IV. Některé poznatky z teorie čísel a z algebry

In: Eduard Čech (author): Čísla a početní výkony. (Czech). Praha: Státní nakladatelství technické literatury, 1954. pp. 138--191.

Persistent URL: http://dml.cz/dmlcz/402584

IV. NĚKTERÉ POZNATKY Z THEORIE ČÍSEL A Z ALGEBRY

§ 1. Nejmenší společný násobek a největší společný dělitel dvou přirozených čísel

Je-li d přirozené číslo, nazýváme jeho *násobkem* každé z přirozených čísel

$$1 \,.\, d = d,\ 2d,\ 3d,\ 4d,\ \ldots \qquad (1,1)$$

Tedy každé přirozené číslo d má nekonečně mnoho násobků; nejmenší z nich je číslo d samo. Následující věta je zřejmá.

Věta 1,1. *Každé přirozené číslo je násobkem čísla* 1.

Sledujeme-li přirozená čísla 1, 2, 3, ... v jejich přirozeném uspořádání, vidíme, že (v případě $d > 1$) nejprve přijde $d - 1$ nenásobků čísla d, potom jeden násobek, za ním zase $d - 1$ nenásobků, znovu jeden násobek atd. Pro $d = 2$ z toho plyne:

Věta 1,2. *Násobky dvou jsou totožné se sudými přirozenými čísly.*

Věta 1,3. *Jsou-li a, b dva násobky přirozeného čísla d, je také $a + b$ násobkem čísla d. Jestliže $a > b$, je také $a - b$ násobkem čísla d.*

Důkaz. Podle předpokladu existují taková přirozená čísla m, n, že $a = md$, $b = nd$, takže

$$a + b = (m + n)\, d\,, \quad a - b = (m - n)\, d\,;$$

$m + n$ je přirozené číslo, a je-li $a > b$, je také $m - n$ přirozené číslo. Následující dvě věty jsou zřejmé.

Věta 1,4. *Násobek násobku přirozeného čísla d je násobkem čísla d.*

Věta 1,5. *Součin dvou přirozených čísel je násobkem každého z nich.*

Jsou-li dána dvě přirozená čísla a, b (nemusíme předpokládat, že $a \neq b$), je patrné z věty 1,5, že existuje aspoň jeden jejich *společný násobek*, t. j. přirozené číslo, které je násobkem každého z nich; podle věty 1,4 je společných násobků čísel a, b nekonečně mnoho. Jelikož společné násobky čísel a, b jsou přirozená čísla, existuje

nejmenší společný násobek přirozených čísel a, b, který označíme nsn (a, b).

Věta 1,6. *Je-li přirozené číslo a násobkem přirozeného čísla b, je* nsn $(a, b) = a$. *Neboť číslo a nemá žádný násobek menší než a.*

Věta 1,7. *Každý společný násobek přirozených čísel a, b je násobkem čísla* nsn (a, b).

Důkaz. Budiž $d = \text{nsn}\,(a, b)$. Předpokládejme, že existuje takový společný násobek c čísel a, b, který není členem posloupnosti (1,1). Podle definice čísla d je $c > d$, takže existuje takové přirozené číslo n, že

$$nd < c < (n + 1)\,d\,.$$

Jestliže zde všude přičteme číslo $-nd$, dostaneme

$$0 < c - nd < d\,.$$

To je však nemožné, neboť přirozené číslo $c - nd$ je podle věty 1,3 společným násobkem čísel a, b, takže nemůže být $c - nd < \text{nsn}\,(a, b)$.

Říkáme, že přirozené číslo d je *dělitelem* přirozeného čísla n nebo že číslo n je *dělitelné* číslem d, je-li n násobkem čísla d neboli, což je totéž, je-li $\frac{n}{d}$ číslo celé. Je-li tomu tak, je zřejmě $d \leqq n$. Z toho plyne, že *každé přirozené číslo n má konečný počet dělitelů*; je zvykem značit tento počet $\tau(n)$. Je-li n libovolné přirozené číslo, jsou

$$\frac{n}{1} = n\,, \quad \frac{n}{n} = 1$$

čísla celá. Tedy: *číslo* 1 *je dělitelem každého přirozeného čísla; každé přirozené číslo je svým vlastním dělitelem.* Protože $d \leqq n$ pro každého dělitele d přirozeného čísla n, má číslo 1 jediného dělitele, totiž samo sebe; je tedy $\tau(1) = 1$. Naproti tomu má každé přirozené číslo $n > 1$ aspoň dva různé dělitele (samo sebe a číslo 1), je tedy $\tau(n) \geqq 2$. Je-li $\tau(n) = 2$, říkáme, že n je *prvočíslo*. Tedy prvočíslem nazýváme přirozené číslo n *větší než jedna*, které mimo samo sebe a mimo číslo 1 už nemá jiného dělitele. O prvočíslech si promluvíme podrobněji v § 2.

Poznámka 1,1. Eukleides, o kterém byla zmínka na str. 15, počítal také číslo 1 mezi prvočísla; podle dnešní vědecké terminologie však číslo 1 není prvočíslem.

Věta 1,8. *Dělitel dělitele přirozeného čísla n je dělitelem čísla n.* To je zřejmé.

Poznámka 1,2. Je zajímavé si všimnout, že věta 1,8 má přesně týž obsah jako věta 1,4. Neboť v obou větách je řeč o třech přirozených číslech, která označíme d, a, n. Věta 1,4 praví, že je-li a násobkem čísla d a je-li n násobkem čísla a, je n násobkem čísla d; věta 1,8 praví, že je-li a dělitelem čísla n a je-li d dělitelem čísla a, je d dělitelem čísla n; rozdíl je pouze slovní, ne věcný.

Buďtež opět dána dvě přirozená čísla a, b (nemusíme předpokládat, že $a \neq b$). Číslo 1 je *společným dělitelem* obou čísel a, b a každé z nich má jen konečný počet dělitelů; čísla a, b tedy mají určitého *největšího společného dělitele*, kterého označíme Nsd (a, b).

Poznámka 1,3. Píšeme nsn s *malým* počátečním n (*nejmenší* společný násobek), ale Nsd s *velkým* počátečním písmenem (*největší* společný dělitel).

Věta 1,9. *Je-li přirozené číslo b dělitelem přirozeného čísla a, je* Nsd $(a, b) = b$, neboť číslo b nemá žádného dělitele většího než b.

