Алгебра. Неофициальный конспект

Лектор: Николай Александрович Вавилов

Конспектировал Леонид Данилевич

Пока только I семестр, осень 2022 г.

Оглавление

Глава 1

Введение в общую алгебру

Лекция I
1 сентября 2022 г.

1.1 Внутренние бинарные алгебраические операции

Рассмотрим произвольное множество $X \neq \varnothing$.

Определение 1.1.1 ((Внутренняя) (бинарная) алгебраическая операция на X)**.** Отображение

$$f : X \times X \to X$$

Часто операции обозначают в *инфиксной* записи, например

$$+ : X \times X \to X; \quad (u, v) \mapsto u + v$$

Запись выше называется *аддитивной*, запись $u \cdot v$ называется *мультипликативной*.

1.1.1 Частые свойства операций

Операции могут обладать некоторыми свойствами:

- *Коммутативность* операции $*$: $\forall x, y \in X : x * y = y * x$. Свойство, к которому все привыкли, но которого часто может не наблюдаться. Так, при отсутствии коммутативности

  $$(f \cdot g)' = f' \cdot g + f \cdot g', \text{ не } f' \cdot g + g' \cdot f$$

  Или же, что невозможно угадать:

  $$\left(\frac{1}{f}\right)' = -\frac{1}{f} \cdot f' \cdot \frac{1}{f}$$

  Предположив, что все операции обладают хорошими свойствами, кроме $\cdot$:

  $$(a + b)^2 = (a + b) \cdot (a + b) = a^2 + ab + ba + b^2$$
  $$(a + b) \cdot (a - b) = a^2 + ba - ab - b^2$$

- *Ассоциативность* операции *: $\forall x, y, z \in X : (x * y) * z = x * (y * z)$. Ассоциативность намного фундаментальнее коммутативности, от неё отказаться непросто. Помнить про её отсутствие намного сложнее, чем про отсутствие коммутативности.

  Практически все структуры, которые мы будем рассматривать, будут ассоциативны.

  Ассоциативность и коммутативность абсолютно независимы, каждая может как выполняться, так и нет, вне зависимости от другой.

- *Дистрибутивность* $*$ относительно $+$: $x * (y + z) = (x * y) + (x * z)$. Дистрибутивность выполняется для двух операций, здесь g дистрибутивна относительно f. Так, для целых чисел $a \cdot (b + c) = a \cdot b + a \cdot c$.

  Самодистрибутивность: $x * (y * z) = (x * y) * (x * z)$. Очень необычное свойство, с которым неожиданно связаны парадоксальные результаты. Так, есть вполне конкретно определённая конечная группа (в которой выполняется самодистрибутивность), для которой истинность некоторого факта (о порядке некоего элемента) зависит от существования больших кардиналов. Всё, что могут просчитать компьютеры, не превосходит 16, но в предположении существования больших кардиналов эта величина может быть сколь угодно большой при больших конечных группах этого типа.

На лекции приводилось определение композиции внутренних функций, действующих из множества в него само: $f \in X^X$. Мне захотелось, поэтому я привёл определение и доказательство более общей композиции, которая, впрочем, от этого перестала быть внутренней операцией.

Определение 1.1.2 (Композиция)**.** Отображение, результат которого — последовательное применение двух. Формально, для функций $f : B \to C$ и $g : A \to B$ композиция определяется, как $f \circ g : A \to C; \quad (f \circ g)(x) = f(g(x))$.

Композиция — внешняя операция (внутренняя для $A = B = C$): $\quad \circ : C^B \times B^A \to C^A$.

Теорема 1.1.1. Композиция ассоциативна: $(f \circ g) \circ h = f \circ (g \circ h)$.

Доказательство. Отображения совпадают, если совпадают их области определения, области значений, а также значения во всех точках области определения.

Пусть $f : E \to F; \quad g : C \to D; \quad h : A \to B$.

$\exists f \circ g \iff D = E; \quad \exists (f \circ g) \circ h \iff B = C$. Аналогично, $\exists f \circ (g \circ h) \iff B = C \wedge D = E$.

Таким образом, левая часть существует, если и только если существует правая — ассоциативность *строгая*.

Кроме того, $(f \circ g) \circ h : A \to F$ и $f \circ (g \circ h) : A \to F$.

Наконец, удостоверимся, что совпадают значения во всех точках области определения A.

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$$

Все четыре знака равенства используют только определение композиции. □

Замечание. В формуле выше, как и во всех правильно написанных формулах, от равенства к равенству не меняется порядок переменных — в данном случае это f, g, h, x.

Теорема 1.1.2. Из ассоциативности следует обобщённая ассоциативность. А именно, в формуле $x_1 \circ x_2 \circ \cdots \circ x_n$ можно как угодно (корректно) расставить скобки, при ассоциативной операции $\circ$ результат не изменится.

Доказательство.

Доказательство по индукции.

<u>База:</u> $n \leq 2$ — всего один вариант расстановки скобок. $n = 3$ — определение ассоциативности.

<u>Переход:</u> докажем, что при любой расстановке скобок выражение можно привести к левонормированной форме: форме

$$(((x_1 \circ x_2) \circ x_3) \dots) \circ x_n$$

Рассмотрим последнюю переменную x_n. Возможны два случая:

- $\circ$, принимающий в качестве правого аргумента x_n, в качестве левого аргумента принимает некое выражение от $x_1, \dots, x_{n-1}$. Тогда, применив предположение индукции, мы можем считать, что левый аргумент — левонормированная форма $((x_1 \circ x_2) \dots) \circ x_{n-1}$.

  В таком случае всё выражение тоже оказалось левонормированным.

- $\circ$, принимающий в качестве правого аргумента x_n, в качестве левого аргумента принимает выражение от переменных $x_i, \dots, x_{n-1}$ $(i > 1)$. Так как $i > 1$, то мы можем применить индукционное предположение к переменным $x_i, \dots, x_n$. Теперь эта часть формулы левонормированная: $(\dots) \circ (((x_i \circ x_{i+1}) \dots) \circ x_n)$. Воспользуемся ассоциативностью, получим $((\dots) \circ (((x_i \circ x_{i+1}) \dots)) \circ x_n$. Таким образом, задача свелась к предыдущему случаю. $\square$

Лекция II

7 сентября 2022 г.

1.1.2 Примеры внутренних бинарных алгебраических операций

- Над числами
- Сумма многочленов
- Произведение многочленов
- Композиция многочленов. $(x+1) \circ x^2 = x^2 + 1$, в то время как $x^2 \circ (x+1) = (x+1)^2$, откуда видно, что композиция некоммутативна.
- *Кронекеровская сумма*. Определим её для простоты над нормированными многочленами f, g (старший коэффициент 1). $f \boxplus g$ — нормированный многочлен, корни которого $\alpha_i + \beta_j$ для всех α_i — корней f, β_j — корней g.
- *Кронекеровское произведение*. Определим его для простоты над нормированными многочленами f, g (старший коэффициент 1). $f \boxtimes g$ — нормированный многочлен, корни которого $\alpha_i \cdot \beta_j$ для всех α_i — корней f, β_j — корней g.
- Над векторами. Будем обозначать вектор $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ или $\begin{pmatrix} x_1, & \cdots & x_n \end{pmatrix}$. Обе записи валидны, но отличаются левым и правым действием. Тогда $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$.
- Скалярное умножение векторов (покомпонентное) $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \cdot y_1 \\ \vdots \\ x_n \cdot y_n \end{pmatrix}$.
- Комплексное умножение векторов $\begin{pmatrix} a, b \end{pmatrix} \cdot \begin{pmatrix} c, d \end{pmatrix} = \begin{pmatrix} ac - bd, ad + bc \end{pmatrix}$.
- Векторное умножение в трёхмерном пространстве $\begin{pmatrix} x_1, x_2, x_3 \end{pmatrix} \times \begin{pmatrix} y_1, y_2, y_3 \end{pmatrix} = \begin{pmatrix} x_2 y_3 - x_3 y_2 \\ -x_1 y_3 + x_3 y_1 \\ x_1 y_2 - x_2 y_1 \end{pmatrix}$.
- Операции над матрицами. Рассмотрим матрицы 2×2 с коэффициентами из R, где $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \dots\}$. Обозначается $M(2, R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in R \right\}$.

  Сложение: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$.
- Умножение матриц по Шуру (по Адамару) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} ? \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a \cdot e & b \cdot f \\ c \cdot g & d \cdot h \end{pmatrix}$.
- Настоящее умножение матриц: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a \cdot e + b \cdot g & a \cdot f + b \cdot h \\ c \cdot e + d \cdot g & c \cdot f + d \cdot h \end{pmatrix}$
- Булевы операции (на булеане) — пересечение, объединение, т. д., т. п..

1.2 Простейшие структуры. Моноиды

Моноид состоит из множества $X \neq \varnothing$ и операции $* : X \times X \to X; \quad (x, y) \mapsto x * y$. Операцию можно ввести кучей ($|X|^{|X|^2}$) способов, но мы будем рассматривать операцию, удовлетворяющую каким-то тождествам.

1.2.1 Полугруппа (semi-group)

Операция $*$ ассоциативна.

1.2.2 Определение моноида

- M1: Полугруппа, т. е. операция $*$ ассоциативна.
- M2: Существует нейтральный элемент $e \in X : \forall x \in X : e * x = x * e = x$. В аддитивной нотации обозначается 0, в мультипликативной — 1.

  Замечание. Если существует и левый, и правый нейтральные элементы, то они совпадают: $e = e * (x * e') = (e * x) * e' = e'$.

Примеры моноидов

- $(\mathbb{N}, \cdot, 1)$.
- $(\mathbb{N}_0, +, 0)$.
- $X = 2^Y \quad (X, \cup, \varnothing) \quad (X, \cap, Y)$.
- Симметрический моноид: $(X^X, \circ, id_X)$ – множество всех преобразований множества X в себя.

  Я просто запишу эти крестики здесь: $X^X \times X^X \to X^X, (f, g) \mapsto g \circ f$

Определения

Определение 1.2.1 ($z \in X$ регулярен)**.** $\begin{cases} \forall x, y \in X((x * z) = (y * z)) \Rightarrow x = y & \text{— регулярен справа} \\ \forall x, y \in X((z * x) = (z * y)) \Rightarrow x = y & \text{— регулярен слева} \end{cases}$

Определение 1.2.2 (Обратимый слева / справа элемент)**.** Элемент $z \in X$ называется обратимым слева $\iff \exists u \in X : u * z = e$. Аналогично, z обратим справа $\iff \exists v \in X : z * v = e$.

Лемма 1.2.1. *z обратим слева / справа $\Rightarrow$ z регулярен слева / справа.*

Доказательство. $\exists u \in X : u * z = e$. Тогда если $z * x = z * y$, то — умножив на u слева — $(u * z) * x = (u * z) * y$ и $x = y$. □

Определение 1.2.3 (Обратимый элемент)**.** Элемент $z \in X$ называется обратимым $\iff \exists u \in X : u * z = z * u = e$. u — обратный (противоположный, симметричный, ...) к z.

Лемма 1.2.2. *В моноиде z — обратим слева и справа $\iff$ z обратим.*

Доказательство. Рассмотрим обратные к z слева u_L и справа u_R. Тогда произведение $u_L = u_L * (z * u_R) = (u_L * z) * u_R = u_R$. □

Пусть $X^* = \left\{ z \in X \middle| \ \exists z^{-1} \in X : z^{-1} * z = e = z * z^{-1} \right\}$ — множество обратимых элементов моноида $(X, *)$.

- $e \in X^*$.
- $x, y \in X^* \Rightarrow (x * y)^{-1} = y^{-1} * x^{-1}$.

  Определение 1.2.4 (Коммутирующие элементы)**.** $x, y \in X$, такие, что $x * y = y * x$.
- $x \in X^* \Rightarrow x^{-1} \in X^*$

Следствие. X^* — группа обратимых элементов моноида X.

1.3 Группы

Пусть G – множество; $* : G \times G \to G$.

Определение 1.3.1 (Группа)**.** $(G, *)$ – группа:

- $*$ ассоциативна
- $\exists e \in G : (\forall x \in G :)\ e * x = x * e = x$.
- Все элементы обратимы: $\forall g \in G : \exists g^{-1} \in G : g * g^{-1} = g^{-1} * g = e$.

Группа G называется коммутативной (или абелевой), если $*$ коммутативна. В абелевых группах принята аддитивная запись: $(*, 1, x^{-1}) \to (+, 0, -x)$

В сигнатуру группы входят 4 вещи: $(G, *, e, inv)$, где $inv : G \to G, x \mapsto x^{-1}$.

Лекция III
8 сентября 2022 г.

Лемма 1.3.1. *В любой группе G есть деление:* $\begin{cases} \forall h, g \in G : \exists!\ x :\ h * x = g \text{ — левое деление} \\ \forall h, g \in G : \exists!\ y :\ x * y = g \text{ — правое деление} \end{cases}$

Доказательство. $x = h^{-1}g$ в случае левого деления; в случае правого деления $y = g^{-1}h$ □

Замечание. Для большинства свойств группы достаточно более слабого, нежели $g * g^{-1} = e$, а именно, часто достаточно $gg^{-1}g = g$.

1.3.1 Примеры групп

Абелева (коммутативная) группа — на самом деле не группа (формально группа, но морально — совсем не так).

- Какая-то группа симметрий, преобразований на себя. Например, повороты кубика Рубика. Нейтральный элемент — не делать поворотов.
- Пусть $(R, +, \cdot, 0)$ — кольцо. Аддитивная группа кольца, группа по сложению $R^+ = (R, +, 0)$. Например, для кольца $\mathbb{Z} : \mathbb{Z}^+$ — бесконечная циклическая группа. Аналогично получаются $\mathbb{R}^+, \mathbb{Q}^+$, однако стоит упоминания, что $\mathbb{Q}, \mathbb{R}$ — это уже поля.

  Замечание. Операции деления и вычитания рассматриваются не как самостоятельные, а как производные операции, поэтому не записываются в сигнатуре. Так, $x - y = x + (-y)$.
- Пусть R — ассоциативное кольцо с единицей. Тогда его мультипликативная группа $R^* = \{x \in R |\ \exists y \in R : xy = 1 = yx\}$. $Z^* = \{-1, 1\}$. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$; $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
- Группа углов $\mathbb{T} = \left\{ z \in \mathbb{C} \middle| |z| = 1 \right\} \cong \mathbb{R}/2\pi\mathbb{Z}$.

  Определение 1.3.2 (Подгруппа)**.** $H \neq \varnothing; H \leq G : H$ называется подгруппой в G, если

  $\forall x, y \in H : \left(xy^{-1} \in H \overset{\text{здесь равносильно}}{\iff} \begin{cases} xy \in H \\ y^{-1} \in H \end{cases} \right)$. Пишут $(H \leq G) \iff (H$ — подгруппа $G)$.
- $\mathbb{R}_{>0} < \mathbb{R}^*$

  $\mathbb{Q}_{>0} < \mathbb{Q}^*$
- Группа корней n-й степени ($n \in \mathbb{N}$) из единицы $M_n = \{z \in \mathbb{C}^* | z^n = 1\} < \mathbb{T}$. $|M_n| = n$.

Определение 1.3.3 (Степень в моноиде)**.** Пусть X — моноид с нейтральным элементом e. $x \in X; \quad n \in \mathbb{N}_0$. Тогда n-я степень x: $x^n = \begin{cases} e, & n = 0 \\ x^{n-1} * x, & n \geq 1 \end{cases}$.

Замечание. Почему-то лектор настаивает на определении $x^n = \begin{cases} e, & n = 0 \\ \left(x^{\frac{n}{2}}\right)^2, & 2 \mid n \\ x^{n-1} * x, & 2 \nmid n \end{cases}$

Однако я бы предпочёл это держать свойством.

Определение 1.3.4 (Степень в группе)**.** Пусть X^* — мультипликативная группа моноида X с нейтральным элементом e. $x \in X; \quad n \in \mathbb{Z}$. Тогда n-я степень x: $x^n = \begin{cases} x^n, & n \geq 0 \\ \left(x^{-1}\right)^{-n}, & n < 0 \end{cases}$.

- «Настоящая» (некоммутативная) группа: $S_X = \text{Bij}(X, X)$ — симметрическая группа множества X. Эквивалентно множеству обратимых элементов симметрического моноида X^X.

  Замечание. Частный случай — $X = \underline{n} = \{1, 2, \dots n\}$. Симметрическая группа $S_n \overset{def}{=} S_{\underline{n}}$. Как известно, $|S_n| = n!$.

  Записывается S_3 следующим образом:

  $$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

  Перемножение: $(p \cdot q)_i = p_{q_i}$. Перемножение, как композиция, считается справа налево. Некоммутативность перемножения:

  $$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

  $$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

- Группа обратимых линейных операторов. $M(n, R)$. В кольце матриц есть нейтральный элемент. $e = \begin{pmatrix}1&0\\0&1\end{pmatrix}$ в случае $M(2, R)$. $GL(n, R) = M(n, R)^*$ — полная линейная группа степени n над R. Например, для поля K : $GL(2, K) = \left\{ \begin{pmatrix}a&b\\c&d\end{pmatrix} \middle| a, b, c, d \in K \wedge ad - bc \neq 0 \right\}$. В самом деле, $\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$.

- Как устроены группы маленьких (конечных) порядков?

  1. $|G| = 1$. Здесь $G = \{1\}$.

     Определение 1.3.5. Для $n \in \mathbb{N}$: $\exists\ C_n \cong M_n$ — группа вращений правильного n-угольника. C от слова cyclic — циклическая группа.

  2. $|G| \in \mathbb{P}$. Существует только циклическая группа такого размера! $C_{|G|}$

  3. $|G| = 4$. Такого размера есть группы $C_4, C_2 \times C_2$.

     Определение 1.3.6 (Прямое произведение групп)**.** $H \times G = \{(h, g) | h \in H, g \in G\}$. Умножение определяется $(h_1, g_1) \cdot (h_2, g_2) = (h_1 h_2, g_1 g_2)$.

  4. $|G| = 6$. Группы такого размера бывают двух типов: $C_6 = C_2 \times C_3; S_3 \cong D_3$.

     Определение 1.3.7 (Диэдральная группа)**.** D_n — группа симметрий (включающих отражение) правильного n-угольника. $|D_n| = 2n$.

Лекция IV

14 сентября 2022 г.

$D_2 \cong V; D_3 \cong S_6$. V — группа симметрий квадрата, получаемых отражением относительно диагоналей.

5. $|G| = 8 \Rightarrow \ldots$. Для составных n задача определения по порядку группы её возможные типы — сложная.

   Существует 5 групп порядка 8:

   - C_8 — циклическая группа.
   - $C_2 \times C_4$
   - $C_2 \times C_2 \times C_2$
   - D_4 — диэдральная группа. Не является абелевой!
   - $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ — группа кватернионных единиц. (**Q**uaternion). Не является абелевой группой!

     Кватернионы, натянутые на эти 4 единицы определяют четырёхмерное пространство; ещё Гамильтон за 60 лет до появления теории относительности писал, что 1 отвечает за временную одномерную ось, а i, j, k — векторы трёхмерного пространства.

     Кватернионы $\mathbb{H} \stackrel{def}{=} \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$, где i, j, k — мнимые единицы, удовлетворяющие тождествам $i^2 = j^2 = k^2 = ijk = -1$ и $xy = -yx$. Ассоциативность проверяется грубой силой с большими затратами, или же специальными матрицами $M(2, \mathbb{C})$ — матрицами Паули.

Определение 1.3.8 (Порядок элемента g в группе G)**.** Наименьшее натуральное $n \in \mathbb{N}$: $g^n = 1_G$.

Замечание. В различности данных пяти групп можно убедиться, заметив различие мультимножеств порядков их элементов.

Описание групп больши́х составных порядков — сложная задача.

Задача 2000 — описать все группы порядка ≤ 2000 до наступления нового века. Задача практически была решена, не удалось лишь перечислить $5 \cdot 10^{10}$ групп порядка 1024, составляющие больше 99% всех групп порядка менее 2000.

1.3.2 Гомоморфизмы

Рассмотрим множество X с операцией $*$ и множество Y с операцией $\circ$.

Определение 1.3.9 (Гомоморфизм)**.** Отображение $f : X \to Y$, такое, что

$$\forall x, y \in X : f(x) \circ f(y) = f(x * y)$$

Примеры гомоморфизмов

- Экспонента. $\exp : \mathbb{R}^+ \to \mathbb{R}_{>0}; \quad x \mapsto e^x$.

  Замечание. $\mathbb{R}^*_{>0} \equiv \mathbb{R}_{>0}$

- Логарифм $\log : \mathbb{R}_{>0} \to \mathbb{R}^+; \quad x \mapsto \log(x)$.

  $\log(\exp(x)) = x \quad \exp(\log(x)) = x$

  Определение 1.3.10 (Изоморфизм)**.** Обратимый гомоморфизм (обратный к которому — тоже гомоморфизм). Часто это то же самое, что и биективный гомоморфизм, но не всегда. Так, если к гомоморфизму есть требование непрерывности, то обратный гомоморфизм тоже обязан не только существовать, но и быть непрерывным.

  Определение 1.3.11 (Изоморфные множества $X \cong Y$)**.** Между ними существует изоморфизм.

Замечание. Важным свойством $\mathbb{R}$ является $\mathbb{R}_{>0} \cong \mathbb{R}^+$, что не выполнятся ни для $\mathbb{Q}$, ни для $\mathbb{A}, \dots$

- Абсолютная величина. $|\cdot| : \mathbb{R} \to \mathbb{R}_{\geq 0}; \quad x \mapsto |x|$.

  Мультипликативный гомоморфизм по умножению.

- Знак. $\operatorname{sign} : \mathbb{R}^* \to \{\pm 1\}; \quad \operatorname{sign}(x) = \begin{cases} +1, & x > 0 \\ -1, & x < 0 \end{cases}; \quad \operatorname{sign}(x \cdot y) = \operatorname{sign}(x) \cdot \operatorname{sign}(y)$

  Замечание. $(x = \operatorname{sign}(x) \cdot |x|) \Rightarrow \mathbb{R}^* \cong (\mathbb{R}_{>0} \times \{\pm 1\})$

- $\mathbb{C}^* \cong \mathbb{R}^*_{>0} \times \mathbb{T}$ — модуль и аргумент. В школе этот факт гомоморфизма называется теоремой сложения для синусов и косинусов.

  Замечание. Также наблюдается гомоморфизм

  $\mathbb{T} \to M(2, \mathbb{R}); \quad x \mapsto \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix}$.

