Можно считать, следовательно, что ψ — многочлен от $\tau_1, \tau_2, \ldots, \tau_r$ над полем рациональных дробей

$$Q = P(x_1, x_2, \ldots, x_n).$$

Система $y_1, y_2, \ldots, y_r$ остается алгебраически независимой над полем Q: если бы для этой системы существовала алгебраическая зависимость с коэффициентами из Q, то, освобождаясь от знаменателей, мы получили бы алгебраическую зависимость в системе (4) против предположения. Опираясь на теорему единственности из предыдущего параграфа, мы получаем теперь, что система $\tau_1, \tau_2, \ldots, \tau_r$ также должна быть алгебраически независимой над полем Q, а поэтому все коэффициенты многочлена ψ равны нулю. Эти коэффициенты являются, однако, многочленами от $\sigma_1, \sigma_2, \ldots, \sigma_n$, а поэтому, снова на основании теоремы единственности для случая одной системы неизвестных (на этот раз системы $x_1, x_2, \ldots, x_n$), все коэффициенты этих последних многочленов сами равны нулю. Этим доказано, что в противоречие с предположением все коэффициенты многочлена φ должны быть равными нулю.

§ 54*. Результант. Исключение неизвестного. Дискриминант

Если дан многочлен $f(x_1, x_2, \ldots, x_n)$ из кольца $P[x_1, x_2, \ldots, x_n]$, то его *решением* называется такая система значений для неизвестных

$$x_1 = \alpha_1, \quad x_2 = \alpha_2, \ldots, \quad x_n = \alpha_n,$$

взятых в поле P или в некотором расширении $\bar{P}$ этого поля, которая обращает многочлен f в нуль:

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0.$$

Всякий многочлен f, степень которого больше нуля, обладает решениями: если неизвестное x_1 входит в запись этого многочлена, то в качестве $\alpha_2, \ldots, \alpha_n$ можно взять по существу произвольные элементы из поля P, лишь бы степень многочлена $f(x_1, \alpha_2, \ldots, \alpha_n)$ оставалась строго положительной, а затем, используя теорему о существовании корня (§ 49), взять такое расширение $\bar{P}$ поля P, в котором многочлен $f(x_1, \alpha_2, \ldots, \alpha_n)$ от одного неизвестного x_1 обладает корнем α_1. Мы видим вместе с тем, что свойство многочлена степени n от одного неизвестного обладать во всяком поле не более чем n корнями для многочленов от нескольких неизвестных перестает быть справедливым.

Если дано несколько многочленов от n неизвестных, то можно поставить вопрос о разыскании решений, общих для всех этих многочленов, т. е. решений той системы уравнений, которая получается в результате приравнивания заданных многочленов нулю. Частный случай этой задачи, а именно случай систем линейных уравнений,

уже был подвергнут во второй главе детальному рассмотрению. Однако для противоположного частного случая одного уравнения от одного неизвестного, но имеющего произвольную степень, мы не знаем о корнях ничего, кроме того, что они существуют в некотором расширении основного поля. Разыскание и изучение решений произвольной нелинейной системы уравнений от нескольких неизвестных является, понятно, еще более сложной задачей, выходящей, впрочем, за рамки нашего курса и составляющей предмет особой математической науки — алгебраической геометрии. Мы же здесь ограничимся лишь случаем системы двух уравнений произвольной степени от двух неизвестных и покажем, что этот случай может быть сведен к случаю одного уравнения от одного неизвестного.

Займемся сперва вопросом о существовании общих корней у двух многочленов от одного неизвестного. Пусть даны многочлены

$$\left.\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \\ g(x) &= b_0x^s + b_1x^{s-1} + \ldots + b_{s-1}x + b_s \end{aligned}\right\} \tag{1}$$

над полем P, причем $a_0 \neq 0$, $b_0 \neq 0$.

Из результатов предшествующей главы без труда вытекает, что *многочлены $f(x)$ и $g(x)$ 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.

