МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ АЛГЕБРЫ. ЧАСТЬ 2

КАНУННИКОВ
АНДРЕЙ ЛЕОНИДОВИЧ и др.

МЕХМАТ МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

БЛАГОДАРИМ ЗА ПОДГОТОВКУ КОНСПЕКТА
СТУДЕНТКУ МЕХАНИКО-МАТЕМАТИЧЕСКОГО ФАКУЛЬТЕТА МГУ
ОНУФРИЕНКО МАРИЮ ВИКТОРОВНУ

Содержание

Лекция 1 **6**
Модули . . . 6
Подмодули . . . 7
Основная теорема о гомоморфизме . . . 7
Прямая сумма . . . 8
Циклические модули . . . 9
Аннулятор модуля . . . 9
Свободные модули . . . 10
Подмодуль циклического модуля . . . 11
Аналог китайской теоремы об остатках . . . 11

Лекция 2 **13**
Основные определения и утверждения . . . 13
Теорема о подмодуле в конечнопорождённом свободном модуле . . . 14
Теорема о согласованных базисах . . . 15
Нормальная форма Смита . . . 16
Примеры . . . 18

Лекция 3 **20**
Основные определения . . . 20
Теорема об изоморфизме . . . 21
Прямая сумма модулей . . . 22
Теорема о прямой сумме . . . 22
Определение подмодуля . . . 23
Лемма Шура для модулей . . . 23
Важный пример . . . 24
Теорема Машке . . . 24
Теорема о разложении в прямую сумму . . . 24

Лекция 4 **26**
Повторение предыдущих лекций . . . 26
Кольцо с противоположным умножением . . . 26
Кольцо эндоморфизмов. Теорема . . . 26
Кольцо эндоморфизмов. Теорема . . . 27
Теорема об изоморфизме кольца эндоморфизмов . . . 27
Теорема об изоморфизме K-алгебр . . . 29
Теорема о степенях неприводимых комплексных представлений . . . 30

Лекция 5 **32**
Нетеровы кольца . . . 32
Теорема о модуле над нетеровым кольцом . . . 32
Пример . . . 33
Теорема Гильберта о базисе . . . 33
Радикал кольца . . . 34

Лекция 6 **36**
Определение целого элемента . . . 36
Теорема 1 . . . 36
Теорема 2 . . . 36
Теорема 3 . . . 37
Алгебраическая зависимость . . . 37
Критерий алгебраической зависимостиь . . . 38
Утверждение о базисе трансцендентности . . . 38
Следствие о базисе трансцендентности . . . 39
Лемма о замене . . . 39
Теорема о степени трансцендентности алгебры A . . . 39

Лекция 7 **41**
Лемма Нетер о нормализации . . . 41
Теорема об алгебраическом расширении . . . 42
Теорема о гомоморфизме и нильпотентном элементе . . . 42
Множество решений . . . 43
Теорема Гильберта о нулях . . . 43

Лекция 8 **45**
Теорема Гильберта о нулях . . . 45
Аффинные алгебраические многообразия . . . 45
Алгебра многочленов на аффинном многообразии . . . 46
Построение аффинного алгебраического многообразия . . . 46
Морфизмы и изоморфизмы аффинных многообразий . . . 48
Теорема о взаимно однозначном соответствии аффинных многообразий и алгебр . . . 49
Топология Зарисского . . . 50

Лекция 9 **54**
Топология Зарисского на аффинном многообразии . . . 54
Гомоморфизм ограничения . . . 54
Топология Зарисского на одномерном пространстве . . . 55
Нетерово топологическое пространство . . . 55
Неприводимое топологическое пространство . . . 56
Критерий неприводимости многообразия . . . 58
Рациональные функции . . . 59
Размерность неприводимого многообразия . . . 60

Лекция 10 **62**
Определение свободной группы . . . 62
Утверждение об изоморфизме свободных групп . . . 62
Ранг свободной группы . . . 63
Проективные свойства свободной группы . . . 64
Приведенное слово . . . 65
Подгруппы свободных групп . . . 65

Теорема Нильсена-Шрайера 65
Два примера свободных групп 67

Лекция 11 **69**
Система порождающих соотношений 69
Пример про группу диэдра 69
Второй пример про группу диэдра 70
Эквивалетные копредставления 70
Литература 71
Проблемы Дена 71
Примеры 71

Лекция 1

Первая часть курса будет посвящена структурным вопросам теории колец, алгебр и модулей.

Модули

Пусть A — ассоциативное кольцо с 1 (можно рассматривать произвольные кольца, но в нашем случае ограничимся ассоциативными. Далее будем рассматривать в большей части лекций ассоциативные коммутативные кольца). *Левый модуль* над A — это абелева группа X с операциями умножения на элементы из A ($x \to ax$) и выполнены следующие условия:

1) $(a+b)x = ax + bx$
2) $a(x+y) = ax + ay$
3) $(ab)x = a(bx)$
4) $1x = x$

Пример 1. 1) Векторные пространства — модули над полями.

2) Абелевы группы — модули над $\mathbb{Z}_i$.

3) A — модуль над A.

4) $A^n = A \times \ldots \times A$ — свободный модуль над A (аналог арифметического векторного пространства).

5) Пусть K —поле, модуль над кольцом многочленов — ${}_{K[t]}V$. Это равносильно тому, что задан $\mathcal{A} : V \to X$ — линейный оператор:

$$tv = \mathcal{A}v, \quad f(t)v = f(\mathcal{A})v.$$

6) Аналогично можно говорить о представлениях данной группы как о модулях над групповой алгеброй. Пусть G — группа, и задано представление $\rho : G \to GL(v)$, где V — векторное пространство над K. Тогда можно задать естественную структуру модуля KG, ${}_{KG}V$:

$$KG = \{\sum_{g \in G} k_g g \mid k_g \in K\}.$$

$$gv := \rho(g)v, \quad (\sum_g k_g g)v = \sum_g k_g \rho(g)v.$$

Определение 1. Подмножество ${}_AX \supset S$ называется *системой порождающих*, если $\forall x \in X \ \exists n \in \mathbb{N}$ существуют $a_1, \ldots, a_n \in A$ и $s_1, \ldots, s_n \in S$:

$$x = \sum_{i=1}^{n} a_i s_i.$$

Модуль, который обладает конечной системой порождающих, называется *конечно порожденным*. Обозначение: $X = \langle S \rangle$. Модуль называется *циклическим*, если

$$X = \langle x \rangle \iff X = Ax.$$

Пример 2. Модуль ${}_AA$ — циклический: $A = A \cdot 1$.

Пример 3. Пусть I — идеал в A. Рассмотрим A/I. Можно ли здесь задать структуру A-модуля. Да:

$$a(b + I) = ab + I,$$
$$a(b + I) = ab + I,$$
$$b - b' \in I \Longrightarrow a(b - b') \in I.$$

Подмодули

Определение 2. *Подмодуль* $Y \leq X$ — подгруппа по сложению, замкнутая относительно элементов кольца: $(Y, +) \leq (X, +)$, $\forall a \in A\ \forall y \in Y$, $ay \in Y$.

Определение 3. Гомоморфизм модулей $f : X \to Y$ — отображение со свойствами

$$f(x_1 + x_2) = f(x_1) + f(x_2),$$
$$f(ax) = af(x).$$

Если есть какая-то алгебраическая структура — множество с заданными операциями, то полезно понимать, как разбивать на это множество на подмножества, то есть вводить отношение эквивалентности, согласованные со всеми операциями. Тогда на классах эквивалентности можно будет индуцировать ту же структуру.

Например, пусть $X_0 \subset X$ — подгруппа. Тогда можно рассмотреть фактор-группу X/X_0. Когда мы на ней можем естественным образом ввести операцию умножения на элементы кольца?

$$a(x + X_0) = ax + X_0.$$

Когда это будет корректно, то есть если $a(x' + X_0) = ax' + X_0$. Иными словами, условия согласования подгруппы с операцией умножения на элементы кольца таковы:

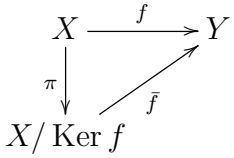
$$x - x' \in X_0 \Longrightarrow a(x - x') \in X_0 \quad \forall x, x' \in X_0,\ \forall a \in A.$$

Тогда X/X_0 — фактор-модуль.

Основная теорема о гомоморфизме

Пусть X_0 — подмодуль. Рассмотрим каноническую проекцию $\pi : X \to X/X_0$, $x \mapsto x + X_0$. Имеет место основная теорема о гомоморфизме.

Теорема 1 (Основная теорема о гомоморфизме)**.** *Если есть некоторый гомоморфизм $f : X \to Y$, тогда есть ядро* $\operatorname{Ker} f = f^{-1}(0) \leq X$ *и* $\operatorname{Im} f = f(X) \simeq X/\operatorname{Ker} f$ *и коммутативная диаграмма*



Прямая сумма

Естественная идея в структурной теории — сводить строение сложных объектов к строению простых. Удобно рассматривать прямые суммы.

Определение 4. Внешняя прямая сумма X и Y это множество формальных пар:

$$X \oplus Y = \{(x, y) \mid x \in X, y \in Y\}.$$

Внутренняя прямая сумма X и Y: $Z \geq X, Y$, Z — внутренняя прямая сумма $Z = X \oplus Y$, если $\forall z \in Z\ \exists! x \in X$ и $\exists! y \in Y$: $z = x + y \iff Z = X + Y$, $X \cap Y = 0$ (единственность разложения).

Эти две конструкции прямых сумм эквивалентны. Действительно, если есть внешняя прямая сумма, то в ней есть два подмодуля $X \times \{0\}$ и $Y \times \{0\}$, и есть взять их внутреннюю прямую сумму, то снова получим $X \oplus Y$. В обратную сторону: если есть внутренняя прямая сумма

$$X \oplus Y \to Z,$$

то отображение, которое из внешней прямой суммы действует в Z по правилу

$$(x, y) \mapsto x + y,$$

то это изоморфизм модулей.

Это можно обобщить на произвольное число слагаемых:

$$\bigoplus_{i=1}^{n} X_i,$$

где каждое слагаемое пересекается с суммой остальных по нулю ()

$$X_i \cap \sum_{j \neq i} X_j = 0.$$

Замечание 1. Три прямые на плоскости не образуют прямую сумму, хотя любые две из низ пересекаются по нулю.

В бесконечном случае под прямой суммой

$$\bigoplus_{i \in I} X_i$$

понимается множество функций (в общем случае, так как говорить о последовательностях можно только в не более, чем счетном случае)

$$f : I \to \cup X_i, \quad f(i) \in X_i,$$

у которых конечный носитель, то есть чтобы почти все $f(i)$ равны нулю.

Циклические модули

Ранее мы поняли, что если рассмотреть кольцо A как левый модуль над собой, то подмодуль над собой — это левый идеал:

$$ {}_AA \geq {}_AI \iff I \text{ — левый идеал в } A. $$

Тогда A/I — фактормодуль, $A/I = \langle 1 + I \rangle$,

$$ a + I = a(1 + I). $$

Давайте поймем, что никаких других циклических модулей нет. Пусть X — циклический модуль, $X = Ax$, $x \in X$. Тогда можно рассмотреть отображение

$$ f : {}_AA \to {}_AX, \quad a \mapsto ax $$

— сюръективный (по определению циклического модуля) гомоморфизм A–модулей:

$$ a + b \mapsto (a + b)x $$

— сумма переходит в сумму, и можно выносить скаляр:

$$ (ba)x = f(ba) = bf(a) = b(ax). $$

Этот гомоморфизм f, вообще говоря, не является инъективным. Если он будет инъективным, то наш модуль изоморфен кольцу A как модулю над собой. В общем же случае имеет место изоморфизм

$$ X \cong A/\operatorname{Ker} f. $$

Аннулятор модуля

Определение 5. *Аннулятором* $\operatorname{Ann} X$ *модуля* X — это все элементы из A, что $aX = 0$:

$$ \operatorname{Ann} X = \{a \in A \mid zX = 0\}. $$

Пример 4. Для $\mathbb{Z}_n$

$$ \operatorname{Ann} \mathbb{Z}_n = n\mathbb{Z}. $$

Очевидно, что аннулятор — это подгруппа по сложению. Кроме того, аннулятор — это левый идеал:

$$ aX = 0 \Longrightarrow baX = 0 $$

и правый идеал

$$ aX = 0 \Longrightarrow abX = 0, \quad bx \subseteq X. $$

Таким образом, аннулятор — это двусторонний идеал в X.

Замечание 2. Можно ли сказать, что $\operatorname{Ker} f = \{a \in A \mid ax = 0\}$ — аннулятор X. Ядро состоит из тех элементов кольца, которые аннулируют x, и не ясно, будут ли они аннулировать любой $x \in X$. Вообще говоря, импликация

$$ ax = 0 \Longrightarrow abx = 0 $$

не верна, но если кольцо коммутативно, то верна. И только тогда (в случае коммутативного кольца) мы можем сказать, что $\operatorname{Ker} f = \operatorname{Ann} X$.

Свободные модули

Определение 6. Система элементов $e_1, \dots, e_n \in X$ называется *базисом* модуля X, если $\forall x \in X\ \exists! a_1, \dots a_n \in A$:

$$x = \sum_{i=1}^{n} a_i e_i$$

$\iff e_1, \dots, e_n$ — линейно независимая над A система порождающих.

Пример 5. Модуль $\mathbb{Z}_n$ не обладает базисом.

Если модуль свободный, то он изоморфен «арифметическому модулю». Можно рассмотреть отображение

$$f : A^n \to X,$$

где X свободный модуль с базисом $e_1, \dots, e_n$:

$$(a_1, \dots a_n) \mapsto \sum_{i=1}^{n} a_i x_i.$$

Отображение f является инъективным и сюръективным гомоморфизмом , то есть это изоморфизм

$$A^n \cong X.$$

Замечание 3. Можно было бы ввести понятие размерности и сказать, что $n = \operatorname{rk} X$. Однако это не всегда так.

Если $A = K$ — поле или $A = \mathbb{Z}$, следовательно,

$$A^m \cong A^n$$

лишь при $m = n$.

Задача 1. *Показать, что в общем случае это неверно.*

Пример 6. Если A — целостное кольцо (его можно вложить в поле частных $Q(A)$), то свойство не выполнено. Не может так быть, что $A^m \cong A^n$ при $m > n$.

Действительно, рассмотрим элементы стандартного базиса $e_1, \dots, e_m$. Отобразим их в A^n. Получим m столбцов с высотой n и они по предположению линейно независимы. Такого быть не может (уже даже над полем) по основной лемме о линейной зависимости.

$$\underbrace{n \left\{ \begin{pmatrix} \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \right.}_{m}$$

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Подмодуль циклического модуля

Будет ли подмодуль циклического модуля циклическим? В случае подгрупп доказательство основано на делении с остатком.

Пусть $X = Ax$ — циклический модуль, $Y \leq X$. Верно ли, что существует $y \in Y$: $Y = Ay$.

Рассмотрим сначала случай, когда X — свободный модуль. Из сказанного выше $X \cong A$ как левый модуль над собой. Каким свойством должно обладать кольцо A, чтобы мы смогли такие же провести рассуждения, как в случае группы $\mathbb{Z}$ целых чисел.

Пусть B — левый идеал в A: ${}_AB \leq {}_AA$; порождается ли он одним элементом? В случае евклидова кольца ответ положительный. Кроме того, если A — кольцо главных идеалов, то всякий подмодуль в A является главным идеалом.

Пример 7. Рассмотрим пример факториального кольца, который не является кольцом главных идеалов: кольцо многочленов $\mathbb{R}[x, y]$. В нем есть идеал (x, y), порожденный x и y, который не является главным:

$$(x, y) \neq \mathbb{R}[x, y] \cdot d, \quad \forall d \in (x, y).$$

Иначе общий делитель x и y выражался бы линейной комбинацией

$$d = fx + gy,$$

что не так, так как при подстановке вместо x и y нулей, получаем противоречие.

Аналог китайской теоремы об остатках

Пусть A — целостное кольцо, элементы $a, b \in A$ взаимно просты: $(a, b) = 1$. Рассмотрим гомоморфизм колец

$$f : A \longrightarrow A/(a) \oplus A/(b),$$

$$f(x) = (x + (a), x + (b)).$$

Фактически мы хотим доказать аналог утверждения

$$\mathbb{Z}_{mn} \cong Z_m \oplus Z_n$$

при $(m, n) = 1$.

Отображение f является гомоморфизмом колец, так как это пара канонических гомоморфизмов. Проверим инъективность. Нужно доказать

$$\operatorname{Ker} f \ni X \Longleftrightarrow f(x) = 0 \Longleftrightarrow x \vdots a, b \Longleftarrow x \vdots ab.$$

Если кольцо факториально, то это, очевидно, верно. В общем случае — задача.

Проверим сюръективность. Если выполнено соотношение Безу, то есть существуют $u, v \in A$:

$$au + bv = 1,$$

то тогда любой элемент имеет прообраз

$$au \mapsto (\bar{0} = (a), \bar{1} = 1 + (b)),$$

$$bv \mapsto (\bar{1} = 1 + (a), \bar{0} = (b)),$$

то есть f сюръективно. Это верно в кольцах главных идеалов.

Мы доказали теорему.

Теорема 2. *Если A — кольцо главных идеалов, то*

$$A/(a, b) \cong A/(a) + A/(b).$$

Задача 2. *Верна ли теорема в случае факториальных колец?*

Лекция 2

Основные определения и утверждения

Пусть ${}_AX$ — конечно порожденный модуль над кольцом главных идеалов A. Примеры: $\mathbb{Z}$, $K[t]$, где K — поле.

Введем основные системы порождающих:

$$X = \langle x_1, \ldots, x_n \rangle = Ax_1 + \ldots + Ax_n.$$

Сумма, очевидно, не обязательно прямая. Если для каждого x существует единственное представление

$$x = \sum_{i=1}^{n} a_i x_i,$$

то система называется базисом, и имеет место изоморфизм

$$X \cong A^n.$$

В случае абелевых групп (кольца $\mathbb{Z}$) число n определено однозначно. Есть обобщение на произвольные целостные кольца:

$${}_AA^n \cong {}_AA^m \iff m = n,$$

если вообще A — простое кольцо.

