3. Третья лекция, 16 апреля 2014 г.

3.1. **Аннулятор модуля. Циклические модули.**

Определение 3.1. Модуль, порождённый одним элементом, называется *циклическим*.

Пример 3.2. Всякий циклический $\mathbb{Z}$-модуль изоморфен либо $\mathbb{Z}$, либо $\mathbb{Z}/m\mathbb{Z}$.

Пусть M — произвольный A-модуль. Рассмотрим множество

$$\operatorname{Ann} M = \{a \in A \mid am = 0 \quad \forall m \in M\} \subset A.$$

Оно называется *аннулятором* модуля M. Ясно, что $\operatorname{Ann} M$ — идеал в A.

Нетрудно видеть, что имеется биекция между циклическими A-модулями и идеалами в A:

Теорема 3.3. *Всякий циклический A-модуль M изоморфен A/I, где I — идеал в A, причем $I = \operatorname{Ann} M$.*

Доказательство. Ясно, что если I — идеал в A, то A/I — циклический модуль. Докажем обратное: пусть $M = \langle x \rangle$ — циклический модуль. Рассмотрим гомоморфизм A-модулей

$$f\colon A \to M, \qquad a \mapsto ax.$$

Ясно, что f сюръективен, и $\operatorname{Ker} f = \operatorname{Ann} M$. Но по теореме о гомоморфизме $M \cong A/\operatorname{Ker} f$. □

3.2. **Базис. Свободные модули.**

Как и в случае векторных пространств, для модулей имеют смысл понятия линейной зависимости и базиса.

Определение 3.4. Элементы $x_1, \ldots, x_n \in M$ называются *линейно независимыми*, если для любых $a_1, \ldots, a_n \in A$, не равных нулю одновременно, $a_1x_1 + \cdots + a_nx_n \neq 0$. Линейно независимая система порождающих A-модуля M называется его *базисом*.

В отличие от векторных пространств, не у всякого модуля имеется базис. Так, например, в $\mathbb{Z}/(m)$ базиса нет — поскольку даже всякая система из *одного* элемента оказывается линейно зависимой (поскольку $mx = 0$ для любого $x \in \mathbb{Z}/(m)$).

Определение 3.5. Конечно порождённый модуль, обладающий базисом, называется *свободным*.

Скажем, всякий свободный циклический модуль изоморфен A.

Далее мы будем считать, что A — кольцо главных идеалов.

Теорема 3.6. *Все базисы свободного A-модуля L содержат одинаковое число элементов.*

Доказательство. Если $A = \mathbb{K}$ — поле, то это просто теорема о размерности векторного пространства.

Пусть теперь A — не поле. Выберем в нём произвольный простой элемент $p \in A$. Мы знаем, что $A/(p)$ — поле.

Рассмотрим в модуле L подмодуль pL, полученный как образ гомоморфизма $\mu_p\colon x \mapsto px$. В фактормодуле L/pL идеал $(p) \subset A$ действует нулём, поэтому L/pL является векторным пространством над $A/(p)$ (продумайте этот момент!).

Если $e_1, \dots, e_n$ — базис в L, то классы базисных элементов $[e_1], \dots, [e_n]$ будут образовывать базис в L/pL как в модуле над $A/(p)$ — то есть как в векторном пространстве. А, как известно, все базисы векторного пространства состоят из одинакового числа элементов. □

Определение 3.7. Число элементов в базисе свободного модуля называется его *рангом*.

В силу предыдущей теоремы это определение корректно.

Всякий свободный модуль L изоморфен $A^{\oplus r}$, где r — ранг L. Изоморфизм, как и в случае векторных пространств, определяется выбором базиса в L.

3.3. **Подмодули свободных модулей.** Возникает естественный вопрос: а каким может быть подмодуль свободного модуля? В случае, когда A — кольцо главных идеалов, оказывается, что подмодуль свободного модуля всегда свободен, причём его ранг не превосходит ранга объемлющего модуля.

Теорема 3.8. *Пусть A — кольцо главных идеалов, M — свободный A-модуль ранга m. Пусть $N \subset M$ — подмодуль. Тогда N свободен, причем* $\operatorname{rk} N \leq m$.

Доказательство. В силу замечания в конце предыдущего пункта можно считать, что $M = A^{\oplus m}$. Докажем теорему индукцией по m.