Сейчас мы укажем другой метод для получения ответа на этот вопрос. Пусть $\overline{P}$ будет некоторое такое расширение поля P, в котором $f(x)$ имеет n корней $\alpha_1, \alpha_2, \ldots, \alpha_n$, а $g(x)$ имеет s корней $\beta_1, \beta_2, \ldots, \beta_s$; в качестве $\overline{P}$ можно взять поле разложения для произведения $f(x)g(x)$. Элемент

$$R(f, g) = a_0^s b_0^n \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j) \tag{2}$$

поля $\overline{P}$ называется *результантом* многочленов $f(x)$ и $g(x)$. Очевидно, что *$f(x)$ и $g(x)$ тогда и только тогда обладают в $\overline{P}$ общим корнем, если* $R(f, g) = 0$. Так как

$$g(x) = b_0 \prod_{j=1}^{s} (x - \beta_j)$$

и поэтому

$$g(\alpha_i) = b_0 \prod_{j=1}^{s} (\alpha_i - \beta_j),$$

то результант $R(f, g)$ может быть записан также в виде

$$R(f, g) = a_0^s \prod_{i=1}^{n} g(\alpha_i). \tag{3}$$

Многочлены $f(x)$ и $g(x)$ используются в определении результанта не симметричным образом. Действительно,

$$R(g, f) = b_0^n a_0^s \prod_{j=1}^{s} \prod_{i=1}^{n} (\beta_j - \alpha_i) = (-1)^{ns} R(f, g). \tag{4}$$

В соответствии с (3) $R(g, f)$ можно записать в виде

$$R(g, f) = b_0^n \prod_{j=1}^{s} f(\beta_j). \tag{5}$$

Выражение (2) для результанта требует знания корней многочленов $f(x)$ и $g(x)$ и поэтому практически бесполезно для решения вопроса о существовании у этих двух многочленов общего корня. Оказывается, однако, что *результант $R(f, g)$ может быть представлен в виде многочлена от коэффициентов $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s$ многочленов $f(x)$ и $g(x)$.*

Возможность такого представления легко вытекает из результатов предшествующего параграфа. В самом деле, формула (2) показывает, что результант $R(f, g)$ является симметрическим многочленом от двух систем неизвестных: системы $\alpha_1, \alpha_2, \ldots, \alpha_n$ и системы $\beta_1, \beta_2, \ldots, \beta_s$. Он представим поэтому, как доказано в конце предшествующего параграфа, в виде многочлена от элементарных симметрических многочленов по этим двум системам неизвестных, т. е., ввиду формул Вьета, в виде многочлена от частных $\frac{a_i}{a_0}$, $i = 1, 2, \ldots, n$, и $\frac{b_j}{b_0}$, $j = 1, 2, \ldots, s$; множитель $a_0^s b_0^n$, включенный в (2), освобождает полученное выражение от a_0 и b_0 в знаменателях. Впрочем, было бы затруднительным разыскивать выражение результанта через коэффициенты при помощи методов, изложенных в предшествующих параграфах, и мы воспользуемся иным приемом.

Выражение для результанта многочленов (1), которое мы найдем, будет годно для любой пары таких многочленов. Мы будем считать, точнее говоря, что система корней

$$\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_s \tag{6}$$

многочленов (1) является системой $n+s$ независимых неизвестных, т. е. системой $n+s$ элементов, алгебраически независимых над полем P в смысле § 51.

Мы получим выражение для результанта, которое, рассматриваемое как многочлен от неизвестных (6) (после замены по формулам Вьета коэффициентов через корни), будет равно правой части равенства (2), также рассматриваемой как многочлен от неизвестных (6).

