Алгебра. Глава 10. Поля

Д. В. Карпов

2023

Расширение полей

Определение

Пусть K — поле, L — надполе K. Тогда L — расширение поля K.

• Если L — расширение поля K, то L — линейное пространство над K, через $[L : K]$ будем обозначать его размерность.

Определение

L — конечное расширение поля K, если степень расширения $[L : K]$ конечна и бесконечное расширение в противном случае.

Теорема 1

Пусть L — расширение поля K, а F — расширение L. Тогда $[F : K]$ конечно, если и только если $[F : L]$ и $[L : K]$ конечны. Более того, $[F : K] = [F : L] \cdot [L : K]$.

Доказательство. $\Leftarrow$. • Пусть $[F : L]$ и $[L : K]$ конечны.

• Пусть $f_1, \ldots, f_n$ — базис F над L, а $e_1, \ldots, e_m$ — базис L над K.

Утверждение 1

$\{f_i e_j\}_{i\in\{1,\ldots,n\},\ j\in\{1,\ldots,m\}}$ — *порождающая система векторов* F *над* K.

Доказательство. • Пусть $x \in F$. Тогда $x = \sum\limits_{i=1}^{n} y_i f_i$, где $y_i \in L$.

• Для каждого i элемент $y_i \in L$ раскладывается по базису над K: $y_i = \sum\limits_{j=1}^{m} \alpha_{i,j} e_j$, где $\alpha_{i,j} \in K$.

• Тогда $x = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} \alpha_{i,j}(e_j \cdot f_i)$, где $\alpha_{i,j} \in K$. □

Утверждение 2

$\{f_i e_j\}_{i\in\{1,\ldots,n\},\ j\in\{1,\ldots,m\}}$ *ЛНЗ над* K.

Доказательство. • Пусть $\alpha_{i,j} \in K$ таковы, что

$$0 = \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{i,j}(e_j \cdot f_i) = \sum_{i=1}^{n}(\sum_{j=1}^{m} \alpha_{i,j} e_j) f_i.$$

• Так как $f_1, \ldots, f_n$ — базис F над L, для всех $i \in \{1, \ldots, n\}$ имеем $\sum\limits_{j=1}^{m} \alpha_{i,j} e_j = 0$.

• Так как $e_1, \ldots, e_m$ — базис L над K, для всех $i \in \{1, \ldots, n\}$ и $j \in \{1, \ldots, m\}$ имеем $\alpha_{i,j} = 0$. □

• По Утверждениям 1 и 2, базис F над K содержит mn элементов, значит, $[F : K] = mn = [F : L] \cdot [L : K]$.

Доказательство. $\Rightarrow$. • Пусть $[F : K]$ конечно.

• Так как L — подпространство F над K, $[L : K] \leq [F : K]$ конечна.

• Так как порождающая система F над K будет порождающей и над L, тогда и $[F : L] \leq [F : K]$ конечна.

□

Теорема 2

Пусть K — поле, $f \in K[x]$ — неприводимый многочлен. Тогда существует такое расширение L поля K, что f имеет в L корень. Более того, $[L : K] \leq \deg(f)$.

Доказательство. • НУО f унитарный. Пусть $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$.

• Докажем, что факторкольцо $L := K[x]/fK[x]$ — поле.

• Пусть $g \in K[x]$, $\overline{g} \neq 0$ в L (что означает $g \not\vdots f$ в $K[x]$).

• Нам нужно доказать, что $\overline{g}$ обратим в L.

• Так как f неприводим, $(f, g) \sim 1$.

• Тогда существуют такие $p, q \in K[x]$, что $fp + gq = 1$ (линейное представление НОД).

• Это означает, что $\overline{g} \cdot \overline{q} = 1$ в L, что нам и нужно.

• Остается заметить, что в L многочлен f имеет корень: $f(\overline{x}) = \overline{f(x)} = 0$. □

Алгебраические и трансцендентные элементы

Определение

Пусть L — расширение поля K.

• Элемент $a \in L$ называется алгебраическим над K, если существует такой многочлен $f \in K[x]$, что $f(a) = 0$. Если такого многочлена нет, то a называется трансцендентным над K.

• Если $a \in L$ — алгебраический над K, обозначим через I_a множество всех многочленов из $K[x]$, корнем которых является a.

• Очевидно, все элементы поля K — алгебраические над K.

Лемма 1

I_a — идеал в $K[x]$.

Доказательство. • Если $f, g \in I_a$, то
$(f + g)(a) = f(a) + g(a) = 0 \Rightarrow f + g \in I_a$.

• Если $f \in I_a$, $h \in K[x]$, то
$(hf)(a) = h(a)f(a) = h(a) \cdot 0 = 0 \Rightarrow hf \in I_a$.

