

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 . \square

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. \square

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 $\varphi^n: x \mapsto x^{p^n}$. Получается, что корни многочлена $x^{p^n} - x$ суть неподвижные точки φ^n . А значит, они образуют подполе. \square

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 $f(x) = a_n x^n + \dots + a_0 \in F[x]$ – 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 $\tilde{\varphi}: F(\alpha) \hookrightarrow K$ столькими способами, сколько различных корней у многочлена $\varphi(f)(x) = \varphi(a_n)x^n + \dots + \varphi(a_0)$.*

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

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

То есть β – это корень $\varphi(f)$.

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

$$\tilde{\varphi}(b_k \alpha^k + \dots + b_0) = \varphi(b_k) \beta^k + \dots + \varphi(b_0)$$

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

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 $L_0 = F \subset L_1 \subset \dots \subset L_s = L, L_{i+1} = L_i(\alpha)$ 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 $\varphi_0: F \hookrightarrow K$. Докажем по индукции, что для каждого i существует вложение $\varphi_{i+1}: L_{i+1} \hookrightarrow K$ продолжающее вложение $\varphi_i: L_i \hookrightarrow K$. По предположению 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 $\varphi_s: L \hookrightarrow K$, 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. \square

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 $a^q = a$. \square

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

Доказательство. Так как $|F| = p^n$, имеем $\text{char} F = p$. 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. \square

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

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

Представления.

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

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

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

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

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 $\sigma \mapsto \text{sgn}(\sigma)$ дает одномерное представление группы S_n .*

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

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

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

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

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

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

Определение 6. Пусть даны представления $\rho: G \rightarrow \text{GL}(V)$ и $\zeta: G \rightarrow \text{GL}(W)$. *Морфизмом* представлений называется линейное отображение $\varphi: V \rightarrow W$ 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 $\rho: G \rightarrow \text{GL}_n(F)$ и $\zeta: G \rightarrow \text{GL}_n(F)$ 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

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

Пример 5. Пусть G – конечная группа порядка n . Рассмотрим n -мерное пространство FG , базисные векторы которого мы индексируем элементами группы: e_{g_1}, \dots, e_{g_n} , где $G = \{g_1, \dots, g_n\}$. Зададим представление $\rho: G \rightarrow \text{GL}(FG)$ 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 $S_n \rightarrow \text{GL}_n(F)$.

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?