Понимая равенство именно в смысле такого тождественного равенства относительно системы неизвестных (6), мы докажем, что

результант $R(f, g)$ *многочленов* (1) *равен следующему определителю порядка* $n+s$:

$$D=\begin{vmatrix} a_0 & a_1 & \dots & a_n & & & & \\ & a_0 & a_1 & \dots & a_n & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & a_0 & a_1 & \dots & a_n & \\ b_0 & b_1 & \dots & b_s & & & & \\ & b_0 & b_1 & \dots & b_s & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & b_0 & b_1 & \dots & b_s & \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} s \text{ строк} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ строк} \end{matrix} \tag{7}$$

(на свободных местах стоят нули). Строение этого определителя достаточно ясно; мы отметим лишь, что на его главной диагонали стоит s раз коэффициент a_0 и затем n раз коэффициент b_s.

Для доказательства нашего утверждения мы двумя способами вычислим произведение $a_0^s b_0^n DM$, где M есть следующий вспомогательный определитель порядка $n+s$:

$$M=\begin{vmatrix} \beta_1^{n+s-1} & \beta_2^{n+s-1} & \dots & \beta_s^{n+s-1} & \alpha_1^{n+s-1} & \alpha_2^{n+s-1} & \dots & \alpha_n^{n+s-1} \\ \beta_1^{n+s-2} & \beta_2^{n+s-2} & \dots & \beta_s^{n+s-2} & \alpha_1^{n+s-2} & \alpha_2^{n+s-2} & \dots & \alpha_n^{n+s-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \beta_1^2 & \beta_2^2 & \dots & \beta_s^2 & \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \beta_1 & \beta_2 & \dots & \beta_s & \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \end{vmatrix}.$$

M является определителем Вандермонда и поэтому равен, как указано в § 6, произведению разностей элементов его предпоследней строки, причем из всякого предшествующего элемента вычитается любой следующий элемент. Таким образом,

$$M=\prod_{1\leqslant i<j\leqslant s}(\beta_i-\beta_j)\cdot\prod_{j=1}^{s}\prod_{i=1}^{n}(\beta_j-\alpha_i)\cdot\prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)$$

и поэтому, ввиду (4),

$$a_0^s b_0^n DM=D\cdot R(g, f)\cdot\prod_{1\leqslant i<j\leqslant s}(\beta_i-\beta_j)\cdot\prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j). \tag{8}$$

Вычислим, с другой стороны, произведение DM на основании теоремы об определителе произведения матриц. Перемножая соответствующие матрицы и учитывая, что все α являются корнями

для $f(x)$, а все β — корнями для $g(x)$, мы получим:

$$DM = \begin{vmatrix} \beta_1^{s-1} f(\beta_1) & \beta_2^{s-1} f(\beta_2) & \dots & \beta_s^{s-1} f(\beta_s) & 0 & 0 & \dots & 0 \\ \beta_1^{s-2} f(\beta_1) & \beta_2^{s-2} f(\beta_2) & \dots & \beta_s^{s-2} f(\beta_s) & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \beta_1 f(\beta_1) & \beta_2 f(\beta_2) & \dots & \beta_s f(\beta_s) & 0 & 0 & \dots & 0 \\ f(\beta_1) & f(\beta_2) & \dots & f(\beta_s) & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \alpha_1^{n-1} g(\alpha_1) & \alpha_2^{n-1} g(\alpha_2) & \dots & \alpha_n^{n-1} g(\alpha_n) \\ 0 & 0 & \dots & 0 & \alpha_1^{n-2} g(\alpha_1) & \alpha_2^{n-2} g(\alpha_2) & \dots & \alpha_n^{n-2} g(\alpha_n) \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \alpha_1 g(\alpha_1) & \alpha_2 g(\alpha_2) & \dots & \alpha_n g(\alpha_n) \\ 0 & 0 & \dots & 0 & g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_n) \end{vmatrix}.$$

Применяя теорему Лапласа, вынося затем общие множители из столбцов определителей и вычисляя остающиеся определители как определители Вандермонда, мы получим:

$$a_0^s b_0^n DM = a_0^s b_0^n \prod_{j=1}^{s} f(\beta_j) \cdot \prod_{1 \leqslant i < j \leqslant s} (\beta_i - \beta_j) \cdot \prod_{i=1}^{n} g(\alpha_i) \cdot \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)$$

