Глава V. Многочлены от одной переменной

§ 18. Многочлены и действия над ними

Б.М.Верников

Уральский федеральный университет,
Институт математики и компьютерных наук,
кафедра алгебры и дискретной математики

Определение

Пусть R — произвольное ассоциативно-коммутативное кольцо с 1. Обозначим через $R[x]$ множество всех последовательностей вида $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ с элементами из кольца R, в которых все элементы, начиная с некоторого, равны 0. Определим сумму и произведение последовательностей из $R[x]$ следующим образом: если $f = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ и $g = (\beta_0, \beta_1, \ldots, \beta_n, \ldots)$, то $f + g = (\gamma_0, \gamma_1, \ldots, \gamma_n, \ldots)$, а $fg = (\delta_0, \delta_1, \ldots, \delta_n, \ldots)$, где $\gamma_k = \alpha_k + \beta_k$ и $\delta_k = \sum\limits_{i+j=k} \alpha_i\beta_j$ для всякого $k \in \mathbb{N} \cup \{0\}$. Последовательности из $R[x]$ будем называть *многочленами* над кольцом R. Последовательность, все элементы которой равны 0, обозначим через o и назовем *нулевым* многочленом.

Как мы увидим позднее, многочлены в смысле данного только что определения — это то же самое, что многочлены от одной переменной в привычном смысле этого слова (разница только в том, что коэффициенты у них могут лежать не в поле $\mathbb{R}$, а в произвольном кольце R).

Замечание о сумме и произведении многочленов

Сумма и произведение двух многочленов над кольцом R являются многочленами над R.

Доказательство. Пусть $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ и $g = (\beta_0, \beta_1, \dots, \beta_n, \dots)$ — многочлены над кольцом R. Существуют такие числа q и r, что $\alpha_n = 0$ для всех $n \geqslant q$ и $\beta_n = 0$ для всех $n \geqslant r$. Положим $f + g = (\gamma_0, \gamma_1, \dots, \gamma_n, \dots)$ и $fg = (\delta_0, \delta_1, \dots, \delta_n, \dots)$. Тогда, очевидно, $\gamma_n = 0$ для всех $n \geqslant \max\{q, r\}$ и $\delta_n = 0$ для всех $n \geqslant q + r$. Следовательно, $f + g, fg \in R[x]$. $\square$

Лемма о кольце многочленов

Множество всех многочленов над кольцом R с операциями сложения и умножения многочленов является ассоциативно-коммутативным кольцом с 1.

Доказательство. Сложение и умножение многочленов над кольцом R являются бинарными операциями на множестве $R[x]$ (см. замечание на предыдущем слайде). Поскольку $\langle R; +\rangle$ — абелева группа, из определения суммы многочленов вытекает, что $\langle R[x]; +\rangle$ также является абелевой группой (нейтральным по сложению элементом является нулевой многочлен). Из определения произведения многочленов непосредственно вытекает, что умножение многочленов коммутативно, а $(1, 0, \ldots, 0, \ldots)$ — нейтральный элемент по умножению. Проверим ассоциативность умножения. Пусть $f = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$, $g = (\beta_0, \beta_1, \ldots, \beta_n, \ldots)$ и $h = (\gamma_0, \gamma_1, \ldots, \gamma_n, \ldots)$. Тогда $f \cdot g = (\delta_0, \delta_1, \ldots, \delta_n, \ldots)$, где $\delta_m = \sum\limits_{k+\ell=m} \alpha_k\beta_\ell$ и $g \cdot h = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n, \ldots)$, где $\varepsilon_r = \sum\limits_{s+t=r} \beta_s\gamma_t$.
Следовательно, $(fg)h = (\mu_0, \mu_1, \ldots, \mu_n, \ldots)$, где

$$\mu_d = \sum_{m+t=d} \delta_m\gamma_t = \sum_{m+t=d} \left(\sum_{k+\ell=m} \alpha_k\beta_\ell\right)\gamma_t = \sum_{k+\ell+t=d} \alpha_k\beta_\ell\gamma_t.$$

Аналогично, $f(gh) = (\nu_0, \nu_1, \ldots, \nu_n, \ldots)$, где

$$\nu_d = \sum_{k+r=d} \alpha_k \varepsilon_r = \sum_{k+r=d} \alpha_k \left(\sum_{s+t=r} \beta_s \gamma_t \right) = \sum_{k+s+t=d} \alpha_k \beta_s \gamma_t .$$

Сравнивая полученные выражения для μ_d и ν_d, получаем требуемое равенство $f(gh) = (fg)h$.

