$\theta((v_0 = w, v_1, \ldots, v_n = w)) = (v_0,v_1)(v_1,v_2)\ldots(v_{n-1},v_n)R.$$

Заметим, что если $\{v_{i-1},v_i,v_{i+1}\} \in K$, то $(v_{i-1},v_i)(v_i,v_{i+1})R = (v_{i-1},v_{i+1})R$, так как R содержит соотношения типа б. Поэтому, если $\alpha \sim \beta$, то $\theta(\alpha) = \theta(\beta)$. Поэтому корректно определено отображение

$$\overline{\theta} : \pi(K,w) \to F/R,\ \ \overline{\theta}([\alpha]) = \theta(\alpha).$$

Проверим, что $\overline{\theta} \circ \overline{\varphi}$ и $\overline{\varphi} \circ \overline{\theta}$ тождественные отображения.

$$\overline{\varphi} \circ \overline{\theta}([\alpha]) = \overline{\varphi} \circ \overline{\theta}([(v_0 = w, v_1, \ldots, v_n = w)]) = \overline{\varphi}((w,v_1)\ldots(v_{n-1},w)R) =$$

$$= \varphi((w,v_1)\ldots(v_{n-1},w)) = [\lambda_w(w,v_1)\lambda_{v_1}^{-1}]\ldots[\lambda_{v_{n-1}}(v_{n-1},w)\lambda_w^{-1}] = [\lambda_w\alpha\lambda_w^{-1}] = [\alpha].$$

Аналогично,

$$\overline{\theta} \circ \overline{\varphi}((v,u)R) = \overline{\theta}([\lambda_v(v,u)\lambda_u^{-1}]) = \lambda_v(v,u)\lambda_u^{-1}R.$$

Все ребра в путях λ_v и λ_u^{-1} лежат в T. Поэтому $\lambda_v R = \lambda_u^{-1}R = R$. Следовательно, $\lambda_v(v,u)\lambda_u^{-1}R = (u,v)R$. Мы показали, что $\overline{\theta}\circ\overline{\varphi}$ тождественное отображение на порождающих F/R. Легко видеть, что $\overline{\theta}$ является гомоморфизмом. Поэтому $\overline{\theta} \circ \overline{\varphi}$ тождественное отображение.

В итоге, $\overline{\varphi}$ — изоморфизм и $\mathcal{T}(K,T) = F/R \simeq \pi(K,w)$. □

Следствие 7. *Пусть K — связный 1-комплекс. Тогда $\pi(K,w)$ — свободная группа. Более того, если T — максимальное дерево, то*

$$\text{rank } \pi(K,w) = |\{\textit{1-симплексы в } K, \textit{ которые не лежат в } T\}|.$$

Доказательство. Действительно, если $(v,u) \in T$, то из соотношений типа а следует, что $(v,u) = 1$ в $\mathcal{T}(K,T)$. Поэтому $\mathcal{T}(K,T)$ порождается элементами $(v,u) \in K \setminus T$. Так как K это 1-комплекс, то все соотношения типа б имеют вид:

$$(v,u)(u,u) = (v,u)$$

$$(v,v)(v,u) = (v,u)$$

$$(v,u)(u,v) = (v,v)$$

При этом $(u,u) = (v,v) = 1$ в $\mathcal{T}(K,T)$ (из соотношения типа а). Поэтому, если $(v,u) \in K \setminus T$, то первые два соотношения становятся тривиальными, а последнее означает, что $(v,u)^{-1} = (u,v)$. Для каждого 1-симплекса $\{v,u\} \in T$ выберем одно из ребер (v,u) или (u,v). Тогда выбранные ребра порождают $\mathcal{T}(K,T)$ и между ними нет нетривиальных соотношений.

□

Определение 15. *Пусть I — множество.* ***Букетом из $|I|$-окружностей*** *называется 1-комплекс B_I, у которого множество вершин*

$$Vert(B_I) = \{w\} \sqcup_{i\in I} \{u_i, v_i\},$$

а множество 1-симплексов состоит из подмножеств вида $\{w,v_i\}, \{v_i,u_i\}$ и $\{w,u_i\}$.

Следствие 8. *$\pi(B_I,w)$ — свободная группа ранга $|I|$.*

Задача 11. *Рассмотрим равнобедренный треугольник ABC. Пусть E,F,G — середины сторон AB, BC и CA соответственно. Рассмотрим 2-комплекс K, на множестве вершин $\{A,B,C,E,F,G\}$, в который входят 2-симплексы $\{A,E,G\}, \{B,E,F\}$ и $\{F,C,G\}$, а также все их подмножества. С помощью теоремы Титце найдите фундаментальную группу K.*

Задача 12. *Рассмотрим комплекс K из задачи 11. Рассмотрим комплекс L, полученный из K выбрасыванием всех 2-симплексов. Найдите фундаментальную группу комплекса L.*

Задача 13. *Пусть есть два связных комплекса K_1 и K_2. Пусть G_1 — фундаментальная группа K_1, а G_2 — фундаментальная группа K_2. Выберем вершину $a \in \text{Vert}(K_1)$ и $b \in \text{Vert}(K_2)$. Рассмотрим комплекс $K = K_1 \sqcup K_2$ и добавим в него ребро $\{a,b\}$. Какая фундаментальная группа у K?*

1.4 Накрытия комплексов. Теорема Нильсена-Шрайера

Пусть $p : K \to K'$ — симплициальное отображение и L' — подкомплекс в K'. Тогда обозначим

$$p^{-1}(L) = \{s \in L \mid p(s) \in L'\}.$$

Для симплекса $s \in K$ обозначим через $|s|$ — множество всех непустых подмножеств s. Тогда $|s|$ — подкомплекс в K.

Определение 16. *Симплициальное отображение комплексов $p : \widetilde{K} \to K$ называется **накрытием**, если для любого симплекса $s \in K$*

$$p^{-1}(|s|) = \sqcup_{i \in I} |\widetilde{s_i}|,$$

где $\widetilde{s_i}$ симплексы в $\widetilde{K}$. При чем ограничение p на любой подкомплекс $\widetilde{|s_i|}$ является изоморфизмом между $\widetilde{|s_i|}$ и $|s|$.

Иными словами прообраз каждого симплекса $s \in K$ — объединение непересекающихся симплексов $\widetilde{s_i}$ из $\widetilde{K}$, которые изоморфны s. При этом между симплексами $\widetilde{s_i}$ нет ребер.

Замечание 7. *Если $p : \widetilde{K} \to K$ накрытие, то каждый симплекс в $\widetilde{K}$ изоморфен своему образу и $\dim \widetilde{K} = \dim K$.*

Доказательство. Пусть $\widetilde{s} \in \widetilde{K}$. Тогда $s = p(\widetilde{s}) \in K$, так как p симплициальное отображение. Имеем

$$p^{-1}(|s|) = \sqcup_{i \in I} |\widetilde{s_i}|.$$

Симплекс $\widetilde{s}$ принадлежит подкомплексу $p^{-1}(|s|)$. Симплексы $\widetilde{s_i}$ не пересекаются и в $\widetilde{K}$ между ними нет ребер. Поэтому $\widetilde{s} \subseteq \widetilde{s_i}$ для некоторого $i \in I$. При этом $p(\widetilde{s}) = s$, а число точек в s такое же, как и в $\widetilde{s_i}$. Значит, $\widetilde{s} = \widetilde{s_i} \simeq s$.

Отсюда следует, что $\dim \widetilde{K} \leq \dim K$. Но прообраз любого симплекса s из K содержит симплексы изоморфные s. Поэтому $\dim \widetilde{K} \geq \dim K$. □

Теорема 11. *Пусть $p : \widetilde{K} \to K$ — накрытие, $\widetilde{w}$ — некоторая точка $\widetilde{K}$ и $w = p(\widetilde{w})$. Для любого пути α в K с началом в точке w существует единственный пусть $\overline{\alpha}$ в $\widetilde{K}$ с началом в $\widetilde{w}$, такой что $p(\overline{\alpha}) = \alpha$.*

Доказательство. Докажем индукцией по длине α. Если длина 1, то $\alpha = (w, u)$. Рассмотрим симплекс $s = \{w, u\} \in K$. Тогда прообраз $|s|$ объединение непересекающихся симплексов вида $\widetilde{s_i} = \{\widetilde{w_i}, \widetilde{u_i}\}$. Точка $\widetilde{w}$ принадлежит $p^{-1}(|s|)$. Значит, существует $i \in I$, такое что $\widetilde{w} = \widetilde{w_i}$. Тогда путь $\overline{\alpha} = \{\widetilde{w_i}, \widetilde{u_i}\}$ — единственный путь с началом в $\widetilde{w}$ накрывающий α.

Пусть $\alpha = (w, u_1, \ldots, u_n)$. Тогда существует единственный путь $\overline{\alpha_1}$ с началом в $\widetilde{w}$, накрывающий путь $(w, \ldots, u_{n-1})$. Также есть единственный путь $\overline{\alpha_2}$ с началом в точке $e(\overline{\alpha})$ накрывающий путь (u_{n-1}, u_n). Тогда $\overline{\alpha} = \overline{\alpha_1 \alpha_2}$ — единственный путь, накрывающий α. □

Лемма 2. *Пусть $p : \widetilde{K} \to K$ — накрытие, $\widetilde{w} \in \widetilde{K}$ и $p(\widetilde{w}) = w$. Пусть α и β — пути в K, которые начинаются в точке w, а $\overline{\alpha}$ и $\overline{\beta}$ — пути, которые начинаются в $\widetilde{w}$ и накрывают α и β соответственно. Тогда, если α и β эквивалентны, то $\overline{\alpha}$ и $\overline{\beta}$ эквивалентны. В частности, $e(\overline{\alpha}) = e(\overline{\beta})$.*

Доказательство. Достаточно разобрать случай, когда

$$\alpha = (w, v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n) \text{ и } \beta = (w, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n),$$

где $s = \{v_{i-1}, v_i, v_{i+1}\}$ — симплекс в K.

Пусть

$$\overline{\alpha} = (\widetilde{w}, \widetilde{v_1}, \ldots, \widetilde{v_{i-1}}, \widetilde{v_i}, \widetilde{v_{i+1}}, \ldots, \widetilde{v_n}).$$

Тогда $\{\widetilde{v_{i-1}}, \widetilde{v_i}, \widetilde{v_{i+1}}\}$ симплекс в $\widetilde{K}$. Тогда путь

$$(\widetilde{w}, \widetilde{v_1}, \ldots, \widetilde{v_{i-1}}, \widetilde{v_{i+1}}, \ldots, \widetilde{v_n})$$

накрывает путь β, а значит совпадает с $\overline{\beta}$. Поэтому $\overline{\alpha}$ и $\overline{\beta}$ эквивалентны. □

Теорема 12. *Пусть $p : \widetilde{K} \to K$ — накрытие, $\widetilde{w}$ — точка в $\overline{K}$ и $p(\widetilde{w}) = w$. Тогда корректно определено отображение*

$$p_\# : \pi(\widetilde{K}, \widetilde{w}) \to \pi(K, w),\ [\alpha] \to [p(\alpha)].$$

При этом $p_\#$ инъективный гомоморфизм.

Доказательство. Нетривиальна только инъектиность $p_\#$. Но инъективность следует из леммы 2. □

Определение 17. *Пусть K — комплекс, w — точка в K и $H \leq \pi(K, w)$. Введем отношение эквивалентности на множестве путей с началом в точке w следующим образом.*

$$\alpha \sim_H \beta \iff e(\alpha) = e(\beta) \text{ и } [\alpha\beta^{-1}] \in H.$$

Обозначим через $[\alpha]_H$ класс эквивалентности α и через K_H множество классов эквивалентности.

Введем на K_H структуру комплекса. Пусть s — симплекс в K и α — путь в K с началом в точке w и концом в некоторой точке s. **Продолжением α в s** будем называть путь β вид $\alpha\alpha'$, где α' — путь в s. Положим

$$S(s, \alpha) = \{[\beta]_H \mid \beta \text{ —продолжение } \alpha \text{ в } s\}.$$

Подмножества $S(s, \alpha)$ будем называть симплексами в K_H.

Лемма 3. *Отображение $[\beta]_H \to e(\beta)$ — биекция между $S(s, \alpha)$ и s.*

Доказательство. Для любой точки s есть продолжение α в s с концом в этой точке. Отсюда следует сюръективность.

С другой стороны все пути в симплексе с одинаковыми началами и концами эквивалентны. Поэтому, если $\beta_1 = \alpha\alpha_1$ и $\beta_2 = \alpha\alpha_2$ — продолжения α с одинаковыми концами, то α_1 и α_2 эквивалентны, а значит $[\beta_1] = [\beta_2]$. Отсюда следует, что и $[\beta_1]_H = [\beta_2]_H$. □

Лемма 4. *Если s' — симплекс в K, который содержится в симплексе s и α — путь с началом в точке w и концом в s', то $S(s', \alpha) \subseteq S(s, \alpha)$.*

Доказательство. Любое продолжение пути α в s' является также продолжением пути в s. □

Лемма 5. *Пусть α и β — пути в K из точки w в некоторые точки s. Тогда множества $S(s, \alpha)$ и $S(s, \beta)$ либо совпадают, либо не пересекаются.*

Доказательство. Рассмотрим путь $\beta' = \beta(e(\beta), e(\alpha))$.
Случай 1. Предположим, что $[\beta']_H = [\alpha]_H$.

Пусть $\alpha\gamma_1$ — некоторое продолжение в s пути α и $\beta\gamma_2$ — некоторое продолжение в s пути β, причем $e(\gamma_1) = e(\gamma_2)$. Тогда $[(e(\beta), e(\alpha))\gamma_1] = [\gamma_2]$ (так как в симплексе s все пути с одинаковыми началами и концами одинаковые).

Тогда $[\beta\gamma_2] = [\beta'\gamma_1]$. Отсюда $[\beta\gamma_2]_H = [\beta'\gamma_1]_H$. С другой стороны

$$[\beta'\gamma_1\gamma_1^{-1}\alpha^{-1}] = [\beta'\alpha^{-1}] \in H.$$

Поэтому $[\beta'\gamma_1]_H = [\alpha\gamma_1]_H$. Следовательно, $S(s,\beta) \subseteq S(s,\alpha)$. Аналогично доказывается, что $S(s,\alpha) \subseteq S(s,\beta)$.
Случай 2. Предположим, что $[\beta']_H \neq [\alpha]_H$.

В тех же обозначениях, что и выше получаем.

$$[\beta'\gamma_1\gamma_1^{-1}\alpha^{-1}] = [\beta'\alpha^{-1}] \notin H.$$

Отсюда $[\beta\gamma_2]_H = [\beta'\gamma_1]_H \neq [\alpha\gamma_1]_H$. Поэтому любое продолжения α в s не эквивалентно относительно H с любым продолжением β в s. □

Лемма 6. *K_H — комплекс и отображение*

$$p : K_H \to K,\ [\alpha]_H \to e(\alpha)$$

— симплициальное.

Доказательство. 1) Одноэлементное множество $\{[\alpha]_H\}$ совпадает с множеством $S(\{e(\alpha)\}, \alpha)$.
2) Пусть $L \subseteq S(s,\alpha)$. Рассмотрим $p(L)$. По лемме 3 $p(L)$ подмножество s, а следовательно, некоторый симплекс s'.

Рассмотрим некоторую точку $v \in s'$. Любое продолжение пути $\alpha' = \alpha(e(\alpha), v)$ в s' является продолжением пути α в s. Поэтому $S(s', \alpha') \subseteq S(s,\alpha)$. При этом $p(S(s',\alpha')) = s'$. Так как p биективно, то $S(s',\alpha') = L$.

Из пунктов 1) и 2) следует, что K_H комплекс. Из леммы 3 следует, что p симплициально. □

Лемма 7. *Пусть K — комплекс и $H \leq \pi(K, w)$. Тогда для любого пути α в K с началом в w есть путь $\overline{\alpha}$ в K_H из точки $\widetilde{w} = [(w,w)]_H$ в точку $[\alpha]_H$, такой что $p(\overline{\alpha}) = \alpha$.*

Доказательство. Пусть $\alpha = (w, v_1, \ldots, v_n)$. Обозначим через $\alpha_i = (w, v_1, \ldots, v_i)$. Множество $s_i = \{v_i, v_{i+1}\}$ — симплекс в K. Тогда $[\alpha_i]_H$ и $[\alpha_{i+1}]_H$ принадлежат $S(s_i, \alpha_i)$. Следовательно, $\overline{\alpha} = (\widetilde{w}, [\alpha_1]_H, \ldots, [\alpha_n]_H)$ — путь в K_H, который накрывает α. □

Теорема 13. *Отображение*

$$p : K_H \to K,\ [\alpha]_H \to e(\alpha)$$

— накрытие и $p_\#(\pi(K_H, \widetilde{w})) = H$. Здесь w — точка из определения 17 и $\widetilde{w} = [(w,w)]_H$. В частности, $\pi(K_H, \widetilde{w}) \simeq H$.

Доказательство. Пусть s — симплекс в K. Рассмотрим множество $p^{-1}(|s|)$. Пусть некоторый симплекс $S(s',\alpha)$ принадлежит $p^{-1}(|s|)$. Тогда $p(S(s',\alpha)) = s' \subseteq s$. По лемме 4 $S(s',\alpha) \subseteq S(s,\alpha)$. При этом по лемме 5 множества $S(s,\alpha) = S(s,\beta)$ либо не пересекаются, либо совпадают. Отсюда следует, что

$$p^{-1}(|s|) = \sqcup S(s,\alpha).$$

Из леммы 3 следует, что ограничение p на комплекс $S(s,\alpha)$ — изоморфизм. Поэтому p — накрытие.

Пусть теперь α — замкнутый путь с началом и концом в точке w. Класс $[\alpha]$ лежит в образе $p_\#$ тогда и только тогда, когда накрывающий путь $\overline{\alpha}$ в K_H с началом в точке $\widetilde{w}$ замкнутый. По теореме 11 накрывающий путь единственный. По лемме 7 конец накрывающего пути совпадает с $[\alpha]_H$.

Получаем, что $[\alpha]$ лежит в образе $p_\#$ тогда и только тогда, когда $[\alpha]_H = \widetilde{w} = [(w,w)]_H$. Последнее равносильно

$$[\alpha(w,w)^{-1}] = [\alpha] \in H$$

. □

Задача 14. *Рассмотрим комплекс K с вершинами $\{1,2,3\}$, который состоит из симплексов $\{1,2\},\{1,3\},\{2,3\}$, а также всех одноэлементных подмножеств. Докажите, что фундаментальная группа K изоморфна $\mathbb{Z}$. Опишите накрытие K, которое соответствует подгруппе $2\mathbb{Z}$. Опишите накрытие K, которое соответствует произвольной подгруппе $\mathbb{Z}$.*

Задача 15. *У букета из двух окружностей фундаментальная группа изоморфна свободной группе с базисом x,y, где x соответствует классу замкнутого пути, проходящего по одной из окружностей, а y соответствует классу замкнутого пути, проходящего по второй окружности. Постройте накрытия для подгрупп $\langle x\rangle$ и $\langle xy\rangle$.*

Теорема 14. *(Теорема Нильсена-Шрайера)*
Пусть F — свободная группа и $H \leq F$. Тогда H свободная группа.