или, используя (3) и (5),

$$a_0^s b_0^n DM = R(f, g) R(g, f) \cdot \prod_{1 \leqslant i < j \leqslant s} (\beta_i - \beta_j) \cdot \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j). \quad (9)$$

Мы получаем, что правые части равенств (8) и (9), рассматриваемые как многочлены от неизвестных (6), равны между собой. Обе части полученного равенства можно сократить на общие множители, не равные тождественно нулю. Общий множитель $R(g, f)$ не равен нулю: так как $a_0 \neq 0$ и $b_0 \neq 0$ по условию, то достаточно подобрать для неизвестных (6) не равные друг другу значения (в основном поле или в некотором его расширении), чтобы из (4) получить отличное от нуля значение для многочлена $R(g, f)$. Так же доказывается, что и другие два общих множителя отличны от нуля. Сокращая на все эти общие множители, мы приходим к равенству

$$R(f, g) = D, \quad (10)$$

которое и требовалось доказать.

Откажемся теперь от требования, чтобы старшие коэффициенты многочленов (1) были отличны от нуля[1]). Об истинных степенях этих многочленов, можно, следова-

[1]) Этот временный отказ от того условия о старшем коэффициенте многочлена, которому мы следовали до сих пор, обусловлен дальнейшими приложениями: мы хотим рассматривать системы многочленов от двух неизвестных и будем одно из этих неизвестных относить в коэффициенты. Старший коэффициент может, следовательно, обратиться в нуль при частных значениях этого неизвестного.

тельно, лишь утверждать, что они не больше их «формальных» степеней n и, соответственно, s. Выражение (2) для результанта не имеет теперь смысла, так как рассматриваемые многочлены имеют, возможно, меньше корней, чем n или s. С другой стороны, определитель (7) и теперь может быть написан, и так как уже доказано, что при $a_0 \neq 0$, $b_0 \neq 0$ этот определитель равен результанту, то и в нашем общем случае назовем его *результантом* многочленов $f(x)$ и $g(x)$ и обозначим через $R(f, g)$.

Теперь уже нельзя, однако, рассчитывать на то, что равенство результанта нулю равносильно существованию у наших многочленов общего корня. Действительно, если $a_0 = 0$ и $b_0 = 0$, то $R(f, g) = 0$ независимо от того, обладают ли многочлены f и g общими корнями или нет. Оказывается, однако, что этот случай будет единственным, когда из равенства результанта нулю нельзя вывести заключение о существовании у данных многочленов общих корней[1]). Именно, справедлива следующая теорема:

Если даны многочлены (1) *с произвольными старшими коэффициентами, то результант* (7) *этих многочленов тогда и только тогда равен нулю, если эти многочлены обладают общим корнем или же если их старшие коэффициенты оба равны нулю.*

Доказательство. Случай $a_0 \neq 0$, $b_0 \neq 0$ уже рассматривался выше, а случай $a_0 = b_0 = 0$ предусмотрен в формулировке теоремы. Нам остается рассмотреть случай, когда один из старших коэффициентов многочленов (1), например a_0, отличен от нуля, а b_0 равно нулю.

Если $b_i = 0$ для всех i, $i = 0, 1, \ldots, s$, то $R(f, g) = 0$, так как определитель (7) содержит нулевые строки. В этом случае, однако, многочлен $g(x)$ равен нулю тождественно и поэтому имеет общие корни с $f(x)$. Если же

$$b_0 = b_1 = \ldots = b_{k-1} = 0, \quad \text{но} \quad b_k \neq 0, \quad k \leqslant s,$$