Если $m \neq n$, то это равносильно существованию двух матриц $C_{m\times n}$ и $D_{n\times m}$ над кольцом A, что

$$CD = E_m,$$

$$DC = E_n.$$

Над полем таких матриц не существует в силу леммы о линейной зависимости.

Если модуль свободный, то он изоморфен «арифметическому модулю». Можно рассмотреть отображение

$$f : A^n \to X,$$

где X свободный модуль с базисом $e_1, \ldots, e_n$:

$$(a_1, \ldots a_n) \mapsto \sum_{i=1}^{n} a_i x_i.$$

Отображение f является инъективным и сюръективным гомоморфизмом,

$$\operatorname{Ker} f = N,$$

то есть это изоморфизм

$$X \cong A^n/N.$$

Теорема о подмодуле

Теорема 3. *Если A — КГИ, ${}_AY \leq {}_AX$ — конечно порожденный свободный модуль, тогда ${}_AY$ — конечно порожденный модуль и* $\operatorname{rk} Y \leq \operatorname{rk} X$.

Доказательство. Будем считать, что $X = A^n$. Докажем индукцией по n. Пусть $n = 1$. Это случай модуля над собой ${}_AA$. Все подмодули — это левые идеалы, которые в случае коммутативного кольца являются идеалами. Идеалы в нашем случае все главные $\Longrightarrow Y = (a) = aA$.

Шаг от $n-1$ к n. Итак, у нас есть подмодуль

$$Y \leq A^n = A^{n-1} \times A = \{(a_1, \ldots, a_{n-1}, 0) \mid a_i \in A\}.$$

Рассмотрим пересечение

$$Y \cap A^{n-1} = \langle y_1, \ldots, y_{m-1} \rangle,$$

где (y_i) образуют базис. Достроим этот базис до базиса Y. Возьмем все последние координаты элементов из Y:

$$B = \{a \in A \mid \exists y \in Y : y = (\ldots, b)\} \leq {}_AA.$$

Следовательно, B — главный идеал, то есть $B = (b)$. Обозначим $y_m = (\ldots, b) \in Y$. Докажем, что $y_1, \ldots, y_m$ — базис в Y. Надо доказать, что эти элементы линейно независимы над A и что это система порождающих.

Если $b = 0$, то доказывать нечего.

1) Рассмотрим линейную комбинацию $a_1y_1 + \ldots + a_{m-1}y_{m-1} + a_ny_m = 0$. Посмотрим на последнюю координату у всей левой части. Так как у первых $m-1$ слагаемых по определению последняя координата равна нулю, то получаем равенство $a_mb = 0$. Тогда $a_m = 0$. Тогда пр подстановке получим, что все a_i равны нулю, так как y_i с 1 по $m-1$ образуют базис в модуле $Y \cap A^{n-1}$. Таким образом, доказали линейную независимость y_i.

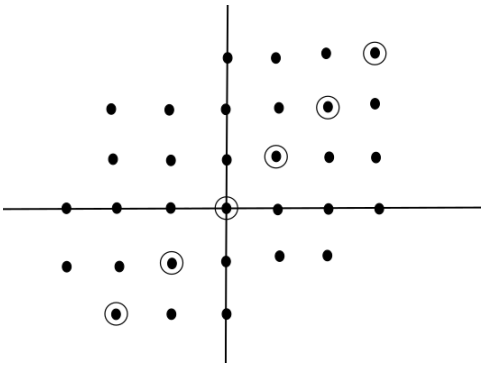
2) Рассмотрим произвольный элемент

$$Y \ni y = (\ldots bc) = cy_m + (y - cy_m),$$

где $(y - cy_m) \in Y \cap A^{n-1}$. Из этой принадлежности следует, что

$$y - cy_m = \sum_{i=1}^{m-1} b_iy_i.$$

Таким образом, $y_1, \ldots, y_m$ — базис. □



Теорема о согласованных базисах

Рассмотрим A^n со стандартным базисом

$$e_1 = (1, 0, \ldots, 0), \quad e_n = (0, 0, \ldots, 1).$$

Верно ли, что во всяком подмодуле $Y \leq A^n$ можно найти базис $u_1 e_1, \ldots, u_m e_m$, $u_i \in A$.

Пример 8. Пусть $A^n = \mathbb{Z}^2$. Можно взять подгруппу, у элементов которой координаты равны. Она, очевидно, не имеет согласованного базиса.

Теорема 4. *Существует такой базис $e'_1, \ldots, e'_n$ в A^n и существует такой базис $f'_1, \ldots, f'_n$ в Y, что существуют $u_1, \ldots, u_m \in A$, $u_1 \mid u_2 \mid \ldots \mid u_m$ (инвариантные множители): $\forall i = 1, \ldots, m$*

$$f'_i = u_i e'_i.$$

Доказательство. Рассмотрим некоторый базис $f_1, \ldots, f_m$ в Y и выразим его через базис $e_1, \ldots, e_n$ в X:

$$(f_1, \ldots, f_m) = (e_1, \ldots, e_n) C_{n \times m}, \quad C \in M_{n \times m}(A).$$

Мы хотим получить

$$(f'_1, \ldots, f'_m) = (e'_1, \ldots, e'_n) C',$$

$$C = \begin{pmatrix} u_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & u_m \\ 0 & \cdots & 0 \end{pmatrix}.$$

Перейдем к штрихованным базисам

$$\bar{f} = \bar{f}' U, \quad \bar{e} = \bar{e}' V,$$

где U и V — обратимые матрицы над $A \iff \det U, \det V \in A^*$.

Найдем обратимые преобразования:

$$\bar{f}' U = \bar{e}' V C,$$

$$\bar{f}' = \bar{e}' V C U^{-1} = \bar{e}' C',$$

$$C' = V C U^{-1}.$$

□

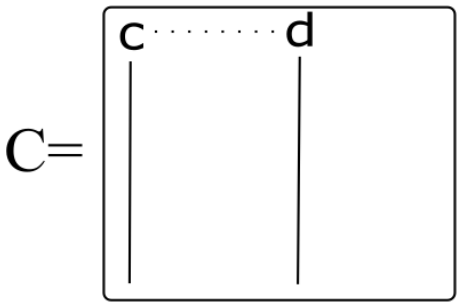


Рис. 1. Матрица для доказательства теоремы о нормальной форме Смита

Нормальная форма Смита

Теорема 5 (Нормальная форма Смита)**.** *Пусть $C \in M_{m\times n}(A)$, A — евклидово $\Longrightarrow$ целочисленными элементарными преобразованиями строк и столбцов C приводится к диагональному вид*

$$\begin{pmatrix} u_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & 0 \\ 0 & \cdots & u_r & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix},$$

где $u_1 \mid \ldots \mid u_r$ и $r \leq \min(m, n)$.

Доказательство. Проведем сначала рассуждения для евклидова кольца (оно повторят рассуждение для кольца целых чисел). Если $C = 0$, то доказывать нечего.

Пусть $C \neq 0$. Индукцией по норме мы уменьшаем элемент c_{11}. Посмотрим на первую строку: если какой-то элемент не делится на c_{11}, то делим с остатком

$$d = cq + r, \quad N(r) < N(d).$$

Тогда из столбца, где стоит d, отнимаем первый столбец с коэффициентом q. Либо $r = 0$, либо переставляем два рассматриваемых столбца. Такие преобразования называются «целочисленные элементарные преобразования» Таким образом, мы можем добиться того, что все элементы первой строки и первого столбца будут делиться на c_{11}. Пусть теперь это выполнено, но какой-то элемент в матрице не делится на c_{11} — обозначим его через t. На первом месте в строке, в которой находится t, есть элемент p, который делится на c_{11}: $p = cq$. Вычитаем первый столбец, получаем $t - qc$ и $c \nmid t - qc$, так как $c \nmid t$. Далее к первой строке прибавляем i-ю строку и получим $d + t - qc$, который не делится на c. Таким образом, свели задачу к предыдущей, и так как элементов в матрице конечное число, и норма всякий раз уменьшается, то в конечном итоге все элементы матрицы будут делиться на верхний левый угловой элемент. После этого мы обнуляем все элементы первой строки и первого столбца с верхним левым угловым элементом c и получим минор C_1,

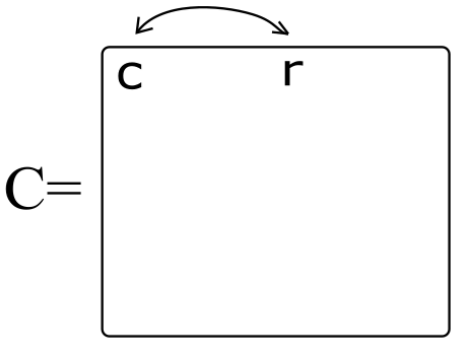


Рис. 2. Матрица для доказательства теоремы о нормальной форме Смита

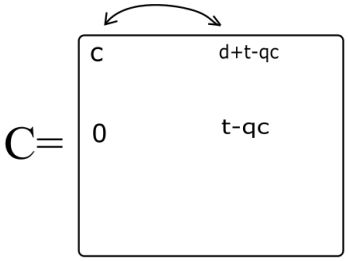


Рис. 3. Матрица для доказательства теоремы о нормальной форме Смита

все элементы которого делятся на c. С этой матрицей C_1 поступаем аналогичным образом. И получаем диагональный вид.

Теперь можно доказать, что есть инвариантная характеризация

$$u_i = \frac{d_i}{d_{i-1}},$$

где d_i — НОД миноров i-го порядка матрицы C, и $d_0 = 1$, $0/0 = 1$. □

Задача 3. *Доказать, что есть инвариантная характеризация*

$$u_i = \frac{d_i}{d_{i-1}},$$

где d_i — НОД миноров i-го порядка матрицы C, и $d_0 = 1$, $0/0 = 1$.

Итак, у нас есть согласованный базис, и теперь можно характеризовать по прямым сомножителям. Мы поняли, что

$$X = Ae'_1 \oplus \ldots \oplus Ae'_n / Af'_1 \oplus \ldots \oplus Af'_n \cong A/(u_1) \oplus \ldots \oplus A/(u_m) \oplus A^{n-m}$$

— общий вид циклического модуля, где $f'_i = u_i e'_i$. Теперь можно рассмотреть разложение

$$u = p_1^{k_1} \ldots p_s^{k_s}.$$

Тогда

$$A/(u) \cong A/(p_1^{k_1}) \oplus \ldots \oplus A/(p_s^{k_s}).$$

Определение 7. Определим *квазиэлементарные преобразования*

$$(x, y) \longrightarrow (ax + by, cx + dy),$$

где матрица

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{A})$$

обратима, то есть $ad - bc \in A^*$.

Ясно, что всякую пару элементов кольца можно привести к виду $(d, 0)$, где $d =$ НОД(x, y). Находим такие коэффициенты a, b, что

$$ax + by = d,$$

и тогда рассматриваем матрицу

$$\begin{pmatrix} a & b \\ -y/d & x/d \end{pmatrix}.$$

Примеры

$$\mathbb{Z}^{n-m} \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_m}$$

$$\mathbb{Z}^r \oplus \bigoplus_{p_j} \mathbb{Z}_{p_i^{k_i j}}$$

$$X = \langle x \rangle \cong A/(A_m X) = A/(p^k).$$

$$A^r \cong A^s$$

$$A^r \oplus A/(p_1^{k_{11}}) \oplus A/(p_1^{k_{12}}) \oplus \ldots \oplus A/(p_1^{k_{1n}}) \oplus A/(p_2^{k_{21}}) \oplus \ldots \oplus A/(p_2^{k_{2n}}) \oplus \cong A^{r'} \oplus \ldots$$

$\Longrightarrow r = r'$.

Пример 9. ${}_K V$, $\mathcal{A} : V \to V$, $\mathcal{A}t = tv$, $(t - \lambda)^k$.

$$\mathbb{C}[t]/(t^3) = \mathbb{C} \oplus \mathbb{C}\bar{t} \oplus \mathbb{C}\bar{t}^2$$

$$\bar{t}^2, \bar{t}, \bar{1} \to \bar{t}^r \to \bar{t}^2 \to \bar{0}.$$

Пусть K —алгебраически замкнутое поле, $\lambda \in K$. Пример модуля: $K[t]/(t-\lambda)^k$. В базисе $(t-\lambda)^{k-1} \ldots (t-\lambda)$ оператор умножается на t и задается жордановой клеткой

$$t(t - \lambda)^{k-2} = \lambda(t - \lambda)^{k-2} + (t - \lambda)^{k-1}$$

$$\begin{pmatrix} \lambda & 1 & \cdots & 0 \\ \vdots & \lambda & \ddots & \vdots \\ \vdots & & \ddots & 1 \\ 0 & \cdots & & \lambda \end{pmatrix}$$

Задача 4. *Пусть X — конечно порожденный модуль над КГИ.*

1) *Всякую ли линейно зависимую над A систему в X можно дополнить до базиса в X?*

2) *Из любой ли системы, порожденной в X, можно выбрать базис?*

3) *Пусть $\operatorname{rk} X = n$. Если $x_1, \ldots, x_n$ — линейно независимая система, то верно ли, что $x_1, \ldots, x_n$ — базис?*

4) *Пусть $\operatorname{rk} X = n$. Если $x_1, \ldots, x_n$ — система порождающих из n элементов, то верно ли, что $x_1, \ldots, x_n$ — базис?*

Лекция 3

Основные определения

Пусть R — ассоциативное кольцо с единицей.

Определение 8. Множество M называется R–модулем, если на нем введены две операции: сложения $+ : M \times M \to M$ и умножения на элемент кольца $\cdot : R \times M \to M$ такие, что выполнены аксиомы:

1) $(M, +)$ — абелева группа;

2) $(a + b)m = am + bm$;

3) $a(m_1 + m_2) = am_1 + am_2$;

4) $(ab)m = a(bm)$;

5) $1 \cdot m = m$.

Замечание 4. Если R — поле, то мы получаем определение векторного пространства.

Если $S \subseteq R$ — подкольцо, то любой R–модуль является S–модулем.

Пример 10. Тривиальный пример: 0 является модулем (нулевой модуль).

Пример 11. Любое кольцо R можно рассмотреть как R–модуль.

Пример 12. Если $S \subseteq R$ — подкольцо, то R можно рассматривать как S–модуль.

Пример 13. Если $I \subseteq R$ — левый идеал, то I является R–модулем.

Пример 14. Любая абелева группа является $\mathbb{Z}$–модулем.

Пример 15. Пусть V — векторное пространство над полем K, и пусть $\varphi : V \to V$ — линейный оператор. Тогда V можно наделить структурой $K[x]$–модуля, задав умножение по формуле

$$f(x) \cdot v = f(\varphi)(v).$$

Например,

$$a_n x^n + \ldots + a_0 = f(x),$$

тогда

$$f(\varphi) = a_n \varphi^n + \ldots + a_1 \varphi + a_0 \cdot \mathrm{id}\,.$$

Пример 16. Пусть K — поле. Множество R называется *K–алгеброй*, если на R заданы три операции: сложения, умножения и умножения на элемент поля K такие, что

1) R с операциями сложения и умножения — кольцо;

2) R с операциями сложения и умножения на число — векторное пространство;

3) $c(xy) = (cx)y = x(cy)$, $c \in K$, $x, y \in R$.

Замечание 5. Пусть R — это K–алгебра с единицей, тогда K вкладывается в R как подкольцо $\langle 1 \rangle$. Мы будем рассматривать только ассоциативные алгебры с единицей, если не оговорено противное.

Замечание 6. Если M — это R–модуль, а R — это K-алгебра, то M является K-векторным пространством.

Определение 9. Пусть R — кольцо, M и N — два R–модуля. Отображение $f : M \longrightarrow N$ называется *R–линейным*, если

1) $f(m_1 + m_2) = f(m_1) + f(m_2)$ для любых $m_1, m_2 \in M$;

2) $f(am) = af(m)$ для любых $a \in R$, $m \in M$.

Множество R–линейных отображений из M в N мы будем обозначать $\mathrm{Hom}_R(M, N)$. На множестве $\mathrm{Hom}_R(M, N)$ можно ввести операцию сложения по формуле

$$(f + g)(m) = f(m) + g(m).$$

Легко видеть, что $\mathrm{Hom}_R(M, N)$ с этой операцией является абелевой группой.

Введем операцию умножения на элемент R на множестве $\mathrm{Hom}_R(M, N)$ по формуле

$$(a \cdot f)(m) = a(f(m)) = f(am).$$

Однако в общем случае эта операция не делает R–модулем множество $\mathrm{Hom}_R(M, N)$. Дело в том, что

$$((ab) \cdot f)(m) = f(abm), \text{ но } (a \cdot (b \cdot f))(m) = b \cdot f(am) = f(bam).$$

Однако видно, что для коммутативного кольца $\mathrm{Hom}_R(M, N)$ является R–модулем.

Следствием из предыдущего является утверждение, что если R — это K–алгебра, то $\mathrm{Hom}_R(M, N)$ является K–векторным пространством (так как K коммутативно).

Теорема об изоморфизме

Теорема 6. *Пусть R — ассоциативное кольцо с единицей и пусть M — R–модуль. Тогда имеет место изоморфизм абелевых групп*

$$\mathrm{Hom}_R(M, N) \simeq M.$$

Более того, если R — это K–алгебра, то этот изоморфизм является изоморфизмом векторных пространств над K.

Доказательство. Определим отображение $\Phi : \mathrm{Hom}_R(M, N) \to M$ по формуле

$$\Phi(f) = f(1).$$

Легко видеть, что Φ — гомоморфизм абелевых групп, так как

$$\Phi(f_1 + f_2) = (f_1 + f_2)(1) = f_1(1) + f_2(1) = \Phi(f_1) + \Phi(f_2).$$

Также, поскольку для $c \in K$ выполнено $\Phi(cf) = cf(1) = c\Phi(f)$.

Осталось доказать биективность Φ. Докажем сперва инъективность. Пусть $\Phi(f) = \Phi(g)$. Тогда $f(1) = g(1)$. Но тогда

$$f(r) = f(r \cdot 1) = rf(1) = rg(1) = g(r \cdot 1) = g(r)$$

для всех $r \in R$. То есть $f = g$.