  В матрицах тригонометрические формулы:

  $\begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix} \cdot \begin{pmatrix} \cos(y) & \sin(y) \\ -\sin(y) & \cos(y) \end{pmatrix} = \begin{pmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{pmatrix}$ — ф-ла А. де Муавра.

  Факт (Коан). $\mathbb{C}^* \cong \mathbb{T}$. Просто факт, просто так.

- Знак перестановки. $\operatorname{sgn} : S_n \to \{\pm 1\}$. Можно определить его, как количество инверсий — пар позиций $i < j : p_i > p_j$.

  Так $\operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = -1, \quad \operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = +1$. Знак перестановки — мультипликативный гомоморфизм.

- Определитель (детерминант) — $\det : M(n, \mathbb{R}) \to \mathbb{R}$.

  Если ввести определитель только от обратимых матриц: $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$, то тоже получится мультипликативный гомоморфизм.

- Аддитивный гомоморфизм взятия производной: $(f + g)' = f' + g'$.

Определение 1.3.12 (Гомоморфизм моноидов)**.** $f : X \to Y$ — гомоморфизм моноидов, если

$$\forall x, y \in X : f(xy) = f(x)f(y) \text{ и } f(1_X) = 1_Y$$

Определение 1.3.13 (Гомоморфизм групп)**.** $f : H \to G$ — гомоморфизм групп, если

$$\forall x, y \in X : f(xy) = f(x)f(y)$$

Замечание. Сигнатура моноида: $(X, \cdot, 1)$. Сигнатура группы: $(G, \cdot, 1, inv)$. По-хорошему, в определение гомоморфизма групп надо включить сохранение единицы и обратного, но

Лемма 1.3.2. *Если $f : H \to G$ — мультипликативный гомоморфизм для групп H, G, то автоматически $f(1_H) = 1_G$ и $f(x^{-1}) = f(x)^{-1}$.*

Доказательство. $1_H \cdot 1_H = 1_H \Rightarrow f(1_H) = f(1_H \cdot 1_H) = f(1_H)^2$. Так как G — группа, то можно сокращать. Поэтому $f(1_H) = 1_G$. Тогда сохраняется и обратный: $1_G = f(1_H) = f(xx^{-1}) = f(x)f(x^{-1})$, откуда в силу единственности обратного $f(x^{-1}) = f(x)^{-1}$. □

Замечание. Для моноидов лемма неверна, так как, например, существует отображение $\{1\} \to M$, где $1 \mapsto x$, x — произвольный идемпотент в моноиде M. Оно не является гомоморфизмом, хотя для него выполняется «правило умножения».

1.4 Дистрибутивность, определение кольца.

Пусть $(X, *, \circ)$ — произвольное множество с двумя операциями.

Определение 1.4.1 (Дистрибутивность)**.** $*$ дистрибутивна слева относительно $\circ$, если

$\forall x, y, z \in X : x * (y \circ z) = (x * z) \circ (x * z)$ и дистрибутивна справа, если $(x \circ y) * z = (x * z) \circ (y * z)$.

Замечание. Для коммутативной операции $*$ говорят только просто о дистрибутивности.

1.4.1 Примеры дистрибутивных операций

- Обычно $x \cdot (y + z) = x \cdot y + x \cdot z$ и $(x + y) \cdot z = x \cdot z + y \cdot z$.
- Булевы операции $\cap, \cup$ — каждая коммутативна и дистрибутивна относительно другой.
- **Определение 1.4.2** (Самодистрибутивность)**.** $*$ — самодистрибутивна слева, если $x*(y*z) = (x * y) * (x * z)$ и справа, если ...

Лекция V

15 сентября 2022 г.

1.4.2 Кольцо

Определение 1.4.3 (Кольцо)**.** Кольцо — множество $R \neq \varnothing$ с двумя операциями $+$ и $\cdot$ — сложение и умножение. Операции такие, что:

- A: $(R, +)$ — абелева (коммутативная) группа.
  1. $(x + y) + z = x + (y + z)$.
  2. $\exists 0 \in R : x + 0 = 0 + x = x$.
  3. $\forall x \in R : \exists - x \in R : x + (-x) = 0 = (-x) + x$.
  4. $x + y = y + x$.

     Замечание. В кольцах с единицей коммутативность сложения автоматически следует из дистрибутивности
- D: $\cdot$ двусторонне дистрибутивно относительно $+$.
  1. $a \cdot (b + c) = a \cdot b + a \cdot c$
  2. $(a + b) \cdot c = a \cdot c + b \cdot c$

1.4.3 Примеры колец

- Кольцо Ли, умножение неассоциативно: $V = \mathbb{R}^3$, сложение — сложение векторов, умножение — умножение векторов.

  Замечание. В таком кольце выполняется *тождество Якóби*: $(xy)z + (yz)x + (zx)y = 0$ и тождество антикоммутативности $x^2 = 0 \overset{\text{следует из раскрытия } (x+y)^2}{\Rightarrow} xy = -yx$.

  Замечание. Тождество Якоби примерно аналогично *тождеству Лейбница*: $D(f \cdot g) = D(f) \cdot g + f \cdot D(g)$.

  Замечание. Часто используют *алгебру* Ли вместо кольца Ли, в алгебре можно ещё умножать на скаляр.

  Замечание. На начальном этапе все рассматриваемые кольца будут ассоциативны.

  Определение 1.4.4 (Ассоциативное кольцо)**.** $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

  Определение 1.4.5 (Кольцо с единицей (унитальное кольцо))**.** Выполняется аксиома M2: все элементы образуют мультипликативный моноид: $\exists 1 \in R : x \cdot 1 = 1 \cdot x = x$.

Определение 1.4.6 (Коммутативное кольцо)**.** Умножение коммутативно. Часто подразумевают, что коммутативное кольцо ассоциативно, но это не следует.

Замечание. Коммутативность влечёт $(x-y)(x+y) = x^2 - y^2$. Без неё

$$(x-y)(x+y) = x^2 + xy - yx - y^2 = x^2 + [x,y] - y^2$$

где $[x,y] \stackrel{def}{=} xy - yx$ — коммутатор x, y. Аналогично

$$(x+y)^2 = x^2 + 2(x \circ y) + y^2$$

где $x \circ y \stackrel{def}{=} \frac{1}{2}(xy + yx)$ — антикоммутатор.

Замечание. Верно для произвольного ассоциативного кольца:

- $0 \cdot x = 0$.
- $(x-y)z = xz - yz$, где $x - y = x + (-y)$.
- $(-x)(-y) = xy$.

Определение 1.4.7 (Тело)**.** R — тело, если R — ассоциативное кольцо с единицей и выполняется M4: $\forall x \in R\ \{0\} : \exists x^{-1} \in R : xx^{-1} = x^{-1}x = 1$

Определение 1.4.8 (Поле)**.** Коммутативное тело, т. е. тело с коммутативным умножением. Часто обозначается K или F. Выполняются аксиомы A1 – A4, D1, D2, M1 – M4, $1 \neq 0$.

- Нулевое кольцо: $0 = 1 \Rightarrow 0 = 0 \cdot x = 1 \cdot x = x$. Кольцо из одного элемента.
- Некольцо: Рассмотрим множество многочленов с коэффициентами из K: $K[x]$.

  $+$ — сложение многочленов.

  $\cdot$ — композицию многочленов.

  Заметим, что $(f+g) \circ h = f \circ h + g \circ h$, но структура — не кольцо, так как $f \circ (g+h) \neq f \circ g + f \circ h$.
- Здесь и далее: коммутативные ассоциативные кольца с единицей.

  Кольцо целых чисел $\mathbb{Z}$. Это коммутативное ассоциативное кольцо с единицей без делителей нуля.

  $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ — поля.
- Булевы кольца. Определим их на булеане множеств. $R = 2^X$.

  $\cdot$ — $\cap$.

  $+$ — ? ($\cup$ брать нельзя, так как нет противоположного). $+$ — $\triangle$ (симметрическая разность).

  Пример булевого кольца над синглетоном: $\mathbb{F}_2 \stackrel{def}{=} \{0; 1\}$.

  Таблицы Кэли для $\mathbb{F}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- Кольцо двоичных дробей: $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{n}{2^m} \middle| n \in \mathbb{Z}, m \in \mathbb{N}_0\right\}$.

  Кольцо десятичных дробей: $\mathbb{Z}\left[\frac{1}{10}\right] = \mathbb{Z}\left[\frac{1}{2}, \frac{1}{5}\right] = \left\{\frac{n}{2^k 5^l} \middle| n \in \mathbb{Z}, k, l \in \mathbb{N}_0\right\}$.

  Замечание. На бесконечных десятичных дробях нельзя ввести арифметические операции, поэтому они бессмысленны. По сути, бесконечные десятичные дроби — последовательность приближений. (Я не уверен, что понял идеологию лектора)

- Целые алгебраические числа $\mathbb{A}$ — корни алгебраических уравнений (многочленов) с целыми коэффициентами и старшим коэффициентом 1. Показать то, что они образуют кольцо, помогает конструкция Кронекера (1.1.2).
  - Подкольцо $\mathbb{A}$ — целые гауссовы числа $\mathbb{Z}[i] = \{m + ni | m, n \in \mathbb{Z}\}$.
  - Подкольцо $\mathbb{A}$ — целые эйзенштейновы числа $\mathbb{Z}[\omega] = \{m + n\omega | m, n \in \mathbb{Z}\}$.

    Здесь $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.
  - Подкольцо $\mathbb{A}$ — целые пифагоровы числа $\mathbb{Z}\left[\sqrt{2}\right] = \left\{m + n\sqrt{2} \middle| m, n \in \mathbb{Z}\right\}$.
- Кольца многочленов: Пусть R — коммутативное ассоциативное кольцо с единицей. Оно порождает $R[x]$.
  - Кольцо формальных степенных рядов $R[[x]]$.
  - Кольцо многочленов Лагранжа $R[x, x^{-1}]$.
- Кольца матриц: $R \mapsto M(n, R), n \in \mathbb{N}$. Для $n \geq 2$ кольцо матриц некоммутативно даже для коммутативного R или поля.

Лекция VI

27 сентября 2022 г.

- **Определение 1.4.9** (Противоположное кольцо)**.** Для кольца $(R, +, \cdot)$ — кольцо R°, построенное на R.

$$x_{R^\circ} + y_{R^\circ} = x + y$$
$$x_{R^\circ} \circ y_{R^\circ} = y \cdot x$$

  Обозначается $(R^\circ, +, \circ)$.

  Определение 1.4.10 (Гомоморфизм колец R и S)**.** Отображение $f : R \to S$, являющееся одновременно и аддитивным, и мультипликативным гомоморфизмом.

  Гомоморфизм, сохраняющий единицу, называют *унитальным*.

  Биективное f соответствует изоморфизму колец.

  Предостережение. Совсем не факт, что $R \cong R^\circ$.

  Тем не менее, $M(n, R) \cong M(n, R)^\circ$ операцией транспонирования.
- **Определение 1.4.11** (Прямая сумма колец $(R_1, +_1, \cdot_1), \ldots, (R_n, +_n, \cdot_n)$)**.** Кольцо, заданное на множестве $R_1 \times \cdots \times R_n$, операции определены покомпонентно.

  Обозначается $(R_1, +_1, \cdot_1) \oplus \cdots \oplus (R_n, +_n, \cdot_n)$.

  Замечание. В прямой сумме обязательно появляются делители нуля: $(x, 0) \cdot (0, y) = (0, 0)$.
- *Кольца классов вычетов*. Для кольца $\mathbb{Z}$ рассмотрим подкольцо $m\mathbb{Z} = \{mn | n \in \mathbb{Z}\}$. Данное кольцо является идеалом (1.6.1), и как и по всякому идеалу, по нему можно профакторизовать, получив структуру кольца (1.6.13).

  Рассмотрим здесь именно данную структуру, $\mathbb{Z}/m\mathbb{Z}$. Чтобы её построить, введём отношение отношение эквивалентности $a \sim b \overset{def}{\iff} a - b \in m\mathbb{Z}$. Другими словами, $a \equiv b \pmod{m}$.

  По данному отношению эквивалентности $\sim$ можно профакторизовать, получив $\mathbb{Z}/m\mathbb{Z} \overset{def}{=} \mathbb{Z}/\sim$. Полученное кольцо — кольцо остатков от деления, или же классов вычетов. А именно, $\mathbb{Z}/m\mathbb{Z}$ построено на множестве $\left\{\{n + k \cdot m | k \in \mathbb{Z}\} \middle| 0 \leq n < m\right\}$, множество $\overline{n} \overset{def}{=} \{n + k \cdot m | k \in \mathbb{Z}\}$ соответствует остатку n по модулю m.

1.4.4 Примеры гомоморфизмов

- **Определение 1.4.12** (Вложение)**.** Инъективный гомоморфизм $f : X \to Y$. В таком случае X вкладывается в Y.

  Часто случается так, что при вложении (особенно каноническом) элемент переходит «в себя». Так, $f : \mathbb{Z} \to \mathbb{R}; \quad x \mapsto x$ — вложение $\mathbb{Z}$ в $\mathbb{R}$.

  По-видимому, таким образом можно определить подкольцо (которое очевидно, что такое, но вроде как на лекциях не определялось).

  Как известно, $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{A} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$.

- Отображения вида $R \to M(n, R)$, где n фиксировано. Например, для $n = 2$ возможны гомоморфизмы

  $$x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \qquad x \mapsto \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

  Что интересно, только второй гомоморфизм является унитальным (1.4.10).

- *Проекции, а также вложения в прямую сумму* Для всякой прямой суммы $R \oplus S$ определено вложение $R \to R \oplus S; \quad x \mapsto (x, 0)$.

  В паре с ним можно рассмотреть гомоморфизм, действующий в обратную сторону — *проекцию* $R \oplus S \to R; \quad (x, y) \mapsto x$.

1.4.5 Примеры полей

- *Конечные поля*, они же *поля Галуа*. Поля порядка (мощности множества) q обозначаются $\mathbb{F}_q$ или $GF(q)$.

  Несложно проверить, что для $q = 2, 3$ полями Галуа являются уже упомянутые кольца вычетов $\mathbb{Z}/2\mathbb{Z}$ и $\mathbb{Z}/3\mathbb{Z}$ соответственно.

  Для порядка 4 $\mathbb{Z}/4\mathbb{Z}$ не является полем, так как $2 \cdot 2 \equiv 0 \pmod 4$. Тем не менее, руководствуясь тем, что в поле есть 1, 0, а также тем, что структура должна быть абелевой группой по сложению и абелевой группой (кроме нуля) по умножению, несложно построить таблицы Кэли:

$+$	0	1	u	v
0	0	1	u	v
1	1	0	v	u
u	u	v	0	1
v	v	u	1	0

$\cdot$	0	1	u	v
0	0	0	0	0
1	0	1	u	v
u	0	u	v	1
v	0	v	1	u

  Ещё использовалось условие, которое мы почему-то хотим, чтобы тоже выполнялось — существование сложения $\mathbb{F}_2 \hookrightarrow \mathbb{F}_4$.

  Определение 1.4.13 (Примарное число)**.** Такое $q \in \mathbb{N}$, что $q = p^m$ для неких $p \in \mathbb{P}, m \in \mathbb{N}$.

  Интересный факт (Теорема Галуа). Конечное поле порядка q существует если и только если q — примарное.

Лекция VII

28 сентября 2022 г.

Интересный факт (Малая теорема Веддербёрна). Любое конечное тело коммутативно — является полем.

Рассмотрим группу кватернионных единиц $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

Построим на ней пример бесконечного тела: тело кватернионов $\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$. Используют также векторную запись (a, b, c, d) и матричную запись — четвёрки Кэли (1.4.6).

Для определения операций обратимся к $\mathbb{C} = \{a + bi | a, b, \in \mathbb{R}\}$. Сложение на парах (a, b) и (c, d) определено покомпонентно: $(a, b) + (c, d) = (a + c, b + d)$. Умножение задаётся следующим выражением: $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Комплексные числа отвечают за вращения и растяжения плоскости; но даже в трёхмерном пространстве вращения некоммутативны, поэтому $\mathbb{H}$ некоммутативно.

Сложение в $\mathbb{H}$ покомпонентно, а умножение определяется следующим образом: сложение дистрибутивно относительно умножения, а умножение базисных элементов — $1, i, j, k$ — определяется таблицей Кэли. Используя ассоциативность умножения и нейтральность 1 относительно умножения, можно вывести всё из тождества $i^2 = j^2 = k^2 = ijk = -1$. В частности, $ij = k;\ jk = i;\ ki = j$.

Теорема 1.4.1. $\mathbb{H}$ — тело.

Доказательство.

- Основная сложность заключается в проверке ассоциативности. Она будет проверена матрицами Кэли (1.4.6).
- Обратимость: $z = a + bi + cj + dk \neq 0$ — хотя бы один из a, b, c, d не равен 0.

  Определим $\overline{z} = a - bi - cj - dk$.

  Определение 1.4.14 (Норма кватерниона)**.** $N(z) = z\overline{z}$. Прямое вычисление даёт $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$.

  Отсюда следует, что $z \cdot \dfrac{\overline{z}}{N(z)} = 1 \quad \Rightarrow \quad z^{-1} = \dfrac{\overline{z}}{N(z)}$.
- Дистрибутивность следует из того, что ассоциативность определяется только на базисе, а остальное как-раз-таки продолжается по дистрибутивности. □

1.4.6 Матрицы Кэли

$$\mathbb{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\} \leq M(2, \mathbb{R}).$$

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & -\overline{z} \end{pmatrix} \middle| z, w \in \mathbb{C} \right\} \leq M(2, \mathbb{C})$$

$$\begin{pmatrix} z & w \\ -\overline{w} & -\overline{z} \end{pmatrix} = \left(\begin{array}{cc|cc} a & b & c & d \\ -b & a & -d & c \\ \hline -c & d & a & -b \\ -d & -c & b & a \end{array} \right) \in M(4, \mathbb{R}) \cong M(2, M(2, \mathbb{R})).$$

Подобным способом можно определить сложение и умножение на матрицах любого натурального порядка — дополнить правый нижний угол нулями.

$\mathbb{H}$ вкладывается в $M(2, \mathbb{C})$ и ассоциативность проверяется бесплатно за счёт ассоциативности умножения матриц. Так,

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Теорема 1.4.2 (Фробениус)**.** Единственными конечномерными (без бесконечно малых и больших) ассоциативными расширениями $\mathbb{R}$ являются $\mathbb{R}, \mathbb{C}, \mathbb{H}$.

Замечание. Ещё используется неассоциативное расширение $\mathbb{R}$ из восьмёрок чисел $\mathbb{O}$.

1.5 Специальные элементы колец. Область целостности

Предположим, что R — ассоциативное кольцо с единицей.

1.5.1 Обратимые и регулярные элементы

Определение 1.5.1 (Обратимый слева (справа) элемент)**.** $x \in R$ обратим слева (справа), если $\exists y \in R : yx = 1$ $(xy = 1)$.

Определение 1.5.2 ((Двусторонне) обратимый элемент $x \in R$)**.** $\exists x^{-1} \in \mathbb{R} : x^{-1}x = 1 = xx^{-1}$.

Лемма 1.5.1. *Если $x \in R$ обратим и слева, и справа, то он обратим.*

Доказательство. Как здесь (1.2.2). □

Замечание. Здесь интересно рассмотреть бесконечные матрицы вида

$$X = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ 0 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \quad Y = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Любопытно, что

$$X \cdot Y = \begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = e, \text{ но } Y \cdot X = \begin{pmatrix} 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \neq e$$

Это связано с тем, что для конечных матриц одна единица в углу будет нулём. Однако в случае $X \cdot Y$ этот угол — правый нижний, то есть, для бесконечных вправо вниз матриц этого угла нет. А в случае $Y \cdot X$ это вполне себе существующий левый верхний угол.

Более того, несложно видеть, что X вообще не обратима слева. Таким образом, из обратимости с одной стороны никак не следует обратимость в общем случае.

Замечание. Тем не менее, можно убедиться, что такое может происходить только в бесконечных кольцах. А именно, вспомнить задачку с практики: *Если элемент в ассоциативном кольце с единицей обратим слева конечным числом элементов, то он обратим справа.*

Определение 1.5.3 (Мультипликативная подгруппа R)**.** $R^* \stackrel{def}{=} \{x \in R | x - \text{обратим}\}$.

Примеры:

1. T – тело $\iff T^* = T \setminus \{0\}$.
2. В кольцах бывает очень мало обратимых: $\mathbb{Z}^* = \{\pm 1\}$; $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$; $\mathbb{Z}[\omega]^* = \{\pm 1, \pm\omega, \pm(1+\omega)\}$
3. Для многочленов над полем K: $K[x]^* = K^*$.
4. $M(n, K)^* = GL(n, K)$ — полная линейная группа степени n над K.

Регулярные элементы: раньше элемент был регулярным, если $\forall y, z \in R : (xy = xz) \Rightarrow (y = z)$. В кольце есть дистрибутивность, поэтому $xy = xz \iff x(y - z) = 0$.

Определение 1.5.4 (Регулярный элемент)**.** $x \in R$ — регулярный слева (справа), если $\forall y \in R : xy = 0$ $(yx = 0) \Rightarrow y = 0$. x регулярен, если он регулярен и слева, и справа.

Определение 1.5.5 (Делитель нуля)**.** Нерегулярный элемент x — левый (правый) делитель нуля, если $\exists y \in R : y \neq 0 \wedge xy = 0$ $(yx = 0)$.

Определение 1.5.6 (Кольцо без делителей нуля)**.** R — такое кольцо, если $(xy = 0) \Rightarrow x = 0 \vee y = 0$.

1.5.2 Области целостности

Определение 1.5.7 (Область целостности, integral domain)**.** Коммутативное кольцо без делителей нуля, такое, что $1 \neq 0$. Идеологически очень похожи на поля.

Примеры областей целостности

1. Поле
2. $\mathbb{Z}$
3. $K[t]$
4. Матрицы ими не являются: $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.
5. Кольцо вычетов тоже не область целостности: $\mathbb{Z}/6\mathbb{Z}\cong\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ по китайской теореме об остатках, а в любой прямой сумме колец есть делители нуля: $(1;0)\cdot(0;1)=(0;0)$.

   История про китайские армии и писцов, которые вычисляли количество солдат по остаткам от деления на разные взаимно простые числа.

   Замечание. В коммутативном случае можно расширить кольцо, чтобы любой регулярный элемент стал обратим.

1.5.3 Нильпотенты и унипотенты

Определение 1.5.8 (Нильпотент)**.** $x\in R$ — нильпотент, если $\exists n\in\mathbb{N}: x^n=0$.