и если

$$\bar{g}(x) = b_k x^{s-k} + b_{k+1} x^{s-k-1} + \ldots + b_{s-1} x + b_s,$$

то, заменяя в определителе (7) элементы $b_0, b_1, \ldots, b_{k-1}$ нулями и применяя теорему Лапласа, мы придем, очевидно, к равенству

$$R(f, g) = a_0^k R(f, \bar{g}). \tag{11}$$

Так как, однако, старшие коэффициенты обоих многочленов f и $\bar{g}$ отличны от нуля, то, по доказанному выше, равенство $R(f, \bar{g}) = 0$ необходимо и достаточно для существования общего корня у многочленов f и $\bar{g}$. С другой стороны, по (11), равенства $R(f, g) = 0$ и $R(f, \bar{g}) = 0$ равносильны, а так как многочлены g и $\bar{g}$ имеют,

---

[1]) Определитель (7) равен нулю, конечно, и при $a_n = b_s = 0$. В этом случае, однако, многочлены (1) имеют общий корень 0.

понятно, одинаковые корни, то мы получаем, что и в рассматриваемом случае равенство нулю результанта $R(f, g)$ равносильно существованию общего корня у многочленов $f(x)$ и $g(x)$. Этим теорема доказана.

Найдем результант двух квадратных многочленов

$$f(x)=a_0x^2+a_1x+a_2, \quad g(x)=b_0x^2+b_1x+b_2.$$

По (7)

$$R(f, g)=\begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{vmatrix},$$

или, вычисляя определитель разложением по первой и третьей строкам,

$$R(f, g)=(a_0b_2-a_2b_0)^2-(a_0b_1-a_1b_0)(a_1b_2-a_2b_1). \tag{12}$$

Так, если даны многочлены

$$f(x)=x^2-6x+2, \quad g(x)=x^2+x+5,$$

то, по (12), $R(f, g)=233$, и потому эти многочлены не имеют общих корней. Если же даны многочлены

$$f(x)=x^2-4x-5, \quad g(x)=x^2-7x+10,$$

то $R(f, g)=0$, т. е. эти многочлены обладают общим корнем; этим корнем является число 5.

Исключение неизвестного из системы двух уравнений с двумя неизвестными. Пусть даны два многочлена f и g от двух неизвестных x и y с коэффициентами из некоторого поля P. Мы запишем эти многочлены по убывающим степеням неизвестного x:

$$\left.\begin{aligned} f(x, y)&=a_0(y)x^k+a_1(y)x^{k-1}+\ldots+a_{k-1}(y)x+a_k(y), \\ g(x, y)&=b_0(y)x^l+b_1(y)x^{l-1}+\ldots+b_{l-1}(y)x+b_l(y); \end{aligned}\right\} \tag{13}$$

коэффициенты будут многочленами из кольца $P[y]$. Найдем результант многочленов f и g, рассматриваемых как многочлены от x, и обозначим его через $R_x(f, g)$; он будет, ввиду (7), многочленом от одного неизвестного y с коэффициентами из поля P:

$$R_x(f, g)=F(y). \tag{14}$$

Пусть система многочленов (13) обладает в некотором расширении поля P общим решением $x=\alpha$, $y=\beta$. Подставляя в (13) вместо y значение β, мы получим два многочлена $f(x, \beta)$ и $g(x, \beta)$ от одного неизвестного x. Эти многочлены обладают общим корнем α, а поэтому их результант, равный, ввиду (14), $F(\beta)$, должен быть равным нулю, т. е. β *должно быть корнем результанта* $R_x(f, g)$. Обратно, если результант $R_x(f, g)$ многочленов (13) обладает корнем β, то результант многочленов $f(x, \beta)$ и $g(x, \beta)$ равен нулю, т. е. *либо*

эти многочлены обладают общим корнем, либо же оба их старших коэффициента равны нулю,

$$a_0(\beta) = b_0(\beta) = 0.$$

Этим путем разыскание общих решений системы многочленов (13) сведено к разысканию корней одного многочлена (14) от одного неизвестного y, т. е., как принято говорить, ***неизвестное x исключено из системы многочленов*** (13).