Теперь докажем сюръективность Φ. Возьмем $m \in M$ и определим $f_m : R \to M$ по формуле $f_m(r) = rm$. Отображение f_m задает R–линейное отображение из R в M такое, что $f_m(1) = m$. □

Прямая сумма модулей

Определение 10. Пусть M и N — R–модули. Прямой суммой $M \oplus N$ этих модулей называется прямая сумма абелевых групп M и N с операцией умножения на элемент r, определенной по правилу

$$r \cdot (m, n) = (rm, rn).$$

Можно проверить, что получится R–модуль.

Аналогично определяется прямая сумма большего количества слагаемых. Пусть $M = M_1 \oplus \ldots \oplus M_k$. Естественные проекции $\pi_i : M \to M_i$, $\pi_i(m_1, \ldots, m_k) = m_i$ являются R–линейными отображениями.

Теорема о прямой сумме

Теорема 7. *Пусть M и N — R–модули. И пусть модуль M раскладывается в прямую сумму модулей $M_1 \oplus \ldots \oplus M_k$. Тогда существует изоморфизм абелевых групп*

$$\mathrm{Hom}_R(M, N) \simeq \mathrm{Hom}_R(M_1, N) \oplus \ldots \oplus \mathrm{Hom}_R(M_k, N).$$

Более того, в случае, когда R является K–алгеброй, это изоморфизм векторных пространств над K.

Доказательство. Рассмотрим следующее отображение

$$\Psi : \mathrm{Hom}_R(M_1, N) \oplus \ldots \oplus \mathrm{Hom}_R(M_k, N) \longrightarrow \mathrm{Hom}_R(M_1 \oplus \ldots \oplus M_k, N),$$

$$\Psi(f_1, \ldots, f_k)(m_1, \ldots, m_k) = f_1(m_1) + \ldots + f_k(m_k).$$

Легко видеть, что Ψ — гомоморфизм абелевых групп и, если R является K–алгеброй, это Ψ — K–линейное отображение.

Если $\Psi(f_1, \ldots, f_k) = \Psi(g_1, \ldots, g_k)$, применим его к $(0, \ldots, 0, m_i, 0, \ldots, 0)$. Получим $f_i(m_i) = g_i(m_i)$. Следовательно, Ψ — инъекция.

Пусть теперь задано R–линейное отображение

$$f : \bigoplus_{i=1}^{k} M_i \longrightarrow N.$$

Определим $f_i : M_i \to N_i$ по формуле

$$f_i(m_i) = f(0, \dots, 0, m_i, 0, \dots, 0).$$

Тогда

$$\Psi(f_1, \dots, f_k)(m_1, \dots, m_k) = \sum f_i(m_i) = \sum f(0, \dots, 0, m_i, 0, \dots, 0) = \\ = f(\sum(0, \dots, 0, m_i, 0, \dots, 0))f(m_1, \dots, m_k).$$

Отсюда следует, что Ψ сюръективно. □

Определение подмодуля

Определение 11. Подмножество N модуля M над кольцом R называется подмодулем, если оно является модулем с теми же операциями.

Заметим, что если R — это K–алгебра, то подмодуль в R–модуле является его подпространством над K.

Определение 12. Модуль M называется простым, если он не имеет подмодулей, кроме $\{0\}$ и M.

Если задано R–линейное отображение R–модулей $\varphi : M \to N$, то $\operatorname{Ker}\varphi$ и $Im\varphi$ являются подмодулями. Сюръективность φ равносильна $Im\varphi = N$. Стандартная лемма для абелевых групп утверждает, что инъективность φ равносильна $\operatorname{Ker}\varphi = \{0\}$.

Лемма Шура для модулей

Лемма 1 (Шур)**.** *Пусть M и N — два простых R–модуля. Тогда любое R–линейное отображение $\varphi : M \to N$ — это либо изоморфизм, либо нулевое отображение. Если же $M = N$ и R является $\mathbb{C}$–алгеброй, то $\varphi = \lambda \operatorname{id}$ для некоторого $\lambda \in \mathbb{C}$.*

Доказательство. Ядро отображения φ — это подмодуль в M. Значит, либо $\operatorname{Ker}\varphi = M$ и тогда φ — нулевое отображение, либо $\operatorname{Ker}\varphi = \{0\}$, что означает, что φ — инъекция. Образ φ — подмодуль в N. Так как N простой, либо $Im\varphi = \{0\}$ и тогда φ — нулевое отображение, либо $Im\varphi = N$, то есть φ — сюръекция. Итак, мы доказали, что если $\varphi \neq 0$, то это биекция, и следовательно, изоморфизм модулей.

Пусть теперь R является $\mathbb{C}$–алгеброй. Тогда $M = N$ — это комплексное векторное пространство и φ — линейный оператор на нем. Тогда у φ существует собственное значение $\lambda \in \mathbb{C}$. Оператор $\varphi - \lambda \operatorname{id}$ вырожденный, следовательно это не изморфизм векторных пространств, а следовательно, не изморфизм модулей.

С другой стороны,

$$(\varphi - \lambda \operatorname{id})(rm) = \varphi(rm) - rm = r\varphi(m) - rm = r(\varphi - \lambda \operatorname{id})(m).$$

Это показывает, что $\varphi - \lambda \operatorname{id}$ — это R–линейное отображение. Что означает, что $\varphi - \lambda \operatorname{id} = 0$, то есть $\varphi = \lambda \operatorname{id}$. □

Важный пример

Пример 17. Пусть K — поле, G — группа. Рассмотрим групповую алгебру $R = KG$ группы G над полем K. Это K–векторное пространство с базисом $\{e_g \mid g \in G\}$, в котором определено умножение базисных элементов по формуле $e_g \cdot e_h = e_{gh}$. Произведение не базисных элементов определяется по дистрибутивности, то есть

$$\Big(\sum_g \lambda_g e_g\Big) \cdot \Big(\sum_h \mu_h e_h\Big) = \sum_{g,h} \lambda_g m u_h e_{gh}.$$

Легко видеть, что KG — это ассоциативная K–алгебра с единицей e_e.

Любое линейное представление ρ группы G в пространстве V над полем K задает структуру KG–модуля на V. В самом деле, можно определить

$$\Big(\sum_g \lambda_g e_g\Big) \cdot v = \sum_g \lambda_g \rho(g)(v).$$

Напротив, если задан KG–модуль M, то M является K–векторным пространством и можно определить соответствующее линейное представление $\rho : G \to GL(M_K)$ по формуле $\rho(g)(m) = e_g m$.

Рутинные проверки убеждают нас в том, что данные отображения корректны и взаимно обратны. Таким образом, у нас есть соответствие между K–представлениями G и KG–модулями.

Более того, инвариантные подпространства в V соответствуют подмодулям в KG–модуле V. Таким образом, неприводимые представления соответствуют простым модулям.

Прямая сумма представлений соответствует прямой сумме модулей.

Теорема Машке

Теорема 8 (Машке)**.** *Пусть G — конечная группа и K — поле, такое что* $\operatorname{char} K \nmid |G|$*. Тогда любой KG–модуль, являющийся конечномерным векторным пространством, есть прямая сумма простых.*

Применим эту теорему к KG–модулю KG. Получим разложение

$$KG = (V_1^1 \oplus \ldots \oplus V_{n_1}^1) \oplus \ldots \oplus (V_1^r \oplus \ldots \oplus V_{n_r}^r),$$

где $V_a^i \simeq V_b^j \iff i = j$.

Теорема о разложении в прямую сумму

Теорема 9. *1) В условиях теоремы Машке любой KG–модуль изоморфен некоторому слагаемому V_a^i.*

2) Пусть $K = \mathbb{C}$ и V — простой KG–модуль. Тогда в любом разложении $\mathbb{C}G$ в прямую сумму простых модулей модули, изоморфные V встречаются $\dim_{\mathbb{C}} V$ *раз.*

Доказательство. 1) Рассмотрим простой KG–модуль V. По доказанной ранее теореме имеем изоморфизм некоторых полей над K:

$$V \simeq \mathrm{Hom}_{KG}(KG, V).$$

С другой стороны, по второй доказанной теореме,

$$\mathrm{Hom}_{KG}(KG, V) \simeq \mathrm{Hom}_{KG}(\oplus V_a^i, V) \simeq \oplus\, \mathrm{Hom}_{KG}(V_a^i, V).$$

Таким образом,

$$V \simeq \oplus\, \mathrm{Hom}_{KG}(V_a^i, V).$$

Это значит, что не все слагаемые нулевые. А следовательно, существует V_a^i, изоморфный V (иначе по лемме Шура $\mathrm{Hom}_{KG}(V_a^i, V) = \{0\}$.

2)

$$\dim_{\mathbb{C}} V = \sum_{j,b} \dim_{\mathbb{C}} \mathrm{Hom}_{KG}(V_b^j, V) = \#\{(j,b) \mid V_b^j \simeq V\} = n_i.$$

Предпоследнее равенство основано на том, что если два простых модуля V и V_b^j не изоморфны, то $\mathrm{Hom}_{KG}(V_b^j, V) = 0$, а если изоморфны, то $\mathrm{Hom}_{KG}(V_b^j, V) = \{\lambda\,\mathrm{id}\} \simeq \mathbb{C}$.

□

Лекция 4

Повторение предыдущих лекций

Пусть R — ассоциативное кольцо с единицей, а M и N — модули над R. Группу (с операцией сложения) R–линейных отображений из M в N мы обозначаем $\mathrm{Hom}_R(M, N)$. Был доказан изоморфизм абелевых групп

$$\mathrm{Hom}_R(R, M) \cong M.$$

Этот изоморфизм $\Phi : \mathrm{Hom}_R(R, M) \to M$ имеет вид

$$\Phi(f) = f(1).$$

Также было введено умножение элементов $\mathrm{Hom}_R(R, M)$ на элементы R по формуле

$$(a \cdot f)(m) = a(f(m)) = f(am).$$

И было объяснено, что $\mathrm{Hom}_R(R, M)$ не является (левым) R-модулем, так как

$$((ab) \cdot f)(m) = f(abm), \text{ но } (a \cdot (b \cdot f))(m) = (b \cdot f)(am) = f(bam).$$

Кольцо с противоположным умножением

Определение 13. Пусть R — кольцо. Определим кольцо R^{op} (кольцо с противоположным умножением) следующим образом:

1) как множество R^{op} совпадает с R;

2) операция сложения на R^{op} совпадает с операцией сложения на R;

3) операция умножения на R^{op} определяется так: $ab = ba$, где справа стоит умножение в R.

Легко видеть, что R^{op} действительно является кольцом. Если кольцо R коммутативно, то оно совпадает с R^{op}. В общем случае $(R^{op})^{op} = R$. Если R ассоциативно/имеет единицу, то и R^{op} тоже.

Заметим, что $\mathrm{Hom}_R(R, M)$ является R^{op}–модулем. Напомним, что (левый) R^{op}–модуль также называется правым R–модулем.

Кольцо эндоморфизмов. Теорема

Определение 14. На множестве $\mathrm{Hom}_R(M, M)$ есть единственная операция умножения, а именно операция композиции. Данная операция умножения дополняет структуру абелевой группы на $\mathrm{Hom}_R(R, M)$ до структуры кольца. Это кольцо называется кольцом эндоморфизмов модуля M и обозначается $\mathrm{End}(M)$.

Рассмотрим частный случай, когда $M = R$.

Теорема 10. *Отображение* Φ *задает изоморфизм между* $\mathrm{End}(M)$ *и* R^{op}.

Доказательство. Мы уже знаем, что отображение $\Phi : \mathrm{Hom}_R(R, M) \to M$, $\Phi(f) = f(1)$ задает изоморфизм абелевых групп. Подставим $M = R$ и проверим, что Ψ переводит умножение в $\mathrm{End}(M)$ в умножение в R^{op}. Имеем

$$\Phi(f \circ g) = f \circ g(1) = f(g(1)) = f(g(1) \cdot 1) = g(1)f(1) = \Phi(g)\Phi(f) = \Phi(f)\Phi(g).$$

□

Кольцо эндоморфизмов. Теорема

Пусть M, N и K — это R–модули. Аналогично умножению на $\mathrm{Hom}_R(M, M)$ мы можем определить (снова как композицию) умножение элементов $\mathrm{Hom}_R(N, K)$ на элементы $\mathrm{Hom}_R(M, N)$, а в результате получается элемент из $\mathrm{Hom}_R(M, K)$. (Порядок в данном случае важен).

Пусть X и Y — два R–модуля. Рассмотрим множество

$$M = \begin{pmatrix} f & g \\ h & t \end{pmatrix},$$

где $f \in \mathrm{End}(X)$, $g \in \mathrm{Hom}_R(Y, X)$, $h \in \mathrm{Hom}_R(X, Y)$, $t \in \mathrm{End}(Y)$. Легко проверить, что M является R^{op}–модулем и кольцом (умножение — это умножение матриц; все подобрано таким образом, что соответствующие элементы можно умножать и получится матрица такого же вида): пусть $f, f' \in \mathrm{End}(X)$, $g, g' \in \mathrm{Hom}_R(Y, X)$, $h, h' \in \mathrm{Hom}_R(X, Y)$, $t, t' \in \mathrm{End}(Y)$

$$\begin{pmatrix} f & g \\ h & t \end{pmatrix} \begin{pmatrix} f' & g' \\ h' & t' \end{pmatrix} = \begin{pmatrix} ff' + gh' & fg' + gt' \\ hf' + th' & hg' + t't \end{pmatrix},$$

где $ff' + gh' \in \mathrm{End}(X)$, $fg' + gt' \in \mathrm{Hom}_R(Y, X)$, $hf' + th' \in \mathrm{Hom}_R(X, Y)$, $hg' + t't \in \mathrm{End}(Y)$.

Теорема об изоморфизме кольца эндоморфизмов

Теорема 11. *Имеет место изоморфизм колец и* R^{op}*–модулей*

$$M \cong \mathrm{End}(X \oplus Y).$$

Доказательство. Рассмотрим отображение

$$\Psi : M \to \mathrm{End}(X \oplus Y),$$

$$\Psi \begin{pmatrix} f & g \\ h & t \end{pmatrix} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} f & g \\ h & t \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} f(x) + g(y) \\ h(x) + t(y) \end{pmatrix} \right\}.$$

Проверки, что Ψ — гомоморфизм колец и R^{op}–модулей стандартны.

Чтобы доказать инъективность, проверим, что $\operatorname{Ker}\Psi = \{0\}$. Пусть

$$\begin{pmatrix} f & g \\ h & t \end{pmatrix} \neq 0.$$

Тогда одно из отображений не равно нулю. Пусть это, например, g. Тогда существует $y \in Y$ такой, что $g(y) \neq 0$. Тогда

$$\Psi \begin{pmatrix} f & g \\ h & t \end{pmatrix} \begin{pmatrix} 0 \\ y \end{pmatrix} - \begin{pmatrix} g(y) \\ t(y) \end{pmatrix} \neq 0,$$

то есть данная матрица не из ядра Ψ. Остальные случаи аналогичны.

Проверим теперь сюръективность Ψ. Напомним, что есть естественные проекции

$$\pi_1 : X \oplus Y \to X, \quad \pi_2 : X \oplus Y \to Y.$$

Пусть $\alpha \in \operatorname{End}(X \oplus Y)$. Положим

$$\begin{aligned} f(x) &= \pi_1 \circ \alpha(x, 0), \quad g(y) = \pi_1 \circ \alpha(0, y), \\ h(x) &= \pi_2 \circ \alpha(x, 0), \quad t(y) = \pi_2 \circ \alpha(0, y). \end{aligned}$$

Несложно видеть, что

$$\Psi \begin{pmatrix} f & g \\ h & t \end{pmatrix} = \alpha.$$

Действительно,

$$\Psi \begin{pmatrix} f & g \\ h & t \end{pmatrix} = \begin{pmatrix} f(x) + g(y) \\ h(x) + t(y) \end{pmatrix},$$

$$\begin{aligned} f(x) + g(y) &= \pi_1 \circ \alpha(x, y), \\ h(x) + t(y) &= \pi_2 \circ \alpha(x, y). \end{aligned}$$

Таким образом, теорема доказана. □

Следствие 1. *Если* $\operatorname{Hom}_R(Y, X) = 0$ *и* $\operatorname{Hom}_R(X, Y) = 0$, *то*

$$\operatorname{End}(X \oplus Y) \cong \operatorname{End}(X) \oplus \operatorname{End}(Y).$$

Следствие 2. *Имеет место изоморфизм*

$$\operatorname{End}(X^{\oplus n}) \cong \operatorname{Mat}_{n \times n}(\operatorname{End}(X)).$$

Следствие 3. *Пусть* $M = X_1^{\oplus n_1} \oplus X_2^{\oplus n_2} \oplus \ldots \oplus X_k^{\oplus n_k}$, *где* $\operatorname{Hom}_R(X_i, X_j) = 0$. *Тогда*

$$\operatorname{End}(M) \cong \operatorname{Mat}_{n_1 \times n_1}(\operatorname{End}(X_1)) \oplus \ldots \oplus \operatorname{Mat}_{n_k \times n_k}(\operatorname{End}(X_k)).$$

Теорема об изоморфизме K-алгебр

Возьмем в качестве R групповую алгебру KG и в качестве модуля M также KG. Тогда в условиях теоремы Машке существует разложение на простые модули

$$KG = V_1^{\oplus n_1} \oplus V_2^{\oplus n_2} \oplus \ldots \oplus V_r^{\oplus n_r}, \quad V_i \ncong V_j,$$

где кратности совпадают с размерностями модулей при $K = \mathbb{C}$. По лемма Шура $\mathrm{Hom}_{KG}(V_i, V_j) = 0$. Тогда по следствию 3 получаем

$$KG^{op} \cong \mathrm{End}(KG) \cong \mathrm{Mat}_{n_1 \times n_1}(\mathrm{End}(V_1)) \oplus \ldots \oplus \mathrm{Mat}_{n_r \times n_r}(\mathrm{End}(V_r)).$$

По лемме Шура каждый элемент $\mathrm{End}(V_i)$ является изоморфизмом и, следовательно, обратим. То есть $\mathrm{End}(V_i)$ — тело, которое является K–алгеброй. Если же $K = \mathbb{C}$, то $\mathrm{End}(V_i) \cong \mathbb{C}$ по лемме Шура.