Доказательство. Пусть X — базис F. Рассмотрим букет из $|X|$ окружностей: $K = B_{|X|}$. Тогда по следствию 8 $\pi(K,w) \simeq F$, для любой точки $w \in K$. Рассмотрим накрытие K_H комплекса K, которое соответствует подгруппе H. Согласно замечанию 7 размерность K_H равна 1. Тогда по следствию 7 фундаментальная группа K_H тоже свободна. Но согласно теореме 13 фундаментальная группа K_H изоморфна H. □

При этом ранг подгруппы H свободной группы F может быть больше чем ранг F.

Пример 8. *Рассмотрим группу $F = F(x,y)$ с базисом $\{x,y\}$. Рассмотрим множество $X = \{x^n y x^{-n} \mid n \in \mathbb{Z}\}$. Тогда подгруппа H, порожденная множеством X, является свободной группой с базисом X. В частности, H имеет счетный ранг.*

Доказательство. Рассмотрим свободную группу G с базисом $Z = \{z_n \mid n \in \mathbb{Z}\}$. Рассмотрим отображение

$$f : Z \to H,\ f(z_n) = x^n y x^{-n}.$$

Существует гомоморфизм $\varphi : G \to H$, продолжающий f. Тогда φ — сюръективный гомоморфизм. Докажем инъективность.

Пусть $w = z_{i_1}^{a_1} \dots z_{i_k}^{a_k}$ — приведенное слово, где $a_i \in \mathbb{Z}$. Тогда

$$\varphi(w) = (x^{i_1} y x^{-i_1})^{a_1} x^{i_2} y^{a_2} x^{-i_2} \dots (x^{i_k} y x^{-i_k})^{a_k} = x^{i_1} y^{a_1} x^{-i_1} \dots x^{i_k} y^{a_k} x^{-i_k} =$$

$$= x^{i_1} y^{a_1} x^{-i_1+i_2} y^{a_2} x^{-i_2+i_3} \dots y^{a_n} x^{-i_n} = w'.$$

Слово w приведенное, поэтому $i_j \neq i_{j+1}$. Поэтому слово w' также приведенное. Поэтому $\varphi(w) \neq 1$. □

Следующий пример показывает, что свободные группы могут содержаться и внутри "классических"групп.

Пример 9. *Пусть* $G = \mathrm{GL}_2(\mathbb{R})$. *Рассмотрим матрицы* $a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ *и* $b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. *Тогда группа* $H = \langle a, b \rangle$ *— свободная группа с базисом* $\{a, b\}$.

Доказательство. Рассмотрим множества

$$X_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid |x| < |y| \right\}$$

и

$$X_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid |y| < |x| \right\}.$$

Тогда $a^k(X_1) \subseteq X_2$ и $b^k(X_2) \subseteq X_1$ при $k \in \mathbb{Z} \setminus \{0\}$. Тогда

$$a^{k_1} b^{k_2} \dots a^{k_r}(X_1) \subseteq X_2.$$

Поэтому $a^{k_1} b^{k_2} \dots a^{k_r} \neq 1$. С другой стороны, для любого слова w от a и b найдется такое k, что слово $a^k w a^{-k}$ начинается и заканчивается степенью a. Поэтому $a^k w a^{-k} \neq 1$, но тогда и $w \neq 1$. Поэтому никакое нетривиальное слово от a и b не равно единице. Отсюда следует, что H — свободная группа с базисом $\{a, b\}$. □

Задача 16. *(Пинг-понг лемма.)*
Пусть группа G *действует на множестве* X, *и элементы* $g_1, \dots, g_k \in G$ *имеют бесконечный порядок. Предположим, что существуют непересекающиеся подмножества* $X_1^+, \dots, X_k^+$ *и* $X_1^-, \dots, X_k^-$, *такие что*

$$g_i(X \setminus X_i^-) \subseteq X_i^+ \text{ и } g_i^{-1}(X \setminus X_i^+) \subseteq X_i^-$$

для всех i. *Докажите, что подгруппа в* G, *порожденная* $g_1, \dots, g_k$, *является свободной группой с базисом* $\{g_1, \dots, g_k\}$.

Задача 17. *Пусть* F *— свободная группа с базисом* $\{g_1, \dots, g_k\}$. *Докажите, что всегда найдется действие* F *на некотором множестве* X, *удовлетворяющее условиям задачи 16.*

Задача 18. *Докажите, что свободная группа ранга 2 и более неразрешима. Выведите отсюда, что любая разрешимая группа не содержит свободных подгрупп ранга 2 и более.*

Глава 2

Теория Галуа

2.1 Конечные расширения полей

Пусть L — поле и K — подполе в L. Тогда L называется **расширением поля** K. Обозначение: L/K.

Легко видеть, что L является векторным пространством над полем K. Размерность поля L над полем K называется **степенью** расширения и обозначается $[L : K]$ или $\dim_K L$.

Пример 1. $[\mathbb{C} : \mathbb{R}] = 2$. *В качестве базиса в* $\mathbb{C}$ *над* $\mathbb{R}$ *можно выбрать* 1 *и* i.

Пример 2. $[\mathbb{R} : \mathbb{Q}] = \infty$, *так как* $\mathbb{Q}$ *счетно, а* $\mathbb{R}$ *нет.*

Если поле K имеет характеристику ноль, то поле K является расширением поля $\mathbb{Q}$. Действительно, лего видеть, что подполе, порожденное 1 в K, изоморфно полю $\mathbb{Q}$. Аналогично, если $\operatorname{char} K = p$, где p — простое, то поле K является расширением поля $\mathbb{Z}_p$.

Следствие 1. *Пусть* K *— конечное поле, то есть* $|K| < \infty$. *Тогда* $|K| = p^n$, *где* p *— простое, а* $n \in \mathbb{N}$.

Доказательство. Так $|K| < \infty$, то $\operatorname{char} K = p > 0$ и $[K : \mathbb{Z}_p] < \infty$. Легко доказать, что конечномерное векторное пространство над полем $\mathbb{Z}_p$ имеет p^n элементов, где n — размерность векторного пространства. □

Определение 1. *Пусть* L/K *— расширение полей и* $a \in L$. *Ненулевой многочлен* $f \in K[x]$ *называется* ***аннулирующим*** *для* a *над полем* K, *если* $f(a) = 0$.

Определение 2. *Пусть* L/K *— расширение полей. Элемент* $a \in L$ *называется* ***алгебраическим*** *над* K, *если для* a *есть аннулирующий многочлен над* K. *В противном случае* a *называется* ***трансцендентным*** *над полем* K.

Пример 3. *Элемент* $\sqrt{2} \in \mathbb{R}$ *является алгебраическим над полем* $\mathbb{Q}$. *В качестве соответствующего многочлена* f *можно выбрать* $x^2 - 2$.

Пример 4. *В конце 19 века было доказано, что числа* π *и* e *являются трансцендентными над полем* $\mathbb{Q}$. *При этом* π *и* e *являются алгебраическими над* $\mathbb{R}$. *В качестве аннулирующих многочленов можно взять, например,* $x - \pi$ *и* $x - e$ *соответственно.*

Определение 3. *Пусть* L/K *— расширение полей и элемент* $a \in L$ *является алгебраическим над* K. *Приведенный многочлен* $f \in K[x]$ *называется* ***минимальным*** *для элемента* a, *если он аннулирующий и имеет минимальную степень среди всех аннулирующих для* a *над полем* K. *Легко доказать, что минимальный многочлен существует, единственен, неприводим над полем* K *и делит любой другой аннулирующий для* a. *Обозначение:* μ_a *или* μ_a^K, *если мы хотим подчеркнуть над каким полем мы рассматриваем минимальный многочлен.*

Пример 5. $\mu^{\mathbb{Q}}_{\sqrt{2}} = x^2 - 2$, $\mu^{\mathbb{R}}_{\sqrt{2}} = x - \sqrt{2}$.

Задача 19. *Найдите минимальные многочлены следующих элементов:*

а) $2 - 3i$ *над* $\mathbb{R}$;

б) $\sqrt{2} + \sqrt{5}$ *над* $\mathbb{Q}$;

в) $\sqrt{2} + \sqrt{5}$ *над* $\mathbb{Q}(\sqrt{5})$;

Задача 20. *Докажите, что* $\cos\frac{2\pi}{n}$ *алгебраическое над* $\mathbb{Q}$ *для любого* n.

Пусть L/K — расширение полей и $a \in L$. Будем через $K[a]$ обозначать подкольцо в L, порожденное K и a, то есть наименьшее кольцо в L, содержащее K и a. Через $K(a)$ будем обозначать подполе в L, порожденное K и a, то есть наименьшее подполе в L, содержащее K и a.

Нетрудно доказать, что $K[a] = \{f(a) \mid f \in K[x]\}$ и $K(a) = \{\frac{f(a)}{g(a)} \mid f, g \in K[x],\ g(a) \neq 0\}$.

Утверждение 1. *1.* $K[a] = \{f(a) \mid f \in K[x]\}$;

2. $K(a) = \{\frac{f(a)}{g(a)} \mid f, g \in K[x],\ g(a) \neq 0\}$.

3. Если a *алгебраический элемент над* K, *то* $K[a] = K(a) \simeq K[x]/(\mu_a)$. *При этом элементы* $1, a, a^2, \ldots, a^{n-1}$ *образуют базис в* $K(a)$ *над* K, *где* $n = \deg\ \mu_a$. *В частности,* $[K(a) : K] = \deg\ \mu_a$.

4. Если a *трансцендентный элемент над* K, *то* $K[a] \simeq K[x]$, $K(a) \simeq K(x)$.

Доказательство. Доказывается в стандартном курсе алгебры, но вообще нетрудное упражнение. □

Пример 6. *Минимальный многочлен для* $\sqrt[3]{2}$ *над* $\mathbb{Q}$ *равен* $x^3 - 2$. *Его степень 3, поэтому поле* $\mathbb{Q}(\sqrt[3]{2})$ *имеет размерность 3 над* $\mathbb{Q}$. *В качестве базиса над* $\mathbb{Q}$ *можно взять элементы* $1, \sqrt[3]{2}, \sqrt[3]{4}$.

Заметим также, что из пункта 3 утверждения 1 следует, что все элементы $\mathbb{Q}(\sqrt[3]{2})$ *можно представить как многочлены степени не больее чем 2 от* $\sqrt[3]{2}$ *с коэффициентами из* $\mathbb{Q}$. *В частности, все обратные элементы можно так представить. Например,* $\frac{1}{\sqrt[3]{2}} = \frac{1}{2}\sqrt[3]{4}$ *и, если я не ошибся,* $\frac{1}{1+\sqrt[3]{2}+\sqrt[3]{4}} = -1 + \sqrt[3]{2}$.

Определение 4. *Расширение полей* L/K *называется* ***алгебраическим****, если все элементы* L *алгебраические над* K.

Утверждение 2. *Конечное расширение полей является алгебраическим.*

Доказательство. Пусть $a \in L$ и $[L : K] = n$. Тогда элементы $1, a, a^2, \ldots, a^n$ линейно зависимы над K (в n-мерном векторном пространстве любые n+1 вектор линейно зависимы). Тогда существуют $a_0 \ldots a_n \in K$, такие что

$$a_0 + a_1 a + \ldots + a_n a^n = 0.$$

Но тогда многочлен $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ — аннулирующий для a над K. □

Утверждение 3. *(Лемма о башне полей)*
Пусть $K \subseteq L \subseteq P$ *— расширения полей. Тогда* $[P : K] = [P : L][L : K]$.

Доказательство. Если P/L или L/K бесконечное расширение, то утверждение тривиально. Иначе пусть $e_1, \ldots, e_n \in L$ — базис в L над полем K и $f_1, \ldots, f_m \in P$ — базис в P над L. Тогда нетрудно проверить, что $e_i f_j$ — базис в P над K.

□

Следствие 2. *Пусть L/K — расширение полей. Тогда алгебраические над K элементы L образуют подполе в L.*

Доказательство. Если $\alpha, \beta \in L$ — алгебраические над K элементы, то $K[\alpha]/K$ — конечное расширение. С другой стороны, элемент β алгебраичен над $K[\alpha]$ поэтому $K[\alpha][\beta]$ — тоже конечное расширение. По лемме о башне полей $K[\alpha][\beta]/K$ — конечное расширение, а значит алгебраическое. Но элементы $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in K[\alpha][\beta]$, так как $K[\alpha][\beta]$ — поле, содержащее и α и β.

□

Следствие 3. *Пусть L/K — конечное расширение полей, имеющее простую степень. Тогда в L нет собственных подполей, содержащих K.*

Если L/K — расширение полей и $\alpha_1, \ldots, \alpha_n \in L$, то через $K(\alpha_1 \ldots, \alpha_n)$ будем обозначать поле, порожденное K и $\alpha_1, \ldots, \alpha_n$.

Следствие 4. *Расширение L/K является конечным тогда и только тогда, когда оно порождено конечным число алгебраических над K элементов.*

Доказательство. Если L/K конечно, то можно взять базис в L над K и это будет конечное число алгебраических над K элементов, порождающих L. В другую сторону, если $L = K(\alpha_1, \ldots, \alpha_n)$, где α_i — алгебраические над K элементы, то L получается присоединением к K конечного числа раз алгебраических элементов:

$$L = K[\alpha_1][\alpha_2] \ldots [\alpha_{n-1}][\alpha_n].$$

Присоединяя каждое новое α_i мы получаем конечное расширение. Из леммы о башне полей следует, что итоговое расширение тоже будет конечным. □

Следствие 5. *Пусть L/K — расширение полей и $\alpha, \beta \in L$ — алгебраические над K элементы. Предположим, что* $(\deg \mu_\alpha^K, \deg \mu_\beta^K) = 1$. *Тогда* $[K(\alpha, \beta) : K] = \deg \mu_\alpha^K \cdot \deg \mu_\beta^K$.

Доказательство. С одной стороны

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K].$$

Поэтому $[K(\alpha, \beta) : K]$ делится на $[K(\alpha) : K] = \deg \mu_\alpha$. Аналогично $[K(\alpha, \beta) : K]$ делится на $\deg \mu_\beta$. Отсюда получаем, что $[K(\alpha, \beta) : K]$ делится на $\deg \mu_\alpha^K \cdot \deg \mu_\beta^K$.

С другой стороны минимальный многочлен для β над полем K является аннулирующим для β над полем $K(\alpha)$. Поэтому

$$[K(\alpha, \beta) : K(\alpha)] = \deg \mu_\beta^{K(\alpha)} \leq \deg \mu_\beta^K = [K(\beta) : K].$$

Следовательно,

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K] \leq [K(\beta) : K][K(\alpha) : K] = \deg \mu_\alpha^K \cdot \deg \mu_\beta^K.$$

□

Следствие 6. *Пусть $K \subseteq L \subseteq P$ — расширения полей. Тогда расширение L/K алгебраическое тогда и только тогда, когда расширения P/L и L/K алгебраические*

Доказательство. Справа налево утверждение тривиально. В другую сторону, если мы рассмотрим элемент $\alpha \in P$, то он алгебраический над L, поэтому существует многочлен

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in L[x],$$

аннулирующий α. Все элементы a_i алгебраические над K. Поэтому расширение $[K(\alpha_0, \ldots, \alpha_n) : K]$ — конечное. Но тогда и расширение $[K(a_0, \ldots, a_n, \alpha) : K]$ — конечное. Поэтому расширение $[K(\alpha) : K]$ — конечное, а следовательно, α — алгебраический элемент над K. □

Определение 5. *Пусть есть две башни расширений полей: $K \subseteq P \subseteq L$ и $K \subseteq Q \subseteq L$.* ***КомпОзит*** *полей P и Q — наименьшее подполе в L, которое содержит и P, и Q.*

Утверждение 4. $[PQ : K] \leq [P : K] \cdot [Q : K]$.

Доказательство. Если P/K или Q/K бесконечные расширения, то утверждения тривиальны. В противном случае по лемме о башне расширений

$$[PQ : K] = [PQ : Q][Q : K].$$

Докажем, что $[PQ : Q] \leq [P : K]$. Пусть $P = K(\alpha_1, \ldots, \alpha_n)$ и $Q = K(\beta_1, \ldots, \beta_m)$, где α_i и β_j — алгебраические элементы над K. Тогда

$$PQ = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = K(\beta_1, \ldots, \beta_m)(\alpha_1, \ldots, \alpha_n) = Q(\alpha_1, \ldots, \alpha_n).$$

Поле $K(\alpha_1, \ldots, \alpha_i)$ содержится в поле $Q(\alpha_1, \ldots, \alpha_i)$. Поэтому

$$\deg \mu_{\alpha_{i+1}}^{K(\alpha_1,\ldots,\alpha_i)} \geq \deg \mu_{\alpha_{i+1}}^{Q(\alpha_1,\ldots,\alpha_i)}.$$

Отсюда следует, что $[Q(\alpha_1, \ldots, \alpha_n)] \leq [P : K]$. □

Пусть $f \in K[x]$ — неприводимый многочлен. Рассмотрим поле $L = K[x]/(f)$. Тогда класс $\overline{x} = x + (f)$ является корнем для f в L. Поэтому говорят, что поле L получается **присоединением** к K коня f.

Если K содержится в некотором поле P и у f есть корни α и β в P, то $K[\alpha] \simeq K[\beta] \simeq L$.

Определение 6. *Пусть $f \in K[x]$ произвольный многочлен. Тогда расширение L/K называется* ***полем разложения*** *многочлена f над полем K, если L минимальное по включению расширение поля K, в котором f раскладывается на линейные множители. Обозначение: $K(f)$.*

Теорема 1. *Для любого многочлена $f \in K[x]$ поле разложения $K(f)$ существует и расширение $K(f)/K$ конечное.*

Доказательство. Пусть $f = f_1 \ldots f_r$ — разложение на неприводимые для f над K. Если все f_i имеют степень 1, то $K(f) = K$. Иначе рассмотрим поле $L = K[x]/(f_i)$, где f_i — некоторый неприводимый многочлен степени хотя бы 2. Тогда над полем L многочлен f разложится в произведение неприводимых многочленов $h_1 \ldots h_s$, где $s > r$. Далее применим индукцию по $\deg f - s$. В итоге получим конечное расширение поля K, над которым f раскладывается на линейные множители.

Построенное таким образом расширение порождено над K корнями многочлена f. Поэтому оно является минимальным по включению расширением K, в котором f раскладывается на линейные множители.

□

Пример 7. *Пусть многочлен $f \in K[x]$ имеет степень 2. Если f приводим, то $K(f) = K$. Если f неприводим, то $K(f) = K[x]/(f)$ и $[K(f) : K] = 2$.*

Пример 8. *Пусть* $\deg f = 3$. *Если* f *раскладывается на линейные множители над* K, *то* $K(f) = K$. *Если* $f = f_1 f_2$, *где*

$$f_1, f_2 \in K[x], \deg f_1 = 2, \ \deg f_2 = 1$$

и f_1 *неприводим, то* $K(f) = K[x]/(f_1)$.

Утверждение 5. *Пердположим, что* $\mathrm{char}\ K \neq 2$. *Пусть* $f \in K[x]$ *— неприводимый многочлен степени 3. Положим*

$$\delta = \sqrt{D(f)} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3),$$

где $\alpha_1, \alpha_2, \alpha_3$ *— корни* f *в* $K(f)$.

1. *Если* $\delta \in K$, *то* $K(f) = K[x]/(f)$ *и* $[K(f) : K] = 3$.
2. *Пусть* $\delta \notin K$. *Положим* $L = K[x]/(f)$. *Тогда в* L *многочлен* f *раскладывается как произведение* $f_1(x - \overline{x})$, *где* f_1 *неприводим, и* $K(f) = L[x]/(f_1)$. *В частности,* $[K(f) : K] = 6$.

