Základy algebry

Kapitola VII. Kořeny algebraických rovnic

In: Vladimír Kořínek (author): Základy algebry. (Czech). Praha: Nakladatelství československé akademie věd, 1953. pp. 336–372.

Persistent URL: http://dml.cz/dmlcz/404233

ČÁST TŘETÍ.

ALGEBRAICKÉ ROVNICE JEDNÉ NEZNÁMÉ.

KAPITOLA VII.

KOŘENY ALGEBRAICKÝCH ROVNIC.

Třetí část knihy je věnována algebraickým rovnicím o jedné neznámé. Taková rovnice má tvar[1])

$$f(\xi) = a_0\xi^n + a_1\xi^{n-1} + \ldots + a_{n-1}\xi + a_n = 0 \,, \tag{1}$$

kdež koeficienty $a_0, a_1, \ldots, a_n$ jsou prvky daného tělesa T. Napíšeme-li vyšetřovanou rovnici ve tvaru (1), bude to znamenat, pokud nebude nic jiného řečeno, že jde o rovnici n-tého stupně, t. j. že $a_0 \neq 0$. Je-li $b \neq 0$ prvek z tělesa T, pak rovnice

$$b\,f(\xi) = a_0b\xi^n + a_1b\xi^{n-1} + \ldots + a_{n-1}b\xi + a_nb = 0 \tag{2}$$

má zřejmě právě tytéž kořeny jako rovnice (1). Jedná-li se o kořeny rovnice, je jedno, zda vyšetřujeme rovnici (1) neb místo ní rovnici (2). Vhodnou volbou prvku b lze docíliti toho, že koeficient u některého členu v (1), který není roven nule, stane se v (2) rovným 1. Nejčastěji se volí $b = a_0^{-1}$. Rovnice (1) přejde pak v ekvivalentní rovnici

$$\xi^n + a_1'\xi^{n-1} + \ldots + a_{n-1}'\xi + a_n' = 0 \,, \tag{3}$$

kdež $a_i' = a_i/a_0$, $i = 1, 2, \ldots, n$. V tomto tvaru se rovnice o jedné neznámé obyčejně vyšetřují.

Vyšetřování algebraické rovnice rozpadá se ve dvě části. Nejprve se musíme zabývat existencí kořenů, t. j. zjistit, za jakých podmínek rovnice (1) neb (3) má vůbec kořeny a stanovit jejich počet. To bude úkolem této kapitoly. Za druhé půjde o řešení této rovnice, t. j. o stanovení kořenů a o vyšetření jejich vlastností. To bude úkolem kapitol dalších.

Pokud se týče prvního úkolu, budeme se nejdříve zabývat rovnicemi s číselnými koeficienty a dokážeme si, že vždy existuje komplexní číslo, které je kořenem takové rovnice. Abychom si tuto věc dokázali, musíme provésti jistá vyšetřování přípravná. To učiníme v § 37, při čemž některé věty z tohoto paragrafu mají i důležitost samy o sobě. Důkaz tak zvané základní věty algebry bude obsahovat § 38. Potom se obrátíme k vyšetřování existence kořenů algebraické rovnice s koeficienty v libovolném tělese T. Tato vyšetřování obsahuje

[1]) Pro účely této třetí části knihy je výhodnější opatřit koeficienty polynomu a rovnice indexy v opačném pořadí než je ten, v němž postupují exponenty neurčité neb neznámé. To je rozdíl proti značení zavedenému v kapitole III. Budu nadále užívat důsledně značení zavedeného v (1).

§ 39. Na ně navazuje druhý důkaz tak zvané základní věty algebry, který je vyložen v § 53 v dodatku. Čtenář, který se zajímá jen o rovnice s číselnými koeficienty, může tato vyšetřování rovnic s koeficienty v libovolném tělese T vynechat.

§ 37. Některé vlastnosti polynomů s komplexními a s reálnými koeficienty.

V tomto paragrafu si odvodíme některé vlastnosti polynomů s komplexními neb reálnými koeficienty. Přitom je výhodné považovat polynomy za komplexní funkce komplexní proměnné x. Půjde totiž v první řadě o to udělat si zhruba přehled, jaké funkční hodnoty, co do absolutní velikosti, daný polynom $f(x)$ nad tělesem komplexních čísel K nabývá v různých částech Gaussovy roviny neb daný polynom $f(x)$ nad tělesem reálných čísel P na různých částech osy reálné.[1]) Dále si dokážeme některé věci o limitách posloupností komplexních čísel. Věty 37,1, 37,2 a 37,5 mají důležitost i při numerickém výpočtu kořenů algebraické rovnice, kdežto ostatní věty a definice budou sloužit toliko jako prostředky pro důkaz tak zvané základní věty algebry v § 38.

37,1. Věta. *Budiž $f(x)$ daný polynom nejméně prvního stupně nad tělesem komplexních čísel* K *a M libovolné reálné nezáporné číslo. Pak existuje vždy kladné číslo R takové, že*

$$|f(x)| > M \quad \text{pro všechna } x, \text{ pro něž platí } \quad |x| > R \ .$$

Poznámka 1. Názorně lze vyslovit obsah této věty takto: Zvolíme-li si libovolně nezáporné číslo M, pak existuje v Gaussově rovině jistá kružnice o středu v počátku a poloměru R taková, že pro všechny body vně této kružnice daný polynom $f(x)$ nabývá funkčních hodnot co do absolutní hodnoty větších než M. R ovšem závisí na volbě M.

Důkaz. Pišme polynom $f(x)$ stupně $n \geqq 1$ ve tvaru

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \ . \tag{1}$$

Budiž

$$A = \max\{|a_1|, |a_2|, \ldots, |a_n|\} \ . \tag{2}$$

Pak máme pro $|x| > 1$

$$|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n| \leqq |a_1| \cdot |x|^{n-1} + |a_2| \cdot |x|^{n-2} + \ldots + |a_n| \leqq$$
$$\leqq A\{|x|^{n-1} + |x|^{n-2} + \ldots + |x| + 1\} \leqq nA|x|^{n-1} \ .$$

Je tedy pro $|x| > 1$

$$|f(x)| = |a_0x^n + a_1x^{n-1} + \ldots + a_n| \geqq$$
$$\geqq |a_0| \cdot |x|^n - |a_1x^{n-1} + \ldots + a_n| \geqq |a_0| \cdot |x|^n - nA|x|^{n-1} =$$
$$= |x|^{n-1}\{|a_0| \cdot |x| - nA\} \ .$$

[1]) Pro jednoduchost bude nám značit $f(x)$ v § 37 a v § 38 nejen polynom $f(x)$, nýbrž i funkční hodnoty tohoto polynomu, které polynom $f(x)$ nabývá pro libovolná čísla x z nějaké množiny čísel, která ovšem musí být vždy určena. Půjde-li jen o konečnou množinu argumentů, nahradíme x nějakým písmenem ze začátku abecedy.

Zvolme si nyní

$$R = \max\left\{1, \frac{nA + M}{|a_0|}\right\} . \tag{3}$$

Je pak pro $|x| > R$

$$|a_0| \cdot |x| - nA > |a_0| \frac{nA + M}{|a_0|} - nA = M \geqq 0$$

a tedy $|f(x)| \geqq |x|^{n-1}\{|a_0|x - nA\} > |x|^{n-1}M > M$, čímž je důkaz proveden. Přesvědčte se, že pro důkaz je podstatné, že stupeň $n \geqq 1$.

Poznámka 2. Zvolme si v 37,1 $M = 0$. Pak je $|f(x)| > 0$ pro všechna $|x| > R$, kdež podle (3)

$$R = \max\left\{1, \frac{nA}{|a_0|}\right\} . \tag{4}$$

Tudíž má-li rovnice

$$f(\xi) = 0 \tag{5}$$

nějaký kořen α v tělese K, pak nutně $|\alpha| \leqq R$. R je horní odhad pro absolutní hodnoty kořenů rovnice (5). Lze však snadno odvodit odhad jiný, který je ve většině případů lepší (viz cv. 37,2). Platí totiž věta:

37,2. Věta. *Pro každý kořen α algebraické rovnice n-tého stupně o komplexních koeficientech*

$$f(\xi) = a_0\xi^n + a_1\xi^{n-1} + \ldots + a_{n-1}\xi + a_n = 0 \tag{6}$$

platí

$$|\alpha| < 1 + \frac{A}{|a_0|} , \tag{7}$$

kdež A je dáno vzorcem (2).

Důkaz. Nejdříve si ukážeme, že platí, je-li $f(x)$ polynom (1),

$$|a_0x^n| > |a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n| \tag{8}$$

pro všechna x, pro něž

$$|x| \geqq 1 + \frac{A}{|a_0|} . \tag{9}$$

Pro $|x| > 1$ je nejprve[2])

$$|a_1x^{n-1} + \ldots + a_{n-1}x + a_n| \leqq |a_1| \cdot |x|^{n-1} + \ldots + |a_{n-1}| \cdot |x| + |a_n| \leqq$$
$$\leqq A\{|x|^{n-1} + \ldots + |x| + 1\} = A\frac{|x|^n - 1}{|x| - 1} < A\frac{|x|^n}{|x| - 1}$$

a tudíž

$$|a_0x^n| - |a_1x^{n-1} + \ldots + a_n| > |a_0| \cdot |x|^n - A\frac{|x|^n}{|x| - 1} =$$
$$= |a_0| \cdot |x|^n \left\{1 - \frac{A}{|a_0|}\frac{1}{|x| - 1}\right\} . \tag{10}$$

[2]) Dávejte pozor, kde v nerovnostech stojí vztah $\geqq$ a kde vztah $>$!

Platí-li (9), pak platí zároveň i $|x| > 1$, neboť pro $A = 0$ je tvrzení (8) samozřejmé, takže možno předpokládat $A > 0$. Jest pak pro (9)

$$1 - \frac{A}{|a_0|}\frac{1}{|x| - 1} \geqq 1 - \frac{A}{|a_0|}\cdot\frac{|a_0|}{A} = 0 \,. \tag{11}$$

Z (10) a (11) plyne ihned (8). Dále máme podle (1) a (8)

$$|f(x)| \geqq |a_0x^n| - |a_1x^{n-1} + \ldots + a_{n-1}x + a_n| > 0$$

pro všechna x, která splňují (9). Je-li tedy α kořenem rovnice (6), musí splňovat nerovnost (7).

Dále platí pro polynomy s komplexními koeficienty tato věta

37,3. Věta. *Budiž $g(x)$ polynom nad tělesem komplexních čísel* K *stupně nejméně prvního tvaru*

$$g(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x \,,$$

t. j. bez absolutního členu, a budiž ε libovolné kladné číslo, pak existuje kladné číslo r takové, že

$$|g(x)| < \varepsilon \quad \textit{pro všechna } x, \textit{ pro něž } |x| < r \,. \tag{12}$$

Poznámka. Ve větě se jedná o polynomy, které mají v počátku nulový bod. Názorně lze vyslovit obsah věty takto: Zvolíme-li si libovolně kladné číslo ε, pak existuje v Gaussově rovině kružnice o středu v počátku a o poloměru r taková, že pro všechny body uvnitř této kružnice nabývá $g(x)$ hodnoty, jichž absolutní hodnota je menší než ε, ať je ε kladné číslo jakkoliv malé. r ovšem závisí na volbě ε.

Důkaz. Položme $A = \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}$. Pak platí pro všechna $|x| \leqq 1$

$$|g(x)| = |a_{n-1}x + a_{n-2}x^2 + \ldots + a_0x^n| \leqq$$
$$\leqq A\{|x| + |x|^2 + \ldots + |x|^n\} = A|x|\frac{1 - |x|^n}{1 - |x|} \leqq A\frac{|x|}{1 - |x|} \,,$$

neboť podle volby x je $0 \leqq 1 - |x|^n \leqq 1$. Nyní jest

$$A\frac{|x|}{1 - |x|} < \varepsilon \;\Leftrightarrow\; A|x| < \varepsilon - \varepsilon|x| \;\Leftrightarrow\; |x| < \frac{\varepsilon}{A + \varepsilon} \,.$$

Avšak pro $|x| < \varepsilon/(A + \varepsilon)$ je vždy $|x| \leqq 1$. Položíme-li tedy $r = \varepsilon/(A + \varepsilon)$, platí (12).

Přímým důsledkem této věty je věta

37,4. Věta. *Budiž $f(x)$ polynom nad tělesem komplexních čísel* K *a budiž ε libovolné kladné číslo. Pak existuje pro každý bod a z* K *kladné číslo r takové, že platí*

$$|f(x) - f(a)| < \varepsilon$$

pro všechna x, pro něž $|x - a| < r$.

Poznámka. Názorně lze opět vyslovit obsah této věty takto: Zvolíme-li si libovolně kladné číslo ε, pak lze najíti pro daný polynom $f(x)$ a daný bod a z K v Gaussově rovině kružnici o středu v a a o poloměru r takovou, že pro všechny body uvnitř této kružnice je rozdíl funkčních hodnot $f(x) - f(a)$ co do absolutní hodnoty menší než ε, ať je ε kladné číslo jakkoli malé, r ovšem závisí na bodu a a na ε.

Všimněte si, že vlastnost polynomů $f(x)$ jakožto komplexních funkcí komplexní proměnné, vyjádřená větou 37,4 je formálně úplně stejná s vlastností že reálná funkce reálné proměnné je spojitá.[3]) Nerovnost $|x - a| < r$ ovšem zde neznamená jistý interval na ose reálné kolem bodu a, nýbrž celý vnitřek kružnice v Gaussově rovině. Věta 37,4 říká, že polynom je *spojitá funkce komplexní proměnné* v celé Gaussově rovině.

Důkaz. Je-li $f(x)$ polynom nulový neb polynom stupně nultého, pak $f(x) - f(a) = 0$ pro každé a a věta je splněna pro jakákoliv kladná r. Je-li $f(x)$ polynom stupně aspoň prvního, položme $y = x - a$, t. j. $x = a + y$ a použijme Taylorova vzorce (17) z 21,7 pro bod a místo b. Dostaneme

$$f(a + y) - f(a) = \frac{f'(a)}{1!} y + \frac{f''(a)}{2!} y^2 + \ldots + \frac{f^{(n)}(a)}{n!} y^n .$$

Na pravé straně této rovnosti je polynom, který má všechny vlastnosti polynomu $g(x)$ z 37,3. Existuje tedy k libovolně zvolenému kladnému ε kladné číslo r takové, že

$$|f(a + y) - f(a)| < \varepsilon \quad \text{pro všechna } y, \text{ pro něž } \quad |y| < r.$$

Dosadíme-li sem místo y zpět $x = a + y$, dostaneme ihned tvrzení věty.

Vyšetřujeme-li rovnice s reálnými koeficienty, pak i pro absolutní hodnoty reálných kořenů těchto rovnic platí samozřejmě odhad (7) z 37,2. Lze však lehko najít pro tento případ odhady, které jsou ve většině případů lepší. Dokážeme si větu:

37,5. Věta. *Budiž* (6) *rovnice s reálnými koeficienty n-tého stupně* ($n \geqq 1$). *Budiž pro jednoduchost* $a_0 > 0$. *Budiž* a_r *první koeficient v posloupnosti* $a_0, a_1, a_2, \ldots, a_n$, *který je záporný. Dále buďtež* $a_{k_1}, a_{k_2}, \ldots, a_{k_s}$, ($k_1 = r$) *právě ty koeficienty z této posloupnosti, které jsou záporné. Položme*

$$B = \max\{|a_{k_1}|, |a_{k_2}|, \ldots, |a_{k_s}|\} .$$

Pak platí pro každý kladný kořen α *rovnice* (6)

$$\alpha < 1 + \frac{B}{a_0} , \tag{13}$$

$$\alpha < 1 + \sqrt[r]{\frac{B}{a_0}} . \tag{14}$$

[3]) Přesvědčte se o tom srovnáním 37,4 s definicí spojitosti pro reálnou funkci reálné proměnné v knize V. Jarník: Úvod do diferenciálního počtu, 1946, kap. V, § 4, str. 172 a § 8, str. 204.

Poznámka. Věta dává nejen horní odhad pro kladné kořeny rovnice (6), nýbrž i dolní odhad pro záporné kořeny této rovnice. Stačí totiž vyšetřovat místo rovnice (6) rovnici $f(-\xi) = 0$. Má-li tato rovnice kladný kořen β, má rovnice (6) záporný kořen $-\beta$ a naopak. Horní odhad pro kladné kořeny právě uvedené rovnice dává tedy, opatříme-li jej znaménkem minus, dolní odhad pro záporné kořeny rovnice (6).

Důkaz. Má-li rovnice (6) kladné kořeny, pak musí být mezi jejími koeficienty koeficienty záporné, neboť by jinak platilo $f(x) > 0$ pro každé $x > 0$.

1. Pro polynom $f(x)$ z (1) platí, je-li $x > 1$

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \geqq a_0x^n - B(x^{n-1} + x^{n-2} + \ldots + 1) =$$
$$= a_0x^n - B\frac{x^n - 1}{x - 1} > a_0x^n - B\frac{x^n}{x - 1} = x^n\left(a_0 - \frac{B}{x - 1}\right).$$

Je-li nyní $x \geqq 1 + B/a_0$, je i $x > 1$ i $x - 1 \geqq B/a_0$. Máme tedy $a_0 - B/(x - 1) \geqq a_0 - B \cdot a_0/B = 0$. To značí, že máme stále $f(x) > 0$. Je-li tedy α kladný kořen rovnice (6), musí pro něj platit (13).

