Конспект по курсу

Теория колец и полей

Contributors:
Андрей Степанов

Лектор:
Ильинский Д.

МФТИ

Последнее обновление: 11 марта 2015 г.

Содержание

Курс состоит из 3 частей:

1. Теория делимости. Обобщение ОТА (основная теорема арифметики).
2. Расширения полей. Основная теорема алгебры. Конечные поля. Коды БЧХ.
3. Как из $\mathbb{Q}$ перейти в $\mathbb{R}$. $\mathbb{Q}_p$.

1 Базовые определения.

Определение 1.1. Кольцо - это тройка $(K, +, \cdot)$. Причем $(K, +)$ – абелева группа, и:

$$\forall a, b, c \in K : (a + b) \cdot c = a \cdot c + b \cdot c$$
$$c \cdot (a + b) = c \cdot a + c \cdot b$$

Определение 1.2. Говорят, что кольцо K обладает

1. Ассоциативностью, если выполнено $\forall a, b, c \in K : (ab)c = a(bc)$
2. Нейтральным элементом, если выполнено $\exists 1 \in K : \forall a \in K : a \cdot 1 = 1 \cdot a = a$
3. Коммутативностью, если выполнено $\forall a, b \in K : ab = ba$

Определение 1.3. Коммутативное кольцо – это такое кольцо, что для умножения выполнена коммутативность и (внезапно) ассоциативность и существование нейтрального элемента.

Замечание. В дальнейшем буквой K будем обозначать коммутативное кольцо (т.е. коммутативное с единицей и ассоциативностью).

Пример.

1. $\mathbb{Z}$ является коммутативным кольцом с единицей и ассоциативностью
2. $\{0\}$ – тривиальное кольцо
3. $2\mathbb{Z}$ – кольцо без единицы, но ассоциативное и коммутативное.
4. $\mathbb{R}^{n \times n}$ – ассоциативная кольцо с единицей, но не коммутативное

Пример. Более интересный пример: Множество матриц со сложением и операцией $[\cdot, \cdot]$: $[A, B] = AB - BA$. Ассоциативность не выполнена. Но выполнено:

1. $[[A, B], C] + [[B, C], A] + [[C, A], B] = 0$
2. $[A, B] = -[B, A]$

Определение 1.4. Пусть K – коммутативное кольцо. Тогда $a \neq 0$ называется делителем нуля, если: $\exists b \neq 0 : ab = 0$.

Определение 1.5. Коммутативное кольцо без делителей нуля называется областью целостности.

Утверждение 1.1. $a \cdot 0 = 0$

Доказательство. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Прибавляя обратный по сложению для $a \cdot 0$, получаем, что $a \cdot 0 = 0$ □

Определение 1.6. F – поле, если:

1. F – ассоциативное коммутативное кольцо с единицей
2. $1 \neq 0$
3. Любой элемент обратим относительно умножения.

Утверждение 1.2. *В поле нет делителей нуля.*

Доказательство. Пусть a – делитель нуля, т.е. $\exists b \neq 0 : ab = 0$. Но у a есть обратный элемент относительно умножения a^{-1}. Умножив слева на a^{-1}, придем к противоречию. □

Определение 1.7. Гауссовы числа ($\mathbb{Z}[i]$) – это комплексные числа с целой мнимой и действительной частью.

Утверждение 1.3. *Гауссовы числа – это область целостности*

Доказательство. Замкнутость относительно операций проверяется тривиальным образом. Коммутативность, дистрибутивность и ассоциативность следует из соответствующих свойств для $\mathbb{C}$. $0 + 0i$ – нейтральный элемент относительно сложения, а $1+0i$ – нейтральный элемент относительно умножения, проверяется тривиальным образом. А делителей нуля в гауссовых числах нет, поскольку что их нет в комплексных числах ($\mathbb{C}$ – это поле). □

Определение 1.8. В области целостности K говорят, что $a|b$ (a делит b), если $\exists c \neq 0 : ac = b$.

Утверждение 1.4. *Свойства делимости: для любых ненулевых a, b, c:*

1. $a|b, b|c \Leftarrow a|c$
2. *Если $b + c \neq 0$, то $a|b, a|c \Leftarrow a|(b + c)$*
3. $a|1 \Leftrightarrow a$ *– обратимый элемент*

Доказательство.

1. $a|b, b|c$ эквивалентно $\exists q_1, q_2 \neq 0 : aq_1 = b, bq_2 = c$. Следовательно, $aq_1q_2 = c$, причем q_1q_2 – не ноль.

2. $a|b, a|c$ эквивалентно $\exists q_1, q_2 \neq 0 : aq_1 = b, aq_2 = c$. Следовательно, $aq_1 + aq_2 = a(q_1 + q_2) = b + c$. Причем $q_1 + q_2$ – не ноль, в противном случае $b + c = 0$

3. $a|1$ эквивалентно $\exists b \neq 0 : ab = 1$ эквивалентно тому, что a – обратимый

□

Замечание. В случае, когда $a|1$, любой элемент поля делится на a:
$x = 1 \cdot x = a \cdot a^{-1} \cdot x$

Определение 1.9. K^* (множество обратимых элементов ассоциативного кольцо с единицей K) называют мультипликативной группой кольца.

