Polynomy

1. Proč kořenový činitel dělí polynom beze zbytku.

11.41. Definice. *Kořen polynomu* p je takové číslo $\alpha \in \mathbf{C}$, pro které je $p(\alpha) = 0$. Pokud α je kořen polynomu p, pak polynom daný vzorcem $x-\alpha$ pro všechna $x \in \mathbf{C}$ nazýváme *kořenový činitel polynomu* p.

Skripta 11.42 str. 170

11.42. Věta. Polynom p je dělitelný svým kořenovým činitelem.

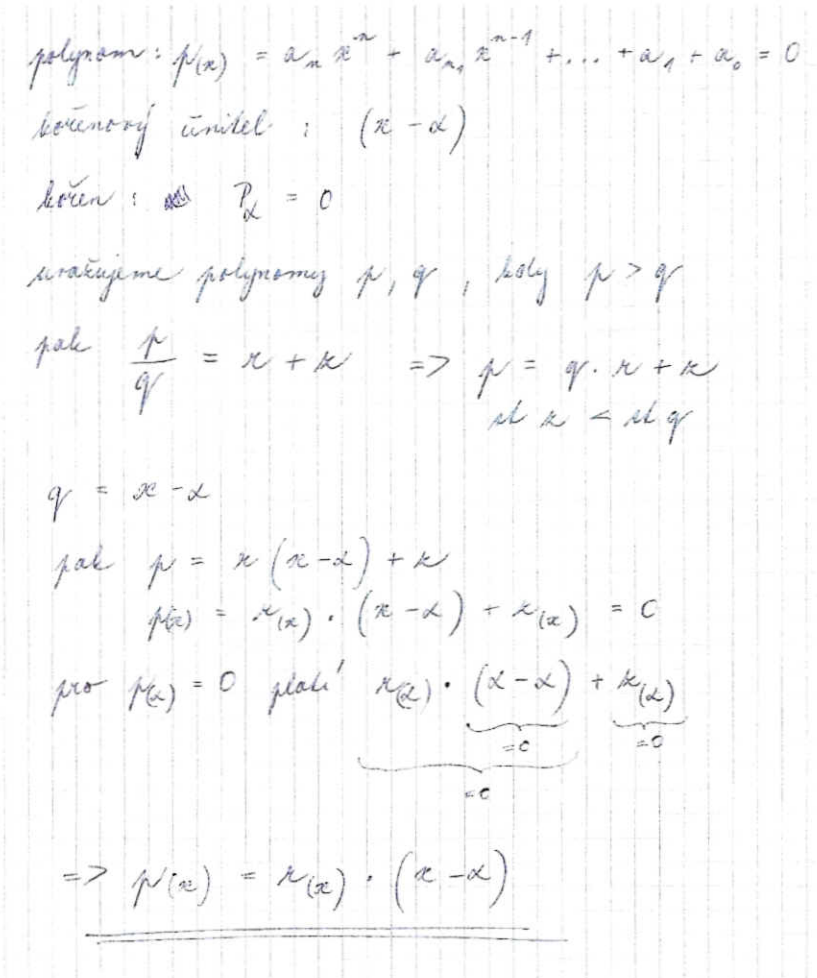
Důkaz. Zbytek po dělení polynomu p polynomem $x-\alpha$ má podle věty 11.31 stupeň menší než 1, tedy jedná se o konstantu. Označme ji c. Pro všechna $x \in \mathbf{C}$ platí: $p(x) = r(x)\,(x-\alpha)+c$. Po dosazení $x=\alpha$ máme $p(\alpha) = r(\alpha)\cdot 0 + c = c$. Protože α je kořen, je $p(\alpha)=0$, takže $c=0$. Skutečně tedy polynom $x-\alpha$ dělí polynom p beze zbytku.

11.43. Poznámka. Nechť α_1 je kořen nenulového polynomu p. Zatím ponecháme stranou problém hledání kořene a spokojíme se s tím, že kořen polynomu p existuje a označíme jej α_1. Podle předchozí věty je možné dělit kořenovým činitelem, neboli $p(x) = r_1(x)\,(x-\alpha_1)$. Z této rovnosti plyne, že všechny kořeny polynomu r_1 jsou zároveň kořeny polynomu p. Polynom p má kromě kořenů polynomu r_1 navíc jen kořen α_1. Je tedy možné hledat další kořeny polynomu p tak, že najdeme kořeny polynomu r_1. Přitom tento polynom má podle věty 11.28 o jedničku menší stupeň, než má polynom p.