2. Pro polynom $f(x)$ z (1) platí, je-li $x > 1$, vynecháme-li v $f(x)$ nezáporné členy $a_1x^{n-1}, a_2x^{n-2}, \ldots, a_{r-1}x^{n-r+1}$ a nahradíme-li koeficienty v ostatních členech jejich dolním odhadem $-B$,

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{r-1}x^{n-r+1} + a_rx^{n-r} + \ldots + a_n \geqq$$
$$\geqq a_0x^n - B\frac{x^{n-r+1} - 1}{x - 1} > a_0x^n - B\frac{x^{n-r+1}}{x - 1} =$$
$$= x^{n-r+1}\left(a_0x^{r-1} - \frac{B}{x - 1}\right) > x^{n-r+1}\left[a_0(x - 1)^{r-1} - \frac{B}{x - 1}\right] =$$
$$= x^{n-r+1}\left[a_0\frac{(x - 1)^r}{x - 1} - \frac{B}{x - 1}\right].$$

Platí-li nyní

$$x \geqq 1 + \sqrt[r]{\frac{B}{a_0}}, \quad \text{t. j.} \quad x - 1 \geqq \sqrt[r]{\frac{B}{a_0}},$$

platí i $x > 1$. Máme pak

$$a_0\frac{(x - 1)^r}{x - 1} \geqq \frac{B}{x - 1}$$

a tedy $f(x) > 0$. Je-li proto α kladný kořen rovnice (6), musí pro něj platit (14).

Příklady.

1. Pro rovnici

$$4\xi^6 - 3\xi^4 - 7\xi^3 + 9\xi^2 - 1 = 0$$

jest $A = 9$, $B = 7$, $r = 2$. Vzorec (7) dává horní odhad absolutní hodnoty kořenů

$$1 + \tfrac{9}{4} = 3{,}25 .$$

Vzorce (13) a (14) dávají tyto horní odhady pro kladné kořeny

$$1 + \tfrac{7}{4} = 2{,}75, \quad \text{resp.} \quad 1 + \sqrt[2]{\tfrac{7}{4}} < 2{,}33 .$$

Dolní odhad pro záporné kořeny dostaneme z horních odhadů pro kladné kořeny rovnice

$$4\xi^6 - 3\xi^4 + 7\xi^3 + 9\xi^2 - 1 = 0 ,$$

pro niž je $B = 3$, $r = 2$. Ze vzorců (13) a (14) dostaneme tyto dolní odhady pro záporné kořeny původní rovnice

$$-(1 + \tfrac{3}{4}) = -1{,}75 \quad \text{resp.} \quad -1{,}87 < -(1 + \sqrt[2]{\tfrac{3}{4}}) .$$

2. Pro rovnici

$$10\xi^7 - 3\xi^6 + 7\xi^5 - 9\xi^4 + 2\xi^3 + 4\xi^2 + 8\xi - 5 = 0$$

je $A = 9$, $B = 9$, $r = 1$. Vzorec (7) dává jako horní odhad absolutní hodnoty kořenů

$$1 + \tfrac{9}{10} = 1{,}9 .$$

Vzorce (13) a (14) dávají zde stejný horní odhad pro kladné kořeny

$$1 + \tfrac{9}{10} = 1{,}9 .$$

Dolní odhady pro záporné kořeny dostaneme z horních odhadů pro kladné kořeny rovnice

$$10\xi^7 + 3\xi^6 + 7\xi^5 + 9\xi^4 + 2\xi^3 - 4\xi^2 + 8\xi + 5 = 0 ,$$

kdež je $B = 4$, $r = 5$. Ze vzorců (13) a (14) dostaneme tyto dolní odhady pro záporné kořeny původní rovnice

$$-(1 + \tfrac{4}{10}) = -1{,}4 \quad \text{resp.} \quad -1{,}84 < -(1 + \sqrt[5]{\tfrac{4}{10}}) .$$

Pro důkaz tak zvané základní věty algebry budeme potřebovat některé věty o limitách posloupností komplexních čísel,[4]) které si na konci tohoto paragrafu odvodíme. Vyjdeme od této definice:

37,6. Definice. Říkáme, že *posloupnost komplexních čísel*

$$\alpha_1, \alpha_2, \alpha_3 , \ldots \tag{15}$$

má za limitu komplexní číslo α

$$\lim_{n\to\infty} \alpha_n = \alpha , \tag{16}$$

[4]) Pojem limity je pojem matematické analysy. Z důvodů, o nichž později bude řeč, se nemůžeme při důkazu tak zvané základní věty algebry vyhnout prostředkům analytickým. Jednotlivé důkazy této věty se liší právě tím, kterých analytických vět používají. V dalších výkladech tohoto paragrafu budu předpokládat, že čtenář je obeznámen s pojmem limity posloupnosti reálných čísel. Viz V. Jarník: Úvod do počtu diferenciálního, 1946, kap. II.

když k libovolně zvolenému kladnému číslu ε lze najíti kladné číslo N takové, že platí

(17) $$|\alpha_k - \alpha| < \varepsilon \quad \text{pro všechny indexy} \quad k > N.$$

Názorně lze říci: Že posloupnost (15) má limitu (16), znamená, že ať si předepíšeme kladné číslo ε jakkoliv malé, vždy lze v posloupnosti (15) najít takový index N, že všechny členy posloupnosti o indexu větším leží uvnitř kružnice o středu v α a poloměru ε. N ovšem závisí obecně na volbě ε.

Všimněte si, že tato definice je po formální stránce úplně stejná jako definice limity posloupnosti čísel reálných. Jen místo absolutní hodnoty čísel reálných vyskytuje se v ní absolutní hodnota čísel komplexních. Protože obě absolutní hodnoty mají stejné základní vlastnosti (viz 13,10), platí celá řada vět o limitách posloupností i pro posloupnosti čísel komplexních (viz cv. 37,10).

PŘÍKLAD. Posloupnost

$$\alpha_1 = 1, \ \alpha_2 = \tfrac{1}{2} + \tfrac{1}{2}i, \ \alpha_3 = \tfrac{1}{3} + \tfrac{2}{3}i, \ \ldots$$

má za limitu číslo i:

$$\lim_{k\to\infty}\left(\frac{1}{k} + \frac{k-1}{k}i\right) = i \ .$$

Jest totiž

$$|\alpha_k - \alpha|^2 = \frac{1}{k^2} + \left(\frac{k-1}{k} - 1\right)^2 = \frac{2}{k^2} \ .$$

Zvolíme-li si k danému ε $N = \sqrt{2}/\varepsilon$, máme skutečně $|\alpha_k - \alpha|^2 = 2/k^2 < \varepsilon^2$ pro $k > N$, t. j. podle 5,12 a) $|\alpha_k - \alpha| < \varepsilon$.

Pojem limity posloupnosti čísel komplexních dá se převésti na limity čísel reálných a to na limity posloupností reálných a imaginárních částí dané komplexní posloupnosti. Platí totiž věta:

37,7. Věta. *Položme v* (15) $\alpha_k = a_k + ib_k$, $k = 1, 2, \ldots$ *a v* (16) $\alpha = a + ib$. *Posloupnost* (15) *má za limitu číslo* α *tehdy a jen tehdy, má-li posloupnost reálných částí této posloupnosti* $a_1, a_2, \ldots$ *za limitu reálnou část a čísla* α *a posloupnost imaginárních částí* $b_1, b_2, \ldots$ *za limitu imaginární část b čísla* α

(18) $$\lim_{n\to\infty} a_n = a \ , \qquad \lim_{n\to\infty} b_n = b \ .$$

DŮKAZ. Nechť platí (18). K libovolně zvolenému ε lze pak najíti kladná čísla N_1 a N_2 tak, že platí

$$|a_k - a| < \frac{\varepsilon}{2} \quad \text{pro} \quad k > N_1 \ ,$$

$$|b_k - b| < \frac{\varepsilon}{2} \quad \text{pro} \quad k > N_2 \ .$$

Položme $N = \max(N_1, N_2)$. Pak pro všechna $k > N$ platí podle H_4 a H_3 z 6,8 a podle 13,10

$$|\alpha_k - \alpha| = |(a_k - a) + i(b_k - b)| \leqq |a_k - a| + |i(b_k - b)| =$$
$$= |a_k - a| + |b_k - b| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \ .$$

Obráceně nechť platí (16). K danému ε zvolme si N tak, aby platilo (17). Pak máme pro všechna $k > N$

$$|\alpha_k - \alpha|^2 = (a_k - a)^2 + (b_k - b)^2 < \varepsilon^2 \ .$$

Musí tedy být $(a_k - a)^2 < \varepsilon^2$, $(b_k - b)^2 < \varepsilon^2$, t. j. podle 5,12 a) $|a_k - a| < \varepsilon$, $|b_k - b| < \varepsilon$, což však značí, že platí (18).

Důsledkem věty o spojitosti polynomu 37,4 je pak věta:

37,8. Věta. *Mějme posloupnost komplexních čísel* (15), *která má limitu* (16). *Budiž* $f(x)$ *libovolně daný polynom o komplexních koeficientech. Pak platí*

a) $$\lim_{n\to\infty} f(\alpha_n) = f(\alpha) \ ,$$

b) $$\lim_{n\to\infty} |f(\alpha_n)| = |f(\alpha)| \ .$$

Důkaz. Zvolme si libovolně ε. Podle 37,4 určíme k němu r tak, že platí $|f(x) - f(\alpha)| < \varepsilon$ pro všechna x, pro něž $|x - \alpha| < r$. K tomuto r určeme N tak, aby platilo $|\alpha_k - \alpha| < r$ pro všechna $k > N$, což v důsledku existence limity (16) lze udělat. Pak ale $|f(\alpha_k) - f(\alpha)| < \varepsilon$ pro $k > N$. Tím je dokázáno a). Podle poznámky k 13,10 platí pro totéž N a pro všechna $k > N$

$$||f(\alpha_k)| - |f(\alpha)|| \leqq |f(\alpha_k) - f(\alpha)| < \varepsilon.$$

Tím je dokázáno b).

Cvičení k § 37.

Cv. 37,1. Najděte, jak musí znít věta 37,5, neučiníme-li předpoklad $a_0 > 0$, t. j. připustíme-li i $a_0 < 0$.

Cv. 37,2. Ř. Označme si h_1 horní odhad z (4) pro absolutní hodnoty kořenů rovnice o komplexních koeficientech (6) a h_2 horní odhad z (7). Vyšetřete, kdy $h_1 \leqq h_2$.

Cv. 37,3. Označme si pro rovnici o reálných koeficientech (6) h_3 horní odhad pro kladné kořeny z (13) a h_4 horní odhad z (14). Budiž h_2 odhad z cv. 37,2. a) Dokažte: Vždy platí $h_2 \geqq h_3$. b) Vyšetřete, kdy platí $h_2 = h_3$.

Cv. 37,4. Ř. Při značení z cv. 37,2 a cv. 37,3 vyšetřete, kdy $h_2 \geqq h_4$.

Cv. 37,5. Ř. Při značení a předpokladech z cv. 37,3 vyšetřete, kdy platí a) $h_3 \geqq h_4$, b) $h_3 = h_4$.

Cv. 37,6. Budiž (1) polynom n-tého stupně s reálnými koeficienty. Dokažte: Pro všechna reálná x splňující nerovnost (9) platí $\operatorname{sign} f(x) = \operatorname{sign} a_0 x^n$.

Cv. 37,7. Nechť polynom $g(x)$ z 37,3 má reálné koeficienty a nechť $a_{n-1} \neq 0$. Dokažte: Existuje kladné číslo r takové, že platí $\operatorname{sign} g(x) = \operatorname{sign} a_{n-1} x$ pro všechna reálná x, pro něž $0 < |x| < r$.

Cv. 37,8. Budiž $g(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-k} x^k$ polynom s reálnými koeficienty, $k \geqq 1$, $a_{n-k} \neq 0$. Dokažte: Existuje kladné číslo r takové, že platí $\operatorname{sign} g(x) = \operatorname{sign} a_{n-k} x^k$ pro všechna reálná x taková, že $0 < |x| < r$.

Cv. 37,9. Zakreslete v Gaussově rovině několik prvních bodů posloupnosti z příkladu v 37,6 a jejich limitu.

Cv. 37,10. Mějme dvě posloupnosti čísel komplexních, které mají limitu

$$\lim_{n\to\infty}\alpha_n = \alpha\ , \qquad \lim_{n\to\infty}\beta_n = \beta\ .$$

Dokažte: a) Posloupnost o obecném členu $\alpha_n + \beta_n$ má limitu $\lim_{n\to\infty}(\alpha_n + \beta_n) = \alpha + \beta$. b) Posloupnost o obecném členu $\alpha_n\beta_n$ má limitu $\lim_{n\to\infty}\alpha_n\beta_n = \alpha\beta$. c) Posloupnost o obecném členu $|\alpha_n|$ má limitu $\lim_{n\to\infty}|\alpha_n| = |\alpha|$. (Návod: Postupujte stejně jako při důkazech obdobných vět pro posloupnosti reálné. Viz V. Jarník: Úvod do počtu diferenciálního, 1946, kap. II, § 2, str. 83 a str. 86.)

Cv. 37,11. Pomocí cv. 37,10 bez použití 37,4 dokažte větu 37,8.

§ 38. Existence kořenů rovnice s komplexními koeficienty.

Otázku o existenci kořenů dané algebraické rovnice rozřešíme si nejdříve pro rovnici s komplexními koeficienty. Řešení dává tak zvaná základní věta algebry. K jejímu důkazu nutno použít speciálních vlastností komplexních čísel. Půjde hlavně o věty z § 37 a bude proto výhodné považovat polynomy za komplexní funkce komplexní proměnné a vyšetřovat nulové body těchto funkcí.

38,1. Tak zvaná základní věta algebry. *Každý polynom aspoň prvního stupně s komplexními koeficienty*[1])

$$f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_{n-1}x + \alpha_n \tag{1}$$

má v tělese komplexních čísel K *aspoň jeden nulový bod, t. j. rovnice*

$$f(\xi) = 0$$

má v tělese K *aspoň jeden kořen.*

Poznámka. Věta nemusí platit ve vlastním podtělese tělesa komplexních čísel. Rovnice $\xi^2 + 1 = 0$ nemá žádný kořen v tělese reálných čísel P, rovnice $\xi^2 - 2 = 0$ v tělese racionálních čísel R.

Postup důkazu. Větu 38,1 dokážeme tím způsobem, že budeme vyšetřovat místo komplexní funkce komplexní proměnné $f(x)$ reálnou funkci komplexní proměnné $|f(x)|$. Důkaz se rozpadá na dvě části. Nejprve dokážeme, že existuje v Gaussově rovině bod ϱ, pro nějž má funkce $|f(x)|$ absolutní minimum, t. j. že platí $|f(x)| \geqq |f(\varrho)|$ pro každé komplexní x.[2]) Za druhé si ukážeme, je-li γ libovolný bod Gaussovy roviny takový, že $|f(\gamma)| > 0$, že pak existuje v okolí

[1]) V 38,1 budeme důsledně značit komplexní čísla malými řeckými písmeny. Budeme-li chtít vyjádřit, že komplexní číslo je reálné, označíme je malým latinským písmenem.

[2]) Protože vždy $|f(x)| \geqq 0$, je množina funkčních hodnot funkce $|f(x)|$ (jsou to čísla reálná) zdola omezená (viz 12,2). Existuje tedy pro tuto množinu infimum m (viz 12,5c). Pak platí $|f(x)| \geqq m$ pro každé x. Funkce ovšem nemusí svého infima v žádném bodě nabývat. První část důkazu spočívá v tom, že ukážeme, že funkce $|f(x)|$ aspoň v jednom bodě svého infima nabývá. Pro tento bod má pak $|f(x)|$ absolutní minimum.

bodu γ bod δ takový, že $|f(\delta)| < |f(\gamma)|$. Odtud ihned plyne, že musí být $|f(\varrho)| = 0$, neboť jinak by $|f(\varrho)|$ nebylo minimem funkce $|f(x)|$.

Důkaz věty 38,1.