Следующая теорема отвечает на вопрос о степени того многочлена, который мы получаем после исключения одного неизвестного из системы двух многочленов с двумя неизвестными:

Если многочлены $f(x, y)$ и $g(x, y)$ имеют по совокупности неизвестных соответственно степени n и s, то степень многочлена $R_x(f, g)$ по неизвестному y не больше произведения ns, если, конечно, этот многочлен не равен нулю тождественно.

Прежде всего, если мы рассматриваем два многочлена от одного неизвестного со старшими коэффициентами, равными единице, то, по (2), их результант $R(f, g)$ является однородным многочленом от $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_s$ степени ns. Отсюда следует, что если в выражение результанта через коэффициенты $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_s$ входит член

$$a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} b_1^{l_1} b_2^{l_2} \ldots b_s^{l_s}$$

и если *весом* этого члена будет названо число

$$k_1 + 2k_2 + \ldots + nk_n + l_1 + 2l_2 + \ldots + sl_s,$$

то *все члены выражения $R(f, g)$ через коэффициенты имеют один и тот же вес, равный ns.* Это утверждение справедливо и в общем случае, для членов результанта (7), если *весом* члена $a_0^{k_0} a_1^{k_1} \ldots a_n^{k_n} b_0^{l_0} b_1^{l_1} \ldots b_s^{l_s}$ будет названо число

$$0 \cdot k_0 + 1 \cdot k_1 + \ldots + nk_n + 0 \cdot l_0 + 1 \cdot l_1 + \ldots + sl_s. \tag{15}$$

Действительно, заменяя в членах определителя (7) множители a_0 и b_0 единицей, мы приходим к уже рассмотренному случаю, однако показатели при этих множителях входят в (15) с коэффициентами 0.

Запишем теперь многочлены f и g в следующем виде:

$$f(x, y) = a_0(y) x^n + a_1(y) x^{n-1} + \ldots + a_n(y),$$
$$g(x, y) = b_0(y) x^s + b_1(y) x^{s-1} + \ldots + b_s(y).$$

Так как n есть степень $f(x, y)$ по совокупности неизвестных, то степень коэффициента $a_r(y)$, $r = 0, 1, 2, \ldots, n$, не может превосходить его индекс r; это же верно и для $b_r(y)$. Отсюда следует, что степень каждого члена результанта $R_x(f, g)$ не больше веса этого члена, т. е. она не больше числа ns, что и требовалось доказать.

Примеры.

1. Найти общие решения системы многочленов

$$f(x, y) = x^2y + 3xy + 2y + 3,$$
$$g(x, y) = 2xy - 2x + 2y + 3.$$

Исключим из этой системы неизвестное x, для чего перепишем ее в виде

$$\left.\begin{aligned} f(x, y) &= y\cdot x^2+(3y)\cdot x+(2y+3), \\ g(x, y) &= (2y-2)\,x+(2y+3); \end{aligned}\right\} \tag{16}$$

тогда

$$R_x(f, g)=\begin{vmatrix} y & 3y & 2y+3 \\ 2y-2 & 2y+3 & 0 \\ 0 & 2y-2 & 2y+3 \end{vmatrix}=2y^2+11y+12.$$

Корнями результанта будут числа $\beta_1=-4$, $\beta_2=-\frac{3}{2}$. При этих значениях неизвестного y старшие коэффициенты многочленов (16) не обращаются в нуль, поэтому каждое из них вместе с некоторым значением для x составляет решение заданной системы многочленов. Многочлены

$$f(x, -4)=-4x^2-12x-5,$$
$$g(x, -4)=-10x-5$$

обладают общим корнем $\alpha_1=-\frac{1}{2}$. Многочлены

$$f\left(x, -\frac{3}{2}\right)=-\frac{3}{2}x^2-\frac{9}{2}x,$$
$$g\left(x, -\frac{3}{2}\right)=-5x$$

