

20. Двадцатая лекция, 11 апреля 2019 г.

20.1. Дискриминант. Рассмотрим многочлен $f(x)$, раскладывающийся на линейные множители:

$$f(x) = a_n(x - t_1) \dots (x - t_n).$$

ОПРЕДЕЛЕНИЕ 20.1. *Дискриминант* многочлена f — это многочлен

$$D(f) = a_n^{2n-2} \prod_{i < j} (t_i - t_j)^2 = \left[a_n^{n-1} \prod_{i < j} (t_i - t_j) \right]^2.$$

Из определения ясно, что дискриминант обращается в нуль тогда и только тогда, когда среди корней многочлена $f(x)$ есть совпадающие.

Далее, дискриминант является симметрическим многочленом от $t_1, \dots, t_n$, поэтому это многочлен от $a_0, \dots, a_{n-1}, a_n$ и a_n^{-1} . (Контрольный вопрос: зачем здесь a_n^{-1} ?) Найдём этот многочлен. Для этого нам потребуется понятие *производной* многочлена.

ОПРЕДЕЛЕНИЕ 20.2. Пусть $f(x) = a_n x^n + \dots + a_1 x + a_0 \in K[x]$ — многочлен. Его *производная* — это многочлен $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \in K[x]$.

ЗАМЕЧАНИЕ 20.3. Это определение производной многочлена является чисто алгебраическим (в отличие от того, которое давалось в курсе математического анализа — в последнем участвовало понятие предельного перехода). Поэтому имеет смысл говорить о производной многочлена над произвольным полем, в том числе ненулевой характеристики. В отличие, скажем, от вещественной или комплексной ситуации, в характеристике p бывают многочлены, имеющие нулевую производную, но отличные от констант — например, x^p .

УПРАЖНЕНИЕ 20.4. Докажите, что сумму и произведение многочленов можно дифференцировать по правилам, известным из математического анализа: $(f + g)' = f' + g'$ и $(fg)' = f'g + fg'$.

ПРЕДЛОЖЕНИЕ 20.5. *Дискриминант многочлена пропорционален результату его самого и его производной:*

$$D(f) = (-1)^{n(n-1)/2} a_n^{-1} \text{Res}(f, f').$$

ДОКАЗАТЕЛЬСТВО. Продифференцируем производную многочлена по правилу Лейбница:

$$f'(x) = \left(a_n \prod_{i=1}^n (x - t_i) \right)' = a_n \sum_{i=1}^n \prod_{j \neq i} (x - t_j).$$

Особенно хорошо выглядит выражение для производной f' в корне t_i многочлена f : там все слагаемые в последней сумме, кроме i -го, обращаются в нуль:

$$f'(t_i) = a_n \prod_{j \neq i} (t_i - t_j).$$

Воспользовавшись предложением 19.4, получим:

$$\text{Res}(f, f') = a_n^{2n-1} \prod_{i=1}^n \prod_{j \neq i} (t_i - t_j) = a_n (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i < j} (t_i - t_j)^2 = a_n (-1)^{n(n-1)/2} D(f),$$

что и требовалось доказать. □

20.2. Нетеровы кольца. Далее в этой лекции мы рассмотрим *нетеровы кольца*: к этому классу колец принадлежит большинство колец, которые мы рассматривали ранее: кольца главных идеалов, кольца многочленов и т.д. Как обычно, под кольцом мы подразумеваем коммутативное ассоциативное кольцо с единицей.

Дадим два разных определения нетерова кольца и докажем их эквивалентность.

ОПРЕДЕЛЕНИЕ 20.6. (1) Кольцо A называется *нетеровым*, если всякий идеал $I \subset A$ порождается конечным числом элементов.

- (2) Кольцо A называется *нетеровым*, если в нем не существует возрастающей последовательности вложенных идеалов. Иначе говоря, для любой цепочки идеалов

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

существует такое число N , что $I_N = I_{N+1} = I_{N+2} = \dots$.

(Последнее условие часто формулируют так: «всякая возрастающая цепочка идеалов стабилизируется» (или «обрывается»)).

ПРЕДЛОЖЕНИЕ 20.7. *Эти определения эквивалентны.*

ДОКАЗАТЕЛЬСТВО. (1) $\Rightarrow$ (2). Предположим, что в кольце A каждый идеал конечно порожден, но при этом нашлась бесконечно возрастающая цепочка идеалов I_k , которая не стабилизируется. Рассмотрим объединение всех идеалов цепочки: $I = \bigcup_{k=1}^{\infty} I_k$. Это идеал в A (почему?). Значит, он конечно порожден: $I = (x_1, \dots, x_m)$ для некоторых элементов $x_1, \dots, x_m$. Каждый из элементов x_i лежит в некотором из идеалов цепочки, то есть существует такое N , для которого $x_1, \dots, x_m \in I_N$. Но тогда получается, что $I = I_N = I_{N+1} = \dots$, то есть цепочка I_k стабилизируется.

