$fu + gv$ РОЛ F - поле

Цяхме в пръстена на полиномите на една променлива с коефициенти от поле. ~~Най-~~ НОД. Еднозначно разлагане в произв. от неразложими

$f \in F[x]$, $f = \langle c \rangle$, $d = (f, g) = НОД(f, g) \Leftrightarrow$
$\langle d \rangle = \langle f \rangle + \langle g \rangle$

Сл 1 от съществ. на Безу

Ако f, g_1, g_2 са полиноми т.о. $\in F[x]$, $f \neq 0_F$, $f / g_1 g_2$ и $(f, g_1) = 1 \Rightarrow$ f / g_2 Док

По т. на Безу за f и g_1 $\exists$ т-т $u, v \in F[x]$, такива че $fu + g_1 v = 1$.
Полученото умн. с g_2 дава $fg_2 u + g_1 g_2 v = g_2$. Сега $f / fg_2 u$, $f / g_1 g_2 v$ дава $f / fg_2 u + g_1 g_2 v = g_2$ □

Сл 2

Ако $f, f_1, g \in F[x]$, $f_1 \neq 0_F$, $f_2 \neq 0_F$, f_1 / g, f_2 / g, $(f_1, f_2) = 1$, то $f_1 f_2 / g$

Док

По дефин. f_1 / g означава $\exists$-не на $q_1 \in F[x]$ с $g = f_1 q_1$. Сега от $f_2 / g = f_2 / f_1 q_1$ с $(f_2, f_1) = 1 \Rightarrow f_2 / q_1$ по сл 1 от Безу. С др. думи $\exists q_2 \in F[x]$ т.че $q_1 = f_2 q_2$ и $g = f_1 f_2 q_2$ т.е. $f_1 f_2 / g$

Алгоритъм на евклид за намиране на $d(x) = НОД(f, g)$ за $f, g \in F[x]$ $\deg f \geq \deg g$

Живота няма смисъл но ние как сега разбора

Деление с частно и остатък

$f = q \cdot q_1 + r_1$, $\deg r_1 < \deg g$

$g = r_1 q_2 + r_2$, $\deg r_2 < \deg r_1$

$r_1 = r_2 q_3 + r_3$, $\deg r_3 < \deg r_2$

Редицата от степени на остатъци $\{\deg r_i\}_{i=0}^{\infty}$ с $\mathbb{Z} \geq 0 \cup \{-\infty\}$ е строго намаляваща и след краен брой стъпки става $-\infty$. Нека не/о минималното естествено с $r_{n+1} = 0$, т.е. r_n е последният ненулев остатък $r_{n-1} = \cancel{r_n \neq 0}$ r_n final

Твърдим че $(f,g) = r_n$ Разпечатваме и за да докажем че r_n е общ делител на f и g, Проверяваме че всеки общ делител d_i на f и g дели r_n чрез ↓

Помощните и и v от тях на вида че номерът чрез изразяването от предпоследното равенство т.е.

$r_n \in r_{n-1} F[x] + r_{n-2} F[x] \subseteq r_{n-2} F[x] r_{n-3} F[x] \subseteq g F[x] + f F[x]$

Неразложим полином над поле

Деф

Полиномът $f(x) \in F_{[x]}$ е неразложим над F ако $f(x) \notin F_n$ и $\forall$ разлагане $f = f_1 f_2$ с $f_1 f_2 \in F_{[x]}$ е с $f_1 \in F^*$ или $f_2 \in F^* = F_{[x]}^*$

Да ноя масна това с моето приятелче
да ходя бос и да пушиваме
да се скитам сам фред тази
и да търся нещо което знам че няма
Линеен полином $ax+b \in F[x]$ е
неразложим над F т.к б
$ax+b = f_1 f_2 \neq 0_F \Rightarrow \deg f_i \geq 0$
$\deg f_1 + \deg f_2 = 1 \Rightarrow \exists\, 1 \leq i \leq 2$ с
$\deg f_i = 0$ т.е. $f_i \in F^*$. Разложимост
та на $\in(x)$ зависи от F Напр
$x^2+1 \in \mathbb{Q}[x] \subset \mathbb{R}[x]$ е неразложим
над $\mathbb{Q}$ и $\mathbb{R}$. но $x^2+1 = (x-i)(x+i)$ е
разложим над $\mathbb{C}$
Лема
Ако неразложим над F полином $p(x) \in F[x]$
дели $f_1 \cdot f_k$ за $f_i \in F[x]$ то $p(x)$ дели
поне един множител $f_i(x)$
Док
Ако p не дели f_1 то НОД $(pf_1) = c \in F^*$
от сл 1 от ТЕК на Безу $\Rightarrow$
$p / f_2 \cdots f_k$ С индукция по k $\Rightarrow$
p / f_i за някое $2 \leq i \leq k$
Теорема
Произволен $f(x) \in F[x] / F$ има
разлагане $f = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ в произведение
на неразложими над F множители
$p_i(x)$ със степенни показатели
$\alpha_i \in \mathbb{N}$
Ако $f = p_1^{\alpha_1} \cdots p_n^{\alpha_n} = q_1^{\beta_1} \cdots q_m^{\beta_m}$ са 2
разлагания на $f \in F[x] / F$ в
произведение на неразложими
над F p_i q_j са $\in \mathbb{N}$ и
деми се 1 на себе си

$n = m$ и $\exists$ пермутация на $q_1 \dots q_m$ т. с. $p_i = c_i q_i$ за $1 \le i \le n$ и $a_i = b_i$

Док-во

$\exists$ - не - с индукция по $d = \deg f$

за $d = 1$ полиномът $f(x) = ax + b \in$ неразложим над F и представянето е само разлагането. В общия случай ако $f \in F[x] / F$ е неразложим над F то f е свое разлагане. Ако $f = f_1 . f_2$ е разложим, $0 < \deg f_1, \deg f_2 < \deg f$ то по инд. предположение $\exists$ разлагане $f_1 = p_1 \dots p_s$ в неразложими над F полиноми $p_i \in F[x]$ и $f_2 = p_{s+1} \dots p_k$ в неразложими над F $p_i \in F[x]$. Сега $f = p_1 \dots p_s, p_{s+1} \dots p_k$ е разлагане на f

Единственост

$p_1 \dots p_k = q_1 \dots q_m$. Тогава $p_k / q_1 \dots q_m \Rightarrow p_k / q_m$ по лемата. Следователно $\exists$ пермутация на $q_1 \dots q_m$

Но за неразл над F полиноми p_k и q_m с $p_k / q_m \Rightarrow p_k = c q_m$ за някое $c \in F^*$ или $q_m = c p_k$. Сега от $p_1 \dots p_{k-1} . c q_m = q_1 \dots q_{m-1} \Rightarrow$

$(p_1 \dots p_{k-1} . c - q_1 \dots q_{m-1}) q_m \equiv 0_F$ в пръстена $F[x]$ откъдето $p_1 \dots p_{k-1} . p_k + c = q_1 \dots q_{m-1}$. Полагаме предп. т.е. при индукция по $k \Rightarrow k-1 = m-1$ и $\exists$ пермутация $q_1 \dots q_{m-1}$ т.к $p_i = c_i q_i$ за $c_i \in F^*$, $p_{k-1} c = c_{k-1} q_{k-1}$. Полагаме $c_{k-1} := c^{-1} c_{k-1}$