Глава III. Многочлены от одной переменной

§ 10. Многочлены как последовательности. Делимость многочленов

Б.М.Верников

Уральский федеральный университет,
Институт естественных наук и математики,
кафедра алгебры и фундаментальной информатики

10.1. Кольцо многочленов

Многочлены, как и целые числа, можно делить друг на друга с остатком. В частности, один многочлен может делиться на другой (без остатка). Изучение связанных с этим вопросов и является основной темой данного параграфа. Но начинается он с определения многочленов и рассмотрения их простейших свойств.

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 $\delta_k = \alpha_0\beta_k + \alpha_1\beta_{k-1} + \cdots + \alpha_{k-1}\beta_1 + \alpha_k\beta_0$ 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.

Многочлены как последовательности (2)

Как мы увидим позднее, многочлены в смысле данного на предыдущем слайде 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 ассоциативно-коммутативном кольце R с 1).

Проверим, что сумма и произведение многочленов над одним и тем же кольцом R являются алгебраическими операциями на множестве $R[x]$.

Замечание 10.1

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 $fg = (\delta_0, \delta_1, \dots, \delta_n, \dots)$, где γ_i и δ_i имеют тот же смысл, что в определении многочлена. Тогда, очевидно, $\gamma_n = 0$ для всех $n \geqslant \max\{q, r\}$ и $\delta_n = 0$ для всех $n \geqslant q + r$. Следовательно, $f + g, fg \in R[x]$. □

Лемма 10.1

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

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

Кольцо многочленов (2)

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 $\varepsilon_m = \sum_{s+t=m} \alpha_s \gamma_t$, а $gh = (\xi_0, \xi_1, \ldots, \xi_n, \ldots)$, где $\xi_m = \sum_{s+t=m} \beta_s \gamma_t$. 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 $(f+g)h = fh + gh$.

Кольцо многочленов (3)

Определение

Кольцо $R[x]$ называется *кольцом многочленов над кольцом* R.

Степень многочлена. Вложение кольца R в $R[x]$

Определение

Пусть $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ — произвольный многочлен. 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. Степень нулевого многочлена по определению равна $-\infty$, причем мы считаем, что $-\infty < m$ и $m + (-\infty) = -\infty + m = -\infty$ для любого целого m. Степень многочлена f обозначается через $\deg f$.

Лемма 10.2

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.

Привычная запись многочленов

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

Определения

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 $\ell m(f)$, а α_n называется *старшим коэффициентом* многочлена f и обозначается через $\ell c(f)$. Элемент α_0 называется *свободным членом* многочлена f.

Степень произведения и суммы многочленов (1)

Замечание 10.2

Пусть f и g — ненулевые многочлены над кольцом R.

1) $\deg(fg) \leqslant \deg f + \deg g$; *при этом* $\deg(fg) = \deg f + \deg g$ *тогда и только тогда, когда R — область целостности.*
2) *Если* $\deg f \neq \deg g$, *то* $\deg(f+g) = \max\{\deg f, \deg g\}$.
3) *Если* $\deg f = \deg g$, *то* $\deg(f+g) \leqslant \deg f$; *при этом* $\deg(f+g) = \deg f$ *тогда и только тогда, когда* $\ell c(f) \neq -\ell c(g)$.

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

1) Очевидно, что в многочлене fg все коэффициенты при x^k, где $k > n+m$, равны 0. Следовательно, $\deg(fg) \leqslant \deg f + \deg g$. Коэффициент при x^{n+m} в многочлене fg равен ab. Если R — область целостности, то $ab \neq 0$, и потому $\deg(fg) = n+m = \deg f + \deg g$. Если же R не является областью целостности, то существуют ненулевые элементы $c, d \in R$ такие, что $cd = 0$. Положим $f = cx^n$, а $g = dx^m$. Тогда $fg = o$ и $\deg(fg) = -\infty \neq n+m = \deg f + \deg g$.

