Teorema. Polinom $t-\alpha$ je faktor polinoma P akko je α korijen tog polinoma.

Dokaz. $\Rightarrow$ Neka je polinom $t-\alpha$ faktor polinoma P. Onda

$P = (t-\alpha)\cdot Q \Rightarrow \Psi(P) = \Psi(t-\alpha)\cdot\Psi(Q)$

$(\forall x \in F)\ \Psi(P)(x) = (x-\alpha)\Psi(Q)(x)$

Specijalno za $x=\alpha$, $\Psi(P)(\alpha) = \underbrace{(\alpha-\alpha)}_{=0}\Psi(Q)(\alpha)$

$\Psi(P)(\alpha)=0$

$\Rightarrow$ α-nula polinomske funkcije $\Psi(A)$ odnosno nula (korijen) polinoma P.

$\Leftarrow$ Neka je α korijen polinoma P. Prema Bezuovoj teoremi vrijednost polinoma P u toj tački jednaka je ostatku R pri dijeljenju polinoma P polinomom $(t-\alpha)$:

$\Rightarrow \underbrace{\Psi(P)(\alpha)}_{0 \text{ (jer je korijen } \alpha)} = R \Rightarrow R=0 \Rightarrow P = (t-\alpha)\cdot Q + 0 \Rightarrow (t-\alpha)$ je faktor polinoma P

Def. Polinom $t-\alpha$ iz prethodne teoreme se naziva korijenim faktorom polinoma P.

Teorema. Svaki polinom $P_n(t)$ (n-tog stepena) ima najviše n-korijena.

Dokaz. Ako polinom $P_n(t)$ nema korijena, dokaz je završen.

Zato, pretpostavimo da polinom $P_n(t)$ ima bar jedan korijen α.

Dokaz. Indukcijom po n (stepen polinoma)

Za $n=1$: $P_1(t) = a_0 + a_1 t$, $a_1 \neq 0$

$\Rightarrow$ Linearni polinom uvijek ~~ima~~ korijen u polju $F \Rightarrow a_0 + a_1 t = 0$

Dalje, $\alpha = -a_1^{-1}\cdot a_0$. $t = -a_1^{-1}\cdot a_0 \in F$.

Neka tvrdnja teoreme vrijedi za $n-1$. Dokažimo da vrijedi i za n

Polinom $P_n(t) = (t-\alpha)\cdot Q_{n-1}(t)$.

Po pretpostavci $\Rightarrow$ $Q_{n-1}(t)$ ima najviše $n-1$ korijena, pa prema tome, polinom $P_n(t)$ ima najviše n-korijena.

Teorema. Svaki polinom P, nad beskonačnim poljem F je nula-polinom akko je svaki element polja F - korijen polinoma P.

Dokaz. $\Rightarrow$ trivijalno.

$\Leftarrow$ Svaki polinom P je ili nula polinom ili je određenog stepena n. Ako je polinom određenog stepena n: $P_n(t)$, onda prema prethodnoj teoremi - ima najviše n-korijena (konačno) što je nemoguće jer je polje F beskonačno polje $\Rightarrow$ P je nula polinom.

Teorema. Polinomi $P=(a_0,\dots,a_n)$, $Q=(b_0,\dots,b_m)$, $n\leq m$, nad beskonačnim poljem F su jednaki akko su im jednake polinomske funkcije. tj. $P=Q \iff \Psi(P)=\Psi(Q)$.

Dokaz. $\Rightarrow$ $P=Q \Rightarrow \Psi(P)=\Psi(Q)$ trivijalno.

