Глава 4

КОЛЬЦА МНОГОЧЛЕНОВ (продолжение)

§ 25. Результант. Исключение неизвестного. Дискриминант

Даны два многочлена:

$$f(x) = a_0x^k + a_1x^{k-1} + \ldots + a_k, \quad a_i \in P;$$

$$g(x) = b_0x^l + b_1x^{l-1} + \ldots + b_l, \quad b_j \in P.$$

При этом мы не предполагаем, что $a_0 \neq 0$ и $b_0 \neq 0$. Можно сформулировать следующий вопрос: существуют ли у них общие корни?

Мы уже знаем, что многочлены f и g тогда и только тогда обладают общим корнем в некотором расширении поля P, если они не являются взаимно простыми. Таким образом, вопрос о существовании общих корней у данных многочленов может быть решен применением к ним алгоритма Евклида.

25.1. Результант двух многочленов от одного неизвестного. Укажем другой метод, позволяющий ответить на поставленный вопрос.

О п р е д е л е н и е. *Результантом* многочленов f и g называется

определитель

$$\mathrm{Res}(f,g)=\begin{vmatrix} a_0 & a_1 & \dots & a_k & 0 & 0 & \dots & 0 \\ 0 & a_0 & \dots & a_{k-1} & a_k & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & a_0 & a_1 & \dots & a_k \\ b_0 & b_1 & \dots & b_l & 0 & 0 & \dots & 0 \\ 0 & b_0 & \dots & b_{l-1} & b_l & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & b_0 & b_1 & \dots & b_l \end{vmatrix}$$

порядка $k+l$.

Из свойств определителей следует равенство

$$\mathrm{Res}(g,f)=(-1)^{kl}\mathrm{Res}(f,g).$$

Целью настоящего параграфа является доказательство следующего утверждения

Т е о р е м а 1. *Пусть*

$$f(x)=a_0x^k+a_1x^{k-1}+\ldots+a_k=a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k),\quad a_0\neq 0;$$

$$g(x)=b_0x^l+b_1x^{l-1}+\ldots+b_l=b_0(x-\beta_1)(x-\beta_2)\ldots(x-\beta_l),\quad b_0\neq 0$$

– два многочлена из $P[x]$. *Тогда*

$$\mathrm{Res}(f,g)=a_0^l\,b_0^k\prod_{\substack{1\le i\le k\\ 1\le j\le l}}(\alpha_i-\beta_j).$$

Для доказательства нам потребуется

Л е м м а 1 (определитель Вандермонда). *Для любых элементов* $z_1,z_2,\ldots,z_n$, $n\ge 2$ *из поля* P *справедливо равенство*

$$\begin{vmatrix} z_1^{n-1} & z_2^{n-1} & \dots & z_n^{n-1} \\ z_1^{n-2} & z_2^{n-2} & \dots & z_n^{n-2} \\ \dots & \dots & \dots & \dots \\ z_1 & z_2 & \dots & z_n \\ 1 & 1 & \dots & 1 \end{vmatrix}=\prod_{1\le i<j\le n}(z_i-z_j).$$

Д о к а з а т е л ь с т в о проведем индукцией по n.

При $n = 2$ имеем

$$\begin{vmatrix} z_1 & z_2 \\ 1 & 1 \end{vmatrix} = z_1 - z_2.$$

Предположим, что формула справедлива при $n-1$, и рассмотрим определитель порядка n. Вычитаем из первой строки вторую, умноженную на z_n, затем из второй – третью, умноженную на z_n, и т. д., и наконец, из $(n-1)$-й строки вычитаем n-ю, умноженную на z_n. Получим:

$$\begin{vmatrix} z_1^{n-1} - z_n \cdot z_1^{n-2} & \dots & z_{n-1}^{n-1} - z_n \cdot z_{n-1}^{n-2} & 0 \\ z_1^{n-2} - z_n \cdot z_1^{n-3} & \dots & z_{n-1}^{n-2} - z_n \cdot z_{n-1}^{n-3} & 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & & & \\ z_1 - z_n & \dots & z_{n-1} - z_n & 0 \\ 1 & \dots & 1 & 1 \end{vmatrix}.$$

Разлагая этот определитель по последнему столбцу, приходим к определителю порядка $n-1$:

$$\begin{vmatrix} z_1^{n-1} - z_n \cdot z_1^{n-2} & \dots & z_{n-1}^{n-1} - z_n \cdot z_{n-1}^{n-2} \\ z_1^{n-2} - z_n \cdot z_1^{n-3} & \dots & z_{n-1}^{n-2} - z_n \cdot z_{n-1}^{n-3} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & & \\ z_1 - z_n & \dots & z_{n-1} - z_n \end{vmatrix}.$$

Вынося из первого столбца $(z_1 - z_n)$, из второго $(z_2 - z_n)$ и т. д., и наконец, из $(n-1)$-го $(z_{n-1} - z_n)$, получим:

$$(z_1 - z_n)(z_2 - z_n)\dots(z_{n-1} - z_n) \begin{vmatrix} z_1^{n-2} & z_2^{n-2} & \dots & z_{n-1}^{n-2} \\ z_1^{n-3} & z_2^{n-3} & \dots & z_{n-1}^{n-3} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & & & \\ z_1 & z_2 & \dots & z_{n-1} \\ 1 & 1 & \dots & 1 \end{vmatrix}.$$

Воспользовавшись предположением индукции, получим нужное равенство. Лемма доказана.