Poznámka 1,4. Všimněme si, že předpoklad věty 1,6 (že a je násobkem čísla b) je totožný s předpokladem věty 1,9 (že b je dělitelem čísla a).

Zvolme nyní přirozená čísla a, b a položme $c =$ nsn (a, b). Podle věty 1,7 je každý společný násobek čísel a, b násobkem čísla c, takže podle věty 1,5 existuje takové přirozené číslo d, že

$$ab = cd\,. \tag{1,2}$$

Protože c je společným násobkem čísel a, b, existují taková přirozená čísla u, v, že

$$c = au\,, \quad c = bv\,. \tag{1,3}$$

Jestliže z (1,3) dosadíme do (1,2), dostaneme $ab = aud$, $ab = bvd$; krácením (t. j. užitím věty II 3,1) vyjde $b = ud$, $a = vd$. Tedy číslo d je společným dělitelem čísel a, b. Dokážeme, že d má tuto vlastnost:

Každý společný dělitel čísel a, b je dělitelem čísla d. (*)

Budiž t kterýkoli společný dělitel čísel a, b, takže existují taková přirozená čísla u, v, že

$$a = ut\,, \quad b = vt\,.$$

Potom je

$$\frac{ab}{t} = bu\,, \quad \frac{ab}{t} = av\,,$$

takže $\frac{ab}{t}$ je přirozené číslo, které je společným násobkem čísel a, b; z toho plyne podle věty 1,7, že existuje takové přirozené číslo s, že $\frac{ab}{t} = cs$ neboli $ab = cst$; dosadíme-li za ab z (1,2), dostaneme $cd = cst$ a po zkrácení vyjde $d = st$, takže t je vskutku dělitelem čísla d. Protože d je společným dělitelem čísel a, b a protože dělitel čísla d nemůže být větší než d, je $d = \text{Nsd}\ (a, b)$.

Právě provedená úvaha je důkazem následujících dvou vět:

Věta 1,10. *Jsou-li a, b přirozená čísla a je-li $c = \text{nsn}\ (a, b)$, $d = \text{Nsd}\ (a, b)$, je $cd = ab$.*

Věta 1,11. *Každý společný dělitel přirozených čísel a, b je dělitelem čísla* Nsd (a, b).

Přirozená čísla a, b nazveme *nesoudělná*, je-li číslo 1 jejich jediným společným dělitelem neboli je-li $\text{Nsd}\ (a, b) = 1$.

Věta 1,12. *Buďtež a, b přirozená čísla a budiž $d = \text{Nsd}\ (a, b)$, takže*

$$\frac{a}{d}, \quad \frac{b}{d} \tag{1,4}$$

jsou přirozená čísla. Čísla (1,4) *jsou nesoudělná.* Neboť kdyby čísla (1,4) měla společného dělitele $t > 1$, byla by

$$\frac{a}{dt}, \frac{b}{dt}$$

přirozená čísla, takže by číslo dt bylo společným dělitelem čísel a, b, ale to je nemožné, neboť $dt > d$.

Věta 1,13. *Nechť a, b, c jsou přirozená čísla. Je-li součin ac dělitelný číslem b a jsou-li čísla a, b nesoudělná, je číslo c dělitelné číslem b.*

Důkaz. Protože $\text{Nsd}\ (a, b) = 1$, je podle věty 1,10

$$\text{nsn}\ (a, b) = ab\ . \tag{1,5}$$

Avšak číslo ac je podle věty 1,5 násobkem čísla a a podle předpokladu též násobkem čísla b, takže z (1,5) plyne podle věty 1,7, že číslo ac je násobkem čísla ab, t. j. že existuje takové přirozené číslo t, že $ac = abt$; krácením vyjde $c = bt$, takže c je násobkem čísla b, a to jsme měli dokázat.

Budiž nyní α libovolné kladné racionální číslo. Můžeme psát α nekonečně mnoha způsoby ve tvaru zlomku

$$\alpha = \frac{a}{b}, \tag{1,6}$$

kde a, b jsou přirozená čísla. Je-li dán určitý tvar (1,6) a je-li k jakékoli přirozené číslo, máme vedle tvaru (1,6) nový tvar

$$\alpha = \frac{ka}{kb}, \tag{1,7}$$

o kterém říkáme, že vznikne z tvaru (1,6) *rozšiřováním*. Zpětný přechod od tvaru (1,7) ke tvaru (1,6) se nazývá *krácení*. Zkrátit tvar (1,6) je možné pouze tehdy, mají-li čitatel a a jmenovatel b nějakého společného dělitele $d > 1$. Potom je $a = a_1 d$, $b = b_1 d$, kde a_1, b_1 jsou přirozená čísla, a krátíme-li tvar (1,6) číslem d, dospějeme k novému tvaru

$$\alpha = \frac{a_1}{b_1}. \tag{1,8}$$

Jsou-li přirozená čísla a, b nesoudělná, nelze tvar (1,6) krátit; pravíme pak, že (1,6) je *základní tvar* kladného racionálního čísla α. Jestliže (1,6) není základní tvar a krátíme-li číslem $d = \mathrm{Nsd}\,(a, b)$, dospějeme ke tvaru (1,8), který podle věty 1,12 je základním. Každé racionální číslo $\alpha > 0$ lze tedy psát v základním tvaru.

Věta 1,14. *Ze základního tvaru* (1,6) *racionálního čísla* $\alpha > 0$ *vznikne každý jiný tvar* (t. j. každé jiné vyjádření zlomkem, jehož čitatel i jmenovatel jsou kladná celá čísla) *rozšiřováním.*

Důkaz. Budiž

$$\frac{a}{b} = \frac{u}{v},$$

kde také u, v jsou přirozená čísla. Potom je

$$av = bu, \tag{1,9}$$

takže součin av je dělitelný číslem b; avšak čísla a, b jsou nesoudělná, takže z věty 1,13 plyne, že číslo v je dělitelné číslem b. Dostáváme pro v vyjádření součinem $v = kb$, kde k je přirozené číslo. Dosadíme-li toto vyjádření do (1,9), dostaneme $akb = bu$ a z toho plyne $u = ka$. Tedy tvar $\frac{u}{v}$ splyne s tvarem (1,7).

Poznámka 1,5. Z věty 1,14 plyne, že základní tvar je jednoznačně

určen. Je jasné, že je to ten tvar, jehož jmenovatel má nejmenší možnou hodnotu.

