Def. Polinom T dijeli polinom S ($T|S$) ili polinom S je djeljiv polinomom T ($S:T$), ako $\exists$ polinom Q takav da je $S = Q \cdot T$

Teorema a) Ako polinomi $S|T$ i $T|R \Rightarrow S|R$.

b) Ako $S|T$ i $T|S$ onda $(\exists a \in F)\ S = aT$

c) Ako $S|T$ i $S|R \Rightarrow S|T+R$ (obrnuto ne vrijedi)

d) Ako $S|T \Rightarrow S|TR$

$\forall S, T, R \in F[t]$.

Def. Polinom W je najveći zajednički djelitelj polinoma S i T ako: 1) $W|S$ i $W|T$

2) $\forall W_1$, $W_1|S$ i $W_1|T \Rightarrow W_1|W$

$W = NZD(S,T)$ (Polinom najvećeg stepena koji dijeli oba polinoma S i T.)

Teorema. Za svaka dva polinoma S i T od kojih je bar jedan različit od nule postoji tačno jedan normiran polinom W koji je njihov zajednički djelilac.

Dokaz. (***).

Posmatrajmo svakom polinomu $P \in F[t]$ tk. polinomsku funkciju $\Psi(P)$, koja preslikava polje F u polje F na sledeći način:

$$(\forall P): P \longmapsto \Psi(P)$$

$$F[t] \qquad Pol(F)$$

$$\Psi(P): F \to F,$$

$$(\forall x \in F)\ \Psi(P)(x) = a_0 + a_1 x + \dots + a_n x^n$$

Označimo sa $Pol(F)$ skup svih polinomijalnih funkcija polinoma iz $F[t]$.

Teorema. $(F^F, +, \cdot)$ – komutativan, asocijativan prsten sa 1 ($\to$ prsten funkcija)

$F^F = \{f \mid f: F \to F\}$

$(f+g)(x) = f(x)+g(x)$

$(f\cdot g)(x) = f(x)\cdot g(x)$

$Pol(F) \leq F^F$ (podskup)

Teorema. Funkcija $\Psi: P \to \Psi(P)$, $\forall P \in F[t]$ $(\Psi(P) \in Pol(F))$ je epimorfizam integralnog domena i podskup $Pol(F) \leq F^F$.

Dokaz. $\forall P, Q \in F[t]$

$\left.\begin{aligned}\Psi(P+Q) &= \Psi(P)+\Psi(Q)\\ \Psi(P\cdot Q) &= \Psi(P)\cdot\Psi(Q)\end{aligned}\right\}$

Zaista, $\forall P = (a_0, a_1, \dots, a_n)$

$Q = (b_0, b_1, \dots, b_m)$

$\Psi(P+Q)(x) = \Psi((a_0,a_1,\dots,a_n)+(b_0,b_1,\dots,b_m))(x) = \Psi((a_0+b_0, a_1+b_1, \dots, a_n+b_n, b_{n+1}, \dots, b_m))$

$\overset{(x)}{=} (a_0+b_0) + (a_1+b_1)x + \dots + (a_n+b_n)x^n + b_{n+1}x^{n+1} + \dots + b_m x^m = a_0 + a_1x + \dots + a_nx^n + b_0 + b_1x + \dots + b_mx^m = \Psi(P)(x) + \Psi(Q)(x)$

$= (\Psi(P)+\Psi(Q))(x)$, $\forall x \in F$

$\Rightarrow \Psi(P+Q) = \Psi(P)+\Psi(Q)$

Slično, $\Psi(P\cdot Q) = \Psi(P)\cdot\Psi(Q)$

Dakle, preslikavanje $\Psi: F[t] \to Pol(F)$ je homomorfizam

ovih str. Dalje je da je Ψ surjekcija

$\forall a_0 + a_1x + \dots + a_nx^n$

$\exists P = (a_0, a_1, \dots, a_n) \in F[t]$

$\Psi(P) = a_0 + a_1x + \dots + a_nx^n$.

Pretpostavimo da preslikavanje Ψ ne mora da bude injekcija, ali jeste injekcija u slučaju beskonačnog polja. Dakle, ako je F-beskonačno polje onda je: $\Psi: F[t] \to Pol(F)$ izomorfizam ovih struktura, pa se svaki polinom P može posmatrati sa svojom polinomskom funkcijom.

U slučaju konačnog polja F preslikavanje Ψ ne mora da bude injekcija.

Npr. $F = \mathbb{Z}_3 = \{0,1,2\}$

$P = (1,2,1,1)$

$Q = (1,0,1)$

$P \neq Q$

$\Psi(P)(x) = 1 + 2x + x^2 + x^3$

$\Psi(Q)(x) = 1 + 0 \cdot x + 1 \cdot x^2$

$\Psi(P) = \Psi(Q)$

Za $x = 0$ $\quad \Psi(P)(0) = 1$, $\Psi(Q)(0) = 1$

$x = 1$ $\quad \Psi(P)(1) = 2$, $\Psi(Q)(1) = 2$

$x = 2$ $\quad \Psi(P)(2) = 2$, $\Psi(Q)(2) = 2$

Primjetimo da u prstenu $Pol(F)$ mogu da postoje djelioci nule, u slučaju da je polje F konačno.