имеют общий корень $\alpha_2=0$. Таким образом, заданная система многочленов имеет два решения:

$$\alpha_1=-\frac{1}{2},\quad \beta_1=-4 \quad \text{и} \quad \alpha_2=0,\quad \beta_2=-\frac{3}{2}.$$

2. Исключить одно неизвестное из системы многочленов

$$f(x, y)=2x^3y-xy^2+x+5,$$
$$g(x, y)=x^2y^2+2xy^2-5y+1.$$

Так как оба многочлена имеют по неизвестному y степень 2, тогда как у одного из них по неизвестному x степень 3, то целесообразно исключить y. Перепишем систему в виде

$$\left.\begin{aligned} f(x, y) &= (-x)\cdot y^2+(2x^3)\cdot y+(x+5), \\ g(x, y) &= (x^2+2x)\,y^2-5y+1 \end{aligned}\right\} \tag{17}$$

и найдем ее результант, применяя формулу (12):

$$\begin{aligned} R_y(f, g) &= [(-x)\cdot 1-(x+5)(x^2+2x)]^2- \\ &\quad -[(-x)(-5)-2x^3(x^2+2x)]\,[2x^3\cdot 1-(x+5)(-5)]= \\ &= 4x^8+8x^7+11x^6+84x^5+161x^4+154x^3+96x^2-125x. \end{aligned}$$

Одним из корней результанта является 0. Однако при этом значении неизвестного x оба старших коэффициента многочленов (17) обращаются в нуль, причем, как легко видеть, многочлены $f(0, y)$ и $g(0, y)$ не имеют общих корней. У нас нет способа найти другие корни результанта. Можно утверждать лишь, что если бы мы их нашли (например, в поле разложения для $R_y(f, g)$), то ни один из них не обращал бы в нуль оба старших коэффициента многочленов (17) и поэтому каждый из этих корней вместе с некоторым значением для y (одним или даже несколькими) составлял бы решение заданной системы многочленов.

Существуют методы, позволяющие последовательно исключать неизвестные и из систем с произвольным числом многочленов и неизвестных. Эти методы, однако, слишком громоздки и поэтому не могут быть включены в наш курс.

Дискриминант. По аналогии с вопросом, который привел нас к понятию результанта, можно поставить вопрос об условиях, при которых многочлен $f(x)$ степени n из кольца $P[x]$ обладает кратными корнями. Пусть

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n, \quad a_0\neq 0,$$

и пусть в некотором расширении поля P этот многочлен имеет корни $\alpha_1, \alpha_2, \ldots, \alpha_n$. Очевидно, что *среди этих корней тогда и только тогда будут равные, если равно нулю произведение*

$$\begin{aligned}\Delta=(\alpha_2-\alpha_1)(\alpha_3-\alpha_1)\ \ldots\ (\alpha_n-\alpha_1)\times\\ \times(\alpha_3-\alpha_2)(\alpha_4-\alpha_2)\ \ldots\ (\alpha_n-\alpha_2)\times\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \times(\alpha_n-\alpha_{n-1})=\prod_{n\geqslant i>j\geqslant 1}(\alpha_i-\alpha_j)\end{aligned}$$

или, что то же, если равно нулю произведение

$$D=a_0^{2n-2}\prod_{n\geqslant i>j\geqslant 1}(\alpha_i-\alpha_j)^2,$$

называемое *дискриминантом* многочлена $f(x)$.

В отличие от произведения Δ, могущего менять знак при перестановке корней, дискриминант D симметричен относительно $\alpha_1, \alpha_2, \ldots, \alpha_n$ и поэтому может быть выражен через коэффициенты многочлена $f(x)$. Для разыскания этого выражения в предположении, что поле P имеет характеристику нуль, можно воспользоваться связью, существующей между дискриминантом многочлена $f(x)$ и результантом этого многочлена и его производной. Наличие такой связи естественно ожидать: мы знаем из § 49, что многочлен тогда и только тогда обладает кратными корнями, если у него есть общие корни с производной $f'(x)$, а поэтому тогда и только тогда $D=0$, если $R(f, f')=0$.

