Г л а в а 3

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

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

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* $z_1, z_2, \ldots, z_n$, $n \geq 2$, *из поля* P *справедливо равенство*

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

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

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

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

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

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

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

Воспользовавшись предположением индукции, получим нужное равенство. Лемма доказана.

Следующая лемма легко устанавливается непосредственной проверкой

Л е м м а 2 (формулы Виета). *Если*

$$x^n + a_1 x^{n-1} + \dots + a_n = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n),$$

то

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

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

.....

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

.....

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

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

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

и матрицу

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

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 $(2,1)$ будет стоять 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 $(l+1, l+1)$ будет стоять 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

$$P\cdot Q=\left(\begin{array}{cccc|cccc} \beta_1^{l-1}f(\beta_1) & \beta_2^{l-1}f(\beta_2) & \dots & \beta_l^{l-1}f(\beta_l) & 0 & 0 & \dots & 0 \\ \beta_1^{l-2}f(\beta_1) & \beta_2^{l-2}f(\beta_2) & \dots & \beta_l^{l-2}f(\beta_l) & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ f(\beta_1) & f(\beta_2) & \dots & f(\beta_l) & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & \dots & 0 & \alpha_1^{k-1}g(\alpha_1) & \alpha_2^{k-1}g(\alpha_2) & \dots & \alpha_k^{k-1}g(\alpha_k) \\ 0 & 0 & \dots & 0 & \alpha_1^{k-2}g(\alpha_1) & \alpha_2^{k-2}g(\alpha_2) & \dots & \alpha_k^{k-2}g(\alpha_k) \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_k) \end{array}\right).$$

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

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

из этих равенств 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 можно сократить?

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

$$\operatorname{Res}(f, g) = \begin{vmatrix} a_0 & a_1 & \ldots & a_k & 0 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{k-1} & a_k & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_k \\ 0 & \ldots & 0 & b_i & \ldots & b_l & \ldots & 0 \\ 0 & \ldots & 0 & 0 & b_i & \ldots & b_l \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 & b_i & \ldots & b_l \end{vmatrix} = a_0^i \operatorname{Res}(f, \overline{g}),$$

где $\overline{g}(x) = b_i x^{l-i} + \ldots + b_l$. Тогда

$$\operatorname{Res}(f, g) = 0 \Leftrightarrow \operatorname{Res}(f, \overline{g}) = 0.$$

По теореме 1 равенство $\operatorname{Res}(f, \overline{g}) = 0$ равносильно тому, что f и $\overline{g}$ имеют общий корень, а это равносильно тому, что f и g имеют общий корень.

Случай 4. $a_0 = 0$, $b_0 \neq 0$. Разбирается аналогично случаю 3. Теорема доказана.

25.3. Исключение неизвестных. Рассмотрим следующую систему алгебраических уравнений:

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0, \\ f_2(x_1, x_2, \ldots, x_n) = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_m(x_1, x_2, \ldots, x_n) = 0. \end{cases}$$

где $f_i \in P[x_1, x_2, \ldots, x_n]$. Для ее решения можно попробовать применить метод исключения неизвестных, используемый для решения систем линейных уравнений, т. е. исключить вначале одну неизвестную получив систему от меньшего числа неизвестных, затем вторую и т. д. Проделаем это для случая системы двух уравнений с двумя неизвестными.

Пусть мы имеем систему двух уравнений от двух неизвестных:

$$\begin{cases} f(x,y) = a_0(y)x^k + a_1(y)x^{k-1} + \ldots + a_k(y) = 0, \\ g(x,y) = b_0(y)x^l + b_1(y)x^{l-1} + \ldots + b_l(y) = 0. \end{cases} \tag{1}$$

Допустим, что мы умеем решать уравнения с одним неизвестным произвольной степени. Надо свести нашу систему к уравнению от одной неизвестной. Рассмотрим

$$\mathrm{Res}_x(f,g) = P(y)$$

т. е рассматривая $f(x,y)$ и $g(x,y)$ как многочлены от x и вычисляя результант, получим многочлен $F(y)$ от переменной y. Если (α,β) – решение системы (1), т. е. общий корень $f(x,y)$ и $g(x,y)$, то $F(\beta) = 0$. Подставив это значение в систему (1), получим два многочлена от одной неизвестных. Мы уже умеем определять: имеют ли они общий корни. Заметим, что среди пар (α,β) существуют «лишние». Это такие β, которые обращают главные члены в нуль.

25.4. Дискриминант. Для многочлена $f \in P[x]$ естественно сформулировать такой вопрос: когда f имеет кратные корни? Алгоритмический ответ ясен. Надо найти наибольший общий делитель многочлена f и его производной f'. Если он является многочленом не нулевой степени, то f имеет кратные корни. Как найти явный ответ?

О п р е д е л е н и е. *Дискриминантом* многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a^n = a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$$

называется элемент

$$\mathrm{Dis}(f) = a_0^{2n-2} \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2.$$

Из этого определения видим, что если $a_0 \neq 0$, то дискриминант равен нулю тогда и только тогда, когда многочлен имеет кратные корни. Но, чтобы вычислить дискриминант, используя это определение, мы должны знать корни. Следующая теорема позволяет вычислить дискриминант по коэффициентам многочлена.

Т е о р е м а 3. *Справедливо равенство*

$$\mathrm{Dis}(f) = (-1)^{C_n^2}\frac{1}{a_0}\mathrm{Res}(f,f'), \quad C_n^m = \frac{n!}{m!(n-m)!}.$$

Д о к а з а т е л ь с т в о. Пусть $\beta_1,\beta_2,\ldots,\beta_{n-1}$ – корни производной f', т. е.

$$f'(x) = na_0(x-\beta_1)(x-\beta_2)\ldots(x-\beta_{n-1}).$$

Тогда по теореме 1 имеем

$$\operatorname{Res}(f, f') = a_0^{n-1}(na_0)^n \prod_{\substack{1\le i\le n\\ 1\le j\le n-1}} (\alpha_i - \beta_j) = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i).$$

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:

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

Подставив значение α_i, получим

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

Тогда

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

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

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

в котором лишь конечное число коэффициентов $a_{k_1k_2\ldots k_n}$ отлично от нуля. *Степенью многочлена* f называется число

$$\max_{k_1,k_2,\ldots,k_n}(k_1+k_2+\ldots+k_n),$$

где максимум берется по всем наборам $k_1,k_2,\ldots,k_n$ для которых $a_{k_1k_2\ldots k_n}\neq 0$. На множестве многочленов естественным образом определяется сумма:

$$\sum_{k_1,k_2,\ldots,k_n} a_{k_1k_2\ldots k_n}x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}+\sum_{k_1,k_2,\ldots,k_n} b_{k_1k_2\ldots k_n}x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}=$$
$$=\sum_{k_1,k_2,\ldots,k_n}(a_{k_1k_2\ldots k_n}+b_{k_1k_2\ldots k_n})x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n},$$

и произведение

$$\sum_{k_1,k_2,\ldots,k_n} a_{k_1k_2\ldots k_n}x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}\cdot\sum_{l_1,l_2,\ldots,l_n} b_{l_1l_2\ldots l_n}x_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}=$$
$$=\sum_{m_1,m_2,\ldots,m_n} c_{m_1m_2\ldots m_n}x_1^{m_1}x_2^{m_2}\ldots x_n^{m_n},$$

где

$$c_{m_1m_2\ldots m_n}=\sum_{k_1+l_1=m_1,\ldots,k_n+l_n=m_n} a_{k_1k_2\ldots k_n}b_{l_1l_2\ldots l_n}.$$

Множество многочленов над кольцом K от переменных $x_1,x_2,\ldots,x_n$ будем обозначать $K[x_1,x_2,\ldots,x_n]$.

Т е о р е м а 1. *Если K – коммутативное кольцо без делителей нуля с единицей, то $K[x_1,x_2,\ldots,x_n]$ – коммутативное кольцо без делителей нуля с единицей.*

Д о к а з а т е л ь с т в о проведем индукцией по n. При $n=1$ теорема доказана ранее.

Пусть $n>1$. Рассмотрим отображение

$$K[x_1,x_2,\ldots,x_n]\longrightarrow K[x_1,x_2,\ldots,x_{n-1}][x_n],$$

которое сопоставляет многочлену $f(x_1,x_2,\ldots,x_n)$ его представление в виде многочлена от одной переменной x_n с коэффициентами из $K[x_1,x_2,\ldots,x_{n-1}]$. Это отображение является изоморфизмом, т. е. $K[x_1,x_2,\ldots,x_n]\simeq K[x_1,x_2,\ldots,x_{n-1}][x_n]$. По предположению индукции $K[x_1,x_2,\ldots,x_{n-1}]$ – коммутативное кольцо, без делителей нуля с единицей. По доказанной теореме о многочленах от одной переменной заключаем, что $K[x_1,x_2,\ldots,x_n]$ – коммутативное кольцо, без делителей нуля с единицей. Теорема доказана.

