Лекция 14

Определение 1. Пусть $h(x) \in F[x]$. Расширение $F \subset K$ называется полем разложения $h(x)$, если $h(x)$ разлагается в $K[x]$ на линейные множители и K порождается над F корнями $h(x)$.

Теорема 1. *Поле разложения любого многочлена $h \in F[x]$ существует.*

Доказательство. Разложим $h(x)$ на неприводимые множители над F. Пусть h_1 – один из этих неприводимых множителей степени больше 1. (Если таких нет, то $K = F$.) Положим $F_1 = F[x]/(h_1)$. Это расширение F, в котором у h_1 есть корень. Таким образом, $h(x)$ над F_1 разлагается на большее число неприводимых множителей, чем над F. Если все они линейны, то $K = F_1$. Иначе снова выберем один из множителей степени ≥ 2 и присоединим его корень и так далее пока не дойдем до поля, в котором h разлагается на линейные множители. Так как мы каждый раз присоединяли некоторый корень $h(x)$, в итоге мы получим поле разложения h над F. □

Лемма 1. *Пусть ψ – автоморфизм поля F. Тогда неподвижные относительно ψ элементы в F образуют подполе $E \subset F$.*

Доказательство. Пусть $\psi(a) = a$ и $\psi(b) = b$. Тогда $\psi(a + b) = \psi(a) + \psi(b) = a + b$, $\psi(ab) = \psi(a)\psi(b) = ab$, $\psi(-a) = -a$, если $a \neq 0$, то $\psi(a^{-1}) = a^{-1}$. То есть множество неподвижных элементов замкнуто относительно сложения, умножения, взятия противоположного и взятия обратного к ненулевому элементу. Значит, это подполе. □

Следствие 1. *Для любого простого p и натурального n существует поле из p^n элементов.*

Доказательство. Рассмотрим поле разложения K многочлена $x^{p^n} - x$ над $\mathbb{Z}_p$. У этого многочлена нет кратных корней. В самом деле, кратные корни – это общие корни многочлена и его производной. Но $(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = -1$. Последнее равенство верно так как мы находимся над $\mathbb{Z}_p$. Значит, у многочлена $x^{p^n} - x$ ровно $q = p^n$ корней. Докажем, что множество корней образует подполе.

Напомним, что для конечного поля характеристики p определен автоморфизм Фробениуса $x \mapsto x^p$. Поле K имеет характеристику p, так как суммирование единиц происходит по сути в поле $\mathbb{Z}_p$. Также K конечно, поскольку это конечное расширение поля $\mathbb{Z}_p$. Рассмотрим автоморфизм $\varphi^n \colon x \mapsto x^{p^n}$. Получается, что корни многочлена $x^{p^n} - x$ суть неподвижные точки φ^n. А значит, они образуют подполе. □

Замечание 1. Так как K порождается корнями $x^{p^n} - x$ и $\mathbb{Z}_p$, а поле, состоящее из корней $x^{p^n} - x$ содержит $\mathbb{Z}_p$ и все корни этого многочлена, получаем, что эти два поля совпадают. То есть K состоит только из корней многочлена $x^{p^n} - x$.

Предложение 1. *Пусть $f(x) = a_n x^n + \ldots + a_0 \in F[x]$ – неприводимый многочлен. Пусть $F(\alpha)$ – поле, полученное присоединением корня α к полю F. И пусть φ – вложение $F \hookrightarrow K$, где K – некоторое поле. Вложение φ продолжается до вложения $\widetilde{\varphi} \colon F(\alpha) \hookrightarrow K$ столькими способами, сколько различных корней у многочлена $\varphi(f)(x) = \varphi(a_n)x^n + \ldots + \varphi(a_0)$.*

Доказательство. Пусть $\widetilde{\varphi}$ существует. Положим $\beta = \varphi(\alpha)$. Тогда

$$0 = \widetilde{\varphi}(0) = \widetilde{\varphi}(a_n\alpha^n + \ldots + a_0) = \varphi(a_n)\alpha^n + \ldots + \varphi(a_0) = \varphi(f)(\beta).$$

То есть β – это корень $\varphi(f)$.