Nechť α_2 je kořen polynomu r_1. Máme tedy $p(x) = r_2(x)\,(x-\alpha_1)\,(x-\alpha_2)$. Další kořeny polynomu p můžeme hledat tak, že najdeme kořeny polynomu r_2. Úvahu opakujeme tak dlouho, až se polynom r_i stane konstantním polynomem nebo až nastane situace, že polynom r_i nebude mít kořeny. Postup skončí určitě po konečně mnoha krocích, neboť stupně polynomu r_i se snižují. V závěru tedy máme

$$p(x) = r_m(x)\,(x-\alpha_1)\,(x-\alpha_2)\cdots(x-\alpha_m), \tag{11.4}$$

kde r_m je polynom bez kořenů (věta 11.49 ukáže, že takový případ nastává jen pro konstatní polynom) a α_i jsou všechny kořeny polynomu p. V zápise (11.4) se mohou některé kořeny α_i vyskytovat vícekrát. Takovým kořenům říkáme vícenásobné, viz následující definice.



2. Proč celočíselný kořen polynomu s celočíselnými koeficienty dělí a_0.

11.58. Věta. Nechť polynom p má celočíselné koeficienty $a_0, a_1, \ldots, a_n$. Je-li α celočíselným kořenem polynomu p, pak α dělí koeficient a_0.

Důkaz. Věta je speciálním případem následující věty pro $d = 1$.

11.59. Věta. Nechť polynom p stupně n má celočíselné koeficienty $a_0, a_1, \ldots, a_n$. Je-li $\alpha = \frac{c}{d}$ racionálním kořenem polynomu p a čísla c, d jsou celá nesoudělná, pak c dělí a_0 a d dělí a_n.

Důkaz. Protože $\frac{c}{d}$ je kořen, platí

$$a_0 + a_1 \frac{c}{d} + a_2 \left(\frac{c}{d}\right)^2 + \cdots + a_n \left(\frac{c}{d}\right)^n = 0.$$

Po převedení a_0 na druhou stranu rovnosti, vynásobení rovnosti číslem d^n a vytknutí čísla c dostáváme

$$c\,(a_1 d^{n-1} + a_2 c d^{n-2} + a_3 c^2 d^{n-3} + \cdots + a_n c^{n-1}) = -a_0 d^n.$$

Číslo $e = -d^n$ je nesoudělné s c a uvedená závorka obsahuje celé číslo, které označíme k. Výše uvedená rovnost má tvar $c \cdot k = a_0 \cdot e$. Číslo c tedy musí dělit a_0. Nyní vyjádříme z původní rovnosti a_n:

$$d\,(a_0 d^{n-1} + a_1 c d^{n-2} + a_2 c^2 d^{n-3} + \cdots + a_{n-1} c^{n-1}) = -a_n c^n.$$

Podobnou úvahou jako před chvílí dospíváme k závěru, že d musí dělit a_n.

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0 = 0$

x = celočíselný kořen
a = celé číslo
} viz zadání

$\Rightarrow a \cdot x$ = celé číslo

$a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x = -a_0$

$-x \underbrace{\left(a_n x^{n-1} + a_{n-1} x^{n-2} + \ldots a_1\right)}_{\text{= celé číslo}} = a_0$

$-\left(a_n x^{n-1} + a_{n-1} x^{n-2} + \ldots a_1\right) = \frac{a_0}{x}$

3. Dokažte, že ke každému kořenu polynomu s reálnými koeficienty existuje kořen komplexně sdružený.

$x = \overline{x}$ právě když $x \in R$, protože $\overline{a + 0i} = a - 0i = a$

11.65. Poznámka. V příkladech 11.61, 11.62, 11.64 vyšly komplexní kořeny vzájemně po dvou komplexně sdružené. Následující věty ukazují, že se nejedná o náhodu, ale pro polynomy s reálnými koeficienty je to zákonitá vlastnost.

11.66. Věta. Je-li α kořen polynomu p s reálnými koeficienty, pak komplexně sdružené číslo $\overline{\alpha}$ je také kořenem polynomu p.