Теорема 12. *Пусть $n_1, \ldots, n_r$ — кратности всех неприводимых представлений конечной группы G над полем K, $\mathrm{char}\, K \nmid |G|$ в разложении представления в групповой алгебре. Тогда для некоторых тел $D_1, \ldots, D_r$, которые являются алгебрами над K, имеет место изоморфизм K–алгебр*

$$KG \cong \mathrm{Mat}_{n_1 \times n_1}(D_1) \oplus \ldots \oplus \mathrm{Mat}_{n_r \times n_r}(D_r).$$

Если же $K = \mathbb{C}$, то все $D_i = \mathbb{C}$.

Доказательство. Из сказанного выше следует, что существует изоморфизм

$$KG^{op} \cong \mathrm{End}(KG) \cong \mathrm{Mat}_{n_1 \times n_1}(S_1) \oplus \ldots \oplus \mathrm{Mat}_{n_r \times n_r}(S_r),$$

где $S_i = \mathrm{End}(V_i)$ — тело и K–алгебра. Положим $D_i = S_i^{op}$. Легко видеть, что это также тело. Кроме того, легко проверить, что $(R_1 \oplus R_2)^{op} = R_1^{op} \oplus R_2^{oplus}$. Далее теорема следует из следующей леммы.

Лемма 2. *Имеет место изоморфизм* $\mathrm{Mat}_{n\times n}(R)^{op} \cong \mathrm{Mat}_{n\times n}(R^{op})$.

Доказательство. Рассмотрим отображение

$$\mathrm{Mat}_{n\times n}(R)^{op} \to \mathrm{Mat}_{n\times n}(R^{op}), \quad A \mapsto A^T.$$

То, что это биекция очевидно. А то, что это гомоморфизм легко проверить.

Пусть

$$\Phi : A \to A^T,$$

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}.$$

Имеем

$$AB = BA.$$

Верно ли, что $\Phi(AB) = \Phi(A) \cdot \Phi(B)$?

$$\Phi(AB) = (AB)^T = (BA)^T = A^T B^T = \Phi(A) \cdot \Phi(B).$$

□

□

Пример 18. Пусть $G = \mathbb{Z}_2 = \langle a \rangle_2$, $K = \mathbb{C}$. Имеем

$$\mathbb{C}\mathbb{Z}_2 = \mathbb{C} \cdot \frac{e+a}{2} \oplus \mathbb{C} \cdot \frac{e-a}{2}.$$

Пример 19. Пусть $G = \mathbb{Z}_3$, $K = \mathbb{C}$, $\mathbb{Z}_3 = \langle a \rangle_3$. Имеем

$$\mathbb{C}\mathbb{Z}_3 = M_1(\mathbb{C}) \oplus M_1(\mathbb{C}) \oplus M_1(\mathbb{C}) = \mathbb{C}\frac{e+a+a^2}{3} \oplus \mathbb{C}\frac{e+\varepsilon a+\varepsilon^2 a^2}{3} \oplus \mathbb{C}\frac{e+\varepsilon a+\varepsilon a^2}{2},$$

где $\varepsilon = e^{\frac{2\pi i}{3}}$.

Пример 20. Пусть $G = S_3$, $K = \mathbb{C}$,

$$\mathbb{C}S_3 = M_1(\mathbb{C}) \oplus M_1(\mathbb{C}) \oplus M_1(\mathbb{C}) = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}S_3 e_3,$$

где

$$e_1 = \sum_{\sigma \in S_3} \sigma, \quad e_2 = \sum_{\sigma \in S_3} \operatorname{sgn} \sigma G,$$
$$e_3 = \frac{2}{3}\operatorname{id} - \frac{1}{3}(1\ 2\ 3) - \frac{1}{3}(1\ 3\ 2).$$

Теорема о степенях неприводимых комплексных представлений

Теорема 13. *Степени неприводимых комплексных представлений конечной группы делят ее порядок.*

Как мы знаем, центр $Z(\mathbb{C}G)$ групповой алгебры $\mathbb{C}G$ состоит из линейных комбинаций, у которых коэффициенты при сопряженных элементах группы равны. Пусть r — число классов сопряженности группы G, $\mathcal{K}_i$ — их сумма. Тогда $K_1, \ldots, K_r$ — базис в $Z(\mathbb{C}G)$. Введем структурные константы алгебры $Z(\mathbb{C}G)$ в этом базисе:

$$K_i K_j = \sum_{s=1}^{r} n_{ij}^s K_s. \tag{1}$$

Лемма 3. *Следующие условия на число $t \in \mathbb{C}$ равносильны:*

1) $t \in \mathbb{Z}_{\mathbb{A}}$ (целое алгебраическое число);

2) $\mathbb{Z}[t]$ — конечно порожденная абелева группа.

Доказательство. $\boxed{(1) \Longrightarrow (2)}$ Если $t^n = a_{n-1}t^{n-1} + \ldots + a_0$, где $a_i \in \mathbb{Z}$, то

$$\mathbb{Z}[t] = \mathbb{Z} \oplus \mathbb{Z}t \oplus \ldots \oplus \mathbb{Z}t^{n-1}.$$

$\boxed{(2) \Longrightarrow (1)}$ Пусть $\mathbb{Z}[t] = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$. Тогда равенства

$$tv_i = a_{i1}v_1 + \ldots + a_{in}v_n, \quad i = 1, \ldots, n$$

означают, что линейная однородная система уравнений с матрицей $tE - A$, где $A = (a_{ij}) \in M_n(\mathbb{Z})$ имеет ненулевое решение $(v_1 \ldots v_n)$ (не все v_i равны 0, так как $1 \in \mathbb{Z}[t]$). □

Доказательство теоремы. Пусть Φ — данное неприводимое комплексное представление группы G в пространстве V размерности n. Продолжим его по линейности до представления групповой алгебры $\mathbb{C}G$, $\Phi : \mathbb{C}G \to \mathrm{End}(V)$. Тогда линейный оператор $\Phi(K_i) \in \mathrm{End}(V)$ перестановочен со всеми $\Phi(g)$ ($g \in G$), а значит по лемме Шура, $\Phi(K_i) = \omega_i \mathcal{E}$. Имеем

$$n\omega_i = \operatorname{tr} \omega_i \mathcal{E} = \operatorname{tr} \Phi(K_i) = \sum_{h \in G} \operatorname{tr}(hg_ih^{-1}) = |\mathcal{K}_i| \chi_\Phi(g_i)$$

$$\Longrightarrow \omega_i = \frac{|\mathcal{K}_i| \chi_\Phi(g_i)}{n}.$$

Применим Φ к (1):

$$\omega_i \omega_j = \sum_{k=1}^{r} n_{ij}^k \omega_k.$$

Значит, $\mathbb{Z}[\omega_1 \dots \omega_r]$ — конечно порожденная абелева группа без кручения, а значит свободная абелева группа конечного ранга. Следовательно, $\mathbb{Z}[\omega_i]$ — свободная абелева группа конечного ранга, откуда по доказанной лемме ω_i — целое алгебраическое число. Аналогично, используя соотношения ортогональности для характеров, получим

$$\frac{|G|}{n} = \frac{|G|}{n}(\chi_\Phi \chi_\Phi)_G = \frac{1}{n} \sum_g \chi_\Phi(g) \overline{\chi_\Phi(g)} = \frac{1}{n} \sum_{i=1}^{r} |\mathcal{K}_i| \chi_\Phi(g_i) \overline{\chi_\Phi(g_i)} = \sum_{i=1}^{r} \omega_i \overline{\chi_\Phi(g_i)}$$

— целое алгебраическое число. Следовательно, $|G|/n \in \mathbb{Z}$. □

Лекция 5

Нетеровы кольца

Пусть A — коммутативное ассоциативное кольцо с 1. Все кольца содержат единицы. Гомоморфизмы переводят 1 в 1.

Определение 15. Кольцо A называется нетеровым кольцом, если выполнено одно из двух эквивалентных условий

1) Всякий идеал в A конечно порожден.

2) Не существует бесконечной строго возрастающей цепочки идеалов $I_1 \subset I_2 \subset I_3 \subset \ldots$ $(I_i \neq I_j)$.

Доказательство эквивалентности. $\boxed{1 \Longrightarrow 2}$ Пусть $I_1 \subset I_2 \subset I_3 \subset \ldots$ — цепочка идеалов. Тогда положим $I = \bigcup_{k=1}^{\infty} I_k$. Так как I — идеал, существуют такие $x_1, \ldots, x_l$, что $I = (x_1, \ldots, x_l)$. Существует такое k, что $x_1, \ldots, x_l \in I_k \Longrightarrow (x_1, \ldots, x_l) \subset I_k \Longrightarrow I = I_k \Longrightarrow$ цепочка $I_1 \subset I_2 \subset I_3 \subset \ldots$ не строго возрастает $(I_k = I_{k+1} = \ldots)$.

$\boxed{2 \Longrightarrow 1}$ Пусть I — идеал в A. Если I нулевой, то $I = \{0\}$. Если нет, то существует $x_1 \in I$, $x_1 \neq 0$. Положим $I_1 = (x_1) \subset I$.

Если $I_1 \neq I$, то существует $x_2 \in I \setminus I_1$. Тогда $I_2 = (x_1, x_2)$, $I_1 \subset I_2$, $I_1 \neq I_2$. И так далее получаем цепочку

$$(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \ldots$$

Следовательно, существует такой k, что $(x_1, \ldots, x_k) = I$. □

Замечание 7. Если A — нетерово кольцо и I идеал в A, то A/I — нётерово. Действительно, обозначим через $\psi : A \to A/I$, $\psi(a) = a + I$. Если $J_1 \subset J_2 \subset J_3 \subset \ldots$ — цепочка идеалов в A/I, то $\psi^{-1}(J_1) \subset \psi^{-1}(J_2) \subset \ldots$ — идеалы в A.

Теорема о модуле над нетеровым кольцом

Теорема 14. *Всякий подмодуль N конечно порожденного модуля M над нетеровым кольцом A конечно порожден.*

Пример 21. Приведем пример не нётерова кольца. Пусть A — кольцо функций $\mathbb{R} \to \mathbb{R}$. Для $n \in \mathbb{N}$ положим

$$I_n = \{f : \mathbb{R} \to \mathbb{R} \mid f|_{[-\frac{1}{n}; \frac{1}{n}]} \equiv 0\}.$$

Цепочка $I_1 \subset I_2 \subset I_3 \subset \ldots$ строго возрастает. Кольцо A — модуль над A. Подмодуль в A — идеал в A. Идеал $I = \bigcup_{n=1}^{\infty} I_n$ — не конечно порожден.

Вернемся к доказательству теоремы.

Лемма 4. *Всякий фактормодуль конечно порожденного модуля конечно порожден.*

Доказательство. Пусть M — модуль и M порожден $m_1, \ldots, m_k$. Тогда если N — подмодуль, то M/N порождается $m_1 + N, \ldots, m_k + N$. □

Лемма 5. *Пусть M_1 — подмодуль модуля M. Если модули M_1 и M/M_1 конечно порождены, то и M конечно порожден.*

Доказательство. Если M_1 порожден $n_1, \ldots, n_r$, а M/M_1 порожден $m_1+M_1, \ldots, m_k+M_k$, то M порожден $n_1, \ldots, n_k, m_1, \ldots, m_k$. □

Доказательство теоремы. Пусть модуль M порожден элементами $x_1, \ldots, x_m$. Проведем индукцию по m.

При $m = 1$. $M \cong A/I$, где I — ядро гомоморфизма модулей $a \to a \cdot x$. Пусть N — подмодуль M. Тогда $N \cong J/I$, где J — идеал, содержащий I. Тогда J конечно порожден и J/I конечно порожден.

При $m > 1$ рассмотрим подмодуль $M_1 \subset M$, порожденный $x_1, \ldots, x_{m-1}$. Положим $N_1 = N \cap M_1$. Тогда N_1 конечно порожден. Но N/N_1 — подмодуль в M/M_1, а M/M_1 порожден элементом $x_m + M_1$. Следовательно, N/N_1 конечно порожден. Тогда по лемме 5 N — конечно порожден. □

Пример

Пример 22. Если $A = \mathbb{Z}$, то A — нётерово (все идеалы в $\mathbb{Z}$ имеют вид (n), $n \in \mathbb{Z}_n$, и $(n) \subset (m) \iff m \mid n$). Модуль над A = абелева группа. Таким образом, теорема, которую мы доказали — обобщение утверждения о том, что подгруппа конечно порожденной абелевой группы конечно порождена.

Теорема Гильберта о базисе

Теорема 15 (Гильберта о базисе)**.** *Кольцо многочленов $A[x]$ над нётеровым кольцом нётерово.*

Доказательство. Пусть I — идеал в $A[x]$. Обозначим через $A[x]_n$ совокупность многочленов степени $\leq n$. Это свободный модуль над A с базисом $1, x, \ldots, x^n$.

Положим $I_n = I \cap A[x]_n$. Тогда I_n конечно порожден (по теореме доказанной выше). Отметим, что $I = \bigcup_{n=1}^{\infty} I_n$.

Обозначим через J_n совокупность коэффициентов при x^n всех многочленов из I_n. Тогда J_n — идеал в A и $J_n \subset J_{n+1}$. Так как A нётерово, то существует такое m, что $J_n = J_m$ при $n \geq m$. Поэтому для всякого $f \in I_n$ найдется такой $g \in I_m$, что $f - x^{n-m} \cdot g \in I_{n-1}$. Поэтому I порождается I_m. Значит, если I_m порождается $f_1, \ldots, f_k$ как A–модуль, то I порождается $f_1, \ldots, f_k$ как идеал в $A[x]$. Следовательно, I конечно порожден. □

Следствие 4. *Кольцо многочленов от любого числа переменных над нётеровым кольцом нётерово (индукция по числу переменных). В частности, кольцо многочленов над любым полем нётерово.*

Радикал кольца

Определение 16. Говорят, что кольцо B порождается элементами $u_1, \ldots, u_n$ над подкольцом A, если каждый элемент B можно представить в виде многочлена $u_1, \ldots, u_n$ с коэффициентами из A. В этом случае имеется сюръективный гомоморфизм

$$f : A[x_1, \ldots, x_n] \to B,$$

$$g(x_1, \ldots, x_n) \to g(u_1, \ldots, u_n),$$

и, следовательно, $B \cong A[x_1, \ldots, x_n]/I$.

Следствие 5. *Всякое кольцо, конечно порожденное над нетеровым подкольцом, нетерово.*

Определение 17. Радикалом кольцо A называется совокупность всех нильпотентов в A. Обозначение: $\operatorname{rad} A$.

Задача 5. *Доказать, что* $\operatorname{rad} A$ *— идеал в* A.

Пример 23. Пусть A — кольцо главных идеалов. Найдем $\operatorname{rad}(A/(n))$, где $n \in A$ — ненулевой необратимый элемент.

Пусть $n = p_1^{k_1} \ldots p_s^{k_s}$ — разложение на простые множители. Элемент $a + (n) \in A/(n)$ нильпотентен $\iff a^n \in (n)$ для некоторого $n \in \mathbb{N} \iff a \vdots p_1 \ldots p_s$. Таким образом, $\operatorname{rad}(A/(n)) = (p_1 \ldots p_s)/(n)$.

Задача 6. *Докажите, что* $\operatorname{rad}(A_1 \oplus \ldots \oplus A_k) = \operatorname{rad} A_1 \oplus \ldots \oplus \operatorname{rad} A_k$.

Определение 18. Идеал I кольца A, не равный A, называется простым, если выполнено одно из двух эквивалентных условий:

1) Из $a \cdot b \in I$ следует, что $a \in I$ или $b \in I$.

2) В A/I нет делителей нуля.

Доказательство эквивалентности. $\boxed{1 \Longrightarrow 2}$ Пусть $(a + I)(b + I) = 0 + I$ в A/I. Тогда $ab \in I$. Но тогда $a \in I$ или $b \in I \Longrightarrow$ или $a + I = 0 + I$, или $b + I = 0 + I$.

$\boxed{2 \Longrightarrow 1}$ Пусть $ab \in I$. Тогда $(a + I)(b + I) = ab + I = 0 + I \Longrightarrow a + I = 0 + I$ или $b + I = 0 + I \Longrightarrow a \in I$ или $b \in I$. □

Теорема 16. *Радикал нётерова кольца* A *совпадает с пересечением простых идеалов.*

Доказательство. Пусть I — простой идеал в A. Если a — нильпотентный элемент, то $a + I$ нильпотентен в $A/I \Longrightarrow a \in I$.

Следовательно, $\operatorname{rad} A$ содержится в пересечении всех простых идеалов. Докажем обратное утверждение. Для этого покажем, что если a — не нильпотентен, то существует простой идеал, не содержащий a.

Рассмотрим множество идеалов в A, не содержащих никакой степени a. Это множество не пусто, так как там лежит нулевой идеал. Так как A — нетерово кольцо,

то в этом множестве есть максимальный идеал, то есть существует идеал I, который не содержит никакой степени a, и при этом не содержится ни в каком другом идеале с таким свойством.

Докажем, что I — простой идеал. Рассмотрим факторкольцо A/I, и пусть $\bar{a} = a + I \in A/I$. Из построений I следует, что $\bar{a}$ не нильпотентен. Но любой ненулевой идеал кольца A/I содержит степень $\bar{a}$. Докажем, что в A/I нет делителей нуля.

Пусть $u, v \in A/I$ и $uv = 0$. Предположим, что $u, v \neq 0$, и рассмотрим идеалы (u) и (v). Тогда существуют такие k и l, что $\bar{a}^k \in (n)$ и $\bar{a}^l \in (v)$. Но тогда $\bar{a}^{k+l} \in (uv) = 0$, что невозможно. □

Лекция 6

Определение целого элемента

Пусть A, B — коммутативные ассоциативные кольца с 1, $A \subseteq B$.

Определение 19. Элемент $b \in B$ цел над A, если существует уравнение целой зависимости $b^m + a_1 b^{m-1} + \ldots + a_{m-1} b + a_m = 0$, $a_1, \ldots, a_m \in A$.

Случай расширения полей: целый элемент $\iff$ алгебраический элемент.

Кольцо B цело над A, если $\forall b \in B$ цел над A.

Случай полей: целое расширение $\iff$ алгебраическое расширение.

Определение 20. Кольцо B конечно над A, если B — конечно порожденный A–модуль. То есть $B = A \cdot b_1 + \ldots + A \cdot b_n$, $b_i \in B$.

Будем рассматривать нетеровы кольца.

