Взаимно прости 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.*

Ако един от най-големите общи делители е ненулева константа, понеже всеки друг се получава от този с умножение на ненулева константа, то всеки НОД на взаимно прости полиноми е ненулева константа. Поради това определението за взаимно прости полиноми е коректно.

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*

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

Д-во:
Нека $f(x)$ и $g(x)$ са взаимно прости. Тогава съществува $c \neq 0$, $c = const$ (НОД за $f(x)$ и $g(x)$) такова, че

$$c = f(x)\,u_1(x) + g(x)\,v_1(x)$$

като умножим с c^{-1} двете страни на това равенство получаваме желаното равенство (*) където $u(x) = u_1(x)c^{-1}$ и $v(x) = v_1(x)c^{-1}$.

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 $f(x)$ *дели* $g(x)\,h(x)$ *и* $(f(x), g(x)) = 1$. *Тогава* $f(x)$ *дели* $h(x)$.

Д-во:
$(f(x), g(x)) = 1 \Rightarrow 1 = f(x)\,u(x) + g(x)\,v(x)$.
като умножим двете страни на това равенство с $h(x)$ получаваме

$$h(x) = f(x)\,u(x)\,h(x) + g(x)\,h(x)\,v(x)$$

откъдето става ясно, че $f(x)$ дели $h(x)$.□

Твърдение 3:

Нека $(f(x), f_i(x)) = 1$, $i = 1, \ldots, s$. *Тогава* $(f(x), f_1(x), \ldots, f_s(x)) = 1$

Д-во:
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

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

Записано по-кратко имаме

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

Съгласно Твърдение1 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 Твърдение3 по очевиден начин следва

Твърдение 4:

Ако $(f_i(x), g_j(x)) = 1$, $i = 1, \ldots, k$; $j = 1, \ldots, s$, *тогава* $(f_1(x) \ldots f_k(x), g_1(x) \ldots g_s(x)) = 1$

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

Твърдение 5:

Нека $(f(x), g(x)) = 1$. Тогава $(f^k(x), g^s(x)) = 1$, за всеки две естествени числа k и s.

Неразложими полиноми

Нека F е поле и $c \in F$, $c \neq 0$ от очевидните равенства

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

Става ясно, че c и c.f(x) делят f(x), за всяко $c \in F$, $c \neq 0$.
c и c.f(x) се наричат несобствени делители на 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 нито са разложими, нито са неразложими. От определението следва, че степента на разложимите полиноми е по-голяма или равна на 2. Следователно полиномите от първа степен са неразложими.

Неразложимостта съществено зависи от полето F.
Примери:

поле	$x^2 - 2$	$x^2 + 1$
Q	не	не
R	$\left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)$	не

C	$(x+\sqrt{2})(x-\sqrt{2})$	$(x+i)(x-i)$

Твърдение 1:

Нека F *е поле*. *Нека* f(x), g(x) ∈ F[x] *и* f(x) *е неразложим над* F. *Тогава или* (f(x), g(x)) = 1, *или* f(x) *дели* g(x).

Д-во:
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 ≠ 0, c ∈ F ⇒ (f(x), g(x)) = 1

Случай 2: d(x) = c.f(x). Понеже d(x) дели g(x) имаме g(x) = d(x).g_1(x) = c.f(x).g_1(x). Следователно f(x) дели g(x).□

Твърдение 2:

Нека F *е поле и* f(x), f_1(x), . . , $f_к$(x) ∈ F[x]. *Ако* f(x) *е неразложим над* F *и* f(x) *дели произведението* f_1(x) . . . f_s(x), *тогава* f(x) *дели някой от полиномите* f_1(x), . . , f_s(x).

Д-во:
Допускаме противното. Съгласно Твърдение 1 имаме (f(x), f_i(x)) = 1, i = 1, . . , к.
Като приложим Твърдение 3 за взаимно простите полиноми получавам, че

(f(x), f_1(x) . . . $f_к$(x)) = 1

което е противоречие□

Твърдение 3:

Нека F *е поле*, f(x)∈ F[x] *и* f(x) *е неразложим над* F. *Ако* ст.f(x) ≥ 2, *тогава* f(x) *няма корени в полето* F.

Д-во:
Допускаме, че f(x) има корен β∈ F.
⇒ f(x) = (x - β).g(x)
ст. f(x) ≥ 2 и ст.g(x) ≥ 1 ⇒ f(x) е разложим над F - противоречие□