П р и м е р. Пусть K – коммутативное кольцо с единицей, P – его подполе, $\alpha_1, \alpha_2, \ldots, \alpha_n$ – некоторые элементы из K. Пусть L – подкольцо, порожденное P и $\alpha_1, \alpha_2, \ldots, \alpha_n$. Тогда

$$L = \{f(\alpha_1, \alpha_2, \ldots, \alpha_n) \mid f \in P[x_1, x_2, \ldots, x_n]\}.$$

Действительно, включение $\supseteq$ очевидно. Чтобы проверить включение $\subseteq$, достаточно убедиться, что множество элементов вида

$$\sum_{k_1,k_2,\ldots,k_n} a_{k_1k_2\ldots k_n}\alpha_1^{k_1}\alpha_2^{k_2}\ldots\alpha_n^{k_n}, \quad a_{k_1k_2\ldots k_n} \in P,$$

образуют подкольцо, которое содержит P и $\alpha_1, \alpha_2, \ldots, \alpha_n$, а потому содержится в L.

В связи с этим примером дадим такое

О п р е д е л е н и е. Элементы $\alpha_1, \alpha_2, \ldots, \alpha_n$ из K называются *алгебраически независимыми над* P, если каждый элемент из L имеет единственную запись $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Таким образом, элементы $\alpha_1, \alpha_2, \ldots, \alpha_n$ алгебраически независимы, если любой элемент

$$\sum_{k_1,k_2,\ldots,k_n} a_{k_1k_2\ldots k_n}\alpha_1^{k_1}\alpha_2^{k_2}\ldots\alpha_n^{k_n}$$

имеет единственную запись или, что равносильно, 0 записывается единственным образом. Действительно, если $\beta = f_1(\alpha_1, \alpha_2, \ldots, \alpha_n) = f_2(\alpha_1, \alpha_2, \ldots, \alpha_n)$, то $0 = (f_1 - f_2)(\alpha_1, \alpha_2, \ldots, \alpha_n)$, т. е 0 записывается двумя способами. Иными словами, элементы $\alpha_1, \alpha_2, \ldots, \alpha_n$ алгебраически независимы над P, если n–ка $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ не является корнем никакого многочлена из $P[x_1, x_2, \ldots, x_n]$.

У п р а ж н е н и е. Если $\alpha_1, \alpha_2, \ldots, \alpha_n$ алгебраически независимы над P, то отображение

$$P[x_1, x_2, \ldots, x_n] \longrightarrow L$$

по правилу $f(x_1, x_2, \ldots, x_n) \longmapsto f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ является изоморфизмом. Таким образом $L \simeq P[x_1, x_2, \ldots, x_n]$.

При $n = 1$ элемент α алгебраически зависимый над P называется *алгебраическим над* P; алгебраически независимый элемент называется *трансцендентным над* P.

26.2. Словарное упорядочивание многочленов. Если мы рассматриваем многочлен

$$f(x_1, x_2, x_3) = x_1^3x_2 + x_1x_2x_3^2 + x_3^4,$$

то неизвестно, какой коэффициент назвать старшим коэффициентом. Введем линейный порядок на одночленах.

О п р е д е л е н и е. Говорим, что одночлен $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ *выше* одночлена $a'x_1^{k'_1}x_2^{k'_2}\dots x_n^{k'_n}$, если $k_1 = k'_1$, $k_2 = k'_2$, $\dots$, $k_{i-1} = k'_{i-1}$, но $k_i > k'_i$.

Высший одночлен в теории многочленов от нескольких переменных играет ту же роль, что и старший коэффициент в теории многочленов от одной переменной.

Л е м м а. *Для любых многочленов f и g из $K[x_1, x_2, \dots, x_n]$ высший член произведения $f \cdot g$ равен произведению высшего члена f и высшего члена g.*

Д о к а з а т е л ь с т в о. Пусть $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ – высший член многочлена f, а $a'x_1^{k'_1}x_2^{k'_2}\dots x_n^{k'_n}$ – любой другой член f; $bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ – высший член многочлена g, а $b'x_1^{l'_1}x_2^{l'_2}\dots x_n^{l'_n}$ – любой другой член g. Пусть

$$k_1 = k'_1, k_2 = k'_2, \dots, k_{i-1} = k'_{i-1}, k_i > k'_i;$$

$$l_1 = l'_1, l_2 = l'_2, \dots, l_{j-1} = l'_{j-1}, l_j > l'_j.$$

Надо доказать, что произведение $abx_1^{k_1+l_1}x_2^{k_2+l_2}\dots x_n^{k_n+l_n}$ выше любого из членов

$$ab'x_1^{k_1+l'_1}x_2^{k_2+l'_2}\dots x_n^{k_n+l'_n},\quad a'bx_1^{k'_1+l_1}x_2^{k'_2+l_2}\dots x_n^{k'_n+l_n},\quad a'b'x_1^{k'_1+l'_1}x_2^{k'_2+l'_2}\dots x_n^{k'_n+l'_n}.$$

Для первых двух членов это очевидно. Докажем для третьего.

Пусть $i \le j$, тогда

$$k_1 + l_1 = k'_1 + l'_1, k_2 + l_2 = k'_2 + l'_2, \dots, k_{i-1} + l_{i-1} = k'_{i-1} + l'_{i-1}, k_i + l_i > k'_i + l'_i.$$

Если $i \ge j$, то

$$k_1 + l_1 = k'_1 + l'_1, k_2 + l_2 = k'_2 + l'_2, \dots, k_{i-1} + l_{i-1} = k'_{j-1} + l'_{j-1}, k_j + l_j > k'_j + l'_j,$$

т. е. мы доказали, что член $abx_1^{k_1+l_1}x_2^{k_2+l_2}\dots x_n^{k_n+l_n}$ выше члена $a'b'x_1^{k'_1+l'_1}x_2^{k'_2+l'_2}\dots x_n^{k'_n+l'_n}$. Лемма доказана.

26.3. Симметрические многочлены. В кольце $K[x_1, x_2, \dots, x_n]$ можно выделить подкольцо симметрических многочленов.

О п р е д е л е н и е. Многочлен называется *симметрическим* если он не изменяется ни при какой перестановке переменных.

П р и м е р ы. 1) Нетрудно проверить, что многочлен

$$x_1^3x_2 + x_2^3x_3 + x_1x_2^3 + x_1x_3^3 + x_2x_3^3 + x_1^3x_3$$

является симметрическим.

2) Следующие многочлены называются *элементарными симметрическими многочленами*

$$\sigma_1 = x_1 + x_2 + \ldots + x_n,$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_k = \sum_{1\le i_1<i_2<\ldots<i_k\le n} x_{i_1}x_{i_2}\ldots x_{i_k},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_n = x_1x_2\ldots x_n.$$

Они возникают в формуле Виета.

Элементарные симметрические многочлены порождают все симметрические многочлены. Более точно, справедлива

Т е о р е м а 2. *Пусть $K_s[x_1, x_2, \ldots, x_n]$ – множество всех симметрических многочленов над K от $x_1, x_2, \ldots, x_n$. Тогда*

1) *$K_s[x_1, x_2, \ldots, x_n]$ – подкольцо кольца $K[x_1, x_2, \ldots, x_n]$;*

2) *$K_s[x_1, x_2, \ldots, x_n]$ порождается кольцом K и многочленами σ_1, σ_2, …, σ_n.*

Д о к а з а т е л ь с т в о. 1) Чтобы проверить, что $K_s[x_1, x_2, \ldots, x_n]$ является подкольцом, достаточно проверить, что если f и g – симметрические многочлены, то многочлены $f+g$, $-f$ и $f\cdot g$ также являются симметрическими. Это непосредственно следует из определения.

2) Проверим, что $K_s[x_1, x_2, \ldots, x_n]$ порождается K и σ_1, σ_2, …, σ_n, т. е. каждый симметрический многочлен можно представить как многочлен над K от σ_1, σ_2, …, σ_n. Пусть $f \in K_s[x_1, x_2, \ldots, x_n]$ и его высший член равен $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$. Так как f симметрический, то $k_1 \ge k_2 \ge \ldots \ge k_n$. Действительно, если бы оказалось, что $k_i < k_{i+1}$, то переставляя x_i и x_{i+1}, получили бы член, который содержится в f и выше $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$.

Рассмотрим
$$f_1 = a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\ldots\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}.$$
По лемме о высшем члене произведения видим, что высший член f_1 равен
$$ax_1^{k_1-k_2}(x_1x_2)^{k_2-k_3}\ldots(x_1x_2\ldots x_n)^{k_n} = ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n},$$
т. е. совпадает с высшим членом многочлена f. Рассмотрим многочлен $f - f_1$. Его высший член ниже высшего члена многочлена f. Пусть $bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}$ – высший член многочлена $f - f_1$. Берем многочлен
$$f_2 = b\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\ldots\sigma_{n-1}^{l_{n-1}-l_n}\sigma_n^{l_n}.$$

Так же как и выше, замечаем, что высший член f_2 равен высшему члену многочлена $f - f_1$. Поэтому высший член $f - f_1 - f_2$ ниже высшего члена $f - f_1$. Продолжая эту процедуру, видим, что процесс оборвется на нулевом многочлене и в результате мы получим искомое разложение

$$f = f_1 + f_2 + \ldots + f_s.$$

Теорема доказана.