Теорема 1

Теорема 17. *Элемент $b \in B$ цел над $A \iff A[b]$ конечно над A.*

Доказательство. $\boxed{\Longrightarrow}$ Имеем

$$b^n + a_1 b^{m-1} + \ldots + a_m = 0 \Longrightarrow$$

$$\Longrightarrow b^m \in A \cdot b^{m-1} + A \cdot b^{m-2} + \ldots + A \cdot b + A \Longrightarrow$$

$$\Longrightarrow b^{m+1} \in A \cdot b^m + A \cdot b^{m-1} + \ldots + A \cdot b \Longrightarrow$$

$$b^{m+2} \in A \cdot b^m + \ldots + A \cdot b \subseteq A \cdot b^{m-2} + \ldots + A$$

и так далее.

В итоге: $A[b]$ порождено как A модуль элементами $b^{m-1}, \ldots, b, 1 \Longrightarrow$ конечно над A.

$\boxed{\Longleftarrow}$ $A[b]$ порождено как A–модуль конечным числом элементов $p_i(b)$, $p_i \in A[x]$ $\Longrightarrow$ $A[b]$ порождено как числом элементов $1, b, \ldots, b^{m-1}$ (как A–модуль). Следовательно, $b^m = a_1 b^{m-1} + \ldots + a_{m-1} b + a_m$ $(a_i \in A) \Longrightarrow b$ цел над A. □

Следствие 6. *Расширение B конечно над $A \Longrightarrow B$ цело над A.*

Доказательство. Для всякого $b \in B$: $A[b] \subseteq B$ — A–подмодуль конечно порожденный A–модуль $\Longrightarrow$ тоже конечно порожден $\Longrightarrow$ по теореме 1 b цел над A. □

Теорема 2

Теорема 18. *Расширение B конечно над $A \iff B = A[b_1, \ldots, b_n]$, b_i целы над A.*

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in ЛЕКЦИИ УЧЕНЫХ МГУ

Доказательство. $\boxed{\Longrightarrow}$ $B = A \cdot b_1 + \ldots + A \cdot b_n$, b_i целы над A по следствию теоремы 1.

$\boxed{\Longleftarrow}$ По теореме 1 $A[b_i]$ конечно над $A \Longrightarrow \exists\, m_1, \ldots, m_n$ для всякого k:

$$b_i^k \in A + A \cdot b_i + \ldots + A \cdot b_i^{m_i - 1}$$

$\Longrightarrow \forall k_1, \ldots, k_n$: $b_1^{k_1} \ldots b_n^{k_n} \in \sum_{l_i < m_i} A \cdot b_1^{l_1} \ldots b_n^{l_n}$. Следовательно, B конечно порожденный A–модуль. □

Следствие 7. *Для конечно порожденной алгебры над полем понятия целого и конечного расширения равносильны.*

Теорема 3

Теорема 19. *Если $A \subseteq B$, $B \subseteq C$ — целые/конечные расширения $\Longrightarrow$ $A \subseteq C$ — тоже целое/конечное расширение.*

Доказательство. Конечные расширения

$$B = A \cdot b_1 + \ldots + A \cdot b_n,$$
$$C = B \cdot c_1 + \ldots + B \cdot c_m$$

$\Longrightarrow C = \sum A \cdot b_i \cdot c_j$ конечно над A, где $i = 1, \ldots, n$, $j = 1, \ldots, m$.

Целые расширения: $\forall c \in C$ существует уравнение целой зависимости $c^m + b_1 c^{m-1} + \ldots + b_m = 0$ $(b_i \in B) \Longrightarrow c$ цел над $A[b_1, \ldots, b_m]$, где b_i целы над A. Следовательно, $A \subseteq A[b_1, \ldots, b_m] \subseteq A[b_1, \ldots, b_m, c] \Longrightarrow A[b_1, \ldots, b_m, c]$ конечно над $A \Longrightarrow c$ цел над A. □

Теорема 20. *$\bar{A} = \{b \in B \mid$ b — целое над A — подкольцо в B. Оно называется целым замыканием A в B. Подкольцо $\bar{A}$ целозамкнуто, т. е. $\forall b \in B$: b — целое над $\bar{A} \Longrightarrow b \in \bar{A}$.*

Доказательство.

1) Пусть $b_1, b_2 \in B$ целы над A. Тогда $A[b_1, b_2]$ конечно над A по теореме 2. Так как $b_1 \pm b_2$, $b_1 \cdot b_2$ целы над A по следствию из теоремы 1.

   Следовательно, $\bar{A}$ — подкольцо.

2) $b \in B$ цел над $\bar{A} \Longrightarrow \bar{A}[b] \supseteq \bar{A} \supseteq A$. Первое включение конечно, а значит цело. Второе включение цело. Следовательно, $\bar{A}[b]$ цело над A по теореме 3.

   Следовательно, b цел над $A \Longrightarrow b \in \bar{A}$.

□

Алгебраическая зависимость

Пусть A — коммутативная ассоциативная алгебра с 1 над полем K без делителей нуля.

Определение 21. Система элементов $a_1, \ldots, a_d \in A$ алгебраически зависима (над K), если существует такой ненулевой многочлен $f \in K[x_1, \ldots, x_d]$, что $f(a_1, \ldots, a_d) = 0$.

Система $\{a_1, \ldots, a_d\}$ — базис трансцендентности алгебры A, если $\{a_1, \ldots, a_d\}$ алгебраически независима, но $\forall a \in A$ система $\{a_1, \ldots, a_d, a\}$ алгебраически зависима.

Пример 24. $A = K[x_1, \ldots, x_n]$ — кольцо многочленов, $\{x_1, \ldots, x_n\}$ — базис трансцендентности.

Замечание 8. $\{a_1, \ldots, a_d\}$ — алгебраически независимая система в A.

Критерий алгебраической зависимости

Лемма 6. *Система $\{a_1, \ldots, a_d\}$ алгебраически зависима $\iff \exists i$: a_i алгебраичен над $K(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d) \subseteq \operatorname{Quot} A$.*

Если $\{a_1, \ldots, a_{d-1}\}$ алгебраически независимая система, то можно взять $i = d$.

Доказательство. $\boxed{\Longrightarrow}$ Возьмем алгебраическую зависимость наименьшей степени: $f(a_1, \ldots, a_d) = 0$, $f \in K[x_1, \ldots, x_d]$, $\deg f = \min$. Пускай f нетривиально зависит от x_i. Если $\{a_1, \ldots, a_d\}$ алгебраически независима, то можно взять $i = d$. Имеем

$$f = f_0 + f_1 x_i + \ldots + f_m x_i^m, \quad f_0, \ldots, f_m \in K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_d], \ f_m \neq 0, m > 0.$$

Следовательно, $f_0(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d) + \ldots + f_m(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d) a_i^m = 0$. Следовательно, a_i алгебраичен над $K(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d)$.

$\boxed{\Longleftarrow}$ Имеем

$$g_0(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d) + \ldots g_n(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d) a_i^n = 0,$$

$$g_k = \frac{p_k}{q_k}, \quad p_k, q_k \in K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_d].$$

Домножив на $q_0 \cdot \ldots \cdot q_n$, получим

$$h = (a_1, \ldots, a_d) = h_0(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d) + \ldots h_n(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d) a_i^n = 0,$$

где $h_k \in K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_d]$, $h \in K[x_1, \ldots, x_d]$.

Следовательно, $\{a_1, \ldots, a_d\}$ алгебраически зависимая система. Следовательно, $\{a_1, \ldots, a_d\}$ — базис трансцендентности в $QuotA$. □

Утверждение о базисе трансцендентности

Утверждение 1. *Любой базис трансцендентности в A является и базисом трансцендентности в* $\operatorname{Quot} A$.

Доказательство. Пусть $\{a_1, \ldots, a_d\}$ — базис трансцендентности в A. Для любого $a \in A$ система $\{a_1, \ldots, a_d, a\}$ алгебраически зависима. По лемме a алгебраичен над $K(a_1, \ldots, a_d)$. Следовательно, $\forall c \in QuotA$ алгебраичен над $K(a_1, \ldots, a_d)$. □

Утверждение 2. $A = K[a_1, \ldots, a_n] \Longrightarrow$ *любая максимальная алгебраически независимая подсистема в* $\{a_1, \ldots, a_n\}$ *является базисом трансцендентности для* A.

Доказательство. Пусть $\{a_1, \ldots, a_d\}$ — максимальная алгебраически независимая подсистема в $\{a_1, \ldots, a_n\}$. Следовательно, $\forall i$: a_i алгебраичен над $K(a_1, \ldots, a_d)$. Следовательно, $\forall a \in A$ алгебраичен над $K(a_1, \ldots, a_d)$. Значит, $\operatorname{Quot} A$ алгебраично над $K(a_1, \ldots, a_d)$. Следовательно, $\{a_1, \ldots, a_d, a\}$ алгебраически зависимая система. □

Следствие о базисе трансцендентности

Следствие 8. *Во всякой конечно порожденной алгебре без делителей нуля существует базис трансцендентности.*

Лемма о замене

Лемма 7 (о замене)**.** *Пусть* $\{a_1, \ldots, a_d\}$ *— базис трансцендентности в* A *и* $a \in A$ *трансцендентен над* $K(a_1, \ldots, a_d)$. *Следовательно,* $\{a, a_1, \ldots, a_d\}$ *— тоже базис трансцендентности в* A.

Доказательство. Так как элемент a трансцендентен над полем, порожденном остальными элементами, система $\{a, a_2, \ldots, a_d\}$ алгебраически независима. И тогда система $\{a, a_1, a_2 \ldots, a_d\}$ будет алгебраически зависима. По лемме a_1 алгебраичен над $K(a_1, \ldots, a_d)$, поле $\operatorname{Quot} A$ алгебраично над $K(a_1, \ldots, a_d)$, следовательно, алгебраично и над $K(a, a_1, \ldots, a_d)$.

Следовательно, для всякого $b \in A$ система $\{a, a_2, \ldots, a_d, b\}$ алгебраически зависима. Следовательно, $\{a, a_2, \ldots, a_d\}$ — тоже базис трансцендентности. □

Теорема о степени трансцендентности алгебры A

Теорема 21. *Все базисы трансцендентности в алгебре* A *содержат одинаковое число элементов. Это число называется степенью трансцендентности алгебры* A $-$ $\operatorname{tr.deg}.A$.

Доказательство. Пусть

$$\{a_1, \ldots, a_d\}, \quad \{b_1, \ldots, b_m\}$$

— два базиса трансцендентности, $d \leq m$. Тогда существует номер i: b_i трансцендентен над $\{a_2, \ldots, a_d\}$ (иначе $b_1, \ldots, b_m$ были бы алгебраичны над $\{a_2, \ldots, a_d\}$, следовательно, все элементы A алгебраичны над $K(b_1, \ldots, b_m)$ и, следовательно, над $K(a_2, \ldots, a_d)$ — противоречие).

Без ограничения общности можно считать, что $i = 1$. По лемме о замене

$$\{b_1, a_2, \ldots, a_d\}$$

— тоже базис трансцендентности.

Далее, аналогично заменяем a_2 на некоторый b_j (с точностью до перенумерации можно считать, что $j = 2$), и так далее. В итоге все элементы базиса $\{a_1, \ldots, a_d\}$ заменили на

$$\{b_1, \ldots, b_d\}$$

— тоже базис трансцендентности. Так как это базис, то $m = d$.

□

Лекция 7

Лемма Нетер о нормализации

Теорема 22 (Лемма Нетер о нормализации)**.** *Пусть K — поле, $|K| = \infty$, $A = K[u_1, \ldots, u_n]$ — конечное алгебраическое поле без делителей нуля. Тогда существует базис трансцендентности $v_1, \ldots, v_d$: A цело над $K[v_1, \ldots, v_d]$.*

Доказательство. Индукция по n. База $n = 1$: $A = K[u_1]$:

- u_1 трансцендентно над K: $v_1 = u_1$;
- u_1 алгебраичен над K.

$$c_m u_1^m + \ldots + c_0 = 0, \quad c_i \in K,$$

$$u_1^m + \frac{c_{m-1}}{c_m} u_1^{m-1} + \ldots + \frac{c_0}{c_m} = 0$$

$$\{v_1, \ldots, v_d\} = \varnothing$$

$$K[v_1, \ldots, v_d] = K.$$

Шаг. Если $u_1, \ldots, u_n$ алгебраически независимы $d = n$.

2) Существует $f \in K[x_1, \ldots, x_n]$: $f(u_1, \ldots, u_n) = 0$, $\deg f = m$,

$$\deg x_1^{a_1} \ldots x_1^{a_n} = \sum a_i$$

$B = K[u_1, \ldots, u_{n-1}] \subset A = K[u_1, \ldots, u_n]$, $\exists v_1, \ldots, v_d \in B$: B цело над $K[v_1, \ldots, v_d]$

$$f = cx^m + p_{n-1}(x_1, \ldots, x_{n-1}) x_n^{m-1} + p_0(x_1, \ldots, x_{n-1})$$

$$0 = f(u_1, \ldots, u_n) = cu_n^m + p_{m-1}(u_1, \ldots, u_{n-1}) u_n^{m-1} + \ldots + p_0(u_1, \ldots, u_{n-1}).$$

$$p_i(u_1, \ldots, u_{n-1}) \in B$$

$$0 = u_n^m + \frac{p_{m-1}(u_1, \ldots, u_{n-1})}{c} u_n^{m-1} + \ldots + \frac{p_0(u_1, \ldots, u_{n-1})}{c}$$

— уравнение целой зависимости на u_n над B.

A цело над B, B цело над $K[v_1, \ldots, v_d] \Longrightarrow A$ цело над $K[v_1, \ldots, v_d]$.

3) Существует $f \in K[x_1, \ldots, x_n]$: $f(u_1, \ldots, u_n) = 0$, $\deg f = m \neq 0$. Сделаем замену $x_i = y_i + a_i y_n$, $x_n = y_n$, $K[x_1, \ldots, x_n] = K[y_1, \ldots, y_n]$

$$f(x_1, \ldots, x_n) = f(y_1 + a_1 y_n, y_2 + a_2 y_n, \ldots, y_{n-1} + a_{n-1} y_n, y_n) = g(y_1, \ldots, y_n),$$

$$\deg g = \deg f = m.$$

$$f = f_0 + f_1 + \ldots + f_m,$$

f_i — однородный многочлен степени i.

$$g = g_0 + g_1 + \ldots + g_m, \quad g_i(y_1, \ldots, y_n) = f_i(y_1 + a_1 y_n, \ldots, y_n).$$

Коэффициент при y_n^m в g_m равен $g_m(0,\dots,0,1) = f_m(a_1,\dots,a_{n-1},1)$.

f_m — ненулевой однородный многочлен, коэффициент при $x_n^m = 0 \Longrightarrow$

$$f_m(a_1,\dots,a_{n-1},1)$$

— ненулевой многочлен от $a_1,\dots,a_{n-1}$.

Найдется бесконечный $f(a_1,\dots,a_{n-1},1)$ — не везде равно 0. Фиксируем такие значения. Существуют $a_1,\dots,a_{n-1}$: $f(a_1,\dots,a_{n-1},1) \neq 0$ в $g(y_1,\dots,y_n)$ коэффициент при $g_n^m \neq 0 \Longrightarrow$ попадает в случай 2. □

Теорема об алгебраическом расширении

Теорема 23. *Пусть A — конечно порожденная алгебра над K. И пусть A — поле. Тогда A — алгебраическое (конечное) расширение K.*

Следствие 9. *Если K алгебраически замкнуто, то в условиях теоремы $A = K$.*

Доказательство теоремы. По лемме Нетер о нормализации $\exists v_1,\dots,v_d \in A$, A цело над $K[v_1,\dots,v_d] = B$.

Докажем, что B — поле. Пусть $u \in B \leq A$, $u \neq 0$. Существует $u^{-1} \in A$, u^{-1} цел над B, т. е.

$$(u^{-1})^m + b_1(u^{-1})^{m-1} + b_{m-1}u^{-1} + b_m = 0 \mid u^{m-1}$$

$$u^{-1} + b_1 + b_2u + \ldots + b_mu^{m-1} = 0$$

$$u^{-1} = -b_1 - b_2u - \ldots - b_mu^{m-1} \in B, \quad b_i \in B,\ u \in B,$$

то есть $u^{-1} \in B$.

$B = K[v_1,\dots,v_d]$, $v_1,\dots,v_d$ — алгебраически независимы над K. A цело над B, следовательно, A — алгебраическое расширение над K. □

Теорема о гомоморфизме и нильпотентном элементе

Теорема 24. *Пусть A — конечное поле над K — алгебраически замкнутое поле, $a \in A$, a — не нильпотент. Тогда $\exists\varphi : A \to K$ — гомоморфизм, такой, что $\varphi(a) \neq 0$.*

Если a нильпотент, то есть a^N, то $\varphi(a)^N = \varphi a$, $\varphi(a) \in K \Longrightarrow \varphi(a) = 0$.

Доказательство. $A' = A[a^{-1}] \cong A[x]/(xa-1)$. Пусть $I' \lhd A'$ — максимальный идеал. Тогда A'/I' — поле — конечное порожденное алгебраическое над K. Порождено $u_1 + I'$, $u_2 + I'$, …, $u_n + I'$, $a^{-1} + I'$. По следствию $A'/I' = K$, $\pi : A' \to A'/I' = K$.

$$a \notin I \Longrightarrow \pi(a) = a + I \neq 0 + I,$$

то есть $\varphi(a) \neq 0$. □

Множество решений

Определение 22. Рассмотрим многочлены $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Скажем, что $H \subset K^n$ — *множество решений*

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

Рассмотрим $A = K[x_1, \ldots, x_n]/I$, $I = (f_1, \ldots, f_m)$,

$$\pi : K[x_1, \ldots, x_n] \to A, \quad \pi(x_i) = x_i + A =: u_i.$$

$$A = K[u_1, \ldots, u_n], \quad a = (a_1, \ldots, a_n) \in M.$$

$$\psi_a : K[x_1, \ldots, x_n] \to K$$

$$f \mapsto f(a).$$

$$\psi : K[x_1, \ldots, x_n] \to K$$

$$x_i \to \psi(x_i) = a_i, \quad \psi = \psi_a.$$

Таким образом, гомоморфизмы $\varphi : A \longrightarrow K$ находятся в биекции с точками $a \in M$.

