Лекция 23

Лемма 1. *Характеристика поля – либо ноль, либо простое число.*

Доказательство. Допустим, что характеристика поля F равна lm.

$0 = \underbrace{1 + 1 + \ldots + 1}_{lm \text{ раз}} = (\underbrace{1 + \ldots + 1}_{l \text{ раз}})(\underbrace{1 + \ldots + 1}_{m \text{ раз}}).$

Так как в поле нет делителей нуля, одна из скобок равна 0. ☐

Определение 1. Простое поле – это поле, в котором нет собственных подполей. (Мы считаем, что в поле $0 \neq 1$, а значит, $\{0\}$ – не подполе.)

Предложение 1. *В каждом поле F есть простое подполе. Если* $\operatorname{char} F = 0$, *то оно изоморфно $\mathbb{Q}$. Если же* $\operatorname{char} F = p$, *то оно изоморфно $\mathbb{Z}_p$.*

Доказательство. 1) Пусть $\operatorname{char} F = p$, рассмотрим

$K = \{0, 1, 1 + 1, 1 + 1 + 1, \ldots, \underbrace{1 + 1 + \ldots + 1}_{\text{(p-1) раз}}\}$

Тогда K – подполе в F, изоморфное $\mathbb{Z}_p$.

2) Пусть $\operatorname{char} F = 0$. Рассмотрим $L = \{0, 1, -1, 1 + 1, -(1 + 1), \ldots\}$. Тогда L – подкольцо в F, изоморфное $\mathbb{Z}$. Рассмотрим отношения всех элементов из L, такие, что знаменатель не ноль. Получим подполе K, изоморфное $\mathbb{Q}$. ☐

Следствие 1. *Количество элементов в конечном поле является степенью простого числа (равного характеристике данного поля).*

Доказательство. Если поле F конечно, то его характеристика не равна нулю. Значит, в нем содержится простое подполе $E \cong \mathbb{Z}_p$. Тогда F – векторное пространство над E. Так как $|F| < \infty$, то и $\dim_E F < \infty$. Пусть $\dim_E F = n$. Тогда $|F| = p^n$. ☐

Пусть $\operatorname{char} F = p$. Рассмотрим следующее отображение $\varphi\colon F \to F$, $\varphi(x) = x^p$.

Предложение 2. *Отображение φ является инъективным гомоморфизмом.*

Доказательство. Очевидно, что $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$. Проверим сохранение сложения: $\varphi(a+b) = (a+b)^p = \sum_{i=0}^{p} C_p^i a^i b^{p-i}$. Так как число p простое, биномиальный коэффициент $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p при $i \notin \{0, p\}$. Так как характеристика поля F равна p, в поле F коэффициент C_p^i равен 0. Значит, в F выполнено $(a+b)^p = a^p + b^p$.

Итак, φ – гомоморфизм. При этом $\operatorname{Ker} \varphi = \{0\}$, поскольку из $a^p = 0$ следует $a = 0$. (В поле нет делителей нуля.) ☐

Определение 2. При $|F| < \infty$, φ – автоморфизм, он называется *автоморфизмом Фробениуса.* Если $|F| = \infty$, то φ может быть не сюръективен.

Заметим, что гомоморфизм из поля в какое-либо кольцо либо нулевой, либо вложение (так как в поле нет нетривиальных идеалов). Значит, изучение гоморфизмов между полями сводится к изучению вложений.

Определение 3. Пусть E – подполе поля F. Тогда поле F называется *расширением* поля E.

Определение 4. Элемент $a \in F$ называется *алгебраическим* над E, если существует ненулевой многочлен $h(x)$ с коэффициентами из E такой, что $h(a) = 0$.

Иначе элемент a называется *трансцендентным* над E.

Определение 5. Расширение полей $E \subset F$ называется *алгебраическим*, если любой элемент $a \in F$ является алгебраическим над E.

Расширение полей $E \subset F$ *конечным*, если $\dim_E F < \infty$. Размерность $\dim_E F$ называется *степенью расширения*.

Предложение 3. *Конечное расширение алгебраическое.*

Доказательство. Пусть $a \in F$ и $\dim_E F = n$. Тогда элементы $1, a, a^2, \ldots, a^n$ линейно зависимы над E. Значит, существуют $c_0, c_1, \ldots, c_n \in E$ такие, что $c_0 + c_1 a + c_2 a^2 + \ldots + c_n a^n = 0$, то есть a алгебраический над E. $\square$

Для любого алгебраического элемента a можно определить минимальный многочлен $f_{min}(x)$ такой, что это многочлен минимальной степени с коэффициентами из E, для которого верно $f_{min}(a) = 0$. Легко показать, что f_{min} неприводим над E и любой многочлен $h(x)$, для которого $h(a) = 0$ делится на f_{min}. Отсюда следует, что f_{min} определен однозначно с точностью до пропорциональности.