Věta 1,15. *Jsou-li a, c dvě nesoudělná přirozená čísla a je-li d dělitelem čísla c, jsou také čísla a, d nesoudělná.*

Důkaz. Budiž b společný dělitel čísel a, d; máme dokázat, že $b = 1$. Avšak b je dělitelem čísla d, které je dělitelem čísla c; podle věty 1,8 je tedy b dělitelem čísla c, takže b je společným dělitelem nesoudělných čísel a, c, a tedy $b = 1$.

Věta 1,16. *Jestliže každé z obou přirozených čísel a, b je nesoudělné s přirozeným číslem c, je také součin ab nesoudělný s číslem c.*

Důkaz. Budiž d společný dělitel čísel ab, c; máme dokázat, že $d = 1$. Protože čísla a, c jsou nesoudělná a d je dělitelem čísla c, plyne z věty 1,15, že čísla a, d jsou nesoudělná; podobně též čísla b, d jsou nesoudělná. Avšak součin ab je dělitelný číslem d; protože čísla a, d jsou nesoudělná, plyne z věty 1,13, že číslo b je dělitelné číslem d. Tedy d je společným dělitelem čísel b, c, která jsou nesoudělná, takže $d = 1$.

Věta 1,17. *Jestliže každé z přirozených čísel*

$$a_1, a_2, \ldots, a_k$$

je nesoudělné s přirozeným číslem c, je také součin $a_1 a_2 \ldots a_k$ nesoudělný s číslem c.

Důkaz provedeme indukcí vzhledem ke k. Pro $k = 1$ je věta zřejmá. Nechť tedy při určitém k je věta dokázána (předpoklad P) a nechť je dáno $k + 1$ přirozených čísel

$$a_1, a_2, \ldots, a_{k+1},$$

z nichž každé je nesoudělné s c. Máme dokázat, že součin $A = a_1 a_2 \ldots$ $\ldots a_{k+1}$ je nesoudělný s c. Je však $A = Ba_{k+1}$, kde $B = a_1 a_2 \ldots a_k$. Podle předpokladu P jsou čísla B, c nesoudělná; protože také čísla a_{k+1}, c jsou nesoudělná, plyne z věty 1,16, že součin $A = Ba_{k+1}$ je nesoudělný s číslem c.

§ 2. Rozklad přirozených čísel na prvočinitele

Věta 2,1. *Každé přirozené číslo $n > 1$ je dělitelné aspoň jedním prvočíslem.*

Důkaz. Číslo n má jistě aspoň jednoho dělitele většího než 1, totiž samo sebe, a ze všech takových dělitelů je jeden nejmenší;

označme jej p. Potom je p prvočíslo, neboť jinak by přirozené číslo p mělo takového dělitele q, že by bylo $q > 1$, $q < p$; pak by však číslo q podle věty 1,8 bylo dělitelem čísla n, a to je nemožné.

Poznámka 2,1. Je-li n prvočíslem, pak ovšem n není dělitelné žádným prvočíslem $p \neq n$.

Snadno zjistíme, že je celkem 25 prvočísel menších než sto; jsou to čísla

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,

53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Věta 2,2. *Existuje nekonečně mnoho prvočísel.*

Důkaz. Budiž S jakýkoli neprázdný soubor konečně mnoha prvočísel; máme ukázat, že existuje prvočíslo, které nenáleží do souboru S. Za tím účelem zvolme nějaké přirozené číslo P, které je dělitelné každým prvočíslem ze souboru S; za P můžeme volit na př. součin všech prvků souboru S. Přirozené číslo

$$N = P + 1 \tag{2,1}$$

je podle věty 2,1 dělitelné nějakým prvočíslem p. Toto prvočíslo nenáleží do souboru S, neboť jinak by obě čísla N, P byla násobky p, takže by podle věty 1,3 také číslo $N - P = 1$ bylo násobkem p, a to je nemožné.

Poznámka 2,1. Je jasné, že je-li $P > 2$, můžeme změnit předcházející důkaz tak, že místo (2,1) volíme (2,2)

$$N = P - 1 . \tag{2,2}$$

Poznámka 2,2. Je nyní vhodná příležitost, abychom si promluvili o tom, že důkazy indukcí lze provádět trochu jinak, než jak jsme to vylíčili v I § 4. Dokázat indukcí větu V_n pro každé přirozené číslo n znamená odvodit větu V_1, z ní odvodit větu V_2, z té potom větu V_3 atd. Tak jsme to dosud prováděli. Je však jasné, že při důkazu věty V_3 můžeme předpokládat nejen správnost věty V_2, nýbrž správnost obou vět V_1 a V_2; při důkazu věty V_3 můžeme předpokládat nejen správnost věty V_3, nýbrž správnost všech tří vět V_1, V_2, V_3, atd. Tedy: *Abychom dokázali, že nějaká věta V_n je správná pro každé přirozené číslo n, stačí nejprve dokázat větu V_1 a potom pro každé přirozené číslo $n > 1$ odvodit správnost věty V_n z předpokladu, že věta V_k je správná pro každé přirozené číslo $k < n$.*

Věta 2,3. *Každé přirozené číslo $n > 1$ lze psát ve tvaru součinu*

$$n = p_1 p_2 \dots p_k , \tag{2,3}$$

jehož každý činitel je prvočíslem. Při tom musíme připustit i možnost $k = 1$, jinak by věta neplatila pro *prvočísla* n.

Důkaz. Protože o čísle 1 se ve větě 2,3 netvrdí nic, postačí podle poznámky 2,2, jestliže pro libovolně dané přirozené číslo $n > 1$ odvodíme správnost věty z předpokladu (nazveme jej předpoklad P), že pro všecka přirozená čísla menší než n je věta dokázána. Jestliže nyní n je prvočíslo, platí (2,3) pro: $k = 1$, $p_1 = n$. Jestliže $n > 1$ není prvočíslem, je n násobkem přirozeného čísla d, které je větší než 1 a menší než n, takže $n = cd$, kde také $c > 1$, $c < n$. Podle předpokladu P máme pro čísla c, d vyjádření

$$\begin{aligned} c &= p'_1 p'_2 \dots p'_r \quad (r \geqq 1)\,, \\ d &= p''_1 p''_2 \dots p''_s \quad (s \geqq 1)\,, \end{aligned} \tag{2,4}$$

kde každý činitel napravo je prvočíslem. Znásobíme-li obě vyjádření (2,4), dostaneme pro číslo $n = cd$ vyjádření žádaného tvaru (2,3).

