ЛЕКЦИЯ 12
ВЗАИМНО ПРОСТИ ПОЛИНОМИ. НЕРАЗЛОЖИМИ ПОЛИНОМИ.

Определение. *Нека F е поле и $f(x)$, $g(x) \in F[x]$. Казваме, че $f(x)$ и $g(x)$ са взаимно прости, ако най-големият общ делител на $f(x)$ и $g(x)$ е ненулева константа.*

От миналата лекция, знаем, че всеки два най-големи общи делители на $f(x)$ и $g(x)$ са асоциирани. Поради това, ако един най-голям делител на $f(x)$ и $g(x)$ е ненулева константа, тогава всеки най-голям общ делител на тези полиноми също е ненулева константа. Следователно дефиницията за взаимно прости полиноми е коректна.

Твърдение 1. *Нека F е поле. Полиномите $f(x)$ и $g(x) \in F[x]$ са взаимно прости тогава и само тогава, когато съществуват $u(x)$, $v(x) \in F[x]$ такива, че*

$$1 = f(x)u(x) + g(x)v(x) \qquad (*)$$

Доказателство:

Нека $f(x)$ и $g(x)$ са взаимно прости и $c \in F$, $c \neq 0$ е НОД на $f(x)$ и $g(x)$. Тогава съгласно Следствие 2 от миналата лекция

$$c = f(x)M(x) + g(x)N(x); \quad M(x),\ N(x) \in F[x].$$

Като умножим с c^{-1} двете страни на това равенство получаваме желаното равенство (*), където $u(x) = M(x)c^{-1}$ и $v(x) = N(x)c^{-1}$.

Да предположим, че е изпълнено равенството (*). Тогава всеки общ делител на $f(x)$ и $g(x)$ дели единицата и следователно е ненулева константа. Поради това $f(x)$ и $g(x)$ са взаимно прости.

Ако $f(x)$ и $g(x)$ са взаимно прости ще пишем $(f(x), g(x)) = 1$

Твърдение 2. *Нека F е поле и $f(x)$, $g(x)$, $h(x) \in F[x]$. Нека $f(x)$ дели $g(x)h(x)$ и $(f(x), g(x)) = 1$. Тогава $f(x)$ дели $h(x)$.*

Доказателство:

Съгласно твърдение 1 имаме $1 = f(x)u(x) + g(x)v(x)$. Като умножим двете страни на това равенство с $h(x)$ получаваме

$$h(x) = f(x)u(x)h(x) + g(x)h(x)v(x).$$

Понеже $f(x)$ дели събираемите отдясно става ясно, че $f(x)$ дели $h(x)$.

Твърдение 3. *Нека F е поле, $f(x)$, $f_i(x) \in F[x]$ и $\big(f(x), f_i(x)\big) = 1$, $i = 1, \ldots, s$. Тогава*

$$\big(f(x), f_1(x) \ldots f_s(x)\big) = 1.$$

Доказателство:

Индукция по s.

База $s = 2$.

$$(f(x), f_1(x)) = 1 \Rightarrow 1 = f(x)u_1(x) + f_1(x)v_1(x)$$

$$(f(x), f_2(x)) = 1 \Rightarrow 1 = f(x)u_2(x) + f_2(x)v_2(x)$$

Като умножим тези равенства получаваме

$$1 = [u_1(x)u_2(x)f(x) + u_1(x)v_2(x)f_2(x) + u_2(x)v_1(x)f_1(x)]f(x) + \big(v_1(x)v_2(x)\big)\big(f_1(x)f_2(x)\big).$$

Записано по-кратко имаме

$$1 = u(x)f(x) + v(x)\big(f_1(x)f_2(x)\big).$$

Съгласно Твърдение 1 имаме $(f(x), f_1(x).f_2(x)) = 1$.

Нека $s \geq 2$.

Полагаме $h(x) = f_1(x).f_2(x) \ldots f_{s-1}(x)$.

От индуктивната хипотеза имаме $(f(x), h(x)) = 1$. Понеже $(f(x), f_s(x)) = 1$ от базата следва $(f(x), h(x).f_s(x)) = 1$.

От Твърдение 3 по очевиден начин следва

Твърдение 4. *Нека F е поле, $f_i(x)$, $g_j(x) \in F[x]$ и $(f_i(x), g_j(x)) = 1$, $i = 1, \ldots, k$; $j = 1, \ldots, s$, тогава $(f_1(x) \ldots f_k(x), g_1(x) \ldots g_s(x)) = 1$*

Прилагаме Твърдение 4 за $f_1(x) = \cdots = f_k(x) = f(x)$ и $g_1(x) = \cdots = g_s(x) = g(x)$ и получаваме

Твърдение 5. *Нека F е поле, $f(x)$, $g(x) \in F[x]$ и $(f(x), g(x)) = 1$. Тогава $(f^k(x), g^s(x)) = 1$, за всеки две естествени числа k и s.*

Твърдение 6. *Нека F е поле, $f(x)$, $f_i(x) \in F[x]$, $\big(f_i(x), f_j(x)\big) = 1$, $i \neq j$ и $f_i(x)$ дели $f(x)$, $i = 1, \ldots, s$. Тогава*

$$f_1(x) \ldots f_s(x) \text{ дели } f(x).$$

Доказателството на Твърдение 6 да се направи самостоятелно.