Пример: $\mathbb{Z}/p^n\mathbb{Z}$. В этом кольце $p^n=0$, но $p^{n-1}\neq 0$.

Определение 1.5.9 (Приведённое (reduced) кольцо)**.** Коммутативное кольцо без нетривиальных нильпотентов: $\forall x\in R: x^n=0\iff x=0$. Например, $\mathbb{Z}/6\mathbb{Z}$.

В матрицах полно нильпотентов: $e_{1,2}=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$; $\quad e_{2,1}=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$. Их квадраты равны $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.

Определение 1.5.10 (Унипотент)**.** u — унипотент, если $(u-1)$ — нильпотент.

Лемма 1.5.2. *Любой унипотент обратим.*

Доказательство. Рассмотрим унипотент $u=1+x$, где $x^n=0$. Тогда $\left(u^{-1}=1-x+x^2-\dots\right)$. Сумма конечна, так как на x^n всё оборвётся. □

1.5.4 Идемпотенты и инволюции

Определение 1.5.11 (Идемоптент)**.** $e\in R$ идемпотент, если $e^2=e$.

Примеры: в любом кольце $(0^2=0)\wedge(1^2=1)$ — тривиальные идемпотенты. Вопрос — есть ли в кольце прочие центральные идемпотенты (идемпотенты, лежащие в централизаторе кольца, коммутирующие со всеми элементами кольца)?

Лекция VIII

29 сентября 2022 г.

1.5.5 Характеристика области целостности. Эндоморфизм Фробениуса

Есть такие штуки, как *гомоморфизм, изоморфизм, мономорфизм, эпиморфизм, эндоморфизм, автоморфизм*. Первая пара уже определена, следующая — будет определена позднее.

Определение 1.5.12 (Эндоморфизм)**.** Гомоморфизм в самого себя: отображение $f: G\to G$.

Определение 1.5.13 (Автоморфизм)**.** Эндоморфизм и изоморфизм: биекция $f: G\to G$.

Пусть R — произвольная область целостности.

Рассмотрим $n\in\mathbb{N}$. Определим $n\cdot 1_R\overset{def}{=}\underbrace{1_R+\dots+1_R}_{n}$.

Заинтересуемся наименьшим $n \in \mathbb{N}$, таким, что $n \cdot 1 = 0$.

Лемма 1.5.3. *Пусть R — область целостности. Если n — минимальное, такое, что $n \cdot 1 = 0$, то $n \in \mathbb{P}$.*

Доказательство.

Пусть оно существует и $n = km$. Тогда $n \cdot 1 = (\underbrace{1 + \cdots + 1}_{k}) \cdot (\underbrace{1 + \cdots + 1}_{m}) = (k \cdot 1)(m \cdot 1)$.

Но в области целостности нет делителей нуля. Тогда получается, что n — простое, неразложимо в произведение. □

Определение 1.5.14 (Характеристика области целостности)**.** Наименьшее $p \in \mathbb{N}$ такое, что $\underbrace{1 + \cdots + 1}_{p} = 0$, либо — если такого p не существует — характеристика определяется как 0. Пишут $\mathrm{char}(R) = p > 0$ или $\mathrm{char}(R) = 0$.

Замечание. Можно определить также для $n \in \mathbb{Z}$: $n \cdot 1 = \begin{cases} n \cdot 1, & n \in \mathbb{N} \\ 0, & n = 0 \\ -(-n \cdot 1), & n < 0 \end{cases}$.

Замечание. Характеристика равна $0 \iff$ отображение $\mathbb{Z} \to R; \quad n \mapsto n \cdot 1$ — инъекция.

Примеры

1. $\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = \mathrm{char}(\mathbb{Q}_p) = 0$. Здесь $\mathbb{Q}_p$ — p-адические числа, будут определены позднее.
2. $\mathrm{char}(\mathbb{F}_p) = p > 0; \quad \mathrm{char}(\mathbb{F}_{p^m}) = p > 0$.

Про характеристику

Замечание. В кольце с ненулевой характеристикой производная многочлена, равная 0, не обязательно влечёт равенство многочлена константе. Так, $(x^p)' = px^{p-1}$, что обращается в 0 в $\mathbb{F}_p$.

Теорема 1.5.1. Пусть $\mathrm{char}(K) = p > 0$ для поля K (даже для коммутативного кольца с единицей), где p — простое. Тогда $f : K \to K; \quad x \mapsto x^p$ является эндоморфизмом, то есть

$$(x + y)^p = x^p + y^p \qquad (xy)^p = x^p \cdot y^p \qquad 1^p = 1$$

Доказательство. Умножение — очевидно из коммутативности.

Сумма в коммутативном кольце раскрывается по формуле бинома (Ньютона): $(x+y)^p = \sum\limits_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$.
Все коэффициенты внутри кратны p, поэтому произведения уходят в 0_K, остаются только $x^p + y^p$. □

Определение 1.5.15. Данный эндоморфизм называется *эндоморфизмом Фробениуса*. Если так оказалось, что f биективно, то поле K называется совершенным, а f — *автоморфизм Фробениуса*.

Определение 1.5.16 (p-многочлены)**.** Пусть $\mathrm{char}(K) = p > 0$. p-многочлены — это $f \in K[x^p]$.

Факт. p-многочлены — кольцо относительно сложения и композиции (выполняется дистрибутивность в обе стороны).

1.6 Идеалы в кольцах

Пусть R — произвольное кольцо с единицей.

Определение 1.6.1 (Идеал)**.** Непустое подмножество $I \subset R$ — левый (правый) идеал, если I — аддитивная подгруппа в R ($\forall x, y \in I : x + y \in I$) и I лево(право)-устойчиво относительно умножения на любой элемент кольца ($\forall x \in I, y \in R : yx \in I$ ($xy \in I$)).

Двусторонний (two-sided ideal) идеал — одновременно и левый, и правый идеал. Обозначают $I \trianglelefteq R$.

Замечание. Быть идеалом — намного более сильное условие, чем быть односторонним идеалом.

Замечание. Очевидно, в случае коммутативного R не надо различать левый, правый и двусторонний идеалы.

1.6.1 Примеры

Определение 1.6.2 (Главный левый идеал в R, порождённый $x \in R$)**.** Множество всех левых кратных x: $Rx = \{yx | y \in R\}$.

С главным правым идеалом аналогично.

Факт. Rx и xR — левый и правый идеалы соответственно.

Замечание. Доказавши что-то для левых идеалов, для правых можно сослаться на конструкцию противоположного кольца.

Определение 1.6.3 (Левый идеал, порождённый $\{x_1, \dots, x_n\} \subset R$)**.**
Левая линейная комбинация с коэффициентами из R: $Rx_1 + \dots + Rx_n = \{y_1x_1 + \dots + y_nx_n | y_1, \dots, y_n \in R\}$

С правым идеалом аналогично.

Определение 1.6.4 (Двусторонний идеал, порождённый $x \in R$)**.** Множество $\left\{ \sum\limits_{i=1}^{n} y_i x z_i \middle| n \in \mathbb{N}_0, y_i, z_i \in R \right\}$.

Иногда обозначается RxR.

Замечание. Для коммутативного кольца $Rx = xR$ — главный идеал, порождённый x.

Матрицей e_{ij} обозначается матрица, где всюду нули, только на пересечении i-й строки и j-го столбца единица.

Рассмотрим $R = M(2, K)$, где $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots\}$.

Тогда кратные матрице $x = e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ — это матрицы с рангом единица (что?).

Замечание. Спойлер: ранг — количество линейно-независимых строчек.

Любопытно заметить, что $e_{22} = e_{21}e_{11}e_{12}$, но $e_{11} + e_{22} = e$ не является кратным e_{11}, так как все её кратные имеют ранг 1.

Лекция IX

5 октября 2022 г.

1.6.2 Кольца главных идеалов

Определение 1.6.5 (Кольцо главных идеалов)**.** (Коммутативная) область целостности — кольцо главных идеалов (principal ideal domain, PID), если все идеалы в ней главные (всякий порождается одним элементом): $\forall I \trianglelefteq R : \exists x \in R : I = Rx$ (фактически, такой x существует в I).

Примеры

- $\mathbb{Z}$ — Кольцо главных идеалов, PID.

  Доказательство. Рассмотрим $I \trianglelefteq \mathbb{Z}, I \neq \{0\}$. В нём есть $x \in I : x \neq 0$, есть противоположный, значит, $I \cap \mathbb{N} \neq \varnothing$. Во вполне упорядоченном множестве $\mathbb{N}$ есть наименьший элемент m, утверждается, что $I = m\mathbb{Z}$.

  Для этого рассмотрим $x \in I$. Из школьной математики $x = qm + r$, где $q \in \mathbb{Z}; 0 \leq r < m$. Отсюда $r = x - qm$, откуда если $r \in I$. Но m был наименьшим элементом идеала, значит, $r = 0$. □

- $K[x, y]$ не является PID. Чтобы убедиться, достаточно рассмотреть идеал многочленов без свободного члена. В идеале есть многочлены x и y, их НОД — любая константа. Но константа не содержится в идеале, данный идеал не породить одним элементом. Он порождается хотя бы двумя элементами, например, $x \cdot K[x, y] + y \cdot K[x, y]$.
- Также $\mathbb{Z}[x]$ не является PID: здесь идеал $x \cdot \mathbb{Z}[x] + 2 \cdot \mathbb{Z}[x]$ — не главный.
- $K[x],\ \mathbb{Z}[i],\ \mathbb{Z}[\omega],\ \left(\mathbb{Z}_{(p)} \stackrel{def}{=} \left\{\frac{m}{n} \middle| m, n \in \mathbb{Z}, p \nmid n\right\}\right)$ — всё это PID.

1.6.3 Простые и максимальные идеалы

Операции над идеалами

Рассмотрим два идеала $A, B \trianglelefteq R$.

- Пересечение идеалов — идеал. $A \cap B \trianglelefteq R$.
- Сумма Минковского двух идеалов — идеал. $A + B \stackrel{def}{=} \{x + y | x \in A \wedge y \in B\} \trianglelefteq R$.

  Чтобы ввернуть лампочку, достаточно 0 математиков, так как это оставлено читателю в качестве упражнения.
- Произведение идеалов — идеал. $AB \stackrel{def}{=} \left\{ \sum_{i=1}^{n} x_i y_i \middle| n \in \mathbb{N}, x_i \in A, y_i \in B \right\} \trianglelefteq R$.

Рассматриваем коммутативное кольцо R.

Определение 1.6.6 (Собственный идеал)**.** $I \trianglelefteq R$ — собственный идеал, если $I \neq R$. Пишут $I \triangleleft R$ или даже $I \lneq R$.

Определение 1.6.7 (Максимальный идеал)**.** $I \triangleleft R$ — максимальный, если он не содержится ни в одном собственном идеале. $\forall A \trianglelefteq R : I \subset A \Rightarrow (A = I \vee A = R)$. $\mathrm{Max}(R)$ — множество максимальных идеалов кольца R; «максимальный спектр» кольца R.

Определение 1.6.8 (Простой идеал)**.** Идеал $\mathfrak{p} \triangleleft R$ — простой, если $\forall x, y \in R : xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}$. Множество простых идеалов обозначается $\mathrm{Spec}(R)$, «спектр» кольца R.

Лемма 1.6.1. *Идеал $\mathfrak{p} \triangleleft R$ простой* $\iff \forall A, B \trianglelefteq R : (AB \subseteq \mathfrak{p}) \Rightarrow (A \subseteq \mathfrak{p} \vee B \subseteq \mathfrak{p})$

Доказательство.

$\Rightarrow$. От противного: $\exists A, B : AB \subseteq \mathfrak{p}$, но $\exists a \in A, b \in B : a \notin \mathfrak{p} \wedge b \notin \mathfrak{p}$. Но так как $AB \subseteq \mathfrak{p}$, то $ab \in \mathfrak{p}$, противоречие с простотой идеала.

$\Leftarrow$. Достаточно рассмотреть главные идеалы, если верно для них, то $\mathfrak{p}$ — уже простой. □

Лемма 1.6.2. *Любой максимальный идеал является простым.*

Доказательство.

Возьмём максимальный идеал $\mathfrak{m} \triangleleft R$. Пусть $x, y \in R, xy \in \mathfrak{m}$. Пойдём от противного: пусть, $x, y \notin R$. Отсюда во включениях $\mathfrak{m} \subseteq \mathfrak{m} + Rx \subseteq R$ и $\mathfrak{m} \subseteq \mathfrak{m} + ry \subseteq R$ первый знак строгий, но так как $\mathfrak{m}$ — максимальный, то второй — превращается в равенство: $\mathfrak{m} \subsetneq \mathfrak{m} + Rx = R$ и $\mathfrak{m} \subsetneq \mathfrak{m} + Ry = R$.

Но тогда $\exists u, v \in \mathfrak{m}; \exists a, b \in R : 1 = u + ax = v + by$. Перемножим (коммутативно).

$$1 = (u + ax)(v + by) = uv + uby + axv + abxy$$

Все слагаемые содержатся в идеале, в частности, последний — так как $xy \in \mathfrak{m}$. Но тогда $1 \in R$ и R оказался несобственным. Противоречие. □

Замечание. Альтернативное доказательство. На самом деле это так по следующей причине:

> **Теорема 1.6.1.** Коммутативное (ассоциативное) кольцо, в котором ровно два идеала — поле.
>
> Более слабая, некоммутативная версия: *ассоциативное кольцо, в котором ровно два левых идеала — тело.*
>
> *Доказательство.*
>
> Рассмотрим $x \in R$. Если $x \neq 0$, то $Rx = R$, то есть $\exists y \in R : yx = 1$. Для коммутативных колец доказательство закончено; для некоммутативных для $y : \exists z : zy = 1$, то есть у y есть и левый, и правый обратные $\Rightarrow z = x$ и x двусторонне обратим. □
>
> Используя факторкольцо (1.6.13) и теорему о гомоморфизме (1.6.3) можно получить следующее:
>
> **Лемма 1.6.3.**
>
> - *В коммутативном кольце* $\mathfrak{m} \triangleleft R$ *— максимальный* $\iff R/\mathfrak{m}$ *— поле.*
> - *В коммутативном кольце* $\mathfrak{m} \triangleleft R$ *— простой* $\iff R/\mathfrak{m}$ *— область целостности.*
>
> *Доказательство леммы.* 1.6.5 □

Из теоремы очевидно следует:

- R — поле $\Rightarrow 0$ — максимальный идеал.
- R — область целостности $\Rightarrow 0$ — простой идеал
- Простой идеал $I \trianglelefteq \mathbb{Z} \Rightarrow (I = 0) \vee (I = p\mathbb{Z}$ для $p \in \mathbb{P})$.

Определение 1.6.9 (Простое кольцо)**.** Кольцо R, такое, что в R ровно 2 двусторонних идеала (0 и R).

Интересный факт. T — тело $\Rightarrow M(n, T)$ — простое.

1.6.4 Сравнение по модулю идеала. Факторкольцо

Зафиксируем R — ассоциативное кольцо с единицей. $I \trianglelefteq R$ — двусторонний идеал.

Определение 1.6.10 (Сравнимость по модулю)**.** $x, y \in R$ — сравнимы по модулю I, если $x - y \in I$. Пишут $x \equiv y \pmod I$ $(x \equiv y\ (I))$ или $x \underset{I}{\equiv} y$.

Лемма 1.6.4. $\equiv_I$ *— отношение эквивалентности на* R.

Доказательство.

- Рефлексивность: $0 \in I \iff x \equiv x \pmod I$.
- Симметричность: $(x \equiv y \pmod I \iff y \equiv x \pmod I) \iff (a \in I \iff -a \in I)$.
- Транзитивность:

$$\begin{gathered} x \equiv y \pmod I \quad \wedge \quad y \equiv z \pmod I \quad \Rightarrow \quad x \equiv z \pmod I \\ (x-y),\,(y-z) \in I \quad \Rightarrow \quad (x-y)+(y-z) = (x-z) \in I \end{gathered}$$

□

Определение 1.6.11 (Конгруэнция)**.** Отношение эквивалентности $\approx$ со следующими свойствами:

$$\begin{cases} x \approx y \\ u \approx v \end{cases} \Rightarrow (x+u \approx y+v) \wedge (xu \approx yv)$$

Лемма 1.6.5. *Отношение $\equiv_I$ — конгруэнция на R.*

Доказательство.

Пусть $x - y \in I$ и $u - v \in I$.

- $(x+u)-(y+v) = (x-y)+(u-v) \in I$
- $xu - yv = (xu-yu)+(yu-yv) = (x-y)u + y(u-v) \in I$, и здесь мы впервые воспользовались тем, что I — не просто аддитивная подгруппа, а идеал. □

Определение 1.6.12 (Класс сравнения по модулю I)**.** Для $x \in R$ и $I \trianglelefteq R$ обозначим

$$\overline{x} = \{\ y \in R \mid x \equiv y \pmod I\ \} = x \overset{\text{по Минковскому}}{+} I$$

Определение 1.6.13 (Факторкольцо R/I)**.** Множество всех классов сравнения

$$R/I = R/_{\equiv_I} \overset{def}{=} \{\overline{x} | x \in R\} = \{x + I | x \in R\}$$

где операции введены в терминах представителей. А именно, $\overline{x} + \overline{y} = \overline{x+y}$ и $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$.

Определение корректно; правая часть не зависит от выбора представителей, так как $\equiv_I$ — конгруэнция. Можно написать: $(x+I)+(y+I) = (x+y)+I$ и $(x+I)(y+I) = xy + I$.

Теорема 1.6.2. Факторкольцо R/I является ассоциативным кольцом с единицей, а отображение $\underbrace{\pi_I}_{\text{проекция}}$ или $\underbrace{\rho_I}_{\text{редукция}} : R \to R/I : x \mapsto \overline{x}$ является сюръективным гомоморфизмом колец (проекция на факторкольцо или редукция по модулю I).

Лекция X

6 октября 2022 г.

Примеры факторколец

1. $\mathbb{Z}/n\mathbb{Z}$
2. $K[t]/f \cdot K[t]$, где $f \in K[t]$.
   - Если f — неприводимый (не разложимый на нетривиальные множители из $K[f]$) многочлен, то $K[t]/fK[t]$ — поле разложения f над K.

     Например, $\mathbb{C} = \mathbb{R}/(t^2+1)\mathbb{R}[t]$. Или же $\mathbb{Q}\left[\sqrt{2}\right] \overset{def}{=} \mathbb{Q}[t]/(t^2-2)\mathbb{Q}[t] = \left\{a + b\sqrt{2} \middle| a, b \in \mathbb{Q}\right\}$.
   - $K[t]/t^n K[t]$ — кольцо усечённых многочленов (truncated polynomials); многочлены степени, строго меньшей n. Часто встречаются $K[t]/t^2K[t]$.

     Для циклических свёрток полезны $K[t]/(t^n-1)K[t]$.

1.6.5 Теорема о гомоморфизме

Пусть $\phi : R \to S$ — гомоморфизм колец (колец с единицами).

Определение 1.6.14 (Ядро гомоморфизма)**.** $\mathrm{Ker}(\phi) = \phi^{-1}(0) = \{x \in R | \phi(x) = 0\}$

Определение 1.6.15 (Образ гомоморфизма)**.** $\mathrm{Im}(\phi) = \phi(R) = \{y \in S | \exists x \in R, \phi(x) = y\}$

Лемма 1.6.6.

- $\mathrm{Im}(\phi) \leq S$ — *подкольцо с единицей в* S.
- $\mathrm{Ker}(\phi) \trianglelefteq R$ — *идеал в* R.

Доказательство. Напрямую следует из того, что ϕ — гомоморфизм. □

Теорема 1.6.3 (О гомоморфизме)**.** Для любого гомоморфизма колец $\phi : R \to S$ имеет место изоморфизм $R/Ker(\phi) \cong \mathrm{Im}(S)$.

Доказательство. Обозначим $I = \mathrm{Ker}(\phi)$. Вот этот изоморфизм: $\overline{\phi} : R/I \to \mathrm{Im}(\phi) : x + I \mapsto \phi(x)$

- $\overline{\phi}$ определён корректно: $x \underset{I}{\equiv} y \Rightarrow \phi(x) - \phi(y) = \phi(x - y) = 0 \Rightarrow \phi(x) = \phi(y) \Rightarrow \overline{\phi}(x + I) = \overline{\phi}(y + I)$.
- $\overline{\phi}$ — гомоморфизм, так как операции определены в терминах представителей.
- Так как $\phi(R) = S$, то $\overline{\phi}$ сюръективно.
- Также $\overline{\phi}$ инъективно (развернуть знаки следования в первом пункте). □

Замечание. Верно и обратное: каждый идеал $I \trianglelefteq R$ — ядро гомоморфизма $\rho_I : R \to R/I$.

Теорема 1.6.4. Пусть $I \trianglelefteq R$. Тогда существует взаимно-однозначное соответствие между A и B, где $A = \{J | I \subseteq J \trianglelefteq A\}$, а $B = \{J | J \trianglelefteq R/I\}$.

Доказательство. Оно определяется так:

$J_A \mapsto J_A/I = \{a + I | a \in J_A\}$, что совпадает с $\rho(J_A)$, где ρ — редукция по идеалу I;

$J_B \mapsto \{b + x | x \in I, b + I \in J_B\}$, что совпадает с $\rho^{-1}(J_B)$. □

Теорема 1.6.5.

- В коммутативном кольце $\mathfrak{m} \in \mathrm{Max}(R) \iff R/\mathfrak{m}$ — поле.
- В коммутативном кольце $\mathfrak{m} \in \mathrm{Spec}(R) \iff R/\mathfrak{m}$ — область целостности.

Доказательство.

$\mathfrak{m} \in \mathrm{Max}(R)$, значит $\{J | \mathfrak{m} \leq J \trianglelefteq R\}$ содержит всего 2 элемента $\overset{1.6.4}{\iff}$ $R/\mathfrak{m}$ имеет два идеала $\overset{1.6.1}{\iff} R/\mathfrak{m}$ — поле.

$\mathfrak{m} \in \mathrm{Spec}(R)$, значит, $\forall J_1, J_2 \trianglelefteq R : (\mathfrak{m} \subsetneq J_1, J_2 \trianglelefteq R \Rightarrow J_1 J_2 \not\subseteq \mathfrak{m}) \iff \forall J_1, J_2 \trianglelefteq R/I : (J_1 \neq \{0\} \wedge J_2 \neq \{0\} \Rightarrow J_1 J_2 \neq \{0\}) \iff \forall x, y \in R/I : (x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0)$, а это определение области целостности. □

Замечание. Формулировка уже приводилась здесь: 1.6.1

1.6.6 Китайская теорема об остатках. Chinese remainder theorem

Определение 1.6.16 (Идеалы $A, B \trianglelefteq R$ комаксимальны)**.** $A + B = R$ (сумма — по Минковскому).