Poznámka 2,3. Činitelé součinu napravo ve (2,3) se jmenují *prvočinitelé* čísla n a vyjádření (2,3) se jmenuje *rozklad na prvočinitele* přirozeného čísla $n > 1$.

Následující věta 2,4 je přípravou k větě 2,5.

Věta 2,4. *Jsou-li* $p_1, p_2, \dots, p_k$ *prvočísla a je-li jejich součin* $p_1 p_2 \dots p_k$ *dělitelný prvočíslem* p, *je* p *rovno některému z čísel* $p_1, p_2, \dots, p_k$. Přitom nevylučujeme možnost $k = 1$.

Důkaz. Je-li p různé od všech čísel $p_1, p_2, \dots, p_k$, plyne z definice prvočísla, že každé z čísel $p_1, p_2, \dots, p_k$ je nesoudělné s číslem p, takže podle věty 1,17

$$\mathrm{Nsd}\,(p_1 p_2 \dots p_k, p) = 1\,, \tag{2,5}$$

a to je nemožné, neboť podle věty 1,9 levá strana ve (2,5) je rovna p.

Věta 2,5. *Rozklad přirozeného čísla* $n > 1$ *na prvočinitele je až na pořadí činitelů jednoznačně určen.*

Důkaz. Protože o čísle 1 se netvrdí nic, postačí podle poznámky 2,2, jestliže pro libovolně dané přirozené číslo $n > 1$ provedeme důkaz za předpokladu (předpoklad P), že pro přirozená čísla menší než n je věta správná. Podle věty 2,1 můžeme zvolit prvočíslo p, které je dělitelem čísla n. Je-li n prvočíslem, je zřejmě $n = p$ jediný jeho rozklad na prvočinitele. Není-li n prvočíslem, je v každém takovém rozkladu počet činitelů větší než 1 a podle věty 2,4 je při každém rozkladu jeden prvočinitel roven p. Jsou-li tedy dány dva rozklady čísla n na prvočinitele, musí míti tvar

$$n = pp_1 \dots p_k\,, \quad n = pp'_1 \dots p'_h\,, \tag{2,6}$$

kde $k \geqq 1$, $h \geqq 1$. Potom je $m = \frac{n}{p}$ přirozené číslo větší než 1 a

$$m = p_1 \dots p_k\,, \quad m = p'_1 \dots p'_h\,; \tag{2,7}$$

avšak $m < n$, takže podle předpokladu P je $k = h$ a oba rozklady (2,7) se mohou lišit jen pořadím činitelů; pak ovšem platí totéž i o rozkladech (2,6).

Poznámka 2,4. Je jasné, že přirozené číslo $n > 1$ je dělitelné každým z prvočísel, která se vyskytují napravo v rozkladu (2,3), a podle věty 2,4 není n dělitelné žádným jiným prvočíslem.

Je-li n libovolné přirozené číslo a je-li p libovolné prvočíslo, pak počet těch prvočinitelů v rozkladu (2,3) čísla n, kteří jsou rovni p, nazveme *řádem* čísla n vzhledem k prvočíslu p a označíme

$$\omega(n; p)\,; \tag{2,8}$$

pro $n = 1$ budiž $\omega(1; p) = 0$ pro každé prvočíslo p. Že řád (2,8) je jednoznačně definován, plyne z věty 2,5. Je-li $n > 1$, existuje aspoň jedno prvočíslo p, pro které řád (2,8) je kladný; takových p je jen konečný počet a pro všecka ostatní p je $\omega(n; p) = 0$. Na př. číslo $n = 60$ má rozklad na prvočinitele

$$60 = 2 \,.\, 2 \,.\, 3 \,.\, 5\,;$$

je tedy $\omega(60; 2) = 2$, $\omega(60; 3) = \omega(60; 5) = 1$ a pro všecka prvočísla p větší než 5 je $\omega(60; p) = 0$.

Podle poznámky 2,4 je $\omega(n; p) \geqq 0$ právě tehdy, jestliže číslo n je dělitelné prvočíslem p.

Věta 2,6. *Přiřaďme každému prvočíslu p nezáporné celé číslo r_p tak, aby byl jen konečný počet ($\geqq 0$) takových p, pro něž $r_p > 0$. Potom existuje právě jedno takové přirozené číslo n, pro které je $\omega(n; p) = r_p$ pro všecka prvočísla p. Je-li $r_p = 0$ pro všecka p, je $n = 1$; v opačném případě, jsou-li $p_1, p_2, \dots, p_k$ ta různá prvočísla, pro která je $r_p > 0$, je*

$$n = p_1^{\omega(n; p_1)} \,.\, p_2^{\omega(n; p_2)} \dots p_k^{\omega(n; p_k)}\,. \tag{2,9}$$

Poznámka 2,5. Pro platnost vyjádření (2,9) je podstatné pouze to, aby se mezi prvočísly $p_1, p_2, \dots, p_k$ vyskytovalo (a to jenom jednou) každé takové prvočíslo p, pro které je $r_p > 0$. Nevadí, jestliže snad mezi $p_1, p_2, \dots, p_k$ bude také ještě jedno nebo i více takových prvočísel p, pro která je $\omega(n; p) = 0$, neboť pro každé takové p je $p^{\omega(n; p)} = 1$ a součin napravo ve (2,9) se nezmění připojením činitelů rovných 1.

Věta 2,7. *Jsou-li m, n přirozená čísla, je*

$$\omega(mn; p) = \omega(m; p) + \omega(n; p)$$

pro každé prvočíslo p. Neboť jsou-li $p_1, p_2, \ldots, p_k$ mezi sebou různá prvočísla, mezi nimiž je každé takové prvočíslo, pro které je buďto $\omega(m; p) > 0$, nebo $\omega(n; p) > 0$, platí jednak

$$m = p_1^{\omega(m; p_1)} \cdot p_2^{\omega(m; p_2)} \ldots p_k^{\omega(m; p_k)},$$

jednak (2,9); potom je však také

$$mn = p_1^{\omega(m; p_1) + \omega(n; p_1)} \cdot p_2^{\omega(m; p_2) + \omega(n; p_2)} \ldots p_k^{\omega(m; p_k) + \omega(n; p_k)}.$$

Poznámka 2,6. Z věty 2,7 plyne indukcí, že

$$\omega(n_1 n_2 \ldots n_k; p) = \omega(n_1; p) + \omega(n_2; p) + \ldots + \omega(n_k; p)$$

pro libovolný počet přirozených čísel $n_1, n_2, \ldots, n_k$ a pro libovolné prvočíslo p.

