Лекция 14.

Гайфуллин Сергей Александрович

МГУ

2 ноября, 2021

Определение

Если $a, b \in R$, $a \neq 0$, $b \neq 0$ и $ab = 0$, то a называется левым делителем нуля, а b – правым делителем нуля.
Совокупность левых и правых делителей нуля называется множеством делителей нуля.

Пример

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Лемма

В кольце с единицей делитель нуля не может быть обратим.

Доказательство. Пусть $ab = 0$ и пусть, например, a – обратимый элемент. Тогда $0 = a^{-1}0 = a^{-1}ab = b$.

Определение

Элемент $x \neq 0 \in R$ называется нильпотентом (нильпотентным элементом), если существует $n \in \mathbb{N}$ такое, что $x^n = 0$.

Пример

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Лемма

Нильпотентный элемент является делителем нуля.

Доказательство. Если n наименьшее со свойством $x^n = 0$, то $x \cdot x^{n-1} = 0$ – делители нуля.

Кольцо вычетов

Пусть m – натуральное число. Рассмотрим множество остатков при делении целых чисел на m. Это множество $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$. Определим сложение и умножение на $\mathbb{Z}_m$ следующим образом. Чтобы сложить два элемента из $\mathbb{Z}_m$ мы складываем их как целые числа, а затем берем остаток. Чтобы умножить два элемента из $\mathbb{Z}_m$ мы умножаем их как целые числа, а затем берем остаток. Получится ассоциативное коммутативное кольцо с единицей.

Теорема

Кольцо $\mathbb{Z}_m$ является полем тогда и только тогда, когда m простое.

Доказательство. Если $m = kl$, то $\overline{k} \cdot \overline{l} = \overline{0}$ – делители нуля, то есть не обратимы.

Пусть m простое и $\overline{x} \neq 0$. Рассмотрим $\overline{x0}, \overline{x1}, \overline{x2}, \ldots, \overline{x(m-1)}$
Они все различны. Действительно, если $\overline{xi} = \overline{xj}$, то $x(i-j)$ делится на m, что не возможно. Значит, среди этих элементов есть $\overline{1}$, то есть $\overline{x}$ обратим.

Задача

При каких n в кольце $\mathbb{Z}_n$ есть нильпотенты?

Определение

Пусть F – поле. Характеристика $\operatorname{char} F$ поля F равна наименьшему натуральному k такому, что сумма k единиц равна нулю, если такое натуральное k существует. Если же такого натурального k не существует, то говорят, что характеристика F равна нулю.

Примеры

$\operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{Q} = 0$;

$\operatorname{char} \mathbb{Z}_p = p$.

Теорема

Характеристика поля либо равна нулю, либо является простым числом.

Доказательство. Допустим, что $\mathrm{char}\, F = mn$. Тогда

$$\underbrace{1+1+\ldots+1}_{mn} = \underbrace{(1+1+\ldots+1)}_{m}\underbrace{(1+1+\ldots+1)}_{n}$$

Так как в поле нет делителей нуля, один из множителей равен нулю.

Лемма

Пусть F – поле характеристики p. Если сложить элемент $a \in F$ с собой pk раз, то получится ноль.

Доказательство. $pka = (1 + 1 + \ldots + 1)ka = 0ka = 0$.

Теорема

Пусть F – поле характеристики p. Тогда для $a, b \in F$ выполнено $(a + b)^p = a^p + b^p$.

Доказательство. По формуле бинома Ньютона

$$(a + b)^p = \sum_{i=0}^{p} C_p^i a^i b^{p-i} = a^p + \sum_{i=1}^{p-1} C_p^i a^i b^{p-i} + b^p.$$

При этом $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p при $i \in \{1, 2, \ldots, p-1\}$. Таким образом, в поле F все слагаемые, кроме крайних равны нулю. То есть $(a + b)^p = a^p + b^p$.

Следствие

Пусть F – поле характеристики p. Тогда для $a_1, \ldots, a_m \in F$ выполнено $(a_1 + \ldots + a_m)^p = a_1^p + \ldots + a_m^p$.

Теорема (малая теорема Ферма)

В кольце $\mathbb{Z}_p$ выполнено $\overline{n}^p = \overline{n}$.

Доказательство.

$$\overline{n}^p = (\overline{1} + \ldots + \overline{1})^p = (\overline{1} + \ldots + \overline{1}) = \overline{n}.$$

Определение

Алгебраическая система – это множество с несколькими операциями (возможно различной арности), удовлетворяющих некоторым аксиомам.