Факт. В $\mathbb{Z}$: $m\mathbb{Z}$ и $n\mathbb{Z}$ комаксимальны $\iff (m, n) = 1 \overset{def}{\iff} m$ и n взаимно просты.

Теорема 1.6.6 (CRT для двух идеалов)**.** Если $A+B = R$, то $A \cap B = A \cdot B$ и $R/(A \cap B) \cong R/A \oplus R/B$, где $\oplus$ — прямая сумма колец (1.4.11).

Доказательство. Построим гомоморфизм $\phi : R \to R/A \oplus R/B : x \overset{\phi}{\mapsto} (x + A, x + B)$. Несложно убедиться, что это действительно гомоморфизм.

- Так как $A + B = R$, то $\exists a \in A, b \in B : a + b = 1$.

  Докажем, что $\mathrm{Im}(\phi) = \{(y + A, z + B) | y, z \in R\}$. Достаточно заметить, чему равно $\phi(az+by)$.

$$az + by + A = az + (1 - a)y + A = y + A$$
$$az + by + B = (1 - b)z + by + B = z + B$$

- $\mathrm{Ker}(\phi) = \{x \in R | x + A = A \wedge x + B = B\} = A \cap B$. Отсюда по теореме о гомоморфизме следует изоморфизм между $R/(A \cap B)$ и $R/A \oplus R/B$.
- Это пересечение равняется произведению идеалов:
  - Очевидно, $AB \subseteq A \cap B$.
  - Рассмотрим $c \in A \cap B$. Так как $a + b = 1$, то $c = ac + bc$, но $ac \in AB$ и $bc \in BA$. Отсюда любой такой $c \in A \cap B$ лежит в AB. □

Теорема 1.6.7 (CRT в общем виде)**.** Пусть есть конечное множество идеалов $\{I_i\}_{1 \le i \le n}$, попарно комаксимальных. Тогда $R/(I_1 \cap \cdots \cap I_n) \cong R/I_1 \oplus \cdots \oplus R/I_n$.

Доказательство.

Докажем по индукции: $R/(I_1 \cap \cdots \cap I_n) = R/\left((I_1 \cdot \ldots \cdot I_{n-1}) \cap I_n\right)$. Единственное, что необходимо проверить — $I_1 \cdot \ldots \cdot I_{n-1} + I_n = R$. Это верно, так как $I_1 \cdot \ldots \cdot I_{n-1} + I_n \supseteq \prod_{i=1}^{n-1} (I_i + I_n) = \prod_{i=1}^{n-1} R = R$. Включение выполняется, так как в произведении все множители, кроме одного, содержат I_n. А последний равен как раз $I_1 \cdot \ldots \cdot I_{n-1}$. □

1.7 Что такое на самом деле кольцо?

1.7.1 Три сущности колец

Как группы идеологически — симметрии, автоморфизмы какой-то структуры, так и кольца тоже имеют внутреннюю идеологию.

Однако кольца — более сложная структура, есть 3 сущности, которые могут представлять кольца. Эти сущности довольно разные, и нахождение гомоморфизмов между кольцами разных сущностей влечёт существенные результаты.

- Кольца операторов. Определены на множестве A^A. Пусть $\phi, \psi : A \to A$. Тогда

$$(\phi + \psi)(x) = \phi(x) + \psi(x)$$
$$(\phi \circ \psi)(x) = \phi(\psi(x))$$

- Кольца функций. Определены на множестве R^X, где R — кольцо. Пусть $f, g : X \to R$. Тогда

$$(f + g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x)$$

- Кольца функций со свёрткой. Определены на множестве R^X, где R — кольцо, X — моноид. Тогда

$$(f+g)(x) = f(x) + g(x)$$
$$(f * g)(x) = \sum_{y \circ z = x} f(y) \cdot g(z)$$

Лекция XI

12 октября 2022 г.

1.7.2 Кольца операторов

Рассмотрим A — абелева группу.

Определение 1.7.1 (Оператор = эндоморфизм)**.** Гомоморфизм в себя $\phi : A \to A$. Множество эндоморфизмов обозначается $\mathrm{End}(A)$.

Свойства эндоморфизмов

- Сумма эндоморфизмов — эндоморфизм.

  $(\phi + \psi)(x + y) \overset{\text{определение } +}{=}$
  $= \phi(x+y) + \psi(x+y) \overset{\text{определение эндоморфизма}}{=}$
  $= (\phi(x) + \phi(y)) + (\psi(x) + \psi(y)) \overset{\text{ассоциативность и коммутативность}}{=}$
  $= (\phi(x) + \psi(x)) + (\phi(y) + \psi(y)) \overset{\text{определение эндоморфизма}}{=}$
  $= (\phi + \psi)(x) + (\phi + \psi)(y)$

  Замечание. Абелевость группы крайне существенна. Так, для некоммутативной группы $(\phi + \psi)(x) \overset{def}{=} \phi(x)\psi(x)$ (так как в некоммутативных группах принята мультипликативная нотация), но в общем случае это не является эндоморфизмом.

- Композиция эндоморфизмов — эндоморфизм. Обозначается, как произведение:

  $(\phi\psi)(x) = (\phi \circ \psi)(x) = \phi(\psi(x))$

  Замечание. Верно, так как композиция гомоморфизмов — гомоморфизм.

Теорема 1.7.1. $\mathrm{End}(A)$ — кольцо. Называется *кольцо эндоморфизмов A*, *кольцо линейных операторов A*.

Доказательство.

- Абелева группа по сложению — так как операторы определены в терминах элементов, которым присуща и коммутативность, и ассоциативность
- Ассоциативность умножения — ассоциативность композиции (1.1.1)
- Левая дистрибутивность

  $$(\phi + \psi)\theta = \phi\theta + \psi\theta$$

  $((\phi + \psi)\theta)(x) = (\phi + \psi)\theta(x) = \phi\theta(x) + \psi\theta(x) = \phi(\theta(x)) + \psi(\theta(x))$.

  Использованы соответственно определения умножения, сложения, умножения.

- Правая дистрибутивность

  $$\phi(\psi + \theta) = \phi\psi + \phi\theta$$

  $(\phi(\psi + \theta))(x) = \phi((\psi + \theta)(x)) = \phi(\psi(x) + \theta(x)) = \phi(\psi(x)) + \phi(\theta(x)) = (\phi\psi)(x) + (\phi\theta)(x)$

  Использованы соответственно определение умножения, аддитивность ϕ, определение сложения, определение произведения. □

Немного о будущем: Пусть R — коммутативное ассоциативное кольцо с единицей. Говорят, что кольцо действует на абелевой группе A, или A — R-модуль, если $R \times A \to A; \quad (\lambda, x) \mapsto \lambda x$.

Здесь определяют кольцо $\mathrm{End}_R(A) = \{\phi \in \mathrm{End}(A) | \forall \lambda \in R, x \in A : \phi(\lambda x) = \lambda \phi(x)\}$

1.7.3 Кольцо функций

Пусть X — множество, R — кольцо. Тогда функции $f \in R^X$ образуют кольцо.

Определение 1.7.2 (Кольцо функций)**.** R^X — кольцо функций на X со значениями в R, если операции в нём — сумма и произведение функций.

Сумма и произведение функций определяется в терминах значений:

$$(f+g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Теорема 1.7.2. R^X — кольцо

Доказательство. Очевидно из того, что все тождества определены в терминах значений. □

Свойства кольца R^X

- Замена переменных: для $\phi : X \to Y$ и $f : Y \to R$ рассмотрим композицию $f \circ \phi$. Заменой переменной называется отображение $\phi^* : R^Y \to R^X; \quad f \mapsto f \circ \phi$.

  Теорема 1.7.3. Замена переменной — гомоморфизм колец.

  Доказательство. Проверим для произведения:

  $$\phi^*(f \cdot g) = \phi^*(f) \cdot \phi^*(g)$$

  $(\phi^*(f \cdot g))(x) = ((f \cdot g) \circ \phi)(x) = (f \cdot g)(\phi(x)) = f(\phi(x)) \cdot g(\phi(x)) = (f \circ \phi)(x) \cdot (g \circ \phi)(x) = (\phi^*(f))(x) \cdot (\phi^*(g))(x) = (\phi^*(f) \cdot \phi^*(g))(x)$ □

- Идеалы в R^X. Пусть $Y \subset X$. Рассмотрим $I_Y = \left\{f \in R^X \middle| \forall y \in Y, f(y) = 0\right\}$. Иначе говоря, $\mathrm{Supp}(f) \cap Y = \varnothing$.

  Определение 1.7.3 (Носитель)**.** Носитель отображения f — множество точек, где функция не обращается в ноль. Пишут $\mathrm{Supp}(f) = \{x \in X | f(x) \neq 0\}$

  Лемма 1.7.1. $I_Y \trianglelefteq R^X$.

  Доказательство. $\forall f, g \in I_Y : \forall y \in Y : (f+g)(y) = f(y) + g(y) = 0 + 0 = 0$.

  $\forall f \in I_Y, g \in R^X : \forall y \in Y : (fg)(y) = f(y)g(y) = 0$. □

  Факт. $R^X / I_Y \cong R^Y$

- **Определение 1.7.4** (Дизъюнктное объединение)**.** $X \sqcup Y = X \cup Y$, если $X \cap Y = \varnothing$. Если они вдруг пересекаются, то сделаем, чтобы они не пересекались: $X \sqcup Y = (X \times \{0\}) \cup (Y \times \{1\})$. *На лекции произнесено примерно следующее: Нам неважно, какие элементы содержатся в дизъюнктном объединении, это не теоретико-множественная операция, а теоретико-категорная. Важно лишь, можем ли мы построить гомоморфизмы.*

  Прямая сумма $R^{X \sqcup Y} = R^X \oplus R^Y$.

  Замечание для 3-го семестра: *Разделение переменных*: $R^{X \times Y} = R^X \otimes R^Y$ — если X, Y — конечны.

1.7.4 Кольца со свёрткой

X — моноид (иногда полугруппа); R — кольцо. Рассматриваем функции $f, g : X \to R$.

В отличие от предыдущих двух типов колец, здесь не две, а три операции — $\circ : X \times X \to X$ и $+, \cdot : R \times R \to R$.

Формула без смысла:

$$(f * g)(x) = \sum_{y,z \in X;\ y \circ z = x} f(y) \cdot g(z)$$

А смысла нет, потому что сумма может быть бесконечной. Можно пытаться рассматривать эту сумму формально, или пытаться занимать теорией приближений, но это прерогатива анализа.

Самое простое — потребовать от суммы конечности, например, потребовать $|X| < \infty$ — конечность множества X. В таком случае формула будет иметь смысл всегда.

Два важнейших частных случая, так получилось, затрагивают бесконечные моноиды X. Однако несложно видеть, что в обоих случаях сумма будет конечной.

1. Свёртка Абеля. $(X, \circ) = (\mathbb{N}_0, +)$. Кольцо получается на множестве функций $R^{\mathbb{N}_0}$. Для

   $$f, g \in R^{\mathbb{N}_0} : \quad (f * g)(n) = \sum_{i+j=n} f(i)g(j)$$

   Сумма для всякого n конечна, так как уравнение $i + j = n$ имеет конечное число решений в $\mathbb{N}_0 \times \mathbb{N}_0$. Конкретнее — $n + 1$ решений.

   $R[[x]]$ — формальные степенные ряды.

2. Свёртка Дирихле. $(X, \circ) = (\mathbb{N}_{>0}, \cdot)$. Кольцо получается на множестве функций $R^{\mathbb{N}_{>0}}$. Для

   $$f, g \in R^{\mathbb{N}_{>0}} : \quad (f * g)(n) = \sum_{i \cdot j = n} f(i)g(j)$$

   Сумма конечна, так как уравнение $i \cdot j = n$ имеет конечное число решений в $\mathbb{N}_{>0} \times \mathbb{N}_{>0}$. Ряды Дирихле, L-ряды — $\sum \dfrac{f(n)}{n^s}$.

   Лемма 1.7.2. *Для произвольных функций $f * g$ имеет смысл в R^X, если $\forall x \in X$ уравнение $y \circ z = x$ имеет конечное число решений.*

3. Формальные ряды Лагранжа.

   Рассмотрим пример $f, g \in R^{\mathbb{Z}}$, где операция на $\mathbb{Z}$ — сложение.

   Пусть $(f*g)(n) = \sum\limits_{i+j=n} f(i)g(j)$. Чтобы формула имела смысл, определим кольцо на функциях f, g со следующим условием:

   $R((x)) = \left\{ f \in R^{\mathbb{Z}} \middle| \exists N \in \mathbb{Z}, \forall n < \mathbb{N} : f(n) = 0 \right\}$. При таком условии сумма отлична от нуля лишь при конечном числе решений.

Лекция XII

13 октября 2022 г.

Вспомним определение носителя: $\mathrm{Supp}(f) = \{x \in X | f(x) \neq 0\}$.

Тогда очевидно, что

$$\mathrm{Supp}(f + g) \subset \mathrm{Supp}(f) \cup \mathrm{Supp}(g)$$
$$\mathrm{Supp}(f \cdot g) \subset \mathrm{Supp}(f) \cap \mathrm{Supp}(g)$$
$$\mathrm{Supp}(f * g) \subset \mathrm{Supp}(f) \circ \mathrm{Supp}(g) \overset{def}{=} \{y \circ z | y \in \mathrm{Supp}(f), z \in \mathrm{Supp}(g)\}$$

Тогда понятно, что свёртка определена, если носитель свёртки конечен.

$R[X]$ — функции $f \in R^X$ такие, что $|\operatorname{Supp}(f)| < \infty$.

Лемма 1.7.3. *Свёртка функций из $R[X]$ всегда определена, и $f * g \in R[X]$.*

1.8 Полугрупповая алгебра

Пусть X — полугруппа с операцией $\circ$. Пусть R — коммутативное ассоциативное кольцо с единицей (можно определить на некоммутативном R, но не нужно).

Теорема 1.8.1. Только что определённое $R[X]$ образует ассоциативное кольцо относительно операций $+, *$.

Если X — моноид, то $R[X]$ — кольцо с единицей.

Если X коммутативно, то $R[X]$ — коммутативное кольцо.

Доказательство.

- Дистрибутивность. $\forall f, g, h \in R[X] : f * (g + h) = f * g + f * h$.

  $\forall x \in X : (f * (g + h))(x) = \sum\limits_{y \circ z = x} f(y) \cdot (g + h)(z) = \sum\limits_{y \circ z = x} (f(y) \cdot g(z) + f(y) \cdot h(z))$

  В формуле выше можно переставить слагаемые (изменить порядок суммирования), так как R — кольцо, и операция $+$ в нём и коммутативна, и ассоциативна.

  $\sum\limits_{y \circ z = x} (f(y) \cdot g(z) + f(y) \cdot h(z)) = \sum\limits_{y \circ z = x} f(y) \cdot g(z) + \sum\limits_{y \circ z = x} f(y) \cdot h(z) = (f * g)(x) + (f * h)(x) = (f * g + f * h)(x)$.

- Ассоциативность

  $\forall f, g, h \in R[X], x \in X$ проверим: $(f * g) * h = f * (g * h)$.

  $$((f*g)*h)(x) = \sum_{y \circ z = x} (f*g)(y) \cdot h(z) = \sum_{y \circ z = x} \left(\sum_{u \circ v = y} f(u) \cdot g(v) \right) \cdot h(z) = \sum_{y \circ z = x} \sum_{u \circ v = y} (f(u) \cdot g(v)) \cdot h(z)$$

  Заметим, что на выше написана следующая сумма: $\sum\limits_{y \circ z = x} \sum\limits_{u \circ v = y} (\dots)$, где $(\dots)$ не зависит от y. Тогда можно записать одну сумму вместо двух:

  $$\sum_{y \circ z = x} \sum_{u \circ v = y} (f(u) \cdot g(v)) \cdot h(z) = \sum_{(u \circ v) \circ z = x} (f(u) \cdot g(v)) \cdot h(z)$$

  Теперь, воспользовавшись ассоциативностью X:

  $$\sum_{(u \circ v) \circ z = x} (f(u) \cdot g(v)) \cdot h(z) = \sum_{u \circ (v \circ z) = x} f(u) \cdot (g(v) \cdot h(z))$$

  После этого осталось пройти весь путь в обратном порядке:

  $$\sum_{y \circ (u \circ v) = x} (f(u) \cdot g(v)) \cdot h(z) = \sum_{y \circ z = x} \sum_{u \circ v = z} f(y) \cdot (g(u) \cdot h(v))$$

  Наконец:

  $$\sum_{y \circ z = x} \sum_{u \circ v = z} f(y) \cdot (g(u) \cdot h(v)) = \sum_{y \circ z = x} f(y) \left(\sum_{u \circ v = z} g(u) \cdot h(v) \right) = \sum_{y \circ z = x} f(y)(g*h)(z) = (f*(g*h))(x)$$

□

δ-функция, символ Кронекера, определяется так: $\delta_x : X \to R$ для любых $x \in X$.

$$\delta_x(y) = \delta_{x,y} = \begin{cases} 1, & x = y \\ 0, \text{иначе} \end{cases}.$$

δ_1 является единицей относительно свёртки:

$$(\delta_1 * f)(x) = \sum_{y \circ z = x} \delta_1(y) f(z) = f(x)$$

Определение 1.8.1 (Полугрупповое кольцо (алгебра))**.** Так построенное кольцо

$$R[X] = \left\{ \sum_{i=1}^{n} a_i \delta_{x_i} \middle| n \in \mathbb{N}_0, a_i \in R, x_i \in X \right\}$$

1.8.1 Примеры

- Так, кольцо многочленов $R[x] = R[\mathbb{N}_0]$.
- Многочлены Лорана $R[\mathbb{Z}] = R[x, x^{-1}]$.
- Кольцо формальных степенных рядов $R[[x]]$ не подходит под определение, надо ослабить определение конечности носителя.

1.8.2 Расширенная полугрупповая алгебра

Определение 1.8.2 (Расширенная полугрупповая алгебра)**.** Пусть X — полугруппа, в которой уравнение $y \circ z = x$ для любого $x \in X$ имеет конечное число решений в $X \times X$. Определим $R[[X]] = R^X$.

Это всё ещё более сильное, чем необходимо, условие, оно позволяет определять формальные степенные ряды $R[[x]]$, но не позволяет — ряды Лорана, конечные в одном (отрицательном) направлении $R((x))$.

Теорема 1.8.2. $R[[X]]$ — ассоциативное кольцо.

Если X — моноид, то $R[[X]] \ni 1$.

Если X — коммутативно, то $R[[X]]$ коммутативно.

$R[[\mathbb{N}_0]] = R[[x]]$.

1.8.3 Многочлены и все-все-все

Трудно формализуемое школьное определение: Выражения типа $a + a_1 x + \cdots + a_n x^n$. Это суммы $\sum_{i=0}^{n} a_i x^i$.	По-другому многочлены можно определить, как последовательность его коэффициентов $(a_0, a_1, \dots)$, где $a_i \in R$ и почти все (кроме конечного числа) коэффициенты $a_i = 0$.	А мы их определяем, как $R[\mathbb{N}_0]$. Это функции $f : \mathbb{N}_0 \to R$, имеющие конечный носитель, неравные нулю в конечном количестве точек. Значит, записываются $f = \sum_{i=0}^{n} a_i \delta_i$.
Здесь при умножении $x^i \cdot x^j = x^{i+j}$. Используются правила ассоциативности, коммутативности, дистрибутивности.	$f + g = (a_0 + b_0, a_1 + b_1, \dots)$ $f \cdot g = (a_0 b_0, a_1 b_0 + a_0 b_1, \dots)$.	Здесь $\delta_i * \delta_j = \delta_{i+j}$. $R[x]$ является кольцом.
Описание стандартных мономов: $1, x, x^2, \dots$	Описание стандартных мономов: $(1, 0, 0, \dots), (0, 1, 0, \dots), \dots$.	Описание стандартных мономов: $\delta_0, \delta_1, \delta_2, \dots$

Получили изоморфизм!

Рассмотрим многочлен $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in R[x]$. Рассмотрим функцию $\tilde{f} : R \to R$; $\tilde{f}$ — значение f в точке c, $f(c) = a_0 + a_1 c + \cdots + a_n c^n$. Подстановка вместо символа x, некоего

элемента кольца $c \in R$ интерпретирование перемножения и возведения в степень, как внутри R. Подстановка значения является гомоморфизмом для коммутативного кольца.

$f = (a_0, a_1, \dots, \underbrace{a_m}_{\neq 0}, 0, \dots, 0, \dots)$, где $\deg f \stackrel{def}{=} n$ — степень многочлена. Если многочлен нулевой, то есть $\forall i : a_i = 0$, то степень — дискуссионный вопрос, можно определить, как $-\infty$.

Все-все-все

- Кольцо формальных степенных рядов $R[[x]]$ — как многочлены, только не требуется конечность носителя. $f = (a_0, a_1, a_2, \dots), a_i \in R$, или же $f = a_0 + a_1 x + a_2 x^2 + \dots$. Степенные ряды являются своеобразным *пределом линейных комбинаций*, так как линейная комбинация — конечная сумма.

  Порядок — аналог степени. Индекс первого ненулевого коэффициента $f = (0, \dots, 0, \underbrace{a_m}_{\neq 0}, a_{m+1}, \dots)$,

  здесь $\operatorname{ord} f \stackrel{def}{=} m$.

- Многочлены Лорана $R[x, x^{-1}]$. $f = \underbrace{a_m}_{\neq 0} x^m + \dots + \underbrace{a_n}_{\neq 0}$. Здесь m — порядок, а n — степень.

  Формальнее, последовательность коэффициентов, среди которых только конечное количество ненулевых. $(\dots, a_{-2}, a_{-1}, a_0, a_{-1}, a_{-2}, \dots)$.

- Формальные ряды Лорана $R((x))$ — вправо бесконечны (полубесконечны, так как только вправо), влево — конечны, хотя и сколь угодно много. Последовательность коэффициентов, среди которых начиная с некоторого места, все коэффициенты левее равны нулю. $(\dots, a_{-2}, a_{-1}, a_0, a_{-1}, a_{-2}, \dots)$.

  Аналогичная конструкция — полубесконечные влево ряды Лорана — $R((x^{-1}))$.