1. Podle 37,1 existuje kladné číslo R takové, že platí

$$|f(x)| > |f(0)| \tag{2}$$

pro všechna $|x| > R$. Vezměme si v Gaussově rovině čtverec K_0 o středu v počátku, který má strany rovnoběžné s reálnou a imaginární osou a stranu dlouhou $D = 2R$. Je to čtverec kružnici $|x| = R$ opsaný. Proto platí pro všechny body x vně tohoto čtverce nerovnost (2). Vrcholy čtverce K_0 jakož i ostatních čtverců, které si dále zavedu, budu udávat vždy jejich kartézskými souřadnicemi. X-ová souřadnice je reálná část, Y-ová souřadnice je imaginární část komplexního čísla, jež představuje příslušný vrchol v Gaussově rovině. Vrcholy čtverce K_0 mějtež proto souřadnice (a_0, c_0), (b_0, c_0), (a_0, d_0), (b_0, d_0), kdež

$$a_0 < b_0 , \qquad c_0 < d_0 ,$$
$$b_0 - a_0 = D , \qquad d_0 - c_0 = D .$$

Čtverec K_0 si rozdělíme symetrálami stran (v tomto případě osami souřadnými, viz obr. 6) na čtyři čtverce menší o délce stran $\frac{1}{2}D$. Aspoň jeden z těchto čtyř menších čtverců musí mít tuto vlastnost (M): Ke každému bodu τ z K_0[3]) existuje v tomto menším čtverci bod ϑ (ϑ závisí na τ) takový, že platí $|f(\tau)| \geqq |f(\vartheta)|$. Nahlédneme to takto: Vezměme si jeden z těchto čtyř čtverců, který si označíme jako první. Nemá-li tento čtverec vlastnost (M), pak existuje v K_0 mimo tento první čtverec bod σ_1 takový, že platí

$$|f(x)| > |f(\sigma_1)| \quad \text{pro všechna } x \text{ z tohoto 1. čtverce.} \tag{3}$$

Bod σ_1 leží tedy v některém ze tří ostatních menších čtverců (po případě ve dvou). Tento čtverec (po případě jeden z nich) si označíme jako druhý. Nemá-li druhý čtverec ještě vlastnost (M), pak existuje v K_0 mimo tento druhý čtverec bod σ_2 takový, že

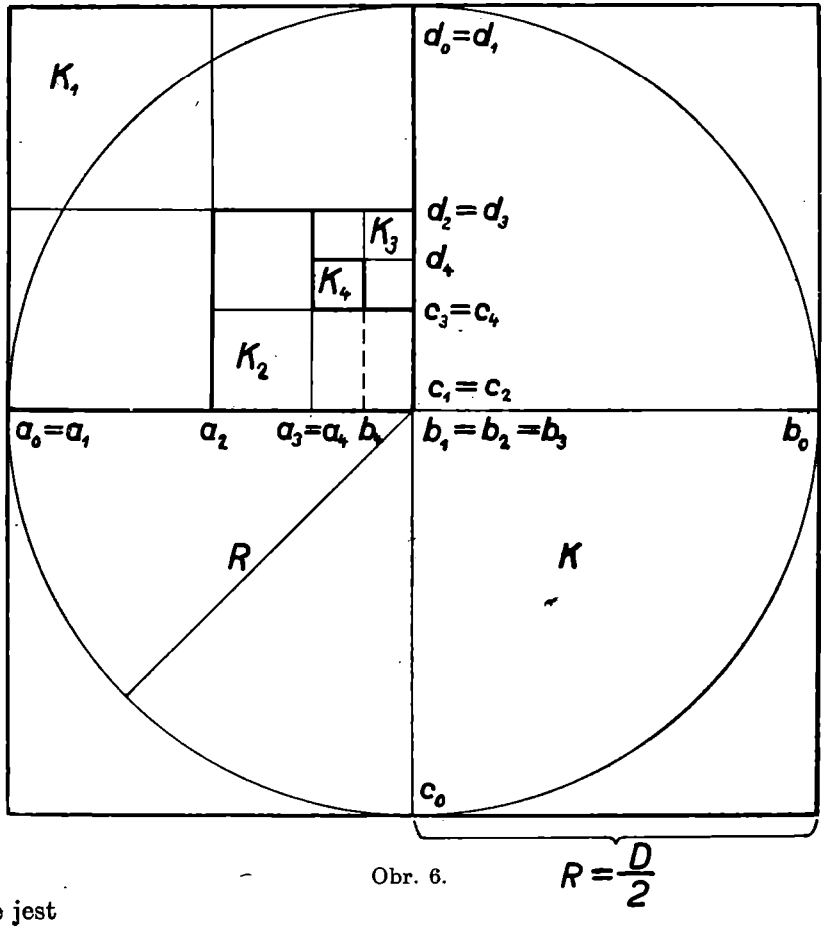
$$|f(x)| > |f(\sigma_2)| \quad \text{pro všechna } x \text{ z 2. čtverce.} \tag{4}$$

Bod σ_2 nemůže ležet v prvním čtverci, protože to odporuje vztahu (3), neboť σ_1 leží v druhém čtverci. Proto leží v jednom ze zbývajících dvou (nebo v obou). Tento čtverec (po případě jeden z nich) si označíme jako třetí. Nemá-li tento třetí čtverec vlastnost (M), existuje v K_0 mimo třetí čtverec bod σ_3 takový, že

$$|f(x)| > |f(\sigma_3)| \quad \text{pro všechna } x \text{ ze 3. čtverce.} \tag{5}$$

V důsledku (3) a (4) nemůže σ_3 ležet ani v prvním, ani v druhém čtverci. Musí tedy

[3]) Ke každému čtverci, o němž zde bude řeč, počítáme vždy i celý jeho obvod. Dva sousední čtverce mají proto body společné, které leží buď na společné části strany, která je odděluje, neb ve společném vrcholu.



Obr. 6.

Zde jest

$$a_0 = a_1 = -\frac{D}{2},\ a_2 = -\frac{D}{2^2},\ a_3 = a_4 = -\frac{D}{2^3},$$

$$b_0 = \frac{D}{2},\ b_1 = b_2 = b_3 = 0,\ b_4 = -\frac{D}{2^4},$$

$$c_0 = -\frac{D}{2},\ c_1 = c_2 = 0,\ c_3 = c_4 = \frac{D}{2^3},$$

$$d_0 = d_1 = \frac{D}{2},\ d_2 = d_3 = \frac{D}{2^2},\ d_4 = 3\frac{D}{2^4}.$$

ležet ve zbývajícím čtvrtém čtverci. Tento čtvrtý čtverec má však již vlastnost (M). Je-li totiž x nějaký bod z prvních tří čtverců, pak z (3), (4), (5) plyne ihned $|f(x)| > |f(\sigma_3)|$. Je-li x libovolný bod ze čtvrtého čtverce, pak platí $|f(x)| \geqq |f(x)|$.

Vybereme si nyní jeden z těchto menších čtverců o straně $\frac{1}{2}D$, který má vlastnost (M), a označíme si jej K_1. Souřadnice vrcholů čtverce K_1 budtež (a_1, c_1), (b_1, c_1), (a_1, d_1), (b_1, d_1) (viz obr. 6), kdež

$$a_0 \leqq a_1 < b_1 \leqq b_0 ,$$
$$c_0 \leqq c_1 < d_1 \leqq d_0 ,$$
$$b_1 - a_1 = \frac{D}{2} , \qquad d_1 - c_1 = \frac{D}{2} .$$

Se čtvercem K_1 opakujeme celý postup znova. Symetrálami stran rozdělíme jej na čtyři stejné čtverce menší o délce strany $D/2^2$. Aspoň jeden z těchto čtyř čtverců musí mít vůči čtverci K_1 vlastnost (M). Vybereme si jeden z těch, které mají vlastnost (M), a označíme si jej K_2.

Obecně máme-li již sestrojen čtverec K_n o souřadnicích vrcholů (a_n, c_n), (b_n, c_n), (a_n, d_n), (b_n, d_n) a délce strany $D/2^n$, rozdělíme symetrálami stran tento čtverec na čtyři stejné čtverce menší o délce strany $D/2^{n+1}$. Aspoň jeden z těchto čtyř menších čtverců musí mít vlastnost (M): Ke každému bodu τ v K_n existuje v tomto menším čtverci bod ϑ takový, že platí $|f(\tau)| \geqq |f(\vartheta)|$. Jeden z těchto čtverců, majících vlastnost (M), si označíme K_{n+1}. Souřadnice jeho vrcholů budtež (a_{n+1}, c_{n+1}), (b_{n+1}, c_{n+1}), (a_{n+1}, d_{n+1}), (b_{n+1}, d_{n+1}). Pak platí

$$\begin{aligned} &a_n \leqq a_{n+1} < b_{n+1} \leqq b_n , \\ &b_n - a_n = \frac{D}{2^n}, \; b_{n+1} - a_{n+1} = \frac{D}{2^{n+1}} , \end{aligned} \tag{6}$$

$$\begin{aligned} &c_n \leqq c_{n+1} < d_{n+1} \leqq d_n, \\ &d_n - c_n = \frac{D}{2^n}, \; d_{n+1} - c_{n+1} = \frac{D}{2^{n+1}} . \end{aligned} \tag{7}$$

Tím jsme sestrojili nekonečnou posloupnost čtverců

$$K_0, K_1, K_2, \ldots , \tag{8}$$

jichž strany konvergují k nule a z nichž každý leží v předcházejícím. Pro X-ové souřadnice vrcholů těchto čtverců platí vzhledem na (6)

$$a_0 \leqq a_1 \leqq a_2 \leqq \ldots \leqq b_2 \leqq b_1 \leqq b_0 .$$

Reálná čísla a_n tvoří posloupnost neklesající a shora omezenou, čísla b_n posloupnost nerostoucí a zdola omezenou. Obě posloupnosti mají limitu.[4]) Označme si r' limitu posloupnosti a_n a r'' limitu posloupnosti b_n. Platí

$$a_n \leqq r' \leqq r'' \leqq b_n \qquad \text{pro každé } n .$$

Z (6) plyne $0 \leqq r'' - r' \leqq b_n - a_n = D/2^n$ pro každé n: Tedy $r' = r''$. Společnou limitu obou posloupností si označme nyní

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = r . \tag{9}$$

[4]) Viz V. Jarník: Úvod do počtu diferenciálního, 1946, kap. II, § 4, str. 100.

Podobně z (7) dostaneme posloupnosti

$$c_0 \leqq c_1 \leqq c_2 \leqq \ldots \leqq d_2 \leqq d_1 \leqq d_0 \ .$$

Stejným způsobem ukážeme, že obě mají stejnou limitu, kterou si označíme s

$$\lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n = s \ . \tag{10}$$

Označme si[5])

$$\varrho = r + is \ .$$

Zvolme si v každém ze čtverců (8) úplně libovolně jeden bod. Bod zvolený v K_n si označme $\varrho_n = r_n + is_n$. Platí nyní

$$a_n \leqq r_n \leqq b_n \ , \qquad c_n \leqq s_n \leqq d_n \ .$$

Odtud ihned dostáváme vzhledem na (9) a (10)

$$\lim_{n\to\infty} r_n = r \ , \qquad \lim_{n\to\infty} s_n = s \ .$$

Podle 37,7 to však značí

$$\lim_{n\to\infty} \varrho_n = \varrho, \tag{11}$$

při čemž ϱ_n byl úplně libovolný bod z K_n.

Nyní již lehko ukážeme, že funkce $|f(x)|$ nabývá v bodě ϱ absolutního minima. Budiž nejprve x libovolný bod v K_0. V důsledku vlastnosti (M) existuje v K_1 bod ϱ_1 takový, že $|f(x)| \geqq |f(\varrho_1)|$. Máme-li již určen bod ϱ_n v K_n, určíme vzhledem na vlastnost (M) v K_{n+1} bod ϱ_{n+1} tak, aby $|f(\varrho_n)| \geqq |f(\varrho_{n+1})|$. Tím dostaneme posloupnost bodů $\varrho_1, \varrho_2, \ldots$, pro něž platí, jak jsme ukázali, (11). Dále platí podle volby bodů ϱ_n v K_n:

$$|f(x)| \geqq |f(\varrho_1)| \geqq f(\varrho_2)| \geqq \ldots \tag{12}$$

Z (11) plyne podle 37,8 b)

$$\lim_{n\to\infty} |f(\varrho_n)| = |f(\varrho)|$$

a z (12) pak plyne ihned $|f(x)| \geqq |f(\varrho)|$. Je-li nyní x bod, který leží vně čtverce K_0, platí pro něj podle (2) $|f(x)| > |f(0)| \geqq |f(\varrho)|$. $|f(\varrho)|$ je skutečné absolutní minimum funkce $|f(x)|$.

2. Budiž za druhé γ komplexní číslo takové, že $|f(\gamma)| > 0$, t. j.

$$f(\gamma) \neq 0 \ .$$

---

[5]) Protože délky stran čtverců (8) konvergují k nule a každý z nich leží v předcházejícím, mají všechny jen jeden bod společný: ϱ. K tomu ukazuje bezprostřední geometrický názor a lehko se to dokáže z (9) a (10). Dále se lehko z názoru nahlédne, že máme-li libovolnou posloupnost komplexních čísel $\varrho_n \in K_n$, $n = 1, 2, \ldots$, platí (11). Lze to lehko dokázat z definice limity komplexních čísel 37,6. Viz cv. 38,2.

Ukážeme, že v Gaussově rovině lze najít v okolí bodu γ bod δ tak, že $|f(\gamma)| > |f(\delta)|$. Píšme pro $f(x)$ Taylorův vzorec pro bod γ (viz 21,7 (16)):

$$f(x) = f(\gamma) + \frac{f'(\gamma)}{1!}(x-\gamma) + \frac{f''(\gamma)}{2!}(x-\gamma)^2 + \ldots + \frac{f^{(n)}(\gamma)}{n!}(x-\gamma)^n \ .$$

V tomto vzorci může být $f'(\gamma) = 0$. Předpokládejme proto obecně, že k je přirozené číslo $1 \leqq k \leqq n$ takové, že platí

$$f'(\gamma) = 0, \ f''(\gamma) = 0, \ \ldots, \ f^{(k-1)}(\gamma) = 0, \ f^{(k)}(\gamma) \neq 0 \ .$$

Takové přirozené číslo vždy existuje. Stupeň polynomu $f(x)$ je totiž podle předpokladu $n \geqq 1$ a proto je jistě $f^{(n)}(\gamma) \neq 0$, neboť by jinak $f(x)$ nebyl polynom n-tého stupně. Je tedy nejvýše $k = n$. Polynom $f(x)$ lze potom psát ve tvaru

(13) $$f(x) = f(\gamma)\{1 + \beta_k(x-\gamma)^k + \beta_k(x-\gamma)^k g(x-\gamma)\} \ ,$$

kdež

$$\beta_k = \frac{1}{k!}\frac{f^{(k)}(\gamma)}{f(\gamma)} \neq 0$$

a $g(x-\gamma)$ je pro $k = n$ polynom nulový, pro $k < n$ polynom stupně $(n-k)$-ho

$$g(x-\gamma) = \frac{k!}{(k+1)!}\frac{f^{(k+1)}(\gamma)}{f^{(k)}(\gamma)}(x-\gamma) + \frac{k!}{(k+2)!}\frac{f^{(k+2)}(\gamma)}{f^{(k)}(\gamma)}(x-\gamma)^2 + \\ + \ldots + \frac{k!}{n!}\frac{f^{(n)}(\gamma)}{f^{(k)}(\gamma)}(x-\gamma)^{n-k} \ ,$$

který je pro $x = \gamma$ roven nule: $g(0) = 0$. Je-li $k < n$, lze podle 37,3 určit k číslu $\frac{1}{2}$ kladné číslo d tak, že

(14) $$|g(x-\gamma)| < \tfrac{1}{2} \quad \text{pro všechna } x, \text{ pro něž } \quad |x-\gamma| < d \ .$$

Je-li $g(x-\gamma)$ polynom nulový, je podmínka (14) splněna pro každé kladné d.

Je nyní zřejmo, že cíle dosáhneme, určíme-li v Gaussově rovině číslo δ tak, že když toto číslo dosadíme za x do (13), bude absolutní hodnota velké závorky menší než 1. Místo δ si však stanovíme rozdíl $\gamma - \delta$, z něhož lze ihned jednoznačně určit δ. K tomu cíli si vyjádříme $\delta - \gamma$ pomocí goniometrických funkcí podle 14,7:

(15) $$\delta - \gamma = s(\cos u + i \sin u) \ .$$

$\delta - \gamma$ a tudíž i δ bude stanoveno, určíme-li si absolutní hodnotu s a amplitudu u. Abychom je určili, pišme koeficient β_k z (13) ve tvaru

(16) $$\beta_k = r(\cos t + i \sin t) \ ,$$

kdež $r > 0$, neboť $\beta_k \neq 0$. s si nyní zvolíme tak, aby platilo

(17) $$0 < s < \min\left(d, \sqrt[k]{\frac{1}{r}}\right) \ ,$$

při čemž připomínám, že podle 12,6 je k-tá kladná odmocnina z čísla $1/r > 0$ jednoznačně určena. Z (17) plyne ihned

$$0 < rs^k < 1 \ . \tag{18}$$

Amplitudu si stanovím takto

$$u = \frac{\pi - t}{k} \ ,$$

t. j.

$$t + ku = \pi \ . \tag{19}$$

Tím dostáváme podle 14,8 z (15), (16) a (19) výraz

$$\begin{aligned} \beta_k(\delta - \gamma)^k &= r(\cos t + i \sin t) \cdot s^k(\cos ku + i \sin ku) = \\ &= rs^k[\cos(t + ku) + i \sin(t + ku)] = rs^k(\cos\pi + i \sin\pi) = -rs^k \ . \end{aligned} \tag{20}$$

Dosadíme-li nyní do (13) δ za x, dostáváme pro absolutní hodnotu závorky na pravé straně podle (20) výraz

$$\begin{aligned} &|1 + \beta_k(\delta - \gamma)^k + \beta_k(\delta - \gamma)^k g(\delta - \gamma)| \leqq \\ &\leqq |1 + \beta_k(\delta - \gamma)^k| + |\beta_k(\delta - \gamma)^k| \cdot |g(\delta - \gamma)| = \\ &= |1 - rs^k| + rs^k |g(\delta - \gamma)| \ . \end{aligned}$$

Z (17) plyne, že $s = |\delta - \gamma| < d$ a tedy podle (14) $|g(\delta - \gamma)| < \frac{1}{2}$. Podle (18) je $1 - rs^k > 0$. Lze tedy psát

$$|1 + \beta_k(\delta - \gamma)^k + \beta_k(\delta - \gamma)^k g(\delta - \gamma)| \leqq 1 - rs^k + \tfrac{1}{2}rs^k = 1 - \tfrac{1}{2}rs^k < 1 \ .$$

Odtud konečně plyne z (13)

$$|f(\delta)| = |f(\gamma)| \cdot |1 + \beta_k(\delta - \gamma)^k + \beta_k(\delta - \gamma)^k g(\delta - \gamma)| < |f(\gamma)| \ .$$

Tím jsme dokázali, že ke každému komplexnímu číslu γ, pro něž $f(\gamma) \neq 0$, existuje číslo δ takové, že $|f(\delta)| < |f(\gamma)|$. V takovém bodě nenabývá proto funkce $|f(x)|$ svého minima. Tím je důkaz tak zvané základní věty algebry proveden.

