1 Простые поля, расширения полей, поле разложения многочлена

Определение 1.1 (Простое поле)**.** Поле - простое, если его подалгебры не являются полями

Определение 1.2 (Собственное подполе)**.**

Теорема 1.3. *Любое просто поле изоморфно либо рациональным числам или полю вычетов по простому числу, то есть F - простое поле, тогда $F \simeq Q$ или $F \simeq \mathbb{Z}_p$, где $p \in \mathbb{Z}$ - простое*

Доказательство. В поле есть 1, поэтому можно строить кратные суммы единиц $(1 + .. + 1)$. Строя такие суммы мы или никогда не получим 0 или получим

1. Никогда не получится 0, то есть $k \cdot 1 \neq 0\,(-(k \cdot 1) \neq 0)$ при $k > 0$.

   В поле для любого элемента есть обратный: $(k \cdot 1)^{-1}$ и $-(k \cdot 1)^{-1}$. В поле можно умножать: $(m \cdot 1)(k \cdot 1)^{-1}$. Так можно заметить что все элементы имеют вид

   $$m \cdot 1 = (m \cdot 1)(1 \cdot 1)^{-1}$$
   $$k \cdot 1 = (1 \cdot 1)(k \cdot 1)^{-1}$$

   Если $m \neq 0, k \neq 0$, то $(m \cdot 1)(k \cdot 1)^{-1} \neq 0$. Так как $\{(m \cdot 1)(k \cdot 1)^{-1}\}$ образует поле и F - простое, то $\{(m \cdot 1)(k \cdot 1)^{-1}\}$ образует всё поле.

   Можно построить изоморфизм где $(m \cdot 1)(k \cdot 1)^{-1} \xrightarrow{\text{h}} \frac{m}{k}$. Покажем что это так. Сначала нужно доказать что это гомоморфизм:

   Да, это гомоморфизм

   Так как поле - это кольцо, для h существует $\operatorname{Ker} h$ и по **??** $\operatorname{Ker} h$ - идеал. Так как поле - тело, то по **??** существует только два идеала: F и $\{0\}$. Ядро гомоморфизма является одним из этих идеалов, и так как оно не может быть равно всему полю F оно равно $\{0\}$ Для того чтобы показать что h - изоморфизм, нужно показать что это инъекция и сюръекция

   (a) Так как $\operatorname{Ker} h = \{0\}$ то по **??** h разнозначно

   (b) для каждого образа $\frac{m}{k} \in \mathbb{Q}$ есть прообраз $(m \cdot 1)(k \cdot 1)^{-1} \in F$

   Следовательно $F \simeq \mathbb{Q}$

2. $k \cdot 1 = 0$ для некоторого $k > 0$

   Выберем наименьшее $k > 0$ для которого $k \cdot 1 = 0$. Мы можем получить элементы $0, 1, 2 \cdot 1, 3 \cdot 1, ..., (k-1) \cdot 1$. Докажем от противного что k должно быть простым:

   Так как k не простое, то оно раскладывается $k = pq$, где $p, q > 1$, $p, q < k$.

   $$0 = k \cdot 1 = (p \cdot 1)(q \cdot 1)$$

   поскольку $p, q < k$, то

   $$(p \cdot 1) \neq 0 \neq (q \cdot 1)$$

   делители нуля. Противоречие, число не составное.

   Возьмём $p = k$, $\mathbb{Z}_p = \{0, ..., p-1\}$ - это кольцо (ассоциативное, коммутативное, с единицей), остаётся проверить наличие обратного. Пусть $x \neq 0$ и $x \in \mathbb{Z}_p$, тогда НОД$(x, p) = 1$. Из этого следует что $nx + mp = 1$ для некоторых $n, m \in \mathbb{Z}_p$

   $$\begin{aligned} nx + mp &= 1 \\ (nx + mp) \bmod p &= 1 \bmod p \\ nx \bmod p + mp \bmod p &= 1 \\ nx \bmod p &= 1 \\ n \bmod p \cdot x \bmod p &= 1 \\ n \bmod p \cdot x &= 1 \end{aligned}$$

   $n \bmod p$ - обратный для произвольного x, соответственно $\mathbb{Z}_p$ - поле.