26.4. Симметрические многочлены от корней многочлена от одной переменной. Рассмотрим многочлен

$$f(x) = x^2 + 1$$

над полем рациональных чисел $\mathbb{Q}$. Как мы знаем, он имеет два комплексных корня: $\alpha_1 = -\mathrm{i}$, $\alpha_2 = \mathrm{i}$. Если мы подставим эти корни в многочлен от двух переменных:

$$h(x_1, x_2) = x_1^2 + x_1x_2 + x_2$$

над $\mathbb{Q}$, то получим элемент $h(\alpha_1, \alpha_2) = \mathrm{i}$, который не лежит в $\mathbb{Q}$. Если же подставить корни в симметрический многочлен $g(x_1, x_2) = x_1^2 + x_1x_2 + x_2^2$, то получим элемент $g(\alpha_1, \alpha_2) = -1$ из $\mathbb{Q}$. Оказывается, что справедливо

П р е д л о ж е н и е. *Пусть $f(x)$ многочлен из $P[x]$ степени n, имеющий корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ в некотором расширении L поля P, а $g = g(x_1, x_2, \ldots, x_n)$ – симметрический многочлен над P. Тогда его значение $g(\alpha_1, \alpha_2, \ldots, \alpha_n)$ от корней $\alpha_1, \alpha_2, \ldots, \alpha_n$ лежит в поле P.*

Пусть многочлен

$$f(x) = a_0x_n + a_1x^{n-1} + \ldots + a_n = a_0(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n), \quad a_i \in P,$$

имеет корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ в некотором поле L, которое является расширением поля P, т. е.

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n), \quad a_i \in P.$$

Если g – симметрический, то по теореме 1 его можно записать как многочлен от σ_1, σ_2, …, σ_n над P, т. е $g = F(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Подставив корни, по теореме Виета получим

$$g(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\sigma_1(\alpha_1, \alpha_2, \ldots, \alpha_n), \sigma_2(\alpha_1, \alpha_2, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \alpha_2, \ldots, \alpha_n)) =$$

$$= F\left(-\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, (-1)^n\frac{a_n}{a_0}\right) \in P.$$

Предложение доказано.

26.5. Алгебраическая независимость элементарных симметрических многочленов. Как мы знаем, кольцо симметрических многочленов $P_s[x_1, x_2, \ldots, x_n]$ порождается полем P и элементарными симметрическими многочленами σ_1, σ_2, …, σ_n. Справедлива

Т е о р е м а 3. *Элементарные симметрические многочлены σ_1, σ_2, …, σ_n алгебраически независимы над основным полем P.*

Д о к а з а т е л ь с т в о. Предположим, что для некоторого многочлена $\varphi \in P[y_1, y_2, \ldots, y_n]$ имеем $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$, т. е 0 представим двумя разными способами. Надо доказать, что $\varphi \equiv 0$.

Пусть $\varphi = \sum_i \varphi_i$, где $\varphi_i = a_i y_1^{k_{i_1}} y_2^{k_{i_2}} \ldots y_n^{k_{i_n}}$. Отсюда

$$\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n) = \sum_i \varphi_i(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Пусть

$$\varphi_i(\sigma_1, \sigma_2, \ldots, \sigma_n) = f_i(x_1, x_2, \ldots, x_n) \in P[x_1, x_2, \ldots, x_n].$$

По лемме о высшем члене произведения имеем

$$(\text{высший член } f_i) = a_i \cdot (\text{высший член } \sigma_1)^{k_{i_1}} \cdot \ldots \cdot (\text{высший член } \sigma_n)^{k_{i_n}} =$$

$$= a_i x_1^{k_{i_1}+k_{i_2}+\ldots+k_{i_n}} x_2^{k_{i_2}+k_{i_3}+\ldots+k_{i_n}} \ldots x_n^{k_{i_n}}.$$

Если высший член многочлена f_i известен, то φ_i можно однозначно восстановить. Тогда по формуле

$$\varphi = \sum_i \varphi_i$$

можем восстановить φ. если бы высшие члены у f_i и f_j совпадали, то $\varphi_i = \varphi_j$, а этого быть не может. Следовательно, все высшие члены у f_j различны. Пусть $b x_1^{l_1} x_2^{l_2} \ldots x_n^{l_n}$ – высший из всех высших членов f_i. Тогда он ни с чем не сократится, а потому $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n) \neq 0$, противоречие. Теорема доказана.

Из доказанной теоремы следует, что кольцо симметрических многочленов изоморфно кольцу многочленов:

$$P_s[x_1, x_2, \ldots, x_n] \simeq P[x_1, x_2, \ldots, x_n] = P[\sigma_1, \sigma_2, \ldots, \sigma_n].$$

§ 27. Комплексные многочлены от одной переменной

Особый интерес представляют поля, которые не надо расширять – алгебраически замкнутые.

О п р е д е л е н и е. Поле P называется *алгебраически замкнутым,* если любой многочлен ненулевой степени из $P[x]$ имеет в P хотя бы один корень.

У п р а ж н е н и е. Поле алгебраически замкнуто тогда и только тогда, когда любой многочлен над этим полем разлагается над ним на линейные множители. (У к а з а н и е: использовать теорему Безу.)

27.1. Алгебраическая замкнутость поля комплексных чисел. В этом пункте мы докажем утверждение о том, что поле комплексных чисел алгебраически замкнуто. Это утверждение иногда называют основной теоремой алгебры. Более правильно было бы назвать ее основной теоремой алгебры многочленов.

Предварительно докажем следующее утверждение, которое представляет и самостоятельный интерес.

Л е м м а 1 (о модуле старшего члена). *Для многочлена*

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

найдется такое вещественное неотрицательное число N, что для всех $x \in \mathbb{C}$, таких, что $|x| \geq N$ справедливо неравенство

$$|a_0x^n| > |a_1x^{n-1} + \ldots + a_n|.$$

Д о к а з а т е л ь с т в о. Имеем

$$|a_1x^{n-1} + \ldots + a_n| \leq |a_1| \cdot |x|^{n-1} + |a_2| \cdot |x|^{n-2} + \ldots + |a_n|.$$

Положим

$$A = \max\{|a_1|, |a_2|, \ldots, |a_n|\}.$$

Тогда

$$|a_1| \cdot |x|^{n-1} + |a_2| \cdot |x|^{n-2} + \ldots + |a_n| \leq A(|x|^{n-1} + |x|^{n-2} + \ldots + 1) = A\frac{|x|^n - 1}{|x| - 1} < A\frac{|x|^n}{|x| - 1}.$$

Найдем те значения x для которых выполняется неравенство

$$A\frac{|x|^n}{|x| - 1} \leq |a_0x^n|.$$

Нетрудно проверить, что оно выполняется тогда и только тогда, когда

$$|x| > 1 + \frac{A}{|a_0|}.$$

Следовательно, полагая

$$N = 1 + \frac{A}{|a_0|},$$

Получим нужное утверждение. Лемма доказана.

Из этой леммы, в частности, следует, что все комплексные корни многочлена $f(x)$ лежат внутри круга с центром в начале координат и радиуса N.

Т е о р е м а. *Поле комплексных чисел алгебраически замкнуто.*

Д о к а з а т е л ь с т в о. Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n, \quad a_0 \neq 0, \quad a_i \in \mathbb{C}.$$

Надо доказать, что f имеет комплексный корень.

Случай 1. Предположим вначале, что $f \in \mathbb{R}[x]$, т. е. все коэффициенты a_i лежат в $\mathbb{R}$. Представим степень многочлена n в таком виде: $n = 2^k q$, где q – нечетное число. Воспользуемся индукцией по k. При $k = 0$ число n нечетно. Ввиду леммы о модуле старшего члена найдется такое неотрицательное вещественное число N, что $f(-N)$ и $f(N)$ имеют разные знаки. В этом случае справедлива следующая лемма, доказанная в курсе математического анализа.

Л е м м а 2. *Всякая вещественная функция, непрерывная на отрезке* $[a, b]$ *и принимающая на его концах значения разных знаков, обращается в* 0 *в некоторой точке* $c \in [a, b]$.

Следовательно, найдется вещественное число c из отрезка $[-N, N]$, которое является корнем многочлена f. Основание индукции установлено.

Пусть теперь $k > 0$. Предположим, что утверждение справедливо для $k - 1$ и докажем его для k. По теореме о существовании корня найдется поле P, являющееся расширением поля $\mathbb{R}$, над которым многочлен f разлагается на линейные множители

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n), \quad \alpha_i \in P.$$

Пусть $c \in \mathbb{R}$. Определим числа $\beta_{ij} = \alpha_i\alpha_j + (\alpha_i + \alpha_j)c$, $1 \leq i < j \leq n$, и рассмотрим многочлен

$$g(x) = \prod_{1 \leq i < j \leq n} (x - \beta_{ij}).$$

Очевидно, что его степень

$$\deg g = \frac{n(n-1)}{2} = 2^{k-1}q',$$

где $q' = q(n - 1)$ – нечетно, так как $k \geq 1$. Надо убедиться, что коэффициенты многочлена g лежат в $\mathbb{R}$. Заметим, что всякий коэффициент g является элементарным симметрическим многочленом от β_{ij} над $\mathbb{R}$, т. е. если переставить пару индексов (i, j) и (r, s), то многочлен $g(x)$ не изменится. Отсюда нетрудно вывести, что если переставить местами любые корни α_i и α_j, то многочлен также не изменится. Следовательно, всякий коэффициент g является симметрическим многочленом над $\mathbb{R}$ от

$\alpha_1, \alpha_2, \ldots, \alpha_n$. По доказанному выше предложению о симметрическом многочлене от корней уравнения заключаем, что всякий коэффициент многочлена g лежит в $\mathbb{R}$, а потому и $g \in \mathbb{R}[x]$. По предположению индукции g имеет хотя бы один корень в $\mathbb{C}$, т. е. хотя бы одно $\beta_{ij} \in \mathbb{C}$.