  $R[x, x^{-1}] = R((x)) \cap R((x^{-1}))$.

Лекция XIII

19 октября 2022 г.

1.9 Матрицы

1.9.1 Матрицы и их части

Пусть I, J — индексные множества. X — множество.

Определение 1.9.1 (Матрица типа (I, J) с коэффициентами из X)**.** Семейство $x : I \times J \to X$.

Определение 1.9.2 (Семейство)**.** Отображение с ослабленным сравнением на равенство: два семейства равны, если их области значений равны, и равны значения в каждой точке. Не требуется равенства области значений, матрицы $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ и $\begin{pmatrix} 1.0 & 2.0 & 3.0 \\ 4.0 & 5.0 & 6.0 \end{pmatrix}$ равны.

Множество всех матриц с данными характеристиками обозначают $M(I, J, X)$.

Записывают $(i, j) \mapsto x_{i,j}$, где $x = (x_{i,j})_{i \in I, j \in J}$, $x_{i,j}$ — матричный элемент.

Здесь I — множество строчных индексов, J — множество столбцовых индексов.

Определение 1.9.3 (Квадратная матрица)**.** Матрица x — квадратная, если $I = J$. Тогда $x = (x_{i,j})_{i,j \in I}$. Обозначается $M(I, X)$.

Предостережение. В определении квадратной матрицы недостаточно условия $|I| = |J|$.

Замечание. Для конечных множеств I и J часто используют натуральную индексацию: $I = \{1, 2, \ldots, n\}; J = \{1, 2, \ldots, m\}$, где $n = |I|, m = |J|$.

В таком случае матрицы $M(I, J, X)$ записываются $M(n, m, X)$. Также пишут $(x_{i,j})_{1 \le i \le n, 1 \le j \le m}$. Здесь (n, m) — размер матрицы $n \times m$. Если такие матрицы квадратные, то их записывают $M(n, X)$. Тут n называется порядком, или степенью.

Как программист, я вижу сразу два преимущества французской натуральной нумерации столбцов и строк матриц: $I = \{0, \ldots, n-1\}; J = \{0; \ldots, m-1\}$.

Во-первых, в таком случае не надо переопределять $M(n, X)$, *так как* $n \stackrel{def}{=} \{0, \ldots, n-1\}$. *Впрочем, понятно, что определив натуральные числа так в теории множеств, мы бы хотели об этом забыть, так что, возможно, я и не прав.*

Во-вторых, мне просто привычнее нумеровать с нуля, причём в некоторых местах эта нумерация выглядит сильно более разумной.

Матрицы с одной строкой отождествляются с горизонтальным вектором — строкой.
$M(1, m, X) = {}^m x$. Также пишут $\begin{pmatrix} x_1, \ldots, x_m \end{pmatrix}$.

Матрицы с одним столбцом отождествляют с вертикальным вектором — столбцом.
$M(n, 1, X) = x^n$. Также пишут $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Определение 1.9.4 (Строка матрицы)**.** Для $i \in I$ i-й строкой матрицы x является строка $x_{i,*} = \begin{pmatrix} x_{i,1} & \ldots & x_{i,m} \end{pmatrix}$, то есть сужение x как отображения на область определения $\{i\} \times J \subset I \times J$.

Определение 1.9.5 (Столбец матрицы)**.** Для $j \in J$ j-м столбцом матрицы x является столбец $x_{*,j} = \begin{pmatrix} x_{1,j} \\ \ldots \\ x_{n,j} \end{pmatrix}$, то есть сужение x как отображения на область определения $I \times \{j\} \subset I \times J$.

Матрицы можно рассматривать, как столбец, составленный из строк, или как строка, составленная из столбцов.

$$x = \begin{pmatrix} x_{*,1} & \ldots & x_{*,m} \end{pmatrix} = \begin{pmatrix} x_{1,*} \\ \vdots \\ x_{n,*} \end{pmatrix}.$$

Здесь знак равенства значит, что существует каноническая (общепринятая) биекция между этими штуками. Прямого равенства не наблюдается:

$$\begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} x_{1,1} & x_{1,2} \end{pmatrix} \\ \begin{pmatrix} x_{2,1} & x_{2,2} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} x_{1,1} \\ x_{2,1} \end{pmatrix} & \begin{pmatrix} x_{2,1} \\ x_{2,2} \end{pmatrix} \end{pmatrix}$$

Определение 1.9.6 (Главная диагональ квадратной матрицы $x \in M(I, X)$)**.** Строка $(x_{i,i})_{i \in I}$.

Определение 1.9.7 (Побочная диагональ квадратной матрицы с натуральной индексацией)**.** Для матрицы $x \in M(n, X)$ это строка $(x_{i,j})_{i+j=n+1}$.

Определение 1.9.8 (Подматрица)**.** Пусть $x \in M(I, J, X)$. Пусть $K \subset I, L \subset J$. Подматрицей x является матрица $(x_{i,j})_{i \in K, j \in L}$. Она является элементом $M(K, L, X)$.

Так, подматрицей $x \in M(3, 4, X)$ для $x = \begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} \end{pmatrix}$ для $K = \{1, 3\}$ и $L = \{2, 3\}$ является матрица $\begin{pmatrix} x_{1,2} & x_{1,3} \\ x_{3,2} & x_{3,3} \end{pmatrix}$

1.9.2 Матрицы с элементами из кольца

Для ассоциативного кольца с единицей R рассмотрим множество матриц $M(m,n,R)$. Пусть $x,y \in M(n,m,R)$.

Определение 1.9.9 (Сумма матриц)**.** $x+y$ — сумма матриц, определена как матрица

$$z \in M(n,m,R), (z_{i,j}) = (x_{i,j} + y_{i,j})$$

Замечание. От R достаточно требовать не структуры кольца, а всего лишь структуры аддитивной абелевой группы.

Лемма 1.9.1. *Для аддитивной абелевой группы* $A : M(n,m,A) \cong A^{mn}$.

Доказательство. Сложение определено покомпонентно. □

Определение 1.9.10 (Умножение на скаляр)**.**

$$\lambda \cdot x = (\lambda x_{i,j}) \text{ — умножение на скаляр слева}$$

$$x \cdot \lambda = (x_{i,j} \cdot \lambda) \text{ — умножение на скаляр справа}$$

Умножение матриц

Замечание. С одной стороны, матрица — линейное отображение. Умножение матриц — композиция этих отображений. С другой стороны, умножение матриц — свёртка.

Рассмотрим две матрицы $x \in M(I,J,R)$ и $y \in M(J,K,R)$, причём $|J| < +\infty$.

Определение 1.9.11 (Произведение матриц)**.** $x \cdot y \in M(I,K,R)$.

$$(x \cdot y)_{i,k} = \sum_{j \in J} x_{i,j} \cdot y_{j,k}$$

Рассмотрим конечные матрицы, проиндексированные натуральными числами $x \in M(l,m,R)$ и $y \in (m,n,R)$.

Интерпретации произведения матриц:

1. Умножение матриц в терминах строк и столбцов: $(x \cdot y)_{i,k}$ — произведение i-й строки x и k-го столбца y.

   $$\begin{pmatrix} x_1 & \dots & x_m \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = x_1 y_1 + \dots + x_m y_m$$

   $(x \cdot y)_{i,k} = x_{i,*} \cdot y_{*,k}$.

2. Для нахождения части произведения, необязательно вычислять всё произведение целиком.

   $$(x \cdot y)_{*,k} = x \cdot y_{*,k}$$

   $$(x \cdot y)_{i,*} = x_{i,*} \cdot y$$

   Замечание. Пусть a,b,c — матрицы, причём a,b — квадратные, а c — столбец. Так как произведение матриц ассоциативно (1.9.3), то вычислительно намного выгоднее считать $a \cdot (b \cdot c)$, чем $(a \cdot b) \cdot c$. Если обозначить размер этих матриц за n, то асимптотика первого способа будет $\mathcal{O}(n^2)$, а второго — $\mathcal{O}(n^3)$.

3. Произведение столбца на строку:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_l \end{pmatrix} \cdot \begin{pmatrix} y_1 & \dots & y_n \end{pmatrix} = \begin{pmatrix} x_1y_1 \dots & x_1y_n \\ \vdots & \ddots & \vdots \\ x_ly_1 \dots & x_ly_n \end{pmatrix}$$

Получилось внешнее произведение, outer tensor.

Определение 1.9.12 (Стандартная матричная единица)**.** $e_{i,j} = (e_{x,y})$, где $e_{x,y} = \begin{cases} 1, & (x,y) = (i,j) \\ 0, & (x,y) \neq (i,j) \end{cases}$.

Иными словами, матрица нулей, где только элемент на пересечении i-й строки и j-го столбца равен 1.

Тогда получается

$$xy = x(e_{1,1} + \dots + e_{m,m})y = x_{*,1}y_{1,*} + \dots + x_{*,m}y_{m,*}$$

Свойства произведения матриц

1. Пусть $x \in M(a,b,R)$, $y \in M(b,c,R)$, $z \in M(c,d,R)$.

   Тогда $xy \in M(a,c,R)$, а $yz \in M(b,d,R)$.

   Отсюда $(xy)z$ и $x(yz)$ — матрицы равного размера.

   Более того, $(xy)z = x(yz)$, они равны (1.9.3).

   Лемма 1.9.2. *Умножение матриц строго ассоциативно: если одно из $(xy)z$ и $x(yz)$ определено, то определено и другое, причём они равны*

2. Коммутативность не выполняется.

   Более того, если xy определено, то совсем необязательно yx определено. В общем случае для $x \in M(l,m,R)$ и $y \in M(m,n,R)$ это действительно так. Или даже они могут быть оба определены, но иметь разные размеры. Так, для $x \in M(n,m,R)$ и $y \in M(m,n,R)$: $xy \in M(n,R)$ и $yx \in M(m,R)$.

   Легко можно построить пример не коммутирующих матриц из $M(2,X)$:

   Лемма 1.9.3. $e_{i,j_1} \cdot e_{j_2,k} = \delta_{j_1,j_2} \cdot e_{i,k}$.

   Используя лемму, видим некоммутативность умножения матриц $M(2,R)$: Здесь $e_{1,1} \cdot e_{1,2} = e_{1,2}$ и $e_{1,2} \cdot e_{1,1} = 0$.

3. Нулевая матрица $0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$.

4. Единичная матрица $e = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$. Единицы на главной диагонали.

5. Проединичная матрица $\begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$. Является единичной для покомпонентного умножения по Шуру или Адамару.

Лекция XIV

20 октября 2022 г.

1.9.3 Умножение матриц в терминах матричных единиц

Рассмотрим квадратные матрицы.

Матричные единицы — множество $\{e_{i,j}\}_{1\le i,j\le n}$. Их произведение $e_{i,j_1}\cdot e_{j_2,k} = \delta_{j_1,j_2}\cdot e_{i,k} = \begin{cases} e_{i,k}, & j_1 = j_2 \\ 0, & j_1 \neq j_2 \end{cases}$.

Чтобы получить полугруппу, добавим в множество матричных единиц δ_0, при умножении на любой элемент дающий δ_0.

$$S = \{e_{i,j} | 1 \le i,j \le n\} \cup \{\delta_0\}$$

Тогда хочется сказать, что $M(n,R) \cong R[S]$. Но это неправда, так как

$$R[S] = \sum_{1\le i,j\le n} x_{i,j}\cdot e_{i,j} + ?\cdot\delta_0$$

Есть дополнительный ненужный коэффициент.

Тогда профакторизуем по нему!

$$M(n,R) \cong R[S]/R[S]\,\delta_0$$

Теперь умножение матриц в терминах матричных единиц стало в точности свёрткой:

Выполняется формула

$$(x*y)_{i,j} = \sum_{(i,k)\circ(k,j)} x_{i,k}\cdot y_{k,j}$$

Здесь $(i,j_1)\circ(j_2,n) \stackrel{def}{=} \delta_{j_1,j_2}\cdot(i,n)$.

Для обобщения этого на неквадратные матрицы, что можно делать? Способ первый — дополнить матрицы нулями, увеличив их размеры, после чего умножить получившиеся квадратные «надматрицы».

Способ второй — обобщить понятие свёртки.

Настоящее определение свёртки

Вместо внутренней операции на полугруппах, введём внешнюю операцию: $\circ : Y\times Z \to X; \quad (y,z)\mapsto y\circ z$. Тогда свёрткой функций $f\in R^Y, g\in R^Z$ является функция $f*g\in R^X$, такая, что

$$(f*g)(x) = \sum_{y\in Y, z\in Z, y\circ z = x} f(y)\cdot g(z)$$

На неквадратных матрицах мы определяем операцию $\circ$ следующим образом:

$$\circ : (I\times J)\times(J\times K); \quad (i,j_1)\circ(j_2,k) = \begin{cases} (i,k), & j_1 = j_2 \\ 0, & j_1 \neq j_2 \end{cases}$$

Таким образом, определив умножение матриц в терминах матричных единиц, мы сделали умножение матриц свёрткой, и доказали его ассоциативность.

На этом введение в общую алгебру закончено.

Глава 2

Арифметика коммутативных колец

Предполагаем, что R — коммутативное ассоциативное кольцо с единицей; часто предполагается, что она к тому же область целостности.

2.1 Основные определения, связанные с делением

Определение 2.1.1 (Делимость: $x \mid y$ или $y \vdots x$)**.** $\exists z \in R : xz = y$. В некоммутативном случае нужно различать $xz = y$ и $zx = y$. Левые и правые делители, левые и правые кратные — это неудобно.

x — делитель y. y — кратное x.

2.1.1 Свойства

$$\forall x \in R : x \mid x$$
$$(x \mid y) \wedge (x \mid z) \Rightarrow x \mid (y + z)$$
$$(x \mid y) \wedge (y \mid z) \Rightarrow x \mid z$$
$$x \mid y \Rightarrow \forall z \in R : x \mid yz$$

Следствие. $\forall x \in R$, множество кратных — главный идеал Rx.

Определение 2.1.2 (Делители нуля)**.** $\{x \in R | \exists y \in R : y \neq 0 \wedge xy = 0\}$

Определение 2.1.3 (Делители единицы)**.** $\{x \in R | \exists y \in R : xy = 1\}$. В точности множество обратимых элементов, R^*.

Замечание. Делитель нуля не может быть делителем единицы, так как обратимые элементы при домножении на что-то не могут давать 0.

Определение 2.1.4 (Ассоциированные элементы $x, y \in R$)**.** $(x \mid y) \wedge (y \mid x)$. Пишут $x \sim y$.

Определение 2.1.5 (Собственный делитель y)**.** Такой $x \in R$, что $x \mid y$, но $y \nmid x$.

Лемма 2.1.1. *Для области целостности R:*

$$x \sim y \text{ в } R \iff \exists u \in R^*, x = uy$$

Доказательство. $x \sim y \iff \exists u, v \in R : \begin{cases} xu = y \\ yv = x \end{cases} \Rightarrow xuv = x \iff x(uv - 1) = 0$. Если $x = 0$, то лемма очевидна — $y = 0$. Иначе $uv = 1$. □

В области целостности есть возможность сокращать:

$$(xz \mid yz) \wedge (z \neq 0) \iff x \mid y$$

Факт.

- $x \mid y \iff Rx \supset Ry$.
- $x \sim y \iff Rx = Ry$.
- x — собственный делитель $y \iff Rx \supsetneq Ry$.

Тем самым, ассоциированность $x \sim y$ стала отношением эквивалентности.

Пример: $\mathbb{Z}$. Здесь $\mathbb{Z}^* = \{\pm 1\}$. Тогда $m \sim n \iff m = \pm n$.

2.1.2 Неприводимые и простые элементы кольца

Для области целостности R:

Определение 2.1.6 (Неприводимый элемент)**.** $x \in R \setminus \{0\}$, такой, что

$$(x \notin R^*) \wedge (\forall y, z \in R : yz = x \Rightarrow (\underbrace{y \sim x}_{\iff z \in R^*} \vee \underbrace{z \sim x}_{\iff y \in R^*}))$$

Эквивалентно тому, что x не представим, как произведение двух собственных делителей.

Множество неприводимых элементов $\mathrm{Irr}(R)$.

Определение 2.1.7 (Простой элемент)**.** $p \in R \setminus \{0\}$, такой, что

$$(p \notin R^*) \wedge (\forall x, y \in R : (p \mid xy \Rightarrow (p \mid x) \vee (p \mid y)))$$

Неприводимость, как и простота, выполняются для всех ассоциированных элементов одновременно.

Лемма 2.1.2. *$p \in R$ — простой $\iff$ Rp — простой идеал (то есть R/Rp — область целостности).*

Доказательство. Следует прямо из определений. □

Лемма 2.1.3. *В области целостности R любой простой элемент $p \in R$ неприводим.*

Доказательство. Для простого $p \in R$ предположим, что $p = xy$. Тогда $x, y \mid p$. С другой стороны, $p \mid xy$, но из простоты $p \mid x \vee p \mid y$. Отсюда $p \sim x$ или $p \sim y$ □

Определение 2.1.8 (Приводимый элемент x)**.** $(x \neq 0) \wedge (x \notin R^*) \wedge (x \notin \mathrm{Irr}(R))$.

Таким образом, все элементы разбиты на четыре группы:

- 0
- R^*
- $\mathrm{Irr}(R)$. Здесь содержатся простые (но множества, вообще говоря, не совпадают)
- Приводимые элементы.

В ситуации, когда все неприводимые элементы простые, выполняется основная теорема арифметики.

Лемма 2.1.4. *$x \in \mathrm{Irr}(R) \iff Rx$ — максимальный идеал среди <u>главных</u> идеалов в R.*

Доказательство. От противного: пусть $Rx \underbrace{\subsetneq}_{x \mid y \wedge x \not\sim y} Ry \underbrace{\subsetneq}_{y \notin R^*} R$. Но тогда $\exists z \in R : x = yz$. Отсюда z — собственный делитель x. □

Определение 2.1.9 (Нётерова область целостности)**.** Каждый идеал порождён конечным числом элементов.

Без этого условия очень неприятно — элемент может быть порождён произведением бесконечного числа простых, или даже просто все его делители сами по себе тоже составные.

2.1.3 gcd & lcm, НОД и НОК соответственно

greatest common divisor & least common multiple.

По-прежнему R — область целостности.

Пусть $x, y \in R$.

Определение 2.1.10 (Наибольший общий делитель gcd)**.** Элемент кольца $z \in R : (z \mid x) \wedge (z \mid y)$ и $\forall w \in R : (w \mid x) \wedge (w \mid y) \Rightarrow (w \mid z)$.

Иными словами, такой элемент z, что $Rz \supset Rx + Ry$, и Rz минимально по включению.

Факт. Наибольшие общие делители образуют класс ассоциированности. Таким образом, если пишут

$$\gcd(u, v) = \gcd(x, y)$$

то имеется в виду, что совпадают классы ассоциированности.

$\gcd(x, y)$ обязательно существует в кольце главных идеалов PID (1.6.5): это элемент, порождающий идеал $Rx + Ry$.

Определение 2.1.11 (Наименьшее общее кратное, lcm)**.** Элемент кольца $z \in R : (x \mid z) \wedge (y \mid z)$ и $\forall w \in R : (x \mid w) \wedge (y \mid w) \Rightarrow (z \mid w)$.

Иными словами, такой элемент z, что $Rz \subset Rx \cap Ry$, и Rz максимально по включению.

Факт. Наименьшие общие кратные образуют класс ассоциированности. Таким образом, если пишут

$$\operatorname{lcm}(u, v) = \operatorname{lcm}(x, y)$$

то имеется в виду, что совпадают классы ассоциированности.

Предостережение. gcd, как и lcm совсем не обязательно существуют. Более того, не исключено, что существует только один из них.

Разумеется, lcm, как и gcd существует в PID.

Лекция XV

25 октября 2022 г.

Определение 2.1.12 (gcd-кольцо)**.** Область целостности R, такая, что для $\forall x, y \in R : \exists \gcd(x, y)$.

Предложение 2.1.1. *Любое* gcd*-кольцо является* lcm*-кольцом.*

Кольца главных идеалов $\subseteq$ факториальные кольца $\subseteq$ gcd-кольца

В основном будем изучать факториальные кольца (2.5.1).

Предостережение. Если $\exists \gcd(x, y), x, y \in R$, то совсем не обязательно $\exists \gcd(xz, yz), z \in R$.

Теорема 2.1.1 (Khurana)**.** $\exists \operatorname{lcm}(x, y) \iff \forall z \in R : \exists \gcd(xz, yz)$.

Контрпример (Обратное не верно). $\mathbb{Z}\left[\sqrt{-d}\right]$ для $d \geq 3$ — в этих кольцах найдутся x, y такие, что $\exists \gcd(x, y)$, но $\nexists \operatorname{lcm}(x, y)$.

2.1.4 Свойства gcd

1. $x \mid y \Rightarrow \gcd(x, y) = x$.
2. $\gcd(x, y) = \gcd(y, x)$
3. $\gcd(x, \gcd(y, z)) = \gcd(\gcd(x, y), z)$

Лемма 2.1.5. *Пусть $x, y, z \in R$, где R — область целостности.*

Если $\exists \gcd(xz, yz)$, то $\exists \gcd(x, y)$ и $\gcd(xz, yz) = z \cdot \gcd(x, y)$.

Доказательство. Если $z = 0$, то верна только та часть леммы, которая про равенство $\gcd(xz, yz) = z \cdot \gcd(x, y)$, причём она верна очевидным образом.

$(z \mid xz, yz) \Rightarrow z \mid \gcd(xz, yz) \Rightarrow \exists d \in R : d = \dfrac{\gcd(xz, yz)}{z}$. Утверждается, что здесь $d = \gcd(x, y)$. С одной стороны, несложно убедиться, что так как R — область целостности и $zd \mid xz, yz$, то $d \mid x, y$ (можно сокращать).

С другой стороны, рассмотрев все прочие делители получаем, что d порождает максимальный идеал:

$$\forall w \in R : (w \mid x, y) \Rightarrow (wz \mid xz, yz) \Rightarrow (wz \mid \gcd(xz, yz) = dz) \Rightarrow (w \mid d)$$

□

Теорема 2.1.2. Если $\exists \gcd(x, y)$ и $\exists \operatorname{lcm}(x, y)$, то $\gcd(x, y) \cdot \operatorname{lcm}(x, y) = xy$.

