## 1.4. Наибольший общий делитель

***Определение 1.4.1.*** Полином $g(x)$ называется *общим делителем* двух полиномов $f_0(x)$ и $f_1(x)$, если $f_0 \vdots g$, $f_1 \vdots g$.

***Определение 1.4.2.*** Общий делитель $d(x)$ полиномов $f_0(x)$ и $f_1(x)$ называется *наибольшим общим делителем* (НОД), если $d(x)$ делится нацело на любой другой общий делитель этих полиномов.

***Определение 1.4.3.*** Полиномы $f_0(x)$ и $f_1(x)$ называются *взаимно простыми*, если они не имеют общих делителей положительных степеней.

**Лемма 1.4.1.** *Наибольший общий делитель двух полиномов определяется с точностью до постоянного сомножителя.*

Доказательство. Пусть даны два различных наибольших общих делителя $d_0(x)$ и $d_1(x)$ полиномов $f_0(x)$ и $f_1(x)$. По определению НОД $d_0(x) = h_1(x)d_1(x)$, а $d_1(x) = h_0(x)d_0(x)$. Следовательно, $d_0(x) = h_1(x)h_0(x)d_0(x)$, поэтому $\deg[h_0(x)h_1(x)] = 0$, отсюда $\deg h_0(x) = \deg h_1(x) = 0$, т. е. полиномы $h_0(x)$ и $h_1(x)$ являются константами.

Приведем конструктивный способ построения НОД двух полиномов $f_0(x)$ и $f_1(x)$, который называется *алгоритмом Евклида*.

Пусть для определенности $\deg f_0(x) \geq \deg f_1(x)$. Делим полином $f_0(x)$ на полином $f_1(x)$ с остатком, получаем $f_0(x) = f_1(x)q_1(x) + r_1(x)$. Теперь полином $f_1(x)$ делим на остаток от деления $r_1(x)$, имеем $f_1(x) = r_1(x)q_2(x) + r_2(x)$. Затем полином $r_1(x)$ делим на $r_2(x)$ и т. д. В итоге получаем цепочку равенств:

$$f_0 = f_1q_1 + r_1,\ f_1 = r_1q_2 + r_2,\ r_1 = r_2q_3 + r_3,\ \ldots,\ r_{k-2} = r_{k-1}q_k + r_k,\ r_{k-1} = r_kq_{k+1}. \quad (1.4.1)$$

Так как $\deg r_1 > \deg r_2 > \cdots > \deg r_{k-1} > \deg r_k$, то цепочка равенств (1.4.1) конечна и в ней существует звено, в котором деление осуществляется нацело. Докажем, что полином $r_k(x)$ является наибольшим общим делителем полиномов $f_0(x)$ и $f_1(x)$.

Действительно, поскольку $r_{k-1} \vdots r_k$, то оба слагаемых в правой части соотношения $r_{k-2} = r_{k-1}q_k + r_k$ делятся на $r_k(x)$, поэтому $r_{k-2} \vdots r_k$. Продолжая подобные рассуждения и передвигаясь по цепочке, получаем, что $f_1 \vdots r_k$, $f_0 \vdots r_k$. Таким образом, $r_k(x)$ является общим делителем полиномов $f_0(x)$ и $f_1(x)$.

Пусть $d(x)$ — произвольный общий делитель указанных полиномов. В силу первого равенства цепочки (1.4.1) $f_0 = f_1q_1 + r_1$ остаток от деления $r_1(x)$ делится нацело на полином $d(x)$. Тогда из второго равенства $f_1 = r_1q_2 + r_2$ следует, что $r_2 \vdots d$. Рассуждая аналогично и перебирая последовательно все равенства (1.4.1), в итоге имеем $r_k \vdots d$. В силу произвольности $d(x)$ и в соответствии с определением НОД получаем, что $r_k(x)$ — наибольший общий делитель полиномов $f_0(x)$ и $f_1(x)$.