Вспоминаем, что β_{ij} зависит от вещественного параметра c. Выбирая другое значение c получим, что какой-то другой β_{rs} является комплексным корнем, но в качестве c мы можем брать любое вещественное число, а число перестановок корней β_{ij} конечно. Следовательно, найдется пара вещественных чисел c_1 и c_2, $c_1 \neq c_2$ таких, что

$$\alpha_i\alpha_j + (\alpha_i + \alpha_j)c_1 = b_1 \in \mathbb{C},$$
$$\alpha_i\alpha_j + (\alpha_i + \alpha_j)c_2 = b_2 \in \mathbb{C}.$$

Тогда

$$\alpha_i + \alpha_j = \frac{b_1 - b_2}{c_1 - c_2} \in \mathbb{C}, \quad \alpha_i\alpha_j \in \mathbb{C}.$$

Пара α_i, α_j является корнями уравнения

$$z^2 - (\alpha_i + \alpha_j)z + \alpha_i\alpha_j = 0$$

с комплексными коэффициентами. По формуле нахождения корней квадратного многочлена видим, что α_i и α_j являются комплексными числами. Следовательно, мы нашли два комплексных корня многочлена f.

Случай 2: $f \in \mathbb{C}[x]$, т. е. все a_i лежат в $\mathbb{C}$. Рассмотрим многочлен

$$\overline{f}(x) = \overline{a_0}x^n + \overline{a_1}x^{n-1} + \ldots + \overline{a_n},$$

и определим

$$F(x) = f(x) \cdot \overline{f}(x) = \sum_{k=0}^{2n} c_k x^k, \text{ где } c_k = \sum_{r+s=k} a_r\overline{a_s}.$$

Ясно, что

$$\overline{c_k} = \overline{\sum_{r+s=k} a_r\overline{a_s}} = \sum_{r+s=k} \overline{a_r\overline{a_s}} = \sum_{r+s=k} \overline{a_r}a_s = c_k,$$

т. е $c_k \in \mathbb{R}$ так как при взятии комплексно-сопряженного его значение не меняется, а потому $F(x) \in \mathbb{R}[x]$. По установленному случаю 1, у него существует корень, т. е. найдется некоторое $\gamma \in \mathbb{C}$, такое, что

$$F(\gamma) = f(\gamma) \cdot \overline{f}(\gamma) = 0$$

Если $f(\gamma)=0$, то γ – корень f. Если $\overline{f}(\gamma)=0$, то

$$\overline{a_0}\gamma^n+\overline{a_1}\gamma^{n-1}+\ldots+\overline{a_n}=0$$

и переходя к комплексно-сопряженному, получим

$$a_0\overline{\gamma}^n+a_1\overline{\gamma}^{n-1}+\ldots+a_n=\overline{0},$$

т. е. $\overline{\gamma}$ – корень многочлена f и $\gamma\in\mathbb{C}$. Теорема доказана.

27.2. Некоторые приложения. Пусть $z=a+\mathrm{i}b$, $a,b\in\mathbb{R}$, – некоторое комплексное число. Как мы знаем, в тригонометрической форме его можно записать так: $z=r(\cos\varphi+\mathrm{i}\sin\varphi)$. Обозначим $\cos\varphi+\mathrm{i}\sin\varphi=\mathrm{e}^{\mathrm{i}\alpha}$, $\alpha\in\mathbb{R}$, и рассмотрим N-угольник. Тогда его вершинами будут являться точки $a_k=\mathrm{e}^{\frac{2k\pi\mathrm{i}}{N}}$, $k=0,1,\ldots,N-1$ на комплексной плоскости. Справедлива

Т е о р е м а (о значении многочлена в центре правильного многоугольника). *Для любого многочлена $f\in\mathbb{C}[x]$ степени n и всякого правильного N-угольника, $N>n$ с центром в точке a и вершинами a_k, $k=0,1,\ldots,N-1$, справедливо равенство*

$$f(a)=\frac{1}{N}\sum_{k=0}^{N-1}f(a_k).$$

Д о к а з а т е л ь с т в о. Можно считать, что $a_k=a+be^{\frac{2\pi ki}{N}}$ при подходящем $b\in\mathbb{C}$. Рассмотрим многочлен $g(x)=f(a+bx)$. Очевидно, $g(0)=f(a)$ и надо доказать, что

$$g(0)=\frac{1}{N}\sum_{k=0}^{N-1}g(e^{\frac{2\pi ki}{N}}).$$

Пусть $g(x)=\sum_{s=0}^{n}a_sx^s$. Тогда подставляя

$$\frac{1}{N}\sum_{k=0}^{N-1}g(e^{\frac{2\pi ki}{N}})=\frac{1}{N}\sum_{k=0}^{N-1}\sum_{s=0}^{n}a_s\left(e^{\frac{2\pi ki}{N}}\right)^s=\frac{1}{N}\sum_{s=0}^{n}a_s\left(\sum_{k=0}^{n-1}e^{\frac{2\pi ksi}{N}}\right)=\frac{1}{N}a_0N=a_0=g(0).$$

Так как

$$\sum_{k=0}^{N-1}e^{\frac{2\pi ksi}{N}}=1+e^{\frac{2\pi si}{N}}+e^{\frac{2\pi s2i}{N}}+\ldots$$

– геометрическая прогрессия, то

$$\sum_{k=0}^{N-1}e^{\frac{2\pi ksi}{N}}=\begin{cases}N & \text{при } s=0,\\ \frac{q^N-1}{q-1}=0 & \text{при } s\neq 0.\end{cases}$$

Теорема доказана.

У п р а ж н е н и е. Где использовалось, что $N > n$?

Всякий многочлен $f(x) \in \mathbb{C}[x]$ мы можем рассматривать как функцию $f : \mathbb{C} \longrightarrow \mathbb{C}$. При этом $|f(x)|$ является функцией, определенной на $\mathbb{C}$ со значениями в $\mathbb{R}$, т. е. $|f| : \mathbb{C} \longrightarrow \mathbb{R}$. Справедлива

Т е о р е м а (отсутствие локальных максимумов модуля). *Ни для какого многочлена $f(x) \in \mathbb{C}[x] \setminus \mathbb{C}$ не существует локальных максимумов функции $|f|$.*

Д о к а з а т е л ь с т в о. Предположим, что точка a является точкой локального максимума функции $|f|$, т. е. $|f(x)| < |f(a)|$ при условии, что $x \neq a$ удовлетворяет неравенству $|x-a| \leq \delta$ для некоторого $\delta > 0$. Пусть $N > n$, где n – степень многочлена f. Обозначим a_k, $k = 0, 1, \ldots, N-1$, – вершины правильного N-угольника с центром в точке a. Тогда по теореме 1 справедливо неравенство

$$|f(a)| \leq \frac{1}{N} \sum_{k=0}^{N-1} |f(a_k)|$$

из которого следует, что $|f(a)| < |f(a)|$. Противоречие.

Отметим, что теоремы 1 и 2 справедливы не только для многочленов, но и для произвольных аналитических функций

$$f(x) = \sum_{k=0}^{\infty} a_k x^k, \quad a_k \in \mathbb{C}.$$

§ 28. Поле частных

Мы знаем. что кольцо целых чисел вкладывается в поле рациональных чисел, кольцо многочленов над полем вкладывается в поле рациональных дробей. Возникает естественный вопрос: всякое ли кольцо вкладывается в поле? Ответ, очевидно, отрицательный, так как некоммутативное кольцо или кольцо обладающее делителями нуля не может быть вложено в поле. Оказывается, что некоммутативность и наличие делителей нуля являются единственными препятствиями к требуемому вложению.

28.1. Вложение целостного кольца в поле. Напомним, что кольцо называется *целостным,* если оно коммутативно и не имеет делителей нуля. В частности, любое поле является целостным кольцом. Действительно, если $ab = 0$ и $a \neq 0$, то существует элемент a^{-1}, а потому $a^{-1}ab = b = 0$, т. е. $b = 0$. Кроме того, легко заметить, что любое подкольцо поля является целостным кольцом.

