Алгебра. Неофициальный конспект

Лектор: Николай Александрович Вавилов

Конспектировал Леонид Данилевич

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 умножения

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

  Или же, что, как мне кажется, невозможно угадать:

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

  Предположив, что $\cdot$ некоммутативно:

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

- *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 $*$ дистрибутивна относительно $+$. 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 отображение $f \circ g : A \to C$; $\quad (f \circ g)(x) = f(g(x))$.

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.

База: $n \leqslant 2$ — всего один вариант расстановки скобок. $n = 3$ — определение ассоциативности.

Переход: 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) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \odot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a \cdot e & b \cdot f \\ c \cdot g & d \cdot h \end{pmatrix}$.
- 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 Моноид

- M1: Множество — 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 используют 1.

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

Примеры моноидов

Ниже указаны моноиды в виде $(\cdots, \cdots, \cdots)$ — запись *сигнатуры*. В сигнатуру моноида входит множество, операция, нейтральный элемент.

- $(\mathbb{N}, \cdot, 1)$.
- $(\mathbb{N}_0, +, 0)$.
- $X = 2^Y \quad (X, \cup, \varnothing) \quad (X, \cap, Y)$.
- Симметрический моноид: $(X^X, \circ, \mathrm{id}_X)$ – 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 $\iff \exists u \in X : u * z = z * u = e$. В таком случае 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. Запишем 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 $(X, *)$.

- $e \in X^*$.

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

Следствие 1.2.1. *X^* — группа обратимых элементов моноида X.*

1.3 Группы

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

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

- M1. $*$ ассоциативна
- M2. $\exists e \in G : (\forall x \in G :)\ e * x = x * e = x$.
- M3. 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: $(*, 1, x^{-1}) \rightsquigarrow (+, 0, -x)$

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

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).

Примеры (Группы).

- 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). $H \neq \varnothing; H \subset G : H$ 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 $(H \leqslant G) \iff (H$ — 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: $x^n = \begin{cases} e, & n = 0 \\ x^{n-1} * x, & n \geqslant 1 \end{cases}$.

  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: $x^n = \begin{cases} x^n, & n \geqslant 0 \\ \left(x^{-1}\right)^{-n}, & n < 0 \end{cases}$.

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

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

  Записывается S_3 следующим образом:

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

  В верхней строчке перечислены элементы X, в нижней, соответственно — их образы при применении данного элемента. Так, для перестановки p образ i обозначается $p(i)$ или p_i.

  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 $GL(n, R)$.

  В кольце матриц $M(n, R)$ существует нейтральный элемент: $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ в случае $M(2, R)$.

  $GL(n, R) \stackrel{def}{=} M(n, R)^*$ — 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, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

- Размер (мощность множества) конечной группы называют *порядком* группы.

  Как устроены группы маленьких (конечных) порядков?

  1. $|G| = 1$. Здесь $G = \{1\}$.
  2. **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.
  3. $|G| \in \mathbb{P}$. Существует только циклическая группа такого размера! $C_{|G|}$
  4. $|G| = 4$. 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 $(h_1, g_1) \cdot (h_2, g_2) = (h_1 h_2, g_1 g_2)$.

5. $|G| = 6$. 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.

6. $|G| = 8 \Rightarrow \ldots$. 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 $\leqslant 2000$ 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. $\exp : \mathbb{R}^+ \to \mathbb{R}^*_{>0}; \quad x \mapsto e^x$.

  Напоминание: $\mathbb{R}^+ = (\mathbb{R}, +, 0)$; $R^*_{>0} = (\mathbb{R}_{>0}, \cdot, 1)$.

- 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, например, не выполнятся ни для $\mathbb{Q}$, ни для $\mathbb{A}$.

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

  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:

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

  Интересный факт (Коан). $\mathbb{C}^* \cong \mathbb{T}$.

- 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: $(G, \cdot, 1, {}^{\complement})$. 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 $x*(y*z) = (x*y)*(x*z)$. Аналогично справа.

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 $x^2 = 0 \overset{\text{из раскрытия } (x+y)^2}{\Rightarrow} xy = -yx$.

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 ниоткуда.

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: $\forall x \in R \setminus \{0\} : \exists x^{-1} \in R : xx^{-1} = x^{-1}x = 1$

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 (**??**).
  - 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 Лорана $R[x, x^{-1}]$.
- Кольца матриц: $R \mapsto M(n, R), n \in \mathbb{N}$. Для $n \geqslant 2$ 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^o, построенное на R.

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

  Обозначается $(R^o, +, \circ)$.

  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 $R \cong R^o$.

  Тем не менее, $M(n, R) \cong M(n, R)^o$ 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 (**??**), и как и по всякому идеалу, по нему можно профакторизовать, получив структуру кольца (**??**).

  Рассмотрим здесь именно данную структуру, $\mathbb{Z}/m\mathbb{Z}$. Чтобы её построить, введём 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 $\left\{\{n + k \cdot m | k \in \mathbb{Z}\} \,\middle|\, 0 \leqslant n < m\right\}$, 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 (**??**).

- *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 вложения $\mathbb{F}_2 \hookrightarrow \mathbb{F}_4$.

  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 (**??**).

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 (**??**).
- Обратимость: рассмотрим $z = a + bi + cj + dk \neq 0$ — 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

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

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

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

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,

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

Интересный факт (Теорема Фробениуса). Единственными конечномерными (конечной размерности над $\mathbb{R}$) 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 (**??**). □

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)**.** $R^* \stackrel{def}{=} \{x \in R | x$ — обратим$\}$.

Примеры:

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

Замена свойству быть регулярным

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.

   Интересный факт. 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: $e_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$; $e_{2,1} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. 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.

Важный вопрос — есть ли в кольце прочие центральные идемпотенты (идемпотенты, лежащие в централизаторе кольца, то есть 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: особое отображение $f : G \to G$.

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

Пусть R — произвольная область целостности.

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

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. Произведение также можно определить 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 $\mathbb{Z} \to R$; $\quad n \mapsto n \cdot 1_R$ — 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 многочлены с коэффициентами из K, у которых ненулевые коэффициенты только перед x^{p^m} для некоего $m \in \mathbb{N}_0$.

Можно записывать $K[x^p]$, подразумевая, что K пополнено многочленом x^p, после чего взято замыкание относительно **композиции**.

Факт 1.5.1. *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 $I \trianglelefteqslant R$.

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 1.6.1. *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* (будет определён позднее) единица.

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.

Таким образом, в некоммутативном кольце двусторонний главный идеал, порождённый x, совсем не обязательно содержит только кратные x.

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): $\forall I \trianglelefteqslant R : \exists x \in R : I = Rx$ (фактически, такой x существует в I).

Примеры

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

  Доказательство. Рассмотрим $I \trianglelefteqslant \mathbb{Z}, I \neq \{0\}$. 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 $q \in \mathbb{Z}; 0 \leqslant r < m$. Отсюда $r = x - qm$, из замкнутости идеала по сложению и умножению на элементы кольца получается $r \in I$. Но m был наименьшим натуральным элементом идеала, значит, $r = 0$. $\square$

- $K[x, y]$ 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 $A, B \trianglelefteqslant R$.

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

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

Рассматриваем коммутативное кольцо R.

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

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

Определение 1.6.8 (Простой идеал)**.** Идеал $\mathfrak{p} \lhd R$ — 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 $\mathfrak{p} \lhd R$ простой* $\iff \forall A, B \trianglelefteqslant R : (AB \subseteq \mathfrak{p}) \Rightarrow (A \subseteq \mathfrak{p} \vee B \subseteq \mathfrak{p})$

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 $\mathfrak{m} \lhd R$. 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 $1 \in \mathfrak{m}$ и $\mathfrak{m}$ оказался несобственным. Противоречие. □

Замечание. Отсюда следует, что «максимальный спектр» кольца является «спектром» кольца.

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

> **Теорема 1.6.1.** Коммутативное (ассоциативное) кольцо, в котором ровно два идеала ($\{0\}$ и R) — поле.
>
> 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 (**??**) и теорему о гомоморфизме (**??**) можно получить следующее:
>
> **Теорема ??.**
>
> - В коммутативном кольце $\mathfrak{m} \lhd R$ — максимальный $\iff R/\mathfrak{m}$ — поле.
> - В коммутативном кольце $\mathfrak{m} \lhd R$ — простой $\iff R/\mathfrak{m}$ — область целостности.

Используя теорему (**??**), очевидно получаем:

- R — поле $\Rightarrow \{0\}$ — максимальный идеал.
- R — область целостности $\Rightarrow \{0\}$ — простой идеал
- Простой идеал $I \trianglelefteqslant \mathbb{Z} \Rightarrow (I = \{0\}) \vee (I = p\mathbb{Z}$ 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. $I \trianglelefteqslant R$ — 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 1.6.3. *$\equiv_I$ — 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 1.6.4. *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 $I \trianglelefteqslant R$ 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 $\mathbb{Q}\left[\sqrt{2}\right] \stackrel{def}{=} \mathbb{Q}[t]/(t^2-2)\mathbb{Q}[t] = \left\{a + b\sqrt{2} \middle| a, b \in \mathbb{Q}\right\}$.
   - $K[t]/t^nK[t]$ — 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 1.6.5.

- $\mathrm{Im}(\phi) \leqslant S$ — *подкольцо с единицей в* S.
- $\mathrm{Ker}(\phi) \trianglelefteqslant R$ — *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 $I = \mathrm{Ker}(\phi)$. Предъявим 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 $I \trianglelefteqslant R$ — ядро гомоморфизма $\rho_I : R \to R/I$.

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

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 $\{J|\mathfrak{m} \leqslant J \lhd R\}$ содержит всего 2 элемента $\overset{??}{\iff}$ $R/\mathfrak{m}$ имеет два идеала $\overset{??}{\iff}$ $R/\mathfrak{m}$ — поле.

$\mathfrak{m} \in \mathrm{Spec}(R)$, значит, $\forall J_1, J_2 \lhd R : (\mathfrak{m} \subsetneq J_1, J_2 \lhd R \Rightarrow J_1 J_2 \nsubseteq \mathfrak{m}) \iff \forall J_1, J_2 \lhd R/I : (J_1 \neq \{0\} \wedge J_2 \neq \{0\} \Rightarrow J_1 J_2 \neq \{0\}) \iff \forall x, y \in R/I : (x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0)$, а это определение области целостности. □

Замечание. Формулировка уже приводилась здесь: **(??)**

1.6.6 Китайская теорема об остатках. Chinese remainder theorem

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

Факт 1.6.2. *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 **(??)**.

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 гомоморфизм сюръективен: $\mathrm{Im}(\phi) = \{(y + A, z + B)|y, z \in R\}$. 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 $\{I_i\}_{1 \leqslant i \leqslant n}$, 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?

На что доцент ответил: «А что такое 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 $\mathrm{End}(A) \subset A^A$, где A — абелева группа. 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 — абелеву 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.

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

  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 (следует из того, что композиция гомоморфизмов — гомоморфизм). Обозначается, как произведение:

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

Теорема 1.7.1. $\mathrm{End}(A)$ — коммутативное 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 (**??**)
- 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 линейной алгебре: 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, $\mathrm{Supp}(f) \cap Y = \varnothing$, где

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

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

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 1.7.1. $R^X / I_Y \cong R^Y$

- **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. Полугрупповая алгебра

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

Здесь уже введены не одна, и не две, а целых 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 Лорана.

   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:

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

Таким образом, ряды Лорана — функции $f : f((-\infty, N) \cap \mathbb{Z}) = \{0\}$ для некоего $N \in \mathbb{Z}$, (образ взят от некоторого (бесконечного) префикса целых чисел).

Лекция XII

13 октября 2022 г.

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

Тогда очевидно, что

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

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

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

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

Полугрупповая алгебра

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

Теорема 1.7.4. 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: $(f * g) * h = f * (g * h)$. *Проверка получится довольно длинной.*

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

  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:

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

□

Определение 1.7.5 (δ-функция, символ Кронекера)**.** Семейство функций $\delta_x : X \to R$ определено 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 1.7.6 (Полугрупповое кольцо (алгебра))**.** Так построенное кольцо

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

1.7.5 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.

1.7.6 Расширенная полугрупповая алгебра

Определение 1.7.7 (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 1.7.5. $R[[X]]$ — ассоциативное кольцо.

Если X — моноид, то кольцо унитальное (с единицей).

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

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

1.7.7 Многочлены и все-все-все

Трудно формализуемое школьное определение: Выражения типа $a + a_1x + \cdots + a_nx^n$. Это суммы $\sum\limits_{i=0}^{n} a_ix^i$.	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, т. е. ненулевые значения в конечном количестве точек. Значит, записываются $f = \sum\limits_{i=0}^{n} a_i\delta_i$.
Здесь при умножении $x^i \cdot x^j = x^{i+j}$. Используются правила ассоциативности, коммутативности, дистрибутивности.	$f + g = (a_0 + b_0, a_1 + b_1, \dots)$ $f \cdot g = (a_0b_0, a_1b_0 + a_0b_1, \dots)$.	Несложно видеть, что $\delta_i * \delta_j = \delta_{i+j}$. $R[x]$ является кольцом относительно сложения и свёртки.
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!

Далее будем записывать многочлены в наиболее привычной форме из левого столбца.

Рассмотрим многочлен $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$. Рассмотрим функцию $\widetilde{f} : R \to R$; $\widetilde{f}$ — значение f в точке c, $f(c) = a_0 + a_1c + \cdots + a_nc^n$. 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 $\deg f \stackrel{def}{=} m$ — 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 $f = a_0 + a_1x + a_2x^2 + \dots$. 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 $R[x, x^{-1}]$. $f = \underbrace{a_m}_{\neq 0}x^m + \cdots + \underbrace{a_n}_{\neq 0}$. Здесь m — порядок, а n — степень.

  Формальнее, последовательность коэффициентов, среди которых только конечное количество ненулевых.

  $$(\underbrace{\dots}_{0}, a_m, \dots, a_{-2}, a_{-1}, a_0, a_{-1}, a_{-2}, \dots, a_n, \underbrace{\dots}_{0})$$

- Формальные ряды Лорана $R((x))$ — вправо бесконечны (говорят, что они полубесконечны), влево — конечны, хотя и сколь угодно много. Последовательность коэффициентов, среди которых начиная с некоторого места, все коэффициенты левее равны нулю.

  $$(\underbrace{\dots}_{0}, a_m, \dots, a_{-2}, a_{-1}, a_0, a_{-1}, a_{-2}, \dots, a_n, \underbrace{\dots}_{\text{что угодно}})$$

  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.

1.8 Матрицы

1.8.1 Матрицы и их части

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

Определение 1.8.1 (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.

Определение 1.8.2 (Матрица типа (I, J) с коэффициентами из X)**.** Семейство $x : I \times J \to X$.

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 1.8.3 (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: $I = \{1, 2, \dots, n\}; J = \{1, 2, \dots, m\}$, где $n = |I|, m = |J|$.

В таком случае матрицы $M(I, J, X)$ записываются $M(n, m, X)$. Также пишут $(x_{i,j})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m}$. 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: $I = \{0, \dots, n-1\}; J = \{0; \dots, m-1\}$.

Во-первых, в таком случае не надо переопределять $M(n, X)$, так как $n \stackrel{def}{=} \{0, \dots, n-1\}$. 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 $\begin{pmatrix}x_1 & \cdots & x_m\end{pmatrix}$.

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 1.8.4 (i-я строка матрицы x, $i \in I$)**.** Строка $x_{i,*} = \begin{pmatrix}x_{i,1} & \cdots & x_{i,m}\end{pmatrix}$, то есть сужение x как отображения на область определения $\{i\} \times J \subset I \times J$.

Определение 1.8.5 (j-й столбец матрицы x, $j \in J$)**.** Столбец $x_{*,j} = \begin{pmatrix}x_{1,j}\\ \vdots\\ x_{n,j}\end{pmatrix}$, 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.

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

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

Определение 1.8.7 (Побочная диагональ квадратной матрицы с натуральной индексацией)**.** Для матрицы $x \in M(n, X)$ это строка $(x_{i,j})_{i+j=n+1}$.

Определение 1.8.8 (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 $\begin{pmatrix} x_{1,2} & x_{1,3} \\ x_{3,2} & x_{3,3} \end{pmatrix}$

1.8.2 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 1.8.9 (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. При рассмотрении матриц, как группы по сложению, от R достаточно требовать не структуры кольца, а всего лишь структуры аддитивной абелевой группы.

Лемма 1.8.1. *Для аддитивной абелевой группы A : $M(n, m, A) \cong A^{mn}$.*

Доказательство. Сложение определено покомпонентно. □

Определение 1.8.10 (Умножение на скаляр)**.**

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

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

Умножение матриц

Замечание. С одной стороны, матрица — линейное отображение (будет пояснено позднее). 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 1.8.11 (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.

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

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

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 (**??**), 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:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_l \end{pmatrix} \cdot \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix} = \begin{pmatrix} x_1 y_1 & \cdots & x_1 y_n \\ \vdots & \ddots & \vdots \\ x_l y_1 & \cdots & x_l y_n \end{pmatrix}$$

   Получилось внешнее произведение, outer tensor.