Věta 2,8. *Jsou-li d, n přirozená čísla, je číslo d dělitelem čísla n* (neboli: *číslo n je násobkem čísla d*) *právě tehdy, jestliže $\omega(d; p) \leqq \omega(n; p)$ pro všecka prvočísla p.* To plyne z vět 2,6 a 2,7.

Jsou-li a, b libovolná čísla, nastane právě jeden ze tří případů $a < b$, $a > b$, $a = b$; je-li $a < b$, položíme

$$\min(a, b) = a\,, \quad \max(a, b) = b\,;$$

je-li $a > b$, položíme

$$\min(a, b) = b\,, \quad \max(a, b) = a\,;$$

je-li $a = b$, položíme

$$\min(a, b) = \max(a, b) = a = b\,.$$

Značku min čteme minimum, značku max čteme maximum. Zřejmě

$$\begin{aligned} &\min(a, b) \leqq a \leqq \max(a, b)\,, \\ &\min(a, b) \leqq b \leqq \max(a, b)\,. \end{aligned} \tag{2,10}$$

$$\min(a, b) + \max(a, b) = a + b\,. \tag{2,11}$$

Věta 2,9. *Jsou-li a, b přirozená čísla a je-li*

$$c = \text{nsn}(a, b)\,, \quad d = \text{Nsd}(a, b)\,,$$

je pro každé prvočíslo p

$$\omega(c; p) = \max [\omega(a; p), \omega(b; p)] ,$$
$$\omega(d; p) = \min [\omega(a; p), \omega(b; p)] . \qquad (2,12)$$

To je přímý důsledek definic a věty 2,8.

Poznámka 2,7. Ze (2,11) a (2,12) plyne podle věty 2,7, že $\omega(cd; p) = \omega(ab; p)$ pro každé prvočíslo p, a to je ovšem v souhlase s větou 1,10.

Věta 2,10. *Je-li* n *přirozené číslo a platí-li* (2,9), *je počet všech dělitelů čísla* n *roven*

$$\tau(n) = [\omega(n; p_1) + 1] . [\omega(n; p_2) + 1] \ldots [\omega(n; p_k) + 1] . \qquad (2,13)$$

Důkaz. Podle věty 2,8 dělitelé čísla n jsou právě ta čísla, která lze psát ve tvaru

$$d = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k} , \qquad (2,14)$$

kde $r_1, r_2, \ldots, r_k$ jsou celá čísla, která vyhovují podmínkám

$$0 \leqq r_1 \leqq \omega(n; p_1), \quad 0 \leqq r_2 \leqq \omega(n; p_2), \ldots, 0 \leqq r_k \leqq \omega(n; p_k) . \qquad (2,15)$$

Podle věty 2,5 lze každého dělitele čísla n psát právě jedním způsobem ve tvaru (2,14). Je tedy hledané číslo $\tau(n)$ rovno počtu všech těch k-tic $[r_1, r_2, \ldots, r_k]$ celých čísel, které splňují podmínky (2,15). Protože počet těch celých čísel r, pro něž je $0 \leqq r \leqq n$, je roven číslu $n + 1$, máme $\omega(n, p_1) + 1$ možných hodnot pro r_1, $\omega(n; p_2) + 1$ možných hodnot pro r_2 atd., takže vzorec (2,13) je přímým důsledkem definice násobení podané na str. 19.

Příklad 2,1. Jest $10\,800 = 2^4 . 3^3 . 5^2$, tedy $\tau(10\,800) = (4 + 1) . (3 + 1) . (2 + 1) = 5 . 4 . 3 = 60$.

§ 3. Symboly Σ a Π

Je-li M libovolná množina, pak

$$x \in M \qquad (3,1)$$

znamená, že x je *prvkem* množiny M. Řecké písmeno epsilon, které odpovídá našemu písmenu e, vyskytuje se ve dvou typech: ϵ a ε. Typu ϵ se dnes v matematice užívá takřka výhradně v právě vysvětleném smyslu. V této knize se označení tvaru (3,1) vyskytne jenom zřídka.

Poznámka 3,1. Typu ε se v matematice užívá v různém smyslu, nejčastěji se však označuje písmenem ε kladné číslo, které lze volit libovolně, při čemž však je zájem soustředěn na jeho „malé" možné hodnoty. V takovém smyslu jsme užili písmena ε na četných místech v kap. III.

Jestliže každému prvku x neprázdného konečného souboru M je podle nějakého pravidla přiřazeno určité číslo $a(x)$, potom symbol

$$\sum_{x \in M} a(x) \tag{3,2}$$

znamená součet všech čísel $a(x)$, která dostaneme, dosadíme-li za x postupně jeden po druhém jednotlivé prvky souboru M. Ačkoli pořadí sčítanců není předepsáno, plyne z obecného komutativního zákona sčítání, že (3,2) má zcela určitý číselný význam. Podobně symbol

$$\prod_{x \in M} a(x) \tag{3,3}$$

znamená součin všech čísel $a(x)$, která dostaneme, probíhá-li x daný soubor M. V důsledku obecného komutativního zákona násobení má (3,3) zcela určitý číselný význam.

Je vhodné nevylučovat případ prázdného souboru M. V tomto případě definujeme, že hodnotou symbolu (3,2) je číslo 0 a že hodnotou symbolu (3,3) je číslo 1.

Poznámka 3,2. Řecké písmeno Σ odpovídá našemu písmenu S, řecké písmeno Π našemu písmenu P. Jsou to počáteční písmena slov suma = součet, produkt = součin.

Poznámka 3,3. Je jasné, že ve (3,2) a (3,3) můžeme písmeno x nahradit jakýmkoli jiným písmenem, jenom nesmí zvolené písmeno být už „zadáno", t. j. nesmíme volit písmeno, kterému už před tím byl dán určitý význam. Místo písmena se může vyskytnout také nějaká složitější značka.