Доказательство. Пусть $f = x^3 + b_2x^2 + b_1x + b_0 \in K[x]$. Предположим, что $\delta \in K$. Пусть α_1 — некоторый корень f в $K[x]/(f)$ (например, $\overline{x}$). Из формул Виета следует, что $\alpha_1+\alpha_2+\alpha_3 = -b_2 \in K$ и $\alpha_1\alpha_2\alpha_3 \in K$. Отсюда $\alpha_2 + \alpha_3, \alpha_2\alpha_3 \in K[x]/(f)$. При этом

$$\delta = (\alpha_1^2 - (\alpha_2 + \alpha_3)\alpha_1 + \alpha_2\alpha_3)(\alpha_2 - \alpha_3).$$

Мы видим, что $\delta \in K \subseteq K[x]/(f)$ и первая скобка выражения выше, тоже принадлежит $K[x]/(f)$. Поэтому $\alpha_2 - \alpha_3 \in K[x]/(f)$. Но отсюда

$$\alpha_2 = \frac{(\alpha_2 + \alpha_3) + (\alpha_2 - \alpha_3)}{2} \in K[x]/(f),$$

$$\alpha_3 = \frac{(\alpha_2 + \alpha_3) - (\alpha_2 - \alpha_3)}{2} \in K[x]/(f).$$

Поэтому в $K[x]/(f)$ многочлен f раскладывается на линейные множители и $K[x]/(f)$ — поле разложения.

Пусть теперь $\delta \notin K$. С одной стороны $\delta \in K(f)$. Но $[K[\delta] : K] = 2$. Поэтому степень $[K(f) : K]$ делится на 2. С другой стороны, если $\alpha \in K(f)$ — любой корень f, то $[K[\alpha] : K] = 3$. Поэтому степень $[K(f) : K]$ делится на 6. Но $K(f) = K[\alpha_1][\alpha_2]$ и $[K[\alpha_1][\alpha_2] : K] \leq 6$. Отсюда получаем, что $[K(f) : K] = 6$. Оставшаяся часть утверждения тривиально следует из выше сказанного. □

Пример 9. *Рассмотрим многочлен* $f = x^3 - 2 \in \mathbb{Q}[x]$. *Он неприводим. Поле* $\mathbb{Q}(\sqrt[3]{2})$ *содержится в* $\mathbb{R}$, *поэтому не содержит двух других комплексных корней* $x^3 - 2$. *Поэтому* $\mathbb{Q}(f) = \mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}e^{\frac{2\pi i}{3}})$ *и* $[\mathbb{Q}(f) : \mathbb{Q}] = 6$.

Пример 10. *Рассмотрим многочлен* $f = 4x^3 - 3x + \frac{1}{2} \in \mathbb{Q}[x]$. *Так как* $\cos 3x = 4\cos^3 x - 3\cos x$, *то числа* $\cos\frac{2\pi}{9}, \cos\frac{4\pi}{9}, \cos\frac{8\pi}{9}$ *являются корнями* f. *С другой стороны* $\cos 2x = 2\cos^2 x - 1$. *Поэтому* $\cos\frac{4\pi}{9}, \cos\frac{8\pi}{9}$ *выражаются через* $\cos\frac{2\pi}{9}$. *Поэтому* $\mathbb{Q}(f) = \mathbb{Q}(\cos\frac{2\pi}{9})$ *и* $[\mathbb{Q}(f) : \mathbb{Q}] = 3$.

Задача 21. *Пусть* $f \in K[x]$ *и* $\deg f = n$. *Докажите, что* $[K(f) : K]$ *делит* $n!$.

Задача 22. *Постройте поля разложения следующих многочленов:*

а) $x^2 + x + 2 \in \mathbb{Q}[x]$;

б) $x^3 + 1 \in \mathbb{Q}[x]$;

в) $x^6 + 3 \in \mathbb{Q}[x]$.

Мы всегда считаем, что при гомоморфизме между полями единица переходит в единицу. Также мы считаем, что в каждом поле $0 \neq 1$. Ядро любого гомоморфизма колец является идеалом, а в поле нет идеалов. Поэтому любой гомоморфизм между полями является вложением.

Если $\varphi : K \to L$ — вложение полей и $f = a_0 + a_1x + \ldots + a_nx^n \in K[x]$, то будем обозначать через f_φ многочлен $\varphi(a_0) + \varphi(a_1)x + +\varphi(a_n)x^n \in L[x]$. Легко видеть, что $(f \pm g)_\varphi = f_\varphi \pm g_\varphi$ и $(fg)_\varphi = f_\varphi g_\varphi$.

Лемма 1. *(Лемма о продолжении вложения.)*
Пусть $\varphi : K \to L$ — вложение полей, поле K является подоплем некоторого поля P, $\alpha \in P$ — алгебраический элемент над K и μ_α — минимальный многочлен α над K.

1. *Пусть вложение $\widetilde{\varphi} : K(\alpha) \to L$ продолжает φ. Тогда $\widetilde{\varphi}(\alpha)$ корень $\mu_{\alpha,\varphi}$.*
2. *Для каждого корня β многочлена $\mu_{\alpha,\beta}$ существует единственное вложение $\varphi_\beta : K(\alpha) \to L$, такое что $\widetilde{\varphi}$ продолжает φ, и $\varphi_\beta(\alpha) = \beta$.*
3. *Число вложений $K(\alpha) \to L$, продолжающих φ, равно числу корней многочлена $\mu_{\alpha,\varphi}$ в L.*

Доказательство. 1) Действительно, пусть $\mu_\alpha = a_0 + a_1x + \ldots + a_nx^n$. Тогда

$$\mu_{\alpha,\varphi}(\widetilde{\varphi}(a)) = \varphi(a_0) + \varphi(a_1)(\widetilde{\varphi}(\alpha)) + \ldots \varphi(a_n)(\widetilde{\varphi}(\alpha)) = \widetilde{\varphi}(a_0 + a_1\alpha + \ldots + +a_n\alpha^n) = \widetilde{\varphi}(\alpha)(0) = 0.$$

2) Каждый элемент поля $K(\alpha)$ имеет вид $f(\alpha)$, где $f \in K[x]$. Для каждого корня β многочлена $\mu_{\alpha,\varphi}$ положим $\varphi_\beta(f(\alpha)) = f_\varphi(\beta)$. Проверим корректность определения φ_β. Если $f(\alpha) = g(\alpha)$, то $(f-g)(\alpha) = 0$, а следовательно, $f-g$ делится на μ_α. То есть $f - g = \mu_\alpha h$, для некоторого $h \in K[x]$.

Но тогда

$$f_\varphi(\beta) - g_\varphi(\beta) = (f-g)_\varphi(\beta) = \mu_{\alpha,\varphi}(\beta)h_\varphi(\beta) = 0.$$

То есть $\varphi_\beta(f(\alpha)) = \varphi_\beta(g(\alpha))$. Легко проверить, что φ_β — гомоморфизм. Единственность φ_β следует из того, что поле $K(\alpha)$ порождено K и α, а следовательно, любой гомоморфизм $K(\alpha) \to L$ однозначно определяется значениями на K и α.

3) Следует из 1) и 2) □

Теорема 2. *Пусть $f \in K[x]$ — многочлен. Тогда поле разложения $K(f)$ существует и единственно.*

Доказательство. Существование было доказано в теореме 1. Докажем единственность. Пусть L_1 и L_2 — поля разложения многочлена f. По определению L_1 и L_2 — расширения поля K, которые порождены над K корнями f. Обозначим $\alpha_1, \ldots, \alpha_n$ — корни f в L_1 (некоторые из них могут совпадать). Тогда $L_1 = K(\alpha_1, \ldots, \alpha_n)$.

Обозначим через φ_0 тождественное вложение K в L_2. Покажем, что φ_0 можно продолжить до вложения $\varphi : L_1 \to L_2$. Обозначим $K_i = K(\alpha_1, \ldots, \alpha_i)$. Будем строить вложения

$$\varphi_i : K_i \to L_2,\ \varphi_i|_{K_{i-1}} = \varphi_{i-1}.$$

Вложение φ_0 уже построено. Предположим, что φ_i построили. Минимальный многочлен $\mu^{K_i}_{\alpha_{i+1}}$ элемента α_{i+1} над полем K_i делит f (так как f — аннулирующий для α_{i+1}). Тогда многочлен $\mu^{K_i}_{\alpha_{i+1},\varphi_i}$ делит $f_{\varphi_i} = f_{\varphi_0} = f$ (последние два равенства справедливы так как коэффициенты f лежат в K).

Многочлен f раскладывается на линейные множители в L_2. Поэтому и $\mu^{K_i}_{\alpha_{i+1},\varphi_i}$ раскладывается на линейные множители. Следовательно, у $\mu^{K_i}_{\alpha_{i+1},\varphi_i}$ есть корень в L_2. По лемме 1 вложение $\varphi_i : K_i \to L_2$ можно продолжить до вложения

$$\varphi_{i+1} : K_{i+1} = K_i(\alpha_{i+1}) \to L_2.$$

В итоге получим вложение $\varphi_n : L_1 \to L_2$. Гомоморфизм полей φ_n является инъективным линейным отображением над полем K. Поэтому $[L_1 : K] \leq [L_2 : K]$. Аналогично можно доказать, что $[L_1 : K] \geq [L_2 : K]$. В итоге $[L_1 : K] = [L_2 : K]$. Но тогда φ_n — изоморфизм векторных пространств. При этом мы знаем, что φ_n — гомоморфизм полей. Но тогда φ_n — изоморфизм полей. □

2.2 Конечные поля. Корни из единицы

Напомним, что если $\operatorname{char} K = p > 0$, то отображение

$$\varphi : K \to K,\ a \to a^p$$

является эндоморфизмом, который называется эндоморфизмом **Фробениуса.** Если поле K конечно, то φ — автоморфизм.

Теорема 3. *Для любого простого p и натурального $n \in \mathbb{N}$ существует ровно одно поле из p^n элементов. Это поле является полем разложения многочлена $x^{p^n} - x$ над полем $\mathbb{Z}_p$.*

Доказательство. Рассмотрим поле $\mathbb{Z}_p$ и многочлен $f = x^{p^n} - x \in \mathbb{Z}_p[x]$. Положим $F = \mathbb{Z}_p(f)$.

Заметим, что $f' = -1$, и поэтому $(f, f') = 1$. Следовательно, у f нет кратных корней в F хотя бы p^n элементов.

С другой стороны элемент $\alpha \in F$ является корнем f тогда и только тогда, когда $\varphi^n(\alpha) = \alpha$, где φ — автоморфизм Фробениуса. Множество неподвижных точек автоморфизма —подполе в F (это легко проверить). Поэтому все корни f образуют подполе в F. Но так как F порождено над $\mathbb{Z}_p$ корнями f, то F состоит из корней f. Но тога в F ровно p^n элементов.

Обратно, пусть F — некоторое поле из p^n элементов. Тогда для любого $a \in F$ верно $a^{p^n} = a$. Но тогда все элементы F — корни многочлена $x^{p^n} - x$. Поэтому F — поле разложения $f = x^{p^n} - x$. □

Поле из p^n элементов обозначается $\mathbb{F}_{p^n}$ или F_{p^n} и называется **полем Галуа**.

Утверждение 6. *Пусть K — поле и $K^* = (K \setminus \{0\}, \cdot)$ — мультипликативная группа поля K. Тогда любая конечная подгруппа в K^* циклическая.*

Доказательство. Было доказано в курсе алгебры. □

Следствие 7. *Для любого простого p и $n \in \mathbb{N}$ существует неприводимый многочлен $f \in \mathbb{Z}_p[x]$ степени n. В частности, $\mathbb{Z}_p[x]/(f) \simeq F_{p^n}$.*

Доказательство. Мультипликативная группа поля F_{p^n} конечна, поэтому циклическая. Пусть α порождающий элемент в $F^*_{p^n}$. Тогда $F_{p^n} = \mathbb{Z}_p(\alpha)$. Положим $f = \mu_\alpha$. Тогда $n = [F_{p^n} : \mathbb{Z}_p] = \deg f$. С другой стороны f неприводим над $\mathbb{Z}_p$ так как это минимальный многочлен для α. □

Теорема 4. *Пусть K — подполе в поле F_{p^n}. Тогда в $|K| = p^d$, где $d|n$. Обратно, для любого делителя d числа n в поле F_{p^n} есть ровно одно подполе из p^d элементов.*

Доказательство. Пусть поле K — подполе F_{p^n}. Тогда $\mathrm{char}\ K = \mathrm{char}\ F_{p^n} = p > 0$. Тогда в K p^d элементов для некоторого d. С другой стороны F_{p^n} — векторное пространство над K. Поэтому

$$p^n = |F_{p^n}| = |K|^l = (p^d)^l = p^{dl}.$$

Отсюда $n = dl$ и d — делитель n.

Теперь пусть $d|n$. Рассмотрим автоморфизм φ^d, где φ — автоморфизм Фробениуса поля F_{p^n}. Пусть K — множество его неподвижных точек этого автоморфизма. Тогда K — подполе в F_{p^n}, которое совпадатс с множеством корней в F_{p^n} многочлена $x^{p^d} - x$. Но многочлен $x^{p^d} - x$ делит $x^{p^n} - x$, который раскладывается на линейные множители в F_{p^n}. Поэтому в K ровно p^d элементов.

Пусть теперь K' некоторое другое подопле в F_{p^n} из p^d элементов. Но все элементы K' удовлетворяют равенству $a^{p^d} = a$. Поэтому являются корнями многочлена $x^{p^d} - x$. Следовательно, $K' = K$.

□

Обозначим через $\Theta(n)$ множество приведенных (то есть со старшим коэффициентом 1) неприводимых многочленов степени n над полем $\mathbb{Z}_p$.

Утверждение 7.

$$\Theta(n) = \frac{1}{n}\sum_{d|n}\mu(d)p^{\frac{n}{d}}.$$

Здесь $\mu(d)$ — функция Мёбиуса.

Доказательство. Докажем, что $x^{p^n} - x$ — произведение всех неприводимых приведенных многочленов в $\mathbb{Z}_p[x]$, у которых степень делит n.

1) Пусть $f \in \mathbb{Z}_p[x]$ — приведенный неприводимый многочлен степени d и f делит $x^{p^n} - x$. Покажем, что $d|n$.

Многочлен $x^{p^n} - x$ раскладывается на линейные множители в F_{p^n}. Поэтому и f раскладывается. Пусть α — некоторый корень f в F_{p^n}. Тогда f — минимальный многочлен для α над $\mathbb{Z}_p$ (так как f приведенный неприводимый многочлен с коэффициентами из $\mathbb{Z}_p$). Поэтому $\mathbb{Z}_p(\alpha) = \mathbb{Z}_p[x]/(f)$ — подполе в F_{p^n}. Получаем $|\mathbb{Z}_p[x]/(f)| = p^d$, и из предыдущей теоремы следует, что $d|n$.

2) Пусть $g \in \mathbb{Z}_p[x]$ — приведенный неприводимый многочлен степени d и $d|n$. Тогда в поле $K = \mathbb{Z}_p[x]/(g)$ ровно p^d элементов. Из теорем 3 и 4 следует, что K изоморфно некоторому подполю в F_{p^n}. Пусть α — некоторый корень g в K. Тогда g — минимальный многочлен для α. С другой стороны α также является корнем $x^{p^n} - x$ (так как все элементы F_{p^n} являются корнями $x^{p^n} - x$). Поэтому $x^{p^n} - x$ делится на g.

3) У многочлена $x^{p^n} - x$ нет кратных корней. Поэтому в его разложении на неприводимые нет кратных множителей.

Из пунктов 1)-3) следует, что $x^{p^n} - x$ — произведение всех приведенных неприводимых многочленов, у которых степень делит n. Сравнивая степени получаем

$$p^n = \sum_{d|n} d\Theta(d).$$

Используя первую формулу обращения Мёбиуса получаем

$$n\Theta(n) = \sum_{d|n}\mu(d)p^{\frac{n}{d}}$$

□

Определение 7. *Пусть K — поле. Элемент $a \in K$ называется* ***корнем степени*** *n* ***из единицы****, если $a^n = 1$. Множество всех корней из единицы будем обозначать $\sqrt[n]{1}$.*

Легко видеть, что $\sqrt[n]{1}$ совпадает с множеством корней многочлена $x^n - 1$. В частности, $|\sqrt[n]{1}| \leq n$.

Утверждение 8. *Пусть K содержит поле разложения многочлена $x^n - 1$. Тогда*

1. *группа $\sqrt[n]{1}$ циклическая группа;*
2. *предположим, что n не делится на характеристику поля K. Тогда $|\sqrt[n]{1}| = n$;*
3. *пусть* $\mathrm{char}\ K = p > 0$ *и $n = p^k m$, где $(m, p) = 1$. Тогда $\sqrt[n]{1} = \sqrt[m]{1} \simeq \mathbb{Z}_m$;*

Доказательство. 1) Легко проверить, что $\sqrt[n]{1}$ подгруппа в K^*, а любая конечная подгруппа в K^* циклическая.
2) Рассмотрим многочлен $f = x^n - 1$. Тогда $f' = nx^{n-1} \neq 0$, если n не делится на $\mathrm{char}\ K$. Поэтому у f нет кратных корней. Тогда в $\sqrt[n]{1}$ ровно n элементов.
3) В этом случае $x^n - 1 = (x^m)^{p^k} - 1 = (x^m - 1)^{p^k}$. Поэтому $\sqrt[n]{1} = \sqrt[m]{1}$.

□

Определение 8. *Элемент $\varepsilon \in \sqrt[n]{1}$ называется* ***первообразным корнем степени*** *n из единицы, если он порождает группу $\sqrt[n]{1}$.*

Далее до конца параграфа, мы будем работать над полем $\mathbb{C}$.

Определение 9. *Многочлен $\Phi_n = \prod(x - \varepsilon_k) \in \mathbb{C}[x]$, где произведение берется по всем первообразным корнями степени n из 1, называется* ***многочленом деления круга****.*

Утверждение 9.

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Более того, $\Phi_n(x) \in \mathbb{Z}[x]$.

Доказательство. Первое утверждение следует из того, что

$$\mathbb{Z}_n = \sqcup_{d|n} \mathbb{Z}_d^*.$$

Второе доказывается индукцией по n. Если $n = 1$, то $\Phi_1(x) = x - 1$. Если мы доказали, для всех $k < n$, то

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n} \Phi_d(x)}.$$

В знаменателе стоит приведенный целочисленный многочлен. Если целочисленный многочлен делится на некоторый приведенный целочисленный многочлен, то частно будет тоже целочисленным (следует из деления уголком). □

Утверждение 10. *Многочлен $\Phi_n(x)$ является неприводимым над $\mathbb{Q}$. В частности, $\Phi_n(x)$ является минимальным многочленом над $\mathbb{Q}$ для любого первообразного корня степени n из единицы.*

Пусть ε — первообразный корень степени n из единицы и μ — минимальный многочлен над $\mathbb{Q}$ для ε.

Лемма 2. *1. $\mu \in \mathbb{Z}[x]$;*

2. Предположим, что $\mu(a) = 0$. Тогда $\mu(a^p) = 0$ для любого простого p взаимно простого с n.

Доказательство. 1) Многочлен $f = x^n - 1$ делится на μ. Тогда $f = \mu g$, где $g \in \mathbb{Q}[x]$. Существуют целые взаимно простые числа a, b, такие что $f = \frac{a}{b}\mu' g'$, где μ' и g' — целочисленные многочлены, у каждого из которых коэффициенты взаимно простые в совокупности, и μ' и g' пропорциональны μ и g соответственно. Тогда $b(x^n - 1) = a\mu' g'$.