Důkaz. Připomenu, že komplexně sdružené číslo značíme pruhem nad číslem a definujeme jako číslo s opačnou imaginární částí, tj. $\overline{a + ib} = a - ib$. Dále je potřeba připomenout základní vlastnosti:

$x = \overline{x}$ právě když $x \in \mathbf{R}$, protože $\overline{a + 0i} = a - 0i = a$.
$\overline{x} + \overline{y} = \overline{x + y}$, protože $\overline{a + ib} + \overline{c + id} = a + c - i(b + d) = \overline{a + ib + c + id}$.
$\overline{x}\,\overline{y} = \overline{xy}$, protože $(a - ib)(c - id) = ac - bd - i(bc + ad) = \overline{ac - bd + i(bc + ad)} = \overline{(a + ib)(c + id)}$.
$\overline{x^n} = \overline{x}^n$, protože $\overline{x} \cdot \overline{x^{n-1}} = \overline{x\,x^{n-1}} = \overline{x^n}$.

Jelikož α je kořen, platí $p(\alpha) = 0$. Máme dokázat, že $p(\overline{\alpha}) = 0$.

$$\begin{aligned} p(\overline{\alpha}) &= a_0 + a_1\overline{\alpha} + a_2\overline{\alpha}^2 + \cdots + a_n\overline{\alpha}^n = \overline{a_0} + \overline{a_1}\,\overline{\alpha} + \overline{a_2}\,\overline{\alpha}^2 + \cdots + \overline{a_n}\,\overline{\alpha}^n = \\ &= \overline{a_0} + \overline{a_1}\,\overline{\alpha} + \overline{a_2}\,\overline{\alpha^2} + \cdots + \overline{a_n}\,\overline{\alpha^n} = \overline{a_0} + \overline{a_1\,\alpha} + \overline{a_2\,\alpha^2} + \cdots + \overline{a_n\,\alpha^n} = \\ &= \overline{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n} = \overline{p(\alpha)} = \overline{0} = 0. \end{aligned}$$

Nejprve jsme využili toho, že koeficienty $a_0, a_1, \ldots, a_n$ jsou reálné. Další rovnosti plynou ze základních vlastností komplexně sdruženého čísla.

Věta nevylučuje případ, že α je reálný kořen. Pak ale $\overline{\alpha} = \alpha$, což je také (tentýž) kořen.

x = komplexní číslo $\neq x = a + ib$

$\overline{x}$ = komplexně sdružené číslo $\neq \overline{x} = a - ib$

základ: $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$

$\overline{x} + \overline{y} = \overline{x + y}$

$\overline{x}^n = \overline{x^n}$

(VÍM) α = kořen $\Rightarrow 0 = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0$

(NEVÍM) $\overline{\alpha}$ = komplexně sdružený $\Rightarrow 0 = a_n\alpha^n + \ldots + a_1\alpha + a_0$

(Dk)

$$a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \ldots + a_1\overline{\alpha} + a_0 \overset{?}{=} 0$$

$$\overline{a}_n\overline{\alpha}^n + \overline{a}_{n-1}\overline{\alpha}^{n-1} + \ldots + \overline{a}_1\overline{\alpha} + \overline{a}_0 \overset{?}{=} 0$$

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$$

$\Rightarrow \overline{p(\alpha)} = 0$

4. Proč ke každým dvěma polynomům p, q (q nenulový) je určen částečný podíl a zbytek jednoznačně?

11.31. Věta. Nechť p, q jsou polynomy, q nenulový. Pak existuje právě jeden polynom r a právě jeden polynom z tak, že (i) $p = rq + z$, (ii) stupeň z je menší než stupeň q.

Důkaz. Existence polynomů r a z vyplývá z následujícího algoritmu, pomocí kterého je možné tyto polynomy na základě daných polynomů p a q najít.

(1) Položme $r = 0$ (nulový polynom) a $z = p$. Dále označme písmenem n stupeň polynomu q a písmenem c jeho koeficient s indexem n (tj. nenulový koeficient u nejvyšší mocniny polynomu q).
(2) Je-li stupeň z menší než n, algoritmus končí.
(3) Nechť m je stupeň polynomu z a nechť d je jeho koeficient s indexem m (koeficient u nejvyšší mocniny). Platí $m \geq n$, protože není splněna podmínka z kroku (2). K polynomu r přičteme polynom daný vzorcem $(d/c)\, x^{m-n}$ a od polynomu z odečteme polynom daný vzorcem $(d/c)\, x^{m-n}\, q(x)$. Vznikají nové polynomy r_1 a z_1, které dále označíme r a z a vracíme se ke kroku (2).