V případě (3,2) nazveme x (nebo tu značku, které použijeme místo x) *sumačním indexem*; v případě (3,3) můžeme mluvit o *multiplikačním indexu.*

Poznámka 3,4. Není nikterak nutné, aby pod značkou Σ nebo Π vždy bylo zapsáno $x \in M$. Naopak právě velmi často píšeme jednodušeji

$$\sum_{x} a(x) \quad \text{resp.} \quad \prod_{x} a(x) \quad \text{a pod.},$$

a není-li obavy z nedorozumění, ještě jednodušeji

$$\sum a(x) \text{ resp. } \prod a(x) \text{ a pod.}$$

a slovy vysvětlíme, který je soubor, jehož prvky má probíhat x (nebo ta značka, které použijeme místo x).

Velmi častý je případ, že jsou dána dvě celá čísla m, n a že množina M se skládá z těch celých čísel x, pro něž je $m \leqq x \leqq n$. Místo (3,2) píšeme v tomto případě obyčejně

$$\sum_{x=m}^{n} a(x) \tag{3,4}$$

a místo (3,3)

$$\prod_{x=m}^{n} a(x)\,; \tag{3,5}$$

při tom místo x může být ovšem jakékoli nezadané písmeno. Nejčastěji se vyskytují případy $m = 1$ a $m = 0$. Je na př.

$$\sum_{x=3}^{5} (x^2 - 2x + 3) = 6 + 11 + 18 = 35\,; \quad \prod_{x=3}^{5} (x^2 - 2x + 3) = 6 \,.\, 11 \,.\, 18 = 1188\,;$$

$$\sum_{x=3}^{3} (x^2 - 2x + 3) = \prod_{x=3}^{3} (x^2 - 2x + 3) = 6\,;$$

$$\sum_{x=5}^{3} (x^2 - 2x + 3) = 0\,, \quad \prod_{x=5}^{3} (x^2 - 2x + 3) = 1\,.$$

Obecně pro $m > n$ znamená (3,4) nulu a (3,5) jedničku.

Příklad 3,1. Větu I 8,1 můžeme zapsat ve tvaru

$$\left| \prod_{k=1}^{n} a_k \right| = \prod_{k=1}^{n} |a_k|\,,$$

větu I 9,7 ve tvaru

$$\left| \sum_{k=1}^{n} a_k \right| \leqq \sum_{k=1}^{n} |a_k|\,.$$

Příklad 3,2. Je-li dána číselná matice I (3,15) typu (m, n), jsou její řádkové součty a součiny

$$\sum_{s=1}^{n} a_{rs}\,, \quad \prod_{s=1}^{n} a_{rs} \qquad (1 \leqq r \leqq m)$$

a její sloupcové součty a součiny jsou

$$\sum_{r=1}^{m} a_{rs}\,, \quad \prod_{r=1}^{m} a_{rs} \qquad (1 \leqq s \leqq n)\,.$$

Věta I 3,16 se dá vyjádřit vzorcem

$$\sum_{r=1}^{n}\sum_{s=1}^{n} a_{rs} = \sum_{s=1}^{n}\sum_{r=1}^{m} a_{rs}\,, \tag{3,6}$$

věta I 3,17 vzorcem

$$\prod_{r=1}^{m}\prod_{s=1}^{n} a_{rs} = \prod_{s=1}^{n}\prod_{r=1}^{m} a_{rs}\,. \tag{3,7}$$

Ve (3,6) máme nalevo i napravo t. zv. *dvojnásobné součty*, ve (3,7) *dvojnásobné součiny*. Všimněme si blíže třebas dvojnásobného součtu

$$\sum_{r=1}^{m}\sum_{s=1}^{n} a_{rs}\,, \tag{*}$$

který se vyskytuje na levé straně vzorce (3,6). Zde máme pro každé r $(1 \leqq r \leqq m)$ určitý *vnitřní součet*

$$\alpha_r = \sum_{s=1}^{n} a_{rs}\,,$$

ve kterém index r má danou číselnou hodnotu, kdežto s je sumačním indexem. Index r se stane sumačním indexem ve *vnějším součtu*

$$\sum_{r=1}^{m} \alpha_r\,,$$

jehož hodnota je totožná s hodnotou dvojnásobného součtu (*).

Příklad 3,3. Budiž n dané přirozené číslo. Jestliže čísla $1, 2, \ldots, n$ jsou rozdělena do určitého počtu k skupin $M_1, M_2, \ldots, M_k$ tak, že každé náleží do právě jedné skupiny, a jsou-li $a_1, a_2, \ldots, a_n$ daná čísla, pak podle obecného komutativního a asociativního zákona sčítání je

$$\sum_{x=1}^{n} a_x = \sum_{r=1}^{m}\sum_{s\in M_r} a_s \tag{3,8}$$

a podle obecného komutativního a asociativního zákona násobení je

$$\prod_{x=1}^{n} a_x = \prod_{r=1}^{m}\prod_{s\in M_r} a_s\,. \tag{3,9}$$

Napravo ve (3,8) máme dvojnásobný součet, napravo ve (3,9) dvojnásobný součin. Všimněme si blíže třeba dvojnásobného součtu

$$\sum_{r=1}^{m}\sum_{s\in M_r} a_s\,, \tag{**}$$

který se vyskytuje na pravé straně vzorce (3,8), a porovnejme jej s dvojnásobným součtem (*). V obou případech je sumační index vnějších součtů označen týmž písmenem r, které probíhá v obou případech tytéž hodnoty $1, 2, \ldots, m$. Ve vnitřních součtech je sumační index v obou případech označen týmž písmenem s. Avšak v případě (*) probíhá index s v každém vnitřním součtu stále tytéž hodnoty $1, 2, \ldots, n$, kdežto v případě (**) je tomu jinak: zde hodnoty, které s probíhá v každém jednotlivém vnitřním součtu, tvoří soubor M_r závislý na hodnotě vnějšího indexu r.