• Значит, I_a — идеал в $K[x]$. □

• I_a — идеал в $K[x]$, а значит, существует такой унитарный (т. е со страшим коэффициентом 1) многочлен $f_a \in K[x]$, что $I_a = f_a \cdot K[x]$.

Определение

Многочлен f_a называется минимальным многочленом элемента a.

• По построению, если $g \in K[x]$ и $g(a) = 0$, то $g \vdots f_a$.

Лемма 2

Минимальный многочлен f_α неприводим.

Доказательство. • Предположим противное, пусть $f_\alpha = g \cdot h$, где $g, h \in K[x]$ и $\deg(g), \deg(h) < \deg(f_\alpha)$.

• Тогда $0 = f_\alpha(\alpha) = g(\alpha) \cdot h(\alpha)$, откуда следует, что $g(\alpha) = 0$ или $h(\alpha) = 0$.

• НУО $g(\alpha) = 0$. Тогда по определению $g \vdots f_\alpha$, что не так. □

Определение

Расширение L поля K — алгебраическое, если все элементы L — алгебраические над K.

Лемма 3

Если L — конечное расширение поля K, то это расширение — алгебраическое.

Доказательство. • Пусть $a \in L$, $n = [L : K]$.

• Тогда $1, a, \ldots, a^n$ — ЛЗ над K, значит, $\exists\ c_0, \ldots, c_n \in K$ такие, что $c_n a^n + \cdots + c_0 = 0$, то есть a — алгебраический элемент над K. □

Определение

Пусть L — расширение поля K, $\alpha_1, \ldots, \alpha_n \in L$. Обозначим через $K(\alpha_1, \ldots, \alpha_n)$ минимальное расширение K — подполе L, содержащее $\alpha_1, \ldots, \alpha_n$.
Будем говорить, что $K(\alpha_1, \ldots, \alpha_n)$ получено из K присоединением $\alpha_1, \ldots, \alpha_n$.

Лемма 4

$K(\alpha_1, \ldots, \alpha_n)$ — пересечение всех расширений K, являющихся подполями L и содержащих $\alpha_1, \ldots, \alpha_n$.

Доказательство. • Пусть $\{F_i\}_{i \in I}$ — все такие расширения K, $F = \bigcap\limits_{i \in I} F_i$.

• Тогда F замкнуто по взятию суммы, призведения, обратных элементов по сложению и умножению (для любых двух $x, y \in F$ все это есть в каждом F_i, а значит и в F).

• Следовательно, F — поле. Так как F содержит $\alpha_1, \ldots, \alpha_n$, мы имеем $F = K(\alpha_1, \ldots, \alpha_n)$. □

Лемма 5

Пусть L — расширение поля K, $\alpha_1, \ldots, \alpha_n \in L$. Тогда $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1)(\alpha_2)\ldots(\alpha_n)$ (то есть, $K(\alpha_1, \ldots, \alpha_n)$ получается последовательным присоединением элементов $\alpha_1, \ldots, \alpha_n$).

Доказательство. • Индукция по n.

• Достаточно доказать, что $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.

• Пусть $F = K(\alpha_1, \ldots, \alpha_{n-1})$.

$\supset$ • Очевидно, $K(\alpha_1, \ldots, \alpha_n) \supset F$. То есть, это расширение поля F, содержащее α_n.

• Следовательно, $K(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_n)$.

$\subset$ • $F(\alpha_n)$ — расширение поля K, содержащее $\alpha_1, \ldots, \alpha_n$.

• Значит, $F(\alpha_n) \supset K(\alpha_1, \ldots, \alpha_n)$. □

Теорема 3

Пусть L — расширение поля K, $\alpha \in L$ — алгебраический элемент. Тогда $K(\alpha) \simeq K[x]/f_\alpha \cdot K[x]$. В частности, $[K(\alpha) : K] = \deg(f_\alpha)$.

Доказательство. • Пусть $\deg(f_\alpha) = n$. Рассмотрим $F = \mathrm{Lin}(1, \alpha, \ldots, \alpha^{n-1})$ (множество линейных комбинаций с коэффициентами из K). Очевидно, $F \subset K(\alpha)$.

• Так как $\deg(f_a) = n$, нет многочлена меньшей степени, корнем которого является α. Значит, $1, \alpha, \ldots, \alpha^{n-1}$ ЛНЗ над K.

• $\alpha^m \in F$ при $m \geq n$ является линейной комбинацией $1, \alpha, \ldots, \alpha^{n-1}$ с коэффициентами из K.

• Таким образом, F содержит $g(\alpha)$ для любого многочлена $g \in K[x]$.

• Значит, F замкнуто по умножению, то есть, это кольцо.

• Пусть $\varphi : K[x] \to F$ — задано формулой $\varphi(f) := f(\alpha)$. Нетрудно проверить, что f — гомоморфизм колец.