База индукции: $m = 1$, тогда подмодуль N модуля A — это идеал в A. Поскольку A — кольцо главных идеалов, $N = (d)$, то есть либо $N = 0$ (если $d = 0$), либо $A \cong N$ (изоморфизм устанавливается соответствием $a \mapsto a \cdot d$).

Переход. Пусть утверждение доказано при $\operatorname{rk} M < m$. Рассмотрим элементы из N как вектор-строки $(a_1, \dots, a_m) \in A^{\oplus m}$. Посмотрим на множество всех первых координат этих вектор-строк: $I = \{a_1 \mid \exists (a_1, \dots, a_m) \in N\} \subset A$. Ясно, что I — идеал в A (убедитесь в этом!). Возможны два варианта. В первом из них $I = 0$, то есть все первые координаты векторов из N нулевые, то есть $N \subset A^{\oplus(m-1)}$ — тогда утверждение теоремы следует из предположения индукции. Если же $I \neq 0$, то $I = (d)$ для некоторого ненулевого d, то есть все первые координаты векторов из N имеют вид $a \cdot d$ при всевозможных a. Рассмотрим подмодуль $N' \subset N$, состоящий из тех векторов из N, первая координата у которых нулевая.

Нетрудно видеть, что $N = A \cdot d \oplus N'$. Действительно, эти подмодули пересекаются по нулю, и каждый элемент из N представляется в виде суммы вектора вида $(a_1, 0, \ldots, 0) \in A \cdot d$ и $(0, a_2, \ldots, a_m) \in N'$. Но по предположению индукции $N' \subset A^{\oplus(m-1)}$ является свободным модулем, ранг которого не превосходит $m-1$ — следовательно, и $N = A \cdot d \oplus N'$ тоже свободен, и его ранг не выше m. □

Задача 3.9. Приведите пример кольца A, не являющегося кольцом главных идеалов, и ненулевого идеала $I \subset A$, не изоморфного A (тем самым I будет подмодулем свободного модуля, но не будет являться свободным модулем).

3.4. **Взаимные базисы.** Из курса линейной алгебры мы знаем, что в векторном пространстве и его подпространстве можно выбрать базисы согласованным образом: а именно, если $U \subset V$, то в V всегда можно выбрать такой базис, что несколько первых его элементов будут базисом в U. В частности, если $U \subset V$ — векторные пространства одинаковой размерности, то $U = V$. Ясно, что с произвольными модулями над кольцами (даже для $A = \mathbb{Z}$) дело обстоит сложнее: например, у абелевой группы $\mathbb{Z}^n$ бывают подмодули полного ранга, не совпадающие с $\mathbb{Z}^n$. Это уже хорошо видно даже в случае $n = 1$: всякий идеал $(d) \subset \mathbb{Z}$ есть подмодуль ранга 1, который не совпадает с $\mathbb{Z}$, если только, конечно, $d \neq \pm 1$. Однако если A — кольцо главных идеалов, то для каждого свободного A-модуля и подмодуля в нём можно выбрать такой базис в объемлющем модуле, что первые несколько его элементов, *умноженные на подходящие элементы кольца A,* будут образовывать базис подмодуля. Это и утверждает теорема о взаимных базисах.

Теорема 3.10 (о взаимных базисах)**.** *Пусть A — кольцо главных идеалов, M — свободный A-модуль ранга m, $N \subset M$ — его подмодуль ранга n. Тогда существует такой базис $e_1, \ldots, e_m$ модуля M и такие элементы $\lambda_1, \ldots, \lambda_n \in A$, что элементы $\lambda_1 e_1, \ldots, \lambda_n e_n$ образуют базис подмодуля N. Более того, данные элементы можно выбрать таким образом, чтобы при всех i элемент λ_i делил бы λ_{i+1} (а значит, и все последующие).*

В прошлом семестре эта теорема уже доказывалась в случае $A = \mathbb{Z}$. Мы приведём набросок доказательства в этом случае, а общее доказательство дадим в следующей лекции.