Npr. $F = \mathbb{Z}_3 = \{0,1,2\}$

$f(x) = x$

$g(x) = x^2 + 2$

$(f \cdot g)(x) = f(x) \cdot g(x) = x \cdot (x^2+2) = x^3 + 2x$

Za $x = 0$ $\quad f \cdot g = 0$

$x = 1$ $\quad f \cdot g = 0$

$x = 2$ $\quad f \cdot g = 0$

$f \cdot g = 0$ ueka je $f \neq 0$ i $f \neq 0$

Pokažimo da ako je polje F konačno, tj. $|F| = m$, onda $|F^*| = |F \setminus \{0\}| = m-1$. $(F^*, \cdot)$ Abelova grupa (multiplikativna).

Dokazuje se da u svakom konačnom polju F, $|F| = m$ vrijedi:

$$x^m - x = 0, \quad \forall x \in F$$

$|F| = m$, $|F^*| = m-1$

Neka je $x \in F^*$, tj. $x \in F, x \neq 0$. Razmotrimo skup:

$H = \{x^u \mid u \in N\}$. Ovaj skup ne može da bude beskonačan, jer je polje F konačno. Dakle, mora stepenovanje x^n imati i jednakih. Neka je, recimo, $x^r = x^t$ za neke $r, t \in N$: Oprost se ne umanjuje ako pretpostavimo da je $r > t$. Onda, $x^{r-t} = e$, gde je e - jedinica multiplikativne grupe F^*. Označimo $r - t = s$. Onda, $x^s = e$.

Neka je $A = \{s \in N \mid x^s = e\} \subseteq N$. Ovo je neprazan skup, podskup skupa prirodnih brojeva koji je dobro uređen, a to znači da svaki neprazni podskup ima najmanji element. Neka je $l = \min A$. Tada, $H = \{x, x^2, x^3, \dots, x^{l-1}\}$, $x^l = e$. $|H| = l \mid m-1$, prema Lagrangeovoj teoremi. To znači, da je $m - 1 = l \cdot k$, za neko k. Onda, $x^{m-1} = x^{lk} = (x^l)^k = e^k = e$, tj. $x^{m-1} = 1$, $\forall x \in F^*$, odnosno za $\forall x \in F$, $x^m = x$ tj. $x^m - x = 0$, $\forall x \in F$.

Vrijednost polinoma P u tački a je ostatak koji se dobije dijeljenjem polinoma P polinomom $x - a$.

a je <u>korijen</u> ili <u>nula</u> polinoma P ako je a korijen ili nula odgovarajuće polinomske funkcije.

<u>Teorema (Bezuova teorema)</u> Vrijednost polinoma P nad poljem F u tački a jednaka je ostatku pri dijeljenju polinoma P polinomom $(x - a, 1) = t - a$.

<u>Dokaz:</u> $P = (b - a) \cdot Q + R$, $R = 0$ ili $\operatorname{st} R < 1$

$\psi(P) = \psi(t - a)\psi(Q) + R \rightarrow$ ili 0 ili konstantni polinom.

$\forall x \in F : \psi(P)(x) = (x-\alpha)\psi(Q)(x) + R$ pa i za $x=\alpha$: $\psi(P)(\alpha) = (\alpha-\alpha)\psi(Q)(\alpha) + R$
$\psi(P)(\alpha) = R$.

2.***) Ако је $S=0 \wedge T\neq 0$, тада је $нзд(S,T)=a^{-1}\cdot T$ где је a водећи коефицијент полинома T.
Аналогно, ако је $S\neq 0$ и $T=0$.
Нека је сада $\deg(S) \geq \deg(T)$. Имамо:

$S = QT + R_1 \wedge (R_1=0 \vee \deg(R_1)<\deg(T))$

$T = Q_1R_1+R_2 \wedge (R_2=0 \vee \deg(R_2)<\deg(R_1))$

$R_1 := Q_2R_2+R_3$

$R_{k-2} = Q_{k-1}R_{k-1}+R_k \wedge (R_k=0 \vee \deg(R_k)<\deg(R_{k-1}))$

$R_{k-1} = Q_kR_k$.

Из горњег алгоритма (познатог под називом Еуклидов алгоритам) за добијање низа полинома $R_1, R_2, \ldots$ очигледно постоји природ. бр. k за који је $R_{k+1}=0 \vee \deg(R_k)=0$, јер је $\deg(T)>\deg(R_1)>\deg(R_2)>\ldots>\deg(R_{k-1})>\ldots$
Сада ћемо показати да је R_k заједнички делилац полинома S и T. Из последње једнакости следи: $R_k|R_{k-1}$, $R_k|R_{k-2}, \ldots$ $R_k|T$, $R_k|S$. Дакле, $R_k=зд(S,T)$.
Претпоставимо да $W_1|S \wedge W_1|T$.
Из прве једнакости, следи $W_1|R_1$, $W_1|R_2, \ldots, W_1|R_k$. Дакле, $R_k=нзд(S,T)$, а тражени нормализован полином је $W=a^{-1}R_k$, где је a водећи коефицијент полинома R_k. Јединственост је јасна.