Следующая лемма легко устанавливается непосредственной проверкой.

Л е м м а 2 (формулы Виета). *Если*

$$x^n + a_1x^{n-1} + \ldots + a_n = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),$$

то

$a_1 = -(\alpha_1 + \alpha_2 + \ldots + \alpha_n)$,

$a_2 = \alpha_1\cdot\alpha_2 + \alpha_1\cdot\alpha_3 + \ldots + \alpha_1\cdot\alpha_n + \alpha_2\cdot\alpha_3 + \ldots + \alpha_{n-1}\cdot\alpha_n$,

.....

$a_i = (-1)^i \sum\limits_{1\le k_1<k_2<\ldots<k_i\le n} \alpha_{k_1}\alpha_{k_2}\ldots\alpha_{k_i}$,

.....

$a_n = (-1)^n\alpha_1\alpha_2\ldots\alpha_n$.

Д о к а з а т е л ь с т в о теоремы 1. Рассмотрим матрицу

$$P = \begin{pmatrix} a_0 & a_1 & \ldots & a_k & 0 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{k-1} & a_k & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_k \\ b_0 & b_1 & \ldots & b_l & 0 & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & b_{l-1} & b_l & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_l \end{pmatrix}$$

и матрицу

$$Q = \left(\begin{array}{cccc|cccc} \beta_1^{k+l-1} & \beta_2^{k+l-1} & \ldots & \beta_l^{k+l-1} & \alpha_1^{k+l-1} & \alpha_2^{k+l-1} & \ldots & \alpha_k^{k+l-1} \\ \beta_1^{k+l-2} & \beta_2^{k+l-2} & \ldots & \beta_l^{k+l-2} & \alpha_1^{k+l-2} & \alpha_2^{k+l-2} & \ldots & \alpha_k^{k+l-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta_1 & \beta_2 & \ldots & \beta_l & \alpha_1 & \alpha_2 & \ldots & \alpha_k \\ 1 & 1 & \ldots & 1 & 1 & 1 & \ldots & 1 \end{array}\right).$$

Найдем их произведение $P\cdot Q$. Заметим, что в матрице $P\cdot Q$ на месте $(1,1)$ будет стоять элемент

$a_0\beta_1^{k+l-1} + a_1\beta_1^{k+l-2} + \ldots + a_k\beta_1^{l-1} = \beta_1^{l-1}(a_0\beta_1^k + a_1\beta_1^{k-1} + \ldots + a_k) = \beta_1^{l-1}f(\beta_1)$;
на месте $(2,1)$ – элемент

$a_0\beta_1^{k+l-2} + a_1\beta_1^{k+l-3} + \ldots + a_k\beta_1^{l-1} = \beta_1^{l-2}f(\beta_1)$
и т. д. Наконец, на месте $(l,1)$ будет стоять элемент

$a_0\beta_1^k + a_1\beta_1^{k-1} + \ldots + a_k = f(\beta_1)$.
На месте $(l+1,1)$ будет стоять элемент

$b_0\beta_1^{k+l-1} + b_1\beta_1^{k+l-2} + \ldots + b_l\beta_1^{k-1} = \beta_1^{k-1}g(\beta_1) = 0$
и т. д.

Рассмотрим элементы, которые получаются при умножении $l+1$-го столбца матрицы Q на матрицу P. На месте $(1,l+1)$ будет стоять элемент

$a_0\alpha_1^{k+l-1} + a_1\alpha_1^{k+l-2} + \ldots + a_k\alpha_1^{l-1} = \alpha_1^{l-1}(a_0\alpha_1^k + a_1\alpha_1^{k-1} + \ldots + a_k) = \alpha_1^{l-1}f(\alpha_1) = 0$;
на месте $(l+1,l+1)$ – элемент

$b_0\alpha_1^{k+l-1} + b_1\alpha_1^{k+l-2} + \ldots + b_l\alpha_1^{k-1} = \alpha_1^{k-1}g(\alpha_1)$;
на месте $(l+k,l+1)$ будет стоять элемент

$b_0\alpha_1^l + b_1\alpha_1^{l-1} + \ldots + b_l = g(\alpha_1)$.

