ЛЕКЦИЯ 17

ТЕОРЕМА О СОГЛАСОВАННЫХ БАЗИСАХ

ТЕОРЕМА О СТРОЕНИИ МОДУЛЕЙ И СЛЕДСТВИЯ

ПОЛЯ

ТЕОРЕМА О СОГЛАСОВАННЫХ БАЗИСАХ

Теорема 1. *Всякий подмодуль N свободного R-модуля L ранга n является свободным R-модулем ранга $m \leqslant n$, причем существует такой базис $\{e_1, \ldots, e_n\}$ модуля L и такие (ненулевые) элементы $u_1, \ldots, u_m \in R$, что $\{u_1 e_1, \ldots, u_m e_m\}$ — базис подмодуля N и $u_1 | u_{i+1}$ при $i = 1, \ldots, m-1$.*

Доказательство. Первое утверждение теоремы при $n = 1$ — это определение кольца главных идеалов (всякий подмодуль кольца R, т.е. всякий идеал кольца R является свободным ранга не выше одного, т.е. порожден одним элементом, т.е. главным).

При $n > 1$ утверждение доказывается точно так же, как и для $R = \mathbb{Z}$.

Напомним доказательство для удобства.

Пусть $n > 1$ и $\{e_1, \ldots, e_n\}$ — базис модуля L. Рассмотрим подмодуль $L_1 = \langle e_1, \ldots e_{n-1} \rangle \subset L$. Это свободный R-модуль ранга $n - 1$.

По предположению индукции модуль $N_1 = N \cap L_1$ является свободным R-модулем ранга $m \leqslant n - 1$. Пусть $\{f_1, \ldots, f_m\}$ — его базис.

Рассмотрим последние координаты всех элементов из N в базисе $\{e_1, \ldots, e_n\}$ модуля L.

Они образуют идеал в кольце R, который по определению кольца главных идеалов имеет вид Ra, $a \in R$. Если $a = 0$, то $N = N_1$ и все доказано.

Если $a \neq 0$, то пусть f_{m+1} — какой-нибудь элемент из N, последняя координата которого равна a. Тогда $\{f_1, \ldots, f_m, f_{m+1}$ — базис модуля N, и также все доказано.

Таким образом, первая часть теоремы (подмодуль свободного модуля свободен) доказана.

Доказательство второго утверждения, как и для $R = \mathbb{Z}$, основано на приведении матрицы C перехода от базиса модуля L к базису модуля N к диагональному виду с помощью элементарных преобразований этих базисов.

В случае, когда R — евклидово кольцо, элементарными преобразованиями системы элементов R-модуля называются:

1) прибавление к одному элементу другого, умноженного на элемент кольца R;

2) перестановка двух элементов;

3) умножение одного элемента на обратимый элемент кольца R.

Приведение матрицы C к диагональному виду в этом случае может быть осуществлено так же, как и для абелевых групп, с той оговоркой, что минимизировать надо не сам элемент c_{11} (что не имеет смысла), а его норму.

В общем случае понятие элементарного преобразования следует расширить. Назовем *квазиэлементарным преобразованием* системы элементов $\{x_1, \ldots, x_p\}$ какого-либо R-модуля замену двух элементов x_i и x_j их линейными комбинациями

$$ax_i + bx_j, \qquad cx_i + dx_j,$$

где $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — обратимая матрица с элементами из кольца R (обратимость матрицы равносильна обратимости ее определителя).

Ясно, что преобразование, обратное к квазиэлементарному, также квазиэлементарно, и что элементарные преобразования являются квазиэлементарными.

Любую пару элементов $\{x, y\}$ самого кольца R с помошью квазиэлементарного преобразования можно привести к виду $\{d, 0\}$, где $d = (x, y)$.

В самом деле, существуют такие $a, b \in R$, что $ax + by = d$.

Рассмотрим матрицу

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

Она обратима, так как ее определитель равен 1. Соответствующее квазиэлементарное преобразование переводит $\{x, y\}$ в $\{d, 0\}$.

Следовательно, если в каком-то столбце и какой-то строке матрицы C имеются элементы x, y, то с помощью квазиэлементарного преобразования строк или столбцов из них можно получить элементы $d, 0$.

Такого рода преобразований достаточно, чтобы, следуя алгоритмы как в абелевых группах, привести матрицу C к искомому диагональному виду. $\square$

ТЕОРЕМА О СТРОЕНИИ

Изучим теперь строение произвольных конечно порожденных R-модулей.

Всякий нетривиальный циклический R-модуль изоморфен либо R, либо $R/(u)$, где u — необратимый ненулевой элемент.

Если $(u, v) = 1$, то изоморфизм колец

$$R/(uv) \cong R/(u) \oplus R/(v),$$

построенный нами раньше, является, как легко понять и изоморфизмом R-модулей.

Следовательно, если $u = p_1^{k_1} \dots p_s^{k_s}$ — разложение элемента u на простые множители, то имеет место изоморфизм R-модулей

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

Определение 1. Конечно порожденный R-модуль M, аннулятор которого содержит степень простого элемента $p \in R$, называется *примарным* или *p-примарным*.