Осталось проверить дистрибутивность умножения относительно сложения. В силу коммутативности умножения, достаточно доказать равенство $(f+g)h = fh + gh$. Ясно, что $(f+g)h = (\mu_0, \mu_1, \ldots, \mu_n, \ldots)$, где

$$\mu_d = \sum_{k+\ell=d} (\alpha_k + \beta_k)\gamma_\ell .$$

С другой стороны, $fh = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n, \ldots)$, где $\varepsilon_m = \sum\limits_{s+t=m} \alpha_s \gamma_t$, а $gh = (\xi_0, \xi_1, \ldots, \xi_n, \ldots)$, где $\xi_m = \sum\limits_{s+t=r} \beta_s \gamma_t$. Следовательно, $fh + gh = (\nu_0, \nu_1, \ldots, \nu_n, \ldots)$, где

$$\nu_d = \varepsilon_d + \xi_d = \sum_{s+t=d} (\alpha_s \gamma_t + \beta_s \gamma_t) = \sum_{s+t=d} (\alpha_s + \beta_s)\gamma_t .$$

Сравнивая полученные выражения для μ_d и ν_d, получаем требуемое равенство $(f+g)h = fh + gh$.

Определение

Пусть $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$. Если $f \neq o$, то существует $m \in \mathbb{N} \cup \{0\}$ такое что $\alpha_m \neq 0$ и $\alpha_k = 0$ для любого $k > m$. Число m называется *степенью* многочлена f и обозначается через $\deg f$. Степень нулевого многочлена по определению равна $-\infty$, причем символ $-\infty$ меньше любого целого числа и $m + (-\infty) = -\infty + m = -\infty$ для любого целого m.

Лемма о многочленах нулевой степени

Совокупность всех многочленов степени $\leqslant 0$ из кольца $R[x]$ образует подкольцо этого кольца, изоморфное кольцу R.

Доказательство. Многочлены нулевой степени — это последовательности вида $(\alpha, 0, \dots, 0, \dots)$, где $\alpha \neq 0$, и только они, а единственный многочлен, степень которого меньше нуля, — это нулевой многочлен. Таким образом, многочлены степени $\leqslant 0$ — это последовательности вида $(\alpha, 0, \dots, 0, \dots)$ и только они. Очевидно, что такие последовательности образуют подкольцо в $R[x]$. Из определения суммы и произведения многочленов с очевидностью вытекает, что отображение $\varphi\colon R \longrightarrow R[x]$, заданное правилом $\varphi(\alpha) = (\alpha, 0, \dots, 0, \dots)$, является изоморфизмом из R на это подкольцо. □

Последовательность $(0, 1, 0, \dots, 0, \dots)$ обозначим через x. По индукции положим $x^m = x^{m-1} \cdot x$ для всякого натурального $m > 1$. Легко проверить, что $x^m = x^{m-1} \cdot x = (\underbrace{0, 0, \dots, 0}_{m \text{ элементов}}, 1, 0, \dots, 0, \dots)$ и

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0 = (\alpha_0, \alpha_1, \dots, \alpha_n, 0, \dots, 0, \dots)$$

для любых $\alpha_0, \alpha_1, \dots, \alpha_n \in R$. Таким образом, многочлен $(\alpha_0, \alpha_1, \dots, \alpha_n, 0, \dots, 0, \dots)$ можно записывать в виде $\alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$. В дальнейшем мы будем придерживаться этой привычной записи многочленов.