Příklad 3,4. Zobecněný distributivní zákon můžeme zapsat ve tvaru

$$\sum_{r=1}^{m} a_r \cdot \sum_{s=1}^{n} b_s = \sum_{r,s} a_r b_s \,, \tag{3,10}$$

kde napravo máme *dvojný součet*. Místo jediného sumačního indexu zde máme dvojici $[r, s]$ sumačních indexů, která probíhá soubor všech takových dvojic celých čísel, pro něž jsou splněny nerovnosti $1 \leqq r \leqq m$, $1 \leqq s \leqq n$. Tento dvojný součet je roven dvojnásobnému součtu

$$\sum_{r=1}^{m} \sum_{s=1}^{n} a_r b_s$$

a také je roven dvojnásobnému součtu

$$\sum_{s=1}^{n} \sum_{r=1}^{m} a_r b_s \,.$$

Příklad 3,5. Nejobecnější distributivní zákon můžeme zapsat ve tvaru

$$\prod_{r=1}^{m} \sum_{s=1}^{n_r} a_{rs} = \sum_{r_1, r_2, \ldots, r_m} a_{1r_1} a_{2r_2} \ldots a_{mr_m} \,,$$

kde součet na pravé straně se vztahuje na všecky takové m-tice $[r_1, r_2, \ldots, r_m]$ přirozených čísel, pro které je

$$r_1 \leqq n_1 \,, \quad r_2 \leqq n_2 \,, \ldots, r_m \leqq n_m \,.$$

Příklad 3,6. Je-li n libovolné přirozené číslo, je $n = \sum_{r=1}^{n} 1$, tedy podle (3,10)

$$n^2 = \sum_{r,s} 1 \,,$$

kde dvojný součet se vztahuje na takové dvojice $[r, s]$ přirozených

čísel, pro které je $r \leqq n$, $s \leqq n$. Sčítance dvojného součtu rozdělíme na skupiny tak, že do téže skupiny dáme ty dvojice $[r, s]$, pro něž má max (r, s) touž hodnotu k. Jest $1 \leqq k \leqq n$ a snadno spočteme, že skupina příslušná číslu k se skládá z $2k - 1$ dvojic. Tedy

$$n^2 = \sum_{k=1}^{n} (2k - 1) ,$$

t. j. *součet prvních n lichých čísel je roven* n^2. Protože

$$\sum_{k=1}^{n} (2k - 1) = 2 . \sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 = 2 . \sum_{k=1}^{n} k - n ,$$

je

$$2 . \sum_{k=1}^{n} k = n^2 + n \ = n(n + 1) ,$$

t. j. *součet prvních n přirozených čísel je roven* $\frac{1}{2}n(n + 1)$.

Příklad 3,7. Přirozené číslo r je dělitelem přirozeného čísla n právě tehdy, jestliže existuje takové přirozené číslo s, že $rs = n$. Tedy je-li $P(n)$ součin všech dělitelů čísla n, je

$$P(n) = \prod_{rs=n} r ,$$

kde součin se vztahuje na ty dvojice přirozených čísel r, s, pro které je $rs = n$. Protože $rs = sr$, je také

$$P(n) = \prod_{rs=n} s ;$$

znásobíme-li obě vyjádření, dostaneme

$$[P(n)]^2 = \prod_{rs=n} n$$

neboli

$$[P(n)]^2 = n^{\tau(n)} .$$

Na př. pro číslo $30 = 2 . 3 . 5$ je $\tau(30) = 8$, dělitelé jsou 1, 2, 3, 5, 6, 10, 15, 30 a jejich součin je

$$P(30) = 810\,000 = 30^4 = 30^{\frac{1}{2}\tau(30)} .$$

Je-li n nezáporné celé číslo, položíme

$$n! = \prod_{k=1}^{n} k , \qquad (3,11)$$

takže $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$ atd. Symbol $n!$ čteme *n faktoriál*. Zřejmě pro každé nezáporné celé n

$$(n + 1)! = n!(n + 1)\,, \tag{3,12}$$

což spolu s rovností $0! = 1$ dává rekurentní definici čísla $n!$.

Pomocí symbolu Π můžeme rozklad přirozeného čísla m na prvočinitele napsat ve tvaru

$$m = \prod_{p} p^{\omega(m;p)},$$

kde napravo p probíhá všecka ta prvočísla p, která jsou děliteli čísla m, a mimo to, chceme-li, ještě konečný počet kterýchkoli jiných prvočísel (viz poznámku 2,5).

Příklad 3,8. Budiž n libovolně dané přirozené číslo. Abychom dostali rozklad čísla $n!$ na prvočinitele, potřebujeme pro každé prvočíslo p najít číslo $\omega(n!; p)$. Z definice (3,11) plyne podle poznámky 2,6, že

$$\omega(n!; p) = \sum_{k=1}^{n} \omega(k; p)\,. \tag{3,13}$$

Avšak pro každé k je p^r dělitelem čísla k právě tehdy, je-li $r \leqq \omega(k; p)$, takže $\omega(k; p)$ je rovno počtu těch přirozených čísel r, pro která p^r je dělitelem čísla k. [Jestliže při daném k není p^r dělitelem čísla k pro žádné přirozené číslo r, je $\omega(k; p) = 0$.] Tedy [viz I (3,13)]

$$\omega(n!; p) = \sum_{[k,r]} 1\,, \tag{3,14}$$

kde $[k, r]$ probíhá ty dvojice přirozených čísel k, r, pro které je $k \leqq n$ a mimo to p^r je dělitelem čísla k. Že platí (3,14), je důsledkem toho, že jestliže napravo seskupíme ty členy, ve kterých k má danou hodnotu, přejde (3,14) ve (3,13). Avšak dvojný součet napravo ve (3,14) můžeme počítat také tak, že seskupíme ty členy, ve kterých r má danou hodnotu. To znamená, že je

$$\omega(n!; p) = \sum_{r} a(r), \tag{3,15}$$

kde $a(r)$ znamená počet těch přirozených čísel $k \leqq n$, která jsou násobky čísla p^r. Součet napravo ve (3,15) se vztahuje na všecka ta přirozená čísla r, pro něž je $a(r) > 0$. Avšak $a(r)$ je počet těch členů posloupnosti

$$p^r, 2p^r, 3p^r, \ldots,$$

které jsou $\leqq n$, t. j. počet těch přirozených čísel x, pro něž platí nerovnost $xp^r \leqq n$ neboli nerovnost $x \leqq \frac{n}{p^r}$, a tento počet je roven celé části čísla $\frac{n}{p^r}$, kterou jsme na str. 121 označili $\left[\frac{n}{p^r}\right]$ nebo $E\left(\frac{n}{p^r}\right)$. Je tedy