Теорема Гильберта о нулях

Теорема 25. *Пусть K — замкнутое поле, M — множество решений*

$$\begin{cases} f_1 = 0, \\ \vdots \\ f_m = 0. \end{cases}$$

Пусть $f \in K[x_1, \ldots, x_n]$, $f|_M = 0$. Тогда существует $k \in \mathbb{N}$:

$$f^k \in I = (f_1, \ldots, f_m).$$

Если существует k: $f^k \in I$, то

$$f^k = h_1 f_1 + \ldots + h_m f_m,$$

$$f^k(z) = h_1(z) f_1(z) + \ldots h_m(z) f_m(z) = 0,$$

где $z \in M$, и все $f_i(z) = 0$.

По определению

$$f^k(z) = (f(z))^k \Longrightarrow f(z) = 0.$$

Так как z произвольно, получаем, что $f|_M = 0$.

Доказательство. Пусть $A = K[x_1, \ldots, x_n]/I$. Рассмотрим $u = \pi(f)$, где

$$\pi : K[x_1, \ldots, x_n] \longrightarrow K[x_1, \ldots, x_n]/I = A.$$

Если n не нильпотентен, то существует

$$\varphi : A \longrightarrow K, \quad \varphi(u) \neq 0.$$

Но $\varphi = \varphi_a$, $a \in M$ (мы обсудили, что гомоморфизмы из A в K находятся в биекции с точками из M). И тогда

$$f(a) = \varphi_a(u) = \varphi(u) \neq 0,$$

но $f|_M = 0$ — противоречие. Итак, u нильпотентен, следоательно, существует k: $u^k = 0$,

$$(f + I)^k = f^k + I = 0 + I.$$

Следовательно, $f^k \in I$. □

Лекция 8

Теорема Гильберта о нулях

Теорема 26. *Пусть K — алгебраически замкнутое поле, $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Пусть $Z \subseteq K^n$ — множество решений САУ*

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0. \end{cases}$$

Пусть $I \lhd K[x_1, \ldots, x_n]$, $f \in K[x_1, \ldots, x_n]$. Тогда $f = 0$ на Z тогда и только тогда, когда $\exists k \in \mathbb{N}$: $f^k \in I$, то есть

$$f^k = f_1 g_1 + \ldots + f_m g_m,$$

где $g_i \in K[x_1, \ldots, x_n]$.

Следствие 10. *Множество Z пусто $\iff 1 \in I$.*

Доказательство. Применим теорему к $f = 1$. Действительно, если Z пустое, то любая функция на нем обращается в ноль, а следовательно, $1 \in I$. И наоборот. □

Аффинные алгебраические многообразия

Определение 23. Пусть у нас есть семейство многочленов $f_j \in K[x_1, \ldots, x_n]$, $j \in J$. Множество решений $Z \subseteq K^n$ САУ

$$\begin{cases} f_j(x_1, \ldots, x_n) = 0, \\ j \in J \end{cases}$$

называется *аффинным алгебраическим многообразием.*

Замечание 9. 1) Рассмотрим $I = (f_j \mid j \in J) \lhd K[x_1, \ldots, x_n]$. Тогда Z задается системой уравнений

$$\begin{cases} f_j(x_1, \ldots, x_n) = 0, \\ f \in I \end{cases}$$

2) По теореме Гильберта о базисе идеала, $I = (f_1, \ldots, f_n)$, множество Z можно задать САУ

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0. \end{cases}$$

3) Среди всех идеалов, задающих данное аффинное алгебраическое многообразие Z есть наибольший $I(Z)$, который состоит из всех многочленов, обращающихся в ноль. Его называют идеал аффинного многообразия Z.

Алгебра многочленов на аффинном многообразии

Определение 24. Многочлен на аффинном многообразии Z — это функция вида $f|_Z$, где $f \in K[x_1, \ldots, x_n]$.

Алгебра многочленов на аффинном многообразии

$$K[Z] = \{\text{многочлены на } Z\}.$$

У нас есть естественный гомоморфизм ограничения

$$\rho : K[x_1, \ldots, x_n] \longrightarrow K[Z],$$

$$f \mapsto f|_Z.$$

Он сюръективен по определению, но, вообще говоря, не инъективен. Его ядро

$$\operatorname{Ker} \rho = I(Z).$$

По основной теореме о гомоморфизме имеем

$$K[Z] \cong K[x_1, \ldots, x_n]/I(Z)$$

— конечно порожденная алгебра без нильпотентных элементов.

Построение аффинного алгебраического многообразия

Заметим, что всякая точка $z \in Z$ задает гомоморфизм

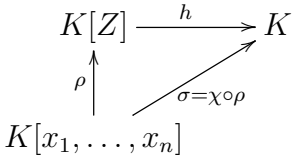
$$\chi_z : K[Z] \longrightarrow K$$

$$g \mapsto g(z).$$

На самом деле любой гомоморфизм в поле

$$\chi : K[Z] \longrightarrow K$$

имеет вид $\chi = \chi_z$. Как это понять? Вспомним, что у нас есть гомоморфизм ограничения ρ



Если мы обозначим $\sigma(x_i) = z_i$ и рассмотрим точку z с координатами z_i, то для любого многочлена $f \in K[x_1, \ldots, x_n]$

$$\sigma(f) = f(z),$$

где $z = (z_1, \ldots z_n)$.

Тогда мы можем заметить, что для любого многочлена $f \in I(Z)$

$$f(z) = \sigma(f) = \chi(\rho(f)) = 0,$$

следовательно, $z \in Z$.

На самом деле верно и обратное. Пусть A — конечно порожденная коммутативная ассоциативная алгебра с 1 над K. Можно построить сюръективный гомоморфизм

$$K[x_1, \ldots, x_n] \longrightarrow A = K[a_1, \ldots, a_n],$$

$$x_i \mapsto a_i.$$

Рассмотрим идеал $I \lhd K[x_1, \ldots, x_n]$, $I = \operatorname{Ker} \pi = (f_1, \ldots, f_n)$. Следовательно, его образ

$$A \cong K[x_1, \ldots, x_n]/I.$$

Если мы теперь рассмотрим $Z \subseteq K^n$, которое задано САУ

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases}$$

то всякая точка многообразия Z задает гомоморфизм

$$\chi_z : A \longrightarrow K,$$

$$a_i \mapsto z_i,$$

и так выглядит любой гомоморфизм $A \longrightarrow K$.

Итак, по конечно порожденной алгебре можно построить аффинное многообразие. Кроме того, если рассмотреть идеал всех многочленов, которые обращаются в ноль, то $I(Z) \subseteq I$, порожденный уравнениями, задающими это аффинное многообразие. По теореме о нулях всякий многочлен из $I(Z)$ в некоторой степени попадает в I. Значит, в соответствующей фактор-алгебре $i(Z)/I$ он равен нулю. Поэтому

$$I(Z)/I = \operatorname{rad} A$$

— идеал, состоящий из всех нильпотентных элементов (радикал A). Таким образом,

$$K[Z] = A/\operatorname{rad} A.$$

Выводы:

1) У нас есть взаимно однозначное соответствие между аффинными алгебраическими многообразиями $Z \subseteq K^n$ и конечно порожденными ассоциативными коммутативными алгебрами с единицей над полем K без нильпотентных элементов вместе с системой порождающих $a_1, \ldots, a_n$.

2) Точки аффинного многообразия Z соответствуют гомоморфизмам

$$\chi : A \longrightarrow K,$$

а многочлены на аффинном алгебраическом многообразии Z соответствуют элементам $g \in A$

$$g(z) = \chi(g).$$

3) Как абстрактное множество аффинное алгебраическое многообразие Z восстанавливается как множество гоморфизмов

$$Z = \{\text{гомоморфизмы } A \longrightarrow K\} =: \operatorname{spec} A$$

— спектр алгебры A.

4) Вложение $Z \hookrightarrow K^n$ соответствует выбору системы n порождающих в A.

Морфизмы и изоморфизмы аффинных многообразий

Определение 25. Пусть $Z \subseteq K^n$ и $W \subseteq K^m$ — аффинные многообразия. *Морфизм* из Z в W — отображение

$$\varphi : Z \longrightarrow W$$

вида

$$\varphi(z) = (f_1(z), \ldots, f_m(z)),$$

где $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$.

Изоморфизм аффинного многообразия — это морфизм, для которого существует обратный морфизм.

Аффинная алгебраическая геометрия изучает внутренние свойства аффинных многообразий (с точностью до изоморфизма).

Заметим, что всякий морфизм $\varphi : X \longrightarrow W$ сопоставлен гомоморфизму

$$\varphi^* : K[W] \longrightarrow K[Z]$$

и

$$(\varphi^* f)(z) = f(\varphi(z)).$$

А именно

$$\begin{array}{ccc} Z & \xrightarrow{\varphi} & W \\ & \searrow^{\varphi^* f} & \downarrow K \\ & & K \end{array}$$

Пусть у нас есть морфизмы

$$Y \xrightarrow{\psi} Z \xrightarrow{\varphi} W,$$

тогда для алгебры многочленов у нас есть гомоморфизм в обратную сторону

$$Y \xleftarrow[\psi^*]{} Z \xleftarrow[\varphi^*]{} W$$

и

$$(\varphi \circ \psi)^* = \psi \circ \varphi.$$

Теорема о соответствии аффинных многообразий и алгебр

Теорема 27. *Имеется взаимно однозначное соответствие между аффинными алгебраическими многообразиями с точностью до изоморфизма и конечно порожденными ассоциативными алгебрами с единицей без нильпотентов, с точностью до изоморфизма*

$$\operatorname{spec} A = Z \longleftrightarrow A = K[Z],$$

и при этом соответствии есть другое соответствие

$$\{\textit{морфизмы } Z \to W\} \longleftrightarrow \{\textit{гомоморфизмы } K[Z] \to K[W]\}.$$

Доказательство. Докажем, что любой гомоморфизм

$$\varphi : K[W] = B \longrightarrow K[Z] = A$$

имеет вид $\Phi = \varphi^*$ для некоторого морфизма

$$\varphi : Z \longrightarrow W.$$

Пусть $A = K[a_1, \ldots, a_n]$, где $a_j = x_j|_Z$ ($x_1, \ldots, x_n$ — координатные функции на $K^n \supseteq Z$). Аналогично $B = K[b_1, \ldots, b_n]$, где $b_j = y_j|_Z$ ($y_1, \ldots, y_n$ — координатные функции на $K^n \supseteq W$). Посмотрим как гомоморфизм

$$\Phi : B \longrightarrow A$$

действует на порождающие элементы. Для $i = 1, \ldots, m$

$$\Phi(b_i) = f_i(a_1, \ldots, a_n)$$

для некоторого $f_i \in K[x_1, \ldots, x_n]$. Для любого $b \in B$:

$$b = f(b_1, \ldots, b_m)$$

для некоторого $f \in K[y_1, \ldots, y_m]$. Следовательно,

$$\Phi(b) = f(\Phi(b_1), \ldots, \Phi(b_m)) = f(f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)).$$

Рассмотрим отображение $\varphi = (f_1, \ldots, f_m)$: $K^n \longrightarrow K^m$. Имеем

$$z = (z_1, \ldots, z_n) \in K^n \longrightarrow \varphi(z) = (f_1(z), \ldots, f_m(z)) \in K^m.$$

Пусть точка $z \in Z$, рассмотрим некоторый многочлен $f \in K[y_1, \ldots, y_m]$, пусть

$$b = f(b_1, \ldots, b_m) \in K[W].$$

Имеем

$$f(\varphi(z)) = f(f_1(z_1, \ldots, z_n), \ldots, f_m(z_1, \ldots, z_m)) = \\ = f(f_1(a_1(z), \ldots, a_n(z)), \ldots f_m(a_1(z), \ldots, a_n(z))) = \Phi(b)(z).$$

Если $f \in I(W)$, то $b = 0$. Следовательно, $f(\varphi(z)) = 0$. Следовательно, $\varphi(z) \in W$, а поэтому

$$\varphi : Z \longrightarrow W$$

— морфизм и $\varphi^* = \Phi$.

Заметим, что φ — изоморфизм $\Longleftrightarrow$ существует обратный морфизм

$$\psi : W \longrightarrow Z,$$

$$\varphi \cdot \psi = \mathrm{id}, \quad \psi \cdot \varphi = \mathrm{id},$$

что равносильно

$$\psi^* \cdot \varphi^* = \mathrm{id}^* = \mathrm{id},$$

$$\varphi^* \cdot \psi^* = \mathrm{id}^* = \mathrm{id}\,.$$

То, что это равносильный переход, основано на том, что есть взаимно однозначное соответствие между морфизмами и гомоморфизмами алгебр, то есть что φ^* — изоморфизм. □

Топология Зарисского

Как уже было сказано ранее, теория аффинных многообразий — это геометрический взгляд на теорию конечно порожденных коммутативных алгебр с единицей. Однако это геометрическое представление интересно само по себе, потому что многообразия как множества, задаваемые системой алгебраических уравнений встречаются довольно часто. Например, в курсе аналитической геометрии рассматривались квадратичные поверхности, кривые второго порядка и т. д. Это простейшие примеры алгебраических многообразий.

Чтобы геометрическая теория была содержательна, нужно вводить дополнительно геометрические и топологические понятия. На всяком геометрическом пространстве есть некое подобие топологии. Оказывается, некая топология существует и на алгебраических многообразиях. Это *топология Зарисского.*

Введем топологию Зарисского на n-мерном координатном пространстве. «Ввести на множестве топологию» — это значит определить класс открытых и класс замкнутых множеств, которые дополняют друг друга: множество открыто тогда и только тогда, когда его дополнение замкнуто. Поэтому неважно, какой класс описывать при задании топологии: если опишем открытые множества, то автоматически определим и замкнутые, и наоборот. Топологию Зарисского удобно описывать через замкнутые множества.

Определение 26. Топология Зарисского на n-мерном координатном пространстве K^n определяется следующим образом: замкнутое подмножество по определению — это алгебраическое многообразие $Z \subseteq K^n$ в n-мерном пространстве, то есть такое подмножество, которое задается системой алгебраических уравнений.

То есть класс замкнутых подмножеств в n-мерном координатном пространстве по отношению к топологии Зарисского — это по определению класс всех аффинных многообразий, то есть таких подмножеств, которые задаются системой алгебраических уравнений.

Надо убедиться, что это действительно топология, то есть что совокупность множеств по отношению к данной топологии удовлетворяет требованиями:

1) множества $\varnothing$ и K^n замкнуты;

2) $\bigcap_{i\in I} U_i$ замкнуты, где U_i замкнуто;

3) $\bigcup_{i=1}^{n} U_i$ замкнуты, где U_i замкнуто.

Проверка условий на топологию:

1) множество $\varnothing$ замкнуто: зададим САУ, которая не имеет решений

$$1 = 0,$$

по определению это алгебраическое многообразие, то есть пустое множество;

1') всё многообразие K^n тоже будет замкнуто, так как задается системой алгебраических уравнений

$$0 = 0$$

(выполнена всегда в любой точке, то есть все точки являются решениями).

2) Докажем, что любые пересечения замкнутых замкнуты, то есть что любые пересечения аффинных многообразий являются аффинными многообразиями, то есть задаются системами алгебраических уравнений.

Пусть $Z_j \subseteq K^n$ $(j \in J)$ замкнуты, следовательно, задаются системами алгебраических уравнений

$$\begin{cases} f_{ij}(x_1, \ldots, x_n) = 0, \\ \forall i \in I_j. \end{cases}$$

Тогда $\bigcap_{i\in I} Z_j$ задается САУ

$$\begin{cases} f_{ij}(x_1, \ldots, x_n) = 0, \\ \forall i, j. \end{cases}$$

Итак, любое пересечение аффинных многообразий будет аффинным многообразием, и следовательно, любое пересечение будет замкнуто.

3) Докажем, что все конечные объединения замкнутых замкнуты, то есть что все конечные объединения аффинных многообразий являются аффинными многообразиями, то есть задаются системами алгебраических уравнений.

Достаточно проверить, что если Z и W аффинные многообразия в аффинном пространстве, то их объединение $Z \cup W$ — тоже. Далее можно доказать по индукции для конечных объединений.

Пусть Z задается САУ

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases}$$

а W задается САУ

$$\begin{cases} g_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ g_k(x_1, \ldots, x_n) = 0. \end{cases}$$

Тогда $Z \cup W$ задается САУ

$$\begin{cases} f_i \cdot g_j = 0, \\ \forall i, j. \end{cases}$$

Действительно, если какая-то точка лежит в Z, то в ней все $f_i = 0$, а значит, и все произведения $f_i \cdot g_j = 0$. Если какая-то точка лежит в W, то в ней все $g_j = 0$, а значит, и все произведения $f_i \cdot g_j = 0$. Если какая-то точка z не лежит ни в Z, ни в W, то существует i и существует j, что

$$f_i(z) \neq 0,$$

$$g_j(z) \neq 0.$$

Тогда в этой точке z имеем $f_i \cdot g_j \neq 0$, и эта точка не удовлетворяет нашей системе.

Таким образом, мы проверили, что множество всех алгебраических многообразий задает топологию на n-мерном пространстве.

Определение 27. Топология Зарисского на произвольном аффинном многообразии $Z \subset K^n$ индуцирована с топологии Зарисского на всем n-мерном пространстве K^n, то есть замкнутыми подмножествами в Z объявляются все пересечения замкнутых подмножеств в K^n с этим множеством Z: так как само множество Z замкнуто, то получаем пересечения замкнутых, которые тоже замкнуты.

Итак, замкнутые подмножества в Z — это аффинные многообразия $W \subseteq Z$.

Замечание 10. Топология Зарисского на аффинном многообразии Z не зависит от вложения $Z \hookrightarrow K^n$, потому что замкнутые подмножества $W \subseteq Z$ — это в точности подмножества, задаваемые системами уравнений вида

$$\begin{cases} g_1(z) = 0, \\ \vdots \\ g_m(z) = 0, \end{cases}$$

где $g_1, \ldots, g_m$ — многочлены из $K[Z]$.

Подробнее. Замкнутые подмножества — это аффинные подмногообразия, которые задаются системами алгебраических уравнений, но поскольку мы рассматриваем только те подмногообразия, которые лежат в Z, то мы можем рассматривать многочлены $g_1, \ldots, g_m$, которые задают множество W и ограничить их на Z. Тогда получим то, что мы называли «многочленами на Z».