Степень произведения и суммы многочленов (2)

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, что $\deg(f + g) \leqslant \deg f$. Коэффициент при x^n в многочлене $f + g$ равен $a + b$. Ясно, что он равен нулю (и потому $\deg(f + g) < \deg f$) тогда и только тогда, когда $a = -b$, т. е. $\ell c(f) = -\ell c(g)$. □

Замечание 10.3

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. □

10.2. Деление многочлена на многочлен с остатком

Теорема 10.1

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 $g \neq 0$. Следовательно, существует многочлен g^{-1}. Имеем $f = f \cdot 1 = f(g^{-1}g) = (fg^{-1})g$ и равенство (1) выполнено при $q = fg^{-1}$ и $r = o$.

Теорема о делении многочленов с остатком (2)

Предположим теперь, что $\deg g > 0$. При $\deg f < \deg g$ достаточно положить $q = o$ и $r = f$. Пусть теперь $\deg f \geqslant \deg g$, $\deg f = k$, $\deg g = m$, $\ell c(f) = \alpha$ и $\ell c(g) = \beta$. В частности, $k \geqslant m$. Положим $q_1 = \frac{\alpha}{\beta} x^{k-m}$ и $r_1 = f - q_1 g$. Тогда $\ell m(q_1 g) = \ell m(f)$, и потому $\deg r_1 < \deg f$. Итак, существуют такие многочлены q_1 и r_1, что $f = q_1 g + r_1$ и $\deg r_1 < \deg f$. Если $\deg r_1 < \deg g$, то требуемое утверждение выполнено при $q = q_1$ и $r = r_1$.

Пусть теперь $\deg r_1 \geqslant \deg g$. Тогда можно подобрать такой многочлен q_2, что $\ell m(q_2 g) = \ell m(r_1)$. Положим $r_2 = r_1 - q_2 g$. Тогда $\deg r_2 < \deg r_1$, $r_1 = q_2 g + r_2$ и $f = q_1 g + r_1 = q_1 g + q_2 g + r_2 = (q_1 + q_2) g + r_2$. Если $\deg r_2 < \deg g$, то требуемое утверждение выполнено при $q = q_1 + q_2$ и $r = r_2$.

Если $\deg r_2 \geqslant \deg g$, продолжим этот процесс. На каждом шаге будут строиться одночлен r_k и многочлен q_k такие, что $\deg r_k < \deg r_{k-1}$ и $f = (q_1 + q_2 + \cdots + q_k) g + r_k$. Поскольку $\deg r_1 > \deg r_2 > \cdots$, при некотором k будет выполнено неравенство $\deg r_k < \deg g$. Полагая $q = q_1 + q_2 + \cdots + q_k$ и $r = r_k$, мы получаем требуемое утверждение.

Теорема о делении многочленов с остатком (3)

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 $q_1 - q_2 \neq o$, 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, $q_1 - q_2 = o$, откуда $q_1 = q_2$. Но тогда $r_2 - r_1 = o \cdot g = o$, и значит $r_1 = r_2$. □

Определение

Если выполнено равенство (1), то многочлен q называется *частным*, а многочлен r — *остатком* от деления f на g (с остатком).

Определения

Если выполнено равенство $f = qg$, то говорят, что многочлен f *делится* на многочлен g, или что g *делит* f; этот факт будет обозначаться через $g \mid f$.

Укажем два простых свойства отношения делимости многочленов.

Свойства делимости многочленов

Пусть $f, g, g_1, g_2, h \in R[x]$. *Тогда:*

1) *если* $f \mid g$, *то* $f \mid (gh)$;
2) *если* $f \mid g_1$ *и* $f \mid g_2$, *то* $f \mid (g_1 + g_2)$.

Доказательство. 1) По условию $g = fa$ для некоторого многочлена $a \in R[x]$. Следовательно, $gh = (fa)h = f(ah)$, и потому $f \mid gh$.