Напротив, если β – это корень $\varphi(f)$, то формула

$$\widetilde{\varphi}(b_k\alpha^k + \ldots + b_0) = \varphi(b_k)\beta^k + \ldots + \varphi(b_0)$$

задает некоторое продолжение вложения φ, которое является ненулевым гомоморфизмом $F(\alpha) \to K$, а следовательно, вложением. □

Теорема 2. *Поле разложения многочлена $h(x)$ над F единственно с точностью до изоморфизма над F. (То есть этот изоморфизм оставляет элементы F на месте.)*

Доказательство. Мы построили L – одно из полей разложения $h(x)$ как цепочку расширений $L_0 = F \subset L_1 \subset ... \subset L_s = L, L_{i+1} = L_i(\alpha)$ для некоторого корня α неприводимого делителя $f(x)$, $\deg f \geq 2$, многочлена $h(x)$. Пусть K – некоторое другое поле разложения h над F. Тогда есть естественное вложение $\varphi_0 \colon F \hookrightarrow K$. Докажем по индукции, что для каждого i существует вложение $\varphi_{i+1} \colon L_{i+1} \hookrightarrow K$ продолжающее вложение $\varphi_i \colon L_i \hookrightarrow K$. По предложению φ_i может быть продолжен до φ_{i+1} столькими способами, сколько корней у $\varphi_i(f)(x)$ в K. Однако $\varphi_i(f)(x)$ – делитель $h(x)$ в $K[x]$. Значит, у него есть корень. Итак, существует вложение $\varphi_s \colon L \hookrightarrow K$, которое неподвижно на F. Осталось доказать сюръективность φ_s. Но если вложение φ_s не сюръективно, то его образ – это собственное подполе K, в котором h разлагается на линейные множители. Значит, K – не поле разложения. □

В программу экзамена не войдет предложение 1 и войдет только формулировка теоремы 2 без доказательства.

Лемма 2. *Пусть $|F| = p^n = q$. Тогда каждый элемент $a \in F$ является корнем многочлена $x^q - x$.*

Доказательство. Очевидно, что ноль является корнем данного многочлена. Пусть $a \in F \setminus \{0\}$. Тогда a лежит в мультипликативной группе $F^\times$. При этом $|F^\times| = q-1$. Значит, по следствию из теоремы Лагранжа, $a^{q-1} = 1$. Умножая обе части на a, получаем $a^q = a$. □

Следствие 2. *F – поле разложения $x^q - x$ над $\mathbb{Z}_p$.*

Доказательство. Так как $|F| = p^n$, имеем $\mathrm{char}F = p$. А значит, в F содержится простое подполе, изоморфное $\mathbb{Z}_p$. Так как любой элемент F – это корень $x^q - x$ и $|F| = q$, многочлен $x^q - x$ имеет q корней в F, а значит, раскладывается на линейные множители. □

Из теоремы 2 и следствия 2 следует следующая теорема.

Теорема 3. *. Поле из p^n элементов единственно с точностью до изоморфизма.*

Поле из p^n элементов обозначается $\mathbb{F}_{p^n}$.

Теорема 4. *В поле F_{p^n} есть подполе, изоморфное F_{p^m} тогда и только тогда, когда $m \mid n$.*

Доказательство. Если $L = F_{p^n}$ содержит подполе $K = F_{p^m}$, то L – векторное пространство над K, а значит, $p^n = |L| = |K|^s = p^{sm}$ где $s = \dim_K L$. То есть $n = sm$.

Наоборот, пусть $n = sm$. Тогда $p^n - 1 = (p^m)^s - 1 = (p^m - 1)t$. Откуда

$$x^{p^n} - x = x(x^{p^n-1} - 1) = x(x^{p^m-1} - 1)T.$$

Таким образом, $x^{p^n} - x$ делится на $x^{p^m} - x$. Элементы, являющиеся корнями $x^{p^m} - x$ образуют подполе, так как это элементы, неподвижные относительно автоморфизма

$\psi\colon a \to a^{p^m}$, который является m-ой степенью автоморфизма Фробениуса. Таких элементов p^m, так как $x^{p^n} - x$ имеет p^n различных корней. □

Представления.

Пусть V – векторное пространство над некоторым полем F. Обозначим через $\mathrm{GL}(V)$ группу обратимых операторов $V \to V$.

Определение 2. *Линейным представлением* группы G называется гомоморфизм $G \to \mathrm{GL}(V)$.

Если в V выбрать базис из n векторов, то каждому оператору сопоставляется матрица $n \times n$. Это устанавливает изоморфизм между $\mathrm{GL}(V)$ и $\mathrm{GL}_n(F)$.

Определение 3. *Матричным представлением* группы G называется гомоморфизм $G \to \mathrm{GL}_n(F)$.

Выбор базиса в V устанавливает биекцию между линейными и матричными представлениями. Если выбрать другой базис, то все операторы представления сопрягутся матрицей перехода.