Důsledek věty 38,1 je podle 18,4 ten, že každý polynom $f(x)$ jedné neurčité nad tělesem komplexních čísel K stupně aspoň druhého je reducibilní a má za dělitele aspoň jeden lineární faktor $x - \alpha$, kdež α je kořenem rovnice $f(\xi) = 0$. O rozkladu polynomu $f(x)$ v ireducibilní faktory platí však v tělese K dokonce tato věta:

38,2. Věta.[6]) *Každý polynom tvaru*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \tag{21}$$

stupně $n \geqq 1$ *s komplexními koeficienty dá se nad tělesem komplexních čísel psát jako součin* n *lineárních faktorů*

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) \ , \tag{22}$$

[6]) Dále v tomto paragrafu budu koeficienty polynomu značit malými latinskými písmeny, i když jsou to čísla komplexní.

při čemž komplexní čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ *jsou všechny kořeny rovnice* $f(\xi) = 0$.

Jediné ireducibilní polynomy jedné neurčité nad tělesem komplexních čísel jsou polynomy prvního stupně.

Důkaz. Rozklad (22) lze psát zřejmě pro každý polynom prvního stupně $ax + b = a(x - (-b)/a)$. Předpokládejme, že máme dokázáno, že každý polynom $(n - 1)$-ho stupně dá se rozložit v lineární faktory. Budiž $f(x)$ polynom n-tého stupně. Podle 38,1 existuje komplexní číslo α_1 takové, že $f(\alpha_1) = 0$. Podle 18,4 máme

$$f(x) = (x - \alpha_1)\, g(x) \ , \tag{23}$$

kdež $g(x)$ je jistý polynom stupně $(n - 1)$-ho. Koeficient u x^{n-1} v $g(x)$ je a_0, jak se lehko zjistí srovnáním koeficientů u x^n nalevo a napravo v rovnosti (23). Podle indukčního předpokladu lze tedy psát pro jistá komplexní čísla $\alpha_2, \alpha_3, \ldots, \alpha_n$: $g(x) = a_0(x - \alpha_2)(x - \alpha_3) \ldots (x - \alpha_n)$. Dosadíme-li tento výraz za $g(x)$ do (23) dostaneme (22).

Z (22) ihned plyne, že komplexní čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ jsou kořeny rovnice $f(\xi) = 0$. Budiž obráceně β libovolné číslo komplexní takové, že $f(\beta) = 0$.[7]) Dosadíme-li β za x do (22), dostaneme

$$a_0(\beta - \alpha_1)(\beta - \alpha_2) \ldots (\beta - \alpha_n) = 0 \ .$$

Musí tedy $\beta = \alpha_i$ aspoň pro jeden index i, $i = 1, 2, \ldots, n$. Tím je věta 38,2 dokázána.

38,3. Význam tak zvané základní věty algebry. Větu 38,1 dokázal po celé řadě ne plně úspěšných pokusů jiných matematiků německý matematik Fr. K. Gauss roku 1797. Dokud se algebra zabývala pouze rovnicemi s číselnými koeficienty, měla tato věta pro algebru základní význam. Zaručovala existenci kořenů jakékoliv algebraické rovnice tehdy vyšetřované, a dávala tak teprve všem ostatním vyšetřováním kořenů těchto rovnic řádný podklad. Proto byla nazvána základní větou algebry. Když však byla algebraická vyšetřování rozšířena i na tělesa, která nejsou číselnými tělesy, pak rázem ztratila tato věta své ústřední postavení v algebře. Věta totiž neříká nic na příklad o rovnicích, jejichž koeficienty jsou racionální funkce z daného tělesa racionálních funkcí. A přece takové rovnice se vyskytují na příklad v teorii algebraických funkcí. Rovněž nelze jí použíti na rovnice, jejichž koeficienty leží v daném tělese charakteristiky p. A přece mezi takové rovnice patří kongruence mod p, které byly sice již dávno vyšetřovány v teorii čísel, nebyly však zahrnovány do algebry. Moderní algebra je považuje dnes za speciální případ rovnic.

Díváme-li se na celý problém existence kořenů z tohoto širšího hlediska moderní algebry, vidíme, že věta 38,1 je větou speciální, která se týká jen tělesa

[7]) O β můžeme dokonce předpokládat, že je to prvek z libovolného nadtělesa nad tělesem komplexních čísel. Rovnice $f(\xi) = 0$ nemá tedy jiné kořeny než $\alpha_1, \alpha_2, \ldots, \alpha_n$ i v libovolném nadtělese nad K.

komplexních čísel K. Všimněme si, že se v důkaze, který jsme zde vyložili, používá zvláštních vlastností tohoto tělesa a zvláštních vlastností polynomů s komplexními koeficienty. Je to především ta vlastnost Gaussovy roviny, že pro každou posloupnost čtverců (8), z nichž každý obsahuje následující a jichž délky stran konvergují k nule, existují body Gaussovy roviny, které leží ve všech čtvercích této posloupnosti (že průnik všech čtverců posloupnosti není prázdný).[8]) Tato vlastnost zaručuje existenci bodu ϱ v první části důkazu. Z vlastností polynomů komplexní proměnné je to hlavně vlastnost vyjádřená větami 37,3 a 37,4, že polynom je funkce spojitá, a dále vlastnost vyjádřená větou 37,1, že absolutní hodnota polynomu dosti daleko od počátku je veliká.

Všechny tyto věty nemáme k disposici pro polynomy s koeficienty z libovolného tělesa. V takových tělesech nemůže však věta ani obecně platit, neboť v poznámce k 38,1 jsme viděli, že neplatí ani pro vlastní podtělesa tělesa komplexních čísel. Nutno v tomto případě postupovat jinak. To bude předmětem příštího paragrafu. V dodatku podávám jiný důkaz věty 38,1, který postupuje co nejvíce algebraicky a využívá zvláštních analytických vlastností tělesa K co nejméně.

Cvičení k § 38.

Cv. 38,1. Ř. Předpokládejte, že existují body komplexní roviny, které leží ve všech čtvercích posloupnosti (8) (že průnik čtverců z posloupnosti (8) není prázdný). Dokažte: Takový bod je jen jeden.

Cv. 38,2. Používajíce výsledku cv. 38,1 dokažte přímo z def. 37,6 bez použití věty 37,7: Zvolíme-li si libovolně bod $\varrho_n \in K_n$, kdež K_n je čtverec z posloupnosti (8), pak posloupnost $\varrho_1, \varrho_2, \ldots$ má za limitu onen jediný bod ϱ ze cv. 38,1.

§ 39. Existence kořenů rovnice s koeficienty z libovolného tělesa.

39,1. Vymezení úlohy.[1]) Mějme dáno nějaké těleso T, jehož prvky budeme značit malými latinskými písmeny. Mějme dále dánu nějakou rovnici $F(\xi) = 0$ s koeficienty v T. Tato rovnice nemusí mít v tělese T vůbec žádný kořen. (Viz poznámku v 38,1.) Proto nutno otázku po existenci kořenů této rovnice formulovat takto: Existuje nadtěleso T′ nad T takové, že obsahuje kořeny rovnice $F(\xi) = 0$? Ukážeme si, že odpověď na tuto otázku je kladná. Protože T je úplně libovolné těleso, nemůžeme existenci tělesa T′ zajistit jinak než tím, že si toto těleso sestrojíme vycházejíce od tělesa T a od oné rovnice. To bude předmětem výkladů v tomto paragrafu.

Dříve si však tuto úlohu poněkud zjednodušíme. Protože $F(x)$ je libovolně

[8]) Že v tom průniku leží jen jeden bod, je již snadným důsledkem toho, že délka stran čtverců konverguje k nule. Viz cv. 38,1.

[1]) Čtenář, který se chce omezit jen na studium rovnic s číselnými koeficienty, může celý tento paragraf vynechat.

daný polynom z $\mathsf{T}[x]$, bude tento polynom obecně reducibilní nad T a dá se proto rozložit podle 19,5 v součin ireducibilních faktorů

$$F(x) = f_1(x)\, f_2(x) \ldots f_r(x) \ . \tag{1}$$

Jest ihned vidět, že daná úloha bude řešena, podaří-li se nám sestrojit nadtěleso T', které obsahuje kořen rovnice $f_1(\xi) = 0$, kdež $f_1(x)$ je nyní ireducibilní polynom. Stačí proto úplně řešit tuto úlohu: Budiž dán libovolný ireducibilní polynom $f(x)$ nad T. Jest sestrojit nadtěleso T' nad T tak, aby obsahovalo kořen rovnice $f(\xi) = 0$. Jak máme provádět tuto konstrukci, to naznačuje věta:

39,2. Věta. *Budiž $f(x)$ ireducibilní polynom z $\mathsf{T}[x]$. Předpokládejme, že existuje nadtěleso T' nad T takové, že obsahuje prvek α, který je nulovým bodem polynomu $f(x)$: $f(\alpha) = 0$. Pak je α nulovým bodem právě těch polynomů z $\mathsf{T}[x]$, které jsou dělitelny polynomem $f(x)$.*

Důkaz. Je-li pro nějaký polynom $F(x)$: $f(x) \mid F(x)$, pak $F(x) = f(x)\, g(x)$ a podle pravidla dosazovacího máme $F(\alpha) = f(\alpha)\, g(\alpha) = 0$. Budiž naopak pro nějaký polynom $F(x)$ z $\mathsf{T}[x]$ $F(\alpha) = 0$. Mezi všemi polynomy z $\mathsf{T}[x]$, které mají α za nulový bod, existují polynomy nejnižšího stupně (viz 5,20). Zvolme si jeden z nich $g(x)$. Podle 18,3 lze psát $F(x) = g(x)\, Q(x) + R(x)$, kdež $R(x)$ je buď polynom nulový neb polynom nižšího stupně než $g(x)$. Dosadíme-li α za x, dostaneme $0 = R(\alpha)$. Vzhledem na volbu polynomu $g(x)$, musí být $R(x)$ polynom nulový. To však znamená $g(x) \mid F(x)$. Máme proto tento výsledek: $g(x)$ dělí každý polynom $F(x)$ takový, že $F(\alpha) = 0$, neboť $F(x)$ si můžeme jinak úplně libovolně zvolit. Proto také $g(x) \mid f(x)$. Protože $f(x)$ je ireducibilní, musí podle 19,1 $f(x) = a \,.\, g(x)$ pro jisté $a \in \mathsf{T}$. Platí tudíž podle 7,9 i $f(x) \mid F(x)$ pro původně daný polynom $F(x)$. Tím je věta dokázána.

Věta 39,2 nás vede k tomu, abychom se pokusili definovat v oboru integrity $\mathsf{T}[x]$ novou rovnost tím, že položíme rovny nule všechny polynomy, které jsou dělitelny polynomem $f(x)$. Ukážeme si, že to skutečně lze provést a že tím dostaneme z $\mathsf{T}[x]$ těleso. Nejdříve se definujeme:

39,3. Definice. Budiž $f(x)$ daný polynom stupně aspoň prvního z $\mathsf{T}[x]$. Když pro dva polynomy $g(x)$ a $h(x)$ platí $f(x) \mid [g(x) - h(x)]$, budeme říkat, že *$g(x)$ je kongruentní s $h(x)$ podle modulu $f(x)$ neb modulo $f(x)$* a budeme psát

$$g(x) \equiv h(x) \mod f(x) \ . \tag{2}$$

Vztah (2) mezi dvěma polynomy se nazývá *kongruence*. $g(x) \equiv 0 \mod f(x)$ značí podle této definice totéž, co vztah $f(x) \mid g(x)$.

Vztah (2) je úplně analogický ke kongruenci mezi dvěma čísly z 9,1. Platí proto i pro kongruenci mezi polynomy věta analogická k 9,2, t. j. vztah (2) splňuje axiomy rovnosti R_0 až R_3, je to vztah reflexivní, symetrický a transitivní. Lze proto podle 1,2 $\mathsf{T}[x]$ rozdělit v disjunktní části, *zbytkové třídy podle modulu $f(x)$ neb modulo $f(x)$*, z nichž každá obsahuje právě všechny polynomy, které jsou spolu kongruentní mod $f(x)$.

Zaveďme si do $\mathsf{T}[x]$ novou rovnost vztahem (2) a vyšetřujme, jaké vlastnosti má sčítání a násobení polynomů z $\mathsf{T}[x]$ při této nové rovnosti. Dostaneme výsledek úplně analogický k výsledku z 9,7, kdy jsme zavedli do oboru integrity celých čísel C novou rovnost jakožto kongruenci podle prvočíselného modulu p. To je způsobeno tím, že ireducibilní polynom $f(x)$ je ireducibilním prvkem v $\mathsf{T}[x]$, jako bylo prvočíslo p ireducibilním prvkem v C. Platí totiž věta analogická k 9,7:

39,4. Věta. *V oboru integrity* $\mathsf{T}[x]$ *budiž dán ireducibilní polynom* $f(x)$. *Definujeme-li v* $\mathsf{T}[x]$ *rovnost vztahem* (2) *jakožto kongruenci* $\bmod f(x)$ *a součet a součin obyčejným způsobem, pak tvoří tento obor integrity těleso* T'.

Důkaz. Protože jsme si mezi polynomy z $\mathsf{T}[x]$ definovali jiným způsobem toliko rovnost a nikoliv součet a součin, platí samozřejmě v T' axiomy A_0, M_0. O A_1 a M_1 musíme však dokázat, že platí, neboť v obou axiomech podstatným způsobem vystupuje rovnost. Za tím účelem mějme tři polynomy $g(x)$, $h_1(x)$, $h_2(x)$ a nechť platí $h_1(x) \equiv h_2(x) \bmod f(x)$, t. j. $f(x) \mid [h_1(x) - h_2(x)]$. Pak platí též $h_1(x) - h_2(x) = [g(x) + h_1(x)] - [g(x) + h_2(x)] \Rightarrow f(x) \mid \{[g(x) + h_1(x)] - [g(x) + h_2(x)]\} \Rightarrow g(x) + h_1(x) \equiv g(x) + h_2(x) \bmod f(x)$. To však značí, že platí A_1. Podobně máme $f(x) \mid [h_1(x) - h_2(x)] \Rightarrow f(x) \mid g(x)[h_1(x) - h_2(x)] \Rightarrow f(x) \mid [g(x)\, h_1(x) - g(x)\, h_2(x)] \Rightarrow g(x)\, h_1(x) \equiv g(x)\, h_2(x) \bmod f(x)$. To je axiom M_1. Platnost axiomů A_1 a M_1 zaručuje, že nahradíme-li v kongruencích $\bmod f(x)$ libovolný polynom polynomem s ním kongruentním $\bmod f(x)$, kongruence zůstane správnou. Nyní je bezprostředně patrno, že platí v T' axiomy A_2 až A_5, M_2 až M_4 a D.

Zbývá nám dokázat platnost M_5. Je-li $g(x)$ libovolný polynom z $\mathsf{T}[x]$ takový, že $g(x) \not\equiv 0 \bmod f(x)$, pak to podle definice 39,3 značí, že $g(x)$ není dělitelný ireducibilním polynomem $f(x)$. To však podle 19,2 znamená, že $f(x)$ a $g(x)$ jsou polynomy nesoudělné. Existují tedy podle 18,7 polynomy $h(x)$, $h_1(x)$ takové, že platí

$$g(x)\, h(x) + f(x)\, h_1(x) = 1 \ .$$

Vezmeme-li tuto rovnost jakožto kongruenci $\bmod f(x)$, dostaneme

$$g(x)\, h(x) \equiv 1 \qquad \bmod f(x) \ , \tag{3}$$

neboť $f(x)\, h_1(x) \equiv 0 \bmod f(x)$. To značí: Ke každému $g(x) \not\equiv 0 \bmod f(x)$ existuje v $\mathsf{T}[x]$ polynom $h(x)$ inversní k $g(x) \bmod f(x)$, t. j. polynom takový, že platí (3). Tím je platnost M_5 dokázána a T' tvoří skutečně těleso.

Poznámka. Zavedeme-li si v oboru integrity $\mathsf{T}[x]$ novou rovnost vztahem (2), říkáme, že v $\mathsf{T}[x]$ *počítáme* $\bmod f(x)$. Platnost axiomu A_1 pro kongruence $\bmod f(x)$ značí toto: Máme-li dány dvě třídy $\bmod f(x)$ a sečteme-li libovolný polynom $g(x)$ z jedné třídy s libovolným polynomem $h(x)$ z druhé třídy, dostaneme tak polynomy, které všechny leží v jedné a téže třídě $\bmod f(x)$. Sčítání polynomů $\bmod f(x)$ můžeme tedy považovat za sčítání zbytkových tříd $\bmod f(x)$,

neboť třídu, v níž leží polynom $g(x) + h(x)$, možno považovat za součet tříd obsahujících polynomy $g(x)$ a $h(x)$. Totéž platí i o součinu dvou polynomů podle M_1. Těleso T′ můžeme považovat tedy za těleso tříd polynomů z $T[x]$ mod $f(x)$. Nazýváme je pak *těleso zbytkových tříd* mod $f(x)$.