$\Leftarrow$ Neka je $\Psi(P)=\Psi(Q)$. To znači da $(\forall x\in F)$: $\Psi(P)(x)=\Psi(Q)(x)$ tj. $a_0+a_1x+\dots+a_nx^n = b_0+b_1x+\dots+b_mx^m \Rightarrow (a_0-b_0)+(a_1-b_1)x+\dots+(a_n-b_n)x^n-b_{n+1}x^{n+1}-\dots-b_mx^m=0$. Prema prethodnoj teoremi, polinom na lijevoj strani je nula polinom $\Rightarrow$

$b_{n+1}=0$, $\dots$, $b_m=0$ onda je $n=m \Rightarrow a_0=b_0, a_1=b_1, \dots, a_n=b_n$

$\Rightarrow$ Preslikavanje $\Psi: F[t]\to Pol(F)$ je injekcija, tj. izomorfizam.

$\Rightarrow$ Ako je F beskonačan, onda je i polinom P može poistovjetiti sa svojom polinomskom funkcijom.

Def. Polinom je svodljiv (reducibilan) ako se može predstaviti kao produkt dva polinoma nižeg stepena od stepena polinoma P. U protivnom, tj. ako je on nesvodljiv (ireducibilan) polinom.

- Konstantni polinomi su ni svodljivi ni nesvodljivi.

Teorema. Neka je $P \in F[t]$ polinom drugog ili trećeg stepena. Polinom P je svodljiv nad poljem F akko ima bar jednu nulu u tom polju.

Dokaz. $\Rightarrow$ Neka je polinom P svodljiv nad poljem F. Po pretpostavci, bar jedan faktor polinoma P je linearan, $(t-\lambda)$, pa je $\lambda \in F \rightarrow$ korijen polinoma P.

$\Leftarrow$ Neka je λ bar jedan korijen polinoma P ($\lambda \in F$), Po teoremi 1, onda je polinom $(t-\lambda)$- faktor polinoma P.
Dakle polinom P je svodljiv nad poljem F.

Teorema. (ekvivalentna prethodnoj). Neka je $P \in F[t]$ -polinom drugog ili trećeg stepena. Onda polinom P je nesvodljiv nad poljem F akko nema nijednu nulu u tom polju.

Teorema. (Osnovni stav algebre). Svaki polinom P_n- nenultog stepena ima nad poljem $\mathbb{C}$ bar jednu nulu (u tom polju)
(bez dokaza, ali Gauss je dao 4 dokaza).

Teorema. Svaki polinom $P_n(t) = a_0 + a_1 t + \dots + a_n t^n$ stepena $n > 0$ nad poljem $\mathbb{C}$ može se zapisati u obliku $P_n(t) = a_n(t-t_1)\dots(t-t_n)$, gdje je $t = (0,1)$ a $a_n, t_1, \dots, t_n \in \mathbb{C}$.

Dokaz. Polinom $P_n(t)$, $n>0$ ima bar jedan korijen t_1 u polju $\mathbb{C}$ prema prethodnoj teoremi. Onda, $P_n = (t-t_1)P_{n-1}$ prema prethodnoj teoremi polinom P_{n-1} ima bar jedan korijen t_2 u polju $\mathbb{C}$, pa je $P_{n-1} = (t-t_2)P_{n-3}$ itd. Dobijamo $P_n = (t-t_1)(t-t_2) - (t-t_{n-1})P_1$ - linearni polinom.

$P_1 = a_0 + a_1 t = a_1(t-t_n)$ gdje je $t_n = -a_1^{-1}a_0 \in F$ tj. $P_1 = a(t-t_n)$
Zapisano u gornjoj jednakosti i izjednačavanje koeficijenata uz t^n, dobijamo $a = a_n$. Konačno $P_n = a_n(t-t_1)(t-t_2)\dots(t-t_n)$.

Teorema. Ako je P polinom nad poljem $\mathbb{R}$ realnih brojeva i λ njegov korijen, onda je njemu konjugirani kompleksni $\bar{\lambda}$ također korijen tog polinoma.

Dokaz. Kako je polje $\mathbb{R}$ beskonačno, onda je $P = \Psi(P)$, tj.