Размерностью представления называется размерность пространства V. Мы ограничимся рассмотрением конечномерных представлений.

Пример 1. *Отображение $\sigma \mapsto \mathrm{sgn}(\sigma)$ дает одномерное представление группы S_n.*

Замечание 2. Одномерные представления отождествляются с гомоморфизмами $G \to F^\times \cong \mathrm{GL}_1(F)$.

Пример 2. *Пусть ε_1 и ε_2 – корни из 1 степени n. Отображение $k \mapsto \begin{pmatrix} \varepsilon_1^k & 0 \\ 0 & \varepsilon_2^k \end{pmatrix}$ дает двумерное представление группы $\mathbb{Z}_n$.*

Пример 3. *Группа $\mathrm{GL}_n(F)$ имеет естественное n-мерное представление, при котором каждая матрица переходит в себя. Такое представление называется тавтологическим. Аналогичное представление можно рассмотреть для любой матричной группы: $\mathrm{SL}_n(F)$, $\mathrm{O}_n(F)$ и др.*

Замечание 3. Линейное представление задает действие группы G на V.

Определение 4. Предаставление $G \to \mathrm{GL}(V)$ называется *точным*, если его ядро состоит только из нейтрального элемента.

Определение 5. Пусть задан гомоморфизм групп $\varphi\colon G \to H$. Тогда по представлению $\rho\colon H \to \mathrm{GL}(V)$ можно построить представление $\rho \circ \varphi\colon G \to \mathrm{GL}(V)$.

Такая ситуация имеет место, например, если G – это подгруппа в H. В этом случае в качестве φ берем вложение $G \subset H$. Полученное представление $\rho \circ \varphi\colon G \to \mathrm{GL}(V)$ называется *индуцированным* представлением.

Определение 6. Пусть даны представления $\rho\colon G \to \mathrm{GL}(V)$ и $\zeta\colon G \to \mathrm{GL}(W)$. *Морфизмом* представлений называется линейное отображение $\varphi\colon V \to W$ такое, что для каждого $g \in G$ и для каждого $v \in V$ выполнено $\varphi(\rho(g)(v)) = \zeta(g)(\varphi(v))$.

Если φ – изоморфизм векторных пространств, то мы называем его *изоморфизмом* представлений.

Замечание 4. Если ρ и ζ – изоморфные линейные представления, то пространства V и W можно отождествить по изоморфизму φ. При этом базис V перейдет в базис W. Если взять эти соответствующие друг другу базисы и получить матричные представления, то получим одинаковые матричные представления.

Таким образом, матричные представления $\rho\colon G \to \mathrm{GL}_n(F)$ и $\zeta\colon G \to \mathrm{GL}_n(F)$ изоморфны тогда и только тогда, когда существует невырожденная матрица C такая, что для каждого $g \in G$ выполнено $C\rho(g)C^{-1} = \zeta(g)$.

Пример 4. *Рассмотрим следующее n-мерное представление группы S_n: перестановка σ переходит в матрицу A, где*

$$a_{ij} = \begin{cases} 1, & \text{если } \sigma(j) = i, \\ 0 & \text{иначе.} \end{cases}$$

Такое представление называется мономиальным.

Например, при $n = 3$ получаем

$$\mathrm{id} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad (1,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad (1,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$(2,3) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad (1,2,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad (1,3,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Пример 5. *Пусть G – конечная группа порядка n. Рассмотрим n-мерное пространство FG, базисные векторы которого мы индексируем элементами группы: $e_{g_1}, \ldots, e_{g_n}$, где $G = \{g_1, \ldots, g_n\}$. Зададим представление $\rho\colon G \to \mathrm{GL}(FG)$ по правилу $\rho(g)(e_{g_i}) = e_{g \cdot g_i}$.*

Такое представление называется регулярным представлением группы G.

На самом деле данное представление есть композиция вложения $G \hookrightarrow S_n$, которое строится в теореме Кэли, и мономиального представления $S_n \to \mathrm{GL}_n(F)$.

На самом деле FG имеет более богатую структуру, чем просто векторное пространство. Элементы FG можно умножать друг на друга по правилу

$$\left(\sum_i \lambda_i e_{g_i}\right)\left(\sum_j \mu_j e_{g_j}\right) = \sum_{i,j} \lambda_i \mu_j e_{g_i g_j}.$$

Упражнение 1. Проверьте, что FG – это ассоциативная алгебра с единицей. Она называется *групповой алгеброй* группы G.