V kroku (3) se snižuje stupeň polynomu z, protože se od tohoto polynomu odečítá sčítanec s nejvyšší mocninou. Tím je zaručeno, že stupeň polynomu z postupně klesá a algoritmus určitě skončí. Krok (2) navíc zaručuje, že je splněno (ii) z tvrzení věty. Další vlastností algoritmu je skutečnost, že v každém okamžiku platí pro polynomy r a z podmínka (i), takže tato podmínka je splněna i po ukončení algoritmu. Především v kroku (1) je $r = 0$ a $z = p$, takže $rq + z = 0q + p = p$ a podmínka (i) je splněna. Dále v kroku (3) máme zaručeno, že $p = rq + z$ a ukážeme, že platí také $p = r_1 q + z_1$. Pro všechna $x \in \mathbf{C}$ je

$$r_1(x)\, q(x) + z_1(x) = \left(r(x) + \frac{d}{c}\, x^{m-n}\right) q(x) + \left(z(x) - \frac{d}{c}\, x^{m-n}\, q(x)\right) =$$
$$= r(x)\, q(x) + \frac{d}{c}\, x^{m-n}\, q(x) + z(x) - \frac{d}{c}\, x^{m-n}\, q(x) = r(x)\, q(x) + z(x) = p(x).$$

Jednoznačnost polynomů r a z je jednoduchým důsledkem věty o stupni součtu a součinu polynomů. Kdyby existovaly polynomy r_2 a z_2, které rovněž splňují (i) a (ii), pak je $p = rq + z = r_2 q + z_2$, takže $(r - r_2)\, q = z_2 - z$. Kdyby $r - r_2$ nebyl nulový polynom, pak stupeň polynomu $(r - r_2)q$ by byl větší nebo roven stupni q, zatímco polynom $z_2 - z$ má stupeň menší než q. To je ovšem spor. Takže musí $r - r_2$ být nulový polynom a pak nutně též $z_2 - z$ je nulový polynom. Jinými slovy $r = r_2$ a $z = z_2$, takže polynomy r, z jsou určeny podmínkami (i) a (ii) jednoznačně.

Ke každým 2 polynomům P a Q, kde Q je nenulový, existují dva polynomy Y a Z splňující vztah:

P = YQ + Z a stp Z < stp Q.

Předpokládejme:

$P = YQ + Z$, $stpZ < stpQ$
$P = Y_1Q + Z_1$, $stpZ_1 < stpQ$

Dosadíme:

$$YQ + Z = Y_1Q + Z_1 \Rightarrow YQ - Y_1Q = Z_1 - Z$$

Upravíme:

$Q(Y - Y_1) = Z_1 - Z$

Z čehož platí:

$stp(Z_1 - Z) < stpQ$

Pro nenulový polynom (Y - Y_1) by muselo platit:

$$stp(Y - Y_1)Q \geq stpQ$$

Jenže dva polynomy různého stupně se nemůžou rovnat, a proto (Y - Y_1) je nulový polynom, takže:

$Y = Y_1$
$Z = Z_1$

A proto je částečný podíl a zbytek určen jednoznačně.

ke $\forall p, q\ (q \neq 0)\ \exists r, z$ tak, že

1) $p = r \cdot q + z$ $\qquad \frac{p}{q} = r + \frac{z}{q}$

2) $st\ z < st\ q$

PROČ JEDNOZNAČNĚ?

ke $\forall p, q\ (q \neq 0)\ \exists r, z$ tak, že
$\exists r', z'$ se stejnými vlastnostmi =
$p = r \cdot q + z = r' \cdot q + z'$

$r \cdot q + z = r' \cdot q + z'$
$(r - r') \cdot q = z' - z$

$st \geq q$ $\qquad$ $st < q$

může platit pouze tehdy, když
$r - r' = 0 \Rightarrow z' - z = 0$
pak $(r - r') : q = z' - z = 0 \Rightarrow z' = z$