Ukážeme si dále, že těleso T′ při vhodném ztotožnění jistých tříd z T′ a prvků z T můžeme považovat za nadtěleso nad T, které obsahuje nulový bod polynomu $f(x)$. Platí totiž věta:

39,5. Věta. *Obsahuje-li nějaká zbytková třída* mod $f(x)$ *z tělesa* T′ *z* 39,4 *prvky z tělesa* T, *pak obsahuje takový prvek jen jeden. Všechny třídy z* T′ *obsahující prvky z* T *tvoří v* T′ *podtěleso isomorfní s tělesem* T. *Ztotožníme-li tedy každou takovou třídu s prvkem z* T, *který ta třída obsahuje, stane se* T′ *nadtělesem nad* T. *Třída, která obsahuje polynom x, je nulovým bodem polynomu* $f(x)$.

Důkaz. Budiž $a \in T$, $b \in T$ a nechť platí $a \equiv b \bmod f(x)$, t. j. $f(x) \mid (a - b)$. Protože a i b jsou buď polynomy nulové neb polynomy nultého stupně a $f(x)$ je podle předpokladu polynom aspoň prvního stupně, musí být $a = b$. Každá třída z T′ obsahuje nejvýše jeden prvek z T. Dále zřejmě zbytková třída, která je součtem (součinem) zbytkových tříd obsahujících a, b, obsahuje prvek $a + b$ (prvek ab). Nyní plyne ze cv. 4,12, že množina všech tříd z $T[x]$ mod $f(x)$ obsahujících prvky z T je těleso isomorfní s T. Označíme-li si konečně α třídu, která obsahuje polynom x, obsahuje třída $f(\alpha)$ polynom $f(x)$, je to tedy třída nulová. Platí proto $f(\alpha) = 0$. Tím je věta dokázána.

Definujeme proto:

39,6. Definice. Budiž $f(x)$ ireducibilní polynom nad tělesem T. Těleso T′ zbytkových tříd mod $f(x)$ z 39,5 se nazývá *kořenové těleso polynomu* $f(x)$ *neb rovnice* $f(\xi) = 0$. Obecněji nazveme kořenovým tělesem polynomu $f(x)$ každé těleso, které obsahuje T a je isomorfní s T′.

Ukážeme si nyní, že každé nadtěleso nad T, které obsahuje aspoň jeden kořen rovnice $f(\xi) = 0$, obsahuje podtěleso isomorfní s T′, kořenové těleso polynomu $f(x)$. Platí totiž věta:

39,7. Věta. *Budiž* $f(x)$ *ireducibilní polynom z* $T[x]$. *Budiž* U *libovolné nadtěleso nad* T, *které obsahuje prvek* α *takový, že* $f(\alpha) = 0$. *Pak* U *obsahuje podtěleso* T″, *které je isomorfní s tělesem* T′ *zbytkových tříd* mod $f(x)$. U *obsahuje tedy aspoň jedno kořenové těleso polynomu* $f(x)$.

Důkaz. Protože těleso U obsahuje prvek α a těleso T, obsahuje i všechny výrazy tvaru $F(\alpha)$, kdež $F(x)$ je libovolný polynom z $T[x]$. Množinu všech těchto výrazů si označme T″. Podle 39,2 platí $F(\alpha) = 0$ právě tehdy, když $f(x) \mid F(x)$ v $T[x]$. Vyšetřujme, kdy platí pro dva polynomy $F(x)$, $G(x)$ z $T[x]$ v tělese U $F(\alpha) = G(\alpha)$. Platí implikace $F(\alpha) = G(\alpha) \Leftrightarrow F(\alpha) - G(\alpha) = 0 \Leftrightarrow f(x) \mid [F(x) - G(x)]$ v $T[x] \Leftrightarrow F(x) \equiv G(x) \bmod f(x)$. Platí tedy v U

$F(\alpha) = G(\alpha)$ právě tehdy, když platí pro příslušné polynomy $F(x) \equiv G(x) \bmod f(x)$ v $\mathsf{T}[x]$. Je-li dále pro výrazy $F(\alpha)$, $G(\alpha)$, $H_1(\alpha)$, $H_2(\alpha)$ z T'' $F(\alpha) + G(\alpha) = H_1(\alpha)$, $F(\alpha)\,G(\alpha) = H_2(\alpha)$, pak je též v $\mathsf{T}[x]$ $F(x) + G(x) \equiv H_1(x) \bmod f(x)$ a $F(x)\,G(x) \equiv H_2(x) \bmod f(x)$ a obráceně. Podle cv. 4,12 je tedy T'' těleso a je isomorfní s tělesem T', přiřadíme-li třídu obsahující prvek $F(\alpha)$ zbytkové třídě $\bmod f(x)$ obsahující polynom $F(x)$.

Poznámka. Bezprostředním důsledkem věty 39,7 je tato věc: *Kořenové těleso T'' polynomu $f(x)$, které obsahuje kořen α rovnice $f(\xi) = 0$, vznikne adjunkcí kořene α k tělesu T.*

Budiž U nějaké nadtěleso nad T obsahující kořen α. Všechna podtělesa v U, která obsahují kořen α a těleso T, obsahují i kořenové těleso T'' z 39,7. Protože T'' samo má také tyto dvě vlastnosti, je T'' průnikem všech těchto podtěles. Přidáme-li tedy k T kořen α a takto vzniklou množinu doplníme dalšími prvky tak, aby tvořila těleso, dostaneme kořenové těleso T''. *Toto těleso budeme značit tedy ve shodě s* 13,11 $\mathsf{T}(\alpha)$.

Zároveň je vidět, že dané nadtěleso U nad T může obsahovat různá kořenová tělesa polynomu $f(x)$. Obsahuje jich právě tolik, kolik obsahuje různých kořenů rovnice $f(\xi) = 0$.

V 38,2 jsme viděli, že každý polynom $F(x)$ stupně aspoň prvního s komplexními koeficienty se dá nad tělesem komplexních čísel rozložit v součin lineárních faktorů. Místo této věty dokážeme si pro polynom $F(x)$ nad libovolným tělesem T, že existuje vždy nadtěleso U nad T takové, že nad U se dá polynom $F(x)$ rozložit v součin lineárních faktorů. Přesněji si dokážeme tuto větu:

39,8. Věta. *Budiž $F(x)$ polynom stupně $n \geq 1$ z oboru integrity $\mathsf{T}[x]$, kdež T je dané těleso. Pak existuje nadtěleso U nad T, které má tyto dvě vlastnosti:*

a) *Nad U se dá polynom $F(x)$ rozložit v součin lineárních faktorů*

$$F(x) = a_0(x - \alpha_1)(x - \alpha_2) \ \ldots \ (x - \alpha_n) \ . \tag{4}$$

b) *Těleso U neobsahuje žádné vlastní podtěleso, které by mělo vlastnost* a).

Důkaz provedeme úplnou indukcí. Věta platí zřejmě pro všechny polynomy prvního stupně nad T. V tomto případě je totiž $\mathsf{U} = \mathsf{T}$. Předpokládejme, že pro každé dané těleso T máme větu již dokázanou pro všechny polynomy stupně nejvýše n-tého. Budiž $F(x)$ polynom stupně $(n + 1)$-ho. Protože na rozdíl od věty 39,7 nepředpokládáme, že $F(x)$ je ireducibilní nad T, budiž $f(x)$ jeden ireducibilní faktor z rozkladu polynomu $F(x)$ v ireducibilní faktory nad T.

K $f(x)$ si sestrojíme podle 39,5 kořenové těleso $\mathsf{T}(\alpha_{n+1})$ nad T, které obsahuje jeden kořen α_{n+1} rovnice $f(\xi) = 0$. Podle 18,4 platí $(x - \alpha_{n+1}) \mid f(x)$ nad $\mathsf{T}(\alpha_{n+1})$ a tedy také $(x - \alpha_{n+1}) \mid F(x)$. Proto lze psát rozklad

$$F(x) = F_1(x)\ (x - \alpha_{n+1}) \ , \tag{5}$$

kdež $F_1(x)$ je polynom n-tého stupně nad $\mathsf{T}(\alpha_{n+1})$. Podle indukčního předpokladu existuje tedy nadtěleso U nad $\mathsf{T}(\alpha_{n+1})$, které má pro polynom $F_1(x)$ vlastnosti a) a b) věty, t. j. nad U platí rozklad

$$F_1(x) = a_0(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) \ . \tag{6}$$

Platí tedy pro $F(x)$ nad U podle (5) rozklad

$$F(x) = a_0(x - \alpha_1)(x - \alpha_2) \ \dots \ (x - \alpha_n)(x - \alpha_{n+1}) \ . \tag{7}$$

Těleso U má proto pro polynom $F(x)$ vlastnost a) věty. Budiž U' podtěleso v U, nad nímž platí rozklad (7), které má tedy pro polynom $F(x)$ vlastnost a). Pak U' obsahuje kořen α_{n+1} rovnice $f(\xi) = 0$, obsahuje tudíž podle 31,7 i kořenové těleso $\mathsf{T}(\alpha_{n+1})$ ireducibilního polynomu $f(x)$. Z (5) a (7) plyne dále, polynom $F_1(x)$ má nad U' rozklad (6), t. j. rozpadá se v lineární faktory. Protože těleso U má pro polynom $F_1(x)$ nad $\mathsf{T}(\alpha_{n+1})$ podle indukčního předpokladu vlastnosti a) i b), nemůže být U' vlastní podtěleso v U. Je tedy $\mathsf{U}' = \mathsf{U}$. Proto má těleso U i pro polynom $F(x)$ vlastnost b). Věta platí i pro polynom $F(x)$ stupně $(n + 1)$-ho. Protože $F(x)$ byl libovolně daný polynom stupně $(n + 1)$-ho nad libovolně daným tělesem T, platí věta pro každý polynom stupně $(n + 1)$-ho nad libovolně daným tělesem T. Tím je věta úplnou indukcí dokázána.

39,9. Definice. Těleso U z 39,8 nazývá se *rozkladové těleso polynomu* $F(x)$ *nad* T.

39,10. Věta. *Budiž* $F(x)$ *polynom stupně* $n \geqq 1$ *nad tělesem* T. *Budiž* U *rozkladové těleso tohoto polynomu a nechť platí pro* $F(x)$ *nad* U *rozklad* (4). *Pak* $\alpha_1, \alpha_2, \dots, \alpha_n$ *jsou kořeny rovnice* $F(\xi) = 0$ *a v žádném nadtělese nad* U *nemá tato rovnice jiné kořeny.*

Těleso U *vznikne adjunkcí všech kořenů* $\alpha_1, \alpha_2, \dots, \alpha_n$ *k tělesu* T. *Proto je budeme značit také* $\mathsf{T}(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Důkaz. Z (4) plyne ihned podle pravidla dosazovacího, že $\alpha_1, \alpha_2, \dots, \alpha_n$ jsou kořeny rovnice $F(\xi) = 0$. Nechť prvek β z nadtělesa U_0 nad U je kořenem této rovnice, t. j. $F(\beta) = 0$. Z (4) dostáváme

$$a_0(\beta - \alpha_1)(\beta - \alpha_2) \ \dots \ (\beta - \alpha_n) = 0 \ .$$

Musí tedy aspoň pro jeden index i, $1 \leqq i \leqq n$ být $\beta = \alpha_i$. Je-li U_1 podtěleso v U, které obsahuje i T i všechny kořeny $\alpha_1, \alpha_2, \dots, \alpha_n$, pak platí již nad U_1 pro $F(x)$ rozklad (4). Musí tedy být podle 39,8 b) $\mathsf{U}_1 = \mathsf{U}$. U je skutečně těleso, které vznikne adjunkcí kořenů $\alpha_1, \alpha_2, \dots, \alpha_n$ k T.

Budiž dáno těleso T a polynom $F(x)$ nad T. Naskytá se nyní otázka, jak dalece je rozkladové těleso U polynomu $F(x)$ tímto polynomem a tělesem T určeno. Odpověď je tato: U je určeno jednoznačně, ovšem jen ve smyslu isomorfismu. To značí: Máme-li dvě rozkladová tělesa U' a U'' polynomu $F(x)$ nad T, pak

jsou si navzájem isomorfní a to tak, že isomorfismus přiřaďuje každý prvek společného podtělesa T sám sobě. Nejdříve si dokážeme jednu pomocnou větu.

39,11. Pomocná věta. *Buďtež* J' *a* J'' *dva isomorfní obory integrity. Budiž* x *neurčitá nad* J' *a* y *neurčitá nad* J''. *Přiřadíme-li každému polynomu z* $J'[x]$

$$a'_0x^n + a'_1x^{n-1} + \ldots + a'_n$$

polynom

$$a''_0y^n + a''_1y^{n-1} + \ldots + a''_n$$

z $J''[y]$, *při čemž* a''_i *je prvek z* J'', *který odpovídá prvku* a'_i *z* J' *v uvedeném isomorfismu, dostaneme isomorfismus oborů integrity* $J'[x]$ *a* $J''[y]$.

Důkaz. Bezprostředně ověříme, že zobrazení oboru integrity $J'[x]$ na $J''[y]$ ve větě uvedené vyhovuje definici isomorfismu z 4,22.

Poznámka 1. Ve větě 39,11 buďtež J' a J'' dvě isomorfní tělesa T' a T''. Protože isomorfismus zobrazuje součin dvou neb více polynomů z $T'[x]$ na součin těch polynomů z $T''[y]$, které jim v isomorfismu odpovídají, plyne z právě uvedené věty ihned toto: Je-li $F'(x)$ polynom z $T'[x]$ a

$$F'(x) = f'_1(x)\, f'_2(x) \ \ldots \ f'_r(x)$$

jeho rozklad v součin ireducibilních polynomů podle 19,5 a 19,6, pak polynom $F''(y)$ z $T''[y]$ jemu v isomorfismu odpovídající má rozklad

$$F''(y) = f''_1(y)\, f''_2(y) \ \ldots \ f''_r(y) \ ,$$

kdež $f''_i(y)$ je ireducibilní polynom z $T''[y]$, který v isomorfismu odpovídá polynomu $f'_i(x)$, $i = 1, 2, \ldots, r$. *Mají tedy sobě odpovídající polynomy z* $T'[x]$ *a* $T''[y]$ *stejné rozklady v součin ireducibilních polynomů.*

Poznámka 2. Buďtež $f'(x)$ ireducibilní polynom z $T'[x]$ z předešlé poznámky a $f''(y)$ polynom z $T''[y]$, který mu v isomorfismu odpovídá. Pak je i $f''(y)$ ireducibilní polynom. *Budiž* $T'(\alpha)$ *kořenové těleso polynomu* $f'(x)$ *nad* T' *a* T'' (β) *kořenové těleso polynomu* $f''(y)$ *nad* T''. *Pak tělesa* $T'(\alpha)$ *a* $T''(\beta)$ *jsou isomorfní. V tomto isomorfismu odpovídá prvku* a' *z* T' *prvek* a'' *z* T'', *který mu odpovídá v původně daném isomorfismu, a prvku* α *prvek* β. Důkaz se provede takto: Podle věty 39,11 jsou si obory $T'[x]$ a $T''[y]$ isomorfní. Podle poznámky 1 odpovídá v isomorfismu každému polynomu $F'(x)$ z $T'[x]$, který je dělitelný polynomem $f'(x)$, vzájemně jednoznačně právě jeden polynom $F''(y)$ z $T''[y]$, který je dělitelný $f''(y)$. To však značí, že isomorfismus z věty 39,11 mezi obory integrity $T'[x]$ a $T''[y]$ zobrazuje všechny polynomy z jedné třídy $T'[x]$ mod $f'(x)$ právě na všechny polynomy jedné třídy $T''[y]$ mod $f''(y)$. Je ihned vidět, že toto zobrazení oboru integrity zbytkových tříd $T'[x]$ mod $f'(x)$ na obor integrity zbytkových tříd $T''[y]$ mod $f''(y)$ je isomorfismus těchto oborů integrity. Protože isomorfismus mezi $T'[x]$ a $T''[y]$ z 39,11, z něhož jsme vyšli, zobrazuje x na y a prvek a' z T' na prvek a'' z T'', který je mu přiřaděn původním isomorfismem mezi T'

a T'', musí třída z $\mathsf{T}'[x] \bmod f'(x)$, která obsahuje x (t. j. prvek α) být zobrazena na třídu z $\mathsf{T}''[y] \bmod f''(y)$, která obsahuje y (t. j. na prvek β) a třída, která obsahuje a' z T' na třídu, která obsahuje a'' z T''. Tím je tvrzení dokázáno.

