§ 10. Результант

В этом параграфе мы предполагаем, что читатель знаком с определителями. Теория определителей будет изложена позднее.

Пусть A — коммутативное кольцо, и пусть $v_0, \ldots, v_n, w_0, \ldots, w_m$ алгебраически независимы над A. Образуем два многочлена

$$f_v(X) = v_0X^n + \ldots + v_n,$$
$$g_w(X) = w_0X^m + \ldots + w_m.$$

Назовем *результантом* наборов (v, w), или многочленов f_v, g_w, определитель

$$\begin{array}{c} m\left\{\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right. \\ n\left\{\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right. \end{array} \underbrace{\begin{vmatrix} v_0 & v_1 & \ldots & v_n & & & & \\ & v_0 & v_1 & \ldots & v_n & & & \\ & & \ddots & \ddots & & \ddots & & \\ & & & v_0 & v_1 & \ldots & v_n & \\ w_0 & w_1 & \ldots & w_m & & & & \\ & w_0 & w_1 & \ldots & w_m & & & \\ & & \ddots & \ddots & & \ddots & & \\ & & & w_0 & w_1 & \ldots & & w_m \end{vmatrix}}_{m+n}$$

Пустые места предполагаются заполненными нулями.

Если подставить вместо (v) и (w) в коэффициенты многочленов f_v и g_w соответственно элементы $(a) = (a_0, \ldots, a_n)$ и $(b) = (b_0, \ldots, b_m)$ из A, то получатся многочлены f_a и g_b с коэффициентами в A, и *мы берем в качестве их результанта определитель, полученный подстановкой* (a) *вместо* (v) *и* (b) *вместо* (w) *в написанный выше определитель*. Результант многочленов f_v, g_w будем обозначать символом

$$R(f_v, g_w) \quad \text{или} \quad R(v, w).$$

Результант $R(f_a, g_b)$ получается подстановкой (a) и (b) вместо соответственно (v) и (w).

Заметим, что $R(v, w)$ — многочлен с целочисленными коэффициентами, т. е. мы можем взять $A = \mathbf{Z}$. Если z — переменная, то

$$R(zv, w) = z^m R(v, w) \quad \text{и} \quad R(v, zw) = z^n R(v, w),$$

что непосредственно видно, если вынести z из первых m строк (соответственно последних n строк) определителя. Таким образом, R однороден степени m по первому набору переменных и однороден степени n по второму набору переменных. Кроме того, будучи пред-

ставлен в виде суммы одночленов, результант $R(v, w)$ содержит одночлен

$$v_0^m w_m^n$$

с коэффициентом 1.

Если подставить в результант 0 вместо v_0 и w_0, то получится 0, поскольку обратится в 0 первый столбец определителя.

Будем теперь действовать над кольцом целых чисел $\mathbf{Z}$. Рассмотрим линейные уравнения

$$\begin{aligned}
X^{m-1}f_v(X) &= v_0X^{n+m-1} + v_1X^{n+m-2} + \ldots + v_nX^{m-1},\\
X^{m-2}f_v(X) &= \qquad\qquad v_0X^{n+m-2} + \ldots + v_nX^{m-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
f_v(X) &= \qquad\qquad\qquad\qquad v_0X^n + \ldots + v_n,\\
X^{n-1}g_w(X) &= w_0X^{n+m-1} + w_1X^{n+m-2} + \ldots + w_mX^{n-1},\\
X^{n-2}g_w(X) &= \qquad\qquad w_0X^{n+m-2} + \ldots + w_mX^{n-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
g_w(X) &= \qquad\qquad\qquad\qquad w_0X^m + \ldots + w_m.
\end{aligned}$$

Пусть C — столбец, составленный из левых частей, и пусть

$$C_0, \ldots, C_{m+n-1}$$

— столбцы из коэффициентов. Наши уравнения могут быть записаны так:

$$C = X^{n+m-1}C_0 + \ldots + 1 \cdot C_{m+n}.$$

По правилу Крамера, примененному к последней неизвестной, а именно к 1, получаем

$$R(v, w) = \det(C_0, \ldots, C_{m+n-1}) = \det(C_0, \ldots, C_{m+n-2}, C).$$

Отсюда мы видим, что существуют такие многочлены $\varphi_{v,w}$ и $\psi_{v,w}$ в $\mathbf{Z}[v, w][X]$, для которых

$$\varphi_{v,w}f_v + \psi_{v,w}g_w = R(v, w).$$

Отметим, что $R(v, w) \in \mathbf{Z}[v, w]$, но многочлены в левой части содержат переменную X.