В свою очередь алгебра многочленов на Z однозначно с точностью до изоморфизма определяется по многообразию Z и от вложения не зависит. Поэтому класс соответствующих подмножеств тоже не зависит от вложения аффинного многообразия в n-мерного пространства. □

Итак, топология Зарисского является внутренним свойством аффинного алгебраического многообразия.

Лекция 9

Топология Зарисского на аффинном многообразии

Определение 28. Топология Зарисского на произвольном аффинном многообразии $Z \subset K^n$ индуцирована с топологии Зарисского на всем n-мерном пространстве K^n, то есть замкнутыми подмножествами в Z объявляются все пересечения замкнутых подмножеств в K^n с этим множеством Z: так как само множество Z замкнуто, то получаем пересечения замкнутых, которые тоже замкнуты.

Итак, замкнутые подмножества в Z — это аффинные подмногообразия $X \subseteq Z$, которые задаются уравнениями вида

$$f_1(x) = \ldots = f_m(x) = 0,$$

где $f_1, \ldots, f_m \in K[Z]$, или идеалами

$$I = (f_1, \ldots, f_m) \lhd K[Z].$$

Среди идеалов, задающих X внутри Z есть наибольший

$$I = I_Z(X) = \{f \in K[Z] \mid f = 0 \text{ на } X\}.$$

Если X задается идеалом $I \lhd K[Z]$, то

$$I_Z(X) = \{f \in K[Z] \mid \exists k : \ f^k \in I\}$$

по теореме Гильберта о нулях.

Таким образом, есть соответствие между аффинными подмногообразиями в Z и идеалами в $K[Z]$.

Гомоморфизм ограничения

Определение 29. Рассмотрим гомоморфизм ограничения (сюръективный)

$$\rho : K[Z] \longrightarrow K[X] \cong K[Z]/I_Z(X),$$

$$\operatorname{Ker} \rho = I_Z(X).$$

Утверждение 3. *Полиномиальные функции (то есть многочлены) и морфизмы аффинных многообразий непрерывны в топологии Зарисского.*

Доказательство. Полиномиальная функция — это то же самое, что морфизм

$$f : Z \longrightarrow K^1.$$

Поэтому достаточно доказать наше утверждение для морфизмов. Рассмотрим морфизм

$$\varphi : Z \longrightarrow W$$

и докажем, что он является непрерывным отображением в топологии Зарисского.

Итак, отображение непрерывно, если прообраз замкнутого множества замкнут. Если в многообразии W есть подмногообразие $Y \subseteq W$, которое задается уравнениями

$$f_1(y) = \ldots = f_m(y) = 0,$$

где $f_1, \ldots, f_m \in K[W]$. У нас есть гомоморфизм алгебр

$$\varphi^* : K[W] \longrightarrow K[Z],$$

который позволяет поднимать многочлены на многообразии W до многочленов на Z,

$$\varphi^* f(x) = f(\varphi(x)).$$

Тогда

$$X = \varphi^{-1}(Y) \subseteq Z$$

задается уравнениями

$$\varphi^* f_1(x) = \ldots = \varphi^* f_m(x) = 0,$$

следовательно, X замкнуто в Z. □

Топология Зарисского на одномерном пространстве

Классическая топология значительно тоньше топологии Зарисского.

Пример 25. Топология Зарисского на одномерном пространстве. Замкнутые подмножества: $\varnothing$, K^1 и аффинные подмногообразия в данном пространстве (то есть многообразия, заданные алгебраическими уравнениями). В данном случае многочлены в уравнении будут от одной переменной. У каждого многочлена есть конечное количество корней. Так как многочленов несколько, рассмотрим пересечение множеств корней этих многочленов. Итак, замкнутые подмножества, которые у нас будут получаться — это замкнутые подмножества. И наоборот, любое конечное подмножество на одномерном векторном пространстве может задано алгебраическими уравнением.

В частности, в этом примере любые два непустые открытые подмножества обязательно пересекаются. Топология Зарисского не хаусдорфова.

Нетерово топологическое пространство

Определение 30. Топологическое пространство называется *нетеровым*, если любая цепочка вложенных замкнутых подмножеств

$$X_1 \supseteq X_2 \supseteq \ldots \supseteq X_k \supseteq \ldots$$

в нем стабилизируется, то есть существует k:

$$X_k = X_{k+1} = X_{k+2} = \ldots$$

Иными словами, если не существует бесконечно убывающей упочки замкнутых подмножеств.

Утверждение 4. *Аффинное пространство нетерово в топологии Зарисского.*

Доказательство. Напомним, что для каждого аффинного подмногообразия Z есть идеал, который состоит из всех многочленов на Z, обращающихся в 0 на этом подмногообразии. Если у нас в Z была цепочка вложенных замкнутых подмножеств, то соответствующая цепочка идеалов имеет обратное вложение

$$I_Z(X_1) \subseteq I_Z(X_2) \subseteq \ldots \subseteq I_Z(X_k) \subseteq \ldots \lhd K[Z].$$

Вспомним, что алгебра многочленов на аффинном многообразии как любая конечно порожденная алгебра является нетеровой алгеброй: $K[Z]$ нетерова алгебра, следовательно, это нетерово кольцо.

Получаем, что цепочка идеалов стабилизируется, то есть существует k:

$$I_Z(X_k) = I_Z(X_{k+1}) = \ldots$$

А так как эти идеалы задают соответствующие многообразия, то

$$X_k = X_{k+1} = \ldots$$

Утверждение доказано. □

Неприводимое топологическое пространство

Определение 31. Непустое топологическое пространство Z называется *неприводимым*, если его нельзя представить в виде объединения двух замкнутых подмножеств

$$Z = X \cup Y,$$

где X, Y замкнуты и не совпадают со всем Z.

Эквивалентное определение: любые два непустых открытых подмножества $U, V \subseteq Z$ пересекаются $U \cap V \neq \varnothing$.

Теорема 28. *Всякое нетерово топологическое пространство Z единственным образом можно представить в виде объединения конечного числа неприводимых замкнутых подмножеств, и это объединение является минимальным: $\forall i\ Z_i \subseteq \bigcup_{j \neq i} Z_j$. Множества Z_i называются неприводимыми компонентами пространства Z.*

Доказательство. Докажем существование такого разложения. Назовем нетерово пространство Z *хорошим*, если для него выполнено утверждение теоремы, то есть его можно представить в виде

$$Z = Z_1 \cup \ldots \cup Z_s,$$

где Z_i замкнутое неприводимое подмножество, и *плохим* в противном случае. (Наша задача доказать, что плохих не бывает.)

Если Z неприводимо, то оно хорошее (объединение состоит из одного единственного множества). Предположим, что существует плохое Z. Тогда

$$Z = X \cup Y$$

и не совпадают с Z, и или Z, или Y — плохое, так как если бы они оба были хорошими, то Z тоже было бы хорошим, что не так по предположению. Без ограничения общности будем считать, что X плохое. Аналогично существуют плохие замкнутые непустые $X' \subset X$, и так далее.

В итоге получим бесконечную убывающую цепочку замкнутых подмножеств

$$Z \supset X \supset X' \supset X'' \supset \dots$$

Это противоречит нетеровости исходного пространства Z.

Если какое-то Z_i содержится в объединение остальных

$$Z_i \subseteq \bigcup_{j \neq i} Z_j,$$

то его можно выкинуть. Так можно делать до тех пор, пока не получим для всякого i: $Z_i \not\subseteq \bigcup_{j \neq i} Z_j$ (то есть условие теоремы).

Докажем теперь единственность. Пусть

$$Z = Z_1 \cup \dots \cup Z_s = W_1 \cup \dots \cup W_t$$

— два разложения на неприводимые компоненты. Для каждого $i \in \{1, \dots, s\}$ имеем

$$Z_i = (Z_i \cap W_1) \cup \dots \cup (Z_i \cap W_t).$$

Каждое пересечение — замкнутое подмножество, так как является пересечением замкнутых. Но так как Z неприводимо, его нельзя представить в виде объединения нескольких собственных замкнутых подмножеств. Значит, одно из замкнутых подмножеств обязано совпадать с самим Z_i: $\exists j \in \{1, \dots, t\}$, что

$$Z_i = Z_i \cap W_j \subseteq W_j.$$

Аналогично для этого j существует $k \in \{1, \dots, s\}$, что $W_j \subseteq Z_k$. Получаем, что

$$Z_i \subseteq W_j \subseteq Z_k.$$

Получается, что $Z_i \subseteq Z_k$. Но у нас в разложении на неприводимые компоненты ни одно Z_i не содержится в объединении остальных, поэтому такое включение возможно, только если $i = k$. Следовательно,

$$Z_i = W_j.$$

Иными словами, каждая компонента из первого разложения равна какой-то компоненте из второго разложения.

Аналогично $\forall j \in \{1, \dots, t\}$ существует $i \in \{1, \dots, s\}$, что

$$W_j = Z_i.$$

Следовательно, разложения совпадают. □

Следствие 11. *Любое аффинное алгебраическое многообразие Z единственным образом представляется в виде объединения неприводимых многообразий*

$$Z = Z_1 \cup \dots \cup Z_s,$$

так что $\forall i : Z_i \not\subseteq \bigcup_{j \neq i} Z_j$.

Критерий неприводимости многообразия

Утверждение 5. *Аффинное многообразие Z неприводимо тогда и только тогда, когда $K[Z]$ не имеет делителей нуля.*

Доказательство. $\boxed{\Longrightarrow}$ Пусть аффинное многообразие Z неприводимо. Докажем от противного: пусть есть делители нуля, то есть существуют два многочлена f и g на Z, $f, g \neq 0$:

$$f \cdot g = 0.$$

Следовательно,

$$X = \{z \in Z \mid f(z) = 0\},$$
$$Y = \{z \in Z \mid g(z) = 0\}$$

замкнуты и не совпадают с Z, но $X \cup Y = Z$ — противоречит неприводимости Z.

$\boxed{\Longleftarrow}$ Докажем в обратную сторону. Пусть теперь $K[Z]$ не имеет делителей нуля. Докажем от противного. Пусть Z приводимо:

$$Z = X \cup Y,$$

где X, Y замкнуты и не совпадают с Y. Они задаются в Z алгебраическими уравнениями. Выберем многочлен $f \in K[Z]$, что

$$f \neq 0, \quad f|_X = 0,$$

и $g \in K[Z]$, что

$$g \neq 0, \quad g|_Y = 0.$$

Следовательно, $f \cdot g = 0$ всюду. Следовательно, в алгебре есть делители нуля и это противоречие. □

Пример 26. В качестве иллюстрации этого критерия рассмотрим алгебраические многообразия, которые принято называть гиперповерхности. Это многообразия, заданные одним уравнением. Пусть f — произвольный многочлен от n переменных, $f \in K[x_1, \ldots, x_n]$, $f \neq \text{const}$. Рассмотрим многообразие $Z \subset K^n$, которое задается уравнением

$$f(x) = 0$$

— гипреповерхность.

Заметим, что кольцо $K[x_1, \ldots, x_n]$ факториально (то есть в нем есть однозначное разложение на неприводимые множители). Давайте докажем, что если многочлен f неприводим как элемент кольца $K[x_1, \ldots, x_n]$ (то есть не разлагается на множители), то тогда соответствующая поверхность Z является неприводимым многообразием в смысле топологии Зарисского.

Доказательство. Покажем, что

$$I(Z) = (f).$$

Это можно сделать с помощью теоремы Гильберта о нулях. Если $g \in I(Z)$, то по теореме Гильбрета о нулях существует k:

$$f \mid g^k.$$

Так как f — неприводимый многочлен, а разложение на множители единственно, то условие выше равносильно следующему:

$$f \mid g.$$

Таким образом, мы показали, что многочлен обращается в ноль тогда и только тогда, когда кратен многочлену f. Следовательно,

$$K[Z] \cong K[x_1, \ldots, x_n]/(f).$$

Поймем, что в этой алгебре нет делителей нуля. Действительно, пусть у нас есть два многочлена $p, q \in K[Z]$, $p \cdot q = 0$. Эти многочлены являются ограничениями некоторых многочленов на пространство Z

$$p = \widetilde{p}|_Z, \quad q = \widetilde{q}|_Z,$$

где $\widetilde{p}, \widetilde{q} \in K[x_1, \ldots, x_n]$. Поскольку произведение $p \cdot q = 0$ в фактор-алгебре, то произведение $\widetilde{p}, \widetilde{q}$ должно лежать в идеале (f), то есть

$$f \mid \widetilde{p}\widetilde{q} \Longrightarrow$$

$$\Longrightarrow f \mid \widetilde{p} \text{ или } f \mid \widetilde{q}.$$

Следовательно, $p = 0$ или $q = 0$. Тем самым мы доказали, что в алгебре нет делителей нуля. Значит, $K[Z]$ не имеет делителей нуля, и тогда Z не приводимое по доказанному выше критерию.

В общем случае

$$f = \lambda_1 f_1^{k_1} \cdot \ldots \cdot f_s^{k_s}, \lambda \in K^*,$$

где $f_1, \ldots, f_s$ неприводимые попарно не пропорциональные многочлены. Тогда гиперповерхность Z можно разложить в объединение

$$Z = Z_1 \cup \ldots \cup Z_s,$$

где каждое Z_i задается уравнением $f_i = 0$. Так как f_i неприводимы, то по ранее доказанному Z_i будут неприводимы, и тогда мы разложили Z в объединение неприводимых компонент. □

Рациональные функции

Определение 32. Пусть Z — неприводимое многообразие. *Поле рациональных функций* — $K(Z) = \operatorname{Quot} K[Z]$ (поле частных). Каждая рациональная функция $f \in K(Z)$ как элемент поля частных может быть представлена как отношение двух многочленов

$$f = \frac{p}{q},$$

где $p, q \in K[Z]$. Всякую рациональную функцию можно рассматривать как функцию, определенную на открытом подмножестве

$$U = \{z \in Z \mid q(z) \neq 0\}.$$

Объединение таких U дает естественную область определения $U_f \subseteq X$ рациональной функции f.

Задача 7. *Найти естественную область определения U_f для*

$$f = \frac{x_1}{x_3}$$

на гиперповерхности $Z \subset K^4$, задаваемой уравнением $x_1x_2 = x_3x_4$.

Размерность неприводимого многообразия

Размерность неприводимого многообразия

Определение 33. *Размерность неприводимого многообразия* определяется как степень трансцендентности алгебры многочленов на этом многообразии, что то же самое, что степень трансцендентности ее поля частных:

$$\dim Z = \operatorname{tr\,deg} K[Z] = \operatorname{tr\,deg} K(Z).$$

Пример 27. Рассмотрим K^n. Имеем по определению

$$\dim K^n = \operatorname{tr\,deg} K[x_1, \ldots, x_n] = n$$

(сами переменные являются базисом трансцендентности).

Теорема 29. *Пусть Z — неприводимое многообразие, а $X \subseteq Z$ — неприводимое подмногообразие. Тогда $\dim X \leq \dim Z$, и равенство достигается только при $X = Z$.*

Доказательство. Рассмотрим гомоморфизм ограничения

$$\rho : K[Z] \longrightarrow K[X] \cong K[Z]/I_Z(X).$$

Предположим, что мы в алгебре многочленов на X выбрали базис трансцендентности $f_1, \ldots, f_d \in K[X]$, где

$$f_i = \widetilde{f}_i|_X, \quad \widetilde{f}_i \in K[Z].$$

Следовательно, $\widetilde{f}_1, \ldots, \widetilde{f}_d$ алгебраически независимы в $K[Z]$. Следовательно,

$$\dim X = d \leq \dim Z.$$

Пусть $X \subset Z$. Возьмем многочлен $f \in I_Z(X)$, $f \neq 0$, и добавим его к $\widetilde{f}_1, \ldots, \widetilde{f}_d$. Докажем, что $\widetilde{f}_1, \ldots, \widetilde{f}_d$ алгебраически независимы в алгебре многочленов $K[Z]$. Иначе существует алгебраическая зависимость

$$F(\widetilde{f}_1, \ldots, \widetilde{f}_d, f) = 0$$

$$F(\widetilde{f}_1, \ldots, \widetilde{f}_d, f) = F_0(\widetilde{f}_1, \ldots, \widetilde{f}_d) + F_1(\widetilde{f}_1, \ldots, \widetilde{f}_d) \cdot f + \ldots + F_m(\widetilde{f}_1, \ldots, \widetilde{f}_m) \cdot f^m.$$

Можно считать, что $F_0(\widetilde{f}_1, \ldots, \widetilde{f}_d) \neq 0$. Иначе нашу алгебраическую зависимость можно сократить на f. Ограничим нашу зависимость на Z. Применим гомоморфизм ограничения ρ и получим

$$F_0(f_1, \ldots, f_d) = 0,$$

то есть получим алгебраическую зависимость многочленов $f_1, \ldots, f_d$. Противоречие с тем, что $f_1, \ldots, f_d$ — это базис трансцендентности в алгебре многочленов в $K[X]$. Следовательно,

$$\dim Z \geq d + 1,$$

$$\dim X = d.$$

Теорема доказана. □

Пример 28. Пусть $f \in K[x_1, \ldots, x_n]$ неприводим, $X \subset K^n$ — гиперповерхность, заданное уравнением $f(x) = 0$. Следовательно,

$$\dim X = n - 1.$$

Доказательство. Пусть f неприводимо зависит от x_n. Следовательно, для всякого $g \in (f)$ нетривиально зависит от x_n. Следовательно, любой многочлен, не зависящий $g \in K[x_1, \ldots, x_{n-1}]$:

$$g|_X \neq 0.$$

Следовательно, $f_i = x_i|_X$, $i = 1, \ldots, n-1$, алгебраически независимы в $K[X]$. Следовательно, $\dim X \geq n - 1, < n$. Следовательно,

$$\dim X = n - 1.$$

□

Задача 8. *Верно обратное: неприводимое подмногообразие $Z \subset K^n$, $\dim Z = n-1$, следовательно, Z — гиперповерхность.*

Лекция 10

Определение свободной группы

Определение 34. Группа F называется *свободной группой*, если существует подмножество $X \subset F$, удовлетворяющее условию: любое отображение $\varphi : X \longrightarrow G$ продолжается (единственным образом) до гомоморфизма $\varphi^* : F \longrightarrow G$:

$$\varphi^*(x) = \varphi(x), \quad \forall x \in X.$$

Из требования единственности вытекает, что X порождает F:

$$F = \langle X \rangle,$$

и X называют системой свободных порождающих.