39,12. Věta. *Budiž $F(x)$ polynom aspoň prvního stupně nad tělesem T. Buďtež U' a U'' dvě rozkladová tělesa tohoto polynomu nad T. Pak tato dvě tělesa jsou isomorfní a isomorfismus lze volit tak, že každý prvek z T (společného podtělesa těles U' a U'') je jím zobrazen sám na sebe.*

Důkaz. Podle 39,10 můžeme vytvořit těleso U' tím, že adjungujeme k T všechny kořeny rovnice $F(\xi) = 0$, které leží v U': $\mathsf{U}' = \mathsf{T}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Podobně můžeme vytvořit U'' tím, že adjungujeme k T všechny kořeny této rovnice, které leží v U'': $\mathsf{U}'' = \mathsf{T}(\beta_1, \beta_2, \ldots, \beta_n)$. Budiž $f_1(x)$ ten ireducibilní faktor polynomu $F(x)$ nad T, který obsahuje kořenový činitel $x - \alpha_1$. $f_1(x)$ rozpadá se ovšem nad U'' též v lineární faktory. Budiž $(x - \beta_1)$ jeden z nich. Pak kořenová tělesa $\mathsf{T}(\alpha_1) = \mathsf{T}_1'$ a $\mathsf{T}(\beta_1) = \mathsf{T}_1''$ jsou navzájem isomorfní podle 39,7, při čemž každý prvek z T je přiřaděn sám sobě. Podle poznámky 1 v 39,11 rozpadá se polynom $F(x)$ stejným způsobem nad T_1' i nad T_1'' v součin ireducibilních polynomů. Budiž α_2 kořen jednoho ireducibilního faktoru stupně aspoň druhého polynomu $F(x)$ nad T_1' a β_2 kořen jemu odpovídajícího ireducibilního faktoru polynomu $F(x)$ nad T_1'' v isomorfismu z poznámky 1 v 39,11. Pak podle poznámky 2 v 39,11 jsou kořenová tělesa $\mathsf{T}_2' = \mathsf{T}_1'(\alpha_2)$, $\mathsf{T}_2'' = \mathsf{T}_1''(\beta_2)$ spolu isomorfní a isomorfismus přiřaďuje každému prvku z T_1' ten prvek z T_1'', který mu odpovídá v isomorfismu sestrojeném mezi T_1' a T_1''. Tedy každý prvek z T odpovídá sám sobě. Není-li ještě $\mathsf{T}_2' = \mathsf{U}'$ a $\mathsf{T}_2'' = \mathsf{U}''$, pokračujeme stejným způsobem dále. Nakonec dostaneme isomorfismus mezi U' a U'', ve kterém každý prvek z T odpovídá sám sobě.

Poznámka. Budiž V nadtěleso nad T a nechť polynom $F(x)$ s koeficienty v T se rozpadá nad V v součin lineárních faktorů. Pak V musí obsahovat aspoň jedno rozkladové těleso U polynomu $F(x)$. V obsahuje však takové těleso jen jedno. Dejme tomu že by V obsahovalo dvě taková tělesa: U a U'. Nechť platí pro $F(x)$ nad U rozklad

$$F(x) = a_0(x - \alpha_1)(x - \alpha_2) \ \ldots \ (x - \alpha_n)$$

a nad U' rozklad

$$F(x) = a_0(x - \beta_1)(x - \beta_2) \ \ldots \ (x - \beta_n) \ .$$

Oba dva rozklady jsou však rozklady polynomu $F(x)$ nad V v ireducibilní polynomy a musí být proto podle 19,6 totožné. To značí, že je při vhodném očíslování $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, $\ldots$, $\alpha_n = \beta_n$. Tedy též $\mathsf{U} = \mathsf{T}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathsf{T}(\beta_1, \beta_2, \ldots, \beta_n) = \mathsf{U}'$.

39,13. Srovnání s tak zvanou základní větou algebry. Pro libovolné těleso T jsme nahradili v tomto paragrafu tak zvanou základní větu algebry 38,1 větami 39,4 a 39,5 a větu 38,2 plynoucí z tak zv. základní věty algebry větami 39,8

a 39,10. Srovnáme-li uvedené věty tohoto paragrafu s větami 38,1 a 38,2, vidíme, že věty tohoto paragrafu dávají v jednom směru více, v druhém však méně než věty 38,1 a 38,2. Věty tohoto paragrafu platí pro polynomy nad libovolným tělesem, kdežto věty 38,1 a 38,2 platí jen pro polynomy nad tělesem komplexních čísel K (pro polynomy s číselnými koeficienty). Po této stránce jsou věty tohoto paragrafu obecnější. Na druhé straně říká na příklad věta 38,2, že každý polynom s komplexními koeficienty se nad tělesem komplexních čísel K rozpadá v lineární faktory, kdežto podle 39,8 se daný polynom $F(x)$ z $\mathsf{T}[x]$ rozpadá v lineární faktory nad svým rozkladovým tělesem U. Těleso U závisí podstatně na polynomu $F(x)$. Jiný polynom $G(x)$ z $\mathsf{T}[x]$ má obecně jiné rozkladové těleso. Obdobná věc platí i pro kořenová tělesa ireducibilních polynomů. V tomto směru říkají věty tohoto paragrafu podstatně méně než věty 38,1 a 38,2.

Cvičení k § 39.

Cv. 39,1. Proveďte podrobně konstrukci kořenového tělesa z 39,4 a 39,5 pro polynom $f(x) = ax + b$ z $\mathsf{T}[x]$.

Cv. 39,2. Proveďte podrobně konstrukci rozkladového tělesa z 39,8 pro polynom n-tého stupně $F(x)$ z $\mathsf{T}[x]$, který je v $\mathsf{T}[x]$ součinem n lineárních polynomů.

Cv. 39,3. Budiž $f(x)$ ireducibilní polynom n-tého stupně z $\mathsf{T}[x]$, $n \geqq 1$. Dokažte: V každé zbytkové třídě z tělesa zbytkových tříd mod $f(x)$ leží právě jeden polynom tvaru

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1},$$

kde a_i jsou libovolné prvky z T.

Cv. 39,4. Budiž T′ kořenové těleso polynomu $f(x)$ z cv. 39,3 a α kořen rovnice $f(\xi) = 0$ z T′. Dokažte: Všechny prvky tělesa T′ dostaneme, když ve výraze

$$a_0 + a_1 \alpha + a_2 \alpha^2 + \ldots + a_{n-1} \alpha^{n-1}$$

položíme za prvky $a_0, a_1, \ldots, a_{n-1}$ nezávisle všechny prvky tělesa T. Každý prvek z T′ dostaneme tímto způsobem jen jednou.

Cv. 39,5. Dokažte: Těleso T′ z cv. 39,4 je modul hodnosti n nad T.

Cv. 39,6. $x^2 + 1$ je ireducibilní polynom nad P. (Viz příklad 4 z 19,1.) Sestrojte podle cv. 39,4 kořenové těleso P′ pro polynom $x^2 + 1$ a srovnejte s tělesem K definovaným v 13,2 jako množina uspořádaných dvojic (a_1, a_2) čísel reálných.

Cv. 39,7. Budiž $d > 0$ racionální číslo, které není úplným čtvercem. Pak polynom $x^2 - d$ je ireducibilní nad R. (Viz příklad 3 z 19,1.) Sestrojte podle cv. 39,4 kořenové těleso R′ pro polynom $x^2 - d$ a srovnejte je s tělesem $\mathsf{R}(\sqrt{d})$ z cv. 12,9.

Cv. 39,8. Pro d z cv. 39,7 je polynom $x^2 + d$ ireducibilní nad R. Sestrojte podle cv. 39,4 kořenové těleso R′ pro polynom $x^2 + d$ a srovnejte je s tělesem $\mathsf{R}(i\sqrt{d})$ z cv. 13,18.

Cv. 39,9. a) Dokažte: $x^2 - 2$ je ireducibilní polynom nad tělesem zbytkových tříd mod3 C_3. [Návod: Použijte cv. 9,4.] b) Sestrojte podle cv. 39,4 kořenové těleso C_3' polynomu $x^2 - 2$ a srovnejte je s tělesem z cv. 9,8.

*

Ve cv. 39,10—39,13 budiž T dané těleso, $f(x)$ ireducibilní polynom stupně n-tého, $n \geqq 1$, z $\mathsf{T}[x]$, T′ jeho kořenové a U jeho rozkladové těleso, které obsahuje T′.

Cv. 39,10. Budiž $f(x)$ a) kvadratický polynom, b) polynom n-tého stupně, který je nad T′ součinem n lineárních faktorů. Dokažte: V obou případech je U = T′.

Cv. 39,11. Nad T′ nechť platí rozklad $f(x) = (x - \alpha)\, g(x)$ a $g(x)$ nechť není součinem samých lineárních polynomů nad T′. Dokažte: U obsahuje jako podtělesa aspoň dvě kořenová tělesa polynomu $f(x)$ od sebe různá.

Cv. 39,12. Budiž U_0 libovolné nadtěleso nad U a nechť T″ je nějaké kořenové těleso polynomu $f(x)$, které leží v U_0. Dokažte: T″ leží již v U.

Cv. 39,13. Dokažte: a) U obsahuje nejvýše tolik kořenových těles polynomu $f(x)$ od sebe různých, kolik má rovnice $f(\xi) = 0$ kořenů od sebe různých. b) Všechna tato kořenová tělesa jsou spolu isomorfní.

§ 40. Násobnost kořenů rovnice.

V tomto paragrafu si odvodíme některé důsledky, které plynou z rozkladu polynomu $f(x)$ v součin lineárních faktorů podle 38,2, jedná-li se o polynom $f(x)$ nad tělesem komplexních čísel K, neb podle 39,8, jedná-li se o polynom nad libovolně daným tělesem T. V tomto posledním případě jde ovšem o rozklad polynomu $f(x)$ nad jeho rozkladovým tělesem U. Proto v tomto paragrafu bude značit T libovolně dané těleso, $f(x)$ daný polynom nad K neb T, a U rozkladové těleso polynomu $f(x)$. Věty vyslovím obyčejně pro polynom $f(x)$ nad K a v závorkách uvedu znění pro polynom $f(x)$ nad T. Totéž platí i pro důkazy vět. Čtenář, který se zajímá jen o polynomy a rovnice s číselnými koeficienty, může všechny tyto poznámky, které se týkají polynomu $f(x)$ nad T, vynechat. V dalším bude tedy značit T libovolné těleso, avšak s tím omezením, že od 40,5 budeme předpokládat, že T má charakteristiku 0.

40,1. Definice. Budiž $f(x)$ daný polynom n-tého stupně nad K (nad T). Pro $f(x)$ platí nad K (nad U) podle 38,2 (39,8) rozklad

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \ \dots \ (x - \alpha_n) \ . \tag{1}$$

Jednotlivé lineární faktory $x - \alpha_i$ nazýváme *kořenovými činiteli polynomu* $f(x)$. Podobně lze psát pro rovnici $f(\xi) = 0$ rozklad

$$f(\xi) = a_0(\xi - \alpha_1)(\xi - \alpha_2) \ \dots \ (\xi - \alpha_n) = 0 \ . \tag{2}$$

Lineární faktory tohoto rozkladu nazývají se *kořenoví činitelé rovnice* $f(\xi) = 0$.

40,2. Násobnost kořenových činitelů. Mějme polynom $f(x)$ nad K (nad T), který má nad K (nad U) rozklad (1) v kořenové činitele. Podle 38,2 (39,10) jsou $\alpha_1, \alpha_2, \dots, \alpha_n$ právě všechny kořeny rovnice (2). Jsou-li to prvky od sebe různé, pak rovnice (2) má právě n kořenů. Vyskytují-li se mezi prvky α_i některé prvky sobě rovné, pak rovnice (2) má kořenů méně. Abychom shrnuli všechny případy, které zde mohou nastat, v případ jediný, pišme rozklad (1) podle 19,7 ve tvaru

$$f(x) = a_0(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \ \dots \ (x - \alpha_r)^{k_r} \ , \tag{3}$$

kdež $\alpha_1, \alpha_2, \dots, \alpha_r$ jsou komplexní čísla (prvky z U) od sebe různá a exponenty jsou přirozená čísla jednoznačně určená příslušnými kořenovými činiteli a taková, že

$$k_1 + k_2 + \dots + k_r = n \ . \tag{4}$$

Číslo k_i se nazývá *násobnost kořenového činitele* $(x - \alpha_i)$ *z* $f(x)$ a říkáme, že $(x - \alpha_i)$ je v $f(x)$ *kořenovým činitelem* k_i*-násobným.*[1]) Platí zřejmě nad K (nad U) $(x - \alpha_i)^{k_i} \mid f(x)$, ale $(x - \alpha_i)^{k_i+1} \nmid f(x)$. Pro kořeny samy zavedeme pak tuto definici:

40,3. Definice. Budiž $f(x)$ polynom stupně $n \geqq 1$ nad K (nad T) a nechť platí pro něj nad K (nad U) rozklad (3). Kořen α_i, $i = 1, 2, \ldots, r$ rovnice $f(\xi) = 0$ se nazývá *kořenem* k_i*-násobným*, je-li k_i exponent příslušný ke kořenovému činiteli $x - \alpha_i$ v rozkladu (3). Přirozené číslo k_i se nazývá *násobnost kořene*. Je-li $k_i = 1$, mluvíme *o kořeni jednoduchém*, je-li $k_i > 1$ *o kořeni vícenásobném.*[2])

Poznámka. Z rozkladu (3) a jeho jednoznačnosti podle 19,7 plyne ihned věta: *Budiž* α *k-násobný kořen rovnice* $f(\xi) = 0$, *pak pro polynom* $f(x)$ *n-tého stupně platí nad* K (*nad* U) *rozklad*

$$f(x) = (x - \alpha)^k g(x) \,, \tag{5}$$

kdež $g(x)$ *je polynom* $(n - k)$*-tého stupně nad* K (*nad* U), *pro nějž* $g(\alpha) \neq 0$. *Obráceně, máme-li rozklad* (5) *polynomu* $f(x)$ *nad* K (*nad* U) *takový, že* $g(\alpha) \neq 0$, *je* α *k-násobným kořenem rovnice* $f(\xi) = 0$.

Na základě definice 40,3 platí věta:

40,4. Věta. *Každá rovnice* $f(\xi) = 0$ *stupně* $n \geqq 1$ *má v tělese* K (U) *právě n kořenů, počítáme-li každý kořen tolikrát, kolik činí jeho násobnost.*

Důkaz plyne ihned z (4).

Násobnost kořene rovnice $f(\xi) = 0$ s koeficienty v libovolném tělese charakteristiky 0 (tedy i v K) souvisí jednoduchým způsobem s kořeny derivací polynomu $f(x)$. Platí totiž věta

40,5. Věta. *Budiž* $f(x)$ *polynom stupně* $n \geqq 1$ *nad* K (*nad tělesem* T *charakteristiky* 0) *a* α *jeden kořen rovnice* $f(\xi) = 0$. *Pak* α *je kořen k-násobný tehdy a jen tehdy, platí-li*

$$f(\alpha) = 0, \; f'(\alpha) = 0, \; \ldots, \; f^{(k-1)}(\alpha) = 0, \quad f^{(k)}(\alpha) \neq 0 \,, \tag{6}$$

t. j. je-li α *zároveň kořenem prvních* $k - 1$ *derivací polynomu* $f(x)$, *není však kořenem derivace k-té.*

Důkaz. Je-li α k-násobným kořenem, pak pro $f(x)$ platí nad K (nad U) rozklad (5), kdež polynom $g(x)$ je jednoznačně určen. Na druhé straně pro každý prvek α z K (z libovolného nadtělesa nad tělesem T charakteristiky 0) existuje celé nezáporné číslo l takové, že platí

$$f(\alpha) = 0, \; f'(\alpha) = 0, \; \ldots, \; f^{(l-1)}(\alpha) = 0, \quad f^{(l)}(\alpha) \neq 0 \,,$$

[1]) Věta 39,12 o jednoznačnosti rozkladového tělesa (viz též poznámku 1 v 39,11) právě zaručuje, že čísla k_i v rozkladu (3) a počet lineárních faktorů r nezávisí na tom, jak si rozkladové těleso U polynomu $f(x)$ zkonstruujeme. Tato čísla jsou tedy již určena polynomem $f(x)$ samým.

[2]) Často je výhodno mluviti i o *kořeni 0-násobném*. Prvek α z K (z U) nazývá se *kořen 0-násobný*, není-li vůbec kořenem rovnice $f(\xi) = 0$, t. j. platí-li $f(\alpha) \neq 0$.

neboť je vždy $f^{(n)}(\alpha) = n!\, a_0 \neq 0$.[3]) Podle Taylorova vzorce (16) z 21,7 platí

$$f(x) = (x-\alpha)^l \left\{ \frac{f^{(l)}(\alpha)}{l!} + (x-\alpha)\frac{f^{(l+1)}(\alpha)}{(l+1)!} + \ldots + (x-\alpha)^{n-l}\frac{f^{(n)}(\alpha)}{n!} \right\} =$$
$$= (x-\alpha)^l h(x) ,$$

při čemž jest $h(\alpha) = f^{(l)}(\alpha)/l! \neq 0$. Musí tedy být $l = k$, $h(x) = g(x)$, čímž je věta dokázána.

Poznámka. Chceme-li určit násobnost kořene α polynomu $f(x)$ podle definice 40,3, musíme znát rozklad polynomu $f(x)$ v kořenové činitele. Věta 40,5 dovoluje určit tuto násobnost, i když rozklad $f(x)$ v kořenové činitele neznáme. Stačí dosazovat do $f(x)$ a jeho derivací α tak dlouho, až přijdeme na derivaci, která se po dosazení nerovná nule. Dosazení provádíme ovšem podle Hornerova schematu 21,9. V tom spočívá hlavní význam věty 40,5.