Для любого просто p и многочлена $q \in \mathbb{Z}[x]$ через $\overline{q}$ будем обозначать многочлен из $\mathbb{Z}_p[x]$, который получается из q заменой всех коэффициентов на остатки по модулю p.

Пусть $b \neq \pm 1$ и b делится на некоторое простое p. Тогда

$$0 = \overline{bf} = \overline{a\mu' g'}.$$

Число a не делится на p, а так как у μ' и g' коэффициенты взаимно простые в совокупности, то $\mu' \neq 0$ и $' \neq 0$. В кольце $\mathbb{Z}_p[x]$ нет делителей нуля. Поэтому получаем противоречие:

$$0 = \overline{a}\mu'\overline{g'} \neq 0.$$

Следовательно, можно считать, что $b = 1$. Но если $a \neq \pm 1$, то a делится на некоторое простое p и мы опять получаем противоречие:

$$0 \neq \overline{f} = \overline{a\mu' g'} = 0.$$

Поэтому можно считать, что $a = 1$. Тогда μ' и g' приведенные многочлены, откуда следует, что $\mu = \mu'$ и $g = g'$.

2) Заметим, что $f(a) = \mu(a)g(a) = 0$. Так как корни f — группа, то $f(a^p) = 0$. Предположим, что $\mu(a^p) \neq 0$. Тогда $g(a^p) = 0$. Рассмотрим многочлен $h(x) = g(x^p)$. Получаем, что $h(a) = 0$. Отсюда следует, что h делится на μ. Тогда $h = \mu \cdot q$, где $q \in \mathbb{Z}[x]$.

Имеем:

$$\overline{\mu q} = \overline{h} \in \mathbb{Z}_p[x].$$

Над полем $\mathbb{Z}_p$ верно равенство $\overline{h}(x) = \overline{g}(x^p) = (\overline{g}(x))^p$. Тогда $\overline{\mu q} = \overline{g}^p$. Но тогда $\overline{\mu}$ и $\overline{g}$ не могут быть взаимно простыми. Следовательно, у $\overline{f} = \overline{x^n - 1} = \overline{\mu g}$ есть кратный корень в поле разложения. Но $\overline{f'} = \overline{nx^{n-1}} \neq 0$, когда n не делится на p. □

Доказательство. (Доказательство утверждения 10)

Все первообразные корни из единицы степени n имеют вид ε^k, где $k = p_1^{a_1} \dots p_r^{a_r}$ и все p_i взаимно простые с n. Тогда

$$\varepsilon^k = (\dots((\varepsilon)^{p_1})^{p_1} \dots)^{p_r}.$$

Из леммы следует, что $\mu(\varepsilon^k) = 0$. Но тогда μ делится на $\Phi_n(x)$. Но так как μ неприводим, то получаем, что $\mu = \Phi_n(x)$.

□

Задача 23. *1. Постройте явно поля $\mathbb{F}_8$ и $\mathbb{F}_9$. Найдите порождающие в $\mathbb{F}_8^*$ и $\mathbb{F}_9^*$.*

2. Сколько подполей в поле из p^{2^n} элементов?

Задача 24. *Докажите, что конечное поле не может быть алгебраически замкнутым.*

Задача 25. *1. Постройте многочлены Φ_8 и $\Phi_{10} \in \mathbb{Z}[x]$.*

2. Пусть p — простое число. Найдите $\Phi_p(x) \in \mathbb{Z}[x]$.

Задача 26. *Докажите, что над полем $\mathbb{Z}_p$ многочлен $\Phi_{p-1}(x)$ приводим при $p > 3$.*

2.3 Сопряженные элементы. Нормальные и сепарабельные расширения

Определение 10. *Пусть L/K — расширение полей. Элементы α и β из L называются* ***сопряженными*** *над K, если $\mu_\alpha^K = \mu_\beta^K$.*

Легко видеть, что элементы α и β сопряжены тогда и только тогда, когда $\mu_\alpha^K(\beta) = 0$.

Пример 11. *В расширении $\mathbb{C}/\mathbb{Q}$ элементы $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$ сопряжены (общий минимальный многочлен $x^4 - 2$).*

В расширении $\mathbb{C}/\mathbb{Q}(\sqrt{2})$ сопряжены элементы $\sqrt[4]{2}, -\sqrt[4]{2}$ (общий минимальный многочлен $x^2 - \sqrt{2}$), а также $i\sqrt[4]{2}, -i\sqrt[4]{2}$ (минимальный многочленх$^2 + \sqrt{2}$), но $\sqrt[4]{2}$ и $i\sqrt[4]{2}$ не сопряжены.

В расширении $\mathbb{C}/\mathbb{Q}(\sqrt[4]{2})$ сопряжены элементы $i\sqrt[4]{2}, -i\sqrt[4]{2}$. Элементы $\sqrt[4]{2}$ и $-\sqrt[4]{2}$ образуют отдельные классы сопряженности.

В расширении $\mathbb{C}/\mathbb{R}$ сопряженным элементом к $z \in \mathbb{C}$ является $\overline{z}$.

Замечание 1. *Пусть $K \subseteq P \subseteq L$ — башня полей. Тогда классы сопряженности в L над K — объединение классов сопряженности в L над P.*

Теорема 5. *Пусть L/K — расширение полей и $\alpha, \beta \in L$. Предположим, что многочлены $\mu_\alpha^K, \mu_\beta^K$ раскладывается на линейные множители в L и*

$$\mu_\alpha^K = (x - \alpha_1)\dots(x - \alpha_n),\ \alpha_i \in L, \quad \mu_\beta^K = (x - \beta_1)\dots(x - \beta_m),\ \beta_j \in L.$$

Обозначим через $*$ одну из операций $+, -, \cdot, /$. Тогда сопряженные элементы с $\alpha * \beta$ содержатся среди элементов $\alpha_i * \beta_j$.

Лемма 3. *Пусть L/K — расширение полей и пусть дано два многочлена*

$$f = (x - \alpha_1)\dots(x - \alpha_n) \in K[x], \quad F(x_1, \dots, x_n, y) \in K[x_1, \dots, x_n, y],$$

где $\alpha_1, \dots, \alpha_n \in L$ и F симметричен по $x_1, \dots, x_n$. Тогда $F(\alpha_1, \dots, \alpha_n, y) \in K[y]$.

Доказательство. Пусть

$$F(x_1, \dots, x_n, y) = \sum_i F_i(x_1, \dots, x_n) y^i,$$

где $F_i \in K[x_1, \dots, x_n]$ — симметрические многочлены. По теореме о симметрических многочленах

$$F_i(x_1, \dots, x_n) = G_i(\sigma_1, \dots, \sigma_n).$$

Здесь $G_i \in K[x_1, \dots, x_n]$ и $\sigma_1, \dots, \sigma_n$ — элементарные симметрические многочлены.

Пусть $f = x_n + a_{n-1}x^{n-1} + \dots + a_0$, где $a_i \in K$. По формулам Виета $\sigma_i(\alpha_1, \dots, \alpha_n) = (-1)^i a_{n-i} \in K$. Поэтому $F_i(\alpha_1, \dots, \alpha_n) \in K$. □

Доказательство. (Теоремы 5)

Рассмотрим многочлен

$$F(x, y_1, \dots, y_m) = \prod_j \prod_i (x - \alpha_i - y_j) = \prod_j \mu_\alpha^K(x - y_j).$$

Многочлен $F(x, y_1, \dots, y_m)$ симметричен по $y_1, \dots, y_m$. Из леммы 3 следует, что $F(x, \beta_1, \dots, \beta_m) \in K[x]$. С другой стороны у $F(x, \beta_1, \dots, \beta_m)$ есть корень $\alpha+\beta$. Следовательно, $\mu_{\alpha+\beta}^K(x) \mid F(x, \beta_1, \dots \beta_m)$. Но у многочлена $F(x, \beta_1, \dots, \beta_m)$ корни — $\alpha_i + \beta_j$. Поэтому корни $\mu_{\alpha+\beta}^K(x)$ содержатся среди элементов $\alpha_i + \beta_j$. □

Теорема 6. *Пусть L/K — расширение полей, $\alpha \in L$ и*

$$\mu_\alpha^K(x) = (x-\alpha_1)\dots(x-\alpha_n) \in K[x],$$

где $\alpha_i \in L$. Тогда $\{f(\alpha_1),\dots,f(\alpha_n)\}$ — множество сопряженных элементов с $f(\alpha)$.

Замечание 2. *Среди $f(\alpha_1)\dots f(\alpha_n)$ элементы могут повторяться.*

Доказательство. Рассмотрим многочлен $g(x) = \mu_{f(\alpha)}^K(f(x)) \in K[x]$. Тогда $g(\alpha) = 0$. Следовательно, $\mu_\alpha \mid g$. Поэтому $\alpha_1,\dots,\alpha_n$ — корни g, но тогда $f(\alpha_1),\dots,f(\alpha_n)$ — корни $\mu_{f(\alpha)}^K$. Следовательно, $f(\alpha_1),\dots,f(\alpha_n)$ сопряжены с $f(\alpha)$.

Рассмотрим многочлен

$$H(x,y_1,\dots,y_n) = \prod_i (x - f(y_i)) \in K[x,y_1,\dots,y_n]).$$

Тогда многочлен $h(x) = H(x,\alpha_1,\dots,\alpha_n) \in K[x]$ по лемме 3. Но тогда $h(f(\alpha)) = 0$ и $\mu_{f(\alpha)}^K \mid h$. Следовательно, все корни $\mu_{f(\alpha)}^K$ содержаться среди $f(\alpha_1),\dots f(\alpha_n)$. Значит у $f(\alpha)$ нет других сопряженных кроме $f(\alpha_1),\dots f(\alpha_n)$.

□

Задача 27. *1. Найдите в $\mathbb{C}$ все элементы сопряженные с $\sqrt{2}+\sqrt{5}$ над $\mathbb{Q}$.*

2. Найдите в $\mathbb{C}$ все элементы сопряженные с $\sqrt{2}+\sqrt{5}$ над $\mathbb{Q}(\sqrt{5})$.

3. Для поля $\mathbb{F}_4 \simeq \mathbb{Z}[x]/(x^2+x+1)$ найдите сопряженные элементы с $\overline{x}$ над $\mathbb{Z}_2$. Найдите остальные классы сопряженности над $\mathbb{Z}_2$.

Определение 11. *Расширение L/K называется **нормальным**, если оно алгебраическое и для каждого элемента $\alpha \in L$ минимальный многочлен μ_α^K раскладывается на линейные множители в L.*

Пример 12. *Любое расширение степени 2 нормально.*

Пример 13. *Расширение $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ненормально.*

Пример 14. *Расширение $\mathbb{A}/\mathbb{Q}$ нормальное, но не конечное. (Здесь $\mathbb{A}$ — поле алгебраических чисел.)*

Пример 15. *Расширение $\mathbb{C}/\mathbb{Q}$ ненормально, так как не алгебраическое.*

Теорема 7. *Конечные нормальные расширения — это в точности поля разложения многочленов.*

Доказательство. Всякое конечное расширение имеет вид $L = K(\alpha_1,\dots,\alpha_n)$, где $\alpha_i \in L$ — алгебраические над K. Если L нормально над K, то $L = K(f)$, где $f = \mu_{\alpha_1}\dots\mu_{\alpha_n}$. Действительно, $\alpha_1,\dots,\alpha_n$ — корни f, поэтому $L \subseteq K(f)$. Но так как L нормально над K, то все остальные корни f также содержаться в L, поэтому $K(f) \subseteq L$.

Теперь докажем, что любое поле разложения — конечное нормальное расширение. Конечность тривиальна, так как поле разложение порождено конечным числом алгебраических элементов. Остается доказать нормальность.

Пусть $L = K(f)$, где $f(x) = (x-\alpha_1)\dots(x-\alpha_n) \in K[x]$, $\alpha_i \in L$. Любой элемент из L имеет вид $g(\alpha_1,\dots,\alpha_n)$, где $g(x_1,\dots,x_n) \in K[x_1,\dots,x_n]$. Докажем, что сопряженные элементы с

$g(\alpha_1, \ldots, \alpha_n)$ имеют вид $g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \in L$, где σ — некоторая перестановка. Рассмотрим многочлен

$$H(x, y_1, \ldots, y_n) = \prod_{\sigma \in S_n} (x - g(y_{\sigma(1)}, \ldots, y_{\sigma(n)})).$$

По лемме 3 многочлен $h(x) = H(x, \alpha_1, \ldots, \alpha_n) \in K[x]$. При этому $h(g(\alpha_1, \ldots, \alpha_n)) = 0$. Значит многочлен $\mu^K_{g(\alpha_1,\ldots,\alpha_n)}$ делит h, который раскладывается на линейные множители. Следовательно, $\mu^K_{g(\alpha_1,\ldots,\alpha_n)}$ раскладывается на линейные множители. □

Задача 28. *Какие из следующих расширений нормальны?*

1. $\mathbb{Q}(i\sqrt[6]{3})/\mathbb{Q}$;
2. $\mathbb{C}(t)/\mathbb{C}(t^4)$;
3. $\mathbb{R}(t)/\mathbb{R}(t^4)$;

Определение 12. *Многочлен $f \in K[x]$ называется* ***сепарабельным****, если f не имеет кратных корней в $K(f)$. Пусть L/K — расширение полей. Элемент $\alpha \in L$ называется* ***сепарабельным****, если μ^K_α — сепарабельный. Расширение полей называется* ***сепарабельным****, если все его элементы сепарабельны.*

Пример 16. *Рассмотрим расширение $\mathbb{Z}_p(x)/\mathbb{Z}_p(x^p)$. Тогда элемент $x \in \mathbb{Z}_p(x)$ несепарабельный над $\mathbb{Z}_p(x^p)$. Действительно, $\mu_x(t) = t^p - x^p = (t - x)^p$.*

Задача 29. *Найдите в $\mathbb{Z}_p(t)$ все элементы сепарабельные над $\mathbb{Z}_p(t^p)$.*

Утверждение 11.
1. *Многочлен $f \in K[x]$ сепарабельный тогда и только тогда, когда $(f, f') = 1$.*
2. *Пусть $f \in K[x]$ — неприводимый многочлен. Тогда f несепарабельный тогда и только тогда, когда $f' = 0$.*
3. *Многочлен $f \in K[x]$ неприводимый и несепарабельный. Тогда* $\operatorname{char} K = p > 0$ *и $f = g(x^p)$, $g \in K[x]$.*
4. *Если α алгебраический над K и несепарабельный, то $(\mu^K_\alpha)' = 0$.*

Доказательство. Первое утверждение доказывается в курсе алгебры. Остальные тривиально вытекают из первого. □

Определение 13. *Поле K называется* ***совершенным****, если все его алгебраические расширения сепарабельны.*

Утверждение 12.
1. *Пусть* $\operatorname{char} K = 0$. *Тогда K совершенно.*
2. *Пусть $|K| < \infty$. Тогда K совершенно.*

Доказательство. 1) Следует из пункта 3 предложения 11.

2) Пусть поле K конечное и α — алгебраический над K элемент. Тогда $K(\alpha)$ — конечное поле. Пусть $|K(\alpha)| = p^n$. Тогда $K(\alpha)$ — поле разложения многочлена $x^{p^n} - x$ и α — корень этого многочлена. Но тогда $\mu_\alpha \mid x^{p^n} - x$. У $x^{p^n} - x$ нет кратных корней. Поэтому и у μ_α нет кратных корней. □

Теорема 8. *(О примитивном элементе) Пусть L/K — расширение полей и $L = K(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n \in L$ — сепарабельные над K элементы. Тогда существует $w \in L$, такое что $L = K(w)$.*

Определение 14. *Элемент w называется* ***примитивным*** *для расширения L/K.*

Пример 17. *Пусть $L = \mathbb{Q}(x^3-2) = \mathbb{Q}(\sqrt[3]{2})(e^{\frac{2\pi}{3}i})$. Расширение $L/\mathbb{Q}$ сепарабельно. Поэтому в L есть примитивный элемент. Например, $2\sqrt[3]{2} + \sqrt[3]{2}e^{\frac{2\pi}{3}i}$.*

Пример 18. *У расширения $\mathbb{Z}_2(x,y)/\mathbb{Z}_2(x^2,y^2)$ нет примитивных элементов. Действительно, $[\mathbb{Z}_2(x,y) : \mathbb{Z}_2(x^2,y^2)] = 4$. Но при этом для любого $w \in \mathbb{Z}_2(x,y)$ мы имеем $w^2 \in \mathbb{Z}_2(x^2,y^2)$. Но тогда $[\mathbb{Z}_2(x^2,y^2)(w) : \mathbb{Z}_2(x,y)] = 2$.*

Доказательство. (теоремы о примитивном элементе)

Пусть $|K| < \infty$. Так как L порождено над K конечным числом алгебраических элементов, то L — конечное расширение K. Но тогда $|L| < \infty$. Но тогда в качестве w можно взять порождающий элемент L^*.

Далее считаем, что $|K| = \infty$. Достаточно доказать для $n = 2$, то есть $L = K(\alpha_1, \alpha_2)$. Будем искать w в виде $w = \alpha_1 + s\alpha_2$, где $s \in K^*$. Заметим, что если $\alpha_2 \in K(w)$, то $K(w) = K(\alpha_1, \alpha_2)$.

Многочлены $\mu^K_{\alpha_2}(x)$ и $\mu^K_{\alpha_1}(w - sx)$ имеют общий корень α_2. Предположим, что

$$(\mu^K_{\alpha_2}(x), \mu^K_{\alpha_1}(w - sx)) = x - \alpha_2.$$

Многочлены $\mu^K_{\alpha_2}(x)$ и $\mu^K_{\alpha_1}(w-sx)$ принадлежат кольцу $K(w)[x]$. Но тогда и их НОД принадлежит $K(w)[x]$. Но в этом случае $\alpha_2 \in K(w)$, а тогда $K(w) = K(\alpha_1, \alpha_2)$.

Докажем, что можно выбрать $s \in K^*$ так, что $(\mu^K_{\alpha_2}, \mu^K_{\alpha_1}(w - sx)) = x - \alpha_2$. Пусть

$$\mu^K_{\alpha_2}(x) = (x - \beta_1)\dots(x - \beta_m), \quad \mu^K_{\alpha_1}(x) = (x - \gamma_1)\dots(x - \gamma_r),$$

где β_i и γ_j принадлежат полю разложению многочлена $\mu_{\alpha_1}\mu_{\alpha_2}$ над L.

Общие корни многочленов $\mu^K_{\alpha_2}(x)$ и $\mu^K_{\alpha_1}(w-sx)$ — элементы β_i, для которых есть γ_j, такие что $w - s\gamma_i = \beta_i$. Но тогда получаем, что $\alpha_1 - \beta_i = s(\gamma_i - \alpha_2)$. Есть только конечное число s, таких что последнее равенство выполнено при $\gamma_i \neq \alpha_2$. Если выберем любое другое, то получаем, что α_2 — единственный общий корень $\mu^K_{\alpha_2}(x)$ и $\mu^K_{\alpha_1}(w - sx)$. Так как α_2 сепарабелен, то у $\mu^K_{\alpha_2}(x)$ нет кратных корней. Поэтому для выбранного s получаем $(\mu^K_{\alpha_2}(x), \mu^K_{\alpha_1}(w - sx)) = x - \alpha_2$.

