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

$\square$

Следствие 1.4. *Внутри каждого поля есть простое подполе*

Доказательство. $\square$

Определение 1.5 (Характеристика поля)**.**

Определение 1.6 (Неразложимый многочлен)**.** Неразложимый многочлен - многочлен, который не раскладывается на множители

Следствие 1.7.

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*

Следствие 1.8. *Неразложимый многочлены - простые элементы кольца многочленов*

Теорема 1.9. *R - кольцо главных идеалов, c - простой элемент, тогда cR - простой идеал*

Следствие 1.10. *Если p - неразложимый многочлен, тогда порождёныый им мдеал является максимальным*

Следствие 1.11. $F(x) \big/ \langle p \rangle$ *- поле*

Теорема 1.12. *Для каждого многочлена существует расширение поля, в котором он разложится на линейные множители.*

Доказательство. □

Следствие 1.13. *Если F - конечное поле, то поле расширений многочлена p тоже конечно*

Следствие 1.14. $degp = n$

Доказательство. □