• Так как $f(\alpha) = 0 \iff f \vdots f_\alpha$, мы имеем $\ker(\varphi) = f_\alpha \cdot K[x]$.

• По теореме о гомоморфизме колец (Глава 0) $F \simeq K[x]/f_\alpha \cdot K[x]$.

• По Лемме 1 мы знаем, что f_a — неприводимый в $K[x]$. По Теореме 2 тогда $K[x]/f_\alpha \cdot K[x]$ — поле, а значит, и F — поле.

• Так как $\alpha \in F$, по определению $K(\alpha)$, тогда $K(\alpha) = F$. □

Теорема 4

Пусть L — расширение поля K, а A — множество всех элементов L, алгебраических над K. Тогда A — поле.

Доказательство. • Пусть $u, v \in A$. Тогда можно считать, что $[K(u) : K] = n \in N$ и $[K(v) : K] = m \in N$.

• По Лемме 5, $K(u, v) = K(u)(v)$.

• Пусть $f_v \in K[x]$ — минимальный многочлен v над K.

• Так как $f_v \in (K(u))[x]$ и $f_v(v) = 0$, минимальный многочлен v над $K(u)$ по Лемме 1 является делителем f_v, а значит, имеет степень не более чем $\deg(f_v) = m$.

• По Теореме 3 тогда $[K(u, v) : K(u)] \leq [K(v) : K] = m$.

• По Теореме 1 имеем $[K(u, v) : K] = [K(u, v) : K(u)] \cdot [K(u) : K] \leq mn$.

• По Лемме 3 тогда все элементы $K(u, v)$ — алгебраические над K, то есть, $K(u, v) \subset A$.

• Таким образом, A замкнуто по сложению, умножению, вычитанию и делению (так как $K(u, v)$ замкнуто), то есть, A — поле. □

Поле разложения многочлена

Определение

Расширение L поля K называется полем разложения унитарного многочлена $f \in K[x]$, если f раскладывается в L на линейные множители: $f = (x - \alpha_1) \dots (x - \alpha_n)$ и $L = K(\alpha_1, \dots, \alpha_n)$.

Теорема 5

Пусть K — поле. Тогда для любого унитарного многочлена $f \in K[x]$ существует поле разложения L, причем $[L : K] \leq n!$, где $\deg(f) = n$.

Доказательство. • Индукция по $\deg(f)$. База для случая $\deg(f) = 1$ очевидна.

• Переход. Пусть для многочленов меньших чем $\deg(f)$ степеней теорема доказана.

• Пусть $f \vdots f_1$, где многочлен f_1 неприводимый.

• По Теореме 3 существует расширение $K(\alpha_1)$ поля K, в котором f_1 (а значит, и f) имеет корень α_1, то есть, $f(x) \vdots x - \alpha_1$.

• Выделим все линейные множители в разложении f в $K(\alpha_1)$: $f(x) = (x - \alpha_1) \dots (x - \alpha_k) g(x)$.

• Корни $\alpha_2, \dots, \alpha_k$ и так есть в $K(\alpha_1)$ — можно считать, что мы их присоединяем без изменения поля.

• По индукционному предположению, существует поле разложение L многочлена g над $K(\alpha_1)$, причем L получено присоединением корней g и $[L : K(\alpha_1)] \leq (\deg(g))! = (n - k)! \leq (n - 1)!$.

• В поле L многочлен f раскладывается на линейные множители.

• По Теореме 1, $[L : K] \leq [L : K(\alpha_1)] \cdot [K(\alpha_1) : K] \leq n \cdot (n - 1)! = n!$. □

• Пусть $\varphi : K \to K'$ — изоморфизм полей. Тогда φ продолжается до изоморфизма колец многочленов $\varphi : K[x] \to K'[x]$ (достаточно положить $\varphi(x) = x$).

Теорема 6

Пусть $\varphi : K \to K'$ — изоморфизм полей, $f \in K[x]$ — унитарный многочлен, $f' := \varphi(f)$. Пусть F и F' — поля разложения многочленов f и f' над K и K' соответственно. Тогда существует изоморфизм полей F и F'.

Доказательство. • Индукция по $m := [F : K]$.

База $m = 1$. Тогда $F = K$, то есть, f раскладывается на линейные множители в K: пусть $f(x) = (x - \alpha_1) \dots (x - \alpha_m)$.

• Тогда $f'(x) = (\varphi(f))(x) =$

$\varphi(x - \alpha_1) \dots \varphi(x - \alpha_m) = (x - \varphi(\alpha_1)) \dots (x - \varphi(\alpha_m))$.

• Следовательно, $F' = K'$.

Переход. Пусть для многочленов меньшей степени утверждение доказано.

• Пусть α — корень f в F, а $g = f_\alpha$ — минимальный многочлен α в $K[x]$.

• По Лемме 1, $f \vdots g$. По Лемме 2, g — неприводимый в $K[x]$.