□

Следствие 1.4. *Внутри каждого поля есть простое подполе*

Доказательство. □

Определение 1.5 (Характеристика поля)**.** Для некоторого поля F его характеристика это

1. если $k \cdot 1 \neq 0$ для всех $k > 0$, то 0 - характеристика поля F
2. если $k \cdot 1 = 0$ для некоторого $k > 0$, то k - характеристика поля F (F - поле конечной характеристики)

Определение 1.6 (Неразложимый многочлен)**.** Неразложимый многочлен - многочлен, который не раскладывается на множители, ни один из которых не является многочленом нулевой степени.

Пример 1.7 (Пример неразложимого многочлена)**.**

Следствие 1.8. *1. Многочлен 1 степени всегда неразложим*

2. *Многочлен 2 или 3 степени неразложим* $\Leftrightarrow$ *не имеет корней*
3. *Если многочлен степени большей 3 не разложим, то он не имеет корней*

Доказательство. □

Следствие 1.9. *Неразложимый многочлены - простые элементы кольца многочленов*

Доказательство. □

Теорема 1.10. R *- кольцо главных идеалов,* c *- простой элемент, тогда* cR *- простой идеал*

Доказательство. Пусть c - простой элемент, допустим что cR - не простой идеал, тогда найдутся $a, b \notin cR$ такие что $ab \in cR$. Сумма идеалов $dR = aR + cR$ - тоже идеал. Потом я не пойму ПОЧЕМУ. □

Теорема 1.11. R *- кольцо главных идеалов,* I *- простой идеал, тогда* I *- максимальный идеал*

Доказательство. Пусть дан простой идеал $I = cR$, дальше магия □

Следствие 1.12. *Если* p *- неразложимый многочлен, тогда порождённый им идеал является максимальным*

Доказательство. Следует из двух предыдущих и 1.9 или из **??** и 1.9 □

Следствие 1.13. $F[x] \Big/ \langle p \rangle$ *- поле*

Доказательство. Следует из того что факторкольцо по протому элементу - это поле, но здесь такой теоремы (пока) нет □

Теорема 1.14. *Для каждого многочлена существует расширение поля, в котором он разложится на линейные множители.*

Доказательство. Пусть $p(x) \in P[x]$. Индукция по степени многочлена p:

Базис. $\deg p = 1$. $p(x) = ax + b$ - линейный, то есть уже разложен

Индукционный шаг. Предположим p раскладывается на два многочлена $p = q \cdot s$, тогда по индукционному предположению для этих многочленов существует поле где они разложатся.

Теперь предположим что p не раскладывается. Построим $F[y] \Big/ \langle p(y) \rangle = F'$ - расширение F. Это будет расширением потому что можно построить изоморфизм $h : F \to F'$, $h(y) = y + \langle p(y) \rangle$

Пусть $\alpha = y + \langle p(y) \rangle$ - корень многочлена p в F', тогда

$$\begin{aligned} p(y + \langle p(y) \rangle) &= \sum_{i=0}^{n} p_i (y + \langle p(y) \rangle)^i \\ &= \sum_{i=0}^{n} p_i (y^i + \langle p(y) \rangle) \\ &= (\sum_{i=0}^{n} p_i y^i) + \langle p(y) \rangle \\ &= p(y) + \langle p(y) \rangle \\ &= 0 \end{aligned}$$

действительно, $\alpha = y + \langle p(y) \rangle$ - корень многочлена p в F' □

Пример 1.15 (Пример расширения поля)**.**

Следствие 1.16. *Если F - конечное поле, то поле расширений многочлена p тоже конечно*

Доказательство. По индукции □

Следствие 1.17. *Пусть $p \in P[x]$ и $\deg p = n$, тогда количество корней p с учётом кратности будет $\leq n$ и существует поле где оно равно n*

Доказательство. Пусть F' - расширение F, в над которым многочлен раскладывается на линейные множители. Тогда $p(x) = a_0(x - a_1)^{n_1} ... (x - a_k)^{n_k}$. Если $\deg p = n$, то $n_1 + ... n_k = n$ □