   Определение 1.8.12 (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

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

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 (**??**).

   Лемма 1.8.2. *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 1.8.3. $e_{i,j_1} \cdot e_{j_2,k} = \delta_{j_1,j_2} \cdot e_{i,k}$.

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.

1.8.3 Умножение матриц в терминах матричных единиц

Рассмотрим квадратные матрицы.

Матричные единицы — множество $\{e_{i,j}\}_{1 \leqslant i,j \leqslant n}$. 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.

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

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

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

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 (более полное) 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 ассоциативность произведения матриц доказана, и введение в общую алгебру завершено.

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 2.1.1. *$\forall x \in R$, 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 2.1.1.

- $x \mid y \iff Rx \supset Ry$.
- $x \sim y \iff Rx = Ry$.
- 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. *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 главных *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. □

2.1.3 gcd & lcm, НОД и НОК соответственно

greatest common divisor & least common multiple.

Пусть $x, y \in R$.

Определение 2.1.9 (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 2.1.2. *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 (**??**): это элемент, порождающий идеал $Rx + Ry$.

Определение 2.1.10 (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 2.1.3. *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 2.1.11 (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 (**??**).

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 $d \geqslant 3$ — 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, $z \neq 0$.*

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

Доказательство. $(z \mid xz, yz) \Rightarrow z \mid \gcd(xz, yz) \Rightarrow \exists d \in R : d = \dfrac{\gcd(xz, yz)}{z}$. 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, $(x \mid x) \Rightarrow \left(x \div \dfrac{\operatorname{lcm}(x, y)}{y} \;\middle|\; x\right)$ (x делится на дробь, так как даже на $x : \frac{xy}{y}$); 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 2.1.12 ($\gcd(x_1, \ldots, x_n) = d$)**.**

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

Определение 2.1.13 ($\operatorname{lcm}(x_1, \ldots, x_n) = l$)**.**

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

Факт 2.1.4. *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 2.2.1. *Как бы то ни было,* $(xR + yR = R) \Rightarrow (\gcd(x, y) = 1)$.

Доказательство. Найдутся $a, b \in R : ax + by = 1$. Тогда все общие делители x, y делят 1, то есть обратимы. □

2.2.1 Свойства взаимной простоты

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

   Доказательство. Доказательство для gcd-колец (вообще можно доказать и в более общем случае, но на лекции было приведено только это):

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

   □

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). 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: (**??**).

Ниже R — кольцо главных идеалов.

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

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:

$$(p \in \mathrm{Irr}(R)) \wedge (p \mid xy) \wedge (p \nmid x) \Rightarrow (\exists a, b : ap + bx = 1) \Rightarrow (apy + b \underbrace{xy}_{p \mid xy} = y) \Rightarrow (p \mid y)$$

□

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

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

Очевидно, PID — нётерово кольцо Безу.

Кольца Безу — gcd-кольца, так как если $Rx + Ry$ — главный, то $\exists \gcd(x, y)$ — это тот элемент, который порождает $Rx + Ry$.

Совпадение неприводимости и простоты верно даже не сугубо в PID, а ещё и просто 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 2.3.1. *В PID взаимная простота совпадает с комаксимальностью. Понятно, что комаксимальность всегда влечёт взаимную простоту (**??**), но верно и обратное.*

2.4 Нётеровы кольца, условие обрыва цепей

Определение 2.4.1 (Нётерова область целостности)**.** Каждый идеал порождён конечным числом элементов.

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

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

В нётеровых кольцах можно проводить *индукцию* (как?); 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 в $\mathbb{Z}$: $p, p^2, p^3, \ldots$).

Впрочем, сильнее оно лишь от того, что мы рассматриваем кольца с единицей.

Лекция XVI

26 октября, 2022 г.

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

Иными словами, $\forall I \trianglelefteqslant R : \exists x_1, \dots, x_n \in R : I = x_1R + \dots + x_nR$

Примеры.

- PID
- Поле $K[x_1, \dots, x_n]$ (согласно (**??**)).
- $\mathbb{Z}[x_1, \dots, x_n]$ (по той же причине).
- $K[x_1, \dots, x_n, \dots]$ — кольцо многочленов от бесконечного числа переменных — **не нётерово**!

Замечание. Для некоммутативного кольца R различают нётеровы кольца слева и справа (про левые и правые идеалы соответственно), одно никак не влечёт другое.

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

Однако обычно нётеровость определяется в теории колец по-другому.

Рассмотрим цепочки идеалов.

Определение 2.4.2 (Цепочка идеалов)**.** Последовательность идеалов $\{I\}_{i \in \mathbb{N}}$.

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

Также различают строго возрастающие / убывающие цепочки.

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

Определение 2.4.3 (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 (максимальность по включению среди идеалов, как множеств).

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. Кажется, я этого не понял, но постарался записать услышанное без искажений.

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

  Рассмотрим $I \coloneqq \left(\bigcup\limits_{i\in\mathbb{N}} I_i\right) \trianglelefteqslant R$. 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: $I = x_1R + \cdots + x_nR$.

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

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

2.4.1 Теорема Гильберта о базисе

Теорема 2.4.2 (Теорема Гильберта о базисе)**.** Если R — нётерово кольцо, то $R[x]$ — нётерово кольцо.

Доказательство.

- Пусть $I \trianglelefteqslant R[x]$. Определим $\forall m \in \mathbb{N} : I_m \trianglelefteqslant R; \quad I_m = \left\{ f[x^m] \middle| f \in I \wedge \deg f = m \right\} \cup \{0\}$, где $f[x^m]$ — коэффициент перед x^m у многочлена f.

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

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

- Убедимся, что $I_1 \leqslant I_2 \leqslant \ldots$ В самом деле, для $a \in I_m : \exists f \in I : f = ax^m + \ldots$. 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. $\exists m \in \mathbb{N} : I_m = I_{m+1} = \ldots$.

- Построим конечную систему, порождающую исходный идеал I.

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

  Утверждается, что X порождает I. Докажем это по индукции, по n: многочлен степени n является линейной комбинацией многочленов $f \in X$ с коэффициентами из $R[x]$.

  – База: $n \leqslant m$ 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 (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 2.4.1. *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 $K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$. □

2.4.2 Артиновы кольца

Определение 2.4.4 (Артиново кольцо)**.** Коммутативное кольцо R, удовлетворяющее условию DCC.

Определение 2.4.5 (Descending chain condition, условие обрыва 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. В общем случае эти условия аналогичны.

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)**.** R — артиново коммутативное кольцо $\iff$ R — нётерово кольцо размерности 0.

Определение 2.4.6 (Размерность Крулля коммутативного кольца R)**.** Длина (за вычетом 1) строго возрастающей цепочки простых идеалов. Обозначается $\dim(R)$.

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

План доказательства данного частного случая

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

Следствие 2.4.2. *В области целостности всегда $\{0\} \trianglelefteqslant R$, 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:*

$$\exists \mathfrak{m}_1, \ldots, \mathfrak{m}_s \trianglelefteqslant R: \quad \mathfrak{m}_1 \cdots \mathfrak{m}_s = \{0\}$$

Определение 2.4.7 (R локально)**.** В R единственный максимальный идеал.

Теорема 2.4.4. Артиново кольцо изоморфно прямой сумме локальных колец. Доказательство является применением китайской теоремы об остатках.

Существенность единицы в кольце

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

В c_{p^∞} — 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.

Лекция XVII

3 ноября 2022 г.

2.4.3 Разложение на неприводимые в нётеровых кольцах

Определение 2.4.8 ($x \in R \setminus \{0\}$ 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. *В нётеровом кольце 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 (**??**),

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

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

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

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

$$pur_1 \ldots r_{n_1} = vp_1 \cdot \ldots \cdot p_{n_2} \cdot wq_1 \cdot \ldots \cdot q_{n_3}$$

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, как нётеровой области целостности, 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 $n \leqslant m$. Найдём противоречие индукцией по n. $p_n \mid q_1 \cdot \ldots \cdot q_m \Rightarrow \exists i : p_n \mid q_i$. Без ограничения общности $i = m$. Так как q_m неприводим, то $p_n \sim q_m$.

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

Теорема 2.5.2. Всякая PID является факториальным кольцом.

Доказательство.

- PID — нётеровы кольца — следует из определения.
- 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, $f \in K[x,y,z] \mapsto \overline{f} \in R, \overline{x} \cdot \overline{y} = \overline{z}^2$.

- $\mathbb{Z}\left[\sqrt{-5}\right] \stackrel{def}{=} \left\{m + ni\sqrt{5} \middle| m,n \in \mathbb{Z}\right\}$. Так, $6 \in \mathbb{Z}\left[\sqrt{-5}\right]$;

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

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

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

  $\mathrm{Trig}_{\mathbb{R}}$ — кольцо, так как 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 $m \geqslant n$.

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

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

  Следствие 2.5.2. $\mathrm{tdeg}\, f = 1 \Rightarrow f$ — *неприводим.*

  Следствие 2.5.3. $(\mathrm{Trig}_{\mathbb{R}})^* = \mathbb{R}^*$

  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 2.6.1.

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

Рассмотрим какой-нибудь конкретный $p \in \mathbb{P}$ в кольце $\mathbb{Z}$. Можно построить абсолютную величину (p-адическую норму) $|x|_p = \dfrac{1}{p^{v_p(x)}}$. Будут выполняться свойства $|xy|_p = |x|_p|y|_p$; $|x+y|_p \leqslant |x|_p + |y|_p$ (на самом деле $|x + y|_p \leqslant \max(|x|_p, |y|_p)$ — 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 $\mathbb{Z}_p$.

$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \middle| m, n \in \mathbb{Z}, n \neq 0, v_p(m) - v_p(n) \geqslant 0 \right\}$ — *интересно, к чему это здесь?*.

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 (R — евклидово кольцо)**.** Такая область целостности, что 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.

Интересный факт. В старых учебниках требовалось условие $(x \mid y) \Rightarrow (\delta(x) \leqslant \delta(y))$, 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 $\forall y \in R : \exists u \in R^*, q \in R : y = qx + u$; дальше определяем числа нормы 2 и так далее, по индукции.

Примеры (здесь не утверждается, что норма — минимальна)

- $R = \mathbb{Z} : \delta(x) = |x|$.
- $R = K[t] : \delta(f) = \deg(f)$.
- $R = \mathbb{Z}[i] : \delta(m + ni) = m^2 + n^2$

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

Доказательство. Пусть $I \trianglelefteqslant R$. 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: $\forall x \in I \setminus \{0\} : \delta(y) \leqslant \delta(x)$.

Утверждается, что $\forall x \in I : y \mid x$. 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 2.7.1. *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 (**??**).

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 всё меньшие натуральные числа (в произвольном кольце — элементы со всё меньшей нормой δ), 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 самого Евклида 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). Этот тип колец называется 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 $\mathbb{Z} : \forall x, y \in \mathbb{Z} : y \neq 0 \Rightarrow \exists! q, r \in \mathbb{Z} : (0 \leqslant q < y) \wedge (x = qy + r)$ В отсутствии предположения $0 \leqslant q$ получаем два разных возможных остатка с нормой δ меньше $\delta(y)$.

Интересный факт. Есть ровно одно кольцо, в котором (есть такая норма, 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: $\deg f \geqslant \deg g$. 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:

  Некоторые свойства степени:

  1. $\deg(f + g) \leqslant \max(\deg(f), \deg(g))$ — равенство, если старшие коэффициенты не сокращаются.
  2. $\deg(f \cdot g) \leqslant \deg(f) + \deg(g)$ — равенство в области целостности.

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

   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 $(q_1 - q_2)g = r_2 - r_1$. 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 факторомножеством, так записывают расширение полей, например,* $\mathbb{C}/\mathbb{R} \iff \mathbb{C} \supset \mathbb{R}$*.)*

В таком случае $K[x] \subset L[x]$.

Следствие 2.7.2 (Независимость делимости от поля)**.** *Если* $f, g \in K[x]$ *и* $g \mid f$ *в* $L[x]$*, то* $g \mid f$ *в* $K[x]$.

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

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

Следствие 2.7.3. $K[x]$ *— PID и* $K[x]$ *— UFD.*

2.7.4 Основная теорема арифметики для многочленов

Определение 2.7.3 (Неприводимый над полем K многочлен $q \in K[x]$)**.** q неприводим, как элемент кольца $K[x]$: $\nexists h, g \in K[x] : q = gh \wedge \deg(g), \deg(h) < \deg(q)$.

Примеры неприводимых многочленов

Неприводимость верна для класса ассоциированности, будем рассматривать нормированные многочлены (старший коэффициент равен 1).

- 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 по памяти, но наверняка что-то упустил.

Определение 2.7.4 (Алгебраически замкнутое поле)**.** Поле, над которым множество неприводимых многочленов — множество линейных многочленов.

Теорема 2.7.4 (Основная теорема высшей алгебры, FTHA)**.** $\mathbb{C}$ алгебраически замкнуто.

Следствие 2.7.4. *Над* $\mathbb{R}$ *неприводимы ровно те многочлены, которые либо линейны, либо второй степени с отрицательным дискриминантом.*

Теорема 2.7.5 (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

$$\left|\prod_{i \in I} p_i\right| + \left|\prod_{i \notin I} p_i\right|$$

Она не меньше 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 2.7.6 (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 выражения 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

Интересный факт. До данного $n \in \mathbb{N}$ асимптотически существует $\frac{n}{\ln n} + o(n)$ простых чисел.

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

Интересный факт. В любой арифметической прогрессии $ak + b, k \in \mathbb{Z}$, где a и b взаимно простые, есть бесконечно много простых.

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

Глава 3

Теория групп

Лекция XX
16 ноября 2022 г.

3.1 Подгруппа, порождённая множеством

Пусть G — группа, $H \subset G$.

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

Пишут $H \leqslant G$.

Таким образом, подгруппа — подмножество группы, само являющееся группой.

Действия с группами (и их подмножествами) чаще всего будут пониматься в смысле «по Минковскому». Так,

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

Пусть $X \subset G$ — произвольное подмножество.

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

Говорят, «X порождает H», «X — множество образ H», пишут $H = \langle X \rangle$.

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

Более того, $S_n = \left\langle \left\{ ([i]\ [i+1]) \middle| 1 \leqslant i < n \right\} \right\rangle$ — симметрическая группа порождается множеством транспозиций соседних элементов (квадратные скобки в записи добавлены для ясности записи).

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 $H \leqslant G$ (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. $\forall x, y \in G : \left[\begin{array}{c} Hx = Hy \\ Hx \cap Hy = \varnothing \end{array}\right.$.

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 $H \leqslant G$)**.** $\forall g \in G : \exists! x \in X : Hg = Hx$.

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 $H \backslash G$.

Предостережение. Не путать с разностью множеств $H \setminus G$.

Увы, похоже, именно эти символы надо использовать, найдите 5 различий.

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 $H \leqslant G$ (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)**.** $|G| = |H| \cdot |G : H|$. Если $|G| < \infty$, то можно поделить: $|G : H| = {}^{|G|}/_{|H|}$.

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 3.2.1. *В конечной группе G любая подгруппа H имеет порядок, являющийся делителем порядка G:* $|H| \;\Big|\; |G|$.

Следствие 3.2.2. *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 3.2.3. $o(g) \;\Big|\; |G|$.

Факт 3.2.1. *$\langle g \rangle \cong C_n$ 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 $F \leqslant H \leqslant G : |G : F| = |G : H| \cdot |H : F|$.

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 $\forall g \in G$.

$$Fg \subseteq Hg \Rightarrow \exists! x \in X : Fg \subset Hx \text{ (такой, что } Hx = Hg)$$

Для такого x верно, что $gx^{-1} \in H$, то есть

$$\exists! y \in Y : Fgx^{-1} = Fy \Rightarrow Fg = Fyx$$

Заметим, что нашлась такая единственная пара (x, y), что $Fg = Fyx$. Отсюда, в частности, следует, что отображение

$$X \times Y \to G; \qquad (x, y) \mapsto x \cdot y \qquad \text{— это инъекция}$$

Получается, $|YX| = |X \times Y| = |G : F|$. □

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 $g^{|G|} = 1_G$, или же $o(g) \mid |G|$. Отсюда сразу следуют теоремы Ферма (**??**) и Эйлера (**??**)).

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 (**??**)

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_k^{n_k}\mathbb{Z})$$

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)**.** $\forall n \perp m : \phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

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 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).

Вообще говоря, можно проще: теперь рассмотрим другую биекцию, $y \mapsto yx$. Там тоже будет элемент — прообраз 1, значит, x обратим и слева, и справа, откуда обратим. □

Таким образом, $\phi(m) = \left|\left\{0 \leqslant x < m, x \in \mathbb{N} \middle| x \perp m\right\}\right|$.

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} $I \trianglelefteqslant R$ сопоставляется факторкольцо R/I.

Паре {группа — нормальная подгруппа} $H \trianglelefteqslant G$ 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 $H \trianglelefteqslant G$.

Лемма 3.4.1. *Следующие условия эквивалентны.*

1. $H \trianglelefteqslant G$
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

- $\{1\} \trianglelefteqslant G; \quad G \trianglelefteqslant G$.