Доказательство. С одной стороны, $(x \mid x) \Rightarrow \left(x \;\middle|\; x \cdot \dfrac{y}{\gcd(x, y)}\right)$; получается,

$$\left(x, y \;\middle|\; \frac{xy}{\gcd(x, y)}\right) \Rightarrow \left(\operatorname{lcm}(x, y) \;\middle|\; \frac{xy}{\gcd(x, y)}\right)$$

С другой стороны, $(x \mid x) \Rightarrow \left(x \div \dfrac{\operatorname{lcm}(x, y)}{y} \;\middle|\; x\right)$; получается,

$$\left(\frac{xy}{\operatorname{lcm}(x, y)} \;\middle|\; x, y\right) \Rightarrow \left(\frac{xy}{\operatorname{lcm}(x, y)} \;\middle|\; \gcd(x, y)\right)$$

Отсюда видно, что $xy \mid \operatorname{lcm}(x, y) \cdot \gcd(x, y)$ и $\operatorname{lcm}(x, y) \cdot \gcd(x, y) \mid xy$, то есть они ассоциированы. □

2.1.5 gcd и lcm нескольких элементов

Для конечного множества $\{x_1, \ldots, x_n\}$

Определение 2.1.13 ($\gcd(x_1, \ldots, x_n) = d$)**.**

- $d \mid x_1, \ldots, x_n$.
- $z \mid x_1, \ldots, x_n \Rightarrow z \mid d$

Определение 2.1.14 ($\gcd(x_1, \ldots, x_n) = d$)**.**

- $x_1, \ldots, x_n \mid d$.
- $x_1, \ldots, x_n \mid z \Rightarrow d \mid z$

Факт. Если существуют gcd и lcm для пар, то они существуют и для произвольных конечных множеств.

Доказательство. Можно доказать по индукции. □

2.2 Взаимная простота и комаксимальность

Пусть R — область целостности.

Определение 2.2.1 ($x, y \in R$ взаимно просты)**.** $\exists \gcd(x, y); \gcd(x, y) = 1$, то есть все их общие делители обратимы.

Обозначается $x \perp y$.

Определение 2.2.2 (x, y комаксимальны)**.** $xR + yR = R$, то есть $\exists a, b \in R : ax + by = 1$.

Говорят, что пара (x, y) унимодальна.

Предостережение (Взаимная простота и комаксимальность — разные вещи). Рассмотрим поле многочленов $K[x, y]$. $\gcd(x, y) = 1$, так как у них нет общих делителей. С другой стороны, $xR + yR \neq R$ — это многочлены без свободного члена.

Факт. Как бы то ни было, $(xR + yR = R) \Rightarrow (\gcd(x, y) = 1)$.

2.2.1 Свойства взаимной простоты

1. $(x \perp y) \wedge (x \perp z) \Rightarrow (x \perp yz)$.

   Доказательство. Доказательство для gcd-колец:

   $$\gcd(x, yz) = \gcd(\gcd(x, xz), yz) = \gcd(x, \gcd(xz, yz)) = \gcd(x, \gcd(x, y) \cdot z) = \gcd(x, z) = 1$$

   □

2. $\forall i, j : x_i \perp y_j \Rightarrow \left(\prod_i x_i\right) \perp \left(\prod_j y_j\right)$

   Доказательство. Можно доказать по индукции. □

3. $x \perp y \Rightarrow x^n \perp y^m$

Для множества $\{x_1, \ldots, x_n\} \subset R$ различают понятия *попарной взаимной простоты* (всякая пара различных взаимно проста) и *взаимной простоты в совокупности* $\gcd(x_1, \ldots, x_n) = 1$.

Предостережение. Это не одно и то же

Это не одно и то же даже в кольце $\mathbb{Z} : \{6, 10, 15\}$ взаимно просты лишь в совокупности.

2.2.2 Свойства комаксимальности

Свойства комаксимальности и взаимной простоты схожи.

1. $xR + yR = xR + zR = R \;\Rightarrow\; xR + yzR = R$.

   Доказательство.

   $$\exists a, b, c, d \in R :$$
   $$ax + by = 1$$
   $$cx + dz = 1$$
   $$\text{Тогда: } 1 = (ax + by)(cx + dz) = (ac + adz + bcy)x + bd \cdot yz$$

   □

2. $xR + yR = R \Rightarrow x^n R + y^m R = R$

2.3 Совпадение неприводимости и простоты в кольцах главных идеалов

Примеры PID: (1.6.2).

Определение gcd и lcm: (2.1.3).

Ниже R — кольцо главных идеалов.

Лемма 2.3.1. *Пусть* $p \in \mathrm{Irr}(R). \forall x \in R : (p \not\mid x \Rightarrow pR + xR = R)$

Доказательство. Рассмотрим идеал $pR + xR$. Несложно видеть, что $pR + xR \gneq pR$. Но так как $pR + xR$ — главный (все главные), то из неприводимости p следует, что $pR + xR = R$. □

Теорема 2.3.1. Неприводимость и простота совпадают в PID

Доказательство. Из простоты неприводимость следует очевидным образом. Убедимся, что из неприводимости следует простота:

$$(p \in \mathrm{Irr}(R)) \wedge (p \mid xy) \wedge (p \not\mid x) \Rightarrow (\exists a, b : ap + bx = 1) \Rightarrow (apy + b \underbrace{xy}_{p \mid xy} = y) \Rightarrow (p \mid y)$$

□

Определение 2.3.1 (R — кольцо Безу)**.** Любой идеал, порождённый конечным числом элементов — главный.

Замечание. R — нётерово кольцо (2.1.9), если все идеалы в нём конечно порождены.

Отсюда PID — нётерово кольцо Безу (про пересечение непонятно, будет ли оно конечно порождено, но так как объединение конечно порождено, то $\exists lcm$, откуда всё-таки $\exists \gcd$).

Неприводимость и простота верны не просто в PID, а даже в кольцах Безу — легко убедиться, что нам требовалось только свойство идеала, порождённого двумя элементами, быть главным.

В кольцах Безу (в частности в PID) имеется линейное представление gcd.

Теорема 2.3.2. В кольце главных идеалов R для $x_1, \ldots, x_n \in R$ следующие условия эквивалентны:

1. $d = \gcd(x_1, \ldots, x_n)$.
2. $\left(d \;\middle|\; x_1, \ldots, x_n\right) \wedge \left(\exists a_1, \ldots, a_n \in R : \sum\limits_{i=1}^{n} a_i x_i = d\right)$.
3. $dR = x_1 R + \cdots + x_n R$.

Доказательство. Уже доказали, что (1) $\iff$ (3) и (1) $\Rightarrow$ (2). Для (2) $\Rightarrow$ (3) достаточно проверить, что если $z \mid x_1, \ldots, x_n$, то $\forall a_1, \ldots, a_n \in R : z \mid \sum\limits_{i=1}^{n} a_i x_i$. □

Следствие. В PID взаимная простота совпадает с комаксимальностью. Понятно, что комаксимальность всегда влечёт взаимную простоту (есть линейная комбинация, дающая 1), но верно и обратное.

Замечание. Нётеровость кольца по-другому: не бывает бесконечных строго возрастающих цепочек идеалов.

В нётеровых кольцах можно проводить *индукцию* (как? я не знаю), но в матанализе встречаются бесконечномерные кольца, не являющиеся нётеровыми, что — совсем другая сущность.

Более сильным условием (которое например не выполняется даже в $\mathbb{Z}$) является артиновость — условие обрыва бесконечных убывающих цепочек идеалов (контрпример: $p, p^2, p^3, \ldots$).

Лекция XVI

26 октября, 2022 г.

2.4 Нётеровы кольца, условие обрыва цепей

Конечные кольца являются нётеровыми, абелевыми, какими хотите (принцип Дирихле говорит, что конечные кольца являются *полными* (?)).

Определение: (2.1.9) Иными словами, $\forall I \trianglelefteq R : \exists x_1, \dots, x_n \in R : I = x_1R + \dots + x_nR$

2.4.1 Примеры

1. PID
2. Поле $K[x_1, \dots, x_n]$ (по теореме Гильберта о базисе).
3. $\mathbb{Z}[x_1, \dots, x_n]$ (по теореме Гильберта о базисе).
4. Кольцо многочленов $K[x_1, \dots, x_n, \dots]$ от бесконечного количества переменных нёторовым не является!

Замечание. Для некоммутативного кольца R различают нётеровы кольца слева и справа, они не связаны между собой.

В левых нётеровых кольцах любой левый идеал конечно порождён.

Двусторонние идеалы не рассматривают в некоммутативных кольцах, они слишком большие.

Однако обычно Нётеровость определяется в теории колец по-другому.

Рассмотрим цепочки идеалов.

Определение 2.4.1 (Цепочка идеалов)**.** Последовательность идеалов $\{I\}_{i \in \mathbb{N}}$.

Возрастающая цепочка идеалов: $I_i \trianglelefteq I_{i+1}$. Убывающая цепочка идеалов: $I_{i+1} \trianglelefteq I_i$.

Также различают строго возрастающие / убывающие цепочки.

Можно определить отдельно конечные цепочки ($0 \leq i \leq n$ для некоего n). Иногда будем считать, что это на деле бесконечная цепочка, стабилизующаяся начиная с некоторого места $\exists M : \forall i > M : I_i = I_M$.

Определение 2.4.2 (ACC (ascending chain condition, условие обрыва возрастающей цепочки))**.** Условие на кольцо: не существует бесконечной строго возрастающей цепочки $I_1 \trianglelefteqslant I_2 \trianglelefteqslant I_3 \dots$

Любая бесконечная возрастающая цепочка стабилизуется; начиная с некоторого места все элементы совпадают.

Теорема 2.4.1. Следующие условия эквивалентны:

1. R — нётерово кольцо
2. R удовлетворяет условию ACC.
3. Любое непустое множество идеалов имеет максимальный элемент.

Доказательство.

- (2) $\iff$ (3). Напрямую следует из леммы Куратовского-Цорна (леммы Цорна).
- $\neg(1) \Rightarrow \neg(2)$. Рассмотрим бесконечно порождённый идеал $I \neq \varnothing$. Рассмотрим $x_1 \in I$. Положим $I_1 = x_1R \trianglelefteqslant I$ (неравенство следует из того, что I — бесконечно порождён, и уж точно не мог оказаться порождённым одним элементов x_1).

  И так далее.

  На i-м шаге рассмотрим $I_i \trianglelefteqslant I$. Возьмём $x_i \in I \setminus I_i$. Положим $I_{i+1} = I_i \cup x_iR$.

Таким образом, мы найдём сколь угодно длинную строго возрастающую цепочку (стабилизующуюся сколь угодно поздно). Более того, всякую конечную цепочку, все элементы в которой являются подмножествами I, можно удлинить.

На этом месте возникло интересное замечание, что это доказательство, хотя и схоже с доказательством того, что во всяком бесконечном множестве есть счётное подмножество, но в отличие от последнего, использует обычную, а не трансфинитную индукцию. Для последней нужна аксиома выбора, а для обычной индукции —- не нужна. А именно, мы не утверждаем, что найдётся бесконечно возрастающая цепочка, мы лишь говорим, что всякую конечную цепочку (с элементами-подмножествами I) можно удлинить. Не уверен, что я это до конца осознал, но это очень интересно, я постарался записать услышанное без искажений.

- $(1) \Rightarrow (2)$. Рассмотрим бесконечную цепочку $I_1 \trianglelefteq I_2 \dots$, которая вдруг не стабилизировалась.

  Рассмотрим $I \coloneqq \left(\bigcup_{i\in\mathbb{N}} I_i\right) \trianglelefteq I$. То, что это идеал, очевидно:

  $$\forall x \in I_i, y \in I_j : (x+y) \in I_{\max(i,j)}; \quad \forall x \in I_i : Rx \subset I_i$$

  Таким образом I — идеал, причём из условия нётеровости, он конечно порождён: $I = x_1R + \dots + x_nR$.

  $$\forall 1 \le i \le n : \exists j(i) : x_i \in I_j(i); \qquad \text{рассмотрим } j = \max_{1\le i\le n} j(i)$$

  Несложно видеть, что $I = I_j$, противоречие, цепочка стабилизировалась. □

2.4.2 Теорема Гильберта о базисе

Теорема 2.4.2. Если R — нётерово кольцо, то $R[x]$ — нётерово кольцо.

Доказательство.

- Пусть $I \trianglelefteq R[x]$. Определим $\forall m \in \mathbb{N} : I_m \trianglelefteq R; \quad I_m = \left\{ f[x^m] \middle| f \in I \wedge \deg f = m \right\} \cup \{0\}$.

  Иными словами, $a \in I_m \iff \exists f \in I : f = ax^m + ? \cdot x^{m-1} + \dots$.

  Очевидно, что I_m — идеал (легко проверить, что сумма двух элементов из I_m лежит там же; что $\forall (c, f) \in R \times I_m : c \cdot f \in I_m$).

- Убедимся, что $I_1 \le I_2 \le \dots$ В самом деле, для $a \in I_m : \exists f \in I : f = ax^m + \dots$. Тогда $\forall n \in \mathbb{N} : (f \cdot x^n) \in I \Rightarrow a \in I_{n+m}$.

- Построенная цепочка стабилизируется, так как R — нётерово. $\exists m \in \mathbb{N} : I_m = I_{m+1} = \dots$.

- Построим конечную систему, порождающую исходный идеал I.

  Пусть I_i порождён старшими коэффициентами многочленов $\mathcal{F}_i \coloneqq \{f_{i,1}, \dots, f_{i,s_i}\}$ (многочленов степени i). Тогда определим множество $X = \bigcup\limits_{0\le i\le m} \mathcal{F}_i$. Оно содержит $\sum\limits_{0\le i\le m} s_i$ многочленов, страшно много.

  Утверждается, что X порождает I.

- По индукции, по n: многочлен степени n является линейной комбинацией многочленов $f \in X$ с коэффициентами из $R[x]$.

  – <u>База: $n \le m$</u> Утверждается, что f является линейной комбинацией многочленов $f \in X$ с коэффициентами даже просто из R. Здесь можно применить отдельную индукцию, докажем лучше от противного: пусть n — наименьшая степень многочлена $g \in I : g$ не порождается X.

  Но тогда по построению X можно породить многочлен со старшим коэффициентом, равным старшему коэффициенту g. Вычтем их, получим многочлен меньшей степени. Противоречие.

Очевидно, нулевой многочлен порождается X, например, как пустая линейная комбинация

– Шаг индукции: Абсолютно аналогично: рассмотрим $g \in I, n = \deg g > m$.

Рассмотрим многочлен h степени m, со старшим коэффициентом, равным старшему коэффициенту g. Домножим h на x^{n-m} и вычтем. Разность по индукции конечно порождена. □

Следствие. R нётерово $\Rightarrow R[x_1, \ldots, x_n]$ — нётерово. В частности,

- $K[x_1, \ldots, x_n]$ нётерово.
- $\mathbb{Z}[x_1, \ldots, x_n]$ нётерово.

Доказательство. Индукция по n, так как $K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$. □

2.4.3 Артиновы кольца

Определение 2.4.3 (Артиново кольцо)**.** Коммутативное кольцо R, удовлетворяющее условию DCC.

Определение 2.4.4 (Descending chain condition, условие брыва убывающих цепочек)**.** Не существует бесконечной строго убывающей цепочки $I_1 \supsetneq I_2 \supsetneq I_3 \ldots$

Замечание. Очевидно, в некоммутативном случае различают артиновы кольца слева и справа.

Существенное отличие артиновости от нётеровости состоит в том, что мы рассматриваем кольца с единицей.

Примеры

1. Любые конечные кольца, например, $\mathbb{Z}/n\mathbb{Z}$.
2. $\mathbb{Z}$ не является артиновым кольцом: $p\mathbb{Z} \supsetneq p^2\mathbb{Z} \supsetneq p^3\mathbb{Z} \ldots$

Теорема 2.4.3 (Частный случай теоремы Акидзуки–Хопкинса–Левицкого)**.** Артиново коммутативное кольцо $\iff$ нётерово кольцо размерности 0.

План доказательства данного частного случая

Определение 2.4.5 (Размерность Крулля Коммутативного кольца R)**.** Длина (за вычетом 1) строго возрастающей цепочки простых идеалов. Обозначается $\dim(R)$.

Так, $\sim (\mathbb{Z}/n\mathbb{Z}) = 0; \quad \dim(\mathbb{Z}) = 1; \dim(\mathbb{Z}[x]) = 2$.

Лемма 2.4.1. *В артиновых кольцах любой простой идеал максимален. Такие кольца называются нульмерными.*

Следствие. В области целостности всегда $\{0\} \trianglelefteq R$, поэтому артинова область целостности — поле.

Лемма 2.4.2. *В артиновом кольце конечное число максимальных идеалов. Такие кольца называются полулокальными.*

Лемма 2.4.3. *В артиновом кольце существует произведение необязательно различных максимальных идеалов, равное 0:*

$$\mathfrak{m}_1 \cdots \mathfrak{m}_s = \{0\}$$

Определение 2.4.6 (R локально)**.** В R единственный максимальный идеал.

Теорема 2.4.4 (Китайская теорема о остатках)**.** Артиново кольцо изоморфно прямой сумме локальных колец.

Существенность единицы в кольце

Контрпример. В $\mathbb{Z}$, как у группе по умножению, не выполняется DCC, но выполняется ACC.

В $c_p\infty$ — наоборот. $c_p\infty = \bigcup\limits_{m=1}^{\infty} \mu_{p^m}$, где μ_{p^m} — группа корней из единицы степени m.

На группе можно ввести структуру кольца, введя сложение, как в группе, и умножение, дающее в результате 0. Только такое кольцо будет без единицы.

В кольцах без единицы нётеровость и артиновость абсолютно аналогичны.

Лекция XVII

3 ноября 2022 г.

2.4.4 Разложение на неприводимые в нётеровых кольцах

Определение 2.4.7 ($x \in R \setminus \{0\}$ разложим на неприводимые множители)**.** x представим в виде $x = \prod\limits_{i=1}^{n} q_i$, где $q_i \in \mathrm{Irr}(R)$, $n \in \mathbb{N}_0$

Часто пишут $x = u \prod\limits_{i=1}^{N} q_i$, где $u \in R^*$.

Замечание. Условие довольно слабое, куда сильнее требование *единственности* этого разложения.

Лемма 2.4.4. *Для* $x \in R : (x \neq 0 \wedge x \notin R^*) \Rightarrow (\exists q \in \mathrm{Irr}(R) : q \mid x)$.

Доказательство.

- Либо $x \in \mathrm{Irr}(R)$, либо у x есть необратимый собственный делитель $x_1 \mid x$.

  Тогда $xR \subsetneq x_1R$.
- Либо $x_1 \in \mathrm{Irr}(R)$, либо $\exists x_2 : x_2 \notin R^*, x_2 \not\sim x_1, x_2 \mid x_1$.

  $xR \subsetneq x_1R \subsetneq x_2R \neq R$.
- ...

  Эта цепочка оборвётся на конечном шаге, мы нашли $x_m \mid x : x_m \in \mathrm{Irr}(R)$. □

Теорема 2.4.5. Любой элемент нётеровой области целостности $x \neq 0$ допускает разложение на неприводимые.

Доказательство.

- $x \in R^* \Rightarrow x = x$ — требуемое разложение.
- $x \in \mathrm{Irr}(R) \Rightarrow x = x$ — требуемое разложение.
- x приводим $\Rightarrow \exists q_1 \in \mathrm{Irr}(x) \wedge q_1 \mid x$. Заметим, что $q_1 \not\sim x \Rightarrow x = q_1x_1$.

  Если x_1 приводим, то $x = x_1q_1$ — требуемое разложение.

  Иначе можно продолжить цепочку, которая из-за нётеровости оборвётся. □

2.5 Факториальные кольца

Определение 2.5.1 (Факториальное кольцо, Unique Factorization Domain)**.**

Область целостности R, в которой $\forall x \in R : (x \neq 0 \wedge x \neq R^*) \Rightarrow$

$\exists$ разложение $x = u \prod\limits_{i=1}^{n} q_i$ при определённых q_i, u (2.4.7),

и для любых двух разложений $x = u \prod\limits_{i=1}^{n_1} p_i = v \prod\limits_{j=1}^{n_2} q_i$:

$$n_1 = n_2$$
$$\exists \pi \in S_{n_1} : p_i \sim q_{\pi_i}$$

Иными словами, разложение на множители всякого элемента единственно с точностью до порядка расположения множителей в произведении и ассоциированности.

Основная теорема арифметики, FTA, говорит, что данное кольцо факториально.

Так, основная теорема арифметики выполняется для $\mathbb{Z}, \mathbb{Z}[x], \ldots$

Предостережение. Не путать с основной теоремой *высшей* алгебры FTHA про корни многочленов.

Теорема 2.5.1 (Критерий факториальности)**.**

Нётерова область целостности факториальна $\iff$ множества неприводимых и простых элементов совпадают.

Доказательство.

$\Rightarrow$. Из простоты следует неприводимость. Проверим, что из неприводимости следует простота.

Рассмотрим $p \in \mathrm{Irr}(p)$. Пусть $p \mid xy$, где $x, y \neq 0$.

Отсюда $\exists z \in R : pz = xy$. Разложим x, y, z на неприводимые:

$$pu\text{ъ}_1 \ldots \text{ъ}_{n_1} = vp_1 \cdot \ldots \cdot p_{n_2} \cdot wq_1 \cdot \ldots \cdot q_{n_3}$$

Из единственности разложения $n_1 + 1 = n_2 + n_3$ и p ассоциирован с каким-то неприводимым делителем x или y.

Таким образом, p прост по определению.

$\Leftarrow$. В R существует разложение на неприводимые. Докажем, что оно единственно.

От противного: пусть $x = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$, $n, m > 0$ (при равенстве нулю $x \in R^*$ и доказывать нечего).

Пусть $n < m$. Найдём противоречие индукцией по n. p_n — простой $\Rightarrow p_n \mid q_1 \cdot \ldots \cdot q_m$. Так как q_i — неприводимые, то (без ограничения общности) $p_n \mid q_m$. Но q_m — неприводим, откуда $p_n \sim q_m$.

Сократим на p_n и q_m, получим совпадающие разложения для $n-1$ и $m-1$. □

Теорема 2.5.2. Всякое PID является факториальным кольцом.

Доказательство.

- PID — нётеровы кольца.
- В PID простота совпадает с неприводимостью. □

2.5.1 Примеры факториальных колец

- $K[x_1, \ldots, x_n]$
- $\mathbb{Z}[x_1, \ldots, x_n]$ — теорема Гаусса.

Замечание. Более полезным является свойство идеала быть представимым, как произведение простых идеалов. . .