Пусть λ: $\mathbf{Z}[v, w] \to A$ — гомоморфизм в коммутативное кольцо A. Положим $\lambda(v) = (a)$, $\lambda(w) = (b)$; тогда

$$\varphi_{a,b}f_a + \psi_{a,b}g_b = R(a, b) = R(f_a, g_b).$$

Таким образом, из общего соотношения для результанта над $\mathbf{Z}$ мы получаем аналогичное соотношение для всякой пары многочленов над любым коммутативным кольцом A.

Предложение 3. *Пусть K — подполе поля L, и пусть f_a, g_b — многочлены в $K[X]$, имеющие общий корень ξ в L. Тогда $R(a, b)=0$.*

Доказательство. Если $f_a(\xi)=g_b(\xi)=0$, то, подставляя ξ вместо X в выражение, полученное для $R(a, b)$, находим, что $R(a, b)=0$.

Исследуем теперь зависимость между результантом и корнями наших многочленов f_v, g_w. Нам потребуется

Лемма. *Пусть $h(X_1, \ldots, X_n)$ — многочлен от n переменных над кольцом целых чисел $\mathbf{Z}$, обращающийся в 0, если подставить X_1 вместо X_2 и оставить все другие X_i неизменными ($i\neq 2$). Тогда $h(X_1, \ldots, X_n)$ делится на X_1-X_2 в $\mathbf{Z}[X_1, \ldots, X_n]$.*

Доказательство. Упражнение для читателя.

Пусть $v_0, t_1, \ldots, t_n, w_0, u_1, \ldots, u_m$ алгебраически независимы над $\mathbf{Z}$. Образуем многочлены

$$f_v=v_0(X-t_1)\ldots(X-t_n)=v_0X^n+\ldots+v_n,$$
$$g_w=w_0(X-u_1)\ldots(X-u_m)=w_0X^m+\ldots+w_m.$$

Таким образом, мы полагаем

$$v_i=(-1)^i v_0 s_i(t) \quad \text{и} \quad w_j=(-1)^j w_0 s_j(u).$$

Предоставляем читателю легкую проверку того, что

$$v_0, v_1, \ldots, v_n, w_0, w_1, \ldots, w_m$$

алгебраически независимы над $\mathbf{Z}$.

Предложение 4. *В предыдущих обозначениях имеем*

$$R(f_v, g_w)=v_0^m w_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(t_i-u_j).$$

Доказательство. Обозначим через S выражение, стоящее в правой части равенства из формулировки предложения.

Так как $R(v, w)$ однороден степени m по своим первым переменным и однороден степени n по вторым переменным, то

$$R=v_0^m w_0^n h(t, u),$$

где $h(t, u)\in\mathbf{Z}[t, u]$ В силу предложения 3 результант обращается в нуль при подстановке t_i вместо u_j ($i=1, \ldots, n$ и $j=1, \ldots, m$), откуда по лемме вытекает, что R, рассматриваемый как элемент из $\mathbf{Z}[v_0, t, w_0, u]$, делится на t_i-u_j для каждой пары (i, j). Следовательно, R делится в $\mathbf{Z}[v_0, t, w_0, u]$ на S, поскольку разность t_i-u_j является, очевидно, простым элементом в этом кольце, и различные пары (i, j) приводят к различным простым элементам.

Из равенства

$$S = v_0^m w_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (t_i - u_j) \tag{1}$$

и из того факта, что

$$\prod_{i=1}^{n} g(t_i) = w_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (t_i - u_j),$$

мы получаем

$$S = v_0^m \cdot \prod_{i=1}^{n} g(t_i). \tag{2}$$

Аналогично

$$S = (-1)^{nm} w_0^n \prod_{j=1}^{m} f(u_j). \tag{3}$$

Из (2) мы видим, что S однородно степени n по (w), а из (3) — что S однородно степени m по (v). Так как R обладает точно теми же свойствами однородности и делится на S, то $R = cS$ для некоторого целого c. Так как и R, и S содержат одночлен $v_0^m w_m^n$, встречающийся в них с коэффициентом 1, то $c = 1$, и наше предложение доказано.

Отметим, что три выражения, найденные выше для S, дают нам разложение на множители результанта R. Мы получаем также обратное утверждение к предложению 3.

Следствие. *Пусть f_a, g_b — многочлены с коэффициентами в некотором поле K, разлагающиеся на множители степени 1 в $K[X]$ и такие, что хотя бы один из старших коэффициентов a_0, $b_0 \neq 0$. Тогда $R(f_a, g_b) = 0$ в том и только в том случае, если f_a и g_b имеют общий корень.*

Доказательство. Пусть результант равен 0, и пусть для определенности $a_0 \neq 0$. Если

$$f_a = a_0 (X - \alpha_1) \ldots (X - \alpha_n),$$

— разложение f_a на множители, то имеет место гомоморфизм

$$\mathbf{Z}[v_0, t, w] \to K,$$

при котором $v_0 \mapsto a_0$, $t_i \mapsto \alpha_i$ и $w_j \mapsto b_j$ для всех i, j. Тогда

$$0 = R(f_a, g_b) = a_0^m \prod_{i=1}^{n} g_b(\alpha_i),$$

откуда следует, что хотя бы один из α_i является корнем многочлена g_b. Обратное уже было доказано.