  Определение 3.4.2 (Простая группа G)**.** $G \neq \{1\}$ и в ней нет никаких нормальных подгрупп, кроме тривиальных — $\{1\}$ и G.

  Теорема ?? (Галуа). Для $n \geqslant 5$ 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.

  Доказательство. См. (**??**). □

  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 $\mathrm{Cent}(G) = \{x \in G | \forall y \in G : xy = yx\}$. Также обозначают $C(G)$.

  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 $\mathrm{Cent}(G) \trianglelefteqslant G$, так как $\mathrm{Cent}(G)$ — абелева подгруппа.

  Любая *центральная подгруппа* $H \trianglelefteqslant \mathrm{Cent}(G)$ 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.

- $|G:H|=2 \Rightarrow H \trianglelefteqslant G$.

  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 $|G:H| = p \Rightarrow H \trianglelefteqslant G$.*

  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 порядка 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 в качестве большой группы $D_3 \cong S_3$.

  $G = S_3$. Рассмотрим $H = \langle (12) \rangle = \{\mathrm{id}, (12)\}$.

  $(13)H = \{(13), (123)\}$, но $H(13) = \{(13), (132)\}$.

Вообще говоря, пример можно обобщить: рассмотрим $S_{n-1} \leqslant S_n$.

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 $1, \dots, n-1$.

- $V \trianglelefteqslant A_4$ — «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 $H \trianglelefteqslant G$ факторгруппу G/H. Для этого введём каноническую проекцию $\pi : G \to G/H$.

$G/H = \{gH | g \in G\}$. Обозначение совпало с обозначением фактормножества по подгруппе (**??**), и с обозначением фактормножества вообще. Тем не менее, все обозначения если имеют смысл, то означают одно и то же, причём когда $H \trianglelefteqslant G$, то можно ещё ввести структуру группы.

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 (**??**).*

Доказательство. $\exists h \in H : x_1 h = x_2$. Отсюда $x_2 y_2 H = x_1 h y_2 H = x_1 (y_2 y_2^{-1}) h y_2 H = x_1 y_2 \underbrace{y_2^{-1} h y_2}_{\in H} H =$

$x_1 y_2 H = x_1 y_1 H$.

Условие $y_2^{-1} h y_2 \in H$ следует из $H \trianglelefteqslant G$. □

Определение через произведение по Минковскому

Определение 3.5.2 (Произведение смежных классов $xH \cdot yH$)**.**

$$xH \cdot yH = \left\{ (xh) \cdot (yg) \middle| h, g \in H \overset{\text{здесь эквивалентно}}{\iff} xh \in xH, yg \in yH \right\}$$

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 $H \not\trianglelefteqslant G : xH \cdot yH$ равно объединению нескольких смежных классов, увы.

Таким образом, на G/H для $H \trianglelefteqslant G$ 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)**.** Группа G/H с определённой выше операцией.

Примеры.

- $\mathbb{Z}/m\mathbb{Z}$ — не только факторкольцо, но и факторгруппа по сложению.
- Вообще, в абелевой группе все подгруппы нормальны, существуют факторгруппы по любым подгруппам.
- В любой группе $\operatorname{Cent}(G) \trianglelefteqslant G$. Группа внутренних автоморфизмов $\operatorname{Inn}(G) \overset{def}{=} G/\operatorname{Cent}(G)$ (**??**).
- **Определение** 3.5.4 (Коммутант группы G). $\langle \{ [x,y] | x, y \in G \} \rangle$. Обозначается $[G;G]$. Здесь $[x,y]$ — коммутатор (**??**).

  Факт 3.5.1. *Коммутант группы G нормален:* ${}^g[x,y] = [{}^g x, {}^g y]$.

  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: $\mathrm{Im}(\phi) \stackrel{def}{=} \phi(H) \leqslant G$.

Ядро — нормальная подгруппа: $\forall h \in H : \phi(hxh^{-1}) = \phi(h)\underbrace{\phi(x)}_{1}\phi(h)^{-1} = 1$.

Имеет место изоморфизм $\overline{\phi} : H/\operatorname{Ker}(\phi) \cong \mathrm{Im}(\phi)$. 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 3.6.1 (Теоремы о соотвествии)**.**

- *Подгруппы в* $\mathrm{Im}(G)$ *образуют взаимно-однозначное соответствие с подгруппами в* H*. содержащими* $\operatorname{Ker}(\phi)$.

  Для проверки изоморфизма сопоставим подгруппе $F \leqslant H \mapsto F/\operatorname{Ker}(\phi)$.

- *Пусть* $H_1 \trianglelefteqslant G_1$ *и* $H_2 \trianglelefteqslant G_2$*. Если есть гомоморфизм* $\phi : G_1 \to G_2$ *такой, что* $\phi(H_1) \leqslant H_2$*, то имеет место гомоморфизм* $\overline{\phi} : G_1/H_1 \to G_2/H_2$*, факторизующий по подгруппам* H_1 *и* H_2*.*

  Доказательство. Гомоморфизм $\overline{\phi} : G_1/H_1 \to G_2/H_2$ устроен следующим образом:

  $$\forall x \in G_1 : \overline{\phi}(xH_1) = \phi(x)H_2$$

  Заметим, что $\overline{\phi}(xH_1) = \phi(x)H_2 \supset \phi(x)\phi(H_1) = \phi(xH_1)$, откуда гомоморфизм определён корректно: от класса, как от множества, берётся образ, после чего выбирается в G_2 смежный класс по H_2, содержащий этот образ.

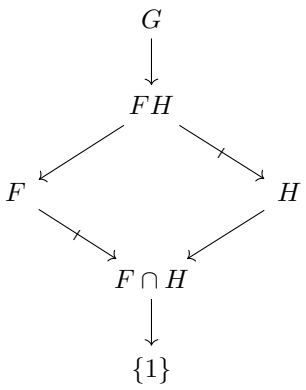
  Также несложно видеть, что $\overline{\phi}$ — гомоморфизм:

  $$\bar{\phi}(xH_1) \cdot \bar{\phi}(yH_1) = \phi(x)H_2\phi(y)H_2 = \phi(x)\phi(y)H_2H_2 = \bar{\phi}(xyH_1)$$ □

3.7 Теоремы об изоморфизме

- **Теорема 3.7.1** (Нётер об изоморфизме)**.** Пусть $F, H \leqslant G$, причём $H \trianglelefteqslant G$.
  1. $FH \leqslant G$ — подгруппа.
  2. $F \cap H \trianglelefteqslant F$ — нормальная подгруппа.
  3. $FH/H \cong F/(F \cap H)$.

Это же изображено на диаграмме Хассе:



Доказательство.

Лемма 3.7.1. *Пусть $F \leqslant G, H \trianglelefteqslant G$. Тогда $\langle F, H\rangle = FH$*

Доказательство леммы.

Ясно, что $F, H \leqslant FH \leqslant \langle F, H\rangle \overset{def}{=} \langle F \cup H\rangle$.

Теперь осталось проверить, почему FH — подгруппа в G.

Так как $H \trianglelefteqslant G$, 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. $\forall x \in F : x(F \cap H)x^{-1} = \underbrace{xFx^{-1}}_{x \in F} \cap xHx^{-1} = F \cap H$.
3. Построим гомоморфизм $\phi : F \to FH/H$. Положим $\phi : f \mapsto fH$ — элемент переходит в смежный класс.

   $\mathrm{Im}(\phi) = FH/H$, так как $\forall h \in H : fhH = fH$, но fh пробегает все значения из FH.

   $\mathrm{Ker}(\phi) = F \cap H$, так как $f \mapsto H \iff f \in H$. □

Лекция XXIII

24 ноября 2022 г.

- Пусть $F \leqslant H \leqslant G$, причём $F, H \trianglelefteqslant G$.

  Предостережение. $F \trianglelefteqslant H \trianglelefteqslant G$ и $F \trianglelefteqslant G$ — разные условия на F. Первое ещё записывают $F \trianglelefteqslant\trianglelefteqslant G$.

  Теорема 3.7.2 (фон Дик)**.** $G/H \cong (G/F)/(H/F)$.

  Доказательство. Воспользуемся теоремой о гомоморфизме: построим $\phi : G/F \to G/H$, построим так, что $gF \mapsto gH$.

  Определение корректно, так как $gF \subseteq gH$ — если $g_1F = g_2F$, то $g_1H = g_2H$. Также несложно видеть, что ϕ — гомоморфизм.

  Осталось вычислить $\mathrm{Im}(\phi) = G/H$ (ϕ сюръективна, все классы достигаются) и $\mathrm{Ker}(\phi)$: $\phi(gF) = H \iff gH = H \iff g \in H$. Таким образом, $\mathrm{Ker}(\phi) = H/F$ — классы, имеющие представителя в H. □

- Пусть $H_1 \trianglelefteqslant G_1$ и $H_2 \trianglelefteqslant G_2$.

  Теорема 3.7.3. $H_1 \times H_2 \trianglelefteqslant G_1 \times G_2$, причём $(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)$.

  Доказательство.

  – Проверка нормальности: пусть $h = (h_1, h_2) \in H_1 \times H_2$, $g = (g_1, g_2) \in G_1 \times G_2$.

    Тогда $ghg^{-1} = (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}) \in H_1 \times H_2$, так как всё нормально.

  – Построим гомоморфизм $\phi : G_1 \times G_2 \to G_1/H_1 \times G_2/H_2$. В отличие от предыдущих теорем о гомоморфизме, здесь — раз уж мы хотим использовать теорему о гомоморфизме — у нас нет выбора (строить гомоморфизм справа налево, или слева направо), так как справа не факторгруппа.

    Очевидно, это произведение проекций: $\phi = \pi_1 \times \pi_2 : (g_1, g_2) \mapsto (g_1 H, g_2 H)$. Произведение гомоморфизмов — гомоморфизм.

    Гомоморфизм сюръективный; $\mathrm{Ker}(\phi) = H_1 \times H_2$. □

3.8 Классы сопряжённости, централизаторы

Введём на группе ещё одно понятие эквивалентности.

Определение 3.8.1 ($x, y \in G$ сопряжены)**.** $\exists g \in G : y = {}^g x = gxg^{-1}$. Здесь y — левый сопряжённый x при помощи g.

Обозначается $x \sim_G y$.

Факт 3.8.1. *Это отношение эквивалентности на* G : gxg^{-1}

- $x = {}^{1_G} x$.
- $y = gxg^{-1} \iff x = g^{-1} y g$.
- $x = {}^g y \wedge y = {}^h z \Rightarrow x = {}^g({}^h z) = {}^{gh} z$.

Определение 3.8.2 (Классы сопряжённости)**.** Классы эквивалентности отношения $\sim$.

Так, класс сопряжённости x — это $\{y \in G | y \sim x\} = \{{}^g x | g \in G\} = x^G$ — почему-то при операции по Минковскому принято писать G справа.

Замечание. В абелевых группах всякий класс сопряжённости состоит из одного элемента: $x^G = \{x\}$. Несложно видеть и обратное — условие значит, что всякий x коммутирует со всяким g.

Определение 3.8.3. Центр $\mathrm{Cent}(G) = \left\{ x \in G \middle| x^G = \{x\} \right\}$ — множество элементов, коммутирующих со всеми остальными. Здесь $\{x\}$ — центральные классы.

Остальные классы не пересекаются с центром, они состоят из больше, чем одного элемента.

Пример. В группе кватернионов $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ центр $\mathrm{Cent}(G) = \{\pm 1\}$ (**??**).

Определение 3.8.4 (Система представителей классов сопряжённости)**.** Такое $X \subseteq G : \forall g \in G : \exists! x \in X : x \sim g$.

Лемма 3.8.1.

$$G = \bigsqcup_{x \in X} x^G$$

где X — система представителей классов сопряжённости.

Следствие 3.8.1. *В случае конечной группы* $\{c_1, \ldots, c_n\} = \left\{ x^G \middle| x \in X \right\}$*, причём* $|G| = |c_1| + \cdots + |c_n|$.

Определение 3.8.5 (Централизатор элемента $x \in G$)**.** $C_G(x) = \{g \in G | gx = xg\} = \{g \in G | {}^g x = x\}$. Из последнего определения видно, что что $C_G(x) \leqslant G$.

Теорема 3.8.1. Имеет место биекция $x^G \leftrightarrow G/C_G(x)$.

Доказательство. ${}^h x = {}^g x \iff {}^{g^{-1}h}x = x \iff g^{-1}h \in C_G(x)$. □

Следствие 3.8.2. $|x^G| = |G : C_G(x)|$, *откуда, в частности, порядок любого класса сопряжённости — делитель порядка группы.*

Следствие 3.8.3. *Отсюда в группе кватернионов порядок центра — степень двойки не больше 8.*

Так как группа некоммутативна, то порядок центра строго меньше 8 — не все элементы коммутируют.

В центре содержатся как минимум ± 1, *но по симметрии, если там ещё есть* i, *то будет и* j, k. *Несложно видеть, что единственный вариант —* $\mathrm{Cent}(G) = \{\pm 1\}$.

3.8.1 Классы сопряжённости S_n

Рассмотрим произвольную перестановку $\pi \in S_n$, например, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 1 & 4 & 8 & 2 & 6 & 9 \end{pmatrix}$, для $n = 9$.

Её цикленнный тип $\pi = (137254)(68)(9) = (137254)(68)$ — тривиальные циклы из одного элемента опускают. Это циклы в ориентированном функциональном графе, где есть ребро $i \to j$, если и только если $\pi_i = j$

Не имеет значения, с какого места писать циклы.

Теорема 3.8.2. $\pi \sim \sigma$ в S_n если и только если π и σ имеют одинаковый цикленный тип — мультимножество (множество с учётом количества) длин независимых циклов.

У рассмотренной выше перестановки цикленный тип $(1, 2, 6)$.

Набросок доказательства.

Сопрягающая перестановка должна переводить циклы одной длины в π в те циклы той же длины в σ. □

Пример. $(123) \sim (517)$ в S_8.

3.9 Группа автоморфизмов G

Определение 3.9.1 (Группа автоморфизмов группы G)**.**

$$\mathrm{Aut}(G) \stackrel{def}{=} \left\{\phi \in G^G \middle| \phi \text{ — биективный эндоморфизм}\right\}$$

На группе определена операция $\circ : \phi \circ \psi$ — композиция автоморфизмов — тоже автоморфизм.

Оказывается, есть естественный гомоморфизм:

$$I : G \to \mathrm{Aut}(G)$$
$$g \mapsto I_g$$

Определение 3.9.2 (Внутренний автоморфизм)**.** $I_g : G \to G$, определённый $x \mapsto {}^g x = gxg^{-1}$.

Это автоморфизм, так как $I_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = I_g(x)I_g(y)$ и $I_g^{-1} = I_{g^{-1}}$.

Легко проверить, что I — гомоморфизм, так как $I_{hg} = I_h I_g$, и это именно та причина, по которой лектор предпочитает писать сопряжение ${}^g x$ слева — иначе бы ($x^g = g^{-1}xg$) получилось $I_{hg} = I_g I_h$, был бы антигомоморфизм.

Определение 3.9.3 (Группа внутренних изоморфизмов G)**.** $\mathrm{Inn}(G) = \{I_g | g \in G\}$.

Как замечено выше, $\mathrm{Inn}(G) \cong G/\mathrm{Cent}(G)$ (это, например, видно из теоремы о гомоморфизме).

Определение 3.9.4 (Группа без центра)**.** Такая группа G, что $\mathrm{Cent}(G) = \{1\}$.

В группах без центра имеет место вложение $G \hookrightarrow \mathrm{Aut}(G)$.

Рассмотрим подгруппу, построенную выше: $\mathrm{Inn}(G) \leqslant \mathrm{Aut}(G)$.

Лемма 3.9.1. $\mathrm{Inn}(G) \trianglelefteqslant \mathrm{Aut}(G)$.

Доказательство. Пусть $\phi \in \mathrm{Aut}(G)$. Тогда $\phi \circ I_g \circ \phi^{-1} = I_{\phi(g)}$.

Проверка равенства:

$$(\phi \circ I_g \circ \phi^{-1})(x) = (\phi \circ I_g)(\phi^{-1}(x)) = \phi(g * \phi^{-1}(x) * g^{-1}) = \phi(g) * x * \phi(g^{-1}) = I_{\phi(g)}(x)$$

□

Определение 3.9.5 (Группа внешних автоморфизмов)**.** $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ — почему бы не профакторизовать, раз уж $\mathrm{Inn}(G) \trianglelefteqslant \mathrm{Aut}(G)$

3.10 Продолжение про сопряжённые

Можно говорить про подмножества $X \subseteq G$.

Назовём ${}^gX = I_g(X) = \left\{gxg^{-1} \middle| x \in X\right\}$ — сопряжение X при помощи g.

Это вводит отношение эквивалентности $Y \sim Z$, где $Y, Z \subseteq X$.

Определение 3.10.1 (Нормализатор $X \subset G$ в G)**.** $N_G(X) = \{g \in G | {}^gX = X\} \leqslant G$ — элементы, коммутирующие с X по Минковскому.