2.5.2 Примеры не факториальных колец

- Конструкция с использованием факторкольца: $R = K[x,y,z]/(xy - z^2)$.

  А именно, $f \in K[x,y,z] \mapsto \overline{f} \in R, \overline{xy} = \overline{z}^2$. $\ldots \mathbb{Z}\left[\sqrt{-5}\right] \stackrel{def}{=} \left\{m + ni\sqrt{5} \middle| m,n \in \mathbb{Z}\right\}$. Так, $6 \in \mathbb{Z}\left[\sqrt{-5}\right]$;

$$6 = \left(\underbrace{1 + i\sqrt{5}}_{\neg(\vdots 2)}\right)\left(\underbrace{1 - i\sqrt{5}}_{\neg(\vdots 2)}\right)$$

- **Определение 2.5.2** ($\mathrm{Trig}_{\mathbb{R}}$)**.**

$$a_0 + \sum_{m=1}^{n}(a_m \cos(mx) + b_m \sin(mx)), \quad a_m, b_m \in \mathbb{R}$$

  $\mathrm{Trig}_{\mathbb{R}}$ — кольцо, произведение тригонометрических функций раскладывается в сумму.

  Определение 2.5.3 (Тригонометрическая степень)**.** Наибольший номер $m \in \mathbb{N}$: $a_m^2 + b_m^2 \neq 0 \iff a_m \neq 0 \wedge b_m \neq 0$.

  Обозначается $\mathrm{tdeg}(f)$.

  Лемма 2.5.1. $\mathrm{tdeg}(f \cdot g) = \mathrm{tdeg}(f) + \mathrm{tdeg}(g)$.

  Доказательство. Будем считать, что $m \geq n$.

$$\begin{aligned}(a_m \cos(mx) + b_m \sin(mx))(c_n \cos(nx) + d_n \sin(nx)) = \\ \frac{a_m c_n}{2}(\cos((m+n)x) + \cos((m-n)x)) + \\ \frac{b_m c_n}{2}(\sin((m+n)x) + \sin((m-n)x)) + \\ \frac{a_m d_n}{2}(\sin((m+n)x) - \sin((m-n)x)) + \\ \frac{b_m d_n}{2}(\cos((m-n)x) - \cos((m+n)x))\end{aligned}$$

  Коэффициенты перед $\sin((m+n)x)$ и $\cos((m+n)x)$ равны $\left(\frac{b_m c_n}{2} + \frac{a_m d_n}{2}\right)$ и $\left(\frac{a_m c_n}{2} - \frac{b_m d_n}{2}\right)$ соответственно. Заметим чудесную вещь:

$$\left(\frac{b_m c_n}{2} + \frac{a_m d_n}{2}\right)^2 + \left(\frac{a_m c_n}{2} - \frac{b_m d_n}{2}\right)^2 = \frac{1}{4} \cdot (a_m^2 + b_m^2)(c_n^2 + d_n^2)$$

  В данном произведении коэффициент перед хотя бы одним из $\sin((m+n)x)$ и $\cos((m+n)x)$ не ноль. Несложно видеть, что произведения множителей с остальными значениями n и m не меняют $\mathrm{tdeg}(f \cdot g)$. □

  Следствие. $\mathrm{Trig}_{\mathbb{R}}$ — область целостности.

  Следствие. $\mathrm{tdeg}\, f = 1 \Rightarrow f$ — неприводим.

  Следствие. $(\mathrm{Trig}_{\mathbb{R}})^* = \mathbb{R}^*$

  Теорема 2.5.3. $\mathrm{Trig}_{\mathbb{R}}$ не является факториальной областью целостности

  Доказательство.

$$\cos(x)^2 + \sin(x)^2 = 1$$
$$\cos(x)^2 = (1 - \sin(x))(1 + \sin(x))$$

  Получили два разных разложения на неприводимые множители... □

Замечание. Для решения этой проблемы надо расширить кольцо: $\mathrm{Trig}_{\mathbb{C}}$ уже является факториальной областью целостности.

Лекция XVIII

9 ноября 2022 г.

2.6 Каноническое разложение на простые. p-адический показатель

Рассмотрим факториальное кольцо R. В нём для $x \neq 0$: $x = up_1 \cdot \ldots \cdot p_n$, $u \in R^*, p_i \in \mathrm{Irr}(R)$.

Выберем по одному представителю в каждом классе ассоциированности неприводимых элементов. Так, для $R = \mathbb{Z}$ в качестве представителей выбираются положительные (простые) числа. Для $R = K[t]$ выбираются нормированные (унитальные) многочлены — со старшим коэффициентом 1.

Назовём $\overline{\mathrm{Irr}(R)}$ — множество канонических представителей простых (неприводимых) элементов.

Определение 2.6.1 (Каноническое разложение на простые)**.** Разложение $x = up_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$, где $u \in R^*, p_i \in \overline{\mathrm{Irr}(R)}$, все p_i — различны.

Здесь m_i — кратность (multiplicity) вхождения простого p_i в произведение.

Определение 2.6.2 (Для $p \in \mathrm{Irr}(R)$: p^m точно делит x)**.** $(p^m \mid x) \wedge (p^{m+1} \nmid x)$.

Записывают $p^m \| x$.

Определение 2.6.3 (Для $x \in R, x \neq 0, p \in \mathrm{Irr}(R)$: p-адический показатель x)**.** Ровно та степень, в которой p **точно** делит x: $p^{v_p(x)} \| x$. $v_p(x) \in \mathbb{N}_0$.

Замечание. Иногда записывают $v_p(0) = \infty$.

Теорема 2.6.1. $\forall x \in R \setminus \{0\} : x$ выражается в виде $x = u \prod\limits_{p \in \overline{\mathrm{Irr}(R)}} p^{v_p(x)}$.

Так как для фиксированного x все, кроме конечного числа, $v_p(x) = 0$, то записывают также $x = u \prod\limits_{i=1}^{n} p_i^{v_p(x)}$.

Следствие.

- $(x \mid y) \iff (\forall p : v_p(x) \leq v_p(y))$.
- $(x \sim y) \iff (\forall p : v_p(x) = v_p(y))$.
- $(d = \gcd(x, y)) \iff (\forall p : v_p(d) = \min(v_p(x), v_p(y)))$.
- $(m = \mathrm{lcm}(x, y)) \iff (\forall p : v_p(m) = \max(v_p(x), v_p(y)))$.
- $v_p(xy) = v_p(x) + v_p(y)$.
- $v_p(x + y) \geq \min(v_p(x), v_p(y))$.
- В *поле частных* $v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y)$.

Здесь были какие-то отвлечённые слова на тему рассмотрения какого-то определённого простого, продолжение параграфа я не берусь понимать. Как и о всё остальном, можно почитать в конспекте лектора. Можно построить абсолютную величину (p-адическую норму) $|x|_p = \dfrac{1}{p^{v_p(x)}}$. Будут выполняться свойства $|xy|_p = |x|_p |y|_p$; $|x + y|_p \leq |x|_p + |y|_p$ (на самом деле $|x + y|_p \leq \max(|x|_p, |y|_p)$ — ультраметрическое неравенство треугольника). $|1|_p = 1; |0|_p = 0$.

Расстояние в таком случае определяется $d_p(x, y) = |x - y|_p$.

По такой величине $\mathbb{Z}$ можно *пополнить* в топологическом смысле. А именно, рассмотреть последовательности Коши. Получатся p-адические числа $\mathbb{Z}_p$.

$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \middle| m, n \in \mathbb{Z}, n \neq 0, v_p(m) - v_p(n) \geq 0 \right\}$.

Вещи разные, пополнение континуально, а $\mathbb{Z}_{(p)}$ — счётно.

2.7 Евклидовы и квазиевклидовы кольца. Алгоритм Евклида

2.7.1 Евклидовы кольца

Определение 2.7.1 (Область целостности R — евклидово кольцо)**.** Существует функция $\delta : R \setminus \{0\} \to \mathbb{N}_0$, (можно считать, что $\delta(0) = -\infty$), такая, что

$$\forall x, y \in R : \exists q, r \in R : x = qy + r \text{ и } \begin{bmatrix} r = 0 \\ \delta(r) < \delta(y) \end{bmatrix}$$

где q — quotient — частное и r — remainder (residue) — остаток.

Замечание. В старых учебниках требовалось условие $(x \mid y) \Rightarrow (\delta(x) \leq \delta(y))$, но существование какой-то функции влечёт существование минимальной, для которой данное свойство верно.

Минимальная функция — функция следующего вида: $\delta(u) = 0$ для $u \in R^*$; $\delta(x) = 1$ для всех $x \notin R^*$, таких, что $\forall y : \exists u \in R^*, q \in R : y = qx + u$; дальше определяем числа нормы 2 и так далее, по индукции.

Примеры

- $R = \mathbb{Z} : \delta(x) = |x|$.
- $R = K[t] : \delta(f) = \deg(f)$.
- $R = \mathbb{Z}[i] : \delta(m + ni) = m^2 + n^2$ — здесь не утверждается, что норма — минимальна.

Теорема 2.7.1. R евклидово $\Rightarrow R$ — PID.

Доказательство. Пусть $I \trianglelefteq R$. Если $I = \{0\}$, то I — главный; иначе $i \neq 0]$, $\exists y \in I \setminus \{0\}$. Но тогда $\varnothing \neq \delta(I \setminus \{0\}) subset \mathbb{N}_0$. Отсюда в $\delta(I \setminus \{0\})$ есть наименьший элемент, пусть он достигается при y: $\forall x \in R \setminus \{0\} : \delta(y) \leq \delta(x)$.

Утверждается, что $\forall x \in R : y \mid x$. В самом деле, $x = qy + r$, где $r = x - qy$. Но $\delta(r) < \delta(y)$, а так как $r \in I$, то $r = 0$. □

Следствие. R — евклидово $\Rightarrow R$ — факториально.

2.7.2 Квазиевклидовы кольца

Определение 2.7.2 (Квазиевклидова область целостности)**.** Существует функция $\delta : R \times (R \setminus \{0\}) \to \mathbb{N}_0$, (можно считать, что $\delta(x, 0) = -\infty$), такая, что

$$\forall x, y \in R : \exists q, r \in R : x = qy + r \text{ и } \begin{bmatrix} r = 0 \\ \delta(y, r) < \delta(x, y) \end{bmatrix}$$

где q — quotient — частное и r — remainder (residue) — остаток.

Теорема 2.7.2. R — квазиеевклидово $\Rightarrow R$ — кольцо Безу (2.3.1).

Доказательство.

Алгоритм Евклида. Достаточно доказать, что любой идеал $I = Rx + Ry$ — главный.

Либо $y = 0$ и $I = Rx$, идеал — главный, либо уж $y \neq 0$, тогда $\exists q, r : x = qy + r$ и идеал $Rx + Ry = Ry + Rr$, но $\begin{bmatrix} \delta(y, r) < \delta(x, y) \text{ — повторяем алгоритм} \\ r = 0 \text{ — идеал главный} \end{bmatrix}$. □

Алгоритм Евклида

Пусть $x, y \in R$. Хотим найти $d \in R : xR + yR = dR$.

Если уж существует, то $d = \gcd(x, y)$.

Алгоритм Евклида ищет $\gcd(x, y)$, не раскладывая на множители:

$$\begin{aligned} x &= q_1 y + r_1 \quad \delta(y, r_1) < \delta(x, y) \\ y &= q_2 r_1 + r_2 \quad \delta(r_1, r_2) < \delta(y, r_1) \\ r_1 &= q_3 r_2 + r_3 \quad \delta(r_2, r_3) < \delta(r_1, r_2) \end{aligned}$$

Получаются все меньшие натуральные числа, в какой-то момент $\delta(r_i, r_{i+1}) = -\infty$, то есть r_{i-1} делится нацело на r_i.

Замечание. В Египте задолго до был известен алгоритм Евклида, где не делили, а вычитали из большего меньшее.

Замечание. Удобно в процессе работы алгоритма Евклида параллельно искать коэффициенты представления r_i, как линейной комбинации x и y.

Замечание. Можно потребовать даже ещё более слабое условие — $\delta(r_{m-1}, r_m) < \delta(x, y)$ после некоторого конечного числа делений с остатком ($m \in \mathbb{N}$) для заданной пары (x, y).

m-step Euclidean algorithm, где m задана для данного кольца. В процессе δ может расти, но должна существовать последовательность из m шагов, уменьшающая $\delta \in \mathbb{N}_0$.

Лекция XIX

10 ноября 2022 г.

Для $\mathbb{Z} : \forall x, y \in \mathbb{Z} : y \neq 0 \Rightarrow \exists! q, r \in \mathbb{Z} : (0 \leq q < y) \wedge (x = qy + r)$ В отсутствии предположения $0 \leq q$ получаем два разных возможных остатка с нормой δ меньше нормы y.

Факт. Есть ровно одно кольцо, в котором (есть норма, такая, что) деление с остатком даёт ровно один результат — кольцо многочленов одной переменной.

2.7.3 Деление многочленов с остатком

Пусть A — коммутативное кольцо с единицей. Рассмотрим кольцо многочленов $R = A[x]$.

Лемма 2.7.1. *Если $g = b_m x^m + \cdots + b_0 \in R$, такой, что $g \neq 0 \wedge b_m \in A^*$, то для любого $f \in R$ можно единственным образом разделить f на g с остатком.*

Доказательство.

Пусть $f = a_n x^n + \cdots + a_0$.

- Существование: Индукция по степени f.

  База: $\deg f < \deg g$. Здесь деление с остатком даст результат $q = 0$ и $r = f$.

  Шаг индукции: $\deg f \geq \deg g$. Рассмотрим $h = f - g \cdot \frac{a_n}{b_m} x^{n-m}$.

  $\deg h < \deg f$ (старшие коэффициенты сократились), поэтому $\exists q', r : h = q'g + r$. Положим $q = q' + \frac{a_n}{b_m} x^{n-m}$. Несложно видеть, что $f = qg + r$, деление с остатком завершено.

- Единственность:

  Свойства степени:

  1. $\deg(f + g) \leq \max(\deg(f), \deg(g))$ — равенство, если старшие коэффициенты не сокращаются.

2. $\deg(f \cdot g) \leq \deg(f) + \deg(g)$ — равенство в области целостности.

3. $\deg(f \circ g) \leq \deg(f) \cdot \deg(g)$ — равенство в области целостности.

4. ...

Более того, условие на принадлежность коэффициентов области целостности можно заменить условием того, чтобы хотя бы один из старших коэффициентов f или g не был делителем нуля.

В нашем случае старший коэффициент g обратим, поэтому он не является делителем нуля.

От противного: $f = q_1 g + r_1 = q_2 g + r_2$. Получаем $(q_q - q_2)g = r_2 - r_1$. В предположении $q_1 \neq q_2$ получаем противоречие, слева степень больше, чем справа.

□

Теорема 2.7.3. Для поля K кольцо $K[x]$ евклидово, причём при делении f на $g \neq 0$ частное и остаток единственны.

Доказательство. В поле старший коэффициент многочлена обязательно обратим. □

Рассмотрим расширение полей L/K *(знак не имеет ничего общего с факторгруппой, так записывают расширение полей, например,* $\mathbb{C}/\mathbb{R} \iff \mathbb{C} \supset \mathbb{R}$*.)*

В таком случае $K[x] \subset L[x]$.

Следствие (Независимость делимости от поля). Если $f, g \in K[x]$ и $f \mid g$ в $L[x]$, то $f \mid g$ в $K[x]$.

Доказательство. $\exists! h \in L[x] : f = gh$. С другой стороны, $\exists! q, r : f = qg + r$.

Так как в $L[x]$ результат деления единственен, то $r = 0$. □

Следствие. $K[x]$ — PID и $K[x]$ — UFD.

2.8 Основная теорема арифметики для многочленов

Определение 2.8.1 (Неприводимый над полем K многочлен $q \in K[x]$)**.** q неприводим, как элемент кольца $K[x]$: $\nexists h, g \in K[x] : q = gh \wedge \deg(g), \deg(h) < \deg(q)$.

2.8.1 Примеры неприводимых многочленов

Неприводимость верна для класса ассоциированности, будем рассматривать нормированные многочлены.

- Линейные многочлены $x - c$ неприводимы над любым полем.
- Неприводимость зависит от поля: $x^2 + 1$ неприводим как многочлен над $\mathbb{R}[x]$, но не как многочлен над $\mathbb{C}[x]$.

В связи с техническими неполадками, конспект (продолжение данной лекции) был частично утерян. Я попытался восстановить содержимое, но наверняка что-то упустил.

Определение 2.8.2 (Алгебраически замкнутое поле)**.** Поле, над которым множество неприводимых многочленов — множество линейных многочленов.

Теорема 2.8.1 (Основная теорема высшей алгебры, FTHA)**.** $\mathbb{C}$ алгебраические замкнуто.

Следствие. Над $\mathbb{R}$ неприводимы ровно те многочлены, которые либо линейны, либо второй степени с отрицательным дискриминантом.

Теорема 2.8.2 (Евклид)**.** Простых чисел в $\mathbb{Z}$ бесконечно много (Евклид формулировал, что их больше любого наперёд заданного числа).

Доказательство. Пусть простых чисел конечное число, $p_1, \ldots, p_n$. Рассмотрим $\forall I \subset \{1, \ldots, n\}$ (у Евклида $I = \varnothing$). Рассмотрим сумму

$$\prod_{i \in I} p_i + \prod_{i \notin I} p_i$$

Она равна хотя бы 2, но для любого простого $p \in \{p_i\} : p$ делит ровно одно из слагаемых, откуда сумма не делится ни на одно из простых $p_1, \ldots, p_n$. Противоречие. □

Замечание. Доказывать то, что простых чисел сколь угодно много, можно по-разному, но данное доказательство позволяет получить все простые, а не какое-то их бесконечное подмножество.

Над какими полями есть бесконечно много неприводимых многочленов? Это, очевидно, бесконечные поля — там линейных многочленов уже бесконечно много.

Но, вообще говоря, все.

Теорема 2.8.3 (Теорема Евклида на бис)**.** Над всяким конечным полем $\mathbb{F}_p$ сколь угодно много неприводимых многочленов (найдётся неприводимый многочлен сколь угодно высокой степени).

Доказательство. Пусть $q_1, \ldots, q_n$ — все неприводимые многочлены над $\mathbb{F}_p$. Рассмотрим суммы вида $(q_1 \cdot \ldots \cdot q_n)^m + 1$ для $m \in \mathbb{N}$. Таких сумм счётное количество, среди них обязательно найдётся необратимый элемент кольца $\mathbb{F}[x]$ (обратимых элементов кольца $|F[x]^*| = |F^*|$).

Такой необратимый элемент q не делится ни на один из ранее найденных. Значит, мы нашли новый неприводимый элемент кольца — либо сам q, либо его простой делитель. □

Некоторые сложные результаты из теории чисел

Теорема 2.8.4. До данного $n \in \mathbb{N}$ $\frac{n}{\ln n} + o(n)$ простых чисел.

Уточнение коэффициентов перед меньшими степенями n — сложная задача, затрагивающая самые разные области математики.

Теорема 2.8.5. В любой арифметической прогрессии $ai + b$, где a и b взаимно простые, есть бесконечно много простых.

Теорема 2.8.6. Более того, в любой арифметической прогрессии $ai + b$, где a и b взаимно простые, ряд $\sum\limits_{(p=ai+b) \wedge (p \in \mathbb{P})} \frac{1}{p}$ расходится.

Глава 3

Теория групп

Лекция XX
16 ноября 2022 г.

3.1 Подгруппа, порождённая множеством

Определение 3.1.1 (Подгруппа $H \leq G$)**.** $\forall h, g \in H : h^{-1}g \in H \overset{\text{здесь эквивалентно}}{\iff} \begin{cases} \forall g, h \in H : hg \in H \\ \forall h \in H : h^{-1} \in H \end{cases}$.

Действия с группами чаще всего будут пониматься в смысле «по Минковскому». Так,

$$XY \overset{def}{=} \{xy | x \in X, y \in Y\}; X^{-1} \overset{def}{=} \left\{x^{-1} \middle| x \in X\right\}$$

Определение 3.1.2 (Подгруппа в G, порождённая X)**.** Наименьшая по включению подгруппа в G, содержащая X.

X порождает H, X — множество образ H, $H = \langle X \rangle$.

Замечание. Она существует, как пересечение всех таких. Здесь мы пользуемся свойством, что пересечение семейства подгрупп — тоже подгруппа.

Это несложно проверить по определению: если элементы g, h принадлежат пересечению, то элемент $h^{-1}g$ тоже принадлежит пересечению, так как принадлежит всем пересекаемым подгруппам.

Пример: $S_n = \left\langle \left\{ (ij) \middle| 1 \leq i \neq j \leq n \right\} \right\rangle$ — симметрическая группа порождается множеством транспозиций.

Более того, $S_n = \left\langle \left\{ (ii+1) \middle| 1 \leq i < n \right\} \right\rangle$.

Предложение 3.1.1. $\langle X \rangle = \left\{ x_1^{\pm 1} \cdot \ldots \cdot x_n^{\pm 1} \middle| x_i \in X, n \in \mathbb{N}_0 \right\}$.

Доказательство.

- $\supset$ — очевидно, что все элементы из объявленного множества принадлежат $\langle X \rangle$.
- Для доказательства $\subset$ надо доказать, что $\left\{ x_1^{\pm 1} \cdot \ldots \cdot x_n^{\pm 1} \middle| x_i \in X, n \in \mathbb{N}_0 \right\}$ — подгруппа.

  Для двух произведений $x_1^{\pm 1} \cdot \ldots \cdot x_n^{\pm 1}$ и $y_1^{\pm 1} \cdot \ldots \cdot y_m^{\pm 1}$ надо проверить, что $\left(x_1^{\pm 1} \cdot \ldots \cdot x_n^{\pm 1}\right) \cdot \left(y_1^{\pm 1} \cdot \ldots \cdot y_m^{\pm 1}\right)^{-1}$ является словом из данного множества. В самом деле,

$$x_1^{\pm 1} \cdot \ldots \cdot x_n^{\pm 1} \cdot \left(y_1^{\pm 1} \cdot \ldots \cdot y_m^{\pm 1}\right)^{-1} = x_1^{\pm 1} \cdot \ldots \cdot x_n^{\pm 1} \cdot y_m^{\mp 1} \cdot \ldots \cdot y_1^{\mp 1}$$

□

В графе Кэли, где есть ориентированное ребро $h \to g$, помеченное x, если $g = hx$, условие того, что $G = \langle x \rangle$ равносильно тому, что граф Кэли для группы G с x-стрелками связен (слабо связен, по ребру можно пройти как в направлении стрелки, так и против).