Выведем еще одно соотношение для результанта в специальном случае. Пусть, как и выше,

$$f_v(X) = v_0X^n + \ldots + v_n = v_0(X - t_1) \ldots (X - t_n).$$

В силу (2) для производной f'_v многочлена f_v

$$R(f_v, f'_v) = v_0^{n-1} \prod_i f'(t_i). \tag{4}$$

Используя правило дифференцирования произведения, находим

$$f'_v(X) = \sum_i v_0(X - t_1) \ldots \widehat{(X - t_i)} \ldots (X - t_n),$$

$$f'_v(t_i) = v_0(t_i - t_1) \ldots \widehat{(t_i - t_i)} \ldots (t_i - t_n),$$

где крышка над членом указывает, что этот член должен быть опущен.

Мы называем дискриминантом многочлена f_v выражение

$$D(f_v) = D(v) = v_0^{2n-2} \prod_{i<j} (t_i - t_j)^2.$$

Предложение 5. Пусть f_v, как и выше, имеет алгебраически независимые коэффициенты над $\mathbf{Z}$. Тогда

$$R(f_v, f'_v) = v_0^{2n-1} \prod_{i \neq j} (t_i - t_j) = (-1)^{\binom{n}{2}} v_0 D(f_v). \tag{5}$$

Доказательство. Подставим выражение, полученное для $f'_v(t_i)$, в произведение (4). Утверждение следует немедленно.

Если мы подставим 1 вместо v_0, то найдем, что дискриминант, как мы его определили в предыдущем параграфе, совпадает с определенным здесь. В частности, получаем явную формулу для дискриминанта. Формулы в случае многочленов степени 2 и 3 приводятся в упражнениях.

УПРАЖНЕНИЯ

1. (а) Сформулировать и доказать аналог теоремы 8 для рациональных чисел.

(б) Сформулировать и доказать аналог теоремы 9 для положительных целых чисел.

2. Пусть f — многочлен от одной переменной над полем k, и пусть X, Y — две переменные. Показать, что в $k[X, Y]$ имеет место разложение в ряд Тейлора

$$f(X + Y) = f(X) + \sum_{i=1}^{n} \varphi_i(X) Y^i,$$

где $\varphi_i(X)$ — некоторые многочлены от X с коэффициентами в k. Если k имеет характеристику 0, то

$$\varphi_i(X) = \frac{D^i f(X)}{i!}.$$

3. Обобщить предыдущее упражнение на многочлены от нескольких переменных (ввести частные производные и показать, что для многочленов от нескольких переменных существует конечное разложение Тейлора).

4. (а) Показать, что многочлены X^4+1 и X^6+X^3+1 неприводимы над полем рациональных чисел.

(б) Показать, что многочлен степени 3 над полем либо неприводим, либо имеет корень в этом поле. Является ли многочлен X^3-5X^2+1 неприводимым над полем рациональных чисел?

(в) Показать, что многочлен от двух переменных X^2+Y^2-1 неприводим над полем рациональных чисел. Неприводим ли он над полем комплексных чисел?

5. Пусть $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ — многочлен с целыми коэффициентами, $a_0 \neq 0$. Показать, что если f имеет корень в поле рациональных чисел, то этот корень должен быть целым рациональным числом, делящим a_0. Обобщить это утверждение на любое факториальное кольцо и его поле частных.

6. (а) Пусть k — конечное поле из q элементов. Пусть $f(X_1, \ldots, X_n)$ — многочлен в $k[X]$ степени d, такой, что $f(0, \ldots, 0) = 0$. Элемент $(a_1, \ldots, a_n) \in k^{(n)}$, для которого $f(a) = 0$, называется нулем f. Показать, что если $n > d$, то f имеет по крайней мере еще один нуль в $k^{(n)}$. [*Указание*: предположить противное и сравнить степени редуцированных многочленов

$$1 - f(X)^{q-1}$$

и $\left(1 - X_1^{q-1}\right) \ldots \left(1 - X_n^{q-1}\right)$. Рассуждение принадлежит Шевалле.]

