Лекция 22.

Гайфуллин Сергей Александрович

МГУ

9 декаря, 2020

Предложение. Пусть $f(x) \in F[x]$ – неразложимый многочлен. Тогда $F[x]/(f(x)) = F(x + (f))$.

Доказательство. $F[x]/(f) = \{g(x) + (f)\}$. Элемент $y = x + (f)$ алгебраический над F, так как $f(y) = 0$. Значит, $F(y) = F[y] \cong F[x]/(f)$.

Определение.

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

Определение.

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. Поле разложения любого многочлена существует.

Доказательство. Разложим $h(x)$ на неприводимые множители над F. Пусть h_1 – один из неприводимых множителей степени больше 1. 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.

Увеличивая количество множителей доведем это количество до $\deg h$. Получаем поле разложения $h(x)$.

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

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

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

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

Продолжение доказательства. Если $a^q = a$ и $b^q = b$, то $(ab)^q = a^q b^q$ и $(a+b)^q = (a+b)^{p^n} = a^q + b^q = a + b$. Аналогично $(a-b)^q = (a+(-b))^q = a^q + (-b)^q$. Если q нечцтно, то $(a-b)^q = a - b$. Если же q четно, то $p = 2$ и $a - b = a + b$.
В любом случае $ab, a+b$ и $a-b$ – корни $x^q - x$. Значит, корни этого многочлена образуют подполе.

Предложение. 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 в K 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
$0 = \widetilde{\varphi}(0) = \widetilde{\varphi}(a_n\alpha^n + \ldots + a_0) = \varphi(a_n)\beta^n + \ldots + \varphi(a_0) = \varphi(f)(\beta)$.
Напротив, пусть β – корень $\varphi(f)$. Тогда формула $\widetilde{\varphi}(b_k\alpha^k + \ldots + b_0) = \varphi(b_k)\beta^k + \ldots + \varphi(b_0)$ задает ненулевой гомоморфизм (а значит, вложение) $F(\alpha) \hookrightarrow K$.

Теорема. 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 $L_0 = F \subset L_1 \subset \ldots \subset L_s = L$, где $L_{i+1} = L_i(\alpha)$ 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 $\varphi_i \colon L_i \hookrightarrow K$, продолжающее вложение $\varphi_{i-1} \colon L_{i-1} \hookrightarrow K$. По предложению φ_{i-1} может быть продолжен до φ_i 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.

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

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

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

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

Лемма. 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.

Теорема. В поле $\mathbb{F}_{p^n}$ есть подполе, изоморфное $\mathbb{F}_{p^m}$ тогда и только тогда, когда $m \mid n$.

Доказательство. Если $L \cong \mathbb{F}_{p^n}$ содержит подполе $K \cong \mathbb{F}_{p^m}$, 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.