Таким образом, всякий периодический циклический R-модуль разлагается в прямую сумму примарных циклических подмодулей.

Теорема 2. *Всякий конечно порожденный R-модуль M разлагается в прямую сумму примарных и свободных циклических подмодулей, причем набор аннуляторов этих подмодулей определяется однозначно.*

Доказательство. Пусть $\{x_1, \ldots, x_n\}$ — система порождающих модуля M. Рассмотрим гомоморфизм

$$\varphi : R^n \to M, \qquad (r_1, \ldots, r_n) \mapsto r_1 x_1 + \cdots + r_n x_n.$$

По теореме о гомоморфизме для модулей

$$M \cong R^n / \ker \varphi = R^n / N.$$

Модуль N является подмодулем свободного конечно порожденного модуля M, поэтому по предыдущей теореме он является свободным, при этом существует такой базис $\{e_1, \ldots, e_n\}$ модуля M и такие элементы $r_1, \ldots, r_m$ $(m \leq n)$ кольца R, что $\{r_1 e_1, \ldots, r_m e_m\}$ — базис модуля N, при этом $r_i | r_{i+1}$.

Рассмотрим гомоморфизм

$$\psi : R^n \to R/(u_1) \oplus \cdots \oplus R/(u_m) \oplus R \oplus \cdots \oplus R,$$

при котором

$$u_1 e_1 + \cdots + u_n e_n \mapsto ([u_1]_{r_1}, \ldots, [u_m]_{r_m}, u_{m+1}, \ldots, u_n).$$

Очевидно, что $\ker \psi = N$. Отсюда следует, что

$$M \cong R/(u_1) \oplus \cdots \oplus R/(u_m) \oplus R \oplus \cdots \oplus R.$$

Таким образом, мы разложили модуль M в конечную сумму свободных циклических модулей и периодических циклических модулей. Каждый периодический циклический модуль, как мы показывали выше, раскладывается в сумму примарных циклических модулей.

Таким образом, мы доказали существование, осталась единственность.

Для доказательства единственности рассмотрим подмодуль кручения

$$\operatorname{Tor} M := \{x \in M \mid ax = 0 \text{ для некоторого } a \in R, a \neq 0\}$$

и, для каждого простого элемента $p \in R$, подмодуль p-кручения

$$\operatorname{Tor}_p M := \{x \in M \mid p^k x = 0 \text{ для некоторого } k \in \mathbb{Z}_+\}.$$

Как и для абелевых групп, доказывается, что $M/\operatorname{Tor} M$ — это модуль без кручения, который оказывается свободным (а в этом случае мы знаем, что количество свободных циклических слагаемых определяется однозначно).

Единственность разложения примарного модуля в прямую сумму примарных циклических подмодулей доказывается по индукции, как и для абелевых групп.

Однако соображение, использовавшее порядок группы, тут не работает.

Вместо него можно применить следующее соображение: если модуль M разложен в прямую сумму p-примарных циклических подмодулей, то число слагаемых равно размерности подмодуля $\{x \in M \mid px = 0\}$ как векторного пространства над полем $R/(p)$. $\square$

ЖОРДАНОВА ФОРМА

В случае $R = \mathbb{F}[t]$ ($\mathbb{F}$ — поле) доказанная теорема описывает строение линейных операторов в векторных пространствах над полем $\mathbb{F}$.

Условие конечной порожденности уж точно будет выполнено, если векторное пространство конечномерно. Более того, в этом случае отсутствуют свободные слагаемые, так как свободный циклический модуль над $\mathbb{F}[t]$ имеет бесконечную размерность над $\mathbb{F}$.

Результат выглядит особенно просто, если поле $\mathbb{F}$ алгебраически замкнуто.

Действительно, в этом случае простыми множителями являются одночлены $(t - \lambda)$, примарными множителями — многочлены $(t - \lambda)^m$, а примарные циклические модули имеют вид

$$\mathbb{F}[t]/((t - \lambda)^m), \qquad \lambda \in \mathbb{F}.$$

Такой модуль является m-мерным векторным пространством над $\mathbb{F}$ с базисом

$$\{[(t - \lambda)^{m-1}], \ldots, [t - \lambda], [1]\},$$

где $[f(t)]$ обозначает класс $f(t) + ((t - \lambda)^m)$.

Оператор умножения на t записывается в этом базисе жордановой клеткой

$$J(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ & \ddots & \ddots & \ddots & \vdots \\ & & & \lambda & 1 \\ & & & 0 & \lambda \end{pmatrix}.$$

Из всех предыдущих расссуждений вытекает

Теорема 3 (теорема о жордановой нормальной форме). *Всякий линейных оператор в конечномерном векторном пространстве над алгебраически замкнутым полем в некотором базисе записывается жордановой матрицей, причем эта матрица определена однозначно с точностью до перестановки клеток.*

Упражнение 1. Получите канонический вид матрицы линейного оператора над полем вещественных чисел.