2) По условию $g_1 = fa_1$ и $g_2 = fa_2$ для некоторых многочленов $a_1, a_2 \in R[x]$. Следовательно, $g_1 + g_2 = fa_1 + fa_2 = f(a_1 + a_2)$, и потому $f \mid (g_1 + g_2)$. □

Ассоциированные многочлены

Очевидно, что отношение делимости на множестве всех многочленов рефлексивно и транзитивно, но не симметрично и не антисимметрично. В частности, оно является квазипорядком, но не является частичным порядком. В соответствии с общим определением ассоциированных элементов квазиупорядоченного множества, которое было дано в § 2, будем называть многочлены f и g над одним и тем же кольцом *ассоциированными*, если $f \mid g$ и $g \mid f$.

Замечание 10.4

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, $\deg \alpha \leqslant 0$, т. е. $\alpha \in F$. Кроме того, $\alpha \neq 0$, так как в противном случае $f = \alpha g = o$.

Достаточность. Если $f = \alpha g$ и $\alpha \in F \setminus \{0\}$, то $g = \alpha^{-1} f$. Из первого равенства вытекает, что $f \mid g$, а из второго — что $g \mid f$. □

10.3. Наибольший общий делитель многочленов

Определение

Пусть F — поле и $f, g \in F[x]$. Многочлен $h \in F[x]$ называется *наибольшим общим делителем* 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 наибольший общий делитель двух многочленов определен не однозначно, а с точностью до ассоциированности.

Замечание 10.5

Пусть d — наибольший общий делитель многочленов f и g. Многочлен e также является наибольшим общим делителем 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 наибольшего общего делителя это означает, что многочлены d и e делят друг друга, т. е. ассоциированы.

Наибольший общий делитель (2)

Достаточность. Пусть d — наибольший общий делитель 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 h делит d, а поскольку d делит e, то и h делит e. Следовательно, e — наибольший общий делитель f и g. □

Теорема о наибольшем общем делителе (1)

Теорема 10.2

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

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

Правая часть равенства (2) называется *линейной формой наибольшего общего делителя*.

Доказательство. Без ограничения общности предположим, что $\deg f \geqslant \deg g$. Применяя теорему 10.1, разделим f на g с остатком: $f = q_1 g + r_1$, где $\deg r_1 < \deg g$. Если $r_1 \neq o$, разделим g на r_1 с остатком: $g = q_2 r_1 + r_2$, где $\deg r_2 < \deg r_1$. Если $r_2 \neq o$, разделим r_1 на r_2 с остатком: $r_1 = q_3 r_2 + r_3$, где $\deg r_3 < \deg r_2$. Будем продолжать этот процесс, деля теперь на каждом шаге предпоследний остаток на последний, при условии, что последний остаток отличен от o. Поскольку $\deg g > \deg r_1 > \deg r_2 > \cdots$, на каком-то шаге степень остатка окажется меньше или равной 0. Если сам остаток при этом будет отличен от o, он станет равным o на следующем шаге.

Теорема о наибольшем общем делителе (2)

Таким образом, описанный выше процесс оборвется. В результате мы получим следующие равенства:

$$\begin{cases} f = q_1 g + r_1,\ r_1 \neq o,\ \deg r_1 < \deg g; \\ g = q_2 r_1 + r_2,\ r_2 \neq o,\ \deg r_2 < \deg r_1; \\ r_1 = q_3 r_2 + r_3,\ r_3 \neq o,\ \deg r_3 < \deg r_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{k-1} = q_{k+1} r_k + r_{k+1},\ r_{k+1} \neq o,\ \deg r_{k+1} < \deg r_k; \\ r_k = q_{k+2} r_{k+1}. \end{cases} \tag{3}$$

Докажем, что r_{k+1} является наибольшим общим делителем 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 свойства 2) делимости многочлена, — что $r_{k+1} \mid r_{k-1}$. Аналогичным образом на каждом следующем шаге, переходя к очередному равенству вида $r_s = q_{s+2} r_{s+1} + r_{s+2}$ и используя уже доказанные к этому моменту соотношения $r_{k+1} \mid r_{s+1}$ и $r_{k+1} \mid r_{s+2}$, мы получаем, что $r_{k+1} \mid r_s$. Дойдя до второго и первого равенств, мы установим, что $r_{k+1} \mid g$ и $r_{k+1} \mid f$ соответственно.