Вычисляя аналогичным образом другие элементы, получим:

$$P\cdot Q = \left(\begin{array}{ccc|ccc} \beta_1^{l-1}f(\beta_1) & \ldots & \beta_l^{l-1}f(\beta_l) & 0 & \ldots & 0 \\ \beta_1^{l-2}f(\beta_1) & \ldots & \beta_l^{l-2}f(\beta_l) & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ f(\beta_1) & \ldots & f(\beta_l) & 0 & \ldots & 0 \\ \hline 0 & \ldots & 0 & \alpha_1^{k-1}g(\alpha_1) & \ldots & \alpha_k^{k-1}g(\alpha_k) \\ 0 & \ldots & 0 & \alpha_1^{k-2}g(\alpha_1) & \ldots & \alpha_k^{k-2}g(\alpha_k) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & g(\alpha_1) & \ldots & g(\alpha_k) \end{array}\right).$$

Вычислим определители этих матриц:

$$\det P = \operatorname{Res}(f,g), \quad \det Q = \prod_{1\le i<j\le k}(\alpha_i-\alpha_j)\cdot\prod_{1\le r<s\le l}(\beta_r-\beta_s)\cdot\prod_{\substack{1\le r\le l\\ 1\le i\le k}}(\beta_r-\alpha_i),$$

$$\det(P\cdot Q)=\prod_{1\le r\le l} f(\beta_r)\cdot\prod_{1\le r<s\le l}(\beta_r-\beta_s)\cdot\prod_{1\le i\le k} g(\alpha_i)\cdot\prod_{1\le i<j\le k}(\alpha_i-\alpha_j)=$$

$$=\prod_{1\le i<j\le k}(\alpha_i-\alpha_j)\cdot\prod_{1\le r<s\le l}(\beta_r-\beta_s)\cdot a_0^l\prod_{\substack{1\le r\le l\\1\le i\le k}}(\beta_r-\alpha_i)\cdot b_0^k\prod_{\substack{1\le i\le k\\1\le r\le l}}(\alpha_i-\beta_r).$$

Учитывая, что

$$\det P\cdot\det Q=\det(P\cdot Q),$$

после сокращения, получим

$$\det P=a_0^l\,b_0^k\prod_{\substack{1\le i\le k\\1\le j\le l}}(\alpha_i-\beta_j).$$

Теорема доказана.

С л е д с т в и е. *Справедливо равенство*

$$\operatorname{Res}(f,g)=a_0^l\prod_{i=1}^{k} g(\alpha_i).$$

У п р а ж н е н и я. 1) Где нужно, чтобы a_0 и b_0 были отличны от нуля? 2) Почему выполненное сокращение законно?

25.2. Критерий совместности двух уравнений с одним неизвестным. Теперь мы готовы дать ответ на вопрос, сформулированный в начале параграфа.

Т е о р е м а 2. *Для многочленов $f,g\in P[x]$ равносильны следующие утверждения*:

1) $\operatorname{Res}(f,g)=0$;

2) *f и g имеют общий корень или $a_0=b_0=0$.*

Д о к а з а т е л ь с т в о разбивается на несколько случаев.

Случай 1. $a_0\neq 0$, $b_0\neq 0$. Сразу следует из теоремы 1.

Случай 2. $a_0=b_0=0$. Тогда целый столбик в определителе $\operatorname{Res}(f,g)$ равен нулю, а потому $\operatorname{Res}(f,g)=0$.

Случай 3. $a_0\neq 0$, $b_0=0$. Если $g(x)\equiv 0$, то $\operatorname{Res}(f,g)=0$, f и g имеют общий корень. Пусть $g(x)\not\equiv 0$, но $b_0=\ldots=b_{i-1}=0$, $b_i\neq 0$.

С другой стороны, для многочлена

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

найдем производную по формуле дифференцирования произведения:

$$f'(x) = a_0 \sum_{i=1}^{n} \prod_{\substack{j\neq i\\ 1\leq j\leq n}} (x-\alpha_j).$$

Подставив значение α_i, получим

$$f'(\alpha_i) = a_0 \prod_{\substack{j\neq i\\ 1\leq j\leq n}} (\alpha_i-\alpha_j).$$

Тогда

$$\operatorname{Res}(f,f') = a_0^{2n-1} \prod_{i=1}^{n} \prod_{\substack{j\neq i\\ 1\leq j\leq n}} (\alpha_i-\alpha_j) = a_0^{2n-2}(-1)^{C_n^2} a_0 \prod_{1\leq i<j\leq n} (\alpha_i-\alpha_j)^2 =$$

$$= (-1)^{C_n^2} a_0 \operatorname{Dis}(f).$$

Теорема доказана.

П р и м е р. Пусть $f(x) = ax^2 + bx + c$. Тогда $f' = 2ax + b$, и, вычисляя дискриминант, получим

$$\operatorname{Dis}(f) = (-1)^{C_2^2} \frac{1}{a} \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = b^2 - 4ac.$$

§ 26. Многочлены от нескольких переменных

26.1. Кольцо многочленов от нескольких переменных. *Многочленом над кольцом K от n переменных* $x_1, x_2, \dots, x_n$ называется выражение

$$f = f(x_1, x_2, \dots, x_n) = \sum_{k_1,k_2,\dots,k_n} a_{k_1k_2\dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}, \quad a_{k_1k_2\dots k_n} \in K,$$