Оглавление

Глава 1

Кольца и поля

1.1. Классификация простых полей

Теорема 1 (классификация простых полей)**.**

1. Поля $\mathbb{Q}$ и $\mathbb{Z}_p$ при $p \in \mathbb{P}$ – простые

   Доказательство.

   - $\mathbb{Q}$
     Пусть $\mathbb{Q}$ **не простое**, и K – подполе $\mathbb{Q}$ $\quad \Longrightarrow\ 0, 1 \in K$

     $$\underbrace{1 + 1 + \cdots + 1}_{n} \in K \quad \forall n \quad \Longrightarrow \mathbb{N} \subset K$$

     Если $n \in K$, то $(-1) \in K \quad \Longrightarrow \mathbb{Z} \subset K$
     Если $n \in K,\ n \neq 0$, то $\frac{1}{n} \in K \quad \Longrightarrow \frac{1}{n} \in K \quad \forall n \in \mathbb{N}$

     $$m \in \mathbb{Z},\ n \in \mathbb{N} \Longrightarrow \frac{m}{n} = m \cdot \frac{1}{n} \in K \quad \Longrightarrow \mathbb{Q} = K$$

   - $\mathbb{Z}_p$
     Аналогично, пусть K – подполе $\mathbb{Z}_p$

     $$\overline{1} \in K$$

     $$\underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{n} \in K \quad \forall n \quad \Longrightarrow \overline{n} \in K \quad \forall n \quad \Longrightarrow \mathbb{Z}_p = K$$

   $\square$

2. Любое простое поле изоморфно $\mathbb{Q}$ или $\mathbb{Z}_p$ для некоторого $p \in \mathbb{P}$

Доказательство. Пусть K — поле
Докажем, что K содержит подполе, изоморфное $\mathbb{Q}$ или $\mathbb{Z}_p$
Возьмём A — минимальное подкольцо K, содержащее 1
Докажем, что $A \simeq \mathbb{Z}$ (взяв все частные из A, получим множество дробей) или $A \simeq \mathbb{Z}_p$:
Пусть $f : \mathbb{Z} \to A$ такое, что

$$f(n) \coloneqq \begin{cases} \underbrace{1+1+\dots+1}_{n}, & n > 0 \\ -(\underbrace{1+1+\dots+1}_{n}), & n < 0 \\ 0, & n = 0 \end{cases}$$

- Докажем, что f — гомоморфизм:
  - Докажем, что $f(n) + f(k) = f(n+k)$:
    Кольцо — это группа по сложению. Умножение n единиц — это возведение в n степень. Знаем, что $1^n * 1^k = 1^{n+k}$, где $*$ — это $+$
  - $f(nk) = f(n) \cdot f(k)$:
    - $n, k > 0$
      $$(\underbrace{1+\dots+1}_{n})(\underbrace{1+\dots+1}_{k}) = \underbrace{1\cdot 1+\dots+1\cdot 1}_{nk} = \underbrace{1+\dots+1}_{nk}$$
    - $n = 0$
      $$f(0) = f(0)f(k)$$
    - $n > 0,\ k < 0$
      Положим $k_1 \coloneqq -k$
      $$f\Big(n(-k_1)\Big) = f(n)f(-k_1) \quad\Longleftarrow\quad -f(nk_1) = f(n)\Big(-f(k_1)\Big)$$

  По теореме о гомомрфизме $\operatorname{Im} f \simeq \mathbb{Z}/_{\ker f}$
  $\operatorname{Im} f$ — подкольцо A
  $\ker f$ — идеал $\implies \ker f = \langle m \rangle$
    - $m = 0$
      $$\ker f = \{\,0\,\} \implies \mathbb{Z}/_{\ker f} = \mathbb{Z}/_{\{\,0\,\}} \simeq \mathbb{Z}$$
    - $m \neq 0$
      $$\operatorname{Im} f \simeq \mathbb{Z}/_{\langle m\rangle} \simeq \mathbb{Z}_m$$
      $\operatorname{Im} f$ — подкольцо поля $K \implies \operatorname{Im} f$ — область целостности
      $\implies \langle m \rangle$ — простой идеал $\implies m \in \mathbb{P}$