Определение 3.10.2 (Централизатор $X \subset G$ в G)**.** $C_G(X) = \left\{g \in G \middle| \forall x \in X : gxg^{-1} = x\right\} \leqslant G$ — элементы, коммутирующие с каждым элементом из X.

Замечание. $C_G(X) = \bigcap\limits_{x \in X} C_G(x)$.

Лемма 3.10.1. $C_G(X) \trianglelefteqslant N_G(X)$.

Доказательство. Рассмотрим $\forall g \in N_G(X), h \in C_G(X)$. Проверим, что $ghg^{-1} \in C_G(X)$.

Но это значит, что $\forall x \in X : I_{ghg^{-1}}(x) = x$. Заметим, что $I_{ghg^{-1}} = I_{I_g(h)}$, то есть достаточно доказать $I_g(h) \in C_G(X)$.

Я не понимаю, как это сделать, мне удобнее провести другую цепочку: $g^{-1}xg \in X \Rightarrow hg^{-1}xgh^{-1} = {}^{g^{-1}}x \Rightarrow ghg^{-1}xgh^{-1}g^{-1} = x$, то есть действительно $I_{ghg^{-1}}(x) \in C_G(X)$. □

Лекция XXIV

30 ноября 2022 г.

3.11 Двойные смежные классы, формула индекса Фробениуса

Пусть $F, H \leqslant G$; $x \in G$ — произвольный элемент.

Определение 3.11.1 (Двойной смежный класс)**.** $FxH = \{fxh | f \in F, h \in H\}$. Называется двойной смежный класс по модулю (F, H).

Лемма 3.11.1. *Имеет место ровно одно из двух:* $\begin{bmatrix} FxH \cap FyH = \varnothing \\ FxH = FyH \end{bmatrix}$.

Доказательство. Пусть пересечение непусто. Значит, $\exists z \in G : z = f_1 x h_1 = f_2 y h_2$. Тогда $x = (f_1^{-1} f_2) y (h_2 h_1^{-1})$.

Отсюда $FxH = F(f_1^{-1} f_2) y (h_2 h_1^{-1}) H \subset FyH$. Аналогично $FyH \subset FxH$, они равны. □

Определение 3.11.2 (Сравнимость по двойному модулю)**.** $x \ {}_F\!\equiv_H y \overset{def}{\iff} FxH = FyH$.

Согласно лемме, ${}_F\!\equiv_H$ — отношение эквивалентности. Оно порождает классы эквивалентности.

Выберем систему представителей двойных смежных классов — *трансверсаль* X.

$\forall g \in G : \exists! x \in X : g \ {}_F\!\equiv_H x$.

Лемма 3.11.2. $G = \bigsqcup\limits_{x \in X} FxH$.

Доказательство. Очевидно. □

Если $|G| < \infty$, то $X = \{x_1, \ldots, x_n\}$; $G = \bigsqcup\limits_{i=1}^{n} Fx_iH$, откуда $|G| = \sum\limits_{i=1}^{n} |Fx_iH|$.

Лемма 3.11.3 (Формула произведения)**.** *Пусть $F, H \leqslant G$. Хотя FH вообще говоря подгруппой не является, можно посчитать*

$$|FH| = \frac{|F| \cdot |H|}{|F \cap H|}$$

Доказательство. $FH = \{fh | f \in F, h \in H\}$.

Когда $f_1 h_1 = f_2 h_2$? Это происходит ровно тогда, когда $h_1 h_2^{-1} = f_1^{-1} f_2$, то есть этот элемент лежит в $F \cap H$.

С другой стороны, пусть $\forall g \in F \cap H$. Тогда $\underbrace{(f_2 g)}_{f_1} \underbrace{(g^{-1} h_1)}_{h_2} = f_1 h_2$.

Таким образом, две пары дают одинаковое произведение $\iff$ отношение $\frac{f_2}{f_1} = \frac{h_2}{h_1} \in F \cap H$. □

Лемма при подсчёте $|Fx_iH|$ неприменима, так как x_iH — не подгруппа. Тем не менее, есть простой способ сделать это подгруппой, не меняя порядок двойного смежного класса.

Следствие 3.11.1.

$$|FxH| = |FxHx^{-1}| = \frac{|F| \cdot |xHx^{-1}|}{|F \cap xHx^{-1}|} = \frac{|F| \cdot |H|}{|F \cap xHx^{-1}|}$$

Несложно видеть, что $|F \cap xHx^{-1}| = |Fx \cap xH| = |x^{-1}Fx \cap H|$.

Следствие 3.11.2. *FxH содержит $\left|H : \left(x^{-1}Fx \cap H\right)\right|$ левых смежных классов по F.*

Пусть $F, H \leqslant G$.

Теорема 3.11.1 (Формула индекса Фробениуса)**.** Пусть $X = \{x_1, \ldots, x_n\}$ — трансверсаль по модулю (F, H).

$$|G : F| = \left|H : \left(x_1^{-1}Fx_1 \cap H\right)\right| + \cdots + \left|H : \left(x_n^{-1}Fx_n \cap H\right)\right|$$

Доказательство. Подставить в формулу суммы формулу произведения. □

Следствие 3.11.3. *Если $H \leqslant G$, причём $|G : H| = p \in \mathbb{P}$, где p — наименьшее простое, делящее $|G|$, то $H \trianglelefteqslant G$.*

Доказательство. Пусть $X = \{x_1, \ldots, x_n\}$ — трансверсаль G по двойному модулю (H, H).

$p = |G : H| = \left|H : \left(x_1^{-1} H x_1 \cap H\right)\right| + \cdots + \left|H : \left(x_n^{-1} H x_n \cap H\right)\right|$.

Так как p — наименьшее простое, делящее порядок группы, то p — наименьшее простое, делящее $|H|$, откуда индекс всякого смежного класса — либо 1, либо p.

Используя то, что $n > 1$ ($H \leqslant G$), получаем, что обязательно $\left|H : \left(x_i^{-1} H x_i \cap H\right)\right| = 1$, откуда $x_i^{-1} H x_i = H$. □

3.12 Коммутант

Определение 3.12.1 (Левонормированный коммутатор $x, y \in G$)**.** $[x, y] = xyx^{-1}y^{-1}$.

Определение 3.12.2 (Коммутант группы G)**.** $[G, G] = \left\langle \left\{ [x, y] \middle| x, y \in G \right\} \right\rangle$.

Предостережение. $\left\langle \left\{ [x, y] \middle| x, y \in G \right\} \right\rangle \neq \left\{ [x, y] \middle| x, y \in G \right\}$.

Однако самая маленькая группа, для которой равенство не наблюдается, имеет порядок 96. В ней множество коммутаторов имеет порядок 29, а сама подгруппа коммутаторов — 32.

Интересный факт. Если рассматривать коммутаторы не обязательно из двух элементов, то получится подгруппа: $\left\langle \left\{ [x, y] \middle| x, y \in G \right\} \right\rangle = \left\{ x_1 \cdot \ldots \cdot x_n x_1^{-1} \cdot \ldots \cdot x_n^{-1} \middle| x_1, \ldots, x_n \in G, n \in \mathbb{N} \right\}$.

Теорема 3.12.1.

1. $[G, G] \trianglelefteqslant G$.
2. $G/[G, G]$ — абелева группа. Именно поэтому обозначается G^{ab}.
3. Коммутант — наименьшая подгруппа, фактор по которой абелев: $\forall H \trianglelefteqslant G$: если G/H — абелева группа, то $H \geqslant [G, G]$.

   Замечание. Неформально говоря, чем меньше коммутант (чем больше центр), тем более группе присуща абелевость.

Доказательство.

1. $\forall g \in G : {}^g[x, y] = [{}^g x, {}^g y]$.
2. Пусть $H = [G, G]$. Тогда элементы G/H — смежные классы; посчитаем множество их коммутаторов. $[xH, yH] = [x, y]H = H$, поэтому любые два элемента в G/H коммутируют.

   Замечание. H можно вынести за $[-; -]$, так как $xH \cdot yH = xyH$ и $(xH)^{-1} = x^{-1}H$ по определению, операции определены в терминах представителей, а подгруппа — нормальная.
3. Если $H \trianglelefteqslant G$, то $\forall x, y \in G : [xH, yH] = [x, y]H = H$, то есть H содержит все коммутаторы. □

Определение 3.12.3 ($H \leqslant G$ — характеристическая подгруппа)**.** $\forall \phi \in \mathrm{Aut}(G) : \phi(H) \leqslant H$.

Определение 3.12.4 ($H \leqslant G$ — вполне характеристическая подгруппа)**.** $\forall \phi \in \mathrm{End}(G) : \phi(H) \leqslant H$.

На самом деле, коммутант является не просто нормальной подгруппой, он является характеристической и даже вполне характеристической подгруппой: $\phi([x, y]) = [\phi(x), \phi(y)]$.

Интересный факт (Галуа). Группа разрешима (и у относящегося к ней уравнения можно найти решение), если цепь «коммутант G — коммутант коммутанта G — коммутант коммутанта коммутанта G — ...» придёт к единице.

1. $[S_n, S_n] = A_n$.
2. $[A_n, A_n] = A_n$, где $n \geqslant 5$.
3. $[A_4, A_4] = V$
4. $[A_m, A_m] = \{1\}$, где $m \leqslant 3$.

Определение 3.12.5 (Группа G совершенна)**.** $G = [G, G]$.

Пример. Так, группа A_5 совершенна.

Пример. В группе дробно-линейных преобразований $GL(n, K)$

$$[SL(n, K), SL(n, K)] \leqslant [GL(n, K), GL(n, K)] \leqslant SL(n, K)$$

Равенство наблюдается практически всегда, за исключением случаев $GL(2, \mathbb{F}_2)$ и $GL(2, \mathbb{F}_3)$.

Здесь $SL(n, k) \stackrel{def}{=} \{g \in GL(n, k) | \det(g) = 1\}$.

Глава 4

Линейная алгебра

4.1 Модули и векторные пространства

Модуль — обобщение понятий «абелевая группа», «векторное пространство», «идеал». Сравнение по *модулю*.

До сих пор мы рассматривали внутренние операции: $X \times X \to X$.

Но можно же рассматривать внешние операции: $X \times Y \to Z$.

Сейчас мы остановимся посередине:

Определение 4.1.1 (Левое действие)**.** $X \times Y \to Y$. Элемент множества X действует на $y \in Y$ слева.

Определение 4.1.2 (Правое действие)**.** $Y \times X \to Y$. Элемент множества X действует на $y \in Y$ справа.

Пусть R — ассоциативное кольцо с единицей, совсем не обязательно обладающее коммутативностью.

Надо различать, левые и правые модули (например, векторные пространства) даже в случае коммутативного кольца R.

Определение 4.1.3 (Левый R-модуль)**.** Множество $M \neq \varnothing$, на котором заданы две операции:

$$\begin{array}{cc} + : M \times M \to M & \cdot : R \times M \to M \\ x + y \mapsto x + y & \lambda, x \mapsto \lambda x \end{array}$$

причём выполняются аксиомы абелевой группы по сложению для M, и следующие свойства действия (написанное ниже верно $\forall \lambda, \mu \in R; \forall x, y \in M$):

V1. Левая внешняя дистрибутивность. $(\lambda + \mu)x = \lambda x + \mu x$

V2. Правая внешняя дистрибутивность. $\lambda(x + y) = \lambda x + \lambda y$.

V3. Левая внешняя ассоциативность. $(\lambda\mu)x = \lambda(\mu x)$.

V4. Унитальность. $1_R \cdot x = x$.

Правый R-модуль иногда будем называть модуль-R, по аналогии с левым R-модулем. В правом модуле-R внешняя операция $M \times R \to M$, $x, \lambda \mapsto x\lambda$.

Определение 4.1.4. Если R — коммутативное кольцо, то элементы R — скаляры; левые R-модули биективно соответствуют правым R-модулям.

Правый модуль-R — то же самое, что левый R^o-модуль, где R^o — противоположное кольцо (**??**).

Примеры.

- $M = \{0\}$. Зададим умножение $\forall \lambda \in R : \lambda \cdot 0 = 0$.
- $M = R$. Зададим умножение в соответствии с внутренней операцией: $\lambda \cdot x = \lambda x$. Всякое кольцо — и левый, и правый модуль над самим собой.

  Левому R-модулю ${}_R R$ соответствует операция $R \times R \to R; \quad \lambda, x \mapsto \lambda x$.

  Правому модулю-R R_R соответствует операция $R \times R \to R; \quad x, \lambda \mapsto x\lambda$.

  Определение 4.1.5 (Бимодуль). M — R-модуль-S, если ещё выполнена двусторонняя ассоциативность
  $$R \times M \times S \to M; \quad \lambda, x, \alpha \mapsto (\lambda x)\alpha = \lambda(x\alpha)$$

  Кольцо над собой является ещё и бимодулем.
- Рассмотрим случай, когда $R = T$ — тело. Левый модуль — левое векторное пространство. Правый модуль — правое векторное пространство.

  В частности, $\mathbb{R}^2, \mathbb{R}^3$ — векторные пространства над $\mathbb{R}$.
- Всякая абелева группа A является $\mathbb{Z}$ модулем: $n, x \mapsto \begin{cases} +(\underbrace{x + \cdots + x}_{n}), & n \geqslant 0 \\ -(\underbrace{x + \cdots + x}_{-n}), & n < 0 \end{cases}$.

  Более того, всякая абелева группа — модуль над $\mathrm{End}(A)$, это следствие того, что $\mathrm{End}(A)$ — кольцо. Так как $\mathbb{Z} \hookrightarrow \mathrm{End}(A)$, то утверждение, что A — $\mathbb{Z}$-модуль — отсюда очевидно.
- $I \trianglelefteqslant R \iff I \leqslant_R R_R$.

  Определение 4.1.6 (N — подмодуль M). (Абелева) подгруппа, замкнутая относительно действия на неё элементов из R. Обозначают $N \leqslant_R M$. Иногда R нижним индексом опускают.
- $R[x]$ — R-модуль. Можно также рассмотреть группу многочленов ограниченной степени: $(R[x]_{\leqslant m}) \leqslant_R R[x]$.

4.1.1 Свободные модули конечного ранга

Понятие ранга будет введено позже; мы будем работать в основном с модулями именно конечного ранга.

Определение 4.1.7 (Левый свободный модуль над R ранга n)**.** Модуль строк длины $n \in \mathbb{N}$.
$${}^n R \stackrel{def}{=} \left\{ \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \middle| x_i \in R \right\}$$

Сложение и умножение на $x \in R$ определены покомпонентно.

Определение 4.1.8 (Стандартный базис ${}^n R$)**.** $\left\{ \underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}}_{f_1}, \underbrace{\begin{pmatrix} 0 & 1 & \cdots & 0 \end{pmatrix}}_{f_2}, \ldots, \underbrace{\begin{pmatrix} 0 & 0 & \cdots & 1 \end{pmatrix}}_{f_n} \right\}$

Всякий элемент ${}^n R$ можно получить, как линейную комбинацию элементов базиса с коэффициентами из R:
$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} = x_1 f_1 + x_2 f_2 + \cdots + x_n f_n = \underbrace{\begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix}}_{\text{строка координат}} \cdot \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix}$$

Определение 4.1.9 (Правый свободный модуль над R ранга n)**.** Модуль столбцов высоты $n \in \mathbb{N}$.
$$R^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \middle| x_i \in R \right\}$$

Сложение и умножение на элемент R определены покомпонентно.

Определение 4.1.10 (Стандартный базис R^n)**.** $\left\{ \underbrace{\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}}_{e_1}, \underbrace{\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}}_{e_2}, \dots, \underbrace{\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}}_{e_n} \right\}$

Всякий элемент R^n можно получить, как линейную комбинацию элементов базиса с коэффициентами из R:

$$\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix} = e_1x_1 + e_2x_2 + \dots + e_nx_n = \begin{pmatrix}e_1 & e_2 & \cdots & e_n\end{pmatrix} \cdot \underbrace{\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}}_{\text{столбец координат}}$$

Вообще говоря, ${}^nR = \underbrace{{}_RR \oplus \dots \oplus {}_RR}_{n}$; $R^n = \underbrace{R_R \oplus \dots \oplus R_R}_{n}$. Знак равенства здесь означает существование канонического изоморфизма.

Определение 4.1.11 (Прямая сумма модулей)**.** Пусть M, N — левые модули над R. Тогда $M \oplus N \stackrel{def}{=} \{(m,n) | m \in M, n \in N\}$, где действия покомпонентны.

Кстати, ${}^mR \oplus {}^nR = {}^{m+n}R$, и аналогично $R^m \oplus R^n = R^{m+n}$.

И ещё, $\downarrow$

Определение 4.1.12 (Подмодуль P — прямое слагаемое в M)**.** Такой подмодуль, что есть второй подмодуль-слагаемое $\exists Q \leqslant M : P + Q = M$ (сумма по Минковскому), причём $P \cap Q = \{0\}$.