Определение

Элементы $\alpha_0, \alpha_1, \dots, \alpha_n$ называются *коэффициентами* многочлена $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$. Если $\alpha_n \neq 0$, то $n = \deg f$, $\alpha_n x^n$ называется *старшим членом* многочлена f и обозначается через $\mathrm{lm}(f)$, а α_n называется *старшим коэффициентом* многочлена f и обозначается через $\mathrm{lc}(f)$. Элемент α_0 называется *свободным членом* многочлена f.

Замечание о степени произведения и суммы многочленов

Если f и g — многочлены над полем F, то

1) $\deg(fg) = \deg f + \deg g$,
2) *если* $\deg f \neq \deg g$, *то* $\deg(f+g) = \max\{\deg f, \deg g\}$,
3) *если* $\deg f = \deg g$, *то* $\deg(f+g) \leqslant \deg f$.

Доказательство. Пусть $\mathrm{lm}(f) = ax^n$, а $\mathrm{lm}(g) = bx^m$. В частности, $a, b \neq 0$.

1) Очевидно, что в многочлене fg все коэффициенты при x^k, где $k > n+m$, равны 0, а коэффициент при x^{n+m} равен ab. Поскольку F — поле, имеем $ab \neq 0$. Следовательно, $\deg(fg) = n+m = \deg f + \deg g$.

2) Положим $r = \max\{n, m\}$. Очевидно, что в многочлене $f+g$ все коэффициенты при x^k, где $k > r$, равны 0, а коэффициент при x^r равен либо a, либо b. В частности, последний коэффициент отличен от 0. Следовательно, $\deg(f+g) = r = \max\{\deg f, \deg g\}$.

3) Очевидно, что в данном случае в многочлене $f+g$ все коэффициенты при x^k, где $k > n$, равны 0. Отсюда вытекает требуемое заключение. □

Отметим, что если $\deg f = \deg g = n$, то $\deg(f+g) < \deg f$ тогда и только тогда, когда $\mathrm{lc}(f) = -\mathrm{lc}(g)$ (так как в этом и только этом случае коэффициент при x^n в $f+g$ равен 0).

Замечание о необратимых многочленах

Ненулевой многочлен f над полем F является необратимым элементом кольца $F[x]$ тогда и только тогда, когда $\deg f \geqslant 1$.

Доказательство. Необходимость. Предположим, что $\deg f \leqslant 0$. Это означает, что $f \in F$. Учитывая, что $f \neq o$, а F — поле, получаем, что многочлен f обратим. Следовательно, если f необратим, то $\deg f \geqslant 1$.

Достаточность. Предположим, что f обратим. Тогда $fg = 1$ для некоторого $g \in F[x]$. Следовательно, $\deg f + \deg g = \deg(fg) = \deg 1 = 0$, откуда $\deg f \leqslant 0$. Следовательно, если $\deg f \geqslant 1$, то f необратим. □

Теорема о делении многочленов с остатком

Пусть F — поле и $f, g \in F[x]$, причем $g \neq o$. Тогда существуют такие однозначно определенные многочлены $q, r \in F[x]$, что

$$f = qg + r \text{ и } \deg r < \deg g. \tag{1}$$

Доказательство. Существование многочленов q и r. По условию $\deg g \geqslant 0$. Если $\deg g = 0$, то $g \in F$. При этом $g \neq 0$. Имеем $f = f \cdot \frac{g}{g} = \frac{f}{g} \cdot g$ и равенство (1) выполнено при $q = \frac{f}{g}$ и $r = 0$. Предположим теперь, что $\deg g > 0$. Существование многочленов q и r в этом случае докажем индукцией по $\deg f$.