∎

Замечание. Характеристику можно определять по простому полю:

$$K \simeq \mathbb{Z}/_{\langle m\rangle} \implies \operatorname{char} \mathbb{Z} = m$$

Отсюда видно, почему характеристика 0, если не существует нужной степени

1.2. Степень расширения

Лемма 1. K — поле, $\qquad L$ — расширение K
Тогда L является векторным пространством над K

Доказательство.

- Операции:
  - $l_1 + l_2, \quad l_1, l_2 \in L$

$- \ kl, \quad k \in K, \ l \in L$

k, l — элементы L, для них операции определены

- L — абелева группа по сложению:

$$(k_1 k_2)l = k_1(k_2 l)$$

□

Примеры.

1. $\mathbb{R} \subset \mathbb{C}$
   Базис — $\{ 1, i \}$
2. $\mathbb{R}(x)$ — бесконечномерное векторное пространство над $\mathbb{R}$

Определение 1. L — расширение K
Степенью расширения L над K называется $\dim_K L$

Обозначение. $|L : K|, \qquad (L : K), \qquad [L : K]$

Если $|L : K|$, то L — конечное расширение K (L конечно над K)
Иначе — бесконечное

Примеры.

1. $|\mathbb{C} : \mathbb{R}| = 2$
2. $|\mathbb{R}(x) : \mathbb{R}| = \infty$
3. $|K : K| = 1$
   Базис — $\{ 1 \}$ ($k \cdot 1$ — множество всех $k \in K$)
   Если $K \subset L, \ |L : K| = 1$, то $L = K$
4. $\mathbb{Q}(\sqrt{2})$ — наименьшее поле, содержащее $\mathbb{Q}$ и $\sqrt{2}$
   Такое поле существует, т. к. $\mathbb{Q} \subset \mathbb{R}$, $\sqrt{2} \in \mathbb{R}$, можно взять наименьшее подполе $\mathbb{R}$, которое содержит $\mathbb{Q}$ и $\sqrt{2}$
   Оно состоит из чисел вида $a + b\sqrt{2}$
   Проверим, что это поле:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2db) + (ad + bc)\sqrt{2}$$

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

$$|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$$

   Базис — $\left\{ 1, \sqrt{2} \right\}$
5. $\mathbb{Q}(\sqrt{2}, i)$ — наименьшее поле, содержащее $\mathbb{Q}, \sqrt{2}, i$
   Оно аналогично является подполем $\mathbb{C}$

   Утверждение 1. $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 4$

   Доказательство.

$$\mathbb{Q}(\sqrt{2}, i) = \left\{ a + bi \mid a, b \in \mathbb{Q}(\sqrt{2}) \right\}$$

   $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})| = 2$, базис — $\{ 1, i \}$
   Базис $\mathbb{Q}(\sqrt{2}, i)$ над $\mathbb{Q}$: $\left\{ 1 \cdot 1, 1 \cdot i, \sqrt{2} \cdot 1, \sqrt{2} \cdot i \right\}$ □

Теорема 2 (мультипликативность степени)**.** $K \subset M \subset L$ — поля с общими операциями
Тогда $|L : K| = |L : M| \cdot |M : K|$

Примечание. Если M конечно над K и L конечно над M, то L конечно над K и выполнено равенство
Иначе L бесконечно над K

Доказательство.

