ЛЕКЦИЯ 11
НАЙ-ГОЛЯМ ОБЩ ДЕЛИТЕЛ НА ПОЛИНОМИ

Преди да дефинираме най-голям общ делител на полиноми ще докажем следната необходима

Теорема 1. *Нека F е поле. За всеки два полинома $f(x)$, $g(x) \in F[x]$, $g(x) \neq 0$ съществуват полиноми $q(x)$, $r(x) \in F[x]$, такива че $f(x) = g(x)q(x) + r(x)$, където* ст. $r(x) <$ ст. $g(x)$ *или $r(x) = 0$ (нулев полином). Полиномите $q(x)$ и $r(x)$ са единствените, които удовлетворяват тези условия.*

Доказателство:

1. Съществуване

Ако $f(x)$ се дели на $g(x)$, тогава $f(x) = g(x)h(x) + 0$ и имаме $q(x) = h(x)$, $r(x) = 0$. Поради това съществуването на $q(x)$ и $r(x)$ е очевидно. Ето защо ще предполагаме, че

$$f(x) \text{ не се дели на } g(x) \qquad (*)$$

Ако ст. $g(x) >$ ст. $f(x)$, тогава

$$\begin{array}{ccc} f(x) = & 0 \,.\, g(x) & + f(x) \\ & \shortparallel & \shortparallel \\ & q(x) & r(x) \end{array}$$

и съществуването на $q(x)$ и $r(x)$ също е очевидно. Поради това ще предполагаме, че

$$\text{ст. } g(x) \leqq \text{ст. } f(x) \qquad (**)$$

По-нататък доказателството ще направим по индукция относно $n =$ ст. $f(x)$. Нека

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,\ a_n \neq 0, \quad \text{ст. } f(x) = n$$

$$g(x) = b_0 + b_1x + \cdots + b_mx^m,\ b_m \neq 0,\ \text{ст.}\, g(x) = m.$$

База $n = 0$. В тази ситуация имаме $f(x) = a_0$, $a_0 \neq 0$. От $g(x) \neq 0$ и (**) имаме $g(x) = b_0$, $b_0 \neq 0$ и очевидно

$$\begin{array}{ccc} f(x) = (a_0b_0^{-1})b_0 & + & 0 \\ \shortparallel & & \shortparallel \\ q(x) & & r(x) \end{array}$$

С което базата е доказана.

Нека $n \geqq 1$. Разглеждаме $h(x) = f(x) - x^{n-m} \cdot \dfrac{a_n}{b_m} \cdot g(x)$

Съгласно (**) $h(x)$ е полином. Съгласно (*) $h(x)$ е ненулев полином. Тъй като $h(x)$ е разлика на два полинома от n-та степен, в които коефициентите пред n-тата степен са равни, имаме $\text{ст.}\, h(x) < n$. За $h(x)$ прилагаме индуктивната хипотеза и получаваме

$$h(x) = q_1(x)g(x) + r_1(x),\ \text{където ст.}\, r_1(x) < \text{ст.}\, g(x) \text{ или } r_1(x) = 0$$

от последното равенство следва

$$f(x) = h(x) + \frac{a_n}{b_m}x^{n-m}g(x) = q_1(x)g(x) + r_1(x) + \frac{a_n}{b_m}x^{n-m}g(x).$$

Откъдето получаваме

$$f(x) = \Big(q_1(x) + \frac{a_n}{b_m}\,x^{n-m}\Big)g(x) + r_1(x)$$

и търсените полиноми $q(x)$ и $r(x)$ са

$$q(x) = q_1(x) + \frac{a_n}{b_m}\,x^{n-m} \quad \text{и} \quad r(x) = r_1(x).$$

2.Единственост

Нека освен

$$f(x) = g(x)q(x) + r(x),\ \text{където ст.}\, r(x) < \text{ст.}\, g(x) \text{ или } r(x) = 0$$

имаме

$$f(x) = g(x)q_1(x) + r_1(x),\ \text{където ст.}\, r_1(x) < \text{ст.}\, g(x) \text{ или } r_1(x) = 0.$$

Като извадим тези две равенства получаваме

$$g(x)\big(q(x) - q_1(x)\big) = r_1(x) - r(x). \qquad (***)$$

Да допуснем, че $q(x) \neq q_1(x)$. Понеже $g(x) \neq 0$ в лявата страна на последното равенство имаме ненулев полином чиято степен не е по-малка от степента на $g(x)$. От ограниченията за $r(x)$ и $r_1(x)$ следва, че в дясната част на (***) не може да има степен по-голяма или равна от степента на $g(x)$. Полученото противоречие доказва, че $q_1(x) = q(x)$. Като заместим в (***) получаваме $r_1(x) - r(x) = 0$, т. е. $r_1(x) = r(x)$. Следователно $q(x)$ и $r(x)$ са единствени.