$(\forall x \in \mathbb{R})\ \Psi(P)(x) = P(x) = a_0 + a_1 x + \dots + a_n x^n = a_n(x-x_1)(x-x_2)\cdots$
$\cdot (x-x_n)$. $\overline{P(x)} = a_0 + a_1 \bar{x} + \dots + a_n \bar{x}^n = P(\bar{x}) = a_n(\bar{x}-x_1)$
$(\bar{x}-x_2)\cdots(\bar{x}-x_n)$.

$P(\bar{x}) = \overline{\overline{P(x)}} = a_n(x-\bar{x}_1)(x-\bar{x}_2)\cdots(x-\bar{x}_n)$.

Neka je λ korijen polinoma P onda je $P(\lambda)=0$, tj. $x_i - \lambda = 0$, za neko $i = \overline{1,n}$, odnosno $x_i = \lambda$. Odavde, $\bar{x}_i = \bar{\lambda}$ $P(\bar{\lambda})=0$ jer je $\bar{\lambda} - \bar{x}_i = 0$, tj. $\bar{\lambda} = \bar{x}_i$.

Teorema. Svaki polinom P nad poljem $\mathbb{R}$ realnih brojeva, može se zapisati u obliku proizvoda polinoma stepena < 3, čiji su koeficijenti realni.

Dokaz. Prema prethodnoj teoremi ako je λ korijen polinoma P nad poljem $\mathbb{R}$ onda je i $\bar{\lambda}$ njegov korijen, to znači da će se u faktorizaciji polinoma P, naći proizvod faktora: $(t-\lambda)(t-\bar{\lambda})$

$= t^2 - \underbrace{(\lambda+\bar{\lambda})}_{-p} t + \underbrace{\lambda\cdot\bar{\lambda}}_{q} = \Big\lceil \lambda = x \pm iy,\ x,y \in \mathbb{R},\ i=\sqrt{-1}$
$\bar{\lambda} = x - iy$
$\lambda + \bar{\lambda} = 2x$
$\lambda\cdot\bar{\lambda} = x^2+y^2 \in \mathbb{R} \Big\rfloor$

$= t^2 + pt + q$

$P = a_n(t^2+p_1t+q_1)\cdots(t^2+p_kt+q_k)\cdot(t-t_{r_1})\cdots(t-t_{r_m})$

$p_i, q_i,\ i=\overline{1,k} \in \mathbb{R}$, $a_n \in \mathbb{R}$
$t_{r_j},\ j=\overline{1,m}$
$\rightarrow$ realni korijeni polinoma

Def. Korijen λ polinoma P je **višestrukosti k** (k-tostruki korijen) ako je polinom P djeljiv polinomom $(t-\lambda)^k$ i nije djeljiv polinomom $(t-\lambda)^{k+1}$. $P = (t-\lambda)^k \cdot Q$, $Q(\lambda)\neq 0$.

Teorema Korijen λ polinoma P je višestrukosti k akko je λ korijen višestrukosti $k-1$ izvodnog polinoma P'. Drugim rječima, λ je korijen višestrukosti k polinoma P akko je λ zajednički korijen polinoma $P, P', P'', \dots P^{(k-1)}$.

Dokaz $\Rightarrow$ $P = (t-\lambda)^k \cdot Q$, $Q(\lambda) \neq 0$

$$P' = k(t-\lambda)^{k-1} \cdot Q + (t-\lambda)^k \cdot Q'$$

$$P' = (t-\lambda)^{k-1} \cdot (\underbrace{kQ + (t-\lambda)\cdot Q'}_{\neq 0})$$

za $t=\lambda$
$kQ(\lambda) \neq 0$ jer $Q(\lambda) \neq 0$

Dalje, λ je korijen izvodnog polinoma P' višestrukosti $k-1$.

$\Leftarrow$ Direktna posljedica $\Rightarrow$. ∎

$F[t]$ - prsten polinoma nad poljem F

Prsten polinoma nad poljem $F[T]$ je značajan. Ima konstrukcije proširenja polja. (teorija polja, odnosno teorija Galoa)