Vlastností uvedenou v této větě lze též definovat násobnost kořene, ovšem jen pro polynomy nad tělesy charakteristiky 0. Definice 40,3 je tedy obecnější, jest však i přirozenější.

Věta 40,5 platí i pro 0-násobné kořeny. Viz poznámku pod čarou [2]).

40,6. Věta. *Budiž $f(x)$ polynom stupně $n \geqq 1$ nad* K (*nad tělesem* T *charakteristiky* 0). *Je-li α k-násobným kořenem rovnice $f(\xi) = 0$, pak je $(k-1)$-násobným kořenem rovnice $f'(\xi) = 0$.*[4])

Důkaz. Věta ihned plyne z 40,5, uvážíme-li, že i-tá derivace polynomu $f(x)$ je $(i-1)$-ní derivace polynomu $f'(x)$. Viz cv. 21,3.

40,7. Věta. *Budiž $f(x)$ daný polynom stupně $n \geqq 1$ z nějakého číselného tělesa* T (*podtělesa tělesa* K), *neb vůbec z nějakého tělesa* T *charakteristiky* 0. *Budiž $d(x)$ největší společný dělitel polynomů $f(x)$ a $f'(x)$ z $\mathsf{T}[x]$. Je-li α k-násobným kořenem rovnice $f(\xi) = 0$, je $(k-1)$-násobným*[4]) *kořenem rovnice $d(\xi) = 0$ a tato rovnice nemá již jiných kořenů. Platí-li tedy pro polynom $f(x)$ rozklad* (3), *je*

$$d(x) = b_0(x-\alpha_1)^{k_1-1}(x-\alpha_2)^{k_2-1}\ldots(x-\alpha_r)^{k_r-1} . \tag{7}$$

Důkaz. Polynomy $f(x)$, $f'(x)$, $d(x)$ rozložíme nad K neb nad rozkladovým tělesem U′ polynomu $f(x)\,f'(x)\,d(x)$ v součin kořenových činitelů. Budiž $(x-\alpha)$ kořenový činitel polynomu $d(x)$ a budiž l jeho násobnost. Pak platí v oboru integrity $\mathsf{K}[x]$ neb $\mathsf{U}'[x]$ $(x-\alpha)^l \mid d(x)$, $d(x) \mid f(x) \Rightarrow (x-\alpha)^l \mid f(x)$. Proto každý kořenový činitel polynomu $d(x)$ je zároveň i kořenovým činitelem polynomu $f(x)$. Budiž k násobnost kořenového činitele $(x-\alpha)$ v $f(x)$. Protože platí $(x-\alpha)^l \mid d(x)$, $d(x) \mid f'(x) \Rightarrow (x-\alpha)^l \mid f'(x)$ a protože podle 40,6 $(x-\alpha)$ jako kořenový činitel polynomu $f'(x)$ má násobnost $k-1$,[3]) musí $l \leqq k-1$.

[3]) Zde podstatně užíváme předpokladu, že těleso T má charakteristiku 0. Takové celé nezáporné číslo l nemusí pro polynomy nad tělesem charakteristiky p existovat, neboť všechny derivace nenulového polynomu $f(x)$ mohou být v tomto případě nulové polynomy. Viz 21,2 a cv. 21,10 a cv. 21,11.

[4]) Věc platí i pro $k = 1$, definujeme-li si 0-násobný kořen podle poznámky pod čarou [3]).

Na druhé straně podle 18,7 existují v oboru integrity $\mathsf{T}[x]$ polynomy $h_1(x)$ a $h_2(x)$ takové, že platí

$$f(x)\,h_1(x) + f'(x)\,h_2(x) = d(x)\ . \tag{8}$$

Budiž $(x - \alpha)$ nějaký kořenový činitel polynomu $f(x)$ násobnosti k a budiž l $(l \geqq 0)$[2]) násobnost tohoto kořenového činitele v $d(x)$. Z (8) plyne $(x-\alpha)^{k-1} \mid f(x)$, $(x-\alpha)^{k-1} \mid f'(x) \Rightarrow (x-\alpha)^{k-1} \mid d(x)$ a tedy $(k-1) \leqq l$. $d(x)$ má tedy za kořenové činitele kořenové činitele z $f(x)$ a každý z nich v násobnosti $k-1$. Pro $d(x)$ platí proto rozklad (7).

Nakonec si odvodíme ještě dva důsledky z věty 40,7.

40,8. Věta. *Budiž $f(x)$ ireducibilní polynom nad daným číselným tělesem* T (*nad tělesem* T *charakteristiky* 0). *Pak $f(x)$ má jen jednoduché kořeny.*

Poznámka. Věta neplatí pro polynomy nad nějakým tělesem T charakteristiky p. V tomto případě může v $\mathsf{T}[x]$ existovat ireducibilní polynom, který má vícenásobné kořenové činitele. Těleso T musí však mít nekonečně mnoho prvků (viz cv. 40,13). Důkaz těchto tvrzení leží však mimo rámec této knihy.

Důkaz. Věta platí triviálně, je-li $f(x)$ prvního stupně. Je-li $f(x)$ ireducibilní polynom stupně $n \geqq 2$, je $f'(x)$ podle 21,2 polynom stupně $(n-1) \geqq 1$. Jsou tedy podle 18,1 a 19,2 $f(x)$ a $f'(x)$ polynomy nesoudělné, t. j. musí platit v (7) $k_i - 1 = 0$, $i = 1, 2, \ldots, r$ čili $k_i = 1$.

40,9. Věta. *Budiž $f(x)$ polynom z $\mathsf{T}[x]$, kdež* T *je dané číselné těleso* (*těleso charakteristiky* 0). *Platí-li pro $f(x)$ rozklad v kořenové činitele* (3), *pak i polynom*

$$g(x) = c_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_r)$$

je polynom z $\mathsf{T}[x]$. Jinými slovy: V $\mathsf{T}[x]$ leží vždy polynom $g(x)$, který má stejné kořenové činitele jak polynom $f(x)$, v němž však každý kořenový činitel je jednoduchý. Jest $g(x) = f(x)/d(x)$.

Poznámka. Věty 40,9 používáme často, překážejí-li nám při vyšetřování nějaké rovnice $f(\xi) = 0$ vícenásobné kořeny. V tomto případě nahradíme tuto rovnici rovnicí $g(\xi) = 0$, která má stejné kořeny jako předešlá, avšak každý jen jednoduchý.

Důkaz. V $\mathsf{T}[x]$ leží polynom $d(x)$ z 40,7. Proto tam leží též polynom $f(x)/d(x)$, který má požadovaný tvar; jak plyne z rozkladů (3) a (7).

Cvičení k § 40.

Cv. 40,1. Ř. a) Najděte, kolikanásobné jsou kořeny 5 a -4 v rovnici $\xi^4 - 2\xi^3 - 39\xi^2 + 40\xi + 400 = 0$. b) Totéž pro čísla 1 a -2 a rovnici $\xi^5 + 4\xi^4 + \xi^3 - 10\xi^2 - 4\xi + 8 = 0$. c) Totéž pro čísla 3, 4, -1 a rovnici $\xi^7 - 11\xi^6 + 41\xi^5 - 16\xi^4 - 42\xi^3 + 108\xi^2 - 81 = 0$.

Cv. 40,2. Dokažte: Rovnice

$$1 + \frac{\xi}{1} + \frac{\xi^2}{2!} + \ldots + \frac{\xi^n}{n!} = 0$$

nemá vícenásobných kořenů.

Cv. 40,3. Ř. Budiž $f(x)$ polynom nad K a nechť platí $f'(x) \mid f(x)$. Najděte tvar polynomu $f(x)$.

Cv. 40,4. a) Dokažte větu 40,6 přímým derivováním výrazu (5) pro $f(x)$. b) Dokažte větu 40,5 přímým derivováním výrazu (5). (Návod: Použijte cv. 21,2.)

Cv. 40,5. Dokažte větu 40,7 z věty 40,6 a rozkladu (3) pomocí cv. 19,14 a cv. 18,12. (Návod: Počítejte nejv. sp. dělitele polynomů $f(x)$ a $f'(x)$ z jejich rozkladů nad K (nad rozkladovým tělesem U' polynomu $f(x)\,f'(x)$) podle cv. 19,14 a pak dokažte pomocí cv. 18,12, že je to nejv. sp. dělitel těchto polynomů, i když je vyšetřujeme v $\mathsf{K}[x]$ neb v $\mathsf{T}[x]$.

Cv. 40,6. Nechť $f(x)$ je polynom nad K (nad T) stupně $n \geqq 1$, který má jen jednoduché kořenové činitele: $f(x) = a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$. Dokažte: Nad K (nad U) platí

$$f'(x) = \frac{f(x)}{x - \alpha_1} + \frac{f(x)}{x - \alpha_2} + \ldots + \frac{f(x)}{(x - \alpha_n)} .$$

Speciálně platí

$$f'(\alpha_i) = a_0(\alpha_i - \alpha_1)(\alpha_i - \alpha_2) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n) .$$

*

Od 40,5 jsme předpokládali, že těleso T, v němž leží koeficienty polynomu $f(x)$, má charakteristiku 0. Pro polynomy $f(x)$ nad tělesem T charakteristiky p platí poněkud jiné věci, jak je vidět z těchto cvičení. (Záleží na pořadí cvičení!)

Cv. 40,7. Dokažte jako náhradu věty 40,5: Budiž $f(x)$ polynom stupně $n \geqq 1$ nad T char. p. Budiž α kořen rovnice $f(\xi) = 0$ z nějakého nadtělesa nad T. Pak α je k-násobný kořen této rovnice tehdy a jen tehdy, platí-li

$$\bar{f}'(\alpha) = 0,\ \bar{f}''(\alpha) = 0,\ \ldots,\ \bar{f}^{(k-1)}(\alpha) = 0,\ \bar{f}^{(k)}(\alpha) \neq 0 ,$$

kdež $\bar{f}^{(i)}(x)$ jsou polynomy (18) z 21,8. (Návod: Místo Taylorova vzorce (16) z 21,7 použijte k důkazu vzorce (20) z 21,8.)

Cv. 40,8. Ř. Dokažte: Pro polynom $f(x)$ z cv. 40,7 je polynom $\bar{f}'(x)$ polynom nulový tehdy a jen tehdy, když $f(x)$ je tvaru

$$a_0x^{kp} + a_1x^{(k-1)p} + \ldots + a_{k-1}x^p + a_k , \tag{9}$$

t. j. když existuje polynom $g(x)$ v $\mathsf{T}[x]$ takový, že $f(x) = g(x^p)$.

Cv. 40,9. Ř. Za předpokladů cv. 40,7 mějž polynom $f(x)$ tvar (9). Dokažte pomocí cv. 40,7: Každý kořen rovnice $f(\xi) = 0$ je nejméně p-násobný.

Cv. 40,10. T. Ř. Za předpokladu cv. 40,7 budiž $f(x)$ polynom, který není tvaru (9). Dokažte: Je-li $f(x)$ ireducibilní nad T, pak má jen jednoduché kořenové činitele. (Návod: Budiž $d(x)$ nejv. sp. dělitel polynomů $f(x)$, $\bar{f}'(x)$, pak platí podle 18,7 $f(x)\,h_1(x) + \bar{f}'(x)h_2(x) = d(x)$ pro vhodné $h_1(x)$, $h_2(x)$ z $\mathsf{T}[x]$. Z této rovnosti dokažte: Má-li $f(x)$ vícenásobný kořenový činitel, pak $d(x)$ je stupně aspoň prvního.)

Poznámka. Je-li T těleso char. p o nekonečně mnoha prvcích, mohou existovat ireducibilní polynomy tvaru (9). Ty pak mají jen vícenásobné kořenové činitele podle cv. 40,9. To způsobuje, že teorie nadtěles nad takovým tělesem T i teorie rovnic s koeficienty v T je daleko složitější než pro případ charakteristiky 0. Je-li T konečné těleso char. p, pak platí i pro polynomy nad T věta 40,8. To je obsahem dalších cvičení.

Cv. 40,11. Ř. Budiž T konečné těleso char. p. Dokažte: V T existuje ke každému prvku a prvek b takový, že $a = b^p$. (Existence p-té odmocniny.) (Návod: Dokažte: V T platí $a^p = b^p \Leftrightarrow a = b$ a odpočítejte ty prvky z T, jež jsou p-tými mocninami jiných prvků.)

Cv. 40,12. T. Ř. Budiž T těleso z cv. 40,11. Budiž $f(x)$ polynom nad T tvaru (9). Dokažte: V T$[x]$ existuje polynom $g(x)$ takový, že $f(x) = [g(x)]^p$. (Návod: Použijte cv. 40,11.)

Cv. 40,13. Ř. Budiž T těleso z cv. 40,11. Dokažte: Každý ireducibilní polynom z T$[x]$ má jen jednoduché kořenové činitele.

§ 41. Rovnice s reálnými a racionálními koeficienty.

Rovnice s koeficienty v tělese čísel reálných P mají některé speciální vlastnosti. Těmto vlastnostem je věnována první část tohoto paragrafu. Druhá část pojednává o způsobu, jakým lze vypočísti racionální kořeny rovnice s racionálními koeficienty.

41,1. Věta. *Budiž*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \tag{1}$$

polynom s reálnými koeficienty. Je-li imaginární číslo $\beta = b_1 + ib_2$ $(b_2 \neq 0)$ *k-násobným kořenem rovnice* $f(\xi) = 0$, *je zároveň i číslo komplexně sdružené* $\overline{\beta} = b_1 - ib_2$ *k-násobným kořenem této rovnice. Rovnice* $f(\xi) = 0$ *má proto vždy sudý počet kořenů imaginárních.*

Důkaz. Nejdříve si dokážeme tuto pomocnou větu: *Je-li β kořenem rovnice* $f(\xi) = 0$, *je i číslo komplexně sdružené $\overline{\beta}$ kořenem této rovnice.* Dosaďme do (1) β za x. Dostaneme výraz

$$0 = f(\beta) = a_0\beta^n + a_1\beta^{n-1} + \ldots + a_n \ .$$

Počítejme výraz $\overline{f(\beta)}$. Podle pravidel o počítání s čísly komplexně sdruženými z 13,6 máme

$$0 = \overline{f(\beta)} = a_0\overline{\beta}^n + a_1\overline{\beta}^{n-1} + \ldots + a_n = f(\overline{\beta}) \ ,$$

neboť pro reálná čísla a_i platí $\overline{a}_i = a_i$.

Budiž nejdříve $f(x)$ z (1) ireducibilní polynom nad P. Pak podle 40,8 má jen jednoduché kořenové činitele. Je-li tedy $x - \beta$ kořenovým činitelem polynomu $f(x)$, je jen činitelem jednoduchým a podle pomocné věty musí být i $x - \overline{\beta}$ jednoduchým kořenovým činitelem v $f(x)$. Za druhé nechť $f(x)$ z (1) je reducibilní nad P a nechť platí pro něj tento rozklad v součin ireducibilních polynomů:

$$f(x) = f_1(x)\, f_2(x) \ldots f_r(x) \ . \tag{2}$$

Je-li $x - \beta$ k-násobným kořenovým činitelem v $f(x)$, musí být jednoduchým kořenovým činitelem právě k ireducibilních faktorů na pravé straně (2). Každý tento faktor musí mít podle toho, co jsme právě dokázali, též jednoduchý kořenový činitel $x - \overline{\beta}$. Žádný jiný ireducibilní faktor z (2) nemůže však již mít kořenový činitel $x - \overline{\beta}$, neboť pak by podle pomocné věty musil mít i kořenový činitel $x - \beta$. Tím je věta dokázána.

Důsledkem této věty je věta:

41,2. Věta. *Každý polynom $f(x)$ o reálných koeficientech stupně $n \geqq 1$ dá se nad tělesem* P *takto rozložit v součin ireducibilních polynomů*

$$(3)\quad f(x) = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_r)(x^2+a_1x+b_1)(x^2+a_2x+b_2)\dots \\ \dots(x^2+a_sx+b_s)\ ,$$

kdež $\alpha_1, \alpha_2, \dots, \alpha_r$ jsou všechny reálné kořeny rovnice $f(\xi) = 0$ a rovnice $\xi^2 + a_i\xi + b_i = 0$, $i = 1, 2, \dots, s$ má za kořeny dvě čísla imaginární, komplexně sdružená. Platí zřejmě

$$(4)\qquad r + 2s = n\ .$$

Důkaz. Protože podle 41,1 lze ke každému kořenovému činiteli $(x-\beta)$ polynomu $f(x)$, kdež β je číslo imaginární, přidružit vzájemně jednoznačně kořenový činitel komplexně sdružený $(x-\overline{\beta})$, lze psát nad tělesem komplexních čísel K rozklad

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_r)(x-\beta_1)(x-\overline{\beta}_1)\dots(x-\beta_s)(x-\overline{\beta}_s)\ ,$$

kdež $\alpha_1, \alpha_2, \dots, \alpha_r$ jsou reálné kořeny a $\beta_1, \overline{\beta}_1, \dots, \beta_s, \overline{\beta}_s$ imaginární kořeny rovnice $f(\xi) = 0$. Je-li $\beta_j = c_j' + ic_j''$, $j = 1, 2, \dots, s$, máme $(x-\beta_j)(x-\overline{\beta}_j) = x^2 - 2c_j'x + c_j'^2 + c_j''^2 = x + a_jx + b_j$, kdež $a_j = -2c_j'$, $b_j = c_j' + c_j''^2$. Platí tedy pro $f(x)$ nad P rozklad (3). Polynom $x^2 + a_jx + b_j$ je nad P ireducibilní, neboť jinak by byl součinem dvou reálných polynomů 1. stupně, t. j. měl by reálné kořenové činitele. Jsou tedy v (3) jednotlivé faktory ireducibilní nad P.