Т е о р е м а 1. 1) *Любое целостное кольцо K изоморфно вкладывается в некоторое поле L.* 2) *Подполе, порожденное образом кольца K в поле L, определено однозначно с точностью до изоморфизма.*

Д о к а з а т е л ь с т в о. Вначале докажем существование такого поля. Для этого рассмотрим множество пар:

$$\{(a,b) \mid a,b \in K, b \neq 0\}$$

и определим на нем отношение $\sim$, полагая $(a,b) \sim (c,d)$ если $ad = bc$. Проверим, что это отношение является отношением эквивалентности. Для этого надо проверить

1) $(a,b) \sim (a,b)$;

2) если $(a,b) \sim (c,d)$, то $(c,d) \sim (a,b)$;

3) если $(a,b) \sim (c,d)$ и $(c,d) \sim (e,f)$, то $(a,b) \sim (e,f)$.

Первые два свойства очевидны. Установим свойство 3). Пусть $(a,b) \sim (c,d)$ и $(c,d) \sim (e,f)$. Это равносильно тому, что $ad = bc$ и $cf = de$. Надо доказать, что $af = be$. Умножая первое равенство на f, а второе на b, получим

$$adf = bcf, \quad bcf = bde.$$

Из этих равенств следует, что $adf = bde$ и, сокращая на d, получим $af = be$, но это и означает, что $(a,b) \sim (e,f)$. Следовательно, отношение $\sim$ действительно является отношением эквивалентности. Относительно этого отношение множество

$$\{(a,b) \mid a,b \in K, b \neq 0\}$$

распадается на классы эквивалентности. Обозначим $\overline{(a,b)}$ множество пар, эквивалентных (a,b), т. е.

$$\overline{(a,b)} = \{(c,d) \mid (c,d) \sim (a,b)\}$$

и рассмотрим фактор-множество

$$L = \{(a,b) \mid a,b \in K, b \neq 0\}/_{\sim}.$$

Определим на L операции сложения и умножения, полагая

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)},$$

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}.$$

Проверим, что эти операции определены корректно, т. е не зависят от выбора представителей. Пусть

$$\overline{(a,b)} = \overline{(a',b')}, \quad \overline{(c,d)} = \overline{(c',d')},$$

т. е

$$(a,b) \sim (a',b'), \quad (c,d) \sim (c',d').$$

Надо проверить, что справедливы равенства

$$\overline{(ad+bc,bd)} = \overline{(a'd'+b'c',b'd')}, \quad \overline{(ac,bd)} = \overline{(a'c',b'd')},$$

т. е.

$$(ad+bc,bd) \sim (a'd'+b'c',b'd'), \quad (ac,bd) \sim (a'c',b'd').$$

Для проверки первого равенства умножим равенство $ab' = ba'$ на dd', а равенство $cd' = dc'$ на bb', складывая эти равенства, получим

$$(ad+bc)b'd' = bd(a'd'+b'c').$$

Следовательно, операция сложения определена корректно.

Проверим справедливость второго равенства. Имеем

$$ab' = ba', \quad cd' = dc'$$

Перемножая эти равенства почленно, получим $acb'd' = bda'c'$. Следовательно, операция умножения определена корректно.

Докажем, что алгебраическая система $\langle L; +, \cdot \rangle$ является полем. Для этого надо проверить все аксиомы поля.

С1) Ассоциативность сложения: $(A+B)+C = A+(B+C)$.

Пусть $A = \overline{(a,b)}$, $B = \overline{(c,d)}$, $C = \overline{(e,f)}$. Тогда

$$A+B = \overline{(ad+bc,bd)}, \quad (A+B)+C = \overline{((ad+bc)f+bde,(bd)f)}$$

С другой стороны,

$$B+C = \overline{(cf+de,df)}, \;\; A+(B+C) = \overline{(adf+b(cf+de),b(df))} = \overline{((ad+bc)f+bde,(bd)f)},$$

т. е ассоциативность сложения выполняется.

С2) Коммутативность сложения: $A+B = B+A$. Очевидно.

С3) В качестве нулевого элемента возьмем класс $\overline{(0,u)}$, где $u \neq 0$.

С4) Противоположным к классу $\overline{(a,b)}$ является класс $-\overline{(a,b)} = \overline{(-a,b)}$.

Аксиомы У1 и У2 выполняются в силу соответствующих аксиом кольца K.

У3) Единичным классом является класс $\overline{(u,u)}$, $u \neq 0$.

У4) Для любого класса $\overline{(a,b)} \neq \overline{(0,u)}$ обратным будет $\overline{(a,b)}^{-1} = \overline{(b,a)}$.

Таким образом, L действительно является полем.

Рассмотрим отображение

$$\varphi : K \longrightarrow L,$$

сопоставляющее каждому элементу из K элемент из L по правилу $a\varphi = \overline{(au, u)}$, $u \in K \setminus \{0\}$. Покажем, что это изоморфизм K в L. Действительно, если $a \neq b$, но $\overline{(au, u)} = \overline{(bu, u)}$, т. е. $(au, u) \sim (bu, u)$, то $au^2 = bu^2$ и, учитывая, что K целостное, вопреки предположению, получим $a = b$. Следовательно, отображение φ унивалентно.

Проверим, что φ сохраняет операцию сложения, т. е.

$$(a + b)\varphi = a\varphi + b\varphi.$$

Левая часть этого равенства:

$$(a + b)\varphi = \overline{((a + b)u, u)};$$

правая часть:

$$a\varphi + b\varphi = \overline{(au, u)} + \overline{(bu, u)} = \overline{(au^2 + bu^2, u^2)} = \overline{((a + b)u, u)}.$$

Следовательно, операция сложения сохраняется.

Аналогично проверяется, что сохраняется и операция умножения.

Таким образом, пункт 1) теоремы установлен.

2) Предположим, что существует два изоморфных вложения φ' и φ'' кольца K в поля L' и L'' соответственно. Обозначим M – подполе поля L', порожденное $\varphi'(K)$, а M' – подполе поля L'', порожденное $\varphi''(K)$. Докажем, что каждое из этих подполей изоморфно полю L. Заметим вначале, что

$$M = \{ab^{-1} \mid a, b \in K, b \neq 0\},$$

где мы отождествляем элементы из K с их образами в $\varphi'(K)$. Действительно, если $a, b \in K$, то в M лежат обратные элементы и произведения. Следовательно, включение $\supseteq$ выполняется. Обратно. Покажем, что элементы ab^{-1} образуют подполе. Для этого надо проверить замкнутость относительно сложения, умножения, взятия противоположного и взятия обратного. Так как

$$ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1}$$

и

$$ab^{-1} \cdot cd^{-1} = (ac)(bd)^{-1},$$

то наше множество замкнуто относительно сложения и умножения. Противоположным к элементу ab^{-1} является элемент $-ab^{-1} = (-a)b^{-1}$. Если $ab^{-1} \neq 0$, то $a \neq 0$ и $(ab^{-1})^{-1} = ba^{-1}$. Заметим, что M содержит K. Действительно, если $a \in K$, то его можно представить в виде $a = (ab) \cdot b^{-1}$. Таким образом, множество элементов ab^{-1}

образует подполе, которое содержит K, а так как M наименьшее с этим свойством, то отсюда следует включение $\subseteq$.

Рассмотрим теперь отображение

$$\omega : M \longrightarrow L,$$

действующее по правилу

$$ab^{-1} \longmapsto \overline{(a,b)}.$$

Покажем, что это отображение является изоморфизмом. То, что ω однозначно, следует из определения. Проверим унивалентность: предположим, что $(ab^{-1})\omega = (cd^{-1})\omega$, т. е. $\overline{(a,b)} = \overline{(c,d)}$, но последнее означает, что $(a,b) \sim (c,d)$, т. е. $ad = bc$, а потому $ab^{-1} = cd^{-1}$. То, что ω сохраняет операции, следует из определения операций в L. Теорема доказана.

О п р е д е л е н и е. Наименьшее поле, содержащее данное целостное кольцо в качестве подкольца называется *полем частных* этого кольца.

Поле частных полностью определяется кольцом K. Будем обозначать его поле частных символом $\ddot{K}$. Очевидно, что для кольца целых чисел $\mathbb{Z}$ его поле частных изоморфно полю рациональных чисел $\mathbb{Q}$.

При работе с полем частных, пару (a,b), $b \neq 0$, записывают в виде дроби $\frac{a}{b}$. Очевидно, что класс $\overline{(a,b)}$ состоит из дробей $\frac{au}{bu}$, $u \neq 0$. Нетрудно проверить, что операции сложения и умножения классов в поле частных согласуются с обычными операциями сложения и умножения дробей.

28.2. Поле рациональных дробей. Рассмотрим кольцо многочленов $P[x_1, x_2, \ldots, x_n]$ над полем P. Как мы знаем, это кольцо является целостным. По доказанной теореме оно вкладывается в поле. Полем частных кольца многочленов $P[x_1, x_2, \ldots, x_n]$ является поле рациональных дробей:

$$P(x_1, x_2, \ldots, x_n) = \left\{ \frac{f}{g} \;\middle|\; f, g \in P[x_1, x_2, \ldots, x_n], g \neq 0 \right\}.$$

При этом $\frac{f}{g} = \frac{f'}{g'}$, если $fg' = gf'$. Сложение и умножение рациональных дробей определяются правилами:

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + gf'}{gg'}, \quad \frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'}.$$

Каждый многочлен можно рассматривать как функцию $P^n \longrightarrow P$. Для рациональной дроби может оказаться, что ее знаменатель обращается в нуль при некоторых значениях переменных.