При $\deg f < \deg g$ достаточно положить $q = 0$, $r = f$. Пусть теперь $\deg f = m \geqslant \deg g$. В частности, $m > 0$. Предположим, что для любого многочлена p степени $< m$ существуют многочлены a и b такие, что $p = ag + b$ и $\deg b < \deg g$. Пусть $\alpha = \mathrm{lc}(f)$ и $\beta = \mathrm{lc}(g)$. Имеем $f = \alpha x^m + f_1$ и $g = \beta x^k + g_1$, где $\deg f_1 < m$, $\deg g_1 < k$ и $\alpha, \beta \neq 0$. Положим $h = \frac{\alpha}{\beta} \cdot x^{m-k}$. Тогда $hg = \alpha x^m + hg_1$, откуда $f - hg = f_1 - hg_1$. Используя замечание о степени произведения и суммы многочленов, имеем $\deg(hg_1) = \deg h + \deg g_1 < m - k + k = m$, и потому $\deg(f - hg) = \deg(f_1 - hg_1) \leqslant \max\{\deg f_1, \deg(hg)_1\} < m$. Применяя к многочлену $f - hg$ предположение индукции, констатируем существование многочленов q и r таких что $f - hg = qg + r$ и $\deg r < \deg g$. Теперь ясно, что $f = (h + q)g + r$.

Единственность многочленов q и r. Предположим, что $f = q_1 g + r_1$ и $f = q_2 g + r_2$ для некоторых многочленов q_1, q_2, r_1 и r_2 таких что $\deg r_1, \deg r_2 < \deg g$. Из равенства $q_1 g + r_1 = q_2 g + r_2$ получаем $(q_1 - q_2)g = r_2 - r_1$. Но если $q_1 - q_2 \neq 0$, то это невозможно, так как $\deg\big((q_1 - q_2)g\big) \geqslant \deg g$, а $\deg(r_2 - r_1) < \deg g$. Следовательно, $q_1 - q_2 = 0$, откуда $q_1 = q_2$ и $r_1 = r_2$. □

Определение

Если выполнено равенство (1), то многочлен q называется *частным*, а многочлен r — *остатком* от деления (с остатком) f на g. Если $r = 0$, то говорят, что многочлен f *делится* на многочлен g; в этом случае $f = qg$. При этом говорят также, что многочлен g *делит* многочлен f; этот факт будет обозначаться через $g \mid f$.

Следующее утверждение проверяется непосредственно.

Предложение о свойствах делимости многочленов

Пусть $f, g, g_1, g_2, h \in R[x]$. Если $f \mid g$, то $f \mid (gh)$, а если $f \mid g_1$ и $f \mid g_2$, то $f \mid (g_1 + g_2)$. □

Очевидно, что

! *отношение делимости на множестве $R[x]$ рефлексивно и транзитивно, т. е. является отношением квазипорядка.* $\square$

В то же время, если R — поле, то это отношение не антисимметрично, поскольку в этом случае многочлены f и αf, где $\alpha \in R \setminus \{0, 1\}$, делят друг друга, но различны. В соответствии с общим понятием ассоциированных элементов квазиупорядоченного множества (см. конец § 2), будем называть многочлены f и g из $R[x]$ *ассоциированными*, если $f \mid g$ и $g \mid f$.

Замечание об ассоциированных многочленах

Ненулевые многочлены f и g над полем F ассоциированы тогда и только тогда, когда $f = \alpha g$ для некоторого $\alpha \in F \setminus \{0\}$.

Доказательство. Необходимость. Если f и g ассоциированы, то $f = \alpha g$ и $g = \beta f$ для некоторых $\alpha, \beta \in F[x]$. Следовательно, $\deg f = \deg g + \deg \alpha$ и $\deg g = \deg f + \deg \beta$, откуда $\deg f = \deg f + \deg \alpha + \deg \beta$. Следовательно, $\deg \alpha = \deg \beta = 0$, т. е. $\alpha, \beta \in F$. Кроме того, $f = \alpha g = \alpha\beta f$. Поскольку $f \neq o$, получаем, что $\alpha\beta \neq 0$. В частности, $\alpha \neq 0$.