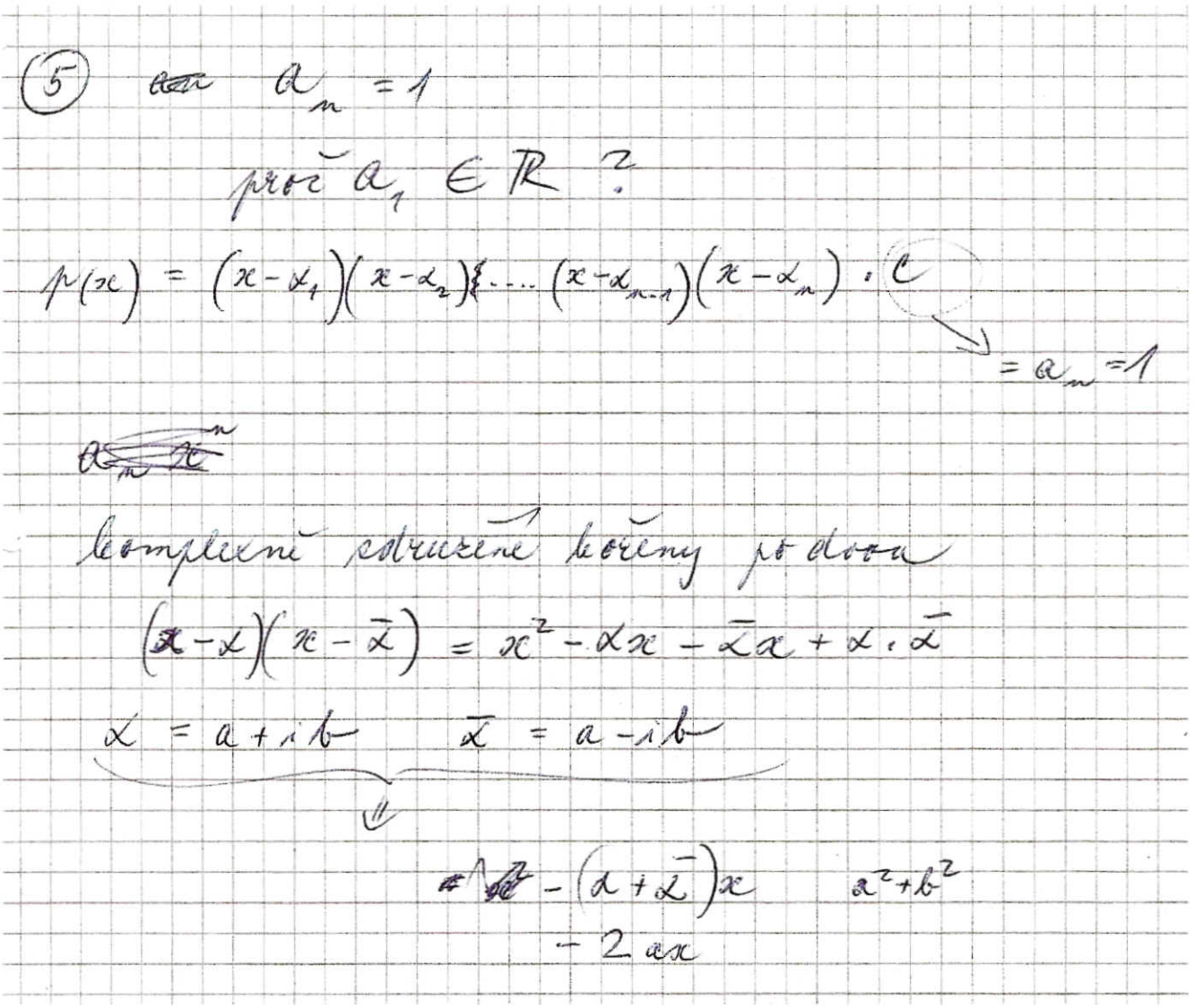
5. Nechť má polynom $a_n = 1$ a má jen reálné nebo po dvou komplexně sdružené kořeny. Proč pak má všechny koeficienty reálné?

asi 11.72, 11.73

Mohlo by to být takto...

ze to byt takhle? Má-li polynom $a_n=1$ jen reálné nebo po dvou komplexně sdružené koeficienty, pak vynásobením dvou faktorů, jejichž kořeny jsou vzájemně komplexně sdružená čísla, dostaneme součin těchto faktorů, který bude polynom s reálnými koeficienty.