28.3. База векторного пространства $P(x)$ над полем P. Множество $P[x_1, x_2, \ldots, x_n]$ образует векторное пространство над полем P. Его базу образуют одночлены вида

$$x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}, \quad k_i \in \mathbb{N} \cup \{0\}.$$

Также легко проверить, что и множество рациональных дробей $P(x_1, x_2, \ldots, x_n)$ образует векторное пространство над полем P. Возникает вопрос об описании базы этого пространства. Здесь мы рассмотрим этот вопрос для случая $n = 1$.

Векторное пространство $P[x]$ обладает базой

$$1, x, x^2, \ldots,$$

и любой многочлен является линейной комбинацией этих многочленов. Но, как легко заметить, эти многочлены уже не образуют базу векторного пространства $P(x)$.

О п р е д е л е н и е. Несократимая дробь $\frac{x^n}{p^m}$, $n \in \mathbb{N} \cup \{0\}$, $m \in \mathbb{N}$, называется *простейшей,* если p – неразложимый многочлен со старшим коэффициентом 1 и $\deg p > n$.

П р и м е р. Простейшими дробями в $\mathbb{R}(x)$ будут дроби

$$\frac{1}{(x-\alpha)^m}, \quad \frac{1}{(x^2+px+q)^m}, \quad \frac{x}{(x^2+px+q)^m},$$

где $\alpha \in \mathbb{R}$, а $x^2 + px + q$ – многочлен, неразложимый над $\mathbb{R}$.

Т е о р е м а 2. *Многочлены $1, x, x^2, \ldots$ и простейшие дроби образуют базу векторного пространства $P(x)$ над полем P.*

Д о к а з а т е л ь с т в о. Докажем вначале линейную независимость. Предположим, что некоторая линейная комбинация равна нулю, т. е.

$$f + \sum_{m=1}^{m_1} \frac{f_{1,m}}{p_1^m} + \sum_{m=1}^{m_2} \frac{f_{2,m}}{p_2^m} + \ldots + \sum_{m=1}^{m_s} \frac{f_{s,m}}{p_s^m} = 0,$$

где $f \in P[x]$, $f_{i,m} \in P[x]$ и $\deg f_{i,m} < \deg p_i$. Здесь мы объединили линейную комбинацию базисных многочленов в f и считаем, что все p_i различны, так как если у двух дробей один и тот же множитель p_i в знаменателе, то мы можем найти их сумму и записать в виде одной дроби. Надо доказать, что $f = 0$ и все $f_{i,m} = 0$. Умножим обе части нашего равенства на $p_1^{m_1} p_2^{m_2} \ldots p_s^{m_s}$ и если $f \neq 0$, то мы получим равенство

$$(\text{старший коэффициент } f)x^{\deg f + m_1 \deg p_1 + \ldots + m_s \deg p_s} + \{\text{остальные слагаемые}\} = 0.$$

Покажем, что это равенство невозможно так как степень первого слагаемого выше степени любого другого слагаемого. Действительно, если рассмотреть первое слагаемое первой суммы:

$$f_{1,1} p_1^{m_1 - 1} p_2^{m_2} \ldots p_s^{m_s},$$

то оно имеет степень

$$\deg f_{1,1}+(m_1-1)\deg p_1+m_2\deg p_2+\ldots+m_s\deg p_s < m_1\deg p_1+m_2\deg p_2+\ldots+m_s\deg p_s.$$

Аналогично проверяется, что и любое другое слагаемое имеет меньшую степень. Следовательно, $f=0$.

Предположим теперь, что $f_{1,m_1}\neq 0$. Умножая на то же произведение $p_1^{m_1}\ p_2^{m_2}\ldots p_s^{m_s}$ слагаемое $\frac{f_{1,m_1}}{p_1^{m_1}}$, получим $f_{1,m_1}p_2^{m_2}\ldots p_s^{m_s}$, а все остальные слагаемые будут содержать p_1. Следовательно,

$$f_{1,m_1}\,p_2(x)^{m_2}\ldots p_s(x)^{m_s}+p_1[\ldots]=0,$$

так как f_{1,m_1} и ни один из сомножителей $p_2,\ \ldots,\ p_s$, не делятся на p_1 (так как все p_i неразложимы), то $f_{1,m_1}=0$. Аналогично проверяется, что и все $f_{i,m_1}=0$.

Докажем максимальность. Возьмем произвольную дробь $\frac{f}{g}\in P(x)$. Пусть $g=p_1^{m_1}p_2^{m_2}\ldots p_s^{m_s}$, где $p_1,p_2,\ldots,p_m$ – различные неразложимые многочлены и старший коэффициент у каждого p_i равен 1. Проведем индукцию по s.

Если $s=0$, то $g=1$ и $\frac{f}{g}$ – просто многочлен, а потому разлагается в линейную комбинацию многочленов $1,x,x^2,\ldots$

Если $s=1$, то $\frac{f}{g}=\frac{f}{p_1^{m_1}}$. Разделим f с остатком на p_1, получим

$$f=p_1q_1+r_1$$

где $r_1=0$ или $\deg r_1<\deg p_1$. Тогда

$$\frac{f}{p_1^{m_1}}=\frac{q_1}{p_1^{m_1-1}}+\frac{r_1}{p_1^{m_1}},$$

и дробь $\frac{r_1}{p_1^{m_1}}$ либо равна нулю, либо является простейшей. Если дробь, $\frac{q_1}{p_1^{m_1-1}}$ не является простейшей, то представим q_1 в виде $q_1=p_1q_2+r_2$ и т. д. Получим разложение $\frac{f}{p_1^{m_1}}$ в виде линейной комбинации простейших дробей.

Предположим, что для $s-1$ утверждение справедливо и рассмотрим два многочлена $p_1^{m_1}$ и $p_2^{m_2}p_3^{m_3}\ldots p_s^{m_s}$. Они взаимно просты, а потому существуют многочлены $u,v\in P[x]$ такие, что

$$p_1^{m_1}u+p_2^{m_2}p_3^{m_3}\ldots p_s^{m_s}v=1.$$

Тогда

$$\frac{f}{g}=\frac{fu}{p_2^{m_2}p_3^{m_3}\ldots p_s^{m_s}}+\frac{fv}{p_1^{m_1}}.$$

По предположению индукции и, разобранному выше случаю $s=1$, каждая из дробей в правой части является линейной комбинацией простейших дробей. Теорема доказана.

В о п р о с. Из каких элементов состоит база векторного пространства $P(x_1, x_2, \ldots, x_n)$ при $n > 1$?

§ 29. Кольцо многочленов как кольцо с однозначным разложением

29.1. Равносильные определения кольца с однозначным разложением. Пусть K – целостное кольцо с единицей. Напомним некоторые определения, введенные ранее. Элементы a и b кольца K называются *ассоциированными*, если $a = b \cdot \varepsilon$ для некоторого $\varepsilon \in K^*$, где K^* – множество обратимых элементов кольца K. Ненулевой, необратимый элемент $a \in K$ называется *неразложимым,* если из того, что $a = bc$ следует, что $b \in K^*$ или $c \in K^*$. Целостное кольцо K с единицей называется *кольцом с однозначным разложением*, если:

а) всякий ненулевой необратимый элемент из K разлагается в произведение неразложимых;

б) если $a = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ – два таких разложения, то $r = s$ и p_i ассоциирован с q_i (возможно после перенумерации) для всех $i = 1, 2, \ldots, r$.

П р и м е р ы колец с однозначным разложением. 1) Кольцо целых чисел $\mathbb{Z}$. Для него $\mathbb{Z}^* = \{\pm 1\}$, ассоциированными являются элементы $\pm a$, а неразложимыми $\pm p$, где p – простое натуральное число.

2) Кольцо многочленов $P[x]$ от одной переменной над полем P. В этом случае множество обратимых элементов совпадает с $P^* = P \setminus \{0\}$, ассоциированными являются элементы αf, где $0 \neq \alpha \in P$, $f \in P[x]$.

Многочлен $f(x)$ неразложимый в кольце $K[x]$ часто называют *неразложимым над* K или *неприводимым над* K.

Следующая теорема дает другое определение кольца с однозначным разложением.

Т е о р е м а 1. *Условия* а) *и* б) *равносильны условиям* а) *и* б′), *где*

б′) *если* $p \mid ab$ *и* p *– неразложим, то* $p \mid a$ *или* $p \mid b$.

Д о к а з а т е л ь с т в о. Докажем вначале, что из условий а) и б) следуют условия а) и б′). Пусть $p \mid ab$, т. е. $ab = pc$ и

$$a = a_1 a_2 \ldots a_k, \quad b = b_1 b_2 \ldots b_l, \quad c = c_1 c_2 \ldots c_n,$$

– разложения в произведение неразложимых. Тогда

$$a_1 a_2 \ldots a_k b_1 b_2 \ldots b_l = p c_1 c_2 \ldots c_n$$

– две записи одного и того же элемента в произведение неразложимых. Тогда по б) p ассоциирован с некоторым a_i или с некоторым b_j, но это означает, что $p \mid a$ или $p \mid b$.