Достаточность. Если $f = \alpha g$ и $\alpha \neq 0$, то $g = \frac{1}{\alpha} \cdot f$. Из первого равенства вытекает, что $f \mid g$, а из второго — что $g \mid f$. $\square$

Из доказательства теоремы о делении многочлена с остатком можно извлечь следующий

Алгоритм деления многочлена на многочлен

Пусть f и g — многочлены над полем F,

$$f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \text{ и } g = \beta_m x^m + \beta_{m-1} x^{m-1} + \cdots + \beta_1 x + \beta_0,$$

причем $\alpha_n, \beta_m \neq 0$ и $n \geqslant m > 0$. Положим $q = 0$. Заменим многочлен f на многочлен $f_1 = f - \frac{\alpha_n}{\beta_m} \cdot x^{n-m} g$, а многочлен q — на многочлен $q + \frac{\alpha_n}{\beta_m} \cdot x^{n-m}$. Будем повторять эти действия до тех пор, пока выполняется неравенство $\deg f_1 \geqslant m$. Так как степень f_1 на каждом шаге уменьшается на m, алгоритм закончит работу. При этом частное будет равно q, а остаток – последнему значению f_1.

Определение

Пусть F — поле и $f, g \in F[x]$. Многочлен $h \in F[x]$ называется *наибольшим общим делителем* (НОД) многочленов f и g, если $h \mid f$, $h \mid g$ и для любого $p \in F[x]$ из того, что $p \mid f$ и $p \mid g$ следует, что $p \mid h$.

Следующее замечание показывает, что НОД двух многочленов определен не однозначно, а с точностью до ассоциированности.

Замечание о многочленах, ассоциированных с НОД

Пусть d — НОД *многочленов f и g. Многочлен e также является* НОД *многочленов f и g тогда и только тогда, когда он ассоциирован с d.*

Доказательство. Необходимость. Пусть d и e — наибольшие общие делители многочленов f и g. Тогда каждый из многочленов d и e делит как f, так и g. По определению НОД это означает, что многочлены d и e делят друг друга, т. е. ассоциированы.

Достаточность. Пусть d — НОД многочленов f и g, а многочлен e ассоциирован с d. Из того, что d делит f и g, а e делит d, вытекает, что e делит f и g. Далее, если h делит f и g, то d делит h, а поскольку e делит d, то и e делит h. Следовательно, e — НОД f и g. $\square$

Теорема о наибольшем общем делителе

Для любых ненулевых многочленов f и g над полем F существует НОД d *и существуют многочлены $u, v \in F[x]$ такие, что*

$$d = uf + vg. \tag{2}$$

Правая часть равенства (2) называется *линейной формой* НОД. В доказательстве теоремы о наибольшем общем делителе содержится *алгоритм Евклида* построения НОД двух многочленов.

Доказательство. Без ограничения общности предположим, что $\deg f \geqslant \deg g$. Применяя теорему о делении многочленов с остатком, запишем равенства:

$$\left.\begin{array}{l} f = q_1 g + r_1, \ r_1 \neq 0, \ \deg r_1 < \deg g; \\ g = q_2 r_1 + r_2, \ r_2 \neq 0, \ \deg r_2 < \deg r_1; \\ r_1 = q_3 r_2 + r_3, \ r_3 \neq 0, \ \deg r_3 < \deg r_2; \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ r_{k-1} = q_{k+1} r_k + r_{k+1}, \ r_{k+1} \neq 0, \ \deg r_{k+1} < \deg r_k; \\ r_k = q_{k+2} r_{k+1}. \end{array}\right\} \tag{3}$$

Поскольку $\deg g, \deg r_1, \deg r_2, \dots \in \mathbb{N} \cup \{0\}$ и $\deg g > \deg r_1 > \deg r_2 > \cdots$, этот процесс должен завершиться получением нулевого остатка.

Докажем, что r_{k+1} является НОД многочленов f и g. Поднимаясь по цепочке равенств (3) снизу вверх, покажем, что $r_{k+1} \mid f$ и $r_{k+1} \mid g$. Из последнего равенства получаем, что $r_{k+1} \mid r_k$, из предпоследнего в силу предложения о свойствах делимости многочленов — что $r_{k+1} \mid r_{k-1}$, из каждого последующего рассматриваемого равенства $r_s = q_{s+2}r_{s+1} + r_{s+2}$, получаем по предложению о свойствах делимости многочленов, что $r_{k+1} \mid r_s$, так как уже доказано, что $r_{k+1} \mid r_{s+1}$ и $r_{k+1} \mid r_{s+2}$. Дойдя до второго и первого равенства, получим $r_{k+1} \mid g$ и $r_{k+1} \mid f$.