□

2.4 Расширения Галуа. Группа Галуа

Пусть L/K — расширение полей. Обозначим через $\mathrm{Aut}(L)$ группу автоморфизмов L. Рассмотрим подгруппу

$$\mathrm{Aut}_K(L) = \{\varphi \in \mathrm{Aut}(L) \mid \varphi(a) = a,\ \forall a \in K\}.$$

Для любого $\varphi \in \mathrm{Aut}_K(L)$ обозначим

$$L^\varphi = \{b \in L \mid \varphi(b) = b\}.$$

Лего видеть, что L^φ — подполе в L, содержащее K. Также для любой подгруппы $H \leq \mathrm{Aut}_K(L)$ рассмотрим множество

$$L^H = \{b \in L \mid \varphi(b) = b,\ \forall \varphi \in H\} = \bigcap_{\varphi \in H} L^\varphi.$$

Утверждение 13. *Пусть $\alpha \in L, f \in K[x],\ f(\alpha) = 0$ и $\varphi \in \mathrm{Aut}_K(L)$. Тогда $f(\varphi(\alpha)) = 0$.*

Доказательство. Пусть $f(x) = a_n x^n + \dots a_0$, где $a_i \in K$. Тогда $0 = f(\alpha) = a_n\alpha^n + \dots + a_0$. Но тогда

$$0 = \varphi(f(\alpha)) = \varphi(a_n\alpha^n + \dots + a_0) = \varphi(a_n)\varphi(\alpha)^n + \dots + \varphi(a_0) = a_n\varphi(\alpha^n) + \dots + a_0 = f(\varphi(\alpha)).$$

□

Утверждение 14. *Пусть L/K — конечное расширение. Тогда $|\mathrm{Aut}_K(L)| \le [L : K]$.*

Доказательство. Пусть $L = K(\alpha_1, \dots, \alpha_n)$. Заметим, что любой автоморфизм $\varphi \in \mathrm{Aut}_K(L)$ — продолжение тождественного вложения $\varphi_0 : K \to L$. Положим $K_i = K(\alpha_1, \dots, \alpha_i)$. Число продолжений некоторого вложения $\varphi_{i-1} : K_{i-1} \to L$ до вложения $\varphi_i : K_i \to L$ равно числу корней многочлена $\mu_{\alpha_i,\varphi_{i-1}}^{K_{i-1}}(x)$ в L, что не превосходит степени многочлена $\mu_{\alpha_i}^{K_{i-1}}(x)$. (смотри лемму 1).

Поэтому число способов продолжить φ_0 до вложения $L \to L$ не превосходит число

$$\prod_i \deg\, \mu_{\alpha_i}^{K_{i-1}}(x) = [K_1 : K][K_2 : K_1] \dots [L : K_{n-1}] = [L : K].$$

□

Пример 19. *Группа $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ состоит из двух автоморфизмов. Первый — тождественный, второй — комплексное сопряжение ($z \to \overline{z}$). Так как $[\mathbb{C} : \mathbb{R}] = 2$, то других автоморфизмов в $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ нет.*

Пример 20. *Группа $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ тривиальна. Действительно, любой автоморфизм $\varphi \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ определяется образом $\sqrt[3]{2}$. Но $\sqrt[3]{2}$ может перейти только в корень многочлена $x^3 - 2$ (см. предложение 13). Однако в $\mathbb{Q}(\sqrt[3]{2})$ у $x^3 - 2$ кроме $\sqrt[3]{2}$ нет корней.*

Теорема 9. *Пусть L/K — конечное расширение полей и $G = \mathrm{Aut}_K(L)$. Тогда следующие условия эквивалентны:*

1. *$|G| = [L : K]$;*
2. *$L^G = K$;*
3. *L/K — нормальное сепарабельное расширение;*
4. *L — поле разложения некоторого сепарабельного многочлена $f \in K[x]$.*

Доказательство. 1) $\implies$ 2). Заметим, что $\mathrm{Aut}_K(L) = \mathrm{Aut}_{L^G}(L)$. Поэтому

$$|G| = [L : K] = [L : L^G][L^G : K] \ge [L : L^G] \ge |\mathrm{Aut}_{L^G}(L)| = |G|.$$

Такое возможно, только когда $[L^G : K] = 1$, что означает $L^G = K$.

2) $\implies$ 3). Пусть $\alpha \in L$. Рассмотрим многочлен

$$f(x) = \prod_{\varphi \in G} (x - \varphi(\alpha).$$

Легко видеть, что $\psi(f) = f$ для любого $\psi \in G$. Поэтому $f \in K[x]$. Но $f(\alpha) = 0$, поэтому $\mu_\alpha^K \mid f$. Так как f раскладывается в L на линейные множители, то и μ_α^K раскладывается. Поэтому L/K нормально.

Чтобы доказать сепарабельность α нужно доказать, что у μ_α нет кратных корней. Для этого рассмотрим подгруппу $H = \{\varphi \in G \mid \varphi(\alpha) = \alpha\}$. Тогда рассмотрим многочлен

$$h(x) = \prod_{\varphi H \in G/H} (x - \varphi(\alpha)).$$

(То есть берем произведение по всем левым смежным классам из G по H). Легко убедиться, что $\psi(h) = h$ для всех $\psi \in G$, откуда следует, что $h \in K[x]$. Но у h нет кратных корней. Действительно, если $\varphi_1(\alpha) = \varphi_2(\alpha)$ тогда и только тогда, когда $\varphi_1\varphi_2^{-1} \in H$, что означает $\varphi_1 H = \varphi_2 H$.

Опять μ_α^K делит h, поэтому у μ_α^K нет кратных корней.

3) $\Longrightarrow$ 4). Воспользуемся теоремой о примитивном элементе. Тогда $L = K(w)$. Рассмотрим $f = \mu_w^K(x)$. Тогда $\mu_w^K(x)$ — сепарабельный над K, так как L/K — сепарабельное расширение.

Но тогда L — поле разложения f над K.

4) $\Longrightarrow$ 1). Пусть $L = K(f)$, где f — сепарабельный многочлен. Тогда $L = K(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n$ — корни f. Положим $K_i = K(\alpha_1, \ldots, \alpha_i)$. Далее повторяем рассуждения из доказательства утверждения 14 и замечаем, что многочлен $\mu_{\alpha_i,\varphi_{i-1}}^{K_{i-1}}$ делит $f_{\varphi_{i-1}}$, который равен f, так как $\varphi_{i-1}|_K = \mathrm{id}$. Но f раскладывается на линейные множители в L и не имеет кратных корней. Поэтому число корней в L у $\mu_{\alpha_i,\varphi_{i-1}}^{K_{i-1}}$ равно его степени. Поэтому число способов продолжить $\varphi_{i-1} : K_{i-1} \to L$ до $\varphi_i : K_i \to L$ равно степени $\mu_{\alpha_i,\varphi_{i-1}}^{K_{i-1}}$. В итоге число способов продолжить тождественное вложение K в L до автоморфизма L равно $[L : K]$. □

Определение 15. *Пусть L/K — конечное расширение, удовлетворяющие одному (всем) из свойств теоремы 9. Тогда L/K называется* ***расширением Галуа****, а группа* $\mathrm{Aut}_K(L)$ *называется* ***группой Галуа*** *расширения L/K и обозначается* $\mathrm{Gal}_K(L)$ *или* $\mathrm{Gal}(K/L)$.

Пример 21. *Расширение $\mathbb{C}/\mathbb{R}$ является расширением Галуа. Например, потому что* $|\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})| = 2 = [\mathbb{C} : \mathbb{R}]$. *Группа Галуа этого расширения* $\mathrm{Gal}_{\mathbb{R}}(\mathbb{C}) \simeq \mathbb{Z}_2$.

Пример 22. *Пусть* $\mathrm{char}\ K = 0$ *и* $[L : K] = 2$. *Тогда L/K — расширение Галуа. Действительно, $L = K(f)$, где f — минимальный многочлен любого элемента $\alpha \in L$. Многочлен f сепарабелен, так как* $\mathrm{char}\ K = 0$. *Группа Галуа этого расширения тоже изоморфна $\mathbb{Z}_2$. Единственный автоморфизм переводит каждый элемент в его сопряженный.*

Пример 23. *Расширение $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ не нормально, поэтому это не расширение Галуа.*

Пример 24. *Расширение $\mathbb{Q}(x^3 - 2)/\mathbb{Q}$ расширение Галуа (по свойству 4). Любой автоморфизм из* $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(x^3 - 2))$ *переставляет корни многочлена $x^3 - 2$, которые порождают $\mathbb{Q}(x^3 - 2)$ над $\mathbb{Q}$. Поэтому* $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(x^3 - 2))$ *изоморфна подгруппе в S_3. Но* $|\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(x^3 - 2))| = 6$, *поэтому* $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(x^3 - 2)) \simeq S_3$.

Пример 25. *Поле $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}((x^2 - 2)(x^2 - 3))$ является расширением Галуа поля $\mathbb{Q}$. Его степень равна 4. Каждый автоморфизм отправляет $\sqrt{2} \to \pm\sqrt{2}$ и $\sqrt{3} \to \pm\sqrt{3}$. Поэтому каждый автоморфизм в квадрате тождественен. Следовательно,* $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Утверждение 15. *1. Расширение $\mathbb{F}_{p^n}/\mathbb{Z}_p$ — расширение Галуа и $\mathrm{Gal}_{\mathbb{Z}_p}(\mathbb{F}_{p^n}) = \langle\varphi\rangle \simeq \mathbb{Z}_n$, где φ — автоморфизм Фробениуса.*

2. Пусть $q = p^n$. Тогда расширение $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение Галуа и $\mathrm{Gal}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = \langle\varphi^n\rangle \simeq \mathbb{Z}_m$.

Доказательство. 1) Степень расширения n, поэтому достаточно доказать, что автоморфизм Фробениуса имеет порядок n. Если $\varphi^k = \mathrm{id}$, где $k < n$, то $a^{p^k} = a$ для любого элемента $a \in \mathbb{F}_{p^n}$, но это не верно для порождающего мультипликативной группы поля $\mathbb{F}_{p^n}$.

2) φ^n — автоморфизм $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$, который имеет порядок m, что равно степени расширения. □

Следствие 8. *Пусть $h \in \mathbb{F}_q[x]$ — неприводимый многочлен. Тогда $\mathbb{F}_q(h) \simeq \mathbb{F}_q/(h)$.*

Доказательство. Действительно, расширение $\mathbb{F}_q(h) \simeq \mathbb{F}_q[x]/(h)/\mathbb{F}_q$ — расширение Галуа, поэтому оно нормально. Многочлен h является минимальным многочленом для элемента $\overline{x}$. Поэтому он раскладывается в $\mathbb{F}_q[x]/(h)$ на линейные множители. □

Задача 30. *Какие из следующих расширений L/K являются расширениями Галуа? Найдите соответствующие группы* $\mathrm{Aut}_K(L)$.

1. $L/K = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.
2. $L/K = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$.
3. $L/K = \mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$.

Задача 31. *Является ли расширение $L/K = \mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ расширением Галуа? Найдите группу* $\mathrm{Aut}_K(L)$.

Задача 32. *Пусть $\varphi \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$.*

1. *Докажите, что φ переводит квадраты в квадраты, а положительные числа в положительные. Докажите, что если $a < b$, то $\varphi(a) < \varphi(b)$.*
2. *Докажите, что если $-\frac{1}{m} < a - b < \frac{1}{m}$, где $m \in \mathbb{Z}$, то $-\frac{1}{m} < \varphi(a) - \varphi(b) < \frac{1}{m}$. Выведите отсюда, что φ — непрерывное отображение.*
3. *Докажите, что группа* $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ *тривиальна.*

2.5 Основная теорема теории Галуа

Определение 16. *Пусть $f \in K[x]$ — сепарабельный многочлен.* ***Группой Галуа*** *многочлена f над полем K называется группа Галуа расширения $K(f)/K$. Обозначение:* $\mathrm{Gal}_K f$.

Лемма 4. *Пусть $L = K(w)$ и $\mu_w^K = (x-w_1)\dots(x-w_s)p_1(x)\dots p_r(x)$, где $w_i \in L$ и $p_1(x)\dots p_r(x) \in L[x]$ — неприводимые многочлены над K степени больше 1. При этом $w_i \neq w_j$. Тогда $|\mathrm{Aut}_K L| = s$ и все автоморфизмы L над K имеют вид $f(w) \to f(w_i)$.*

Доказательство. Пусть $\varphi \in \mathrm{Aut}_K L$. Тогда $\varphi(w)$ — корень $\mu_w^K(x)$, поэтому $\varphi(w) = w_i \in \{w_1, \dots, w_s\}$. Но тогда для любого $f \in K[x]$ мы имеем $\varphi(f(w)) = f(\varphi(w)) = f(w_i)$.

С другой стороны, легко проверить, что отображение $f(w) \to f(w_i)$ является автоморфизмом L над K. □

Заметим, что группа $\mathrm{Gal}_K L$ действует на L, а группа $\mathrm{Gal}_K f$ действует на $K(f)$ (в обоих случая результат действия автоморфизма φ на элемент a есть $\varphi(a)$).

Утверждение 16. *Пусть L/K — расширение Галуа, а f — сепарабельный многочлен.*

1. *Тогда орбиты* $\mathrm{Gal}_K L$ *это в точности классы сопряженности в L над K.*
2. $\mathrm{Gal}_K f$ *сохраняет корни f.*
3. $\mathrm{Gal}_K f$ *действует транзитивно на корнях f тогда и только, тогда когда f неприводим над K.*

Доказательство. 1) Так как L/K, то существует $w \in L$, такое что $L = K(w)$. Так как L/K — нормальное сепарабельное расширение, то многочлен $\mu_w^K(x)$ раскладывается в L на линейные множители и не имеет кратных корней:

$$\mu_w^K(x) = (x - w_1)\dots(x - w_n),\ w_i \neq w_j.$$

Произвольный элемент $a \in L$ имеет вид $f(w)$ для некоторого многочлена $f \in K[x]$. По теореме 6 класс сопряженности с a в L состоит из элементов $f(w_1), \dots f(w_n)$. Но по предыдущей лемме элементы $f(w_i)$ лежат в одной орбите с элементом $f(w)$.

2) Следует из утверждения 13.

3) Если f неприводим над K, то f — минимальный многочлен над K для своих корней. В этому случае из п 1) следует, что группа Галуа действует транзитивно на корнях. Если f приводим, то $f = gh$, где $gh \in K[x]$ и не имеют общих корней в L. Но тогда группа Галуа переставляет отдельно корни g, и отдельно h.

□

Пусть L/K — расширение Галуа. Обозначим через G группу Галуа $\mathrm{Gal}_K L$. Через $\mathcal{L}(K, L)$ — множество подполей в L, которые содержат K. Тогда определим отображения

$$H \leq G \to L^H = \{a \in L \mid (a) = a,\ \forall \varphi \in K\}$$

и

$$P \in \mathcal{L}(K, L) \to G_P = \{\varphi \in G \mid \varphi(p) = p, \forall p \in P\}.$$

Теорема 10. *(Основная теорема теории Галуа, часть 1)*
Пусть L/K — расширение Галуа.

1. *Отображения $H \to L^H$ и $P \to G_P$ взаимно обратные, и устанавливают биекции между множеством всех подгрупп в группе G и элементами $\mathcal{L}(K, L)$. При этом эти биекции обращают включения, то есть если $H_1 \subseteq H_2$, то $L^{H_2} \subseteq L^{H_1}$, а если $P, Q \in \mathcal{L}(K, L)$ и $P \subseteq Q$, то $G_Q \leq G_P$.*

2. *Если $P \in \mathcal{L}(K, L)$, то L/P — расширение Галуа и $\mathrm{Gal}_P L = G_P$.*

3. *$[L : P] = |G_P|$ и $[P : K] = [G : G_P]$.*

4. *Если $P, Q \in \mathcal{L}(K, L)$, то $G_{P \cap Q} = \langle G_P, G_Q \rangle$ и $G_{PQ} = G_P \cap G_Q$.*

Доказательство. Докажем сначала 2). Для любого $a \in L$ минимальный многочлен $\mu_a^K(x)$ раскладывается на линейные множители в L и не имеет кратных корней, так как L/K — расширение Галуа. Многочлен $\mu_a^P(x)$ делит $\mu_a^K(x)$. Поэтому $\mu_a^P(x)$ тоже раскладывается на линейные множители и не имеет кратных корней. Поэтому L/P — расширение Галуа.

При этому группа Галуа $\mathrm{Gal}_P L$ состоит из автоморфизмов L, которые тождественны на P. Но это в точности G_P.

1) Докажем, что $G_{L^H} = H$ для любой подгруппы $H \leq G$. Нетрудно убедиться, что $G_{L^H} \geq H$. По пункту 2) расширение L/L^H — расширение Галуа и $\mathrm{Gal}_{L^H} L = G_{L^H}$. При этому $[L : L^H] = |G_{L^H}|$.

Так как L/L^H — расширение Галуа, то $L = L^H(w)$ для некоторого $w \in L$. Тогда $\deg \mu_w^{L^H}(x) = [L : L^H]$. Рассмотрим многочлен

$$g(x) = \prod_{\varphi \in H} (x - \varphi(w)).$$

Он инвариантен относительно H, поэтому $g(x) \in L^H[x]$. Так как $g(w) = 0$, то $\mu_w^{L^H}(x)$ делит g. Заметим также, что степень g равна $|H|$. Собирая все выше сказанное получаем:

$$|H| \leq |G_{L^H}| = [L : L^H] = \deg \mu_w^{L^H} \leq \deg g = |H|.$$

Отсюда $|H| = |G_{L^H}|$. Поэтому $H = G_{L^H}$.

Докажем теперь, что $L^{G_P} = P$ для любого $P \in \mathcal{L}(K, L)$. Включение $P \subseteq L^{G^P}$ тривиально. Но так как L/P — расширение Галуа и G_P — группа Галуа этого расширения, то $L^{G_P} = P$ по пункту 2) теоремы 9.

Итак мы доказали, что отображения $H \to L^H$ и $P \to G_P$ взаимно обратные, а значит биекции. То что они обращают включения проверяется тривиально.

3) Так как L/P — расширение Галуа, то $[L : P] = |G_P|$. При этом

$$|G| = [L : K] = [L : P][P : K].$$

Отсюда следует, что $[P : K] = [G : G_P]$.

4) Поле $P \cap Q$ — наибольшее подполе в $\mathcal{L}(K, L)$, содержащееся и в P, и в Q. Поэтому группа $G_{P\cap Q}$ — наименьшая подгруппа в G, содержащее и G_P, и G_Q. Поэтому это группа, порожденная G_P и G_Q.

Аналогично, PQ — наименьшее поле, содержащее и P и Q. Поэтому G_{PQ} наибольшая группа, содержащиеся и в G_P, и в G_Q.