Докажем теперь, что из условий а) и б′) следуют условия а) и б). Пусть

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

– два разложения одного элемента в произведения неразложимых. Если $p_i \mid q_1 q_2 \dots q_s$, то по б)' $p_i \mid q_1$ или $p_i \mid q_2 \dots q_s$. Если $p_i \mid q_1$, то $q_1 = p_i c_i$ для некоторого $c_i \in K$, а так как q_1 неразложим, то $c_i \in K^*$, а потому p_i ассоциирован с q_1. Если $p_i \mid q_2 \dots q_s$, то опять, либо $p_i \mid q_2$ либо $p_i \mid q_3 \dots q_s$ и т. д. Следовательно, p_i ассоциирован с некоторым q_j. Теорема доказана.

Л е м м а 1. *Если K – кольцо с однозначным разложением, то для любых ненулевых a_1, a_2, …, a_s из K существует элемент $d \in K$ для которого выполняются следующие условия*:

а) $d \mid a_1$, $d \mid a_2, \dots, d \mid a_s$;

б) *если некоторый d' делит $a_1, a_2, \dots, a_s$, то $d' \mid d$.*

Это d единственно с точностью до множителя из K^* и называется *наибольшим общим делителем* элементов a_1, a_2, …, a_s.

Д о к а з а т е л ь с т в о. Пусть $a_i = \varepsilon_i p_1^{\alpha_{i1}} p_2^{\alpha_{i2}} \dots p_r^{\alpha_{ir}}$, где $\varepsilon_i \in K^*$, $p_1, p_2, \dots, p_r$ – различные неразложимые и α_{ij} – неотрицательные целые. Возьмем $d = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, где $\alpha_j = \min\{\alpha_{1j}, \alpha_{2j}, \dots, \alpha_{sj}\}$. Это и есть наибольший общий делитель. Действительно, так как $d \mid a_i$, $i = 1, 2, \dots, s$, то условие а) выполняется. Если $d' \mid a_i$, то $d' = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, где $\beta_i \le \alpha_i$. Следовательно, $d' \mid d$ и условие б) также выполняется. Лемма доказана.

29.2. Примитивные многочлены. Пусть K – кольцо с однозначным разложением. Многочлен $f \in K[x]$ называется *примитивным,* если наибольший общий делитель его коэффициентов обратим в K, т. е. лежит в K^*.

П р и м е р. Пусть $K = \mathbb{Z}$ и $f(x) = -30x^2 + 12x - 3$. Легко проверить, что наибольший общий делитель его коэффициентов равен 3, а потому $f(x)$ не является примитивным (напомним, что $\mathbb{Z}^* = \{\pm 1\}$).

Л е м м а 2. *Произведение двух примитивных многочленов является примитивным многочленом.*

Д о к а з а т е л ь с т в о. Предположим, что утверждение леммы не верно, т. е. существуют примитивные многочлены

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$

и

$$g(x) = b_0 + b_1 x + \dots + b_m x^m$$

такие, что их произведение

$$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \dots + a_n b_m x^{n+m}$$

не является примитивным многочленом, т. е. найдется общий делитель коэффициентов, который неразложим в K. Пусть p – неразложимый элемент из K, делящий все коэффициенты многочлена fg. Заметим, что p не может делить все коэффициенты f и не может делить все коэффициенты g. Пусть

$$p \mid a_0, \quad p \mid a_1, \ldots, p \mid a_{i-1}, \quad \text{но} \quad p \nmid a_i;$$

$$p \mid b_0, \quad p \mid b_1, \ldots, p \mid b_{j-1}, \quad \text{но} \quad p \nmid b_j.$$

В произведении fg коэффициент при x^{i+j} имеет вид

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0.$$

Заметим, что все слагаемые, стоящие перед $a_i b_j$ делятся на p и все слагаемые, стоящие после $a_i b_j$ также делятся на p. Так как по предположению все коэффициенты у fg делятся на p, то произведение $a_i b_j$ делится на p. Учитывая, что K – кольцо с однозначным разложением, заключаем, что $p \mid a_i$ или $p \mid b_j$. Полученное противоречивое и доказывает лемму.

29.3. Кольцо многочленов над кольцом с однозначным разложением – само кольцо с однозначным разложением. Докажем предварительно некоторые утверждения, которые потребуются нам в дальнейшем.

Л е м м а 3. *Множество обратимых элементов кольца $K[x]$ совпадает с множеством обратимых элементов кольца K.*

Д о к а з а т е л ь с т в о. Пусть $f \in K[x]$ обратим. Тогда для некоторого многочлена $g \in K[x]$ имеем $fg = 1$, но так как при умножении многочленов степени складываются, то многочлены f и g имеют нулевую степень, т. е. лежат в K, а так как их произведение равно 1, то f является обратимым элементом кольца K.

Обратно, если $\alpha \in K^*$, то $\alpha \in K[x]$, а потому является обратимым элементом кольца $K[x]$. Лемма доказана.

Л е м м а 4. *Элемент $a \in K$ разложим в K тогда и только тогда, когда a разложим в $K[x]$.*

Д о к а з а т е л ь с т в о. Пусть $a = bc$ – разложение в K, где $b, c \notin K^*$, но по лемме 3 это значит, что $b, c \notin K[x]^*$, а потому a разложим в $K[x]$.

Обратно. Пусть $a = bc$ – разложение в $K[x]$, т. е. $b, c \in K[x] \setminus K[x]^*$, но учитывая, что $\deg, a = 0$, заключаем, что и $\deg, b = \deg, c = 0$, т. е. $b, c \in K$, а потому $b, c \in K \setminus K^*$. Лемма доказана.

Л е м м а 5. *Пусть K – кольцо с однозначным разложением, $\ddot{K}$ – его поле частных. Тогда*: 1) *для всякого $f \in \ddot{K}[x]$ найдутся $\alpha \in \ddot{K}$ и примитивный многочлен g из $K[x]$ такие, что $f = \alpha g$*; 2) *эти α и g определяются единственным образом с точностью до множителя из K^**; 3) *многочлен f разложим в $\ddot{K}[x]$ тогда и только тогда, когда g разложим в $K[x]$.*

Д о к а з а т е л ь с т в о. 1) Докажем существование. Напомним, что

$$\ddot{K} = \left\{ \frac{a}{b} \mid a, b \in K, b \neq 0 \right\}.$$

Пусть

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \ldots + \frac{a_n}{b_n}x^n.$$

Вынося знаменатели всех коэффициентов, получим

$$f(x) = \frac{1}{b_0 b_1 \ldots b_n} F(x),$$

где

$$F(x) = a_0 b_1 b_2 \ldots b_n + a_1 b_0 b_2 \ldots b_n x + \ldots + a_n b_0 b_1 \ldots b_{n-1} x^n$$

– многочлен из $K[x]$. Пусть d – наибольший общий делитель его коэффициентов, т. е. $F(x) = dg(x)$, где $g(x)$ – примитивный многочлен из $K[x]$. Полагая $\alpha = \frac{d}{b_0 b_1 \ldots b_n}$, получим искомое разложение.

П р и м е р. Для многочлена

$$f(x) = \frac{15}{7}x^3 - \frac{30}{35}x + \frac{5}{7} = \frac{5}{35}\left(15x^3 - 6x + 5\right)$$

имеем $\alpha = \frac{5}{35}$ и $g(x) = 15x^3 - 6x + 5$.

2) Докажем единственность. Пусть $f = \alpha g$, где $\alpha \in \ddot{K}$, а g – примитивный многочлен из $K[x]$. С другой стороны, f имеет разложение $f = \alpha' g'$, где $\alpha' \in \ddot{K}$, а g' – примитивный многочлен из $K[x]$. Пусть $\alpha = \frac{c}{d}$, $\alpha' = \frac{c'}{d'}$ для некоторых c, d, c', d' из K. Тогда из равенства $\alpha g = \alpha' g'$, получим $cd'g = c'dg'$. Заметим, что наибольший общий делитель коэффициентов многочлена из левой части равен cd', а наибольший общий делитель коэффициентов многочлена из правой части равен $c'd$. По лемме 1 $cd' = \varepsilon c'd$, где $\varepsilon \in K^*$. Отсюда

$$\frac{c}{d} = \varepsilon \frac{c'}{d'},$$

т. е. $\alpha = \varepsilon\alpha'$. Из равенства $\alpha g = \alpha' g'$, заключаем, что $g' = \varepsilon g$.

3) Докажем импликацию $\Rightarrow$. Пусть f разложим в $\ddot{K}[x]$, т. е. $f = f_1 f_2$, где f_1 и f_2 – необратимые элементы в $\ddot{K}[x]$, т. е. f_1 и f_2 – многочлены ненулевой степени. Имеем

$$f = \alpha g, \quad f_1 = \alpha_1 g_1, \quad f_2 = \alpha_2 g_2,$$

где $\alpha, \alpha_1, \alpha_2 \in \ddot{K}$, g, g_1, g_2 – примитивные многочлены из $K[x]$. Отсюда $\alpha g = \alpha_1 \alpha_2 g_1 g_2$ и по лемме 2 многочлен $g_1 g_2$ является примитивным. По предположению леммы

о единственности разложения, $g = \varepsilon g_1 g_2$, $\varepsilon \in K^*$ и g_1, g_2 – многочлены ненулевой степени. Значит, g разложим в $K[x]$.