Budu-li takto násobit příslušné dvojice a nakonec je vynásobím faktory, které mají reálné kořeny, pak musíme obdržet polynom s reálnými koeficienty.



6. Proč polynom lichého stupně s reálnými koeficienty musí mít alespoň jeden reálný kořen?

Polynom lichého stupně **má lichý počet kořenů**!!!

Kořeny mohou být
- reálné
- komplexně - má vždy i kořen komplexně sdružený

Protože komplexní kořeny jsou seskupeny do komplexně sdružených dvojic - např. $(1 - i)(1 + i)$, pak nereálných kořenů je sudý počet.

Polynom lichého stupně, má ale lichý počet kořenů, takže alespoň jeden kořen MUSÍ BÝT REÁLNÝ.

7. Proč nemůže mít polynom stupně *n* více než *n* vzájemně různých kořenů?

11.53. Poznámka. Důsledkem věty 11.49 je skutečnost, že polynom r_m ve vzorci (11.4) je konstantní. Z toho a z věty 11.28 také plyne, že polynom p má ve vzorci (11.4) tolik kořenových činitelů, kolik je jeho stupeň. Počítáme-li tedy každý kořen tolikrát, kolik je jeho násobnost, můžeme říci, že polynom má stejný počet kořenů, jako je jeho stupeň. Konečně, protože $(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m) = 1x^m + \cdots$, musí být konstantní polynom r_m roven koeficientu a_m, což je nenulový koeficient u nejvyšší mocniny polynomu p. Všechny tyto poznatky zformulujeme do následující věty.

11.54. Věta. Nechť p je nenulový polynom stupně n s koeficienty $a_0, a_1, \ldots, a_n$ a nechť $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbf{C}$ jsou všechny jeho navzájem různé kořeny. Nechť k_i je násobnost kořenu α_i pro $i \in \{1, 2, \ldots, s\}$. Pak platí $k_1 + k_2 + \cdots + k_s = n$ a dále pro všechna $x \in \mathbf{C}$ je

$$p(x) = a_n (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \cdots (x - \alpha_s)^{k_s}.$$

Tomuto zápisu říkáme *rozklad polynomu na kořenové činitele.*

Důkaz. Viz poznámku 11.53.

11.55. Věta. Nenulový polynom stupně n má nejvýše n různých komplexních kořenů.

Důkaz. Věta je přímým důsledkem věty 11.54.

Polynom stupně n si napíšeme jako rozklad polynomu na kořenové činitele

$$p(x) = a_n(x - a_1)^{k_1}(x - a_2)^{k_2} \cdots (x - a_s)^{k_s}$$

kde k je násobnost kořenu.

Součet všech k je roven n, tudíž počet kořenů je také roven n

8. Proč je polynom stupně n určen jednoznačně svými hodnotami v $n+1$ různých bodech?

11.56. Věta. Pokud se dva polynomy stupně nejvýše n shodují v $n+1$ různých bodech, pak jsou totožné. Jinými slovy, polynom stupně n je jednoznačně určen svými hodnotami v $n+1$ bodech.

Důkaz. Předpokládáme, že pro polynomy p a q existují vzájemně různá čísla $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}$ taková, že $p(\alpha_i) = q(\alpha_i)$ pro $i \in \{1, 2, \ldots, n, n+1\}$. Protože polynomy p a q mají stupeň nejvýše n, je podle věty 11.28 rozdíl $p - q$ polynom stupně nejvýše n, který má kořeny $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}$. Těch kořenů je více, než je jeho stupeň. To podle věty 11.55 není možné jinak, než že je polynom $p - q$ nulový. Takže $p = q$ a důkaz je hotov.