Несложно видеть, что при таких условиях $P + Q \cong P \oplus Q$: отображение $(p,q) \mapsto p + q$ биективно. Инъективность следует из $p_1 + q_1 = p_2 + q_2 \iff \underbrace{p_1 - p_2}_{\in P} = \underbrace{q_2 - q_1}_{\in Q}$, что 0 при данных условиях.

Определение 4.1.13 (Проективный модуль)**.** Такой модуль P, что $\exists Q : P + Q \cong R^n$.

Замечание. Проблема в том, что даже над хорошими коммутативными кольцами проективные модули не факт, что свободны; над ними есть система координат, но нет базиса.

4.2 Линейные отображения

Линейное отображение — это гомоморфизм модулей. Подробнее:

Пусть M, N — два правых модуля-R. Отображение $\phi : M \to N$ называется *R-линейным*, если

1. оно аддитивно $\phi(x + y) = \phi(x) + \phi(y)$
2. и согласовано с умножением на скаляр $\phi(x)\lambda = \phi(x\lambda)$.

Предостережение (Почему мы рассматриваем правые модули). Рассмотрим некоммутативное кольцо R. Зафиксируем некоторую матрицу $\phi \in M(n, R)$. Все линейные отображения ${}^nR$ в себя исчерпываются умножениями на матрицы справа **(??)**

Если обозначать умножение на матрицу за $\overline{\phi}$, то в определении линейности выполняются тождества

$$\overline{\phi}(\lambda x) = \lambda \overline{\phi}(x)$$

Это совсем не значит, что $\phi \cdot (\lambda x) = \lambda \cdot (\phi x)$, так как матрица ϕ может никак не коммутировать со скаляром. Проблема в том, что мы не привыкли записывать отображения наоборот: $(x)\phi$. Таким образом, чтобы не путать умножение на матрицу ϕx, и применение гомоморфизма $\phi(x)$, намного удобнее рассматривать правые модули-R.

4.2.1 Основной пример линейных отображений

Все линейные отображения между свободными модулями — умножения на матрицу линейных отображений:

$$\phi \in M(m,n,R); \quad \phi : R^n \to R^m; \quad x \mapsto \phi x$$

Отображение линейно, так как $\phi(x+y) = \phi(x) + \phi(y)$ — дистрибутивность, и $\phi(x\lambda) = (\phi x)\lambda$ — ассоциативность умножения матриц.

Операция транспонирования помогает ввести биекцию между правыми и левыми действиями на модули: $M(m,n,R) \xrightarrow{t} M(n,m,R^o)$. Так, $(\phi\psi)^t = \psi^t\phi^t$.

Примеры (Примеры линейных отображений).

- Евклидовы движения.
- Линейные (координатные) проекции $e_i^* : R^n \to R$; $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_i$. Несложно видеть, что $e_i^* = f_i$.
- Дифференцирование: $(f+g)' = f'+g'$; $\quad(\lambda f)' = \lambda f'$. Также важнейшей формулой дифференцирования (дифференциальных операторов) является тождество Лейбница $(fg)' = f'g + fg'$.

Лекция XXV

1 декабря 2022 г.

Что можно делать с линейными отображениями?

1. Поточеченая сумма двух линейных отображений — линейное отображение.
2. Обозначим $\mathrm{Hom}(M,N)$ — множество всех R-линейных отображений $M \to N$. Несложно видеть, что Hom — абелева группа по сложению.

   Если M или N — бимодуль, то Hom образует модуль:

   А именно, $\mathrm{Hom}\left({}_SM_R, N_R\right)$ образует правый модуль-S:

   $$\forall \phi \in \mathrm{Hom}\left({}_SM_R, N_R\right), \alpha \in S, x \in M : (\phi\alpha)(x) \coloneqq \phi(\alpha x)$$

   Иначе, $\mathrm{Hom}(M_R, {}_SN_R)$ — левый S-модуль:

   $$\forall \phi \in \mathrm{Hom}(M_R, {}_SN_R), x \in M, \alpha \in S : (\alpha\phi)(x) \coloneqq \alpha \cdot \phi(x)$$

   Таким образом, если R — коммутативное кольцо, то $\mathrm{Hom}_R(M,N)$ — R-бимодуль.
3. Композиция линейных отображений линейна:

   Пусть $\psi : M \to N$; $\quad\phi : N \to P$. Им соответствует $\phi \circ \psi : M \to P$.

   Ассоциативность композиции доказана (**??**), покажем согласованность с умножением на скаляр:

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

   В частности, $\mathrm{End}_R(M) \overset{def}{=} \left\{\phi \in \mathrm{End}(M) \middle| \phi - R\text{-линейно}\right\}$ — ассоциативное кольцо с единицей (id_M). То, что это кольцо, следует из замкнутости по операциям, а также того, что $\mathrm{End}_R(M) \leqslant \mathrm{End}(M) = \mathrm{End}_{\mathbb{Z}}(M)$ (последнее — кольцо, см. (**??**)).

   Замечание. Тождество $\forall \lambda \in R, \phi, \psi \in \mathrm{End}_R(M) : \phi(\lambda\psi) = \lambda(\phi\psi) = (\lambda\phi)\psi$, показывающее согласованность композиции с умножением на скаляр, иногда называют *аксиомой алгебры*.

4.3 Линейная комбинация, линейная оболочка

Определение 4.3.1 (Правая линейная комбинация $x_1, \ldots, x_n \in M$ с коэффициентами $\lambda_1, \ldots, \lambda_n \in R$)**.** $x_1\lambda_1 + \cdots + x_n\lambda_n$.

Замечание. В данном определении при желании можно усмотреть неоднозначность — является ли линейной комбинацией само выражение, или же его значение, как элемент из M? Даже если и так, мне эта неоднозначность поначалу не кажется проблемной, у нас же нет сложностей с понятием суммы, хотя вроде бы та же история.

Возможно, потом я изменю своё мнение.

Определение 4.3.2 (Линейная оболочка элементов $x_1, \ldots, x_n \in M$)**.** Всё множество линейных комбинаций с коэффициентами из R.

$$L(x_1, \ldots, x_n) \stackrel{def}{=} \left\{ x_1\lambda_1 + \cdots + x_n\lambda_n \middle| \lambda_i \in R, i \in 1..n \right\}$$

Определение 4.3.3 (Подмодуль, порождённый элементами $x_1, \ldots, x_n$)**.** Минимальный по включению подмодуль, содержащий $x_1, \ldots, x_n$. Обозначается $\langle x_1, \ldots, x_n \rangle$.

Теорема 4.3.1. Линейная оболочка $L(x_1, \ldots, x_n)$ — в точности $\langle x_1, \ldots, x_n \rangle$.

Доказательство.

$\Rightarrow$. Включение $\subset$ очевидно — всякая линейная комбинация должна содержаться в подмодуле, так как он замкнут относительно сложения и умножения на элементы R.

$\Leftarrow$. Покажем, что $L(x_1, \ldots, x_n)$ — подмодуль.

$$(x_1\lambda_1 + \cdots + x_n\lambda_n) + (x_1\mu_1 + \cdots + x_n\mu_n) = \cdots = x_1(\lambda_1 + \mu_1) + \cdots + x_n(\lambda_n + \mu_n)$$
$$(x_1\lambda_1 + \cdots + x_n\lambda_n)\mu = \cdots = x_1(\lambda_1\mu) + \cdots + x_n(\lambda_n\mu)$$

□

Замечание. Имеет место полезная равносильность

$$\phi : M \to N \text{ линейно} \iff \forall x_i, \lambda_i : \phi(x_1\lambda_1 + \cdots + x_n\lambda_n) = \phi(x_1)\lambda_1 + \cdots + \phi(x_n)\lambda_n$$

которая тривиально доказывается по индукции.

Пусть $X \subset M$, где необязательно $|X| < \infty$. Тогда *линейная комбинация элементов из* X — конечная сумма понятного вида, то есть почти все (кроме конечного числа) $\lambda_x = 0$ в сумме $\sum\limits_{x \in X} x\lambda_x$.

Определение 4.3.4 (Линейная оболочка множества)**.** $L(X) \stackrel{def}{=} \langle X \rangle$ — множество всех линейных комбинаций элементов из X.

Если $M = \langle X \rangle$, то говорят, что X порождает M, или же является системой образующих M.

Чаще всего мы будем изучать ситуации конечнопорождённых модулей — тех, у которых существует конечная система образующих.

4.4 Фактормодули, теорема о гомоморфизме

Пусть $N \leqslant_R M$ — R-модули. Тогда $M/N \stackrel{def}{=} \{x + N | x \in M\}$ — фактормодуль.

Теорема 4.4.1. Операции по Минковскому задают на M/N структуру R-модуля, причём

$$\pi : M \to M/N; \quad x \mapsto x + N$$

является R-линейным отображением.

Доказательство.

- M/N — абелева группа по сложению: $(x+N)+(y+N)=(x+y)+N$.
- $(x+N)\lambda = x\lambda + N$, так как N содержит кратные всех своих элементов.
- Тождества выполняются, так как операции определены в терминах представителей. □

4.4.1 Теорема о гомоморфизме

Пусть $\phi : M \to N$. С отображением можно связать два подмодуля: $\operatorname{Ker}(\phi) = \{x \in M | \phi(x) = 0\} \leqslant M$ и $\operatorname{Im}(\phi) = \{y \in N | \exists x \in M : \phi(x) = y\} \leqslant N$.

Теорема 4.4.2 (О гомоморфизме)**.** $\forall \phi : M \to N$, где ϕ линейно, имеет место изоморфизм

$$\operatorname{Im}(\phi) \cong M/\operatorname{Ker}(\phi)$$

Замечание. Фактор по ядру ещё обозначают $M/\operatorname{Ker}(\phi) = \operatorname{CoIm}(\phi)$ — кообраз.

Фактор по образу ещё обозначают $\operatorname{CoKer}(\phi) = N/\operatorname{Im}(\phi)$ — коядро (в данной теореме фактор по образу не используется, но вообще серьёзным отличием от произвольных некоммутативных групп является именно то, что образ — подгруппа, поэтому по нему можно устроить фактормодуль, что позднее пригодится).

Доказательство. Данный изоморфизм выглядит так: $\overline{\phi} : M/\operatorname{Ker}(\phi) \to \operatorname{Im}(\phi); \quad x + \operatorname{Ker}(\phi) \mapsto \phi(x)$.

Проверим корректность определения данного изоморфизма

$$x + \operatorname{Ker}(\phi) = y + \operatorname{Ker}(\phi) \iff x - y \in \operatorname{Ker}(\phi) \iff \overline{\phi}(x + \operatorname{Ker}(\phi)) = \overline{\phi}(y + \operatorname{Ker}(\phi))$$

(данная выкладка заодно и инъективность проверяет);

проверим сюръективность данного изоморфизма ($z = \phi(x) \Rightarrow z = \overline{\phi}(x + \operatorname{Ker}(\phi))$);

проверим, что изоморфизм является гомоморфизмом (он же определён в терминах представителей)

$$\overline{\phi}(x + \operatorname{Ker}(\phi)) + \overline{\phi}(y + \operatorname{Ker}(\phi)) = \phi(x) + \phi(y) = \phi(x+y) = \overline{\phi}(x + y + \operatorname{Ker}(\phi))$$ □

4.4.2 Сумма и пересечение подмодулей, теорема Нётер об изоморфизме

Пусть $L, N \leqslant M$ — подмодули.

Определение 4.4.1 (Сумма подмодулей)**.** Сумма по Минковскому. Является подмодулем:

$$\forall x_1, x_2 \in L, \forall y_1, y_2 \in N : \quad (x_1 + y_1) + (x_2 + y_2) = \underbrace{(x_1 + x_2)}_{\in L} + \underbrace{(y_1 + y_2)}_{\in N}$$

и к тому же

$$\forall x \in L, \forall y \in N : \quad (x+y)\lambda = \underbrace{x\lambda}_{\in L} + \underbrace{y\lambda}_{\in N}$$

Над нётеровым кольцом (**??**) подмодули конечно порождённого модуля конечно порождены.

Доказательство. Для простоты рассмотрим случай коммутативного кольца R.

Индукция по количеству порождающих модуль.

<u>База:</u> Докажем, что подмодули R-модуля $\langle x \rangle$ конечно порождены. Рассмотрим произвольный подмодуль $N \leqslant \langle x \rangle$. Положим $I \coloneqq \{\lambda \in R | x\lambda \in N\}$.

Несложно проверить по определению, что $I \trianglelefteqslant R$.

Получается, $N = \langle xi_1, \ldots, xi_s \rangle$, где $i_1, \ldots, i_s$ — элементы, порождающие идеал.

<u>Переход:</u> Пусть $M \coloneqq \langle x_1, \ldots, x_n \rangle$. Рассмотрим произвольный подмодуль $L \leqslant M$.

Обозначим $M' \coloneqq \langle x_1, \ldots, x_{n-1} \rangle$ и $L' \coloneqq L \cap M'$. Согласно индукционному предположению, L' конечно порождён; пусть $L' = \langle l_1, \ldots, l_m \rangle$.

Аналогично убедимся, что $J \coloneqq \{\lambda \in R | x_n \lambda \in L\} \trianglelefteqslant R$ — идеал. Обозначим элементы, его порождающие $j_1, \ldots, j_k$.

Теперь несложно видеть, что $L = \langle l_1, \ldots, l_n, x_n j_1, \ldots, x_n j_k \rangle$. □

Определение 4.4.2 (Пересечение подмодулей)**.** Теоретико-множественное пересечение. Является подмодулем.

Опять же, $L, N \leqslant M$ — подмодули.

Теорема 4.4.3 (Нётер)**.** $(L + N)/L \cong N/(L \cap N)$.

Доказательство. Построим гомоморфизм $\phi : N \to (L + N)/L; \quad y \mapsto y + L$.

ϕ является гомоморфизмом; он сюръективен; наконец, его ядро $\{y \in N | y + L = L\} = L \cap N$. □

Следствие 4.4.1. *Важным следствием является теорема о размерности суммы и пересечения (??)*

4.5 Линейная зависимость и независимость

Определение 4.5.1 (Векторы $x_1, \ldots, x_n$ линейно зависимы)**.** $\exists \lambda_1, \ldots, \lambda_n \in R$, не все равные нулю (линейная комбинация нетривиальна), такие, что $\sum\limits_{i=1}^{n} x_i \lambda_i = 0$.

Если же таких не нашлось, то они линейно независимы.

Замечание. Встречаются линейно-зависимые множества из одного элемента. Так, рассмотрим $\mathbb{Z}/m\mathbb{Z}$ – модуль над $\mathbb{Z}$. $\overline{1} = 1 + m\mathbb{Z}$.

$$m \neq 0, \text{ но } m \cdot \overline{1} = m\mathbb{Z} = \overline{0}$$

Определение 4.5.2 (Элемент кручения $x \in M$)**.** Как раз такой элемент: $\exists \lambda \in R \setminus \{0\} : x\lambda = 0$.

Определение 4.5.3 (Базис)**.** Линейно независимая система образующих.

Примеры (Примеры линейно независимых систем).

- $M = \mathbb{C}, R = \mathbb{R}$. Например, $\{1, i\}$ является базисом.
- $\mathbb{H}$ над $\mathbb{R}$. Например, $\{1, i, j, k\}$ является базисом.
- R^n над R. Можно взять стандартный базис $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \end{pmatrix}, \ldots$
- ${}^nR$. Опять-таки, есть много базисов, мы уже знаем стандартный.
- $R[t]$. Стандартный базис — $1, t, t^2, \ldots$
- $R[[t]]$ — формальные степенные ряды. Здесь $1, t, t^2, \ldots$ — не базис в нашем определении (есть элементы, которые не получаются, как конечная линейная комбинация элементов базиса).
- $M(m, n, R)$. Здесь базис — матричные единицы $\{e_{i,j}\}_{i=1..m; j=1..n}$.

Замечание. В отличие от векторных пространств, в модулях над кольцом, не являющимся полем, базис существует редко, так как в кольце делить нельзя.

Лекция XXVI

7 декабря 2022 г.

Пусть $X \subset M$ — произвольное подмножество.

Определение 4.5.4 (X линейно зависимо)**.** В X найдётся конечное линейно зависимое подмножество.

В противном случае, очевидно, X — *линейно независимо*.

4.5.1 Свободные модули

Определение 4.5.5 (Свободный модуль)**.** Модуль, у которого есть базис.

Лемма 4.5.1. *Если $\{x_1, \dots, x_n\}$ — базис модуля-R M, то*

$$\forall x \in M : \exists! \lambda_1, \dots, \lambda_n \in R : x = x_1\lambda_1 + \dots + x_n\lambda_n$$

Здесь элементы $\lambda_1, \dots, \lambda_n$ называются координатами *элемента x.*

Доказательство. Существование вытекает из того, что базис — система образующих. Единственность легко доказать от противного: в случае двух различных равных линейных комбинаций, их разность равна 0, но это — нетривиальная линейная комбинация. □

Рассмотрим координаты в базисе, как функции $R^n \to M$. Несложно видеть, что такие функции оказались линейными:

$$x = x_1\lambda_1 + \dots + x_n\lambda_n; \quad y = x_1\mu_1 + \dots + x_n\mu_n \quad \Rightarrow \quad x + y = x_1(\lambda_1 + \mu_1) + \dots + x_n(\lambda_n + \mu_n)$$
$$x = x_1\lambda_1 + \dots + x_n\lambda_n; \quad \Rightarrow \quad x \cdot \mu = x_1(\lambda_1 \cdot \mu) + \dots + x_n(\lambda_n \cdot \mu)$$

Лемма 4.5.2. *Всякий свободный модуль-R с базисом $\{x_1, \dots, x_n\}$ изоморфен R^n. Аналогично, свободный R-модуль изоморфен ${}^nR$.*

Доказательство. Задаём произвольным образом изоморфизм на базисе, он по линейности продлевается на всё пространство. □

Замечание. Свободные модули существуют и при базисах произвольного размера (мощности). Так, $R[x]$ — свободный модуль над R, например, есть стандартный базис $\{1, x, x^2, \dots\}$.