Доказательство. Пусть $A = \mathbb{Z}$. Выберем какие-нибудь базисы в M и N; пусть это $v_1, \ldots, v_m$ и $w_1, \ldots, w_n$ соответственно. Векторы второго базиса можно разложить по первому:

$$w_i = \sum_{j=1}^{m} c_{ij} v_j.$$

Возникает прямоугольная матрица $C = (c_{ij})$, по строкам которой записаны разложения векторов w_i по базису v_j. Наша цель — выбрать базисы таким образом, чтобы матрица C была бы диагональной (то есть $c_{ii} = \lambda_i$ и $c_{ij} = 0$ при $i \neq j$), причём чтобы дополнительно каждый следующий диагональный элемент делился бы на предыдущий.

Будем приводить C к диагональному виду методом Гаусса. Для этого мы будем производить над базисами v_j и w_i преобразования, переводящие базис в базис (т.е. не меняющие линейной оболочки базисных векторов). Выделим три вида таких преобразований, знакомые из линейной алгебры:

- прибавление некоторого кратного одного базисного вектора к другому (т.е. замена v_i на $v_i + av_j$, где $a \in \mathbb{Z}$; то же с w_i);
- перестановка двух базисных векторов местами;
- умножение базисного вектора на *обратимый* элемент.

Если выполнять такие преобразования над элементами базиса $v_1, \ldots, v_m$, над матрицей C будут производиться соответствующие элементарные преобразования столбцов. При преобразовании элементов базиса $w_1, \ldots, w_n$ соответствующим образом будут преобразовываться строки матрицы.

Опишем алгоритм приведения матрицы C к диагональному виду. Будем вести индукцию по абсолютной величине элемента c_{11}, стоящего в левом верхнем углу матрицы (если изначально $c_{11} = 0$, то перестановками строк и/или столбцов добьемся того, чтобы в углу стояло бы нечто ненулевое). На каждом шаге будем стремиться уменьшить эту величину.

Рассмотрим элементы, стоящие в первом столбце матрицы. Пусть среди них есть элемент c_{i1}, не делящийся на c_{11}. Тогда c_{i1} можно поделить на c_{11} с остатком: $c_{i1} = qc_{11} + r$, где $0 < r < c_{11}$. Вычтем из i-той строки первую, умноженную на q; получим в i-той строке на первом месте элемент, меньший c_{11}. Поменяем местами i-ю и первую строки и вернёмся к началу алгоритма.

Если же этого не удалось сделать, это значит, что все элементы первого столбца делятся на c_{11}. Тогда из каждой строки можно вычесть подходящее кратное первой строки и сделать так, чтобы весь первый столбец, кроме первого элемента, состоял бы из одних нулей.

Далее рассмотрим первую строку; действуя аналогично, элементарными преобразованиями столбцов добьемся того, чтобы в ней все элементы, начиная со второго, были бы равны нулю.

Посмотрим теперь на элементы матрицы в строках и столбцах с номерами 2 и выше. Мы бы хотели сделать так, чтобы они все делились на c_{11}. Пусть среди них есть элемент c_{ij}, не делящийся на c_{11}. Тогда прибавим i-ю строку к первой; получится, что первый элемент первой строки останется равным c_{11} (т.к. $c_{i1} = 0$), а c_{1j} не

делится на c_{11}. Вернёмся к началу алгоритма; поделив с остатком c_{i1} на c_{11}, уменьшим левый верхний элемент матрицы.

Получится, что матрица C будет приведена к блочному виду: первый столбец и первая строка, за исключением элемента c_{11}, состоят из нулей, а все оставшиеся элементы (образующие матрицу $\widetilde{C}$ размера $(n-1) \times (m-1)$) делятся на c_{11}. Далее применим ту же процедуру к матрице $\widetilde{C}$, и так далее. В конце концов получим диагональную матрицу, в которой каждый предыдущий элемент на диагонали делит все последующие. □

Замечание 3.11. Разумеется, данный алгоритм может не быть оптимальным для практических целей; любители программирования могут подумать о том, как можно было бы его усовершенствовать, чтобы он завершал бы работу по возможности быстрее.

Замечание 3.12. Мы могли бы взять в качестве $w_1, \ldots, w_n$ не базис модуля N, а произвольную конечную систему его порождающих, не обязательно линейно независимую; в результате в ходе работы алгоритма у матрицы C могли бы получаться строки из одних нулей. Это бывает полезно на практике (скажем, при нахождении базиса решётки, заданной системой порождающих).

E-mail address: esmirnov@hse.ru