Опускаясь по цепочке равенств (3) сверху вниз, покажем, что если $h \mid f$ и $h \mid g$, то $h \mid r_{k+1}$. Пусть $h \mid f$ и $h \mid g$. Из первого равенства получаем $r_1 = f - q_1 g$; по предложению о свойствах делимости многочленов получаем $h \mid r_1$. Рассматривая следующее равенство, получаем $r_2 = g - q_2 r_1$, откуда в силу предложения о свойствах делимости многочленов следует , что $h \mid r_2$. Опускаясь по цепочке равенств (3) сверху вниз, получим, что $h \mid r_s$ при $s = 3, \ldots, k+1$.

Осталось доказать равенство (2). Из предпоследнего равенства в системе (3) вытекает, что $r_{k+1} = r_{k-1} - q_{k+1} r_k$. Подставим в это равенство выражение $r_k = r_{k-2} - q_k r_{k-1}$, полученное из предыдущего равенства системы (3). Получим:

$$r_{k+1} = r_{k-1} - q_{k+1}(r_{k-2} - q_k r_{k-1}) = -q_{k+1} r_{k-2} + (q_{k+1} q_k + 1) r_{k-1}.$$

Алгоритм Евклида (3)

Полагая $u_2 = -q_{k+1}$, $v_2 = q_{k+1}q_k + 1$, имеем $r_{k+1} = u_2 r_{k-2} + v_2 r_{k-1}$. Подставляя в это равенство выражение $r_{k-1} = r_{k-3} - q_{k-1}r_{k-2}$, полученное из соответствующего равенства системы (3), получим

$$r_{k+1} = u_2 r_{k-2} + v_2(r_{k-3} - q_{k-1}r_{k-2}) = v_2 r_{k-3} + (u_2 - v_2 q_{k-1})r_{k-2}.$$

Следовательно, $r_{k+1} = u_3 r_{k-3} + v_3 r_{k-2}$, где $u_3 = v_2$, а $v_3 = u_2 - v_2 q_{k-1}$. Продолжая движение снизу вверх, на каждом шаге будем получать равенство $r_{k+1} = u_s r_{k-s} + v_s r_{k-s+1}$ для некоторых u_s и v_s, где $s = 4, \ldots, k-1$. При $s = k-1$ получаем $r_{k+1} = u_{k-1}r_1 + v_{k-1}r_2$. Подставляя в это равенство выражение $r_2 = g - q_2 r_1$, полученное из второго равенства системы (3), получаем

$$r_{k+1} = u_{k-1}r_1 + v_{k-1}(g - q_2 r_1) = v_{k-1}g + (u_{k-1} - v_{k-1}q_2)r_1.$$

Подставляя в равенство $r_{k+1} = v_{k-1}g + (u_{k-1} - v_{k-1}q_2)r_1$ выражение $r_1 = f - q_1 g$, полученное из первого равенства системы (3), окончательно имеем

$$\begin{aligned} r_{k+1} &= v_{k-1}g + (u_{k-1} - v_{k-1}q_2)(f - q_1 g) = \\ &= (u_{k-1} - v_{k-1}q_2)f + \big(v_{k-1}(1 + q_1 q_2) - u_{k-1}q_1\big)g. \end{aligned}$$

Полагая $u = u_{k-1} - v_{k-1}q_2$ и $v = v_{k-1}(1 + q_1 q_2) - u_{k-1}q_1$, получаем $r_{k+1} = uf + vg$. Поскольку, как показано выше, r_{k+1} является НОД многочленов f и g, это завершает доказательство. $\square$

Определение

Многочлены f и g над полем F называются *взаимно простыми*, если 1 является их НОД.

Учитывая замечание об ассоциированных многочленах и замечание о многочленах, ассоциированых с НОД, мы видим, что

!! *если многочлены f и g над полем F взаимно просты, то любой ненулевой элемент из F является их* НОД. В этой ситуации мы будем для краткости писать $\text{НОД}(f, g) = 1$.

