Конспект по курсу

Теория колец и полей

Contributors:
Андрей Степанов

Лектор:
Ильинский Д.

МФТИ

Последнее обновление: 25 февраля 2015 г.

Содержание

nograhol@gmail.com
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:

1. $(K, +)$ – абелева группа
2. $\forall a, b, c \in K : (a+b) \cdot c = a \cdot c + b \cdot c$
3. $\forall a, b, c \in K : c \cdot (a+b) = c \cdot a + c \cdot b$

Определение 1.2. Свойство $\forall a, b, c : (ab)c = a(bc)$ называют ассоциативностью.

Определение 1.3. Свойство $\exists 1 : \forall a : a \cdot 1 = 1 \cdot a = a$ называют существованием нейтрального элемента

Определение 1.4. Свойство $\forall a, b : ab = ba$ называют коммутативностью.

Определение 1.5. Свойство $\forall a \neq 0 : \exists b : ab = ba = 1$ называют существованием обратного элемента.

Определение 1.6. Ассоциативное кольцо – это такое кольцо, что для умножения выполнена ассоциативность.

Определение 1.7. Кольцо с единицей – это такое кольцо, где есть нейтральный элемент относительно умножения.

Определение 1.8. Коммутативное кольцо – это такое кольцо, что для умножения выполнена коммутативность и (внезапно) ассоциативность и существование нейтрального элемента.

Замечание. Буквой K будем обозначать коммутативное кольцо (т.е. коммутативное с единицей и ассоциативностью).

Определение 1.9. Кольцо с обратными – это такое кольцо, что умножения обратимо.

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

Определение 1.11. Коммутативное кольцо без делителей нуля называется областью целостности.

Упражнение. $a \cdot 0 = 0$

Определение 1.12. F – поле, если:

1. F – ассоциативное коммутативное кольцо с единицей

2. $1 \neq 0$

3. Любой элемент обратим относительно сложения.

Утверждение 1.1. *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 1.13. Гауссовы числа ($\mathbb{Z}[i]$) – это комплексные числа с целой мнимой и действительной частью.

Утверждение 1.2. *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, потому что их нет в комплексных числах ($\mathbb{C}$ – это поле). □

Определение 1.14. Говорят, что $a|b$ (a делит b), если $\exists c : ac = b$.

Утверждение 1.3. *Свойства делимости:*

1. $a|b, b|c \Leftarrow a|c$

2. $a|b, a|c \Leftarrow a|(b + c)$

3. $a|1 \Leftrightarrow \exists b : ab = 1 \Leftrightarrow a$ – *обратимый элемент*

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

Определение 1.15. K^* (множество обратимых элементов К) – мультипликативная группа кольца.

Определение 1.16. Будем называть два элемента a и b ассоциированными, если $a = rb, r \in K^*$.

Упражнение. Ассоциированность – это отношение эквивалентности.

Замечание. План доказательства ОТА:

1. Докажем, что любое число раскладывается на произведение простых.
2. Докажем лемму Евклида.
3. Докажем единственность разложения на простые с помощью леммы Евклида.

Определение 1.17. 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 1.18. Элемент $0 \neq x \notin K^*$ кольца K называется простым, если: $x|ab \Rightarrow x|a \vee x|b$

2 Факториальные кольца.

Определение 2.1. 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. $\square$

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 $x = up_1 \dots p_k, x = vq_1 \dots q_l$, 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 $p_i|wq_{j_1}q_{j_2}\dots q_{j_s}$. Поскольку p_i простое, то получим, что $p_i|q_j$. Тогда $p_i u = q_j$, но така как q_j неразложим, получаем, что $u \in K^*$. А значит, $p_i \approx q_j$. Противоречие $\square$

Определение 2.2. 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 $N(r) \leq |r| < ||bc|| = N(b)$

$\square$

Пример.

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