□

Определение 17. *Пусть L/K — расширение полей. Поля $P, Q \in \mathcal{L}(K, L)$ называются **сопряженными**, если существует автоморфизм $\varphi \in \mathrm{Aut}_K L$, такой что $\varphi(P) = Q$.*

Теорема 11. *(Основная теорема теории Галуа, часть 2)*
Пусть L/K — расширение Галуа, $P, Q \in \mathcal{L}(K, P)$ и $\varphi \in G = \mathrm{Gal}_K L$. Тогда

1. *Если $\varphi(P) = Q$, то $G_Q = \varphi G_P \varphi^{-1}$.*
2. *Расширение P/K — расширение Галуа тогда и только тогда, когда группа G_P нормальна в G. В этом случае $\mathrm{Gal}_K P \simeq G/G_P$.*

Доказательство. 1)

$$\psi \in G_Q \iff \psi(q) = \varphi(q), \forall q \in Q \iff \psi(\varphi(p)) = \varphi(p), \forall p \in P \iff \varphi^{-1}\psi\varphi(p) = p, \forall p \in P \iff$$

$$\varphi^{-1}\psi\varphi \in G_P \iff \psi \in \varphi G_P \varphi^{-1}.$$

Отсюда следует, что $G_Q = \varphi G_P \varphi^{-1}$.

2) Заметим, что P/K всегда сепарабельное расширение, так как минимальные многочлены всех элементов из L над K сепарабельны. Поэтому P/K расширение Галуа тогда и только тогда, когда P/K нормальное расширение.

Расширение P/K нормально тогда и только тогда, когда вместе с каждым элементом $a \in P$ в P содержаться все сопряженные с a элементы. Так как множество сопряженных с a элементов есть орбита группы Галуа, то последнее равносильно $\varphi(P) = P$ для всех $\varphi \in \mathrm{Gal}_K L$. Поля $\varphi(P)$ и P совпадают тогда и только тогда, когда группы $G_{\varphi(P)}$ и G_P совпадают (часть 1) теоремы 10). Получаем, что P/K нормально тогда и только тогда, когда $G_{\varphi(P)} = \varphi G_P \varphi^{-1} = G_P$ для всех $\varphi \in \mathrm{Gal}_K L$. Это равносильно нормальности группы G_P в G.

Теперь докажем, что если P/K расширение Галуа, то $\mathrm{Gal}_K P \simeq G/G_P$. Рассмотрим гомоморфизм

$$\Theta : G \to \mathrm{Gal}_K P,\ \varphi \to \varphi|_P.$$

Этот гомоморфизм корректно определен, так как, если P/K нормальное расширение, то $\varphi(P) = P$ для всех $\varphi \in \mathrm{Gal}_K P$. Ядро Θ — группа G_P. Докажем сюръективность Θ.

Пусть $P = K(w)$ и $\mu_w^K = (x - w_1) \dots (x - w_s) \in P[x]$ (так как P/K расширение Галуа, то μ_w^K раскладывается в P на линейные множители и кратных корней нет). По лемме 4 все автоморфизмы P над K имеют вид $\overline{\varphi_i} : f(w) \to f(w_i)$.

Но $\{w_1, \ldots, w_s\}$ — множество сопряженных с w элементов, что есть орбита группы Галуа $\mathrm{Gal}_K L$. Поэтому есть автоморфизм φ_i, который переводит w в w_i. Но тогда $\varphi|_P = \overline{\varphi_i}$. Значит, Θ сюръективный гомоморфизм.

□

Приведем примеры соответствия Галуа.

Пример 26. *Найдем группу* $\mathrm{Gal}_{\mathbb{Q}}(x^4 - 4x^2 + 1)$. *Перечислим корни этого многочлена*

$$\alpha_1 = \sqrt{2+\sqrt{3}},\ \alpha_2 = -\sqrt{2+\sqrt{3}},\ \alpha_3 = \sqrt{2-\sqrt{3}},\ \alpha_4 = -\sqrt{2-\sqrt{3}}.$$

Мы видим, что

$$\alpha_2 = -\alpha_1, \alpha_3 = \frac{1}{\alpha_1}, \alpha_4 = -\frac{1}{\alpha_1}.$$

Поэтому $\mathbb{Q}(f) = \mathbb{Q}(\alpha_1)$ *(здесь* $f = x^4 - 4x^2 + 1$.*) Легко убедиться, что* f *неприводим над* $\mathbb{Q}$. *Поэтому* f *минимальный многочлен для* α_1 *над* $\mathbb{Q}$. *Поэтому* $[\mathbb{Q}(f) : \mathbb{Q}] = 4$. *Следовательно,* $|\mathrm{Gal}_{\mathbb{Q}}(f)| = 4$.

Из пункта 3 утверждения 16 следует, что группа Галуа действует транзитивно на множестве $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. *Так как* $\mathbb{Q}(f)$ *порождается* α_1, *то любой элемент группы Галуа однозначно определяется образом* α_1. *В итоге для каждого* i *у нас есть ровно один элемент* φ_i *группы Галуа, который переводит* α_1 *в* α_i.

Если $i = 1$, *то мы получаем тождественный автоморфизм* $\varphi_1 = id$. *Он соответствует тождественной перестановке на множестве* $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$.

Если $i = 2$, *то есть* $\varphi_2(\alpha_1) = \alpha_2$, *то*

$$\varphi_2(\alpha_2) = \varphi_2(-\alpha_1) = -\varphi(\alpha_1) = -\alpha_2 = \alpha_1,$$

$$\varphi_2(\alpha_3) = \varphi(\frac{1}{\alpha_1}) = \frac{1}{(\alpha_1)} = \frac{1}{\alpha_2} = \alpha_4$$

$$\varphi(\alpha_4) = \varphi(-\alpha_3) = -\alpha_4 = \alpha_3.$$

Получили перестановку $(12)(34)$.

Аналогично при $i = 3$ *получаем, что*

$$\varphi_3(\alpha_1) = \alpha_3,\ \varphi_3(\alpha_2) = \alpha_4,\ \varphi_3(\alpha_3) = \alpha_1, \varphi_3(\alpha_4) = \alpha_2.$$

Соответствующая перестановка — $(13)(24)$.

Для $i = 4$ *получаем*

$$\varphi_4(\alpha_1) = \alpha_4,\ \varphi_4(\alpha_2) = \alpha_3,\ \varphi_4(\alpha_3) = \alpha_2, \varphi_4(\alpha_4) = \alpha_1$$

и перестановку $(14)(23)$. *В итоге получаем, что* $\mathrm{Gal}_{\mathbb{Q}}(f) = V_4$.

В V_4 *есть пять подгрупп. Ниже указано соответствие Галуа между подгруппами и подполями в* $\mathbb{Q}(f)$*:*

$$H_0 = V_4,\ L^{H_0} = \mathbb{Q}$$

$$H_1 = \langle (12)(34) \rangle, L^{H_1} = \mathbb{Q}(\alpha_1\alpha_2) = \mathbb{Q}(\sqrt{3})$$

$$H_2 = \langle (13)(24) \rangle, L^{H_2} = \mathbb{Q}(\alpha_1 + \alpha_3) = \mathbb{Q}(\sqrt{6})$$

$$H_3 = \langle (14)(23) \rangle,\ L^{H_3} = \mathbb{Q}(\alpha_1 + \alpha_4) = \mathbb{Q}(\sqrt{2}),$$

$$H_4 = \{id\},\ L^{H_4} = \mathbb{Q}(f).$$

Пример 27. *Найдем группу* $\mathrm{Gal}_{\mathbb{Q}}(x^4-4x^2+2)$. *Перечислим корни этого многочлена*

$$\alpha_1=\sqrt{2+\sqrt{2}},\ \alpha_2=-\sqrt{2+\sqrt{2}},\ \alpha_3=\sqrt{2-\sqrt{2}},\ \alpha_4=-\sqrt{2-\sqrt{2}}.$$

Теперь имеет

$$\alpha_2=-\alpha_1, \sqrt{2}=\alpha_1^2-2, \alpha_3=\frac{\sqrt{2}}{\alpha_1},\ \alpha_4=-\frac{\sqrt{2}}{\alpha_1}.$$

Поэтому $\mathbb{Q}(f)=\mathbb{Q}(\alpha_1)$. *Опять можно проверить, что* f *неприводим, поэтому* f *—минимальный многочлен для* α_1, *следовательно,* $[\mathbb{Q}(f):\mathbb{Q}]=4$ *и* $|\mathrm{Gal}_{\mathbb{Q}}(f)|=4$.

Как и в предыдущем примере каждый элемент группы Галуа однозначно определяется образом α_1. *На этот раз получаем перестановки* $id, (12)(34), (1324), (1423)$. *То есть* $\mathrm{Gal}_{\mathbb{Q}}(x^4-4x^2+2)\simeq\langle(1324)\rangle\simeq\mathbb{Z}_4$.

В группе $\mathbb{Z}_4$ *есть три подгруппы. Получаем следующее соответствие между подгруппами и подполями:*

$$H_0=\langle(1324)\rangle\simeq\mathbb{Z}_4,\ L^{H_0}=\mathbb{Q}$$
$$H_1=\langle(12)(34)\rangle\simeq 2\mathbb{Z}_4,\ L^{H_1}=\mathbb{Q}(\alpha_1\alpha_3)=\mathbb{Q}(\sqrt{2})$$
$$H_2=\{id\},\ L^{H_2}=\mathbb{Q}(f)$$

Задача 33. *Найдите группу Галуа следующих многочленов над* $\mathbb{Q}$:

1. x^4-14x^2+9;
2. x^4+4;
3. $(x^2-2)(x^2-3)(x^2-5)$;
4. $(x^3-2)(x^3-3)$;

В каждом случае кажите все подполя в соответствующем поле разложения.

Пример 28. *Найдем группу* $\mathrm{Gal}_{\mathbb{Q}}(x^4-4x^2-1)$. *Перечислим корни* f:

$$\alpha_1=\sqrt{\sqrt{5}+2},\ \alpha_2=-\sqrt{\sqrt{5}+2},\ \alpha_3=i\sqrt{\sqrt{5}-2},\ \alpha_4=-i\sqrt{\sqrt{5}-2}.$$

Мы видим, что $\alpha_3\notin\mathbb{Q}(\alpha_1)\subseteq\mathbb{R}$. *При этому* $\mathbb{Q}(f)=\mathbb{Q}(\alpha_1)(\alpha_3)=\mathbb{Q}(\alpha_1)(i)$. *Следовательно,* $[\mathbb{Q}(f):\mathbb{Q}]=8$, *поэтому* $|\mathrm{Gal}_{\mathbb{Q}}(f)|=8$. *Каждый элемент группы* $\mathrm{Gal}_{\mathbb{Q}}(f)$ *определяется перестановкой корней* $\alpha_1,\dots,\alpha_4$. *Поэтому группа* $\mathrm{Gal}_{\mathbb{Q}}(f)$ *вкладывается в* S_4. *Но тогда это силовская 2-подгруппа в* S_4. *Все силовские 2-подгруппы сопряжены, поэтому изоморфны. Есть силовская 2-подгруппа изоморфная* D_4. *Поэтому* $\mathrm{Gal}_{\mathbb{Q}}(f)\simeq D_4$.

Расставим корни в вершины квадрата по часовой стрелке в следующем порядке: $\alpha_1,\alpha_3,\alpha_2,\alpha_4$. *Обозначим через* σ_1 *симметрию относительно диагонали* α_1,α_2; *через* σ_2 *— симметрию относительно серединного перпендикуляра к стороне* α_1,α_3; *через* σ_3 *— симметрию относительно диагонали* α_3,α_4; *и через* σ_4 *симметрию относительно серединного перпендикуляра к стороне* α_3,α_2. *Через* R_φ *обозначим поворот на угол* φ.

Тогда соответствие между подгруппами и подполями выглядит следующим образом:

$$D_4\to\mathbb{Q};$$
$$\langle\sigma_1,\sigma_3\rangle\to\mathbb{Q}(\sqrt{5});$$
$$\langle\sigma_2,\sigma_4\rangle\to\mathbb{Q}(i);$$

$$\langle R_{\frac{\pi}{2}} \rangle \to \mathbb{Q}(i\sqrt{5});$$
$$\langle \sigma_1 \rangle \to \mathbb{Q}(\alpha_1);$$
$$\langle \sigma_3 \rangle \to \mathbb{Q}(\alpha_3);$$
$$\langle R_{\pi} \rangle \to \mathbb{Q}(i, \sqrt{5});$$
$$\langle \sigma_2 \rangle \to \mathbb{Q}(\alpha_1 + \alpha_3);$$
$$\langle \sigma_4 \rangle \to \mathbb{Q}(\alpha_1 - \alpha_3);$$
$$\{0\} \to \mathbb{Q}(f).$$

Пример 29. *Пусть $f \in K[x]$ — неприводимый многочлен степени 3 и* $\mathrm{char}\ K = 0$.

Если $\sqrt{D} \notin K$, то $[K(f) : K] = 6$ и $\mathrm{Gal}_K(f) \simeq S_3$. Если мы обозначим корни f через $\alpha_1, \alpha_2, \alpha_3$, то соответствие между подгруппами S_3 и подполями в $K(f)$ выглядит следующим образом:

$$S_3 \to K;$$
$$A_3 \to K(\sqrt{D});$$
$$\langle (12) \rangle \to K(\alpha_3);$$
$$\langle (13) \rangle \to K(\alpha_2);$$
$$\langle (23) \rangle \to K(\alpha_1).$$

Если $\sqrt{D} \in K$, то $[K(f) : K] = 3$ и $\mathrm{Gal}_K(f) \simeq \mathbb{Z}_3$. В этом случае нетривиальных подполей нет.

Утверждение 17. *Пусть $f \in K[x]$ — неприводимый многочлен и* $\mathrm{char}\ K = 0$. *Обозначим через $\overline{G} = \mathrm{Gal}_K(f) \cap A_n$. Тогда*

1. $\sqrt{D} \in K \iff \overline{G} = G$;
2. $K(f)^{\overline{G}} = K(\sqrt{D})$.

Доказательство. 2) Пусть $a \in K(f)^{\overline{G}}$. Тогда $a + ga \in K(f)^G = K$ для любого $g \in G \setminus \overline{G}$. Заметим, что $g\sqrt{D} = -\sqrt{D}$ и $g(a - ga) = -(a - ga)$ для всех $g \in G \setminus \overline{G}$. Но тогда $\sqrt{D}(a - ga) \in K(f)^G = K$, то есть $a - ga \in K(\sqrt{D})$. Поэтому $a = \frac{1}{2}(a + ga + (a - ga)) \in K(\sqrt{D})$.

Пункт 1) следует из пункта 2) и основной теоремы теории Галуа. □

2.6 Разрешимость в радикалах

Напомним классические результаты про решения уравнений второй, третий и четвертой степени.

Корни многочлена $x^2 + bx + c$ над полем характеристики не 2 выражаются с помощью хорошо знакомой всем формулы:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Чтобы найти корни многочлена $x^3 + ax^2 + bx + c$ над полем характеристики не 2 и не 3 следует сначала сделать замену $x \to x - \frac{a}{3}$ и получить многочлен вида $x^3 + px + q$.

Из формулы $(a + b)^3 = 3ab(a + b) + a^3 + b^3$ следует, что число $x = (a + b)$ является корнем многочлена $x^3 - 3abx - (a^3 + b^3)$. Подберем a, b так, чтобы $-3ab = p,\ a^3 + b^3 = -q$.

Получаем $a^3b^3 = -\frac{p^3}{27},\ b^3 = -q - a^3$. Имеем квадратное уравнение на a^3 :

$$a^6 + qa^3 - \frac{p^3}{27} = 0$$

откуда

$$a^3, b^3 = \frac{-q \pm \sqrt{q - \frac{4}{27}p^3}}{2}.$$

Тогда

$$x_{1,2,3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}.$$

Последняя формула называется формулой Кардано. В ней нужно извлекать корни кубические таким образом, чтобы

$$\left(\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}\right)\left(\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}\right) = -\frac{p}{3}.$$

Наконец, чтобы найти корни уравнения $x^4 + ax^2 + bx + c$ заметим, что это легко сделать, если $b = 0$ (тогда уравнение биквадратное). Если $b \neq 0$, то введем параметр y, так чтобы последние три слагаемых образовывали полный квадрат:

$$(x^2 + \frac{y}{2})^2 + (a - y)x^2 + bx + c - \frac{y^2}{4}.$$

Дискриминант квадратного трехлена $(a - y)x^2 + bx + c - \frac{y^2}{4}$ равен

$$D(y) = b^2 - 4(a - y)(c - \frac{y^2}{4}).$$

Мы видим, что $D(y)$ — кубический многочлен. С помощью формулы Кардано находим y_1, для которого $D(y_1) = 0$. Получим многочлен вида

$$(x^2 + \frac{y_1}{2})^2 + (l)^2 = (x^2 + \frac{y_1}{2} + il)(x^2 + \frac{y_1}{2} - il),$$

где l — линейный многочлен. Корни такого многочлена легко находятся. Этот метод называется методом Феррари, а многочлен $D(y)$ называется резольвентой Феррари.

Определение 18. *Расширение L/K называется* ***простым радикальным*** *расширением, если $L = K(b)$ и $b^r \in K$.* ***Радикальной башней*** *называется башня полей:*

$$K - K_1 - K_2 - \ldots - K_n,$$

где K_i/K_{i-1} — простое радикальное расширение. Расширение L/K называется ***радикальным,*** *если существует радикальная башня*

$$K - K_1 - K_2 - \ldots - K_n = L.$$

Мы говорим, что многочлен $f \in K[x]$ ***разрешим в радикалах*** *над полем K, если существует радикальное расширение L/K, содержащее $K(f)$.*

Наша ближайшая цель доказать следующую теорему.

Теорема 12. *(Критерий разрешимости в радикалах) Пусть $f \in K[x]$ — сепарабельный многочлен и* $\mathrm{char}\ K = 0$. *Тогда следующие условия эквивалентны:*

1. *Многочлен f разрешим в радикалах;*
2. *Группа $\mathrm{Gal}_K(f)$ разрешима.*

Заметим, что если для многочлена $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{C}[x]$ есть радикальная формула для корней, то f разрешим в радикалах над полем $\mathbb{C}(a_{n-1}, \ldots a_0)$. Здесь мы думаем про $a_{n-1}, \ldots, a_0$ как про формальные переменные.

Многочлен $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{C}(a_{n-1}, \ldots, a_0)[x]$ называется **общим многочленом**.

Утверждение 18. *Общий многочлен сепарабелен и $\mathrm{Gal}_K(f) = S_n$, где $K = \mathbb{C}(a_{n-1}, \ldots a_0)$.*

Доказательство. Пусть $x_1, \ldots, x_n$ — корни общего многочлена f. Докажем, что $x_1, \ldots x_n$ алгебраически независимы над $\mathbb{C}$. Пусть $g(x_1, \ldots, x_n) = 0$. Рассмотрим многочлен

$$F(y_1, \ldots, y_n) = \prod_{\sigma \in S_n} g(y_{\sigma(1)}, \ldots, y_{\sigma(n)}).$$

Заметим, что выражение $F(x_1, \ldots, x_n)$ симметрично по $x_1, \ldots, x_n$. Из формул Виета следует, что $F(x_1, \ldots, x_n) = H(a_{n-1}, \ldots a_0)$. Но с другой стороны $F(x_1, \ldots, x_n) = 0$. Поэтому $H(a_{n-1}, \ldots, a_0) = 0$, что противоречит алгебраической независимости $a_{n-1}, \ldots, a_0$.

Так как $x_1, \ldots, x_n$ алгебраически независимы, то они все различные. Значит, f сепарабелен.

По формулам Виета все коэффициенты a_i выражаются через $x_1, \ldots, x_n$. Поэтому $\mathbb{C}(x_1, \ldots, x_n) = K(x_1, \ldots, x_n) = K(f)$.