Теорема 1 (Теорема о башне расширений)**.** *Пусть $E \subset F$ и $F \subset K$ – конечные расширения полей, причем $\dim_E F = m$, $\dim_F K = n$. Тогда расширение $E \subset K$ такиже конечное и $\dim_E K = mn$.*

Доказательство. Пусть $\{f_1, \ldots, f_m\}$ – базис F над E и $\{k_1, \ldots, k_n\}$ – базис K над F. Тогда для любого $k \in K$ выполнено $k = \sum \lambda_i k_i$, $\lambda_i \in F$. При этом $\lambda_i = \sum_{j=1}^{n} \mu_{ij} f_j$, $\mu_{ij} \in E$. Получается, что $k = \sum_{i,j} \mu_{ij} f_j k_i$. Таким образом, система $f_j k_i$ полная в K над E. Докажем линейную независимость. Пусть $\sum_{ij} \mu_{ij} f_j k_i = 0$. Тогда $\sum_i (\sum_j \mu_{ij} f_j) k_i = 0$. Так как $\{k_1, \ldots, k_n\}$ – базис K, имеем для каждого i: $\sum_j \mu_{ij} f_j = 0$. Значит, так как $\{f_1, \ldots, f_m\}$ – базис F, получаем $\mu_{ij} = 0$ для всех i и j. $\square$

Определение 6. Пусть $E \subset F$ – расширение полей. Пусть S – некоторое подмножество F. Назовем минимальное подполе в F, содержащее E и S *полем, порожденным S над E* и будем обозначать $E(S)$.

Лемма 2. *Поле $E(S)$ состоит из элементов $\frac{g(s_1,\ldots,s_n)}{h(s_1,\ldots,s_n)}$ для всех возможных конечных наборов $s_1, \ldots, s_n$ и многочленов $g, h \in E[y_1, \ldots, y_n]$ с условием $h(s_1, \ldots, s_n) \neq 0$.*

Доказательство. Так как в поле $E(S)$ лежат все s_i и коэффициенты из E, и в этом поле можно складывать и умножать, значит, любой многочлен $g(s_1, \ldots, s_n) \in E(S)$. Так как в этом поле можно делить, $\frac{g(s_1,\ldots,s_n)}{h(s_1,\ldots,s_n)} \in E(S)$. С другой стороны, множество дробей $\frac{g(s_1,\ldots,s_n)}{h(s_1,\ldots,s_n)}$ замкнуто относительно сложения, умножения, взятия противоположного и обратного к ненулевому элементу. Значит, это подполе. $\square$

Лемма 3. *Пусть элемент $a \in F$ алгебраический над $E \subset F$ причем $\deg f_{min} = n$. Тогда $E(a) = \{P(a) \mid \deg P < \deg f_{min}\}$. В частности расширение $E \subset E(a)$ конечное степени n.*

Доказательство. Рассмотрим $\frac{g(a)}{h(a)} \in E(a)$. Так как $h(a) \neq 0$, $h(x)$ не делится на $f_{min}(x)$. Значит, так как f_{min} неприводим, НОД$(h, f_{min}) = 1$, то есть существуют $u(x)$ и $v(x)$ такие, что $uh + vf_{min} = 1$. Домножим числитель $\frac{g(x)}{h(x)}$ на 1:

$\frac{g(x)}{h(x)} = \frac{g(uh+vf_{min})}{h} = gu + \frac{gvf_{min}}{h}$.

Теперь подставим сюда $x = a$, учитывая $f_{min}(a) = 0$, получаем $\frac{g(a)}{h(a)} = g(a)u(a) = Q(a)$. Далее поделим $Q(x)$ на $f_{min}(x)$ с остатком: $Q(x) = q(x) f_{min}(x) + P(x)$, $\deg P < n$. Подставляя a, получаем $Q(a) = P(a)$. $\square$

Следствие 2. *Поле, порожденное конечным числом алгебраических элементов дает конечное расширение.*

Доказательство. В цепочке $E \subset E(a_1) \subset E(a_1, a_2) \subset \ldots E(a_1, \ldots, a_n)$ все расширения конечны. Значит, и $E \subset E(a_1, \ldots, a_n)$ конечно. □

Предложение 4. *Пусть $f(y) \in F[y]$ – неразложимый многочлен. Обозначим $\alpha = y + (f) \in F[y]/(f)$. Тогда $F[y]/(f) = F(\alpha)$, причем α – это корень $f(x)$, рассматриваемого как многочлен из $F(\alpha)[x]$.*

Доказательство. Очевидно, что α лежит в $F[y]/(f)$. Значит, $F(\alpha) \subseteq F[y]/(f)$. С другой стороны $F[y]/(f) = \{g(y) + (f)\} = \{g(\alpha)\}$. Это показывает обратное включение.

Элемент α алгебраический над F так как $f(\alpha) = f(y) + (f) = 0$. Так как f неприводим, это минимальный многочлен α. Значит, $F(\alpha) = F[\alpha] = F[y]/(f)$. □

Определение 7. Расширение $F[x]/(f)$ называется *присоединением корня* многочлена f к полю F.

Определение 8. 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 2. *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 4. *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 3. *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 5. *Пусть $f(x) = a_n x^n + \ldots + a_0 \in F[x]$ – неприводимый многочлен. Пусть $F(\alpha)$ – поле, полученное присоединением корня α многочлена f 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 $\beta = \widetilde{\varphi}(\alpha)$. Тогда

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

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 3. *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 К. 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. □

Лемма 5. *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 4. *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 3 и следствия 4 следует следующая теорема.

Теорема 4. . *Поле из p^n элементов единственно с точностью до изоморфизма.*

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

Теорема 5. *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

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

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. $\square$