Odtud plyne ihned věta:

41,3. Věta. *Jedinými ireducibilními polynomy nad tělesem reálných čísel jsou polynomy prvního stupně a ty polynomy druhého stupně, jež mají dva komplexně sdružené imaginární kořeny.*

41,4. Věta. *Budiž $f(\xi) = 0$ rovnice o reálných koeficientech lichého stupně. Pak tato rovnice má vždy aspoň jeden reálný kořen. Obecně má tato rovnice lichý počet reálných kořenů, je-li každý počítán ve své násobnosti.*

Důkaz. V (4) jsou r a s čísla celá nezáporná. Protože n je liché, musí být i r liché, tedy při nejmenším 1.

*

Máme-li rovnici $f(\xi) = a_0\xi^n + a_1\xi^{n-1} + \dots + a_n = 0$ s racionálními koeficienty, pak se dá lehko zjistit, zda tato rovnice má racionální kořeny. K tomu cíli si rovnici $f(\xi) = 0$ upravíme takto: Vynásobíme ji společným jmenovatelem všech koeficientů. Tím dostaneme rovnici, která má celé koeficienty. Koeficienty této rovnice vydělíme případně ještě největším společným dělitelem těchto koeficientů. Tak dostaneme rovnici

$$(5)\qquad g(\xi) = b_0\xi^n + b_1\xi^{n-1} + \dots + b_n = 0\ ,$$

která je zřejmě ekvivalentní původní rovnici a má za koeficienty celá nesoudělná čísla.[1]) Rovnici budeme v dalším vždy psát v tomto tvaru a její racionální kořen budeme psát r/s, kdež r, s jsou dvě čísla celá, nesoudělná. Vyhledávání racionálních kořenů se děje pak pomocí následujících dvou vět:

41,5. Věta. *Budiž* (5) *rovnice o celých koeficientech. Bez újmy obecnosti lze předpokládat* $b_n \neq 0$.[2]) *Má-li tato rovnice racionální kořen* r/s, *kdež* r, s *jsou celá nesoudělná čísla, pak musí*

$$r \mid b_n , \qquad s \mid b_0 .$$

Důkaz. Máme

$$s^n g\left(\frac{r}{s}\right) = b_0 r^n + b_1 r^{n-1} s + \ldots + b_{n-1} r s^{n-1} + b_n s^n = 0 .$$

Protože v tomto součtu celých čísel je prvních n sčítanců dělitelno r, musí i $r \mid b_n s^n \Rightarrow r \mid b_n$ podle 7,20, neboť r, s jsou čísla nesoudělná. Stejným způsobem dostaneme $s \mid b_0 r^n \Rightarrow s \mid b_0$.

Pro stanovení racionálních kořenů stačí tedy najíti všechny dělitele čísel b_0, b_n i se znaménky, skombinovat je všemi způsoby ve zlomky r/s a dosazením do (5) se přesvědčit, které z nich jsou kořeny rovnice (5). Počet zkoušek lze podstatně zmenšit pomocí této věty:

41,6. Věta.[3]) *Je-li racionální číslo* r/s, r, s *celá nesoudělná čísla, kořenem rovnice* (5) *o celých koeficientech, pak musí*

$$(6) \qquad (r - s) \mid g(1) , \qquad (r + s) \mid g(-1) .$$

Důkaz. Pro polynom $g(x)$ platí rozklad

$$(7) \qquad g(x) = \left(x - \frac{r}{s}\right) h(x) .$$

Polynom $h(x)$ musí mít rovněž celé koeficienty, jak plyne ze cv. 41,1. Položíme-li do (7) $x = 1$ a $x = -1$, dostaneme $s\,g(1) = (s - r)\,h(1)$, $s\,g(-1) = (-s - r)\,h(-1)$. Odtud plyne $(r - s) \mid s\,g(1)$, $(r + s) \mid s\,g(-1)$, a protože $r - s$, $r + s$ jsou čísla nesoudělná s s, dostáváme odtud podle 7,20 (6).

Příklad. Mějme rovnici

$$(8) \qquad \xi^6 - \tfrac{13}{10}\xi^5 - \tfrac{4}{5}\xi^4 + \tfrac{19}{10}\xi^3 - \tfrac{53}{10}\xi^2 + \tfrac{19}{10}\xi + \tfrac{3}{5} = 0 .$$

Vynásobením nejmenším společným jmenovatelem koeficientů dostaneme

$$(9) \qquad g(\xi) = 10\xi^6 - 13\xi^5 - 8\xi^4 + 9\xi^3 - 53\xi^2 + 19\xi + 6 = 0 .$$

[1]) Volíme rovnici s nesoudělnými koeficienty proto, že taková rovnice má mezi všemi rovnicemi s celými koeficienty tvaru $k\,f(\xi) = 0$, k racionální číslo, koeficienty o nejmenších absolutních hodnotách.

[2]) Jinak má rovnice kořen 0 a vydělením příslušnou mocninou ξ dostaneme rovnici s absolutním členem různým od 0.

[3]) Zobecnění této věty viz cv. 41,2.

Dělitelé čísla 6 jsou $\pm 1, \pm 2, \pm 3, \pm 6$, dělitelé čísla 10 jsou $\pm 1, \pm 2, \pm 5, \pm 10$. Racionálními kořeny rovnice (8) mohou být podle 41,5 toliko některá z těchto čísel

$$(10)\qquad \begin{array}{l} \pm 1, \pm 2, \pm 3, \pm 6, \\ \pm \tfrac{1}{2}, \quad \pm \tfrac{3}{2}, \\ \pm \tfrac{1}{5}, \pm \tfrac{2}{5}, \pm \tfrac{3}{5}, \pm \tfrac{6}{5}, \\ \pm \tfrac{1}{10}, \quad \pm \tfrac{3}{10}\,. \end{array}$$

Hornerovým schematem (viz 21,9) vypočteme $g(1) = -30$, $g(-1) = -60$. 1 a -1 nejsou tedy kořeny rovnice (8). Zkoušíme nejdříve celé kořeny. Pro 2 máme $2 - 1 = 1$, $2 + 1 = 3$ a skutečně $1 \mid g(1)$, $3 \mid g(-1)$. Proto 2 může být podle 41,6 kořenem rovnice (9). Dosadíme $\xi = 2$ do (9). Hornerovo schema dává

	10,	−13,	−8,	9,	−53,	19,	6
2|		20,	14,	12,	42,	−22,	−6
	10,	7,	6,	21,	−11,	−3,	0.

2 jest proto kořenem rovnice (8). Nyní vyšetřujeme rovnici $g(\xi)/(\xi - 2)$, jejíž koeficienty tvoří třetí řádek Hornerova schematu:

$$(11)\qquad g_1(\xi) = 10\xi^5 + 7\xi^4 + 6\xi^3 + 21\xi^2 - 11\xi - 3 = 0\,.$$

Jest $g_1(1) = 30$, $g_1(-1) = 20$. Z celých kořenů (10) přicházejí nyní v úvahu podle 41,5 jen 3, −3. Jest $3 - 1 = 2$, $3 + 1 = 4$ a skutečně $3 \mid 30$, $4 \mid 20$, kdežto $-3 - 1 = -4$ a $4 \nmid 30$. Dosadíme tedy $\xi = 3$ do $g_1(1)$ a Hornerovo schema dává

	10,	7,	6,	21,	−11,	−3	
3|		30					
	10,	37					.

Dále není třeba počítat, neboť jest již vidět, že $g_1(3) > 0$. Tím jsme ukázali, že žádné číslo mimo 2 z prvního řádku tabulky (10) nemůže být kořenem rovnice (8). Pro rovnici (11) přicházejí podle 41,5 v úvahu jen necelá čísla z 1. a 3. sloupce tabulky (10). Pro $\frac{1}{2}$ máme $1 - 2 = -1$, $1 + 2 = 3$ a $3 \nmid g_1(-1)$, kdežto pro $-\frac{1}{2}$ dostáváme podle 41,6 $1 + 2 = 3$, $1 - 2 = -1$ a skutečně $3 \mid g_1(1)$, $-1 \mid g_1(-1)$. Dosadíme do $g_1(\xi)$ $\xi = -\frac{1}{2}$:

	10,	7,	6,	21,	−11,	−3	
$-\frac{1}{2}$|		−5,	−1,	$-\frac{5}{2}$			.
	10,	2,	5				.

Dále není třeba počítat, neboť podle cv. 41,1 nemůže již $-\frac{1}{2}$ být kořenem. Pro $\frac{3}{2}$ máme $3 - 2 = 1$, $3 + 2 = 5$ a jest $1 \mid g_1(1)$, $5 \mid g_1(-1)$. Dosadíme $\xi = \frac{3}{2}$ do $g_1(\xi)$:

	10,	7,	6,	21,	−11,	−3	
$\frac{3}{2}$|		15,	33,	$\frac{33}{2}$,			
	10,	22,	39				.

$\frac{3}{2}$ není též kořenem. Pro $\xi = -\frac{3}{2}$ dostáváme $3 + 2 = 5$, $3 - 2 = 1$ a opět $5 \mid g_1(1)$, $1 \mid g_1(-1)$. Dosadíme $\xi = -\frac{3}{2}$ a dostáváme

$$\begin{array}{r|rrrrrr} & 10, & 7, & 6, & 21, & -11, & -3 \\ -\frac{3}{2}| & & -15, & 12, & -27, & 9, & 3 \\ \hline & 10, & -8, & 18, & -6, & -2, & 0 \end{array} .$$

$-\frac{3}{2}$ je proto kořenem rovnice (8). Třetí řádek tohoto Hornerova schematu dává $g_2(\xi) = g_1(\xi)/2(\xi + \frac{3}{2})$

$$g_2(\xi) = 5\xi^4 - 4\xi^3 + 9\xi^2 - 3\xi - 1 = 0 . \tag{12}$$

Z čísel (10), která ještě nebyla zkoušena, přicházejí v úvahu jen $\pm\frac{1}{5}$.[4]) Jest $g_2(1) = 6$, $g_2(-1) = 20$. Pro $\xi = \frac{1}{5}$ máme $1 - 5 = -4$ a $-4 \nmid g_2(1)$. $\frac{1}{5}$ není tedy kořenem rovnice (12). Pro $\xi = -\frac{1}{5}$ máme $1 + 5 = 6$, $1 - 5 = -4$ a jest $6 \mid g_2(1)$, $-4 \mid g_2(-1)$. Proto dosadíme do (12) $\xi = -\frac{1}{5}$

$$\begin{array}{r|rrrrr} & 5, & -4, & 9, & -3, & -1 \\ -\frac{1}{5}| & & -1, & 1, & -2, & 1 \\ \hline & 5, & -5, & 10, & -5, & 0 \end{array} .$$

$-\frac{1}{5}$ jest dalším kořenem. Rovnice $g_2(\xi)/5(\xi + \frac{1}{5}) = g_3(\xi)$ má tvar

$$g_3(\xi) = \xi^3 - \xi^2 + 2\xi - 1 = 0 .$$

Tato rovnice podle 41,5 nemůže již mít za kořen žádné z čísel $-\frac{1}{5}$, $\pm\frac{2}{5}$, $\pm\frac{1}{10}$. Rovnice (8) má proto jen tyto racionální kořeny 2, $-\frac{3}{2}$, $-\frac{1}{5}$ a každý z nich jen jednoduchý.

Cvičení k § 41.

***Cv. 41,1.** Ř. Dokažte: Je-li α necelý racionální kořen rovnice (5), pak v Hornerově schematě pro α

$$\begin{array}{r|ccccc} & b_0, & b_1, & \ldots, & b_{n-1}, & b_n \\ \alpha| & & \alpha b_0, & & \alpha b'_{n-2} & \alpha b'_{n-1} \\ \hline & b_0, & b'_1 & & b'_{n-1}, & 0 \end{array} ,$$

kdež $b'_i = b_i + \alpha b'_{i-1}$, $i = 1, 2, \ldots, n$, $b'_0 = b_0$, jsou v druhém a třetím řádku samá celá čísla. Odtud plyne, že ve vztahu $g(x) = (x - \alpha)\, g_1(x)$ $g_1(x)$ má celé koeficienty.

Cv. 41,2. Dokažte zobecnění věty 41,6: Je-li racionální číslo r/s, r, s celá nesoudělná čísla, kořenem rovnice (5), je-li m libovolné celé číslo, pak musí $(r - sm) \mid g(m)$. Této věty lze použít k vyloučení dalších čísel při stanovení racionálních kořenů rovnice. Je to výhodné tehdy, když jsme byli v průběhu výpočtu nuceni vypočísti hodnotu $g(m)$ pro nějaké m. (Návod: Postupujte stejně, jako při důkaze 41,6.)

Cv. 41,3. Ř. Najděte racionální kořeny rovnic

a) $\xi^4 + \xi^3 - 3\xi^2 + 7\xi - 6 = 0$,

b) $4\xi^4 - 2\xi^3 + \xi - 6 = 0$,

[4]) Pro rovnici (12) nutno vlastně zkoušet číslo $-\frac{1}{5}$ znovu, neboť rovnice (8) a tedy i rovnice (11) by mohla mít kořen $-\frac{1}{5}$ vícenásobný. Tento kořen však podle 41,5 pro rovnici (12) odpadá, neboť $3 \nmid (-1)$.

c) $15\xi^6 + 2\xi^5 + 29\xi^4 + 49\xi^3 - 11\xi^2 - 5\xi + 1 = 0$,
d) $6\xi^5 + 5\xi^4 + 6\xi^3 + 4\xi^2 - 17\xi + 6 = 0$,
e) $5\xi^4 - 3\xi^3 + 7\xi^2 - \xi - 3 = 0$.

Cv. 41,4. Dokažte: Každému racionálnímu kořenu α rov. (5) odpovídá celý kořen $\beta = b_0\alpha$ rovnice

$$h(\eta) = \eta^n + b_1\eta^{n-1} + b_2b_0\eta^{n-2} + \ldots + b_{n-1}b_0^{n-2}\eta + b_nb_0^{n-1} = 0 \tag{13}$$

a naopak. Lze tedy vyšetřovat jen celé kořeny rov. (13) a počítat jen s celými čísly. Jest to ovšem výhodné jen pro rovnice s malým $|b_0|$. Přesvědčte se, že by tento postup nebyl výhodný u rov. (9) v příkladu z 41,6.

Cv. 41,5. Ř. Dokažte: Rov. (5) nemá žádné celé kořeny, jsou-li čísla $g(0)$, $g(1)$ obě liché. (Návod: Užijte věty 41,5 a 41,6.)

Cv. 41,6. Ř. Dokažte: Jestliže v rov. (5) čísla b_0, b_n a aspoň jedno z čísel $g(1)$, $g(-1)$ jsou lichá, pak (5) nemá žádný racionální kořen. (Návod: Užijte vět 41,5 a 41,6.)

Cv. 41,7. Ř. Dokažte: Jestliže v rov. (5) žádné z čísel b_0, b_n, $g(1)$, $g(-1)$ není dělitelno 3, pak rov. (5) nemá žádný racionální kořen.

KAPITOLA VIII.

SYMETRICKÉ FUNKCE.

§ 42. Pojem symetrické funkce.

Než přikročíme k výkladu o řešení algebraických rovnic, musíme si vyložit vlastnosti jistých speciálních polynomů a racionálních funkcí n neurčitých, zvaných symetrické funkce, které hrají při řešení algebraických rovnic důležitou úlohu. Těmto racionálním funkcím bude věnována tato kapitola.

42,1. Permutace prováděné na neurčité v polynomech. Mějme polynom $f(x_1, x_2, \ldots, x_n)$ n neurčitých $x_1, x_2, \ldots, x_n$ nad daným oborem integrity J. Provedeme-li na pořadí neurčitých $(x_1, x_2, \ldots, x_n)$ v polynomu nějakou permutaci, na př. permutaci (1) z 29,1, dostaneme pořadí $(x_{k_1}, x_{k_2}, \ldots, x_{k_n})$. (Viz 29,4.) Tím vznikne z polynomu $f(x_1, x_2, \ldots, x_n)$ polynom $f(x_{k_1}, x_{k_2}, \ldots, x_{k_n}) = g(x_1, x_2, \ldots, x_n)$, který je obecně různý od polynomu $f(x_1, x_2, \ldots, x_n)$. Říkáme, že *polynom* $g(x_1, x_2, \ldots, x_n)$ *dostaneme z* $f(x_1, x_2, \ldots, x_n)$ *permutací* (1) z 29,1.

Příklad 1: Polynom 3 neurčitých

$$f(x_1, x_2, x_3) = x_1^4 + x_1^2x_2x_3 + x_2^3x_3 + x_2x_3^3 + x_1^2 + x_2x_3 + x_2 + x_3$$

přejde permutací P_4 z 29,2 v polynom

$$f(x_2, x_3, x_1) = g(x_1, x_2, x_3) =$$
$$= x_2^4 + x_1x_2^2x_3 + x_1x_3^3 + x_1^3x_3 + x_2^2 + x_1x_3 + x_3 + x_1 ,$$