(2) $\Rightarrow$ (1). Предположим, что I — бесконечно порожденный идеал. Выберем в нем некоторый ненулевой элемент x_1 . Пусть $I_1 = (x_1)$. Далее выберем $x_2 \in I \setminus I_1$ и положим $I_2 = (x_1, x_2)$, и так далее. На каждом шаге разность идеалов будет непуста, т.к. противное обозначало бы конечную порожденность идеала I . Мы получили бесконечную цепочку идеалов $I_1 \subset I_2 \subset \dots$, которая не стабилизируется. $\square$

ПРИМЕР 20.8. Всякое кольцо главных идеалов, очевидно, будет нетеровым, т.к. каждый идеал в нем порожден одним элементом.

ПРИМЕР 20.9. Кольцо $\mathbb{K}[x_1, x_2, \dots]$ многочленов (т.е. конечных сумм мономов) от счетного числа переменных не является нетеровым.

Выясним, как могут быть устроены конечно порожденные модули над нетеровыми кольцами.

ТЕОРЕМА 20.10. *Всякий подмодуль N конечно порожденного модуля M над нетеровым кольцом A конечно порожден.*

ЗАМЕЧАНИЕ 20.11. Если $M = A$, то получается просто первое определение нетерова кольца.

Начнем со следующих двух очевидных лемм о модулях над произвольным кольцом (не обязательно нетеровым).

ЛЕММА 20.12. *Всякий подмодуль конечно порожденного модуля конечно порожден.*

ЛЕММА 20.13. *Пусть $M' \subset M$ — подмодуль. Если M' и M/M' конечно порождены, то и M конечно порожден.*

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 20.10. Пусть модуль M порожден элементами $x_1, \dots, x_m$. Докажем утверждение индукцией по m .

База: $m = 1$. Тогда $M \cong A/I$, где I — идеал в кольце A . Значит, $N = J/I$, где J — некоторый идеал, содержащий I . По определению нетерова кольца J конечно порожден как A -модуль; но тогда, по лемме 20.12, и N конечно порожден.

Пусть $m > 1$. Рассмотрим подмодуль $M' \subset M$, порожденный элементами $x_1, \dots, x_m$. Положим $N' = N \cap M'$. По предположению индукции N' конечно порожден. Но фактормодуль N/N' есть подмодуль в циклическом модуле M/M' , то есть тоже конечно порожден. Тогда из леммы 20.13 получается, что и N конечно порожден. $\square$

Основной способ доказательства нетеровости какого-либо кольца дает *теорема Гильберта о базисе идеала*.

ТЕОРЕМА 20.14 (Гильберта о базисе идеала). *Кольцо многочленов $A[x]$ над нетеровым кольцом A нетерово.*

ДОКАЗАТЕЛЬСТВО. Пусть I — идеал в кольце $A[x]$. Обозначим через $A[x]_n$ множество всех многочленов степени не выше n . Это свободный A -модуль с базисом $\{1, x, x^2, \dots, x^n\}$. Положим $I_n = I \cap A[x]_n$. По теореме 20.10 I_n будет конечно порожденным A -модулем. Ясно, что $I = \bigcup_{n=0}^{\infty} I_n$.

Обозначим через J_n множество старших коэффициентов (т.е. коэффициентов при x^n) всех многочленов из I_n . Ясно, что $J_n \subset A$ будет идеалом, и $J_n \subset J_{n+1}$. В силу нетеровости кольца A существует такое m , для которого $J_n = J_m$ при $n \geq m$. Поэтому для всякого многочлена $f \in I_n$, где $n \geq m$, существует многочлен степени не выше m из I_m с тем же старшим коэффициентом, т.е. такой $g \in I_m$, что $f - x^{n-m}g \in I_{n-1}$. Стало быть, идеал I кольца $A[x]$ порождается своей компонентой m -й степени I_m . Значит, если I_m порождается какими-то многочленами $f_1, \dots, f_k$ как A -модуль, то I порождается этими же многочленами как $A[x]$ -модуль. $\square$

СЛЕДСТВИЕ 20.15. *Кольцо многочленов $A[x_1, \dots, x_n]$ над нетеровым кольцом от любого конечного числа переменных нетерово.*

Про теорему Гильберта о базисе можно думать следующим образом. Рассмотрим некоторую бесконечную систему полиномиальных уравнений $f_\alpha(x_1, \dots, x_m) = 0$ от m неизвестных. Левые части этих уравнений образуют некоторый идеал $I \subset \mathbb{K}[x_1, \dots, x_m]$. Можно рассмотреть множество решений этой системы (его обычно обозначают $V(I)$). Теорема Гильберта о базисе гарантирует, что любую такую систему уравнений можно заменить на *конечную* систему, эквивалентную данной (т.е. с тем же множеством решений $V(I)$), выбрав конечный базис идеала I .

Отметим лишь, что теорема Гильберта не дает никакого *конструктивного* способа находить эту конечную систему уравнений, а только гарантирует ее существование. Утверждают, что современник Гильберта и крупнейший специалист того времени по теории инвариантов Пауль Гордан, узнав об этом результате Гильберта, воскликнул: «Это не математика, это теология!».