- Докажем, что если $e_1, \dots, e_r \in M$ ЛНЗ над K и $f_1, \dots, f_s \in L$ ЛНЗ над M, то $g_{ij} \coloneqq e_i f_j$ ЛНЗ над K:
  Пусть $a_{ij} \in K : \sum a_{ij} g_{ji} = 0$
  $$a_{11}e_1f_1 + a_{12}e_1f_2 + \dots + a_{21}e_2f_1 + a_{22}e_2f_2 + \dots\dots\dots\dots = 0$$
  Сгруппируем по элементам f:
  $$\Big(a_{11}e_1f_1 + a_{21}e_2f_1 + \dots\Big) + \Big(a_{12}e_1f_2 + a_{22}e_2f_2 + \dots\Big) + \dots\dots\dots\dots = 0$$
  $$\underbrace{(a_{11}e_1 + a_{21}e_2 + \dots)}_{\in M} f_1 + \underbrace{(a_{12}e_1 + a_{22}e_2 + \dots)}_{\in M} f_2 + \dots\dots\dots\dots = 0$$
  Пусть $b_j \coloneqq a_{1j}e_1 + a_{2j}e_2 + \dots + a_{rj}e_r$
  Тогда $b_j \in M, \quad b_1 f_1 + \dots b_s f_s = 0$
  $f_1, \dots f_s$ ЛНЗ над $M \implies b_1 = b_2 = \dots = b_s = 0$
  $$a_{1j}e_1 + \dots + a_{rj}e_r = b_j = 0$$
  $e_1, \dots, e_r$ ЛНЗ над $K \implies a_{ij} = 0 \quad \forall i, j$
- Конечный случай
  Пусть $e_1, \dots, e_r$ — базис M над K, $\quad f_1, \dots, f_s$ — базис L над M
  Докажем, что $g_{ij} \coloneqq e_i f_j$ — базис L над K:
  ЛНЗ уже доказана. Осталось доказать, что любой элемент порождается g_{ij}:
  Пусть $c \in L \quad \implies \exists\, b_i \in M : \quad c = b_1 f_1 + \dots + b_s f_s$
  $$b_j \in M, \quad e_i \text{ порожд. } M \text{ над } K \implies \forall j \quad \exists\, a_{ij} : \quad b_j = a_{1j}e_1 + \dots + a_{rj}e_r$$
  $$\implies c = \sum a_{ij} e I f_j = \sum a_{ij} g_{ij}$$
- Бесконечный случай
  Нужно доказать, что $\forall N \quad \exists\, N$ ЛНЗ элементов L над K (т. е. существует сколь угодно большая ЛНЗ система)
  Можно выбрать $e_1, \dots e_N$ ЛНЗ, или $f_1, \dots f_N$ ЛНЗ
  Тогда $e_i f_j$ ЛНЗ над K

$\square$

Следствие. L — конечное расширение над K, $\qquad K \subset M \subset L$
Тогда $|M : K|$ и $|L : M|$ — делители $|L : K|$

Следствие. L — конечное расширение K, $\qquad |L : K|$ — простое число
$$\implies \nexists\, M : \quad K \subset M \subset L, \quad M \neq K, \ M \neq L$$

Пример. Не существует поля $M : \quad \mathbb{R} \subset M \subset \mathbb{C}$, отличного от них
По основной теореме алгебры поле $\mathbb{C}$ большое — в нём есть корень любого многочлена
С другой стороны, оно маленькое — только что мы выяснили, что оно довольно близко к $\mathbb{R}$

Следствие. $K \subset M \subset L$
Тогда

- если $|M : K| = |L : K|$, то $M = L$
- если $|L : M| = |L : K|$, то $M = K$

Следствие. $K \subset M \subset L, \qquad L$ бесконечно над K
Тогда M бесконечно над K или L бесконечно над M

Пример. $\mathbb{R}(x)$ над $\mathbb{R}$ бесконечно
Значит, не существует $M: \quad \mathbb{R} \subset M \subset \mathbb{R}(x)$, и M кончено над $\mathbb{R}$, и $\mathbb{R}(x)$ конечно над M

Замечание. Нельзя построить "башню" из любого количества полей так, чтобы все шаги были конечны