Тем не менее при использовании данных определений, стандартные мономы $\{1, x, x^2, \dots\}$ не образуют базиса кольца формальных степенных рядов $R[[x]]$, так как там встречаются (и часто) элементы, не представимые в виде конечной линейной комбинации элементов базиса.

Универсальное свойство базиса

Теорема 4.5.1. Множество $\{u_1, \dots, u_n\} \subset M$ является базисом в M, если и только если для любого модуля N, для любых n его элементов $x_1, \dots, x_n \in N$, найдётся единственное линейное отображение $\phi : M \to N$, переводящее $u_i \mapsto x_i$.

Доказательство.

$\Rightarrow$. Определим ϕ на базисе, как требуется: $\phi(u_i) = x_i$ и продлим его по линейности на всё остальное M. Корректность и линейность следуют из единственности координат.

Единственность такого отображения ϕ приятно показать так:

$$\phi(u_1\mu_1 + \dots + u_n\mu_n) = \phi(u_1)\mu_1 + \dots + \phi(u_n)\mu_n$$

$\Leftarrow$. Предположим противное: $\{u_1, \ldots, u_n\}$ — не система образующих. $\exists u \notin \langle u_1, \ldots, u_n \rangle$. Рассмотрим $N = M/\langle u_1, \ldots, u_n \rangle$. В силу сделанного предположения, $N \neq \{0\}$.

Таким образом, существуют как минимум 2 отображения $M \to M$, переводящие все u_i в 0 — каноническая проекция, и тождественный 0, противоречие.

Теперь предположим, что $\{u_1, \ldots, u_n\}$ — линейно зависимы. Рассмотрим $N = R^n$ и выберем в нём базис $\{x_1, \ldots, x_n\}$.

Так как существует линейное $\phi : M \to N$, такое, что $\phi : u_i \mapsto x_i$, то $\{x_1, \ldots, x_n\}$ тоже линейно зависимы, но это базис, противоречие. □

Приведём несколько фактов про свободные модули и линейные отображения:

- **Лемма 4.5.3.** *Линейное отображение между свободными модулями инъективно, если и только если оно переводит линейно независимые системы в линейно независимые.*

  Доказательство.

  $\Rightarrow$. От противного: ϕ линейно и инъективно, $u_1, \ldots, u_n$ линейно независимы, но получилось так, что $\phi(u_1)\lambda_1 + \cdots + \phi(u_n)\lambda_n = 0$. Согласно линейности ϕ получаем $\phi(u_1\lambda_1 + \cdots + u_n\lambda_n) = 0$. Так как $\phi(0) = 0$, то из-за инъективности $u_1\lambda_1 + \cdots + u_n\lambda_n = 0$, противоречие.

  $\Leftarrow$. От противного: $\operatorname{Ker}\phi \neq \{0\}$, то есть $\exists \lambda_1 u_1 + \cdots + \lambda_n u_n \neq 0$ (для базиса $\{u_1, \ldots, u_n\}$). Значит, образ базиса линейно зависим, противоречие. □

- **Лемма 4.5.4.** *Линейное отображение между свободными модулями сюръективно, если и только если оно переводит системы образующих в системы образующих.*

  Доказательство.

  $\Rightarrow$. Всякая система образующих, образовывающая x с коэффициентами $\lambda_1, \ldots, \lambda_n$, будет образовывать $\phi(x)$ с такими же коэффициентами.

  $\Leftarrow$. Покажем, что у всякого элемента x есть прообраз: рассмотрим произвольную систему образующих $u_1, \ldots, u_n$, разложим $x = \phi(u_1)\lambda_1 + \cdots + \phi(u_n)\lambda_n$ по образу данной системы, после чего воспользуемся линейностью: $x = \phi(u_1\lambda_1 + \cdots + u_n\lambda_n)$. □

- **Лемма 4.5.5.** *Два свободных R-модуля изоморфны, если и только если в них найдутся два равномощных базиса.*

  Замечание. В силу проблемы о единственности ранга, необязательно **любые** два базиса будут равномощны, даже если найдётся парочка. Об этом позже.

  Доказательство.

  $\Rightarrow$. Выберем в первом R-модуле произвольный базис, и рассмотрим его образ, как базис во втором. Он — действительно базис — в силу предыдущих лемм.

  $\Leftarrow$. Пусть нашлись два равномощных базиса. Зададим отображение, биективно переводящее один из них — в другой. Согласно универсальному свойству базиса, это отображение единственным образом доопределяется на остальных элементах.

  Также несложно показать по отдельности его инъективность и сюръективность. □

Лекция XXVII

8 декабря 2022 г.

Рассмотрим V — модуль над **полем** K. Модуль над кольцом, являющимся полем (вообще говоря, над телом, но мы будем рассматривать поля), называется *векторным пространством*.

4.6 Линейная зависимость над полем

Рассмотрим V — векторное пространство над полем K.

Замечание. Несколько раз ниже будет встречаться запись $v_1, \ldots, \widehat{v_j}, \ldots, v_n$, обозначающая набор векторов $v_1, \ldots, v_n$, среди которых удалили v_j.

Лемма 4.6.1. *$v_1, \ldots, v_n$ линейно зависимы $\iff$ один из них — линейная комбинация остальных.*

Доказательство.

$\Leftarrow$. $v_j \in \langle v_1, \ldots, \widehat{v_j}, \ldots, v_n \rangle \Rightarrow v_j = \sum\limits_{i=1; i\neq j}^{n} \lambda_i v_i \Rightarrow \sum\limits_{i=1; i\neq j}^{n} \lambda_i v_i + (-1) \cdot v_j = 0.$

$\Rightarrow$. Пусть есть нетривиальная нулевая линейная комбинация $\sum\limits_{i=1}^{n} \lambda_i v_i = 0$.

Нетривиальность означает $\exists j : \lambda_j \neq 0$. Перенесём $\lambda_j v_j$ в другую часть и поделим на $-\lambda_j$. □

Следствие 4.6.1. *Если $\{v_1, \ldots, v_n\}$ линейно независимы, и $x \notin \langle v_1, \ldots, v_n \rangle$, то $\{v_1, \ldots, v_n, x\}$ линейно независимо.*

Следствие 4.6.2. *Если $\{v_1, \ldots, v_n\}$ линейно независимы, а $\{v_1, \ldots, v_n, x\}$ линейно зависимы, то $x \in \langle v_1, \ldots, v_n \rangle$.*

Теорема 4.6.1 (Штейниц о линейной зависимости линейных комбинаций)**.**

Если $u_1, \ldots, u_m \in \langle v_1, \ldots, v_n \rangle$, причём $m > n$, то $\{u_1, \ldots, u_m\}$ линейно зависимы.

Доказательство методом исключения. Индукция по n.

База: $n = 1$. В таком случае $u_1 = v_1\lambda; u_2 = v_1\mu$. Если $\lambda = 0$, то $u_1 = 0$, и система $\{u_1, u_2\}$ линейно зависима. Иначе $\lambda \neq 0$, тогда $u_2 = u_1\mu\lambda^{-1}$.

Переход: Если $u_1, \ldots, u_m \in \langle v_1, \ldots, v_{n-1} \rangle$, то применим индукционное предположение.

Иначе $\exists j : u_j = \sum\limits_{i=1}^{n} v_i\lambda_{i,j}$, такое, что $\lambda_{n,j} \neq 0$. Без потери общности $j = m$. Получается,

$$v_n \in \langle v_1, \ldots, v_{n-1}, u_m \rangle$$

Положим $w_i = u_i - u_m \cdot \lambda_{n,m}^{-1} \cdot \lambda_{n,i} = \sum\limits_{k=1}^{n} v_k \cdot \lambda_{k,i} - \sum\limits_{k=1}^{n} v_k \cdot \lambda_{k,m} \cdot \lambda_{n,m}^{-1} \cdot \lambda_{n,i}$ для $i \in [1; m)$.

Несложно видеть, что $w_i \in \langle v_1, \ldots, v_{n-1} \rangle$ — коэффициент перед v_n обращается в 0. Согласно индукционному предположению, $\{w_1, \ldots, w_{m-1}\}$ линейно зависимы.

Значит, существуют не все нулевые коэффициенты $\alpha_1, \ldots, \alpha_{m-1}$, такие, что $\sum\limits_{i=1}^{m-1} w_i\alpha_i = 0$. Выразив w_i через u_i, получим $\left(\sum\limits_{i=1}^{m-1} u_i\alpha_i\right) + u_m \cdot A = 0$, где $A \in K$. Эта комбинация нетривиальна, так как среди α_i есть ненулевой коэффициент. □

Теорема 4.6.2 (Штейниц. Обобщение предыдущей)**.** Пусть $u_1, \ldots, u_m \in \langle v_1, \ldots, v_n \rangle$, причём $\{u_1, \ldots, u_m\}$ линейно независимы. Тогда можно так перенумеровать $v_1, \ldots, v_n$, что $\langle v_1, \ldots, v_n \rangle = \langle u_1, \ldots, u_m, v_{m+1}, v_n \rangle$.

Доказательство методом замены.

Лемма 4.6.2 (Штейниц о замене)**.** $\left.\begin{array}{c} x \notin \langle v_1, \ldots, v_{n-1} \rangle \\ x \in \langle v_1, \ldots, v_{n-1}, v_n \rangle \end{array}\right\} \Rightarrow \langle v_1, \ldots, v_{n-1}, v_n \rangle = \langle v_1, \ldots, v_{n-1}, x \rangle.$

Доказательство леммы.

Из нижней строчки системы $x = \sum\limits_{i=1}^{n} \lambda_i v_i$. Из верхней следует $\lambda_n \neq 0$.

Тогда получается, что $v_n \in \langle x, v_1, \ldots, v_{n-1} \rangle$. □

Индукция по n.

База: $n = 1$. В таком случае $u_1 \in \langle v_1 \rangle$, откуда $\langle u_1 \rangle = \langle v_1 \rangle$. После этого из линейной независимости $u_1, \ldots, u_m$ следует $m = 1$.

Переход:

- Если $u_1, \ldots, u_m \in \langle v_2, \ldots, v_n \rangle$, то применим индукционное предположение.

  Иначе $\exists i : u_i \notin \langle v_2, \ldots, v_n \rangle$. Без потери общности, $i = 1$.

  Используя лемму о замене, получаем $\langle v_1, v_2, \ldots, v_n \rangle = \langle u_1, v_2, \ldots, v_n \rangle$.

- Если $u_2, \ldots, u_m \in \langle u_1, v_3, \ldots, v_n \rangle$, то применим индукционное предположение. Здесь стоит упомянуть, что в результате доказательства u_1 останется, так как u_i линейно независимы.

  Иначе $\exists i : u_i \notin \langle u_1, v_3, \ldots, v_n \rangle$. Без потери общности $i = 2$.

  Используя лемму о замене, получаем $\langle v_1, \ldots, v_n \rangle = \langle u_1, u_2, v_3, \ldots, v_n \rangle$.

- И так далее. Если в какой-то момент не останется ни одного v_i, то из линейной независимости u_i получаем, что и u_i тоже кончатся. □

4.7 Минимальные системы образующих. Максимальные независимые системы

Пусть V — векторное пространство над полем K.

Теорема 4.7.1. Касательно минимальной системы образующих

$v_1, \ldots, v_n$ — базис $V \iff v_1, \ldots, v_n$ — минимальная (по включению) порождающая система.

Доказательство.

$\Rightarrow$. Если базис — не минимальная система, то $\exists v_j$, которое можно исключить, то есть $v_j \in \langle v_1, \ldots, \widehat{v_j}, \ldots v_n \rangle$, и векторы линейно зависимы.

$\Leftarrow$. Если $v_1, \ldots, v_n$ линейно зависимы, то опять же можно найти $v_j \in \langle v_1, \ldots, \widehat{v_j}, \ldots, v_n \rangle$, и порождающая система не минимальна. □

Касательно максимальной независимой системы

$v_1, \ldots, v_n$ — базис $V \iff v_1, \ldots, v_n$ — максимальная линейно независимая система.

Доказательство.

$\Rightarrow$. Если базис — не максимальная система, то $\exists x$, которое можно добавить, то есть $x \notin \langle v_1, \ldots, \widehat{v_j}, v_n \rangle$, и получили противоречие с тем, что $\{v_1, \ldots, v_n\}$ — базис.

$\Leftarrow$. Если $v_1, \ldots, v_n$ — не порождающая система то опять же можно найти $x \notin \langle v_1, \ldots, v_n \rangle$, тогда $\{v_1, \ldots, v_n, x\}$ — опять линейно незавивимая система, значит, была не максимальная. □

Получили пять критериев базиса:

1. Определение: линейно-независимая система образующих.
2. Любой вектор единственным образом раскладывается по базису.

3. Универсальное свойство.

Пусть V — векторное пространство, необязательно конечное.

Теорема 4.7.2. Касательно максимальной независимой системы

Всякую линейно независимую систему X можно дополнить до базиса.

Доказательство. Рассмотрим Ω — множество всех линейно независимых подмножеств V, содержащих X.

Всякая цепочка мажорируется её объединением, применим лемму Куратовского — Цорна. □

Касательно минимальной системы образующих

Из всякой системы образующих X можно выделить базис.

Доказательство. Рассмотрим Ω — множество всех линейно независимых систем, являющихся подмножествами X.

Среди них найдётся максимальная — аналогично предыдущему случаю. Назовём её Y.

Докажем, что она — система образующих. От противного: $\exists v \in V : v \notin \langle Y \rangle$. Так как X — базис, то $v = \sum\limits_{i=1}^{n} x_i \lambda_i$.

Так как $v \notin \langle Y \rangle$, то $\exists x_i : x_i \notin \langle Y \rangle$. Значит, можно просто дополнить Y этим элементом x_i, получаем противоречие с максимальностью Y. □

Замечание. В случае $\dim(V) < \infty$ лемма Куратовского — Цорна не нужна. Цепочка оборвётся уже на конечном шаге, так как не построить линейно независимое множество, имеющее элементов больше $\dim(V)$.

Интересный факт. В любом векторном пространстве любые два базиса равномощны, как множества — при условии аксиомы выбора, разумеется.

В конечномерном пространстве это следует из теоремы Штейница.

Лекция XXVIII

14 декабря 2022 г.

4.8 Размерность векторного пространства

Определение 4.8.1 (Размерность векторного пространства)**.** Количество элементов любого базиса. Как упомянуто выше, при условии аксиомы выбора размерность определена однозначно.

Если $\dim V < \infty$, то V называют бесконечномерным.

Примеры.

- $\dim_{\mathbb{R}} \mathbb{C} = 2$.
- $\dim_{\mathbb{C}} \mathbb{C} = 1$.
- $\dim_{\mathbb{Q}} \mathbb{R} = \infty$. В предположении аксиомы выбора можно сказать точнее: $\dim_{\mathbb{Q}} \mathbb{R} = 2^{\aleph_0}$.
- $\dim_{\mathbb{F}_q} \mathbb{F}_{q^m} = m$. В общем случае, $\dim_K L = |L : K|$, если $K \hookrightarrow L$.
- $\dim_K K^n = \dim_K {}^nK = n$.
- $\dim_K M(m, n, K) = m \cdot n$.
- $\dim_K K[t] = \infty$, а именно, $\aleph_0$.

- $\dim_K K(t) = \max\{\aleph_0, |K|\}$, где $K(t)$ — кольцо рациональных дробей. Доказательство будет позднее.

Теорема 4.8.1. Пусть $\dim(V) = n < \infty$. Тогда для $v_1, \ldots, v_n \in V$ следующие условия эквивалентны:

- $v_1, \ldots, v_n$ — базис.
- $v_1, \ldots, v_n$ — система образующих.
- $v_1, \ldots, v_n$ — линейно независимы.

Доказательство. Все базисы конечномерного пространства имеют одинаковый размер. □

Следствие 4.8.1. *В предположении* $U \leqslant V, \dim V < \infty$ *выполняется равносильность* $U = V \iff \dim U = \dim V$.

4.9 Относительные базисы

Пусть $U \leqslant V$ — два векторных пространства над K.

Определение 4.9.1 (Система образующих V относительно U)**.** Такие $v_1, \ldots, v_n \in V$, что $V = U + \langle v_1, \ldots, v_n \rangle$.