Докажем импликацию $\Leftarrow$. Пусть g разложим в $K[x]$, т. е. $g = g_1 g_2$, где g_1 и g_2 необратимы в $K[x]$. Так как g_1 и g_2 не являются обратимыми элементами кольца $K[x]$, то они не лежат в $K[x]^* = K^*$. Если $g_1 \in K$, то $g_2 \in K \setminus K^*$, но g_1 не может лежать в K так как это противоречит примитвности g, т. е. $g_1, g_2 \notin K$, а потому g_1 и g_2 являются нетривиальными многочленами (имеют степень больше нуля). Ввиду установленного пункта 1) имеем

$$f = \alpha g = \alpha g_1 g_2,$$

где αg_1 и g_2 – многочлены ненулевой степени, а потому мы построили нетривиальное разложение в $\ddot{K}[x]$. Следовательно, f разложим в $\ddot{K}[x]$. Лемма доказана.

Из этой леммы вытекает такое следствие, которое мы использовали при построении примера целостного кольца с неоднозначным разложением.

С л е д с т в и е. *Многочлен $f(x) \in \mathbb{Z}[x]$ разложим в $\mathbb{Z}[x]$ тогда и только тогда, когда он разложим в $\mathbb{Q}[x]$.*

Теперь мы готовы доказать основное утверждение настоящего параграфа.

Т е о р е м а 2. *Если K – кольцо с однозначным разложением, то $K[x]$ – кольцо с однозначным разложением.*

Д о к а з а т е л ь с т в о. Мы знаем, что $\ddot{K}[x]$ и K – кольца с однозначным разложением. Надо проверить, что кольцо $K[x]$ удовлетворяет определению кольца с однозначным разложением.

а) Пусть f – ненулевой, необратимый элемент из $K[x]$. Как элемент из $\ddot{K}[x]$ многочлен f разлогается на неразложимые сомножители:

$$f = f_1 f_2 \dots f_s,$$

где f_i – неразложимы и лежат в $\ddot{K}[x]$. Тогда по лемме 5

$$f_1 f_2 \dots f_s = (\alpha_1 g_1)(\alpha_2 g_2) \dots (\alpha_s g_s) = \alpha g_1 g_2 \dots g_s, \quad \alpha = \alpha_1 \alpha_2 \dots \alpha_s \in K,$$

где α_i лежат в $\ddot{K}$, а g_i – примитивные из $K[x]$. Учитывая, что K – кольцо с однозначным разложением, получим разложение в $K[x]$:

$$f = \alpha g_1 g_2 \dots g_s = \overline{\alpha}_1 \overline{\alpha}_2 \dots \overline{\alpha}_r g_1 g_2 \dots g_s,$$

где $\alpha = \overline{\alpha}_1 \overline{\alpha}_2 \dots \overline{\alpha}_r$, все $\overline{\alpha}_j$ неразложимы и лежат в K, что следует из леммы 4, а все элементы g_i неразложимы в $K[x]$, что следует из леммы 5. Таким образом, мы нашли разложение на неразложимые множители.

б) Пусть мы имеем два разложения на неразложимые множители:

$$f = \alpha_1\alpha_2\dots\alpha_r g_1 g_2\dots g_s = \alpha'_1\alpha'_2\dots\alpha'_{r'} g'_1 g'_2\dots g'_{s'}$$

где $\alpha_i, \alpha'_i \in K$, а g_j, g'_j – неразложимы в $K[x]$ и не лежат в K. Надо доказать, что число множителей в этих разложениях одинаково и сами множители ассоциированы.

Можно считать, что все g_j, g'_j примитивны. По лемме 5

$$\alpha_1\alpha_2\dots\alpha_r = \varepsilon\alpha'_1\alpha'_2\dots\alpha'_{r'}, \tag{1}$$

и

$$\varepsilon g_1 g_2\dots g_s = g'_1 g'_2\dots g'_{s'}. \tag{2}$$

По лемме 4 все α_i, α'_i неразложимы в K. Так как K – кольцо с однозначным разложением, то $r = r'$ и возможно после перенумерации:

$$\alpha_1 \text{ ассоциирован с } \varepsilon\alpha'_1 \text{ т. е. ассоциирован с } \alpha'_1,$$

$$\alpha_2 \text{ ассоциирован с } \alpha'_2,$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\alpha_r \text{ ассоциирован с } \alpha'_r.$$

Рассмотрим теперь разложение (2). В кольце $\ddot{K}[x]$ имеем $s = s'$ и возможно после перенумерации:

$$g_1 \text{ ассоциирован с } \varepsilon g_1 \text{ т. е. ассоциирован с } g'_1,$$

$$g_2 \text{ ассоциирован с } g'_2,$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$g_s \text{ ассоциирован с } g'_s.$$

Если $1g_j = \delta_j g'_j$, $\delta_j \in \left(\ddot{K}[x]\right)^* = \ddot{K}^*$, а так как $\delta_j = 1\varepsilon_j$, $\varepsilon_j \in K^*$ то $\delta_j \in K^* = K[x]^*$. Теорема доказана.

Из доказанной теоремы легко получается такое

С л е д с т в и е. *Всякое кольцо $K[x_1, x_2, \dots, x_n]$, где K – кольцо с однозначным разложением, тоже является кольцом с однозначным разложением. В частности, $\mathbb{Z}[x_1, x_2, \dots, x_n]$ и $P[x_1, x_2, \dots, x_n]$ являются кольцами с однозначным разложением.*

29.4. Неразложимые многочлены над $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ и $\mathbb{Z}$. Неразложимые многочлены над $\mathbb{C}$ – это линейные многочлены вида $x - \alpha$, $\alpha \in \mathbb{C}$, что следует из алгебраической замкнутости поля $\mathbb{C}$ и теоремы Безу. Действительно, так как всякий многочлен $f(x) \in \mathbb{C}[x]$ ненулевой степени имеет корень в $\mathbb{C}$, то

$$f(x) = (x - \alpha)g(x), \quad g(x) \in \mathbb{C}[x].$$

Многочлены первой степени уже неразложимы.

Многочлены, неразложимые над $\mathbb{R}$, могут быть первой и второй степени. Пусть $f(x) \in \mathbb{R}[x]$ и степень $\deg f \geq 3$. Если α – корень многочлена $f(x)$, то $\overline{\alpha}$ – также корень $f(x)$. Если $\alpha \in \mathbb{R}$, то по теореме Безу

$$f(x) = (x - \alpha)g(x), \quad g(x) \in \mathbb{R}[x].$$

Если $\alpha \notin \mathbb{R}$, то $\overline{\alpha} \neq \alpha$ и опять по теореме Безу

$$f(x) = (x - \alpha)(x - \overline{\alpha})h(x).$$

Рассмотрим многочлен

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha}) + \alpha\overline{\alpha}.$$

Так как $\alpha + \overline{\alpha} \in \mathbb{R}$ и $\alpha\overline{\alpha} = |\alpha|^2 \in \mathbb{R}$, то $(x-\alpha)(x-\overline{\alpha}) \in \mathbb{R}[x]$, а потому $f(x)$ делится на квадратичный многочлен с действительными коэффициентами, т. е. $f(x)$ разложим над $\mathbb{R}$.

Над полем $\mathbb{Q}$ существуют неразложимые многочлены любой степени.

У п р а ж н е н и е. Доказать, что для любого простого числа p и всякого натурального n многочлен $x^n - p$ неразложим над $\mathbb{Q}$.

Заметим, что если многочлен с целыми коэффициентами неразложим над $\mathbb{Q}$, то по следствию леммы 5 он неразложим и над $\mathbb{Z}$. Укажем алгоритм распознавания разложимости или неразложимости многочлена над $\mathbb{Z}$.

Пусть $f \in \mathbb{Z}[x]$ и n – его степень. Хотим проверить, представим ли он в виде $f = dh$. Можно считать, что $\deg d = N \leq \left[\frac{n}{2}\right]$, где $[a]$ – целая часть числа a. Выберем различные целые числа $x_0, x_1, \ldots, x_N$. Если $d(x)|f(x)$, то $d(x_i)|f(x_i)$, $i = 0, 1, \ldots, N$. Найдем все возможные делители $f(x_i)$. Затем по интерполяционной формуле Лагранжа найдем некоторый многочлен $p(x)$, пользуясь таблицей

x	x_0	$\ldots$	x_i	$\ldots$	x_N
$f(x)$	$f(x_0)$	$\ldots$	$f(x_i)$	$\ldots$	$f(x_N)$
$d(x)$	$d(x_0)$	$\ldots$	$d(x_i)$	$\ldots$	$d(x_N)$

т. е. $p(x_i) = d(x_i)$. Если $p(x) \mid f(x)$, то мы найдем разложение многочлена $f(x)$. Если, перебрав все такие делители, не найдем многочлена $p(x)$, который делит $f(x)$, то последний неразложим над $\mathbb{Z}$.