Из теоремы о наибольшем общем делителе вытекает

Следствие о взаимно простых многочленах

Многочлены f и g над полем F являются взаимно простыми тогда и только тогда, когда существуют многочлены $u, v \in F[x]$ такие, что

$$uf + vg = 1. \tag{4}$$

Доказательство. Необходимость обеспечивается равенством (2).

Достаточность. Пусть выполнено равенство (4). Предположим, что h — общий делитель многочленов f и g, т. е. $f = hp$ и $g = hq$ для некоторых многочленов p и q. Тогда

$$1 = uf + vg = uph + vqh = (up + vq)h,$$

т. е. h делит 1. Следовательно, НОД$(f, g) = 1$. □

Предложение о взаимно простых многочленах

Пусть f, g и h — многочлены над полем F.

1) *Если f и g взаимно просты, $f \mid h$ и $g \mid h$, то $(fg) \mid h$.*
2) *Если f и g взаимно просты и $f \mid (gh)$, то $f \mid h$.*
3) *Если f и h взаимно просты и g и h взаимно просты, то fg и h взаимно просты.*

Доказательство. 1) Пусть $h = fp$ и $h = gq$ для некоторых над многочленов p и q. Так как f и g взаимно просты, в силу следствия о взаимно простых многочленах существуют многочлены u и v такие, что выполняется равенство (4). Умножая обе части этого равенства на h, получим $h = huf + hvg$, откуда $h = gquf + fpvg = fg(qu + pv)$.

2) По условию $gh = fp$ для некоторого многочлена p. В силу следствия о взаимно простых многочленах $uf + vg = 1$ для некоторых многочленов u и v. Следовательно, $huf + hvg = h$, откуда $h = huf + fpv = f(hu + pv)$. Следовательно, f делит h.

3) В силу следствия о взаимно простых многочленах $uf + vh = 1$ для некоторых многочленов u и v. Следовательно, $ufg + vhg = g$. Предположим, что $p = \text{НОД}(fg, h) \neq 1$. Тогда, с одной стороны, p делит h, а значит и vhg, а с другой, p делит fg, а значит и ufg. Следовательно, p делит $vgh + ufg = g$. Но это противоречит взаимной простоте g и h. Следовательно, $\text{НОД}(fg, h) = 1$. $\square$

Пусть $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ — многочлен над кольцом R. Многочлен f можно рассматривать как отображение из кольца R в себя, сопоставляющее каждому элементу $\xi \in R$ элемент $f(\xi) \in R$, определяемый равенством

$$f(\xi) = \alpha_n \xi^n + \alpha_{n-1}\xi^{n-1} + \cdots + \alpha_1 \xi + \alpha_0.$$

Элемент $f(\xi)$ называется *значением многочлена* $f(x)$ в кольце R при $x = \xi$.

Пусть $f(x)$ — многочлен степени $n \geq 1$ над полем F, $\alpha \in F$, а $q(x)$ и $r(x)$ — частное и остаток от деления многочлена $f(x)$ на $x - \alpha$ соответственно. Тогда $\deg r(x) < \deg(x - \alpha) = 1$, т. е. $\deg r(x) \leq 0$. С другой стороны, $\deg\big(q(x)(x-\alpha)\big) \geq \deg(x - \alpha) = 1$. Учитывая замечание о степени произведения и суммы многочленов, имеем:

$$\deg f(x) = \deg\big(q(x)(x-\alpha) + r(x)\big) = \deg\big(q(x)(x-\alpha)\big) = \\ = \deg q(x) + \deg(x-\alpha) = \deg q(x) + 1,$$

откуда $\deg q(x) = \deg f(x) - 1 = n - 1$.

Теорема Безу

Пусть $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$ — многочлен над полем F и $\alpha \in F$.