Определение 4.9.2 (Линейная независимость $v_1, \ldots, v_n \in V$ относительно U)**.** $\forall \lambda_1, \ldots, \lambda_n : v_1\lambda_1 + \cdots + v_n\lambda_n \in U \iff \lambda_1 = \cdots = \lambda_n = 0$.

Определение 4.9.3 (Базис V относительно U)**.** Линейно независимые $v_1, \ldots, v_n$, являющиеся системой образующих V относительно U.

Теорема 4.9.1. Следующие условия эквивалентны.

- $v_1, \ldots, v_n$ — базис V относительно U.
- $\forall v \in V : \exists! u \in U, \exists! \lambda_1, \ldots, \lambda_n \in K : v = u + v_1\lambda_1 + \cdots + v_n\lambda_n$.
- $v_1 + U, \ldots, v_n + U$ — базис факторпространства V/U.
- $v_1, \ldots, v_n$ — дополнение какого-то (любого) базиса U до базиса V.

Доказательство. Было приведено на лекции. Аналогично доказательству аналогичных фактов про абсолютные базисы. □

Теорема 4.9.2. Для любого подпространства $U \leqslant V$ существует базис V относительно U; любые два относительных базиса V относительно U состоят из равного количества элементов.

Доказательство. Каждому базису V относительно U соответствует базис V/U. □

Определение 4.9.4 (Коразмерность)**.** Количество элементов в относительном базисе V/U. Обозначается $\operatorname{codim}(U, V)$.

Следствие 4.9.1. *Если* $\dim V < \infty$*, то* $\operatorname{codim}(U, V) = \dim(V) - \dim(U)$.

Определение 4.9.5 ($U \leqslant V$ имеет конечную коразмерность в V)**.** $\operatorname{codim}(U, V) < \infty$. Если $\operatorname{codim}(U, V) = 1$, то U называется *гиперплоскостью* в V.

4.10 Теоремы о размерности ядра, образа, суммы, пересечения

Пусть $\phi : U \to V$ — гомоморфизм.

Теорема 4.10.1 (Former Theorem of Linear Algebra, о размерности ядра и образа)**.**

$$\dim(\operatorname{Ker}\phi) + \dim(\operatorname{Im}\phi) = \dim(U)$$

Доказательство. Теорема о гомоморфизме: $U/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$. □

Теорема 4.10.2. $U \cong V \iff \dim(U) = \dim(V)$.

Доказательство. Критерий изоморфизма свободных модулей **(??)**. □

Теорема 4.10.3 (О размерности суммы и пересечения)**.** Пусть $U, W \leqslant V$. Выполняется

$$\dim(U+W) + \dim(U \cap W) = \dim(U) + \dim(W)$$

Для удобства доказательства считаем $\dim V < \infty$

Доказательство. Согласно теореме Нётер об изоморфизме **(??)**, выполняется $\dim((U+W)/U) = \dim(W/(U \cap W))$.

Отсюда $\operatorname{codim}(U, U+W) = \operatorname{codim}(U \cap W, W)$, или же $\dim(U) + \dim(W) = \dim(U \cap W) + \dim(U+W)$. □

Определение 4.10.1 (Прямая сумма подпространств $U, W \leqslant V$)**.** $U \oplus W = U + W$, если $U \cap W = \{0\}$.

4.11 Матрица перехода от базиса к базису

Пусть V — конечномерное векторное пространство, правый модуль над R.

Рассмотрим два базиса, назовём один из них $u_1, \ldots, u_n$ — старый базис; а другой $v_1, \ldots, v_n$ — новый базис.

Выразим новый базис через старый:

$$\begin{array}{ccc} u_1\lambda_{1,1} & \cdots & u_1\lambda_{1,n} \\ + & & + \\ \vdots & \ddots & \cdots \\ + & & + \\ u_n\lambda_{n,1} & \cdots & u_n\lambda_{n,n} \\ \| & & \| \\ v_1 & \cdots & v_n \end{array}$$

Данное семейство вертикальных равенств написано для соответствия с конспектом лектора, в котором написано всего-навсего $v_j = \sum\limits_{i=1}^{n} u_i\lambda_{i,j}$. Сдаётся мне, в случае левых R-модулей всё было бы более горизонтально, но я решил не совершать изменений.

Матрица $(\lambda_{i,j})_{1 \leqslant i,j \leqslant n} \stackrel{def}{=} (u \rightsquigarrow v)$ — матрица перехода от базиса u к базису v.

Заметим, что j-й столбец этой матрицы — столбец координат v_j в базисе $u_1, \ldots, u_n$. Будем его обозначать $[v_j]_u$; вообще, в записи $x = \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{[x]_u}$ так обозначим столбец координат.

Здесь мы не пользовались тем, что K — поле, достаточно работать с кольцом, в котором выполняется единственность ранга (в случае отсутствия единственности матрица перехода неквадратная, что вызывает некоторые неожиданные следствия).

Из определения перемножения матриц $\begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} = \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} (u \rightsquigarrow v)$. В частности,

$$v_j = \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} \cdot \begin{pmatrix} \lambda_{1,j} \\ \vdots \\ \lambda_{n,j} \end{pmatrix}$$

Лемма 4.11.1.

1. $(u \rightsquigarrow u) = 1_{GL(n,K)} \in GL(n, K)$ — *очевидно.*
2. $(u \rightsquigarrow v) = (v \rightsquigarrow u)^{-1}$ — *вытекает из следующего для* $w = u$.
3. $(u \rightsquigarrow v) \cdot (v \rightsquigarrow w) = (u \rightsquigarrow w)$.

Доказательство.

$$\begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} = \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} (u \rightsquigarrow v)$$
$$\begin{pmatrix} w_1 & \cdots & w_n \end{pmatrix} = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} (v \rightsquigarrow w)$$

откуда

$$\begin{pmatrix} w_1 & \cdots & w_n \end{pmatrix} = \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} (u \rightsquigarrow v)(v \rightsquigarrow w) \qquad \square$$

Интересный факт. Invariant Basis Number — единственность ранга. Автоматически выполнено, если R — коммутативно: если $R^n \cong R^m$, то $n = m$ для коммутативного кольца.

Лекция XXIX

15 декабря 2022 г.

4.12 Преобразования координат вектора

Пусть $x \in R^n$, где $x = \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} \underbrace{\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}}_{[x]_u} = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} \underbrace{\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}}_{[x]_v}$.

Запишем

$$x = \underbrace{\begin{pmatrix} u_1 & \dots & u_n \end{pmatrix} (u \rightsquigarrow v)}_{\begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix}} (u \rightsquigarrow v)^{-1} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

Но разложение по базису единственно.

Теорема 4.12.1. Координаты вектора преобразуются *контравариантно* по отношению к преобразованиям базиса:

$$\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} = (u \rightsquigarrow v)^{-1} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

4.13 Базис модуля линейных отображений

Пусть R^m, R^n — два свободных модуля над коммутативным кольцом R. Ниже мы покажем, что всякое линейное преобразование $R^m \to R^n$ имеет вид $x \mapsto Cx$, где $C \in M(n, m, R)$.

Теорема 4.13.1. $\mathrm{Hom}_R(R^m, R^n)$ — свободный R-модуль, в качестве базиса которого можно взять $\phi_{i,j} : R^m \to R^n$, где $i = 1..n, j = 1..m$, а само отображение $\phi_{i,j}(u_h) = \delta_{j,h} v_i$, где $u_1, \ldots, u_m$ — базис R^m, а $v_1, \ldots, v_n$ — базис R^n.

Доказательство.

- Возьмём произвольный $\phi \in \mathrm{Hom}_R(R^m, R^n)$. Он полностью определяется заданием своих значений на базисных векторах $u_1, \ldots, u_m \in R^n$. Заведём матрицу $(\lambda_{i,j})_{i=1..n, j=1..m}$, где $\lambda_{*,j} = [\phi(u_j)]_v$ — столбец координат $\phi(u_j)$ в разложении по базису v.

  Рассмотрим сумму, где $\phi_{i,j}$ определён на базисе, как $\phi_{i,j}(u_h) = \delta_{j,h} v_i$, и продолжен на всё пространство по линейности:

  $$\left(\sum_{i,j} \lambda_{i,j} \phi_{i,j} \right) (u_h) = \sum_i \lambda_{i,h} v_i = \sum_i v_i \lambda_{i,h} = \phi(u_h)$$

  Несложно видеть, что $\phi = \sum\limits_{i,j} \lambda_{i,j} \phi_{i,j}$ — равенство выполняется при аргументах из базиса u, чего достаточно.

- Покажем линейную независимость $\{\phi_{i,j}\}$: пусть нашлись такие коэффициенты $\lambda_{i,j}$, что:

  $$\left(\sum_{i,j} \lambda_{i,j} \phi_{i,j} \right) = 0$$

  Это равносильно тому, что любой базисный вектор переходит в 0.

  $$0 = \left(\sum_{i,j} \lambda_{i,j} \phi_{i,j} \right) (u_h) = \sum_i \lambda_{i,h} v_i = \sum_i v_i \lambda_{i,h}$$

  Но v_i — базис, он линейно независим, значит, $\forall i, h : \lambda_{i,h} = 0$, противоречие. □

Замечание. В доказательстве выше была крайне существенна коммутативность.

4.13.1 Матрица линейного отображения

Какой смысл имеет матрица координат $\phi \in \mathrm{Hom}_R(R^m, R^n)$ в базисе $\{\phi_{i,j}\}_{i=1..n, j=1..m}$?

Матрица строится по двум базисам u и v.

$$\phi = \sum_{i,j} c_{i,j} \phi_{i,j}; \quad \text{Рассмотрим } C = \{c_{i,j}\}_{i=1..n, j=1..m}$$

Заметим, что здесь $C_{*,j}$ — координаты разложения $\phi(u_j)$ в базисе v.

Теорема 4.13.2. $\forall x \in R^m : [\phi(x)]_v = C \cdot [x]_u$.

Доказательство. $x = \sum\limits_{j=1}^{m} u_j x_j \Rightarrow \phi(x) = \sum\limits_{j=1}^{m} \phi(u_j) x_j$.

Так как $\phi(u_j) = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} C_{*,j}$, то $\phi(x) = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} \sum\limits_{j=1}^{m} C_{*,j} x_j = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} C \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$.

□

Таким образом, мы видим, что никаких других линейных отображений в коммутативном кольце между конечномерными модулями нет:

Следствие 4.13.1. $\mathrm{Hom}_R(R^m, R^n) = M(n, m, R)$ *при стандартном выборе базиса.*

4.14 Двойственный модуль. Ковекторы, они же линейные функционалы

Ключевая идея конечномерной линейной алгебры — двойственность.

Пусть R — коммутативное кольцо, а M — модуль-R.

Определение 4.14.1 (Множество линейных отображений; двойственный к M модуль)**.**

$$M^* = \mathrm{Hom}_R(M, R)$$

Всякое $\eta \in M^*$ — разумеется, линейное отображение, но для двойственных модулей будем называть $\eta \in M^*$ — *линейный функционал*, он же *ковектор*.

$$\eta : M \to R; \quad \forall x, y \in M : \eta(x + y) = \eta(x) + \eta(y); \quad \forall \lambda \in R : \eta(x\lambda) = \eta(x)\lambda$$

Введём структуру R-модуля на M^*:

$$(\eta + \theta)(x) = \eta(x) + \theta(x); \quad (\lambda\eta)(x) = \lambda\eta(x)$$

Если не требовать коммутативности кольца, то существенно, что скаляр умножается на линейный функционал слева. Таким образом, при M — правом модуле-R — двойственный модуль M^* является левым R-модулем.

Нас будут интересовать случаи, когда M — свободный.

Теорема 4.14.1. $(R^n)^* = {}^nR$.

Доказательство. Согласно **(??)**, $(R^n)^* = M(1, n, R) = {}^nR$. □

Таким образом, при применении элемента двойственного модуля к элементу модуля, получится элемент кольца:

$$M^* \times M \to R$$
$$\eta, x \mapsto \eta(x)$$

В частности,

$${}^nR \times R^n \to R$$
$$\underbrace{\begin{pmatrix}\eta_1 & \cdots & \eta_n\end{pmatrix}}_{\text{ковектор}}, \underbrace{\begin{pmatrix}x_1 \\ \vdots \\ x_n\end{pmatrix}}_{\text{вектор}} \mapsto \sum_{i=1..n} \eta_i x_i$$

Данное отображение $M^* \times M$ называется *каноническим спариванием*.

4.14.1 Двойственный базис. Преобразования координат ковектора

В предыдущем параграфе построен базис $\mathrm{Hom}_R(R^m, R^n)$.

В частности, $e_1^*, \ldots, e_n^*$ — базис $(R^n)^*$ (здесь e_i^* — координатная проекция, равная f_i из стандартного базиса). Заметим, что $e_i^*(e_j) = \delta_{i,j}$.

$$\begin{pmatrix}e_1^* \\ \vdots \\ e_n^*\end{pmatrix} \begin{pmatrix}e_1 & \cdots & e_n\end{pmatrix} = E, \text{ где } E \text{ — единичная матрица}$$

Пусть $u_1, \dots, u_n$ — произвольный базис в R^n. Определим u_i^* по аналогии с u_i, как линейное отображение:

$$u_i^* : R^n \to R; \qquad u_i^* : u_h \mapsto \delta_{i,h} \cdot 1_R$$

и продолжим по линейности на всё пространство.

Теорема 4.14.2. Двойственный базис преобразуется контравариантно по отношению к исходному.

$$\begin{pmatrix} u_1^* \\ \vdots \\ u_n^* \end{pmatrix} = (e \rightsquigarrow u)^{-1} \begin{pmatrix} e_1^* \\ \vdots \\ e_n^* \end{pmatrix}$$

Умножая обе части равенства с e_i^* и e_i справа на $(e \rightsquigarrow u)$, получим

$$\begin{pmatrix} e_1^* \\ \vdots \\ e_n^* \end{pmatrix} \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} = (e \rightsquigarrow u)$$

Теперь заметим, что $\begin{pmatrix} u_1^* \\ \vdots \\ u_n^* \end{pmatrix} \cdot \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} = 1_R$, с помощью чего несложными преобразованиями получаем требуемое равенство.

Теорема 4.14.3. Координаты ковекторов в двойственном базисе преобразуются ковариантно по отношению к преобразованию исходного базиса.

Доказательство. $\eta = \begin{pmatrix} \eta_1 & \cdots & \eta_n \end{pmatrix} \begin{pmatrix} e_1^* \\ \vdots \\ e_n^* \end{pmatrix} = \begin{pmatrix} \eta_1 & \cdots & \eta_n \end{pmatrix} (e \rightsquigarrow u) \underbrace{(e \rightsquigarrow u)^{-1} \begin{pmatrix} e_1^* \\ \vdots \\ e_n^* \end{pmatrix}}_{\begin{pmatrix} u_1^* \\ \vdots \\ u_n^* \end{pmatrix}}$ □

Итог. Пусть в свободном модуле R^n нашлись два базиса $\{e_1, \dots, e_n\}$ и $\{u_1, \dots, u_n\}$. Матрица перехода между ними $(e \rightsquigarrow v)$:

$$\begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} (e \rightsquigarrow u) = \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix}$$

- Отсюда сразу видно, что базисные вектора преобразуются ковариантно самим себе (**??**).
- Координаты произвольного вектора преобразуются контравариантно преобразованиям координат базиса (**??**).
- При условии коммутативности кольца R, двойственный базис e_i^* и u_i^* преобразуется контравариантно исходному (**??**).
- Наконец, при условии коммутативности кольца R, координаты произвольного двойственного вектора при разложении по двойственному базису преобразуются ковариантно исходному базису (**??**)

Лекция XXX

21 декабря 2022 г.

4.14.2 Преобразование матрицы, линейные отображения.

Пусть $\{u_1, \cdots, u_m\}$ и $\{u'_1, \cdots, u'_m\}$ два базиса. А ещё $\{v_1, \cdots, v_n\}$ и $\{v'_1, \cdots, v'_n\}$ — два других базиса.

Пусть $\phi : R^m \to R^n$ — линейное отображение;

$$x = u_1x_1 + \cdots + u_mx_m \mapsto \phi(x) = v_1y_1 + \cdots + v_ny_n$$
$$x = u'_1x'_1 + \cdots + u'_mx'_m \mapsto \phi(x) = v'_1y'_1 + \cdots + v'_ny'_n$$

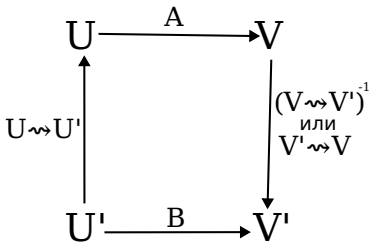
Введём две матрицы, переводящие столбец координат по базису u или u' в столбец координат по базису v или v' соответственно:

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \qquad B \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_m \end{pmatrix} = \begin{pmatrix} y'_1 \\ \vdots \\ y'_n \end{pmatrix}$$

Запишем

$$\begin{pmatrix} y'_1 \\ \vdots \\ y'_n \end{pmatrix} = (v \rightsquigarrow v')^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (v \rightsquigarrow v')^{-1} A \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = (v \rightsquigarrow v')^{-1} A (u \rightsquigarrow u') \begin{pmatrix} x'_1 \\ \vdots \\ x'_m \end{pmatrix}$$

Отсюда видно, что $B = (v \rightsquigarrow v')^{-1} A (u \rightsquigarrow u')$. Также это можно видеть из следующей диаграммы:



4.14.3 Двойственность

Рассмотрим векторное пространство $V = R^n$. Как определено ранее, $V^* = {}^nR = \mathrm{Hom}(V, R)$ — двойственный модуль.