**Теорема 1.4.1.** *Если* $d(x)$ *— это наибольший общий делитель полиномов* $f_0(x)$ *и* $f_1(x)$, *то существуют такие полиномы* $u_0(x)$ *и* $u_1(x)$, *что*

$$d(x) = u_0(x) f_0(x) + u_1(x) f_1(x). \qquad (1.4.2)$$

Доказательство. Для доказательства воспользуемся цепочкой (1.4.1). В соответствии с алгоритмом Евклида $d(x) = r_k(x)$. Но $r_k = r_{k-2} - r_{k-1}q_k = a_1^{(k-2)}r_{k-2} + a_2^{(k-1)}r_{k-1}$, где $a_1^{(k-2)} = 1$, $a_2^{(k-1)} = -q_k$. Из (1.4.1) следует, что $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$. Поэтому, подставляя в выражение для $r_k$, получаем $r_k = a_1^{(k-2)}r_{k-2} + a_2^{(k-1)}[r_{k-3} - r_{k-2}q_{k-1}] = a_1^{(k-3)}r_{k-3} + a_2^{(k-2)}r_{k-2}$, где $a_1^{(k-3)} = a_2^{(k-1)}$, $a_2^{(k-2)} = a_1^{(k-2)} - a_2^{(k-1)}q_{k-1}$. Далее заменяем $r_{k-2}$ и т. д. В итоге будем иметь, что $r_k = a_1^{(1)}r_1 + a_2^{(2)}r_2$. Но $r_1 = f_0 - f_1q_1$, а $r_2 = f_1 - r_1q_2 = f_1 - (f_0 - f_1q_1)q_2$. Поэтому окончательно имеем

$$r_k = a_1^{(1)}(f_0 - f_1q_1) + a_2^{(2)}[f_1 - (f_0 - f_1q_1)q_2] = u_0 f_0 + u_1 f_1,$$

где $u_0 = a_1^{(1)} - a_2^{(2)}q_2$, $u_1 = -a_1^{(1)}q_1 + a_2^{(2)}(1 + q_1q_2)$.

**Следствие 1.4.1.** *Полиномы* $f_0(x)$ *и* $f_1(x)$ *взаимно просты тогда и только тогда, когда существуют полиномы* $u_0(x)$ *и* $u_1(x)$, *для которых*

$$u_0(x) f_0(x) + u_1(x) f_1(x) = 1. \qquad (1.4.3)$$

Необходимость данного условия очевидна, а достаточность легко доказывается от противного.

**Следствие 1.4.2.** *Если полином* $f_0(x)$ *взаимно прост с каждым из полиномов* $f_1(x)$ *и* $f_2(x)$, *то он взаимно прост и с их произведением* $f_1(x) f_2(x)$.

Доказательство. Так как $f_0(x)$ и $f_1(x)$ взаимно просты, то существуют такие полиномы $u_0(x)$ и $u_1(x)$, что справедливо (1.4.3). Умножим обе части соотношения (1.4.3) на $f_2(x)$, получаем $[u_0(x) f_2(x)] f_0(x) + u_1(x)[f_1(x) f_2(x)] = f_2(x)$. Если предположить, что полиномы $f_0(x)$ и $f_1(x) f_2(x)$ имеют общий делитель положительной степени, то он должен быть делителем и полинома $f_2(x)$. Но по условию $f_0(x)$ взаимно прост с $f_2(x)$, следовательно, полином $f_0(x)$ и произведение $f_1(x) f_2(x)$ являются взаимно простыми полиномами.

**Следствие 1.4.3.** *Если произведение* $f_1(x) f_2(x)$ *делится нацело на полином* $f_0(x)$, *причем* $f_1(x)$ *и* $f_0(x)$ *являются взаимно простыми, то* $f_2 \,\vdots\, f_0$.

Доказательство. Поскольку $f_0(x)$ и $f_1(x)$ взаимно просты, то существуют такие полиномы $u_0(x)$ и $u_1(x)$, что справедливо (1.4.3). Умножим обе части соотношения (1.4.3) на $f_2(x)$, получаем $[u_0(x) f_2(x)] f_0(x) + u_1(x)[f_1(x) f_2(x)] = f_2(x)$. Левая часть последнего равенства, очевидно, делится нацело на $f_0(x)$. Следовательно, должна делиться нацело и правая часть, т. е. $f_2 \,\vdots\, f_0$.