В каком случае алгебра FG коммутативна?

Заметим, что одномерные матричные представления изоморфны тогда и только тогда, когда они совпадают. В самом деле, так как группа $\mathrm{GL}_1(F) \cong F^\times$ коммутативна, сопряжение в ней не изменяет представление.

Теорема 5. *Существует n различных (неизоморфных) комплексных одномерных представлений группы $\mathbb{Z}_n$*

Доказательство. Пусть $\rho\colon \mathbb{Z}_n \to F^\times$ – одномерное представление. Тогда

$$\rho(1)^n = \rho(n) = \rho(0) = 1.$$

То есть $\varepsilon = \rho(1)$ – корень n-ой степени из 1. При этом $\rho(k) = \varepsilon^k$, то есть образом единицы задается ρ. Наоборот, если взять в качестве ε любой корень из 1 n-ой степени, то получим одномерное представление по формуле $\rho(k) = \varepsilon^k$.

Получаем, что одномерных представлений группы $\mathbb{Z}_n$ столько же, сколько корней из 1 степени n. То есть в случае $F = \mathbb{C}$ их n. И все они имеют вид $\rho(k) = \varepsilon^k$ для некоторого корня из 1 n-ой степени ε. □

Следствие 3. *Пусть G – абелева группа порядка n. Существует n различных (неизоморфных) комплексных одномерных представлений группы G.*

Доказательство. Группа G изоморфна прямой сумме циклических групп

$$\mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}.$$

Аналогично теореме элемент $(0, \ldots, 0, 1, 0, \ldots 0)$, где 1 стоит на i-м месте может переходить в любой корень n_i степени из 1. Если же $\rho((0, \ldots, 0, 1, 0, \ldots 0)) = \varepsilon_i$, то $\rho((a_1, \ldots, a_k)) = \varepsilon_1^{a_1} \ldots \varepsilon_k^{a_k}$. Число способов выбрать $\varepsilon_1, \ldots, \varepsilon_k$ равно n. □

Предложение 2. *Пусть A – абелева группа и G – произвольная группа. И пусть $\varphi\colon G \to A$ – гомоморфизм. Тогда*

1) $G' \subset \operatorname{Ker}\varphi$,

2) $\varphi = \psi \circ \pi_{G'}$ для некоторого гомоморфизма $\psi\colon G/G' \to A$,

3) соответствие $\varphi \leftrightarrow \psi$ является биекцией между множествами гомоморфизмов $G \to A$ и $G/G' \to A$.

Доказательство. 1) $\varphi([g,h]) = [\varphi(g), \varphi(h)] = e$. Значит, $G' \subseteq \operatorname{Ker}\varphi$.

2) Определим $\psi\colon G/G' \to A$ по формуле $\psi(gG') = \varphi(g)$. Проверим корректность. Пусть $g_1G' = g_2G'$. Тогда $g_2 = g_1h$, где $h \in G'$. Имеем,

$$\varphi(g_2) = \varphi(g_1h) = \varphi(g_1)\varphi(h) = \varphi(g_1).$$

Проверим, что ψ – гомоморфизм. Действительно,

$$\psi((g_1G')(g_2G')) = \psi(g_1g_2G') = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1G')\psi(g_2G').$$

Коме того

$$\psi \circ \pi_{G'}(g) = \psi(gG') = \varphi(g),$$

то есть $\psi \circ \pi_{G'} = \varphi$.

3) По гомоморфизму ψ мы можем однозначно построить гомоморфизм $\varphi = \psi \circ \pi_{G'}$, а по гомоморфизму φ однозначно восстанавливается ψ. Значит, это биекция. □

Следствие 4. *Любое одномерное представление $\rho\colon G \to F^\times$ группы G имеет вид $\zeta \circ \pi_{G'}$, где $\zeta\colon G/G' \to F^\times$ – одномерное представление группы G/G'. И это задает биекцию между одномерными представлениями G и одномерными представлениями G/G'.*

Доказательство. Утверждение следствия получается применением предложения 2 к случаю $A = F^\times$. □

Из предыдущего следствия и следствия 3 вытекает следующее утверждение.

Следствие 5. *У группы G ровно $|G/G'|$ одномерных комплексных представлений.*

Замечание 5. Если отказаться от алгебраической замкнутости поля, то утверждение предыдущего предложения будет неверным. Действительно $x \mapsto \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x. \end{pmatrix}$ является неприводимым 2-мерным представлением $(\mathbb{R}, +)$ над $\mathbb{R}$