Заметим, что $V \cong V^*$ (столбцы на строки меняем): $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}$. Данный изоморфизм наблюдается только благодаря коммутативности кольца: раньше мы домножали строку слева на матрицу справа; теперь мы домножаем транспонированную матрицу слева на столбец справа в двойственном модуле.

Так как умножение переворачивается, то двойственный левому модулю – правый, и наоборот. Но из-за коммутативности кольца можно утверждать наличие изоморфизма.

Рассмотрим $(V^*)^*$ — двойственный двойственному модуль.

Теорема 4.14.4. Между V и V^{**} имеется канонический изоморфизм, не зависящий от выбора базиса.

Доказательство. Определим отображение из V в V^{**} так: сопоставим вектору $u \in V$ функционал $\theta_u = u^{**} \in V^{**}$.

Этот функционал при применении справа к любому отображению $\phi \in V^*$, даёт значение отображения в точке u:

$$V^* \times V^{**} \to R; \qquad (\phi)u^{**} = \phi(u)$$

Теперь заметим, что данное отображение $u \mapsto u^{**}$:

- Действительно не зависит от выбора базиса: он просто не участвует в определении.
- Корректно: $u^{**} \in V^{**}$, то есть линейно относительно канонического спаривания с элементами из V^*. А именно, аддитивно

$$\forall \phi, \psi \in V^*, u^{**} \in V^{**} : \qquad (\phi + \psi)u^{**} = (\phi + \psi)(u) = \phi(u) + \psi(u) = (\phi)u^{**} + (\psi)u^{**}$$

  и однородно

$$\forall \phi \in V^*, u^{**} \in V^{**}, \lambda \in R : \qquad (\lambda\phi)u^{**} = \lambda\phi(u) = \lambda \cdot (\phi)u^{**}$$

- Само по себе — линейное отображение, то есть аддитивно

$$\forall \phi \in V^{**}, u, v \in V : \qquad (\phi)(u + v)^{**} = \phi(u + v) = \phi(u) + \phi(v) = (\phi)u^{**} + (\phi)v^{**}$$

  и согласовано с умножением на скаляр

$$\forall \phi \in V^{**}, u \in V, \lambda \in R : (\phi)(u\lambda)^{**} = \phi(u\lambda) = \phi(u)\lambda = (\phi)u^{**} \cdot \lambda$$

- Инъективно. Здесь мы докажем, что $\mathrm{Ker}(u \mapsto u^{**}) = \{0\}$:

$$u^{**} = 0 \Rightarrow \forall \phi \in V^* : (\phi)u^{**} = \phi(u) = 0 \Rightarrow u = 0$$

- В конечномерном случае это — изоморфизм, так как переводит произвольный базис $\{u_1, \ldots, u_n\}$ в базис дважды двойственного пространства $\{u_1^{**}, \ldots, u_n^{**}\}$. В самом деле, $\{u_1^{**}, \ldots, u_n^{**}\}$ — базис, так как $u_i^{**} = (u_i^*)^*$:

$$(u_j^*)u_i^{**} = u_j^*(u_i) = \delta_{i,j} \cdot 1_R$$

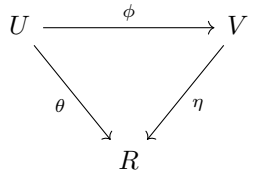
□

Интересный факт. В бесконечномерном случае отображение остаётся инъективным, но перестаёт быть сюръективным; если V — бесконечномерно, то $\dim(V^*) > \dim(V)$.

4.14.4 Перевод линейным отображением одного функционала в другой

В данном разделе R необязательно коммутативно, U, V — правые модули-R. Так как линейный функционал, как элемент U^* — по определению элемент $\mathrm{Hom}(U, R)$, то линейные отображения $U \to V$ являются линейными отображениями не только на элементах пространства V, но и на функционалах из V^*:

Всякий функционал $\eta \in V^*; \eta : V \to R$ переводится линейным отображением $\phi : U \to V$ в линейный функционал $\theta = \eta \circ \phi : U \to R$ согласно следующей диаграмме:



Данное отображение, сопоставляющее функционалу $\eta : V \to R$ функционал $\theta : U \to R$ называется называется *двойственным* к ϕ отображением:

$$\phi^* : V^* \to U^* \qquad \phi^* : \eta \mapsto (\eta)\phi^* = \eta \circ \phi$$

Свойства двойственного отображения

Не уверен, было ли это на лекции, но без этих фактов раздел выглядит совсем куцо.

- ϕ^* — линейное отображение. Проверим аддитивность, применив $(\eta+\theta)\phi^*$ к произвольному $x \in U$:

  $$((\eta+\theta)\phi^*)(x) = ((\eta+\theta)\circ\phi)(x) = (\eta+\theta)(\phi(x)) = \eta(\phi(x))+\theta(\phi(x)) = (\eta\circ\phi+\theta\circ\phi)(x) = ((\eta)\phi^*+(\theta)\phi^*)(x)$$

  Аналогично проверяется согласованность с умножением на скаляр $\lambda \in R$:

  $$((\lambda\eta)\phi^*)(x) = ((\lambda\eta)\circ\phi)(x) = \lambda\eta(\phi(x)) = \lambda(\eta\circ\phi)(x) = \lambda((\eta)\phi^*)(x)$$

- Пусть кольцо R коммутативно; пусть $\{e_1,\dots,e_n\}$ — базис U, $\{f_1,\dots,f_m\}$ — базис V. Как известно, ϕ определяется своими значениями на элементах базиса e; Рассмотрим $(x_{i,j})_{i=1..m,j=1..n}$ — матрицу ϕ. А именно, $x_{*,j} = [\phi(e_j)]_f$.

  Утверждается, что в таком случае матрица отображения ϕ^*, выраженная в двойственных базисах $\{f_1^*,\dots,f_m^*\}$ и $\{e_1^*,\dots,e_n^*\}$ равна x.

  Доказательство. Рассмотрим произвольный $u \in U$; ему соответствует $\phi(u) \in V$.

  Из определения матрицы x (U, V — **правые** модули) понятно, что

  $$[u]_e = x \cdot [\phi(u)]_f$$

  где $[u]_e$ и $[\phi(u)]_f$ — столбцы разложения соответствующих векторов по соответствующим базисам.

  Теперь рассмотрим **левые** модули U^*, V^*, и соответствующие двойственные базисы $\{e_1^*,\dots,e_n^*\}$ и $\{f_1^*,\dots,f_n^*\}$.

  Элементы двойственных модулей рассматриваем, как соответствующие им строки координат, канонические спаривания $U^* \times U \to R$ и $V^* \times V \to R$ стали умножением строки на столбец. Матрицу отображения ϕ^* назовём x^*, хотя скоро мы увидим, чему она равна на самом деле.

  Теперь для любого $u \in U, \eta \in V^*$:

  $$((\eta)\phi^*)(u) = \eta(\phi(u)) \qquad \Rightarrow \qquad ([\eta]_{f^*} \cdot x^*) \cdot [u]_e = [\eta]_{f^*} \cdot (x \cdot [u]_e)$$

  то есть матрица ϕ^* — это $x^* = x$, что следует просто-напросто из ассоциативности. □

- $(\phi+\psi)^* = \phi^* + \psi^*$.
- $(\lambda\phi)^* = \phi^*\lambda$.
- $(\phi\circ\psi)^* = \psi^*\circ\phi^*$.
- $\mathrm{id}_V^* = \mathrm{id}_{V^*}$.
- $\phi^{**} = \phi$.

Лекция XXXI

22 декабря 2022 г.

4.15 Случайные факты *не* из линейной алгебры

В данной лекции мы отвлечёмся от линейной алгебры, которой посвящён данный раздел, и докажем одну нетривиальную теорему.

4.15.1 Теорема Галуа

Лемма 4.15.1. *A_n порождается циклами длины 3.*

Доказательство. A_n — подгруппа чётных перестановок в S_n, то есть перестановок, порождённых чётным числом транспозиций. Отсюда очевидно, что всякий элемент в S_n порождён перестановками вида $(ij)(kl)$, то есть парой транспозиций.

Для доказательства леммы покажем, что всякая пара транспозиций является произведением 3-циклов. Если среди i, j, k, l 3 различных числа, то произведение $(ij)(kl)$ уже является 3-циклом.

Иначе $(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$.

С другой стороны, каждый 3-цикл сам по себе лежит в A_n. □

Лемма 4.15.2. *Любая перестановка порождается транспозициями:*

$$S_n = \langle \{(ij)\} \rangle$$

Доказательство. Разложим перестановку на произведение независимых циклов и породим каждый цикл следующим образом:

$$(i_1 i_2 \dots i_k) = (i_1 i_2) \dots (i_{k-2} i_{k-1})(i_{k-1} i_k)$$

□

Лемма 4.15.3. *Любая перестановка порождается* фундаментальными *транспозициями — транспозициями соседних элементов:*

$$S_n = \langle \{(ij) | i + 1 = j\} \rangle$$

Доказательство. Докажем, что каждая транспозиция порождается фундаментальными. Обозначим транспозицию i-го и j-го элементов $w_{i,j}$. Докажем по индукции, что $w_{j,k} \in \langle (i, i+1) \rangle$.

База: $|j - k| = 1$.

Индукционный переход: $|j-k| > 1$. Найдётся m строго между j, k. Заметим, что $w_{j,k} = w_{j,m} w_{m,k} w_{j,m}$, что завершает доказательство. □

Другой способ доказательства. Применим алгоритм сортировки пузырьком, который за $\mathcal{O}(n^2)$ фундаментальных транспозиций поменяет элементы из любого порядка в любой другой. □

Определение 4.15.1 (k-транзитивность)**.** Подгруппа $H \leqslant S_n$ является k-транзитивной, если

$$\forall (i_1, \dots, i_k), (j_1, \dots, j_k), \text{ таких, что все } i \text{ различны, все } j \text{ — тоже различны, } \exists \pi \in H : \begin{cases} \pi(i_1) = j_1 \\ \dots \\ \pi(i_k) = j_k \end{cases}$$

Так, S_n является n-транзитивной, так как допустим любой набор из n чисел внизу табличной записи.

Неформально говоря, k-транзитивность означает, что мы можем переставить любые k чисел в таком порядке, в каком хотим. Дальше уже могут начаться проблемы, не на все из оставшихся мест можно поставить все из оставшихся чисел.

Лемма 4.15.4. *A_n — $(n-2)$-транзитивна.*

Любая $\pi \in A_n$ имеет вид $\pi = \begin{pmatrix} i_1 & \cdots & i_{n-2} & i_{n-1} & i_n \\ j_1 & \cdots & j_{n-2} & * & * \end{pmatrix}$, где вместо «*» в каком-то [в таком, чтобы итоговая перестановка получилась чётной] порядке стоят j_{n-1} и j_n.

Теорема 4.15.1 (Галуа о простоте A_n)**.** A_n при $n \geqslant 5$ проста.

Доказательство. Пусть $H \trianglelefteq A_n$. $|A_n| \geqslant 60 \Rightarrow A_n \neq \{\mathrm{id}\}$.

Если $H \neq \{\mathrm{id}\}$, то $\exists \pi \in H : \pi \neq \mathrm{id}$.

«Потрясающая идея, но её не я придумал»: прокоммутируем с чем-то маленьким.

Заметим, что $A_n = \langle (abc) \rangle$. π не коммутирует сразу со всеми (abc), иначе $\pi \in \mathrm{Cent}(A_n)$, но $\mathrm{Cent}(A_n) = \{\mathrm{id}\}$ при $n \geqslant 4$ (в то время, как A_3 всё ещё абелева).

Таким образом, если $\pi \neq \mathrm{id}$, то $\exists (abc) : \pi(abc) \neq (abc)\pi$, то есть

$$\mathrm{id} \neq \sigma \coloneqq [\pi, (abc)] = \pi(abc)\pi^{-1}(abc)^{-1}$$

С одной стороны, $\sigma = \pi\left((abc)\pi^{-1}(abc)^{-1}\right) = \pi \circ {}^{(abc)}\left(\pi^{-1}\right) \in H$.

С другой стороны, $\sigma = \left(\pi(abc)\pi^{-1}\right)(abc)^{-1} = {}^{\pi}(abc) \circ (abc)^{-1}$, то есть произведение двух 3-циклов; назовём $\sigma = (ijh)(klm)$.

Сколько букв среди этих шести представляют собой различные значения? $3 \leqslant t \coloneqq |\{i, j, h, k, l, m\}| \leqslant 6$.

Проведём перебор в поисках 3-цикла в H:

- $t = 3$: σ — 3-цикл, $\sigma \in H$, 3-цикл нашёлся.
- $t = 4$:

  1° $\sigma = (ijh)(jhk) = (ij)(hk)$ — произведение двух транспозиций. Именно здесь появляется Vierergruppe как нормальная подгруппа в A_4. Разберёмся с этим случаем позже.

  2° $\sigma = (ijh)(jkh) = (ijk)(h) = (ijk)$ — 3-цикл нашёлся.
- $t = 5$: $\sigma = (ijh)(hkl) = (ihjkl)$ — 5-цикл (приведём к 3-циклу позже).
- $t = 6$: $\sigma = (ijh)(klm)$. Прокоммутируем:

  $$[\sigma, (hkl)] = (ijh)(klm)(hkl)(kml)(ijh)(hlk) = (ilkhm)(j) = (ilkhm)$$

  Опять же, получили 5-цикл.

Разбираемся с 5-циклами.

Прокоммутируем, мы же уже поняли, что получается что-то из H и полюбили коммутаторы, да? Ну, вот:

$$[(ijhkl), (ijh)] = (ijhkl)(ijh)(lkhji)(hji) = (ikj)(h)(l) = (ijk)$$

Разбираемся со случаем 1° при $t = 4$.

Что мы делаем? Правильно:

$$[(ij)(hk), (hkl)] = (ij)(hk)(hkl)(hk)(ij)(hlk) = (i)(j)(hkl) = (hkl)$$

Заметим, что здесь нам понадобилась буква l, которой там не было, то есть всего различных букв должно быть хотя бы 5. То есть необходимое условие состоит в том, что $n \geqslant 5$.

Интересно заметить, что это единственное место, которое не работает при $n = 4$. В самом деле, $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ — нормальная подгруппа (причём не только в A_4, но даже и в S_4).

Таким образом при $n \geqslant 5$ в любой нормальной нетривиальной ($\neq \{\mathrm{id}\}$) подгруппе существует 3-цикл.

В силу $(n-2)$-транзитивности (а $n-2 \geqslant 3$, пам-пам!) в H содержатся **все** 3-циклы $\Rightarrow H \geqslant A_n \Rightarrow H = A_n$: данный 3-цикл можно так сопрячь, чтобы получился другой 3-цикл, в силу $(n-2)$-транзитивности сопрягающая перестановка лежит в A_n. □

4.15.2 Колокола в Англии

В Англии всего 8 колоколов, причём они звонят очень хитрым образом.

Сначала они звонят в порядке $[1, 2, \ldots, 8]$, а потом служители меняют какую-то пару из них. После этого они звонят в новом порядке, и так далее.

В итоге все $8! = 40320$ перестановок обзваниваются по одному разу.

Может ли быть такое (и как)?

Доказательство. Нарисуем граф, неориентированное ребро проходит между двумя перестановками π и σ, такими, что $\pi = (ij)\sigma$ для некоторых i, j.

Докажем,что при $n \geq 3$ для любой пары перестановок π, σ разной чётности существует гамильтонов путь из одной в другую.

Заметим, что условие достаточно проверять только для одной из перестановок, равной id (домножение всех перестановок — вершин в графе — на фиксированную перестановку α сохраняет рёбра, *изоморфизм графа*, если позволите).

Будем действовать по индукции.

База: $n = 2$. В графе 2 перестановки, между ними есть ребро.

Переход: $n \geqslant 3$. Зафиксируем некий индекс i, такой, что $\pi_i \neq \sigma_i$. Перечислим в некотором порядке числа $1..n$ так, чтобы первым оказалось число π_i, а последним — число σ_i.

Будем по очереди перебирать перестановки в графе, составляя путь, так, чтобы сначала пройти по всем перестановкам $\beta : \beta_i = \pi_i$, потом — по всем перестановкам $\beta : \beta_i$ — второе число из списка, и так далее.

Так как $n!$ чётно, то действительно путь будет вести из перестановки одной чётности в перестановку другой чётности. Внутри частей пути $\{\beta_j\}_{j=1}^{n!}$ с фиксированным β_i путь строится по индукции, вне частей β_i меняется так, чтобы стать следующим числом в списке. □