- Пусть $g' = \varphi(g)$. Тогда многочлен g' неприводим в $K'[x]$.
- $f \vdots g \Rightarrow f' \vdots g'$ (если $f = gq$ в $K[x]$, то $f' = g'q'$ в $K'[x]$, где $q' := \varphi(q)$).
- Так как f' раскладывается на линейные множители в F', g' тоже раскладывается на линейные множители в F'.
- В частности, $\exists \alpha' \in F'$ такой, что $g'(\alpha') = 0$.
- По Теореме 3 тогда $K(\alpha) \simeq K[x]/gK[x]$ и $K'(\alpha') \simeq K'[x]/g'K'[x]$.
- Напомним, что $\varphi : K[x] \to K'[x]$ — изоморфизм колец и $\varphi(g) = g'$.
- Значит, φ индуцирует изофоморфизм

$$\overline{\varphi} : K[x]/gK[x] \to K'[x]/g'K'[x],$$

заданный формулой $\overline{\varphi}(\overline{h}) := \varphi(h)$ (это несложно проверить).

- Пусть $P := K(\alpha)$ и $P' := K'(\alpha')$. Так как композиция изоморфизмов — изоморфизм, существует изофоморфизм полей $\psi : P \to P'$.
- Изоморфизм ψ продолжается на кольца многочленов $P[x]$ и $P'[x]$.

• В $P[x]$ многочлен f имеет корень (так как $f \vdots g$ и g имеет корень), а значит, $k \geq 1$ линейных множителей:

$f(x) = (x - \alpha_1) \dots (x - \alpha_k) h(x)$.

• Положим $\psi(\alpha_i) = \alpha'_i$ для всех $i \in \{1, \dots, k\}$. Тогда в $P'[x]$ имеем

$$f'(x) = (x - \alpha'_1) \dots (x - \alpha'_k) h'(x), \quad \text{где } h' = \psi(h).$$

• По Лемме 4, при построении поля разложения порядок присоединения корней не имеет значения. Значит, при построении F можно было начать с присоединения α, а при построении F' — с присоединения α'.

• Тогда, по построению поля разложения, F — поле разложения h над P, а F' — поле разложения h' над P'.

• Значит, по индукционному предположению, $F \simeq F'$. □

Следствие 1

Пусть K — поле, а $f \in K[x]$. Тогда поле разложения многочлена f над K единственно с точностью до изоморфизма.

Конечные поля

• Все поля из $p \in \mathbb{P}$ элементов изоморфны $\mathbb{Z}/p\mathbb{Z}$. Будем применять обозначение $\mathbb{F}_p$ для поля $\mathbb{Z}/p\mathbb{Z}$ (при $p \in \mathbb{P}$).

• Далее будем считать, что любое поле характеристики p содержит подполе $\mathbb{F}_p$.

Лемма 6

Пусть $q \in \mathbb{N}$, K — поле, $|K| = q$. Тогда $q = p^n$, где $p = \mathrm{char}(K) \in \mathbb{P}$, а $n = [K : \mathbb{F}_p]$.

Доказательство. • Так как $\mathbb{Q}$ бесконечно, по Теореме 0.4 имеем $\mathrm{char}(K) \neq 0$.

• Значит, $\mathrm{char}(K) = p \in \mathbb{P}$ и $\mathbb{F}_p$ — подполе K.

• Тогда K — линейное пространство над своим подполем $\mathbb{F}_p$ размерности $n := [K : \mathbb{F}_p]$. Следовательно, $n \in \mathbb{N}$.

• Каждый элемент поля K имеет разложение по n-элементному базису K над $\mathbb{F}_p$, а значит, записывается как столбец из n координат из $\mathbb{F}_p$.

• Каждая координата из $\mathbb{F}_p$ может принимать ровно p значений, поэтому, существует ровно p^n различных столбцов из n координат.

• Разные разложения по базису соответствуют разным векторам, поэтому, разным столбцам из n элементов $\mathbb{F}_p$ соответствуют разные элементы поля K. Значит, $q = p^n$. □

Лемма 7

Пусть $p \in \mathbb{P}$, $k, n \in \mathbb{N}$, причем $0 < k < p^n$. Тогда $C_{p^n}^k \vdots p$.

Доказательство. • Напомним, что $C_{p^n}^k = \frac{p^n!}{k!(p^n-k)!}$.

• Посчитаем степени вхождения p в числитель и знаменатель это дроби.

• p входит в $(p^n)!$ с показателем $\alpha = \sum\limits_{i=1}^{n} \frac{p^n}{p^i} = \sum\limits_{j=0}^{n-1} p^j$.