Определение. *Нека K е комутативен пръстен и $f(x)$, $g(x) \in K[x]$. Най-голям общ делител (НОД) на $f(x)$ и $g(x)$ в пръстена $K[x]$ наричаме такъв полином $d(x) \in K[x]$, че:*

1) $d(x)$ дели $f(x)$ и $g(x)$;

2) ако $d_1(x)$ дели $f(x)$ и $g(x)$, тогава $d_1(x)$ дели $d(x)$.

Теорема 2. *Нека F е поле. Тогава всеки два полинома от $F[x]$ имат НОД във $F[x]$.*

Доказателство:

Нека $f(x)$, $g(x) \in F[x]$. Ако $f(x) = g(x) = 0$, тогава НОД е нулевият полином (в тази ситуация всеки полином от $F[x]$ е общ делител на $f(x)$ и $g(x)$, но единствено нулевият полином удовлетворява второто условие за НОД). Поради това ще предполагаме, че

$$\text{поне единият от } f(x),\ g(x) \text{е ненулев} \qquad (\#)$$

Дефинираме

$$S = \big\{M(x)f(x) + N(x)g(x) \mid M(x), N(x) \in F[x]\big\}$$

Като положим $N(x) = 0$ и $M(x) = 1$ получаваме $f(x) \in S$, а като положим $N(x) = 1$ и $M(x) = 0$ получаваме $g(x) \in S$. Следователно $f(x)$, $g(x) \in S$. От $(\#)$ става ясно, че в S има ненулеви полиноми. Измежду всички ненулеви полиноми в S избираме такъв ненулев полином $d(x)$, който има най-ниска възможна степен. Имаме

$$\text{ст.}\, d(x) \leqq \text{ст.}\, h(x),\ \text{за всеки ненулев } h(x) \in S \qquad (\#\#)$$

От $d(x) \in S$ следва

$$d(x) = M_0(x)f(x) + N_0(x)g(x) \qquad (\#\#\#)$$

Ще докажем че $d(x)$ е най-голям общ делител на $f(x)$ и $g(x)$. Понеже $S \subseteq F[x]$, $d(x) \in F[x]$.

I. Защо $d(x)$ е общ делител на $f(x)$ и $g(x)$.

Допускаме, че $d(x)$ не дели $f(x)$. Тогава $f(x) = d(x)q(x)+r(x)$, където $r(x) \neq 0$ и $\text{ст.}\, r(x) < \text{ст.}\, d(x)$. Като използваме $(\#\#\#)$ получаваме

$$r(x) = f(x) - d(x)q(x) = f(x) - \big(M_0(x)f(x) + N_0(x)g(x)\big)q(x) =$$
$$= \underbrace{\big(1 - M_0(x)q(x)\big)}_{M(x)} f(x) - \underbrace{N_0(x)q(x)}_{N(x)} g(x)$$

Следователно, $r(x) = M(x)f(x) + N(x)g(x)$ и поради това $r(x) \in S$. Полиномът $r(x)$ принадлежи на множеството S и има степен по-малка от $d(x)$, което противоречи на $(\#\#)$. Това противоречие доказва, че $d(x)$ дели $f(x)$. По-същият начин се доказва, че $d(x)$ дели $g(x)$.

II. Нека $d_1(x)$ дели $f(x)$ и $g(x)$. От $(\#\#\#)$ следва, че $d_1(x)$ дели $d(x)$. Теорема 2 е доказана.

Очевидно е вярно следното твърдение

Твърдение. *Ако $f(x)$ дели $g(x)$, тогава $f(x)$ е* НОД *на $f(x)$ и $g(x)$.*

Определение. *Казваме, че полиномите $f(x)$ и $g(x)$ са асоциирани, ако всеки от тях може да се получи от другия с умножение с ненулева константа.*

По-нататък ще ни е необходима следната

Лема. *Нека K е комутативен пръстен, в който няма делители на нулата. Ако два полинома от $K[x]$ се делят взаимно, то те са асоциирани.*

Доказателство:

Нека $f(x)$, $g(x) \in K[x]$ и се делят взаимно. Тогава

$$f(x) = g(x).h(x)$$
$$g(x) = f(x).t(x).$$

От тези равенства следва, че ако единият от полиномите е нулев, другият също е нулев и твърдението е очевидно. Нека $f(x)$ и $g(x)$ са ненулеви полиноми. Тогава от горните равенства получаваме $f(x) = f(x).t(x).h(x)$. Понеже в K няма делители на нулата

$$\text{ст.}\, f(x) = \text{ст.}\, f(x) + \text{ст.}\, t(x) + \text{ст.}\, h(x).$$

Това равенство ни дава, че

$$\text{ст.}\, t(x) + \text{ст.}\, h(x) = 0,$$

т. е.

$$\text{ст.}\, h(x) = \text{ст.}\, t(x) = 0.$$

Доказахме Лемата тъй като $h(x) = \text{const} \neq 0$ и $t(x) = \text{const} \neq 0$.