Утверждение об изоморфизме свободных групп

Утверждение 6. *Пусть F_1 и F_2 — свободные группы с базисами X_1 и X_2. Тогда*

$$F_1 \cong F_2 \Longleftrightarrow |X_1| = |X_2|,$$

где $|X|$ — мощность X.

Доказательство. Пусть $|X_1| = |X_2|$ и

$$f_1 : X_1 \longrightarrow X_2,$$

$$f_2 : X_2 \longrightarrow X_1$$

— биекции. Возникают отображения

$$\varphi_1 : X_1 \longrightarrow F_2, \quad \varphi_2 : X_2 \longrightarrow F_1.$$

По определению существуют гомоморфизмы

$$\varphi_1^* : F_1 \longrightarrow F_2,$$

$$\varphi_2^* : F_2 \longrightarrow F_1,$$

но если мы рассмотрим гомоморфизм $\varphi_2^*\varphi_1^*$:

$$f_2 f_1 = \mathrm{id}_{X_1}$$

$$\Longrightarrow \varphi_2^*\varphi_1^* \text{ и } i : X_1 \longrightarrow F_1$$

— продолжения вложения $X_1 \longrightarrow F_1$. Следовательно

$$\varphi_2^* = (\varphi_1^*)^{-1},$$

следовательно, это изоморфизм групп.

Обратно: если F_1 — свободная группа со свободных базисом X, то $|X|$ однозначно определена. Рассмотрим

$$N = \langle f^2 \mid f \in F \rangle \Longrightarrow$$

группа F/N абелева, в которой для всякого элемента верно $\bar{f}^2 = e$. Следовательно, это свободная абелева группа, ее ранг равен $|X|$. □

Ранг свободной группы

Определение 35. Мощность любого базиса свободной группы F называется рангом группы F.

Утверждение 7. *Для любой мощности $|S|$ существует свободная группа F с базисом X такой мощности.*

Доказательство. Рассмотрим $W(X)$ — множество слов

$$w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n},$$

где $n = 1, 2, \dots$, а для $n = 0$ получаем пустое слово. Здесь

$$\varepsilon_i = \pm 1.$$

Удобно добавить к X формальное множество X^{-1}:

$$X^{-1} = \{x^{-1} \mid x \in X\},$$

и тогда w — слово в алфавите $X \cup X^{-1}$. Теперь на множестве $W(X)$ введем умножение — конкатенация (приклеивание слов): если есть слова

$$w_1 = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \quad w_2 = x_{n+1}^{\varepsilon_{n+1}} \dots x_{n+m}^{\varepsilon_{n+m}},$$

то конкатенация дает

$$w_1 w_2 = x_1^{\varepsilon_1} \dots x_{n+m}^{\varepsilon_{n+m}}.$$

Данная операция очевидно ассоциативна, $\varnothing = e$, следовательно, $W(X)$ — моноид. Определим на $W(X)$ бинарное отношение: $w_1 \sim w_2$ эквивалентны, если w_2 получается из w_1 вставкой или удалением некоторых подслов вида $x^{-1}x$ или xx^{-1}.

Так как пустое слово эквивалентно $x^{-1}x$:

$$\varnothing \sim x^{-1}x \sim xx^{-1},$$

получаем x^{-1} — обратный элемент к x. Если теперь у нас есть слово

$$w = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n},$$

то

$$w = x_1^{-\varepsilon_1} \dots x_n^{-\varepsilon_n}.$$

Назовем группой $F(= F(X))$ множество классов эквивалентности слов: $[w]$ — класс эквивалентности w. Определим классы

$$[w_1][w_2] = [w_1 w_2],$$

$$[w]^{-1} = [w^{-1}].$$

(Необходимо проверить корректность этого определения: если $w_1 \sim w_1'$ и $w_2 \sim w_2'$, то $w_1 w_2 \sim w_1' w_2'$.) □

Проективные свойства свободной группы

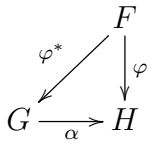
Определение 36. Проективное свойство группы F: если имеется сюръективный гомоморфизм

$$\alpha : G \longrightarrow H,$$

где G и H — группы, то любой гомоморфизм $\varphi : F \longrightarrow H$ порождает единственный гомоморфизм

$$\varphi^* : F \longrightarrow G.$$

Иными словами, имеет место коммутативная диаграмма (φ^* делает эту диаграмму коммутативной)



$$\varphi = \alpha\varphi^*.$$

Давайте увидим, что если F свободная группа, то существование такого гомоморфизма следует из основного определения. В данном случае

$$\operatorname{Im}\alpha = H,$$

и для всякого h рассмотрим $g \in \alpha^{-1}(h)$. Отображение

$$\beta : F \longrightarrow \{\alpha^{-1}(h) \mid h \in H\}.$$

Утверждение 8. *Если группа F свободна, то она обладает проективным свойством. Можно доказать, что верно обратное.*

Утверждение 9. *Любая группа G является гомоморфным образом некоторой свободной группы.*

Доказательство. Пусть группа G порождается некоторым множеством образующих S:

$$G = \langle S \rangle.$$

Рассмотрим свободную группу $F(X)$ с множеством порождающих X, которое биективно соответствует множеству порождающих S. Это биективное соответствие дает биективное отображение

$$\varphi(x) = s.$$

В таком случае существует гомоморфизм

$$\varphi^* : F \longrightarrow G$$

— сюръекция. Что и требовалось доказать. □

Тогда

$$G \cong F(X)/\operatorname{Ker}\varphi^*;$$

порождающие ядра $\operatorname{Ker}\varphi^*$ — определяющие соотношения для группы G.

Приведенное слово

Определение 37. Приведенное (редуцированное) слово — это слово, не содержащее подслов xx^{-1} и $x^{-1}x$. Длина элемента $f \in F$ с базисом X — длина редуцированного слова, представляющего f.

Утверждение 10. *Каждый класс эквивалентности слов содержит единственное редуцированное слово (это можно доказать индукцией по длине слов).*

Для редуцированных слов нормальная форма:

$$w = x_1^{k_1} \dots x_m^{k_m}, \quad k_i \in \mathbb{Z},$$

где $w \neq e$ — не все $k_i = 0$.

Утверждение 11. *1) Если G — такая группа, что если существует сюръективный гомоморфизм*

$$\psi : G \longrightarrow F,$$

где F — свободная, то и сама G свободна.

2) Группа F свободная тогда и только тогда, когда всякий элемент f имеет единственную нормальную форму.

Подгруппы свободных групп

Утверждение 12. *Если F — свободная группа, ранг которой больше 1, то F содержит свободную подгруппу бесконечного ранга.*

Доказательство. Пусть x и y — базисные элементы F ($x \neq y$). Обозначим через

$$V - \{y^{-n}xy^n \mid n \in \mathbb{Z}\}$$

множество, состоящее из «независимых» элементов, то есть $\langle V \rangle$ свободная, бесконечного ранга.

□

Утверждение 13. *Если F свободная, то коммутант $F' = [F, F]$ — свободная группа бесконечного ранга.*

Теорема Нильсена-Шрайера

Теорема 30. *Если F — свободная группа, G — подгруппа в F, то G свободна.*

Доказательство. Доказательство будет приведено из книги Р. К. Линдона, П. Шупа «Комбинаторная теория групп» с некоторыми сокращениями (предложение 3.8).

Если $G < F$, то группа F разлагается в объединение правых смежных классов

$$F = \bigcup_{t \in T} Gt,$$

где T — полная система представителей смежных классов, T называют правой трансверсалью.

Система T имеет шраеровское свойство, если для всякого элемента t, представимого как

$$t = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$$

все начальные отрезки этого слова, которые имеют вид

$$x_1^{\varepsilon_1} \dots x_i^{\varepsilon_i}, \quad i \leq n,$$

также входят в T.

Для доказательства нужно показать, что существует максимальная «шраеровская» трансверсаль T

$$(\exists t \in T, \quad t = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \Longrightarrow$$
$$\Longrightarrow tx \notin T,$$

а все начальные отрезки принадлежат T).

Заметим, что в разложении $F = \cup Gt$ группа F переставляет смежные классы с помощью правого умножения

$$Gt \longrightarrow Gtf, \quad f \in F.$$

Получается подстановка на множестве T.

Утверждение 14 (Вспомогательное утверждение)**.** *Пусть $F(X)$ — свободная группа с базисом X, $T \subset F$ обладает шраеровским свойством. Если задано действие*

$$\pi : F \longrightarrow S(T),$$

причем, для всякого t

$$\pi(t) : 1 \longrightarrow t.$$

Для $w \in T$ обозначим

$$\bar{w} = 1 \cdot \pi(w)$$

(действие справа),

$$\gamma(w) = w\bar{w}^{-1}.$$

Тогда

1) *если*

$$\gamma(t_1 x_1) = \gamma(t_2 x_2) = 1,$$

то $t_1 = x_1$, $x_1 = x_2$.

2) *Если обозначить*

$$\Gamma = \{\gamma(tx) \neq 0 \mid t \in T, x \in X\},$$

следовательно, Γ — базис некоторой свободной подгруппы.

В нашем контексте обозначим $\widetilde{G} = \langle \Gamma \rangle$. Нужно будет доказать, что $\widetilde{G} = G$, то есть G свободна, что и требовалось. □

Два примера свободных групп

Пример 29. Рассмотрим две функции

$$\alpha(x) = x + 2,$$

$$\beta(x) = \frac{x}{2x+1},$$

определенные на $\mathbb{C} \cup \{\infty\}$. Договоренности:

$$\frac{1}{0} = \infty, \quad \frac{\infty}{\infty} = 1.$$

Эти функции обратимы:

$$y = x + 2, \quad x = y - 2, \Longrightarrow$$

$$\Longrightarrow \alpha^{-1}(y) = y - 2,$$

$$y = \frac{x}{2x+1}, \quad x = \frac{y}{1-2y} \Longrightarrow$$

$$\Longrightarrow \beta^{-1}(y) = \frac{y}{1-2y}.$$

Получается, что $\alpha, \beta \in S_{\mathbb{C}\cup\infty}$. И они порождают

$$\langle \alpha, \beta \rangle = H$$

свободную группу с базисом α, β. Любой элемент из H единственным образом представляется в виде произведений степей α, β.

Пример 30. Каждой матрице

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

сопоставим

$$f_A(x) = \frac{ax+b}{cx+d},$$

где $|A| \neq 0$.

Получается, что есть гомоморфизм

$$f : GL(2, \mathbb{C}) \longrightarrow PGL(2, \mathbb{C}),$$

а именно,

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \longrightarrow \alpha,$$

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \longrightarrow \beta.$$

Из примера 1 следует, что

$$\langle A, B \rangle$$

— свободная подгруппа в группе $GL(2, \mathbb{C})$.

Эти два примера связаны. На следующей последней лекции будут подробно рассмотрены другие примеры, связанные с ними задачи и дан список литературы по теме данного спецкурса.

Лекция 11

Система порождающих соотношений

Если G — некоторая группа, порождаемая множеством элементов S, то существует свободная группа

$$F = \langle X \rangle,$$

причем $|X| = |S|$ и эпиморфизм

$$\pi : F \longrightarrow G,$$

такой что $\pi(X) = S$.

По теореме о гомоморфизме

$$G \cong F/\operatorname{Ker}\pi.$$

По теореме Нильсена-Шрайера N — свободная подгруппа в F, кроме того, N — нормальная подгруппа в F. Пусть R — система порождающих N как нормальной подгруппы: N порождается элементами вида

$$N - \langle f^{-1}rf \mid r \in R,\ f \in F\}.$$

Такая порожденная подгруппа называется нормальным замыканием R. Тогда

$$G = \langle S \mid R \rangle,$$

где R — система порождающих, S — система определяющих соотношений.

Обозначим через R_1 систему определяющих соотношений для H. Скажем, что соотношения из R_1 — следствия соотношений из R, если из того, что $\pi(w) = 1$ для $w(x_1, \ldots, x_n) \in R$, то есть $w(g_1, \ldots g_n) = 1$ следует, что $w(h_1, \ldots h_n) = 1$, где h_i — порождающие группы H. Из накрывающего свойства свободной группы тогда следует, что существует эпиморфизм

$$\theta : G = \langle S \mid R \rangle \longrightarrow H = \langle S_1 \mid R_1 \rangle.$$

Пример про группу диэдра

Пример 31. Пусть H — группа диэдра D_n — полная группа симметрии правильного n-угольника.

$$D_n = \{\mathcal{A}, \mathcal{A}^2, \ldots, \mathcal{A}^{n-1}, \mathcal{A}^n = \mathcal{E}, S_1, \ldots, S_n\},$$

где $\mathcal{A}$ — поворот на угол $\frac{2\pi}{n}$, для любой S_i имеем

$$S_i^2 = \mathcal{E},$$

и

$$S^{-1}\mathcal{A}S = \mathcal{A}^{-1}.$$

Для любого S_i

$$S_i = \mathcal{A}^i S_1,$$

следовательно, $D_n = \langle \mathcal{A}, \mathcal{B} = S_1 \rangle$. Это поможет нам доказать, что эта группа изоморфна группе с порождающими соотношениями

$$a^n = 1, \quad b^2 = 1, \quad b^{-1}ab = a^{-1}.$$

Чтобы к этом прийти, необходимо понять, что из соотношений для a и b следует, что любое слово $w(a, b)$ можно привести к виду a^k или $a^k b$. Определим

$$\theta : G \longrightarrow D_n,$$

$$\theta(a) = \mathcal{A}, \quad \theta(b) = \mathcal{B}.$$

Следовательно, θ продолжается до эпиморфизма из G на D_n. Так как $|D_n| = 2n$ и $|G| \leq 2n$, можно проверить, что все элементы вида $a^k b$ для различных k разные, откуда следует, что θ — изоморфизм.

Второй пример про группу диэдра

Пример 32. Можно задать группу диэдра соотношениями

$$D_n \cong \langle a, c \mid a^2 = c^2 = 1, \quad (ac)^n = 1 \rangle,$$

$$a \longleftrightarrow a,$$

$$c \longleftrightarrow b = ac.$$

Способ $\pi : F \longrightarrow G = \langle S \mid R \rangle$ называется заданием группы с помощью образующих и определяющих соотношений (копредставление).

Эквивалетные копредставления

Определение 38. Если есть два разных задания группы

$$G = \langle X \mid R \rangle \text{ и } \langle X' \mid R' \rangle,$$

то скажем, что второе задание получается из первого преобразованием Титце (аналог элементарного преобразования), если

$$X' = X \cup \{x\}, \quad x \notin X$$

или $w \in F$,

$$R' = R \cup \{r\},$$

$$r = x^{-1}w.$$

Тогда можно понять, что группы $\langle X \mid R \rangle \cong \langle X' \mid R' \rangle$.

Задания эквивалентны, если одно получается из другого с помощью конечного числа преобразований Титце.

Утверждение 15. *Пусть есть два задания, что $|X|, |X'|, |R|, |R'| < \infty$. Тогда*

$$\langle X \mid R \rangle \cong \langle X' \mid R' \rangle$$

тогда и только тогда, когда они получаются друг из другая конечным числом преобразований Титце. Говорят, что G конечно задана.

Литература

[1] Коксетер Г.С.М., Мозер У.О.Дж. «Порождающие элементы и определяющие соотношения дискретных групп» (1980).

[2] Вавилов Н.А. «Конкретная теория групп».

Проблемы Дена

1) Проблема равенства слов.

   Пусть $w(s_1, \ldots, s_n) \in G = \langle S \mid R \rangle$. Есть ли алгоритм, позволяющий проверить, что $w(s_1, \ldots, s_n) = 1$.

   Это верно, если G задано одним соотношением.

2) Пусть даны два слова $w_1(s_1, \ldots, s_n), w_2(s_1, \ldots, s_n) \in G$. Можно ли проверить, что данные два слова сопряжены?

3) Проблема изоморфизма: есть ли алгоритм, который проверяет изоморфизм.

$$\langle X \mid R \rangle \cong^? \langle X' \mid R' \rangle$$

   В общем случае проблема имеет отрицательное решение.

Примеры

Пример 33. Пусть $G = S_n$, $n \geq 3$. Кокстеровское задание S_n:

$$G = \langle S_1, \ldots, S_{n-1} \mid S_i^2 = 1,\ S_i S_j = S_j S_i,\ \text{если } |i-j| \geq 2,\ (S_i S_{i+1})^3 = 1 \rangle.$$

Существует ли эпиморфизм $\theta : G \longrightarrow S_n$ и верно ли, что $|G| \leq n!$? Отсюда будет следовать изоморфизм $G \cong S_n$.

Для реализации эпиморфизма θ можно взять

$$\sigma_i = (i, i+1), \quad i = 1, \ldots, n-1,$$

$$\sigma_i^2 = e,$$

$$(i, i+1)(j, j+1) = (j, j+1)(i, i+1), \quad j \geq i+2,$$

$$(i, i+1)(i+1, i+2) = (i, i+1, i+2)$$

— три цикла.

Также

$$S_n = \langle (1\,2) = a, (1\,2\ldots n) = b \rangle,$$

$$(1\,2)^2 = e,$$

$$b^n = e,$$

$$a^{-1} b a = b^{-1}.$$

Пример 34. Треугольные группы.

$$T(k,l,m) = \langle x, y, z \mid x^k = y^l = z^m = 1,\ xyz = 1 \rangle.$$

Утверждение 16. *Группа $T(k,l,m)$ конечна тогда и только тогда, когда*

$$\frac{1}{k} + \frac{1}{l} + \frac{1}{n} > 1.$$

В этом случае $|T(k,l,m)| = \frac{2klm}{n}$, где

$$n = klm(\frac{1}{k} + \frac{1}{l} + \frac{1}{n} - 1).$$

Группа $T(k,l,m)$ изоморфна группе, порожденной поворотами сферической плоскости, евклидовой плоскости или гиперболической плоскости вокруг его вершин на углы, кратные

$$\frac{2\pi}{k}, \quad \frac{2\pi}{l}, \quad \frac{2\pi}{m}.$$

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