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 $r_1 = f - q_1 g$; в силу свойств делимости многочленов получаем, что $h \mid r_1$.

Теорема о наибольшем общем делителе (3)

Рассматривая следующее равенство, получаем, что $r_2 = g - q_2 r_1$, откуда, в силу свойств 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, что $r_{k+1} = uf + vg$ для некоторых многочленов u и v. 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:

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

Таким образом, $r_{k+1} = u_2 r_{k-2} + v_2 r_{k-1}$ для некоторых многочленов u_2 и v_2. 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, $r_{k+1} = u_3 r_{k-3} + v_3 r_{k-2}$ для некоторых многочленов u_3 и v_3.

Теорема о наибольшем общем делителе (4)

Продолжая движение снизу вверх по системе (3), 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

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

т. е. $r_{k+1} = u_k g + v_k r_1$ для некоторых u_k и v_k. Подставляя в это равенство выражение $r_1 = f - q_1 g$, полученное из первого равенства системы (3), окончательно имеем

$$r_{k+1} = u_k g + v_k(f - q_1 g) = v_k f + (u_k - v_k q_1) g,$$

т. е. $r_{k+1} = uf + vg$ для некоторых u и v. □

Алгоритм Евклида

В доказательстве теоремы 10.2 содержится алгоритм построения наибольшего общего делителя двух многочленов, который называется *алгоритмом Евклида*. Сформулируем его в явном виде.

Алгоритм 10.1 (алгоритм Евклида)

Даны ненулевые многочлены f и g над полем такие, что $\deg f \geqslant \deg g$. Требуется найти наибольший общий делитель d многочленов f и g. Полагаем $r_{-1} = f$, $r_0 = g$ и $k = 0$. Если $r_k \neq o$, делим r_{k-1} на r_k, остаток от деления обозначаем через r_{k+1} и увеличиваем значение k на 1. Если $r_k \neq o$, повторяем указанные действия. Если $r_k = o$, полагаем $d = r_{k-1}$ и завершаем работу алгоритма.

Поскольку $\deg r_{k+1} < \deg r_k$ для всякого k, существует k такое, что $\deg r_k \leqslant 0$. При этом если $r_k \neq o$, то $r_{k+1} = o$. Следовательно, алгоритм завершит работу через конечное число шагов.

Взаимно простые многочлены (1)

Определение

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

Из теоремы 10.2 вытекает

Следствие 10.1

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. $h \mid 1$. Следовательно, можно считать, что наибольший общий делитель f и g равен 1.

Взаимно простые многочлены (2)

Предложение 10.1

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 многочленов p и q. Так как f и g взаимно просты, в силу следствия 10.1 существуют многочлены u и v такие, что выполняется равенство $uf + vg = 1$. Умножая обе части этого равенства на h, получим $h = huf + hvg$, откуда $h = gquf + fpvg = fg(qu + pv)$. Следовательно, $(fg) \mid h$.

Взаимно простые многочлены (3)

2) По условию $gh = fp$ для некоторого многочлена p. В силу следствия 10.1 $uf + vg = 1$ для некоторых многочленов u и v. Следовательно, $huf + hvg = h$, откуда $h = huf + fpv = f(hu + pv)$. Следовательно, $f \mid h$.

3) В силу следствия 10.1 $uf + vh = 1$ для некоторых многочленов u и v. Следовательно, $ufg + vhg = g$. Обозначим через p наибольший общий делитель fg и h. Тогда, с одной стороны, p делит h, а значит и vhg, а с другой, p делит fg, а значит и ufg. Следовательно, p делит $vgh + ufg = g$. Поскольку g и h взаимно просты, а p делит и g, и h, получаем, что $p = 1$. □