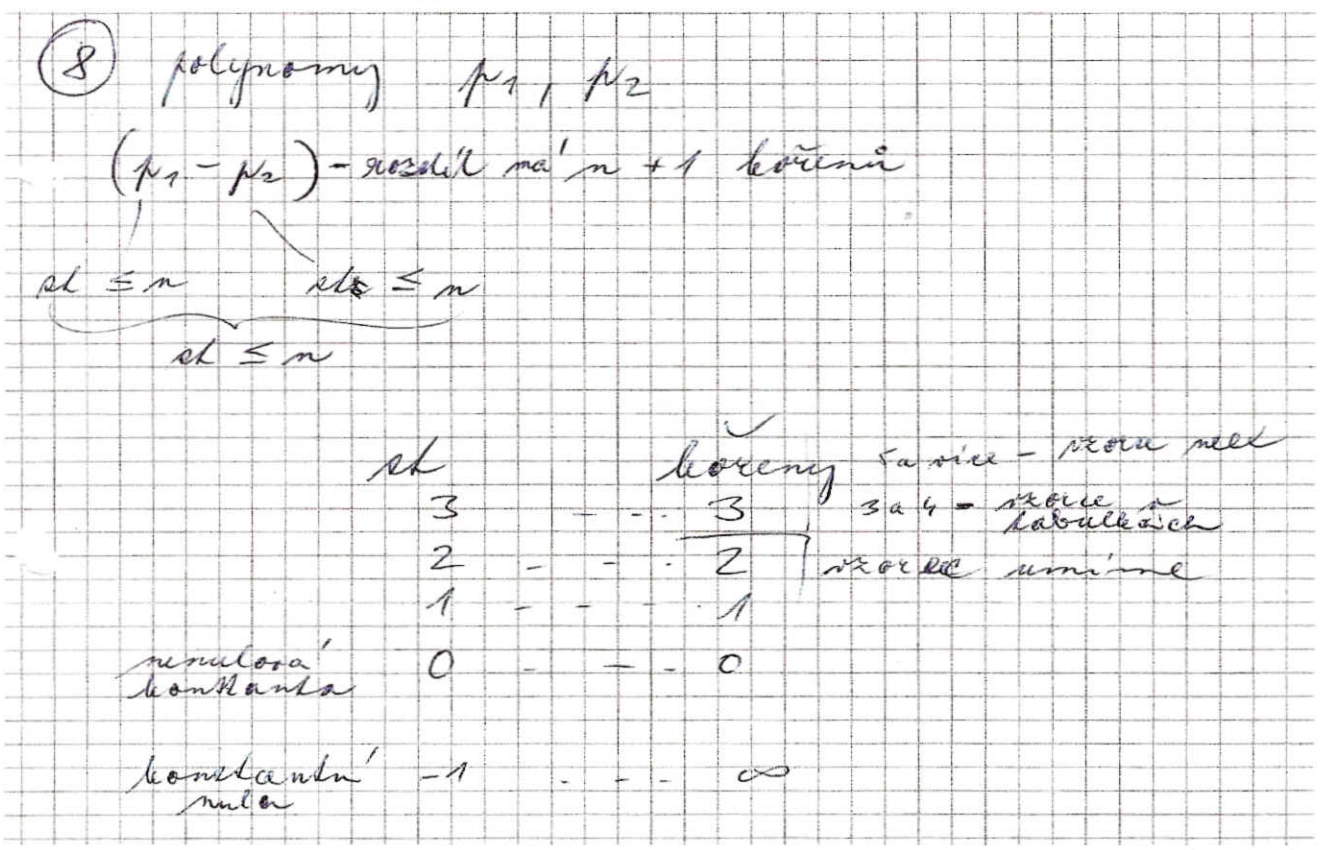
11.28. Věta. Nechť p je polynom stupně m a q je polynom stupně n. Pak $p + q$ je polynom stupně nejvýše $\max(m, n)$, αp je polynom stupně m pro $\alpha \neq 0$ a je to polynom stupně -1 pro $\alpha = 0$. Konečně pro nenulové polynomy p a q je pq polynom stupně $m + n$. Je-li p nebo q nulový, pak pq je polynom stupně -1.

Důkaz. Tvrzení plyne přímo z vět o počítání koeficientů součtu a součinu polynomů a z definice stupně polynomu.

11.29. Poznámka. Je potřeba si uvědomit, že stupeň součtu polynomů nemusí dosahovat maximum stupňů jednotlivých polynomů, které sčítáme. Kupříkladu

$$(x^3 + 2x^2 - x + 1) + (-x^3 - 2x^2 + 2x + 3) = x + 4.$$

Součet těchto polynomů stupně 3 je polynom stupně 1. Je dobré si také uvědomit, že stupeň součtu určitě nabývá máxima stupňů jednotlivých polynomů, které sčítáme, pokud stupně sčítaných polynomů jsou různé.

Věta 11.55

Nenulový polynom stupně n má nejvýše n různých komplexních kořenů.