По формуле (3) настоящего параграфа

$$R(f, f')=a_0^{n-1}\prod_{i=1}^{n}f'(\alpha_i).$$

Дифференцируя равенство

$$f(x)=a_0\prod_{k=1}^{n}(x-\alpha_k),$$

мы получаем:

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

После подстановки сюда α_i вместо x все слагаемые, кроме i-го, обращаются в нуль и поэтому

$$f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j),$$

откуда

$$R(f, f') = a_0^{n-1} \cdot a_0^n \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j).$$

В это произведение для любых i и j, $i > j$, входят два множителя: $\alpha_i - \alpha_j$ и $\alpha_j - \alpha_i$. Их произведение равно $(-1) \cdot (\alpha_i - \alpha_j)^2$, а так как существует $\frac{n(n-1)}{2}$ пар индексов i, j, удовлетворяющих неравенствам $n \geqslant i > j \geqslant 1$, то

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_0^{2n-1} \prod_{n \geqslant i > j \geqslant 1} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_0 D.$$

Пример. Найдем дискриминант квадратного трехчлена

$$f(x) = ax^2 + bx + c.$$

Так как $f'(x) = 2ax + b$, то

$$R(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a(-b^2 + 4ac).$$

В нашем случае $\frac{n(n-1)}{2} = 1$ и поэтому

$$D = -a^{-1} R(f, f') = b^2 - 4ac.$$

Это совпадает с тем, что в школьной алгебре называют обычно дискриминантом квадратного уравнения.

Другой способ разыскания дискриминанта состоит в следующем. Составим определитель Вандермонда из степеней корней $\alpha_1, \alpha_2, \ldots, \alpha_n$. Как доказано в § 6,

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{n \geqslant i > j \geqslant 1} (\alpha_i - \alpha_j) = \Delta,$$

а поэтому дискриминант равен квадрату этого определителя, умножённому на a_0^{2n-2}. Умножая этот определитель на его транспониро-

ванный по правилу умножения матриц и вспоминая определенные в предыдущем параграфе степенные суммы, мы получим:

$$D = a_0^{2n-2} \begin{vmatrix} n & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{vmatrix}, \tag{18}$$

где s_k есть сумма k-х степеней корней $\alpha_1, \alpha_2, \dots, \alpha_n$.

Пример. Найдем дискриминант кубичного многочлена $f(x) = x^3 + ax^2 + bx + c$. По (18)

$$D = \begin{vmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}.$$

Как мы знаем из предыдущего параграфа,

$$s_1 = \sigma_1 = -a,$$
$$s_2 = \sigma_1^2 - 2\sigma_2 = a^2 - 2b,$$
$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = -a^3 + 3ab - 3c.$$

Пользуясь формулой Ньютона, мы найдем также, ввиду $\sigma_4 = 0$, что

$$s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 = a^4 - 4a^2b + 4ac + 2b^2.$$

Отсюда

$$D = 3s_2s_4 + 2s_1s_2s_3 - s_2^3 - s_1^2s_4 - 3s_3^2 =$$
$$= a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2. \tag{19}$$

В частности, при $a = 0$, т. е. для неполного кубичного многочлена, мы получаем

$$D = -4b^3 - 27c^2$$

в полном соответствии с тем, что было сказано в § 38.

§ 55*. Второе доказательство основной теоремы алгебры комплексных чисел

Доказательство основной теоремы, приведенное в § 23, было совершенно неалгебраическим. Мы хотим изложить сейчас другое доказательство, использующее большой алгебраический аппарат — так, в нем существенно используется основная теорема о симметрических многочленах (§ 52), а также теорема о существовании поля разложения для всякого многочлена (§ 49),— в то время как неалгебраическая часть этого доказательства является минимальной и сведена к одному весьма простому утверждению.

Заметим сначала, что в § 23 доказана лемма о модуле старшего члена многочлена. Считая коэффициенты многочлена $f(x)$ действи-