(б) Усилить предыдущий результат, доказав, что число N нулей многочлена f в $k^{(n)}$ сравнимо с нулем по mod q. Рассуждать следующим образом. Пусть i — целое число $\geqslant 0$. Показать, что

$$\sum_{x \in k} x^i = \begin{cases} q-1 = -1, & \text{если } q-1 \text{ делит } i, \\ 0 & \text{в противном случае.} \end{cases}$$

Обозначим предыдущую функцию от i через $\psi(i)$. Показать, что

$$N \equiv \sum_{x \in k^{(n)}} (1 - f(x)^{q-1})$$

и что для каждого набора $(i_1, \ldots, i_n)$ целых чисел $\geqslant 0$ будет

$$\sum_{x \in k^{(n)}} x_1^{i_1} \cdots x_n^{i_n} = \psi(i_1) \ldots \psi(i_n).$$

Показать, что оба члена в сумме для N дают 0 mod p. (Приведенное рассуждение принадлежит Варнингу.)

(в) Распространить теорему Шевалле на r многочленов $f_1, \ldots, f_r$ степеней $d_1, \ldots, d_r$ соответственно от n переменных. Показать, что если эти

многочлены не имеют постоянных членов и $n > \sum d_i$, то у них есть нетривиальный общий нуль.

(г) Показать, что произвольная функция $f\colon k^{(n)} \to k$ может быть представлена многочленом. (Как и прежде, k — конечное поле.)

7. Пусть A — коммутативное целостное кольцо и X — переменная над A. Пусть $a, b \in A$, причем a — единица в A. Показать, что отображение $X \mapsto aX + b$ продолжается и притом единственным образом до автоморфизма кольца $A[X]$, индуцирующего тождественное отображение на A. Каков обратный автоморфизм?

8. Показать, что любой автоморфизм кольца $A[X]$ имеет вид, указанный в упражнении 7.

9. Пусть A — коммутативное целостное кольцо, K — его поле частных и $K(X)$ — поле частных кольца $A[X]$ (или, что то же самое, кольца $K[X]$). Показать, что всякий автоморфизм поля $K(X)$, индуцирующий тождественное отображение на K, имеет вид

$$X \mapsto \frac{aX + b}{cX + d},$$

где $a, b, c, d \in K$ таковы, что $(aX + b)/(cX + d)$ не лежит в K, или, что эквивалентно, $ad - bc \neq 0$.

10. Показать, что дискриминант многочлена $aX^2 + bX + c$ равен $b^2 - 4ac$.

11. Показать, что дискриминант многочлена $f(X) = a_0X^3 + a_1X^2 + a_2X + a_3$ равен

$$a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3.$$

В частности, дискриминантом многочлена $f(X) = X^3 + bX + c$ будет $-4b^3 - 27c^2$.

12. Показать, что дискриминант многочлена обращается в нуль тогда и только тогда, когда многочлен имеет кратный корень. (Вы можете предполагать, что многочлен разлагается на множители степени 1 в некотором поле.)

13. Пусть w — некоторое комплексное число. Показать, что существует постоянная $c = c(w)$, для которой справедливо следующее. Пусть F, G — ненулевые многочлены от одной переменной с комплексными коэффициентами степеней d и d' соответственно и R — их результант. Тогда

$$|R| \leqslant c^{d+d'}\left[\frac{|F(w)|}{|F|} + \frac{|G(w)|}{|G|}\right]|F|^{d'}\,|G|^{d}\,(d+d')^{d+d'}.$$

(Мы обозначаем через $|F|$ максимум абсолютных значений коэффициентов многочлена F.)

14. Показать, что можно определить простейшие дроби для положительных рациональных чисел, т. е получить разложение, аналогичное разложению из теоремы 8. Показать, что группа $\mathbf{Q}/\mathbf{Z}$ изоморфна прямой сумме аддитивных групп $\mathbf{Z}[1/p]/\mathbf{Z}$, взятой по всем простым p. Обобщить на произвольное кольцо главных идеалов A. Если K — поле частных кольца A, то что представляет собой K/A?

15. Следующее упражнение несколько труднее предыдущих. Пусть m/n — рациональное число, представленное в виде отношения взаимно простых

целых чисел m, n. Назовем его *высотой* $H(m/n)$ максимум из $|m|$, $|n|$. Пусть

$$\varphi(X) = \frac{f(X)}{g(X)}$$

— элемент из $\mathbf{Q}(X)$, представленный в виде отношения двух взаимно простых многочленов f, g. Назовем *степенью* элемента φ максимум из $\deg f$, $\deg g$. Если число $a \in \mathbf{Q}$ таково, что $g(a) \neq 0$, то мы можем образовать $\varphi(a) = f(a)/g(a)$; в этом случае мы говорим, что функция φ определена в a. Пусть φ имеет степень d. Показать, что существуют две константы $c_1, c_2 > 0$, такие, что для всех рациональных чисел a, в которых φ определена, имеют место неравенства

$$c_1 H(a)^d \leqslant H(\varphi(a)) \leqslant c_2 H(a)^d.$$

[*Указание*: одно из неравенств тривиально. Для получения другого показать, что функция $H(x)^d/H(\varphi(x))$ ограничена.]