Но тогда на поле $\mathbb{C}(x_1, \ldots, x_n)$ действует группа S_n перестановками $x_1, \ldots, x_n$. Все симметрические функции от $x_1, \ldots, x_n$ будут инвариантны, поэтому поле $\mathbb{C}(a_{n-1}, \ldots, a_0)$ будет сохранятся при этих перестановках. Но это означает, что $S_n \subseteq \mathrm{Gal}_K(f)$. Но любой элемент группы $\mathrm{Gal}_K(f)$ однозначно определяется перестановкой корней $x_1, \ldots, x_n$. Поэтому $\mathrm{Gal}_K(f) = S_n$. □

В качестве следствия получаем теорему Абеля:

Теорема 13. *(теорема Абеля)*
Не существует радикальной формулы для корней общего многочлена степени 5 и более.

Доказательство. Как мы доказали выше группа Галуа общего многочлена — S_n. Из курса алгебры мы знаем, что S_n неразрешимая группа при $n \geq 5$. □

Задача 34. *Пусть p — простое. Докажите, что группа Галуа многочлена $x^p - 2 \in \mathbb{Q}[x]$ изоморфна группе матриц $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, где $a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p$.*

Задача 35. *Найдите какой-нибудь корень уравнения $x^3 - 6x^2 - 6x - 2 = 0$.*

Задача 36. *Найдите какой-нибудь корень уравнения $x^4 + 4x^3 - 4x^2 - 20x - 5 = 0$.*

2.7 Критерий разрешимости в радикалах

Перейдем к доказательству теоремы 12.

Определение 19. *Расширение L/K называется **циклическим**, если это расширение Галуа с циклической группой Галуа.*

Если $b^n = a \in K$, то расширение $K(b)$ будем обозначать $K(\sqrt[n]{a})$, не уточняя, какой именно корень из a мы присоединяем.

Теорема 14. *Пусть* $\operatorname{char} K = 0$.

1. *Пусть p простое. Тогда $K(\sqrt[p]{1})/K$ — циклическое расширение.*
2. *Пусть группа $\sqrt[n]{1}$ содержится в K и $a \in K$. Тогда $K(\sqrt[n]{a})/K$ — циклическое расширение степень, которого делит n.*
3. *Пусть группа $\sqrt[n]{1}$ содержится в K и L/K — циклическое расширение степени n. Тогда $L = K(\sqrt[n]{a})$ для некоторого $a \in K$.*

Доказательство. Докажем 1). Как мы доказывали выше группа $\sqrt[p]{1} \simeq \mathbb{Z}_p$. Тогда $K(\sqrt[p]{1}) = K$, либо $K(\sqrt[p]{1}) = K(x^p - 1)$ (первый случай, если мы присоединяем 1, либо K уже содержит все корни степени p из 1). В обоих случаях $K(\sqrt[p]{1})/K$ — расширение Галуа.

Пусть $\varphi \in \operatorname{Gal}_K K(\sqrt[p]{1})$ и ε —первообразный корень степени p из 1. Тогда $\varphi(\varepsilon) = \varepsilon^k$, где $k \neq 0$. Обозначим $k = k_\varphi$. Получаем отображение

$$\theta : \operatorname{Gal}_K K(\sqrt[p]{1}) \to \mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1},\ \varphi \to k_\varphi.$$

Легко проверить, что θ — инъективный гомоморфизм. Поэтому $\operatorname{Gal}_K K(\sqrt[p]{1})$ изоморфна подгруппе циклической группы, а значит сама циклическая.

Докажем 2). В этом случае имеем:

$$x^n - a = (x - \sqrt[n]{a})(x - \varepsilon\sqrt[n]{a}) \dots (x - \varepsilon^{n-1}\sqrt[n]{a}),$$

где $\varepsilon \in \sqrt[n]{1}$ — первообразный корень. Поэтому $K(\sqrt[n]{a}) = K(x^n - a)$. Следовательно $K(\sqrt[n]{a})/K$ — расширение Галуа. Для каждого $\varphi \in \operatorname{Gal}_K(K(\sqrt[n]{a}))$ имеем $\varphi(\sqrt[n]{a}) = \varepsilon^k \sqrt[n]{a}$ для некоторого k. Обозначим $\varepsilon^k = \varepsilon_\varphi$. Опять легко проверить, что отображение

$$\Theta : \operatorname{Gal}_K(K(\sqrt[n]{a})) \to \sqrt[n]{1},\ \varphi \to \varepsilon_\varphi$$

инъективный гомоморфизма. Поэтому $\operatorname{Gal}_K(K(\sqrt[n]{a}))$ циклическая группа.

Для доказательства 3) нам понадобится следующая лемма.

Лемма 5. *Пусть L/K — расширение полей и $\varphi_1 \dots \varphi_k \in \operatorname{Aut}_K L$ — попарно различные автоморфизмы. Тогда $\varphi_1 \dots \varphi_k$ — линейно независимы над K.*

Доказательство. Пусть k — минимальное число, такое что есть $\varphi_1, \dots, \varphi_k \in \operatorname{Aut}_K L$ линейно зависимы. Тогда существуют $\lambda_1, \dots, \lambda_k \in K$, такие что для любого $a \in L$ имеем:

$$\lambda_1\varphi_1(a) + \dots + \lambda_k\varphi_k(a) = 0.$$

Подставим вместо a элемент $a_1 a$, где $a_1 \in L$:

$$\lambda_1\varphi_1(a_1 a) + \dots + \lambda_k\varphi_k(a_1 a) = \lambda_1\varphi_1(a_1)\varphi_1(a) + \dots + \lambda_k\varphi_k(a_1)\varphi_k(a) = 0.$$

Вычитая из второй линейной комбинации первую, домноженную на $\varphi_1(a_1)$, получим:

$$\lambda_2(\varphi_2(a_1) - \varphi_1(a_1))\varphi_2(a) + \dots + \lambda_k(\varphi_k(a_1) - \varphi_1(a_1))\varphi_k(a) = 0.$$

Существует такое a_1, что $\varphi_1(a_1) \neq \varphi_2(a_1)$. При этом a_1 получаем нетривиальную линейную комбинацию, которая равна нулю и в которую входят $k - 1$ автоморфизм. □

Теперь докажем пункт 3 теоремы 14. Так как L/K — циклическая, то $\mathrm{Gal}_K L = \langle\varphi\rangle$. Пусть ε — первообразный корень степени n из 1 и $a \in L$. Рассмотрим элемент

$$(a,\varepsilon) = a + \varepsilon\varphi(a) + \varepsilon^2\varphi^2(a) + \ldots + \varepsilon^{n-1}\varphi^{n-1}(a).$$

Существует $a \in L$, такое что $(a,\varepsilon) \neq 0$ (иначе $\mathrm{id}, \varphi, \ldots \varphi^{n-1}$ линейно зависимы). Тогда $\varphi^k((a,\varepsilon)) = \varepsilon^{-k}(a,\varepsilon)$. Отсюда следует, что (a,ε) не инвариантен относительно никаких нетривиальных автоморфизмов группы Галуа. Из основной теоремы теории Галуа следует, что (a,ε) не содержится ни в каком собственном подполе L, содержащим K. Поэтому $K((a,\varepsilon)) = L$.

При этом $\varphi((a,\varepsilon)^n) = \varphi((a,\varepsilon))^n = (a,\varepsilon)^n$. Поэтому $(a,\varepsilon)^n$ инвариантен относительно всех автоморфизмов группы Галуа, а значит $(a,\varepsilon)^n \in K$. Тогда $L = K(\sqrt[n]{b})$, где $b = (a,\varepsilon)$. □

Теперь докажем теорему 12.

Доказательство. Пусть L/K — радикальное расширение и $K(f) \subseteq L$. Тогда существует радикальная башня:

$$K - K_1 - K_2 - \ldots - K_m = L,$$

где $K_i = K_{i-1}(\sqrt[n_i]{a_i})$, где $a_i \in K_{i-1}$. Можно считать, что все n_i — простые. Пусть $p_1, \ldots, p_s$ — все простые, которые встречаются среди $n_1, \ldots, n_m$. Тогда рассмотрим радикальную башню:

$$K = Q_0 - Q_1 - \ldots - Q_s = P_0 - P_1 - \ldots - P_m = P,$$

где $Q_i = Q_{i-1}(\sqrt[p_i]{1})$, $P_i = P_{i-1}(\sqrt[n_i]{a_i})$. Расширение P/K — поле разложения многочлена

$$(x^{p_1} - 1)\ldots(x^{p_s} - 1)(x^{n_1} - a_1)\ldots(x^{n_m} - a_m).$$

Поэтому P/K — расширение Галуа. Расширение Q_i/Q_{i-1} циклические по пункту 1 теоремы 14, а расширение P_i/P_{i-1} циклическое по пункту 2 теоремы 14 (мы уже добавили все нужные корни из 1).

По основной теореме теории Галуа башне

$$K = Q_0 - Q_1 - \ldots - Q_s = P_0 - P_1 - \ldots - P_m = P$$

соответствует цепочке групп

$$G - G_1 - \ldots - G_{m+s},$$

где $G = \mathrm{Gal}_K P$ и $G_{m+s} = \{\mathrm{id}\}$. Так как Q_1/Q_0 — циклическое расширение, то это расширение Галуа, а значит G_1 нормально в G. Группа $\mathrm{Gal}_{Q_0} Q_1$ циклическая и изоморфна G/G_1. Поэтому G разрешима тогда и только тогда, когда G_1 разрешима. (Здесь мы пользуемся критерием разрешимости). Аналогично G_1 разрешима тогда и только тогда, когда G_2 разрешима. И т.д. Так как G_{m+s} разрешима, то G разрешима.

Поле $K(f)$ содержится в P, при это $K(f)/K$ расширение Галуа. Пусть H — подгруппа в G, соответствующая $K(f)$. Тогда H нормальна в G и $\mathrm{Gal}_K K(f) \simeq G/H$. Так как G разрешима, то и G/H разрешима.

Пусть теперь группа $G = \mathrm{Gal}_K\ f$ разрешима. Тогда существует ряд подгрупп

$$G \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_m = \{id\},$$

где $G_i/G_{i+1} \simeq \mathbb{Z}_{p_i}$. Из основной теоремы теории Галуа следует, что есть ряд соответствующих подполей в $K(f)$:

$$K - K_1 - \ldots - K_m = K(f),$$

причем K_{i+1}/K_i расширение Галуа и $\mathrm{Gal}_{K_i}K_{i+1} \simeq G_i/G_{i+1}$. Пусть $K_i = K_{i-1}(g_i)$, где $g_i \in K_{i-1}[x]$. Рассмотрим башню полей

$$K = Q_0 - Q_1 - \ldots - Q_m = P_0 - P_1 - \ldots P_m,$$

где $Q_i = Q_{i-1}(\sqrt[p_i]{1})$ и $P_i = P_{i-1}(g_i)$ (легко видеть, что $K_i \subseteq P_i$).

Заметим, что $\mathrm{Gal}_{P_i}P_{i+1} \leq \mathrm{Gal}_{K_i}K_{i+1}$. Действительно, любой автоморфизм P_{i+1} над P_i переставляет корни g_{i+1} и тривиально действует на P_i, а значит и на K_i. Поэтому этот автоморфизм сохраняет K_{i+1} над K_i. Отсюда следует, что P_{i+1}/P_i циклическое расширение.

Расширения Q_{i+1}/Q_i —простые радикальные расширения, так как порождаются любым первообразным корнем из единицы степени p_{i+1}. Расширения P_{i+1}/P_i — простые радикальные расширения по пункту 3 теоремы 14. Поэтому P_m/K — радикальное расширение и P_m содержит $K(f)$.

□

Пример 30. *Пусть $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Многочлен f неприводим над $\mathbb{Q}$ по признаку Эйзенштейна. Группа $\mathrm{Gal}_{\mathbb{Q}}f$ — подгруппа в группе S_5. Так как $[\mathbb{Q}(f) : \mathbb{Q}]$ делится на 5, то порядок группы Галуа делится на 5, а значит в группе Галуа есть цикл длины 5.*

Можно доказать, что у f есть три вещественных корня и два комплексных, сопряженных друг другу. Поэтому сопряжение индуцирует автоморфизм $\mathbb{Q}(f)$, который переставляет два комплексных корня и оставляет на месте три вещественных корня. Значит в группе Галуа есть транспозиция. Можно убедиться, что S_5 порождается любым циклом длины 5 и любой транспозицией. Потому $\mathrm{Gal}_{\mathbb{Q}}f = S_5$. Значит уравнение $f = 0$ не разрешимо в радикалах над $\mathbb{Q}$.

2.8 Алгебраически замкнутые поля

Определение 20. *Поле K называется **алгебраически замкнутым**, если выполнено одно из следующих эквивалентных условий.*

1. *У любого многочлена $f \in K[x]$ положительной степени есть корень в K.*
2. *Любой многочлен $f \in K[x]$ положительной степени раскладывается на линейные множители в K.*
3. *Многочлен $f \in K[x]$ неприводим тогда и только тогда, когда он имеет степень 1.*
4. *Если L/K алгебраическое расширение, то $L = K$.*

Доказательство. Эквивалентность пунктов 1, 2, 3 тривиальна и обсуждается в первом семестре. Докажем эквивалентность 3 и 4. Если L/K нетривиальное алгебраическое расширение, то для любого элемента $a \in L \setminus K$ минимальный многочлен μ_a^K — неприводимый многочлен степени выше чем 1. Поэтому из 3 следует 4.

Если выполнено 4, то для любого неприводимого многочлена $f \in K[x]$ расширение $(K[x]/(f))/K$ — алгебраическое расширение, степень которого равна степени f. Поэтому у любого неприводимого многочлена должна быть степень 1. □

Теорема 15. *(Основная теорема алгебры)*
Поле $\mathbb{C}$ — алгебраически замкнутое.

Доказательство. Будем использовать два факта. Первый, то что у многочлена $f \in \mathbb{R}[x]$ нечетной степени есть корень в $\mathbb{R}$. Отсюда следует, что у $\mathbb{R}$ нет расширений нечетной степени.

Второй факт — в поле $\mathbb{C}$ многочлен вида $x^n - a$ раскладывается на линейные множители. Это легко следует из явной формулы для нахождения корней из комплексного числа. Из этого факта, следует, что у $\mathbb{C}$ нет нетривиальных радикальных расширений.

Перейдем к доказательству. Докажем, что у каждого многочлена $g \in \mathbb{C}[x]$ положительной степени есть корень. Заметим, что у g есть корень тогда и только тогда, когда у $g\overline{g}$ есть корень. А многочлен $g\overline{g}$ имеет вещественные коэффициенты. Поэтому достаточно доказать, что у любого многочлена $f \in \mathbb{R}[x]$ положительной степени есть корень. Рассмотрим поле разложения $\mathbb{R}(f)$. Расширение $\mathbb{R}(f)/\mathbb{R}$ — расширение Галуа. Пусть $G = \mathrm{Gal}_{\mathbb{R}} f$ и H — силовская 2-подгруппа в G. Тогда рассмотрим поле $K = K(f)^H$. Степень расширение $[K : \mathbb{R}] = [G : H]$ — нечетна. Поэтому $K = \mathbb{R}$.

Значит, $H = G$, а следовательно G разрешима, как 2-группа. Но тогда уравнение $f = 0$ разрешимо в радикалах над $\mathbb{R}$, а значит и над $\mathbb{C}$. Но тогда поле разложения $\mathbb{C}(f)$ содержится в $\mathbb{C}$. Значит у f есть корень в $\mathbb{C}$. □

Теорема 16. *Пусть L/K — расширение полей и L — алгебраически замкнутое поле. Пусть P — подполе в L, состоящее из всех алгебраических над K элементов. Тогда P алгебраически замкнуто.*

Доказательство. Пусть $f(x) = a_0 + a_1 x + \dots a_n x^n \in P[x]$. Тогда у f есть корень $\alpha \in L$. Расширение $K[a_0, \dots, a_n, \alpha]/K$ алгебраическое. Поэтому α алгебраический элемент. Следовательно $\alpha \in P$. □

Определение 21. *Пусть R — коммутативное ассоциативное кольцо с единицей. Идеал $I \lhd R$ называется **собственным**, если $I \neq R$. Идеал I называется **максимальным**, если он максимальный по включению среди всех собственных идеалов.*

Утверждение 19. *Пусть R — коммутативное ассоциативное кольцо с единицей. Тогда*

1. *каждый собственный идеал содержится в каком-то максимальном идеале;*
2. *если M — максимальный идеал, то R/M — поле.*

Доказательство. 1) Пусть I — собственный идеал. Рассмотрим множество A собственных идеалов в R, которые содержат I. Это частично упорядоченное множество. Если есть цепь

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_k \subseteq \dots,$$

состоящая из идеалов из A, то идеал $J = \cup I_j$ также лежит в A. Действительно, он содержит I, так как все I_j содержат I и он не равен R, так как $1 \notin I_j$ для всех j. По лемме Цорна в A есть максимальный элемент.

2) Следует из двух фактов. Первый говорит то, что коммутативное ассоциативное кольцо с единицей является полем тогда и только тогда, когда в нем нет нетривиальных идеалов. Второй факт говорит, что есть биекция между идеалами в факторкольце R/I и идеалами в R, содержащими I. Оба факта — нетрудные упражнения. □

Теорема 17. *(теорема Артина)*
Всякое поле содержится в алгебраически замкнутом поле.

Доказательство. Пусть K — поле. Построим расширение K_1/K, так чтобы любой многочлен $f \in K[x]$, который не константа, имел корень в K_1.

Для каждого $f \in K[x] \setminus K$ введем формальную переменную x_f и обозначим через X множество всех переменных x_f. Рассмотрим кольцо многочленов от этих переменных $K[X]$. В этом кольце есть идеал $I = (x_f \mid f \in K[x] \setminus K)$. Докажем, что $I \neq K[X]$.

Если $1 \in I$, то существуют $g_1, \ldots, g_k \in K[X]$ и $f_1, \ldots, f_k \in K[x] \setminus K$, такие что

$$1 = f_1(x_{f_1})g_1 + \ldots + f_k(x_{f_k})g_k.$$

Пусть $L = K(f_1 \ldots f_k)$. Пусть α_i — корень f_i в L. Подставим в равенство выше вместо x_{f_i} элемент α_i. Получим $1 = 0$ — противоречие.

Тогда существует максимальный идеал M, содержащий I. Факторкольцо $K[X]/M$ — поле, которое содержит K. Положим $K_1 = K[X]/M$. Если $f \in K[x] \setminus K$, то элемент $x_f + M$ будет корнем f.

Аналогично строим $K_2 \subseteq K_3 \subseteq ...$ так, чтобы любой многочлен из $K_i[x]$ имел корень в K_{i+1}. Рассмотрим поле $L = \cup_i K_i$. Докажем, что L алгебраически замкнуто. Если $g \in L[x]$, то

$$g = a_0 + a_1 x + \ldots + a_n x^n.$$

Существует такое r, что все $a_i \in K_r$. Но тогда $g \in K_r[x]$. Поэтому в $K_{r+1} \subseteq L$ у g есть корень. □

Определение 22. *Пусть K — поле. Будем говорить, что поле L является* ***алгебраическим замыканием*** *поля K, если расширение L/K алгебраическое и L алгебраически замкнутое поле. Обозначение: $L = \overline{K}$.*

Лемма 6. *(вторая лемма о продолжении вложения.)*

Пусть K'/K — алгебраическое расширение и L — алгебраически замкнутое поле. Тогда любое вложение $\varphi_0 : K \to L$ продолжается до вложения $\varphi : K' \to L$.