• p входит в $k!(p^n - k)!$ с показателем

$$\beta = \sum_{i=1}^{n-1} [\tfrac{k}{p^i}] + \sum_{i=1}^{n-1} [\tfrac{p^n-k}{p^i}] \leq \sum_{i=1}^{n-1} \tfrac{k+p^n-k}{p^i} = \sum_{j=1}^{n-1} p^j < \alpha.$$

• Следовательно, $C_{p^n}^k \vdots p^{\alpha-\beta} \vdots p$. □

Теорема 7

Пусть $p \in \mathbb{P}$, $n \in \mathbb{N}$. Тогда существует единственное с точностью до изоморфизма поле $\mathbb{F}_{p^n}$ из p^n элементов, и это поле является полем разложения многочлена $x^{p^n} - x$ (все элементы $\mathbb{F}_{p^n}$ — в точности корни $x^{p^n} - x$).

Доказательство. ! • Пусть K — поле из p^n элементов.

• Через K^* обозначается мультипликативная группа поля K (группа всех ненулевых элементов по умножению). Тогда $|K^*| = p^n - 1$.

• По теореме Лагранжа (Теореме 6.1) мы знаем, что $p^n - 1 \vdots \operatorname{ord}(a)$, следовательно, для любого $a \in K^*$ выполнено $a^{p^n-1} = 1$.

• Теперь ясно, что все p^n элементов поля K — корни многочлена $x^{p^n} - x$ степени p^n, который по Теореме 3.7 имеет не более чем p^n корней.

• Значит, элементы K — все различные корни $x^{p^n} - x$. В частности, это означает, что K — поле разложения многочлена $x^{p^n} - x$ над $\mathbb{F}_p$.

• По Теореме 6 поле разложения $x^{p^n} - x$ над $\mathbb{F}_p$ единственно с точностью до изоморфизма.

$\exists$ • Пусть L — поле разложения многочлена $x^{p^n} - x$ над $\mathbb{F}_p$, а K — множество всех корней $f(x) = x^{p^n} - x$ в L.

• Возьмем производную: $f'(x) = p^n \cdot x^{p^n-1} - 1 = -1$.

• Значит, f не имеет кратных корней (если $f(x) \vdots (x-a)^2$, то $f'(x) \vdots (x-a)$, что не так).

• Таким образом, $|K| = p^n$. Докажем, что K — поле. Пусть $x, y \in K \Rightarrow x^{p^n} = x$ и $y^{p^n} = y$ в K.

Замкнутость по $+$: $(x+y)^{p^n} = \sum\limits_{k=0}^{p^n} \mathrm{C}_{p^n}^k x^k y^{p^n-k} = x^{p^n} + y^{p^n}$ $= x + y \Rightarrow f(x+y) = 0 \Rightarrow x + y \in K$.

(Мы использовали, что $\mathrm{C}_{p^n}^k \vdots p$ при $0 < k < p^n$ по Лемме 7.)

Замкнутость по $\cdot$: $(xy)^{p^n} = x^{p^n} y^{p^n} = xy \Rightarrow f(xy) = 0 \Rightarrow xy \in K$.

Обратный элемент по $+$: $f(-x) = -f(x) = 0$, так как p^n нечетно, следовательно, $-x \in K$

Обратный элемент по $\cdot$:
$(x^{-1})^{p^n} = (x^{p^n})^{-1} = x^{-1} \Rightarrow f(x^{-1}) = 0 \Rightarrow x^{-1} \in K$.

• Следовательно, K — поле. По определению поля разложения, $L = K$.

• Таким образом, существует поле из p^n элементов. $\square$

• Далее для $q = p^n$, где $p \in \mathbb{P}$ и $n \in \mathbb{N}$ будем через $\mathbb{F}_q$ обозначать поле из $q = p^n$ элементов.

Теорема 8

Пусть $p \in \mathbb{P}$ и $n \in \mathbb{N}$. Тогда подполя $\mathbb{F}_{p^n}$ — это в точности все поля $\mathbb{F}_{p^d}$, где $d \in \mathbb{N}$ и $n \vdots d$.

Доказательство. • Пусть K — подполе $\mathbb{F}_{p^n}$.

• Тогда K — конечно, значит, $K = \mathbb{F}_q$, где q — степень простого числа.

• Кроме того, $\mathbb{F}_{p^n}$ — конечное расширение $\mathbb{F}_q$, пусть $\ell = [\mathbb{F}_{p^n} : K]$.

• Аналогично рассуждению Леммы 6 получаем, что $p^n = q^\ell$, откуда следует, что $q = p^d$, где $d\ell = n$.

• Осталось доказать, что при каждом $n \vdots d$ поле $\mathbb{F}_{p^d}$ является подполем $\mathbb{F}_{p^n}$.

• По Теореме 7, $\mathbb{F}_{p^d}$ — поле разложение многочлена $x^{p^d} - x$, а $\mathbb{F}_{p^n}$ — поле разложение многочлена $x^{p^n} - x$.

• При $n \vdots d$ мы имеем $x^{p^n} - x \vdots x^{p^d} - x$, поэтому, $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$.