Неразложими полиноми

Нека F е поле, $f(x) \in F[x]$ и $c \in F$, $c \neq 0$. От очевидните равенства

$$f(x) = c\big(c^{-1} f(x)\big) = c^{-1}\big(c.f(x)\big)$$

става ясно, че c и $c.f(x)$ делят $f(x)$, за всяко $c \in F$, $c \neq 0$. Делителите c и $c.f(x)$ се наричат *несобствени делители* на $f(x)$

Ясно е, че ако $g(x)$ дели $f(x)$ и ст. $g(x) =$ ст. $f(x)$, то $f(x) = c.g(x)$, $c \in F$, т. е. $g(x)$ не е собствен делител на $f(x)$. Поради това е вярно

Твърдение 1. *Нека F е поле, $f(x)$, $g(x) \in F[x]$, $f(x) \neq 0$ и $g(x)$ е делител на $f(x)$. Тогава*

$$g(x) \text{ е собствен делител } \Leftrightarrow 0 < \text{ст. } g(x) < \text{ст. } f(x).$$

Определение. *Казваме, че полиномът $f(x) \in F[x]$ е неразложим над полето F, ако са изпълнени следните условия:*

1) ст. $f(x) \geq 1$;

2) $f(x)$ има само несобствени делители.

Определение. *Нека $f(x) \in F[x]$. Казваме, че $f(x)$ е разложим над F, ако $f(x) = f_1(x).f_2(x)$, където $f_1(x)$, $f_2(x) \in F[x]$ и* ст. $f_1(x) \geq 1$, ст. $f_2(x) \geq 1$.

Константите не са нито разложими, нито неразложими полиноми (по определение разложимите и неразложимите полиноми не са константи). От Твърдение 1 виждаме, че полиномите от първа степен нямат собствени делители. Поради това за всяко поле F, линейните полиноми в $F[x]$ са неразложими над F. Полиномите от степен по-голяма или равна от 2 във $F[x]$ или са неразложими или са разложими над F.

Неразложимостта съществено зависи от полето F.

Примери.

поле	x^2-2	x^2+1
$\mathbb{Q}$	не	не
$\mathbb{R}$	$(x+\sqrt{2})(x-\sqrt{2})$	не
$\mathbb{C}$	$(x+\sqrt{2})(x-\sqrt{2})$	$(x+i)(x-i)$

Твърдение 2. *Нека F е поле. Нека $f(x)$, $g(x) \in F[x]$ и $f(x)$ е неразложим над F. Тогава или $(f(x), g(x)) = 1$, или $f(x)$ дели $g(x)$.*

Доказателство:

Нека $d(x)$ е НОД на $f(x)$ и $g(x)$. Тогава $d(x)$ дели $f(x)$. Понеже $f(x)$ е неразложим, $d(x)$ е несобствен делител на $f(x)$. Поради това имаме следните две възможности:

Случай 1: $d(x) = c$, $c \neq 0$, $c \in F \Rightarrow (f(x), g(x)) = 1$.

Случай 2: $d(x) = c.f(x)$. Понеже $d(x)$ дели $g(x)$, ще получим $g(x) = d(x).g_1(x) = c.f(x).g_1(x)$. Следователно $f(x)$ дели $g(x)$.

Твърдение 3. *Нека F е поле и $f(x)$, $g(x) \in F[x]$. Ако $f(x)$ и $g(x)$ са неразложими над F, тогава или $(f(x), g(x)) = 1$ или $f(x)$ и $g(x)$ са асоциирани.*

Доказателство:

Да допуснем, че $f(x)$ и $g(x)$ не са взаимно прости. Тогава от Твърдение 2 следва, че $f(x)$ и $g(x)$ се делят взаимно. Съгласно лемата от миналата лекция, $f(x)$ и $g(x)$ са асоциирани.

Твърдение 4. *Нека F е поле и $f(x)$, $f_1(x)$, $\ldots$, $f_s(x) \in F[x]$. Ако $f(x)$ е неразложим над F и $f(x)$ дели произведението $f_1(x) \ldots f_s(x)$, тогава $f(x)$ дели някой от полиномите $f_1(x)$, $\ldots$, $f_s(x)$.*

Доказателство:

Допускаме противното. Съгласно Твърдение 1 имаме $\big(f(x), f_i(x)\big) = 1$, $i = 1, \ldots, s$.

Като приложим Твърдение 3 за взаимно простите полиноми получаваме, че

$$(**) \qquad \big(f(x), f_1(x)\dots f_s(x)\big) = 1.$$

От друга страна $f(x)$ дели $f_1(x)f_2(x)\dots f_s(x)$ и поради това $f(x)$ е НОД на $f(x)$ и $f_1(x)f_2(x)\dots f_s(x)$. Понеже $f(x)$ не е константа, това противоречи на (**).

Твърдение 5. *Нека F е поле, $f(x) \in F[x]$ и $f(x)$ е неразложим над F. Ако* ст. $f(x) \geq 2$, *тогава $f(x)$ няма корени в полето F.*

Доказателство:

Допускаме, че $f(x)$ има корен $\beta \in F$. Тогава $f(x) = (x-\beta).g(x)$. Понеже $\beta \in F$, $g(x) \in F[x]$. От ст. $f(x) \geq 2$ имаме ст. $g(x) \geq 1$. Получихме, че $f(x)$ е разложим над F, което е противоречие.

Следващото твърдение се доказва лесно.

Твърдение 6. *Нека F е поле, $f(x) \in F[x]$ и* ст. $f(x)$ *е равна на 2 или на 3. Тогава*

$$f(x) \text{ е неразложим над } F \Leftrightarrow f(x) \text{ няма корен във } F.$$

Доказателството на твърдението да се направи самостоятелно.