Доказательство. Поскольку кольцо было ассоциативное и с единицей, то ассоциативность операции группы и существование единицы выполнены. Поскольку в K^* только обратимые элементы, то операция в группе также обратимы. Отсалось проверить замкнутость, то есть $\forall a, b \in K^* : ab \in K^*$ Это действительно так, обратный к ab – это $b^{-1}a^{-1}$ □

Определение 1.10. Будем называть два элемента a и b ассоциированными (обозначение: $a \sim b$), если $a = rb, r \in K^*$.

Упражнение. – это отношение эквивалентности.

Доказательство.

1. $a = rb \to r^{-1}a = b$

2. $a = rb, b = sc \to a = rsc$

3. $a = 1 \cdot a$

□

2 Делимость. Факториальные кольца. Евклидовы кольца

Замечание. План доказательства ОТА в $\mathbb{Z}$ был таков:

1. Докажем, что любое число раскладывается на произведение простых.

2. Докажем лемму Евклида.

3. Докажем единственность разложения на простые с помощью леммы Евклида.

Определение 2.1. Элемент $x \neq 0$ кольца K называется неприводимым или неразложимым, если:

1. $x \notin K^*$

2. $x = ab \Rightarrow \exists a^{-1} \vee \exists b^{-1}$

Определение 2.2. Элемент $0 \neq x \notin K^*$ кольца K называется простым, если: $x|ab \Rightarrow x|a \vee x|b$

Определение 2.3. Область целостности K называется факториальным кольцом, если:

1. $\forall x \neq 0 : \exists u \in K^*, p_1, \ldots, p_k$ – неприводимые : $x = up_1p_2 \ldots p_k$
2. Если существует два разложения, то они равны по подулю перестановки и ассоциируемости

Замечание. Чтобы доказать, что область целостности является факториальным, нужно выполнить 3 шага:

1. $\exists$ разложение
2. Доказываем, что каждый неразложимый элемент – простой
3. Доказываем единственность разложения

Утверждение 2.1. *Простой элемент неразложим.*

Доказательство. Пусть $x = ab$ – простой. Тогда $a|x, b|x$. Кроме того $x|ab$. Если $x|a$, то $x \approx a$. А значит, $b \in K^*$. Если же $x \approx b$, то проводим аналогичное доказательство. □

Замечание. Обратное верно не всегда.

Утверждение 2.2. *Если для кольца мы уже доказали п.1 и п.2, то единственность разложения будет из этого следовать.*

Доказательство. Мы хотим доказать единственность. Пусть $x = up_1 \ldots p_k, x = vq_1 \ldots q_l$, где $u, v \in K^*$. Возьмем какое-нибудь p_i, если $\exists q_j : q_j \approx p_i$, то их сократим, и так далее, пока можем. Получили, что какое-нибудь $p_i|wq_{j_1}q_{j_2} \ldots q_{j_s}$. Поскольку p_i простое, то получим, что $p_i|q_j$. Тогда $p_iu = q_j$, но така как q_j неразложим, получаем, что $u \in K^*$. А значит, $p_i \approx q_j$. Противоречие □

Определение 2.4. Область целостности K называется Евклидовым кольцом, если: $\exists ||x|| : K \setminus \{0\} \mapsto \mathbb{N}_0$ – норма, для которой выполнено:

1. $\forall a, b \neq 0 : ||ab|| \geq ||a||$
2. $\forall a, b \neq 0 : \exists q, r \in K : a = bq + r \Rightarrow (r = 0 \vee ||r|| < ||b||)$

Утверждение 2.3. *Свойство 1 лишнее.*

Доказательство. Положим

$$N(a) = \min_{b \neq 0, b \in K} ||ab||$$

Заметим, что свойство 1 выполнено. Докажем, что свойство 2 выполнено: пусть $0 \neq a, b \in K$. $N(b) = ||bc||$. Разделим a на bc с остатком. $a = q(bc) + r$. Если $r \neq 0$, то $N(r) \leq |r| < ||bc|| = N(b)$

□

Пример.

1. $\mathbb{Z}$
2. $K[x_1, \ldots, x_n]$, где K – поле, $||P|| = degP$
3. $\mathbb{Z}[i]$

Утверждение 2.4. *Целые Гауссовы числа и числа Эйзенштейна – это евклидовы кольца.*

Теорема 2.5. *Евклидовы кольца факториальны: (1) доказываем, что разложение существует (2) неразложимый элемент простой*

Утверждение 2.6. *Если K – евклидово кольцо, то выполнено свойство (1).*

Доказательство. Пусть это не вполнено. Расрим тай необрай элемент $x \neq 0$, что его норма минимальна среди всех элементов, для которых свойство (1) не выполнено. Пусть $x = x_1x_2$. Если для любого такого разложения $x_1|x_2 \in K^*$, тогда x неразложим. Проотиворечие. Пусть $x = x_1x_2$, т.ч. $x_1, x_2 \notin K^*$. $N(x) = N(x_1x_2) = N(x_2) \Leftrightarrow x_2 \in K^*$. Тогда $N(x_1) < N(x), N(x_2) < N(x)$. Раскладываем x_1, x_2 на простые. Противоречие. $\square$

Определение 2.5. $a, b \in K \setminus \{0\}$. $(a, b) = x : a|x, b|x, N(x)$ максимальна

<++>