3.1.1 Смежные классы по подгруппе

Пусть $H \leq G$ (H — подгруппа в G). Пусть $x \in G$ — некий элемент.

Определение 3.1.3 (Левый смежный класс G по H с представителем x)**.** $Hx \stackrel{def}{=} \{hx | h \in H\}$.

Определение 3.1.4 (Правый смежный класс G по H с представителем x)**.** $xH \stackrel{def}{=} \{xh | h \in H\}$.

Замечание. В Москве левые и правые смежные классы устроены наоборот.

Лемма 3.1.1. $\forall x, y \in G : \begin{bmatrix} Hx = Hy \\ Hx \cap Hy = \varnothing \end{bmatrix}$.

Доказательство. Пусть $Hx \cap Hy \neq \varnothing$, то есть $\exists z \in G : z = hx = gy$ для некоторых $g, h \in H$. Но тогда $y = g^{-1}hx$, откуда $Hy \subseteq Hx$. С другой стороны, $x = h^{-1}gy$, откуда $Hx \subseteq Hy$. □

Получается, разбиение на классы смежности является отношением эквивалентности.

Заметим, что $\forall x, y : Hx = Hy \iff \exists h, g \in H : hx = gy \iff xy^{-1} \in H$.

Определение 3.1.5 ($x \underset{H}{\equiv} y$, эквивалентность слева)**.** $Hx = Hy \stackrel{\text{здесь эквивалентно}}{\iff} xy^{-1} \in H$.

Определение 3.1.6 ($x \equiv_H y$, эквивалентность справа)**.** $xH = yH \stackrel{\text{здесь эквивалентно}}{\iff} x^{-1}y \in H$.

3.1.2 Смежные классы по подгруппе. Трансверсаль

Трансверсаль по-русски — система представителей смежных классов.

По особым просьбам подписчиков, по-немецки это будет Nebenklassenvertretersystem.

Определение 3.1.7 ($X \subseteq G$ — левая трансверсаль к $H \leq G$)**.** $\forall g \in G : \exists! x \in X : Hg = Hx$.

Из того, что трансверсаль — выбор одного представителя из каждого класса, сразу следует $G = \bigcup\limits_{g \in G} Hg = \bigsqcup\limits_{x \in X} Hx$.

При данном левом трансверсале X правым трансверсалем является, например, X^{-1}. В самом деле, $(Hx)^{-1} = x^{-1}H$.

Определение 3.1.8 (Фактормножество G по подгруппе H слева)**.** $\{Hg | g \in G\} = \{Hx | x \in X\}$.

Обозначается $H \backslash\!\!\backslash G$.

Предостережение. Не путать с разностью множеств $H \setminus G$.

Замечание. Вроде общепринятый наклон как-раз-таки практически совпадает с разностью множеств, что поделать. Я постарюсь придерживаться введённого мною обозначения, хотя вряд ли оно будет часто встречаться.

Определение 3.1.9 (Фактормножество G по подгруппе H справа)**.** $\{gH | g \in G\} = \left\{x^{-1}H \middle| x \in X\right\}$. Здесь X — из предыдущего определения, левая трансверсаль.

Обозначается $G \,/\!\!/ H$.

Таким образом, наблюдается естественное взаимно-однозначное соответствие между левыми и правыми фактормножествами (или их представителями).

3.2 Индекс подгруппы, теорема Лагранжа, теорема об индексе

Пусть $H \leq G$ (H — подгруппа в G).

Определение 3.2.1 (Индекс H в G)**.** $|G : H| = |G/H| = |H\backslash G|$ — порядок фактормножества G по H.

Порядки равны, так как есть взаимно-однозначное соответствие.

Обозначение $G : H$ в отрыве от $|\cdot|$ не используется.

Теорема 3.2.1 (Лагранж)**.** $|G| = |H| \cdot |G : H|$. При условии $|G| < \infty : |G : H| = {}^{|G|}/_{|H|}$.

Доказательство.

> **Лемма 3.2.1.** $\forall g \in G : |Hg| = |H|$
>
> *Доказательство леммы.*
>
> Очевидна биекция $hg \leftrightarrow h$. □

Так как $G = \bigsqcup\limits_{g \in X} Hg$, то $|G| = |X| \cdot |H|$ (множества G и $X \times H$ равномощны). □

Интересный факт (Кановей, Москва). Если не верить в аксиому выбора, а принять что-то другое, то можно доказать, что есть отношение $\sim$, такое, что $\mathbb{R} \prec \mathbb{R}/\sim$.

Следствие. В конечной группе G любая подгруппа H имеет порядок, являющийся делителем порядка G: $|H| \;\Big|\; |G|$.

Следствие. В G нет нетривиальных подгрупп, если $G \cong C_p$ — циклическая группа простого порядка.

Определение 3.2.2 (Порядок элемента $g \in G$)**.** $o(g) = |\langle g \rangle|$.

Следствие. $o(g) \;\Big|\; |G|$.

Следствие. $\langle g \rangle \cong C_n$ для некоего $n \in \mathbb{N}$, либо $\langle g \rangle \cong \mathbb{Z}$.

Интересный факт (Ольшанский А. Ю.). Можно построить группу бесконечного порядка, где каждый элемент имеет простой конечный порядок.

Теорема 3.2.2 (Об индексе)**.** Для $F \leq H \leq G : |G : F| = |G : H| \cdot |H : F|$.

Доказательство. Рассмотрим X — трансверсаль в G к H, Y — трансверсаль в H к F.

Докажем, что $X \times Y$ имеет мощность трансверсаля к F в G. Рассмотрим $\forall g \in G$.

$$Fg \subseteq Hg \Rightarrow \exists! x \in X : Hg = Hx$$

Все остальные $\tilde{x} \in X$ представляют смежные классы, не содержащие Fg.

Для такого x верно, что $gx^{-1} \in H$, то есть

$$\exists! y \in Y : Fgx^{-1} = Fy \Rightarrow Fg = Fyx$$

Получается, $|YX| \simeq |X \times Y| \simeq |G : F|$. □

Замечание. Теорема Лагранжа является частным случаем теоремы об индексе для $F = \{1\}$.

Лекция XXI

17 ноября 2022 г.

3.3 Теоремы Ферма и Эйлера

Для группы G по теореме Лагранжа $g^{|G|} = e$, или же $|\langle g\rangle| = o(g) \;\Big|\; |G|$. Отсюда сразу следуют теоремы Ферма (3.3.2) и Эйлера (3.3.1)).

Рассмотрим $R = \mathbb{Z}/m\mathbb{Z}$. Такому кольцу соответствует группа R^*.

Пусть $m = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$, где p_i попарно различны. По китайской теореме об остатках (1.6.6)

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_k^{n_k}\mathbb{Z})$$

Более того,

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{n_k}\mathbb{Z})^*$$

что вытекает из предыдущего равенства.

Определение 3.3.1 (Функция Эйлера числа m)**.** $\phi(m) \stackrel{def}{=} |(\mathbb{Z}/m\mathbb{Z})^*|$.

Лемма 3.3.1 (Мультипликативность функции Эйлера)**.** $\forall n \perp m : \phi(n \cdot m) \cdot \phi(n) \cdot \phi(m)$.

Доказательство. Вытекает из разложения n и m на примарные (степени простых). □

Замечание. При отсутствии условия $m \perp n$ в теории чисел аналогичное свойство называется *полная мультипликативность*.

Лемма 3.3.2. *В конечном кольце всякий элемент — либо делитель нуля, либо обратим.*

Доказательство. Принцип Дирихле.

Рассмотрим отображение $y \mapsto xy$ для некоего фиксированного x, не делителя нуля.

Оно инъективно, значит, оно сюръективно, значит, $\exists z : xz = 1$.

Дальше (не заметив очевидное решение $y \mapsto yx$), если в кольце $xz = 1$ и $zx \neq 1$, то можно построить бесконечную систему матричных единиц, (домножая $(zx - 1)$ на z, x слева и справа), что бы это ни значило (я не понял). □

Таким образом, $\phi(m) = \left|\left\{0 \le x < m, x \in \mathbb{N} \middle| x \perp m\right\}\right|$.

Лемма 3.3.3. $\phi(p^n) = p^n - p^{n-1} = p^n\left(1 - \frac{1}{p}\right)$

Доказательство. Видно из предыдущего равенства. □

В частности, $\phi(p) = p - 1$.

Теорема 3.3.1 (Эйлер)**.** $x \in \mathbb{Z} : x \perp m \Rightarrow x^{\phi(m)} \equiv 1 \pmod m$.

Теорема 3.3.2 (Ферма (малая))**.** $p \nmid x \Rightarrow x^{p-1} \equiv 1 \pmod p$.

Часто теорему Ферма формулируют $x^p \equiv x \pmod p$.

3.4 Нормальные подгруппы

Паре {кольцо — идеал} $I \trianglelefteq R$ сопоставляется факторкольцо R/I.

Паре {группа — нормальная подгруппа} $H \trianglelefteq G$ сопоставляется факторгруппа G/H.

Определение 3.4.1 (H — нормальная подгруппа в G)**.** $\forall x, y \in G : xy \in H \iff yx \in H$. Обозначается $H \trianglelefteq G$.

Лемма 3.4.1. *Следующие условия эквивалентны.*

1. $H \trianglelefteq G$
2. $\forall x \in G : Hx = xH$
3. ${}_H\equiv$ — *то же самое, что и* $\equiv_H$
4. $\forall x \in G : {}^xH = H$, *где* ${}^xH$ *по определению — левое сопряжённое* xHx^{-1}. *Можно было написать правое сопряжённое* $H^x = x^{-1}Hx$, *что одно и то же, так как* $\forall x \in G : x^{-1} \in G$.

Доказательство.

- (2) $\iff$ (3) просто по определению.
- (1) $\iff$ (3)
$$x\ {}_H\equiv\ y \iff Hx = Hy \iff xy^{-1} \in H$$
$$x \equiv_H y \iff xH = yH \iff y^{-1}x \in H$$
Осталось рассмотреть y вместо y^{-1}.
- (2) $\iff$ (4) $xH = Hx \iff H = xHx^{-1} = {}^xH$. □

3.4.1 Примеры нормальных подгрупп

- $\{1\} \trianglelefteq G; \quad G \trianglelefteq G$.

  Определение 3.4.2 (Простая группа G)**.** $G \neq \{1\}$ и в ней нет никаких нормальных подгрупп, кроме тривиальных — $\{1\}$ и G.

  Интересный факт (Галуа). Для $n \geq 5$ групп A_n проста. Группа A_n — группа чётных перестановок, $\mathrm{Ker}(\mathrm{sgn})$, если угодно, где $\mathrm{sgn} : S_n \to \{\pm 1\}$ — знак перестановки.

  Именно по этой причине уравнения степени 5 и выше не разрешимы в радикалах.

- В абелевой группе G любая подгруппа нормальна.

  Определение 3.4.3 (Центр группы G)**.** Множество элементов $C(G) = \{x \in G | \forall y \in G : xy = yx\}$.

  Замечание. $xy = yx \iff x$ и y коммутируют, или же коммутатор равен 1.

  Определение 3.4.4 (Коммутатор x, y). $[x, y] \stackrel{def}{=} xyx^{-1}y^{-1}$

  Иногда рассматривают правонормированный коммутатор $x^{-1}y^{-1}xy$.

  Несложно проверить, что $C(G) \trianglelefteq G$, $C(G)$ — абелева подгруппа.

  Любая *центральная подгруппа* $H \trianglelefteq C(G)$ нормальна.

- Существует ли неабелева группа, в которой все подгруппы — нормальные?

  Да, существует, и так как одна из них — Q_8, то такие группы называются *гамильтоновы*.

  В Q_8 существуют подгруппы $\{\pm 1\}, \{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}$, которые нормальны

- $|G : H| = 2 \Rightarrow H \trianglelefteq G$.

  В самом деле, $G = H \sqcup Hx$ для $\forall x \notin H$, откуда $Hx = G \setminus H$, но с другой стороны $xH = G \setminus H$, получается, $xH = Hx$.

  Задача 3.4.1 (Подумать)**.** *Если* p — *наименьший простой делитель* $|G|$, *то* $|G : H| = p \Rightarrow H \trianglelefteq G$.

  Замечание. A_5 — группа порядка $\frac{5!}{2} = 60$, но в ней нет элементов порядка 15, так как группа порядка 15 — одна с точностью до изоморфизма, циклическая. Но в группе A_5 максимальный порядок элемента — 5, даже 6, как в S_5 нет.

- Найдём подгруппу индекса 3, не являющуюся нормальной. Так как 3 должно быть не минимальным простым делителем порядка, то разумно взять $D_3 \cong S_3$.

  $G = S_3$. Рассмотрим $H = \langle (12) \rangle = \{e, (12)\}$.

$(13)H = \{(13), (123)\}$, но $H(13) = \{(13), (132)\}$.

Вообще говоря, пример можно обобщить: рассмотрим $S_{n-1} \leq S_n$.

А именно, $S_{n-1} = \left\{ \begin{pmatrix} 1 & \dots & n-1 & n \\ \dots & \dots & \dots & n \end{pmatrix} \right\}$. $|S_n : S_{n-1}| = n$, но S_{n-1} никогда не является нормальной. Например, $\pi \cdot S_{n-1} \neq S_{n-1} \cdot \pi$ при $\pi_n \neq n$ — в первом случае все перестановки σ таковы, что $\sigma_n = \pi_n$, во втором — σ_n принимает любое значение из $1, \dots, n-1$.

- $V \trianglelefteq A_4$ — «Фау», Vierergruppe, нормальная подгруппа в A_4.

  $A_4 = \Big\{ e, \underbrace{(12)(34), (13)(24), (14)(23)}_{V \cong C_2 \times C_2,\ \text{произведение независимых транспозиций}} \Big\} \cup \underbrace{\Big\{ (ijk) \Big| i < j \neq k; i, j, k \in \{1, 2, 3, 4\} \Big\}}_{\text{3-циклы}}$.

  Замечание. Для нахождения корней многочлена степени 4 сначала составляется кубический многочлен («кубическая резольвента»), корнями которого являются $x_1x_2 + x_3x_4, x_1x_3 + x_2x_4$ и $x_1x_4 + x_2x_3$.

Лекция XXII

23 ноября 2022 г.

3.5 Факторгруппа

Свяжем с $H \trianglelefteq G$ факторгруппу G/H. Для этого введём каноническую проекцию $\pi : G \to G/H$.

$G \diagup H = \{gH | g \in G\}$. Оно же с другим (?) слешом — фактормножество.

Вообще-то, слеш тот же самый, и вот почему:

3.5.1 Произведение классов

Можно определить разными способами, в обоих случаях возникают некоторые вопросики.

Определение через представителей

Определение 3.5.1 (Произведение смежных классов xH и yH)**.** $xH \cdot yH = xyH$.

Проверим, что определение корректно.

Лемма 3.5.1 (Корректность определения выше)**.** $\begin{cases} x_1H = x_2H \\ y_1H = y_2H \end{cases}$. *Проверим, что* $x_1y_1H = x_2y_2H$.

Таким образом, мы проверим, что сравнимость $\underset{H}{\equiv}$ *— конгруэнция (1.6.11).*

Доказательство. Значит, $\exists h \in H : x_1h = x_2$. Отсюда $x_2y_2H = x_1hy_2H = x_1(y_2y_2^{-1})hy_2H = x_1y_2 \underbrace{y_2^{-1}hy_2}_{\in H} H = x_1y_2H = x_1y_1H$.

Принадлежность следует из $H \trianglelefteq G$. □

Определение через произведение по Минковскому

Определение 3.5.2 (Произведение смежных классов $xH \cdot yH$)**.**

$$xH \cdot yH = \Big\{ (xh)(yg) \Big| h, g \in H \overset{\text{здесь эквивалентно}}{\iff} xh \in xH, yg \in yG \Big\}$$

Лемма 3.5.2. *Произведение смежных классов по нормальной подгруппе — смежный класс по нормальной подгруппе.*

Доказательство.

$xHyH = xy(y^{-1}Hy)H = xy(H \cdot H) = xyH$. Или даже проще, $x(Hy)H = x(yH)H = xyH$. □

Замечание. В общем случае $H \not\trianglelefteq G : xH \cdot yH$ равно объединению нескольких смежных классов, увы.

Таким образом, на G/H для $H \trianglelefteq G$ можно ввести операцию.

Теорема 3.5.1. Эта операция превращает G/H в группу.

Причём $\pi : G \to G/H; \quad x \mapsto xH$ является гомоморфизмом групп, таким, что $\operatorname{Ker}(\pi) = H$.

Доказательство.

$\pi(xy) = xyH = xHyH = \pi(x)\pi(y)$.

$x \in \operatorname{Ker}(\pi) \iff \pi(x) = 1_{G/H} = 1 \cdot H = H \iff xH = H \iff x \in H$. □

Определение 3.5.3 (Факторгруппа по **нормальной** подгруппе)**.** Так построенная группа G/H.

Пример.

- $\mathbb{Z}/m\mathbb{Z}$ — не только факторкольцо, но и факторгруппа по сложению.
- Вообще, в абелевой группе все подгруппы нормальны, существуют факторгруппы по любым подгруппам.
- В любой группе центр $\operatorname{Cent}(G) \trianglelefteq G$. Группа внутренних автоморфизмов $\operatorname{Inn}(G) \stackrel{def}{=} G/\operatorname{Cent}(G)$.
- *Определение* 3.5.4 (Коммутант группы G). $\langle\{[x,y] | x,y \in G\}\rangle$. Обозначается $[G;G]$. Здесь $[x,y]$ — коммутатор (3.4.4).

  Факт. Коммутант группы G нормален: ${}^g[x,y] = [{}^gx, {}^gy]$.

  Наибольшей абелевой подгруппы может не быть, но $G/[G;G] = G^{\text{ab}}$ — наибольшая абелева факторгруппа.
- Для группы кватернионных единиц $Q_8/\{\pm 1\} \cong V$. Здесь центр групп совпадает с коммутантом. $\operatorname{Cent}(Q_8) = [Q_8;Q_8] = \{\pm 1\}$.
- $\mathbb{R}^*/\{\pm 1\} \cong \mathbb{R}^*_{>0}$.
- $S_n/A_n \cong \{\pm 1\}$.

3.6 Теорема о гомоморфизме

Теорема 3.6.1 (О гомоморфизме)**.** Пусть $\phi : H \to G$ — гомоморфизм.

Образ гомоморфизма — подгруппа в G $\operatorname{Im}(\phi) \stackrel{def}{=} \phi(H) \leq G$.

Ядро — нормальная подгруппа: $\forall h \in H : \phi(hxh^{-1}) = \phi(h)\underbrace{\phi(x)}_{1}\phi(h)^{-1} = 1$.

Имеет место изоморфизм $\overline{\phi} : H/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$. Определим $\overline{\phi} : x\operatorname{Ker}(\phi) \mapsto \phi(x)$.

Доказательство.

- Проверим, что $\overline{\phi}$ определена корректно.

  Пусть $x\operatorname{Ker}(\phi) = y\operatorname{Ker}(\phi)$. Тогда $\overline{\phi}(x\operatorname{Ker}(\phi)) = \phi(x)$, но $\overline{\phi}(y\operatorname{Ker}(\phi)) = \phi(y)$.

  Однако равенство $x\operatorname{Ker}(\phi) = y\operatorname{Ker}(\phi)$ означает $\exists h \in \operatorname{Ker}(\phi) : xh = y$, откуда $\phi(y) = \phi(xh) = \phi(x)\phi(h) = \phi(x)$.

- Теперь остаток должен быть очевиден: $\overline{\phi}$ сюръективна: если $\phi(x) = y$, то $\overline{\phi}(x \operatorname{Ker}(\phi)) = y$.
- $\overline{\phi}$ инъективна: $\overline{\phi}(x \operatorname{Ker}(\phi)) = \overline{\phi}(y \operatorname{Ker}(\phi)) \iff \phi(x) = \phi(y) \iff \phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = 1 \iff xy^{-1} \in H \iff x \underset{H}{\equiv} y$.
- $\overline{\phi}$ — гомоморфизм, так как умножение классов может быть определено в терминах представителей. □

Следствие (Теоремы о соотвествии). • Подгруппы в $\operatorname{Im}(G)$ образуют взаимно-однозначное соответствие с подгруппами в H. содержащими $\operatorname{Ker}(\phi)$.

Для проверки изоморфизма сопоставим подгруппе $F \leq H \mapsto F/\operatorname{Ker}(\phi)$.

- Пусть $H_1 \trianglelefteq G_1$ и $H_2 \trianglelefteq G_2$. Если есть гомоморфизм $\phi : G_1 \to G_2$ такой, что $\phi(H_1) \leq H_2$, то имеет место гомоморфизм $\overline{\phi} = G_1/H_1 \to G_2/H_2$, факторизующий по подгруппам H_1 и H_2.

3.7 Теоремы об изоморфизме

•

Теорема 3.7.1 (Нётер об изоморфизме)**.** Пусть $F, H \leq G$, причём $H \trianglelefteq G$.

1. $FH \leq G$ — подгруппа.
2. $F \cap H \trianglelefteq F$ — нормальная подгруппа.
3. $FH/H \cong F/(F \cap H)$.

Доказательство.

Лемма 3.7.1. *Пусть $F \leq G, H \trianglelefteq G$. Тогда $\langle F, H\rangle = FH$*

Доказательство леммы.

Ясно, что $F, H \leq FH \leq \langle F, H\rangle \overset{def}{=} \langle F \cup H\rangle$.

Теперь осталось проверить, почему FH — подгруппа в G.

Так как $H \trianglelefteq G$, то $\forall f \in F : Hf = fH \Rightarrow HF = FH$.

Теперь заметим, что произведение любых двух элементов лежит в подгруппе $FH \cdot FH = F(HF)H = (FF)(HH) = FH$

и обратный к любому элементу лежит в подгруппе: $(FH)^{-1} = H^{-1}F^{-1} = HF$. □

1. Следует из леммы.
2. $\forall x \in F : x(F \cap H)x^{-1} = \underbrace{xFx^{-1}}_{x \in H} \cap xHx^{-1} = F \cap H$.
3. Построим гомоморфизм $\phi : F \to FH/H$. Положим $\phi : f \mapsto fH$ — элемент переходит в смежный класс.

   $\operatorname{Im}(\phi) = FH/H$, так как $\forall h \in H : fhH = fH$, но fh пробегает все значения из FH.

   $\operatorname{Ker}(\phi) = F \cap H$, так как $f \mapsto H \iff f \in H$. □