Определение

Пусть есть две одинаковые алгебраические системы A и B (то есть с одинаковым количеством операций одинаковой арности).Гомоморфизм из A в B – это отображение множеств, переводящее операции в операции. То есть если α – m-арная операция на A, β – m-арная операция на B, и $\varphi\colon A \to B$ – гомоморфизм, то

$$\varphi(\alpha(x_1, \ldots, x_m)) = \beta(\varphi(x_1), \ldots, \varphi(x_m)).$$

Примеры гомоморфизмов

1) $\varphi\colon (\mathbb{Z}, +) \to (\mathbb{Z}_n, +), \varphi(k) = \overline{k}$ – гомоморфизм групп.
2) $\varphi\colon ((\mathrm{GL}_n(\mathbb{R}), \cdot) \to (\mathbb{R}^\times, \cdot), \varphi(A) = \det A$ – гомоморфизм групп.
3) $\varphi\colon (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot), \varphi(k) = \overline{k}$ – гомоморфизм колец.
4) $\varphi\colon (\mathbb{Z}, +, \cdot) \to (\mathbb{Q}, +, \cdot), \varphi(k) = k$ – гомоморфизм колец.

Определение

Изоморфизм алгебраических систем – это биективный гомоморфизм.
Изоморфные системы являются одинаковыми с точки зрения алгебры.

Если одна из изоморфных систем удовлетворяет некоторой алгебраической аксиоме, то и другая тоже.

Пример

$\varphi\colon (\mathbb{Z}_2, +) \to (\{1, -1\}, \cdot)$, $\varphi(0) = 1$, $\varphi(1) = -1$ – изоморфизм групп.

Комплексные числа

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Каждое расширение мотивировано тем, что хотелось бы решать новые задачи.

- Переход от натуральных чисел к целым мотивирован тем, что хочется всегда уметь вычитать числа.
- Переход от целых чисел к рациональным мотивирован тем, что хочется всегда уметь делить на число отличное от нуля.
- Переход от рациональных чисел к вещественным мотивирован тем, что хочется всегда уметь брать предел последовательности. Также связано с невозможностью извлекать корни из положительных чисел.
- Переход от вещественных чисел к комплексным мотивирован тем, что хочется всегда уметь решать алгебраические уравнения.

Определение

Комплексные числа – это множество пар вещественных чисел $(a, b) \in \mathbb{R}^2$ с операциями

- сложение $(a, b) + (c, d) = (a + c, b + d)$.
- умножение $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Множество комплексных чисел обозначается $\mathbb{C}$.

Теорема

Комплексные числа образуют поле.

Лемма

Алгебраическая структура комплексных чисел изоморфна алгебраической структуре $\mathbb{M}$ матриц вида $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}; a, b \in \mathbb{R}$ с операциями сложения и умножения.

Доказательство. Определим отображение $\varphi\colon \mathbb{C} \to \mathbb{M}$, $\varphi(a,b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Очевидно, что φ – биекция. Кроме того

$$\varphi((a,b)+(c,d)) = \varphi(a+c, b+d) =$$
$$= \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \varphi(a,b)+\varphi(c,d);$$

$$\varphi((a,b)\cdot(c,d)) = (ac-bd, ad+bc) =$$
$$= \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \varphi(a,b)\cdot\varphi(c,d).$$

Таким образом, φ – гомоморизм. Однако, очевидно, что φ – биекция. То есть φ – изоморфизм.

Доказательство теоремы.

У нас есть множество $\mathbb{C}$ с двумя операциями: сложением и умножением. Надо проверить все аксиомы.

1-4) по сложению $\mathbb{C}$ – абелева группа. Очевидно. При этом $0 = (0, 0)$ и $-(a, b) = (-a, -b)$.

5-6) дистрибутивности. Следуют из $\mathbb{C} \cong \mathbb{M}$ и того, что умножение матриц дистрибутивно.

7) ассоциативность умножения. Следует из $\mathbb{C} \cong \mathbb{M}$ и того, что умножение матриц ассоциативно.

8) Существование единицы. $1 = (1, 0) \leftrightarrow E$.

9) Коммутативность умножения. Следует из формулы $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

10) Любой ненулевой элемент обратим. Следует из $\mathbb{C} \cong \mathbb{M}$ и того, что

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Вложение вещественных чисел

Рассмотрим множество L чисел вида $(a, 0)$. И рассмотрим отображение

$$\psi : \mathbb{R} \to L, \qquad a \mapsto (a, 0).$$

Легко видеть, что ψ – изоморфизм. Таким образом $(\mathbb{R}, +, \cdot) \cong (L, +, \cdot) \subset (\mathbb{C}, +, \cdot)$ – подполе. В дальнейшем не будем различать $\mathbb{R}$ и L.

Заметим, что $(a, 0) \cdot (c, d) = (ac, ad)$. Получаем, что на $\mathbb{C}$ есть операции сложения и умножения на $\mathbb{R}$. С этими операциями $\mathbb{C}$ – векторное пространство над $\mathbb{R}$, изоморфное $\mathbb{R}^2$. Его базис – это $1 = (1, 0)$ и $i = (0, 1)$.

Заметим, что $i^2 = -1$. Этот элемент называется мнимой единицей.

Получаем $(a, b) = a + bi$ – алгебраическая форма комплексного числа.

Новый взгляд на операции

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

$$(a+bi)\cdot(c+di) = ac+(ad+bc)i+bdi^2 = (ac-bd)+(ad+bc)i.$$