• Тогда понятно, что $\mathbb{F}_{p^d}$ — подполе $\mathbb{F}_{p^n}$. □

Теорема 9

Пусть $\mathbb{F}_q$ — конечное поле. Тогда его мультипликативная группа (то есть группа обратимых элементов по умножению) $\mathbb{F}_q^*$ — это циклическая группа порядка $q-1$.

Доказательство. • Начнем с двух вспомогательных утверждений.

Утверждение 1

Пусть $a, b \in \mathbb{F}_q^*$, $(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$. Тогда $\operatorname{ord}(ab) = \operatorname{ord}(a) \cdot \operatorname{ord}(b)$.

Доказательство. • Пусть $m = \operatorname{ord}(a)$, $n = \operatorname{ord}(b)$, $\operatorname{ord}(ab) = k$.

• Так как группа абелева, $1 = (ab)^k = a^k b^k$.

• Тогда $a^k = (b^k)^{-1}$, откуда $\frac{m}{(k,m)} = \operatorname{ord}(a^k) = \operatorname{ord}(b^k) = \frac{n}{(k,n)}$.

• Пусть $p \in \mathbb{P}$, $p^\alpha \| n$, $\alpha \geq 1$. Тогда $m \not\vdots p$.

• Пусть $p^\gamma \| k$. Если $\gamma < \alpha$, то $\frac{n}{(k,n)} \vdots p$, а $\frac{m}{(k,m)} \not\vdots p$, противоречие.

• Значит, если $n \vdots p$, то p входит в k с неменьшим показателем, чем в n, а значит, $k \vdots n$.

• Аналогично, $k \vdots m$, откуда ввиду $(m, n) = 1$ имеем $k \vdots mn$.

• Остается заметить, что $(ab)^{mn} = a^{mn} b^{mn} = 1$. □

• Пусть m — это НОК порядков элементов $\mathbb{F}_q^*$.

Утверждение 2

В $\mathbb{F}_q^*$ есть элемент порядка m.

Доказательство. • Пусть $m = p_1^{k_1} \dots p_s^{k_s}$.

• Для каждого i в $\mathbb{F}_q^*$ есть элемент с порядком, кратным $p_i^{k_i}$, а значит, и элемент a_i порядка $p_i^{k_i}$.

• Докажем индукцией по $t \leq s$, что $\operatorname{ord}(a_1 \dots a_t) = p_1^{k_1} \dots p_t^{k_t}$. База $t = 1$ очевидна.

Переход $t - 1 \to t$.

• Так как $(p_1^{k_1} \dots p_{t-1}^{k_{t-1}}, p_t^{k_t}) = 1$, по Утверждению 1 имеем $\operatorname{ord}(a_1 \dots a_{t-1}a_t) = \operatorname{ord}(a_1 \dots a_{t-1})\operatorname{ord}(a_t) = p_1^{k_1} \dots p_t^{k_t}$ □

• Однако, $\forall a \in \mathbb{F}_q^*$ мы имеем $\operatorname{ord}(a) \mid m$, откуда $a^m - 1 = 0$. Значит, все элементы $\mathbb{F}_q^*$ — корни многочлена $x^m - 1$.

• Все элементы $\mathbb{F}_q^*$ — корни многочлена $x^{q-1} - 1$. Значит, $q - 1 \vdots m$. Если $m < q - 1$, то, очевидно, в $\mathbb{F}_q^*$ менее $q - 1$ элементов, что не так.

• Значит, $m = q - 1$. Тогда по Утверждению 2 существует такой $a \in \mathbb{F}_q^*$, что $\operatorname{ord}(a) = q - 1$. Очевидно, в этом случае $\mathbb{F}_q^* = \langle a \rangle$. □

Лемма 8

Пусть $p \in \mathbb{P}$, $k, n \in \mathbb{N}$, $q = p^n$. Отображение $\varphi : \mathbb{F}_q \to \mathbb{F}_q$, заданное формулой $x \to x^{p^k}$ — автоморфизм поля $\mathbb{F}_q$.

Доказательство. • Достаточно доказать, что $\varphi(x) := x^p$ — автоморфизм $\mathbb{F}_q$ (так как композиция автоморфизмов — автоморфизм).

• Пусть $x, y \in \mathbb{F}_q$. Очевидно, $(xy)^p = x^p y^p$.

• По Лемме 7, $(x+y)^p = \sum\limits_{k=0}^{p} \mathrm{C}_p^k x^k y^{p-k} = x^p + y^p$.

• Таким образом, φ — гомоморфизм полей.

• Так как $\ker(\varphi)$ — идеал в $\mathbb{F}_{p^n}$ и, очевидно, $\ker(\varphi) \neq \mathbb{F}_{p^n}$ (например, $\varphi(1) = 1 \neq 0$), то $\ker(\varphi) = \{0\}$.