ПРИМЕРЫ ПОЛЕЙ

Пример 1. Числовые поля $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ являются основными примерами полей для нас.

Пример 2. Для каждого простого числа p мы имеем поле вычетов $\mathbb{Z}_p$ из p элементов.

Пример 3. Поля из 4, 8, 9, 27 элементов легко строятся как

$$\mathbb{Z}_2[x]/(x^2+x+1), \quad \mathbb{Z}_2[x]/(x^3+x+1), \quad \mathbb{Z}_3[x]/(x^2+1), \quad \mathbb{Z}_3[x]/(x^3+x^2+x-1).$$

Пример 4. Для любого натурального числа n, свободного от квадратов, существует поле $\mathbb{Q}[\sqrt{n}]$, которое получается как

$$\mathbb{Q}[x]/(x^2-n).$$

Пример 5. Для любого поля $\mathbb{F}$ можно рассмотреть поле $\mathbb{F}(x)$ рациональных дробей над $\mathbb{F}$. Оно состоит из дробей

$$\frac{f(x)}{g(x)}, \quad f(x), g(x) \in \mathbb{F}[x], \quad g(x) \neq 0.$$

ХАРАКТЕРИСТИКА ПОЛЯ

В поле всегда есть единица, не равная нулю. В аддитивной группе поля единица порождает циклическую подгруппу $\langle 1 \rangle = \{1, 1+1, 1+1+1, \dots\}$. Если данная группа конечна и содержит n элементов, то говорят, что характеристика поля равна n. Если циклическая группа $\langle 1 \rangle$ бесконечна, то говорят, что характеристика поля - нулевая.

Замечание 1. Если у поля $\mathbb{F}$ характеристика равна $n > 0$, то n — простое число.

Действительно, если $n = mk$, то в поле $\mathbb{F}$ сумма m единиц (не равная нулю), умноженная на сумму k единиц (не равную нулю) равна нулю. Значит, в поле имеются делители нуля, что невозможно. Таким образом, положительная характеристика всегда является простым числом.

Если единица в поле имеет порядок p или бесконечный порядок, то такой же порядок имеет и любой ненулевой элемент:

$$a+a+\dots+a+a = a\cdot 1+a\cdot 1+\dots+a\cdot 1 = a(1+1+\dots+1).$$

Лемма 1. *Если поле* $\mathbb{F}$ *имеет характеристику* 0, *то в него естественно вложено подполе* $\mathbb{Q}$ *рациональных чисел. Если поле* $\mathbb{F}$ *имеет характеристику* p, *то в него естественно вложено подполе* $\mathbb{Z}_p$.

Доказательство. Действительно, пусть характеристика поля $\mathbb{F}$ равна нулю. Тогда целые числа можно вложить в поле $\mathbb{F}$ следующим образом: если $n > 0$, то $n = 1 + 1 + \cdots + 1$ (сумма n единиц), отображаем ее в сумму того же числа единиц; ноль отображаем в ноль, а противополжное к n — в противоположное к его образу.

Такое отображение, очевидно, будет гомоморфизмом. Если бы какой-то ненулевой элемент принадлежал ядру этого гомоморфизма, то сумма конечного числа единиц была бы равно нулю в поле $\mathbb{F}$, что невозможно. Значит, это вложение.

Таким образом, можно считать, что целые числа лежат в поле $\mathbb{F}$. Рациональные числа тогда лежат в нем как отношения целых к натуральным.

Если у поля $\mathbb{F}$ характеристика равна p, то то же самое отображение имеет ядро — все целые числа, кратные p. ТАким образом, образ $\mathbb{Z}$ — это $\mathbb{Z}_p$, которое является полем. □

Лемма 2. *Конечное поле может содержать только p^n элементов, где p — простое, n — натуральное число.*

Доказательство. Любое поле является линейным пространством над своим подполем (прямая проверка). В конечном поле характеристики p (ясно, что конечное поле не может иметь характеристику ноль) содержится подполе $\mathbb{Z}_p$. Также ясно, что конечное поле конечномерно. Пусть его размерность над $\mathbb{Z}_p$ равна n. Тогда в нем ровно p^n элементов. □

Упражнение 2. Существует ли бесконечное поле положительной характеристики?

Лемма 3. *Если поле $\mathbb{F}$ характеристики p конечно, то отображение $x \mapsto x^p$ является его автоморфизмом.*

Доказательство. Действительно, это отображение, очевидно, мультипликативно. Оно аддитивно, так как

$$(x+y)^p = x^p + C_p^1 x^{p-1} y + C_p^2 x^{p-2} y^2 + \cdots + C_p^{p-1} x y^{p-1} + y^p,$$

а так как C_p^i для $i = 1, \ldots, p-1$ делится на p, то эта сумма равна $x^p + y^p$ в поле $\mathbb{F}$.

Отображение инъективно, так как из $x^p = y^p$ следует $x^p - y^p = 0 \Longrightarrow (x-y)^p = 0 \Longrightarrow x - y = 0$.

Благодаря конечности поля оно оказывается биективным. $\square$