Доказательство. Пусть $\mathcal{M}$ — множество пар вида (P, ψ), где P — подполе в K', содержащее K, и $\psi : P \to L$ — вложение, продолжающее φ_0. Введем на $\mathcal{M}$: будем говорить, что (P_1, ψ_1) меньше (P_2, ψ_2), если $P_1 \subsetneq P_2$ и $\psi_2|_{P_1} = \psi_1$. Рассмотрим цепь в $\mathcal{M}$:

$$(P_1, \psi_1) \leq (P_2, \psi_2) \leq \ldots (P_k, \psi_k) \leq \ldots$$

Положим $P = \cup P_i$ и $\psi : P \to L$, такое что $\psi_{P_i} = \psi_i$. Тогда $(P_k, \psi_k) \leq (P, \psi)$. Поэтому (P, ψ) — верхняя грань. Следовательно, в $\mathcal{M}$ есть максимальный элемент (Q, φ). Если $Q \neq K'$, то рассмотрим любой элемент $\alpha \in K' \setminus Q$. Он алгебраический над Q. По (старой) лемме о продолжении вложений существует вложение $\psi' : Q(\alpha) \to L$, продолжающее ψ. Это противоречит максимальности (Q, φ).

Значит $Q = K'$ и φ — искомое продолжение. □

Теорема 18. *Для любого поля алгебраическое замыкание существует и единственно.*

Доказательство. Пусть K — поле. По теореме Артина существует алгебраически замкнутое расширение L/K. Пусть P — все алгебраические над K элементы в L. По теореме 16 поле P алгебраически замкнутое. Значит P — алгебраическое замыкание K.

Докажем единственность. Пусть L_1 и L_2 — алгебраические замыкания K. Рассмотрим тождественное вложение $\varphi_0 : K \to L_2$. Из второй лемме о продолжении вложений следует, что существует вложение $\varphi : L_1 \to L_2$. Тогда $\varphi(L_1)/K$ — алгебраически замкнутое алгебраическое расширение K. Но тогда $L_2/\varphi(L_1)$ — алгебраическое расширение алгебраически замкнутого поля. Поэтому $L_2 = \varphi(L_1)$. □

Пример 31. *1.* $\overline{\mathbb{R}} = \mathbb{C}$.

2. $\overline{\mathbb{Q}} = \mathbb{A}$ *— поле алгебраических чисел.*

Пример 32. *Построим алгебраическое замыкание поля $\mathbb{Z}_p$. Так как расширение $\mathbb{F}_{p^n}/\mathbb{Z}_p$ алгебраическое, то $\overline{\mathbb{F}_{p^n}} = \overline{\mathbb{Z}_p}$.*

Если $n|m$, то есть вложение $\varphi_{n,m} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ (по теореме 4). Вложения $\varphi_{n,m}$ можно выбрать таким образом, чтобы если $n|m$ и $m|k$, то $\varphi_{n,k} = \varphi_{m,k} \circ \varphi_{n,m}$. (Это не совсем тривиальный факт, но мы не будем его доказывать). Тогда $\overline{\mathbb{Z}_p} = \varinjlim \mathbb{F}_{p^n}$ — копредел полей $\mathbb{F}_{p^n}$. Расшифруем, что это значит. Мы берем дизъюнктное объединение полей $\sqcup \mathbb{F}_{p^n}$ и вводим там отношение эквивалентности. Пусть $a \in \mathbb{F}_{p^n}$ и $b \in \mathbb{F}_{p^m}$. Будем говорить, что $a \sim b$, если существует такое k, что $n|k$ и $m|k$ и $\varphi_{n,k}(a) = \varphi_{m,k}(b)$. Как множество $\overline{\mathbb{Z}_p}$ совпадат с множеством классов эквивалентности по отношению $\sim$. А операции устроены так. Если мы хотим сложить или умножить произвольный элемент $x \in \mathbb{F}_{p^n}$ и $y \in \mathbb{F}_{p^m}$, то результатом будем сложение или произведение элементов $\varphi_{n,nm}(x)$ и $\varphi_{m,nm}(y)$ в $\mathbb{F}_{p^{nm}}$. Легко проверить, что эти операции уважают отношение эквивалентности.

Пример 33. *Пусть K — алгебраически замкнутое поле характеристики ноль. Можно предъявить алгебраически замкнутое поле, которое содержит поле $K(x)$. Это будет поле дробно-степенных рядов или рядов Пюизо:*

$$K\{\{x\}\} = \{\sum_{i \geq n_0} a_i x^{\frac{i}{N}} \mid a_i \in K,\ n_0 \in \mathbb{Z},\ N \in \mathbb{N}\}.$$

Это алгебраически-замкнутое поле, в которое вкладывается $K(X)$, но это не будет алгебраическим замыканием поля $K(x)$.

Глава 3

Модули над кольцами

3.1 Модули. Подмодули. Фактормодули

Определение 1. *Пусть R — ассоциативное кольцо. Абелева группа M называется* ***(левым) модулем над*** *R, если определено отображение*

$$R \times M \to M,\ (r, m) \to rm,$$

такое что для любых $r, s \in R$ и $m, n \in M$ выполнены следующие свойства:

1. $(r + s)m = rm + sm$;
2. $(rs)m = r(sm)$;
3. $r(m + n) = rm + rn$;
4. *Если в R — кольцо с единицей, то мы дополнительно будем требовать, чтобы $1m = m$.*

Пример 1.

1. *Абелева группа = модуль над $\mathbb{Z}$;*
2. *Векторное пространство над полем K = модуль над K;*
3. *Если V — векторное пространство над полем K и $\varphi \in L(V)$ — линейный оператор, то V — модуль над $K[x]$. Действительно, определим умножение многочлена $f \in K[x]$ на вектор $v \in V$ следующим образом:*
$$fv = f(\varphi)(v).$$
Обратно, пусть на векторном пространстве определена структура модуля над $K[x]$. (Так, чтобы умножение на константы из $K[x]$ совпадало с умножением на скаляры в векторном пространстве). Тогда отображение $v \to xv$ — линейный оператор.
4. *Если R — ассоциативное кольцо, то R модуль над самим собой.*
5. *Если $\varphi : R_1 \to R_2$ — гомоморфизм колец, то R_2 — модуль над R_1. Умножать элементы из R_2 на элементы из R_1 можно следующим образом:*
$$r_1 r_2 = \varphi(r_1)r_2,\ r_1 \in R_1,\ r_2 \in R_2.$$

Задача 37. *Пусть M — модуль над R. Докажите, что $r0 = 0$ и $0m = 0$ для любых $r \in R$ и $m \in M$.*

Определение 2. *Пусть M — модуль над R. Подгруппа N в M называется* ***подмодулем****, если для любого $r \in R$ и $n \in N$ элемент $rn \in N$.*

Пример 2. *1. Если A — модуль над $\mathbb{Z}$, то подмодуль = подгруппа;*

2. Если V — модуль над полем K, то подмодуль = подпространство;

3. Если V — модуль над $K[x]$, то подмодуль = подпространство инвариантное относительно линейного оператора $v \to xv$.

4. Если R — кольцо и модуль над самим собой, то подмодуль = левый идеал.

Определение 3. *Пусть M и N — модули над R. Гомоморфизм групп $f : M \to N$ называется* ***гомоморфизмом модулей над*** *R, если для любого $m \in M$ и $r \in R$ выполнено $f(rm) = rf(m)$. Множество всех гомоморфизмов из M в N обозначается* $\mathrm{Hom}_R(M, N)$.

Задача 38. *Пусть $f : M \to N$ — гомоморфизм модулей над R. Докажите, что*

1. $\mathrm{Ker}\ f$ *— подмодуль в M.*

2. $\mathrm{Im}\ f$ *— подмодуль в N.*

3. Если R — коммутативное кольцо, то $\mathrm{Hom}_R(M, N)$ *— модуль над R.*

Определение 4. *Пусть M — модуль над R и $N \subseteq M$ — подмодуль. Тогда факторгруппа M/N является модулем над R, который называется* ***фактормодуль.*** *Действительно, умножение на элементы из R устроено следующим образом:*

$$r(m + N) = rm + N.$$

Задача 39. *1. (Первая теорема о гомоморфизме.) Пусть $f : M \to N$ — гомоморфизм $R-$модулей. Докажите, что* $\mathrm{Im}\ f = M/\mathrm{ker}\ f$.

2. (Вторая теорема о гомоморфизме.) Пусть N_1, N_2 — подмодули $R-$модуля M. Тогда

$$(N_1 + N_2)/N_1 \simeq N_2/(N_1 \cap N_2).$$

3. (Третья теорема о гомоморфизме.) Пусть M — R-модуль и $A \subseteq B$ — подмодули M. Тогда

$$(M/A)/(B/A) \simeq M/B;$$

4. (Четвертая теорема о гомоморфизме.) Пусть N — подмодуль $R-$модуля M. Тогда есть биекция между подмодулями в M/N и подмодулями в M, содержащими N.

Задача 40. *Приведите пример модулей M, N и гомоморфизма групп $f : M \to N$, который не является гомоморфизма модулей.*

Задача 41. *Пусть R — коммутативное ассоциативное кольцо с единицей. Докажите, что модуль* $\mathrm{Hom}_R(R, M)$ *изоморфен модулю M.*

3.2 Свободные модули. Тензорное произведение модулей

В этом разделе под кольцом будем иметь в виду ассоциативное кольцо с единицей.

Пусть M — модуль над кольцом R и $N_1, \ldots, N_k$ — подмодули. Сумма подмодулей $N_1, \ldots, N_k$ определяется как подмодуль

$$N_1 + \ldots + N_k = \{n_1 + \ldots + n_k \mid n_i \in N_i\}.$$

Если A — подмножество в M. Подмодулем, порожденным множеством A называется подмодуль:

$$RA = \{r_1 a_1 + \ldots + r_k a_k \mid a_i \in A, r_i \in R\ \}.$$

Определение 5. *Подмодуль M называется конечно порожденным, если существует конечное подмножество $A \subseteq M$, такое что $M = RA$. Модуль называется* ***циклическим****, если существует такой элемент $a \in M$, что $M = Ra$.*

Если $\{M_i\}$ — семейство R-модулей, то прямым произведением модулей M_i называется декартово произведение M_i, гду сумма и умножение на элементы R производятся покоординатно.

Прямой суммой модулей M_i называется подмодуль в M_i, состоящий из финитных последовательностей.

Утверждение 1. *Пусть $N_1, \ldots, N_k \subseteq M$ — подмодули. Тогда следующие условия эквивалентны.*

1. *Отображение*

$$\pi : N_1 \times \ldots \times N_k \to N_1 + \ldots + N_k,\ (n_1, \ldots, n_k) \to n_1 + \ldots + n_k$$

   является изоморфизмом R-модулей.

2. *$N_i \cap (\sum_{j \neq i} N_j) = \{0\}$ для всех j.*

3. *Для любого $x \in N_1 + \ldots + N_k$ существует единственные $n_i \in N_i$, такие что*

$$x = n_1 + \ldots + n_k.$$

Определение 6. *Если $M = N_1 + \ldots + N_k$ и подмодули N_i удовлетворяют условиям 1)-3) утверждения 1, то говорят что M (внутренняя) прямая сумма подмодулей $N_1, \ldots N_k$. Обозначение: $M = N_1 \oplus \ldots \oplus N_k$.*

Определение 7. *Говорят, что R-модуль M является* ***свободным R-модулем с базисом*** *$A \subseteq M$, если для любого $x \in M$ существуют единственные $r_1, \ldots, r_k \in R$ и $a_1, \ldots, a_k \in A$, такие что*

$$x = r_1 a_1 + \ldots + r_k a_k.$$

Определение 8.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ — свободный $\mathbb{Z}_2$-модуль.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ не является свободным $\mathbb{Z}$-модулем.

Векторное пространство над полем K является свободным K-модулем.

Теорема 1. *(Универсальное свойство свободных R-модулей)*

Пусть F — свободный R-модуль с базисом A, M — R-модуль и $f : A \to M$ — отображение. Тогда существует единственный гомоморфизм R-модулей $\varphi : F \to M$, который продолжает f.

Следствие 1. *Если F — свободный R-модуль с базисом A, то F изоморфен модулю $\oplus_{a\in A}R$.*

Определение 9. *Абелева группа M называется* ***правым*** *R-модулем, если определено отображение $MR \to M$, которое удовлетворяет следующим условиям:*

1. $m(r+s) = mr + mr$;
2. $m(rs) = (mr)s$;
3. $(m+n)r = mr + nr$;
4. *Если в R — кольцо с единицей, то мы дополнительно будем требовать, чтобы $m1 = m$.*

Если R — кольцо, то можно определить кольцо R^{op}. Как абелева группа R^{op} совпадает с R, а умножение $*$ определяется следующим образом $r_1 * r_2 = r_2 r_1$. Если M — левый R-модуль, то M — правый R^{op}-модуль. Здесь мы определяем умножение $m*r$ как rm. Если R — коммутативное кольцо, то $R = R^{op}$ и любой левый R-модулем является также правым R-модулем.

Пример 3. *Если V — векторное пространство, то V является левым $L(V)$-модулем. Но сопряженном пространстве V^* можно определить структуру правого $L(V)$-модуля следующим образом:*

$$l * \varphi(v) = l(\varphi(v)),\ l \in V^*,\ v \in V,\ \varphi \in L(V).$$

Абелева группа M называется (S,R)-бимодулем, если M — левый S-модуль, правый R-модуль и при этом

$$s(mr) = (sm)r.$$

Пример 4.
1. *Если R — коммутативное кольцо, то любой левый R-модуль является также (R,R)-бимодулем.*
2. *Если S — подкольцо в кольце R, то R является (S,R)-бимодулем (как и (R,S)-бимодулем).*

Определение 10. *Пусть M — правый R-модуль и N — левый R-модуль. Пусть $F(M\times N)$ — свободный $\mathbb{Z}$-модуль с базисом $M \times N$.* ***Тензорным произведением модулей M и N над кольцом*** *R называется фактормодуль $F(M\times N)$ по подмодулю, порожденном элементами вида:*

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$

$$(mr, n) - (m, rn).$$

Обозначение: $M \otimes_R N$.

Определение 11. *Пусть L — абелева группа. Отображение $\varphi : M \times N \to L$ называется* ***внутренне R-линейным****, если выполнены следующие условия:*

$$\varphi((m_1 + m_2, n)) = \varphi((m_1, n)) + \varphi((m_2, n))$$

$$\varphi((m, n_1 + n_2)) = \varphi((m, n_1)) + \varphi((m, n_2))$$

$$\varphi((mr, n)) = \varphi((m, rn)).$$

Отображение $i : M \times N \to M \otimes_R N,\ (m,n) \to m \otimes n$ является внутренне R-линейным.

Теорема 2. *(Универсальное свойство тензорного произведения)*

1. *Если $\Phi : M \otimes_R N \to L$ — гомоморфизм абелевых групп, то композиция $\varphi : \Phi \circ i$ — внутренне R-линейное отображение.*

2. *Для любой абелевой группы L и любого R-линейного отображения $\varphi : M \times N \to L$ есть единственный гомоморфизм групп $\Phi : M \otimes_R N \to L$, такой что $\varphi = \Phi \circ i$.*

Пусть M — (S, R)-бимодуль и N — левый R-модуль. Тогда на $M \otimes_R N$ можно ввести структуру левого S-модуля, определив умножение на элементы s следующим образом:

$$s(\sum_i m_i \otimes n_i) = \sum_i sm_i \otimes n_i),$$

где $m_i \in M, n_i \in N, s \in S$. Самое трудное — проверить корректность, то есть то, что если $\sum_i m_i \otimes n_i = \sum_j m'_j \otimes n'_j$, то результат умножения на s не изменится. Это делается с помощью универсального свойства тензорного произведения.

Определение 12. *Пусть S — подкольцо в R. Тогда R — (R, S)-бимодуль. Пусть N — левый S-модуль. Тогда $R \otimes_S N$ — левый R-модуль. Этак конструкция называется* ***расширение констант****.*

Пример 5. *Пусть V — векторное пространство над полем $\mathbb{R}$. Тогда V — левый $\mathbb{R}$-модуль, а поле $\mathbb{C}$ — $(\mathbb{C}, \mathbb{R})$-бимодуль. Тогда $\mathbb{C} \otimes_{\mathbb{R}} V$ — левый $\mathbb{C}$-модуль. Это конструкция называется* ***комплексификацией*** *векторного пространства.*

Пример 6. *Пусть $\rho : G \to \mathrm{GL}_K(V)$ — представление над полем K. Рассмотрим групповую алгебру $[G]$. Тогда V — левый $K[G]$-модуль. Пусть G — подгруппа некоторой группы H. Тогда $K[G]$ подкольцо в $K[H]$. Тогда можно рассмотреть тензорное произведение $K[H] \otimes_{K[G]} V$. Это будет $K[H]$-модуль, а следовательно представление группы H. Это представление называется* ***индуцированным*** *представлением.*

Пример 7. *Если R — коммутативное кольцо, то любой правый R-модуль является левым R-модулем. Поэтому группа $M \otimes_R N$ является R-модулем.*

Пример 8. *1. $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \simeq \mathbb{Z}$ (как абелевы группы или как $\mathbb{Z}$-модули).*

2. *$R \otimes_R N \simeq N$ как левые R-модули.*

3. *$\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \simeq \{0\}$.*

4. *$\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \not\simeq \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ как $\mathbb{R}$ — модули.*

Утверждение 2. *Группа $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \simeq \mathbb{Z}_{(n,m)}$.*

Доказательство. Пусть $\sum_i \overline{a_i} \otimes \overline{b_i} \in \mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m$. Тогда

$$\sum_i \overline{a_i} \otimes \overline{b_i} = \sum_i a_i\overline{1} \otimes b_i\overline{1} = \sum_i a_i b_i \overline{1} \otimes \overline{1}.$$

Поэтому $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m$ порождено $\overline{1} \otimes \overline{1}$ как абелева группа. Значит это циклическая группа. При этом

$$n \cdot \overline{1} \otimes \overline{1} = \overline{n} \otimes \overline{1} = 0 = \overline{1} \otimes \overline{m} = m\overline{1} \otimes \overline{1}.$$

Поэтому порядок $1 \otimes 1$ делит и n и m, а значит делит (n, m).

Рассмотрим отображение

$$\varphi : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_{(n,m)},\ (\overline{a}, \overline{b}) \to \overline{a} \cdot \overline{b}.$$

Легко видеть, что φ корректно определено и внутренне $\mathbb{Z}$-линейно.

Тогда существует отображение $\Phi : \mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \to \mathbb{Z}_{(n,m)}$, такое что $\varphi = \Phi \circ i$. При этом $\Phi((\overline{a} \otimes \overline{b})) = \varphi((\overline{a}, \overline{b})) = \overline{a}\overline{b}$. Легко видеть, что φ сюръективно, поэтому и Φ сюръективно. Но тогда мощность множества $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m$ не меньше чем (n, m).

□

Задача 42. *Докажите, что* $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \not\simeq \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ *как* $\mathbb{C}$*-модули.*

Задача 43. *Докажите, что* $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ *как абелевы* $\mathbb{Q}$*-модули и как абелевы группы.*

Задача 44. *Пусть* $n = p^k m$*, где* p *— простое число и* $(p, m) = 1$*, и пусть* A *— абелева группа порядка* n*. Докажите, что группа* $\mathbb{Z}_{p^k} \otimes_{\mathbb{Z}} A$ *изоморфна силовской* p*-подгруппе* A*.*

Задача 45. *Докажите, что* $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{C}$ *как* $\mathbb{R}$*-модули.*