• Значит, φ — инъекция. Так как $\mathbb{F}_{p^n}$ конечно, φ — биекция, то есть, это автоморфизм поля $\mathbb{F}_{p^n}$. □

Лемма 9

Пусть $p \in \mathbb{P}$, $q = p^n$, $k \in \mathbb{N}$, $\beta \in \mathbb{F}_{q^k}$ — корень многочлена $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in \mathbb{F}_q[x]$. Тогда $f(\beta^q) = 0$.

Доказательство. • По Лемме 8, $\varphi(y) := y^q$ — автоморфизм $F_{q^k}^*$. Очевидно, $c^q = c$ для любого $c \in \mathbb{F}_q$.

• Тогда $0 = \varphi(f(\beta)) = f(\varphi(\beta)) = f(\beta^q)$.

Определение

Пусть $a \in \mathbb{F}_q$ таков, что $\mathbb{F}_q^* = \langle a \rangle$. Тогда a — примитивный элемент поля $\mathbb{F}_q$.

Теорема 10

Пусть p — степень простого числа, $q = p^n$, α — примитивный элемент поля $\mathbb{F}_q$, а f_α — его минимальный многочлен над $\mathbb{F}_p$. Тогда $\mathbb{F}_q$ — поле разложения f_α.

Доказательство. • Так как $F_q^* = \langle \alpha \rangle$, мы имеем $\mathbb{F}_q \subset \mathbb{F}_p(\alpha)$. Значит, $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

• Пусть $f_\alpha(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$.

• По Лемме 9, α, α^p, $\ldots$, $\alpha^{p^{n-1}}$ — корни f_α.

• Пусть $\alpha^{p^k} = \alpha^{p^m}$ и $0 \leq k < m \leq n-1$. Тогда $0 = \alpha^{p^m} - \alpha^{p^k} = \alpha^{p^k} \cdot (\alpha^{p^m - p^k} - 1) \Rightarrow \alpha^{p^m - p^k} = 1$.

• Так как $\operatorname{ord}(\alpha) = q - 1 = p^n - 1$ в $\mathbb{F}_q^*$, должно быть $p^m - p^k \vdots p^n - 1$, что, очевидно, не так.

• Таким образом, в поле $\mathbb{F}_q$ есть n различных корней многочлена f_α степени n. Значит, $\mathbb{F}_q$ — поле разложения f_α. $\square$

Следствие 3

Пусть $p \in \mathbb{P}$, $q = p^n$, $m \in \mathbb{N}$. Тогда существует неприводимый унитарный многочлен $f \in \mathbb{F}_q[x]$ с $\deg(f) = m$.

Доказательство. • Из доказанного ранее понятно, что существует расширение $\mathbb{F}_{q^m}$ степени m поля $\mathbb{F}_q$.

• Пусть $\alpha \in \mathbb{F}_{q^m}$ — примитивный элемент, а f_α — минимальный многочлен α над $\mathbb{F}_q$.

• Тогда $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ по Теореме 12, откуда следует, что $\deg(f_\alpha) = [\mathbb{F}_{q^m} : \mathbb{F}_q] = m$.

• По Лемме 2 мы знаем, что f_α неприводим. □

• Теорема 10 позволяет нам строить поле из q^n элементов, как факторкольцо $\mathbb{F}_q[x]$ по идеалу, порожденному любым неприводимым многочленом степени n над $\mathbb{F}_q$.

• К сожалению, ни одного разумного критерия неприводимости даже над $\mathbb{F}_p$ не известно. Это обстоятельство используется в теории кодирования.

Теорема 11

Пусть $p \in \mathbb{P}$, $q = p^n$, $f \in \mathbb{F}_q[x]$ — неприводимый унитарный многочлен, $\deg(f) = d$, а L — поле разложения f. Тогда $L \simeq \mathbb{F}_{q^d}$ и $x^{q^d} - x \vdots f$.

Доказательство. • Пусть α — корень f в L.

• Так как f — неприводим, f — минимальный многочлен α над $\mathbb{F}_q[x]$.

• По Теореме 3, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$. Значит, по Теореме 7, можно считать, что $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$ (конечное поле единственно с точностью до изоморфизма).

• По Лемме 9, элементы $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}} \in \mathbb{F}_{q^d}$ — корни f.

• Докажем, что все эти корни различны — тогда $\mathbb{F}_{q^d}$ окажется полем разложения f.

• Пусть $0 \leq k < m \leq d-1$ и $\alpha^{q^k} = \alpha^{q^m} \Rightarrow$
$\alpha^{q^{d+k-m}} = (\alpha^{q^k})^{q^{d-m}} = (\alpha^{q^m})^{q^{d-m}} = \alpha^{q^d} = \alpha$.