Следствие 1. *Нека F е поле и $f(x)$, $g(x) \in F[x]$. Тогава всеки два НОД на тези полиноми са асоциирани.*

Доказателство:

Съгласно определението за НОД всеки два най-големи общи делители на $f(x)$ и $g(x)$ се делят взаимно. Понеже във F няма делители на нулата от Лемата следва, че всеки два НОД на $f(x)$ и $g(x)$ са асоциирани.

Следствие 2. *Нека F е поле и $f(x)$, $g(x) \in F[x]$. Тогава всеки НОД $d(x)$ на $f(x)$ и $g(x)$ може да се представи във вида:*

$$d(x) = M(x)f(x) + N(x)g(x), \qquad M(x), N(x) \in F[x]$$

Доказателство:

В доказателството на Теорема 2 показахме, че един НОД на $f(x)$ и $g(x)$ може да се представи в желания вид. Съгласно Следствие 1 всеки друг НОД може да се получи от този НОД с умножаване с ненулева константа и поради това също се представя в желания вид. Следствие 2 е доказано.

Следствие 3. *Нека F е поле и $f(x)$, $g(x) \in F[x]$. Елементът $\alpha \in F$ е общ корен на $f(x)$ и $g(x)$ тогава и само тогава, когато α е корен на НОД на $f(x)$ и $g(x)$.*

Доказателство:

1. Нека $d(x)$ е НОД на $f(x)$ и $g(x)$ и α е корен на $f(x)$ и $g(x)$, т. е. $f(\alpha) = g(\alpha) = 0$.

Съгласно Следствие 2, $d(x) = M(x)f(x) + N(x)g(x)$. Следователно $d(\alpha) = M(\alpha)f(\alpha) + N(\alpha)g(\alpha) = 0$, т. е. α е корен на $d(x)$.

2. Нека α е корен на $d(x)$, т. е. $d(\alpha) = 0$. Понеже

$$f(x) = d(x)f_1(x) \Rightarrow f(\alpha) = 0.$$
$$g(x) = d(x)g_1(x) \Rightarrow g(\alpha) = 0.$$

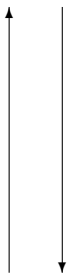
Следователно α е общ корен на $f(x)$ и $g(x)$.

По нататък НОД на $f(x)$ и $g(x)$, макар да не е определен еднозначно, ще го означаваме с $(f(x), g(x))$.

Алгоритъм на Евклид за намиране на НОД

Нека F е поле и $f(x)$ и $g(x) \in F[x]$. Прилагайки последователно Теорема 1 получаваме равенствата:

$$
\begin{aligned}
f(x) &= g(x)q_1(x) + r_1(x), && \text{където ст.}\, r_1(x) < \text{ст.}\, g(x)\\
g(x) &= r_1(x)q_2(x) + r_2(x), && \text{където ст.}\, r_2(x) < \text{ст.}\, r_1(x)\\
r_1(x) &= r_2(x)q_3(x) + r_3(x), && \text{където ст.}\, r_3(x) < \text{ст.}\, r_2(x)\\
r_2(x) &= r_3(x)q_4(x) + r_4(x), && \text{където ст.}\, r_4(x) < \text{ст.}\, r_3(x)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_k(x) &= r_{k+1}(x)q_{k+2}(x) + r_{k+2}(x), && \text{където ст.}\, r_{k+2}(x) < \text{ст.}\, r_{k+1}(x)\\
r_{k+1}(x) &= r_{k+2}(x)q_{k+3}(x) + 0
\end{aligned}
$$



където $r_{k+2}(x)$ е последният ненулев остатък.

Твърдение. *$r_{k+2}(x)$ е НОД на $f(x)$ и $g(x)$*

Доказателство:

Движейки се по равенствата отдолу нагоре последователно получаваме, че $r_{k+2}(x)$ дели $r_{k+1}(x)$, $r_k(x)$, $\ldots$, $r_1(x)$, $f(x)$ и $g(x)$. Ако $d(x)$ дели $f(x)$ и $g(x)$ чрез движение по равенствата отгоре надолу доказваме последователно, че $d(x)$ дели $r_1(x)$, $r_2(x)$, $\ldots$, $r_{k+2}(x)$.