(i) *Остаток от деления $f(x)$ на $x - \alpha$ равен $f(\alpha)$.*

(ii) *Обозначим частное от деления $f(x)$ на $x - \alpha$ через $b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_0$. Тогда*

$$b_{n-1} = a_n,\ b_k = a_{k+1} + \alpha b_{k+1} \text{ при } k = 0, 1, \dots, n-2 \\ \text{и } f(\alpha) = a_0 + \alpha b_0. \tag{5}$$

Доказательство. Обозначим частное и остаток от деления $f(x)$ на $x - \alpha$ через $q(x)$ и $r(x)$ соответственно. Тогда $f(x) = q(x)(x - \alpha) + r(x)$, где $\deg r < \deg(x - \alpha)$. Последнее означает, что $\deg r \leqslant 0$, т. е. $r \in F$. Подставив α вместо x в равенство $f(x) = q(x)(x - \alpha) + r(x)$, имеем $f(\alpha) = q(\alpha) \cdot 0 + r$, откуда $r = f(\alpha)$. Учитывая, что

$$
\begin{aligned}
&a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = \\
&= (b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1 x + b_0)(x - \alpha) + f(\alpha) = \\
&= b_{n-1}x^n + (-\alpha b_{n-1} + b_{n-2})x^{n-1} + \dots + (-\alpha b_1 + b_0)x + \big(-\alpha b_0 + f(\alpha)\big),
\end{aligned}
$$

получаем, что $b_{n-1} = a_n$, $-\alpha b_{n-1} + b_{n-2} = a_{n-1}$, $\dots$, $-\alpha b_1 + b_0 = a_1$, $-\alpha b_0 + f(\alpha) = a_0$, откуда вытекают равенства (5). $\square$

- Равенства (5) указывают простой способ вычисления всех коэффициентов частного от деления $f(x)$ на $x - \alpha$ и остатка от этого деления по коэффициентам многочлена $f(x)$ и скаляру α: сначала по формулам $b_{n-1} = a_n$, $b_{n-2} = a_{n-1} + \alpha b_{n-1}$, $\dots$, $b_0 = a_1 + \alpha b_1$ последовательно находятся коэффициенты частного, а затем по формуле $f(\alpha) = a_0 + \alpha b_1$ вычисляется остаток.

Определение

Пусть $f(x)$ — многочлен над полем F. Элемент $\alpha \in F$ называется *корнем* многочлена $f(x)$, если $f(\alpha) = 0$ (другими словами, если α — корень уравнения $f(x) = 0$).

Из теоремы Безу вытекает

Следствие из теоремы Безу

Пусть $f(x)$ — многочлен над полем F и $\alpha \in F$. Элемент α является корнем многочлена $f(x)$ тогда и только тогда, когда $f(x) = q(x)(x - \alpha)$ для некоторого многочлена $q(x) \in F[x]$.

Доказательство. Достаточность очевидна: если $f(x) = q(x)(x - \alpha)$, то $f(\alpha) = q(\alpha)(\alpha - \alpha) = q(\alpha) \cdot 0 = 0$.

Необходимость. Пусть α — корень многочлена $f(x)$. В силу теоремы Безу $f(x) = q(x)(x - \alpha) + f(\alpha)$ для некоторого многочлена $q(x)$. Следовательно,

$$0 = f(\alpha) = q(\alpha)(\alpha - \alpha) + f(\alpha) = q(\alpha) \cdot 0 + f(\alpha) = 0 + f(\alpha) = f(\alpha).$$

Следствие доказано. □

Кратность корня многочлена

Определение

Натуральное число k называется *кратностью* корня α многочлена $f(x)$, если $f(x) = g(x)(x-\alpha)^k$ для некоторого многочлена $g(x)$ такого, что $g(\alpha) \neq 0$.

Если многочлен $f(x)$ степени > 0 над полем F имеет в этом поле m корней $\alpha_1, \alpha_2, \ldots, \alpha_m$ и кратность корня α_i равна k_i, где $i = 1, 2, \ldots, m$, то $f(x)$ делится на $(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_m)^{k_m}$. Поэтому $k_1 + k_2 + \cdots + k_m \leqslant \deg f$. Ясно также, что число корней многочлена не превосходит суммы их кратностей. Следовательно,

- *как число корней многочлена степени > 0, так и сумма кратностей всех его корней, не могут быть больше степени многочлена.* $\square$