• Таким образом, α — корень многочлена $x^{q^{d+k-m}} - x = 0$, а значит, α принадлежит его полю разложения $\mathbb{F}_{q^{d+k-m}} \subsetneq \mathbb{F}_{q^d}$.

• Противоречие с $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$. □

Теорема 12

Пусть $p \in \mathbb{P}$, $q = p^n$, $m \in \mathbb{N}$. Тогда $x^{q^m} - x$ равен в $\mathbb{F}_q[x]$ произведению всех неприводимых многочленов всех степеней $d \mid m$ в первых степенях.

Доказательство. • Пусть $f \in \mathbb{F}_q[x]$ — неприводимый многочлен степени d и $x^{q^m} - x \vdots f$. Тогда все корни f лежат в $\mathbb{F}_{q^m}$.

• Значит, $\mathbb{F}_{q^m}$ содержит поле разложения f, а это $\mathbb{F}_{q^d}$ по Теореме 13. Тогда $d \mid m$ по Теореме 8.

• Наоборот, пусть $d \mid m$ и $f \in \mathbb{F}_q[x]$ — неприводимый многочлен степени d.

• По Теореме 11, $x^{q^d} - x \vdots f \Rightarrow x^{q^m} - x \vdots x^{q^d} - x \vdots f$.

• Так как разные неприводимые многочлены попарно взаимно просты, $x^{q^m} - x$ кратно произведению всех неприводимых многочленов из $\mathbb{F}_q$, степени которых делят m.

• Очевидно, $x^{q^m} - x$ взаимно прост с $(x^{q^m} - x)' = -1$.

• Следовательно, $x^{q^m} - x$ не имеет кратных корней, а значит, каждый из описанных выше неприводимых многочленов входит в разложение $x^{q^m} - x$ в 1 степени. □

Определение

Пусть $p \in \mathbb{P}$, $m, n \in \mathbb{N}$, $q = p^n$. Обозначим через $\psi_m(q)$ количество неприводимых многочленов степени m в $\mathbb{F}_q[x]$.

Следствие 4

$\psi_m(q) = \frac{1}{m} \cdot \sum\limits_{d \mid m} \mu(\frac{m}{d}) \cdot q^d$.

Доказательство. • Для каждого d пусть $f_{d,1}, \ldots, f_{d,\psi_d(q)}$ — все неприводимые многочлены степени d в $\mathbb{F}_q[x]$.

• По Теореме 12, $x^{q^m} - x = \prod\limits_{d \mid m} \left(\prod\limits_{i=1}^{\psi_d(q)} f_{d,i}(x) \right)$.

• Просуммировав степени многочленов в правой части равенства, получим $q^m = \sum\limits_{d \mid m} d \cdot \psi_d(q)$.

• По Формуле обращения Мёбиуса для функции $d \cdot \psi_d(q)$ получаем $\psi_m(q) = \frac{1}{m} \cdot \sum\limits_{d \mid m} \mu(\frac{m}{d}) \cdot q^d$. □

Теорема 13

Пусть F_p — конечное поле, $q = p^m$, $\beta \in \mathbb{F}_q$. f_β — минимальный многочлен β в $\mathbb{F}_q$. Пусть $d \in \mathbb{N}$ — минимальное такое, что $\beta^{p^d} = \beta$. Тогда выполнены следующие утверждения.

1) *Пусть f_β — минимальный многочлен β в $\mathbb{F}_q$. Тогда* $f_\beta(x) = \prod_{i=0}^{d-1}(x - \beta^{p^i})$.

2) $\deg(f) = d \leq m$.

Доказательство. 1) • По Лемме 9, β^{p^i} — корень f_β.

• Значит, $f_\beta(x) \vdots g(x) := \prod_{i=0}^{d-1}(x - \beta^{p^i})$.

• Остается доказать, что
$g(x) = a_{d-1}x^{d-1} + \dots a_1 x + a_0 \in \mathbb{F}_P[x]$.

• Вспомним, что $\varphi(a) := a^p$ — автоморфизм поля $\mathbb{F}_p$.

• Так как $\mathbb{F}_p$ — поле разложение многочлена $x^p - x$,
Имеющего в $\mathbb{F}_q$ в точности p корней, $\varphi(a) = a \iff a \in \mathbb{F}_p$.

• Автоморфизм φ переставляет корни g по циклу:

$\beta \to \beta^p \to \dots \to \beta^{p^{d-1}} \to \beta^{p^d} = \beta$.

• Так как по Теореме Виета коэффициенты g однозначно выражаются через корни, это означает, что многочлены $\varphi(g)$ и g имеют одинаковые коэффициенты, то есть $\varphi(a_i) = a_i$ для любого $i \in [0..d-1]$.

• Следовательно, $g \in \mathbb{F}_P[x]$, откуда $f_\beta = g$.

2) Из $x^{p^m} = x$ следует $m \leq d$ $\square$