$$a(r) = E\left(\frac{n}{p^r}\right),$$

takže (3,15) dá

$$\omega(n!; p) = \sum_r E\left(\frac{n}{p^r}\right), \qquad (3,16)$$

kde součet se vztahuje na ta přirozená čísla r, pro která $p^r \leqq n$; můžeme však připojit i sčítance, pro něž $p^r > n$, neboť pro takové sčítance je $E\left(\frac{n}{p^r}\right) = 0$. Abychom dostali rozklad čísla $n!$ na prvočinitele, stačí ještě uvážit, že číslo $n!$ je dělitelné pouze prvočísly $p \leqq n$. Budiž na př. $n = 10$. Zde jde o prvočísla 2, 3, 5, 7. Jest

$$E\left(\frac{10}{2}\right) = E(5) = 5\,, \quad E\left(\frac{10}{2^2}\right) = E\left(\frac{5}{2}\right) = 2\,,$$

$$E\left(\frac{10}{2^3}\right) = E\left(\frac{5}{4}\right) = 1, \quad E\left(\frac{10}{2^r}\right) = 0 \quad \text{pro } r \geqq 4\,;$$

$$E\left(\frac{10}{3}\right) = 3\,, \quad E\left(\frac{10}{3^2}\right) = 1, \quad E\left(\frac{10}{3^r}\right) = 0 \quad \text{pro } r \geqq 3\,;$$

$$E\left(\frac{10}{5}\right) = 2\,, \quad E\left(\frac{10}{5^r}\right) = 0 \quad \text{pro } r \geqq 2\,;$$

$$E\left(\frac{10}{7}\right) = 1\,, \quad E\left(\frac{10}{7^r}\right) = 0 \quad \text{pro } r \geqq 2\,;$$

$$\omega(10!; 2) = 5 + 2 + 1 = 8\,;$$

$$\omega(10!; 3) = 3 + 1 = 4\,;$$

$$\omega(10!; 5) = 2\,; \quad \omega(10!; 7) = 1\,.$$

Tedy

$$10! = 2^8 \,.\, 3^4 \,.\, 5^2 \,.\, 7\,.$$

Poznámka 3,5. Pro $n = 10$ jsme pro každé prvočíslo p, které je dělitelem čísla $n!$, stanovili jednotlivé sčítance součtu napravo ve (3,16) nezávisle jeden na druhém. Při větších n je však mnohem pohodlnější určovat členy posloupnosti $\left\{E\left(\frac{n}{p^r}\right)\right\}_{r=1}^{\infty}$ rekurentně podle vzorce

$$E\left(\frac{n}{p^{r+1}}\right) = E\left(\frac{E\left(\frac{n}{p^r}\right)}{p}\right), \tag{3,17}$$

který se snadno dokáže. Budiž

$$E\left(\frac{n}{p^r}\right) = \alpha_r, \quad E\left(\frac{n}{p^{r+1}}\right) = \alpha_{r+1}.$$

Podle definice symbolu E je α_r celé číslo takové, že

$$\alpha_r \leqq \frac{n}{p^r} < \alpha_r + 1.$$

Z toho však plyne, že

$$\frac{\alpha_r}{p} \leqq \frac{n}{p^{r+1}} < \frac{\alpha_r + 1}{p}. \tag{3,18}$$

Je-li nyní $\beta_r = E\left(\frac{\alpha_r}{p}\right)$, je β_r takové celé číslo, že

$$\beta_r \leqq \frac{\alpha_r}{p} < \beta_r + 1. \tag{3,19}$$

Pro celá čísla α_r, β_r platí tedy nerovnost

$$\alpha_r < p(\beta_r + 1),$$

ze které podle věty I 9,8 plyne

$$\alpha_r + 1 \leqq p(\beta_r + 1)$$

neboli

$$\frac{\alpha_r + 1}{p} \leqq \beta_r + 1. \tag{3,20}$$

Ze (3,18), (3,19) a (3,20) plyne

$$\beta_r \leqq \frac{n}{p^{r+1}} < \beta_r + 1,$$

takže $\beta_r = E\left(\frac{n}{p^{r+1}}\right) = E\left(\frac{\alpha_r}{p}\right)$, a to je totéž jako (3,17). Budiž na př. $n = 100$. Je třeba vyšetřit všecka prvočísla $p < 100$, vyjmenovaná na str. 144. Z rekurentního vzorce (3,17) vypočteme

$$E\left(\frac{100}{2}\right) = 50\,,\ E\left(\frac{100}{2^2}\right) = E\left(\frac{50}{2}\right) = 25\,,\ E\left(\frac{100}{2^3}\right) = E\left(\frac{25}{2}\right) = 12\,,$$

$$E\left(\frac{100}{2^4}\right) = E\left(\frac{12}{2}\right) = 6\,,\ E\left(\frac{100}{2^5}\right) = E\left(\frac{6}{2}\right) = 3\,,\ E\left(\frac{100}{2^6}\right) =$$

$$= E\left(\frac{3}{2}\right) = 1\,,$$

$$E\left(\frac{100}{2^r}\right) = 0 \quad \text{pro} \quad r \geqq 7\,;$$

$$E\left(\frac{100}{3}\right) = 33\,,\ E\left(\frac{100}{3^2}\right) = E\left(\frac{33}{3}\right) = 11\,,\ E\left(\frac{100}{3^3}\right) = E\left(\frac{11}{3}\right) = 3\,,$$

$$E\left(\frac{100}{3^4}\right) = E\left(\frac{3}{3}\right) = 1\,,\ E\left(\frac{100}{3^r}\right) = 0 \text{ pro } r \geqq 5\,;$$

$$E\left(\frac{100}{5}\right) = 20\,,\ E\left(\frac{100}{5^2}\right) = E\left(\frac{20}{5}\right) = 4\,,\ E\left(\frac{100}{5^r}\right) = 0 \quad \text{pro} \quad r \geqq 3;$$

$$E\left(\frac{100}{7}\right) = 14\,,\ E\left(\frac{100}{7^2}\right) = E\left(\frac{14}{7}\right) = 2\,,\ E\left(\frac{100}{7^r}\right) = 0 \quad \text{pro} \quad r \geqq 3\,.$$

Pro $p > 7$, tedy $p \geqq 11$, je $p^2 > 100$, tedy $E\left(\frac{100}{p^r}\right) = 0$ pro $r \geqq 2$. Mimo to je

$$E\left(\frac{100}{11}\right) = 9\,,\ E\left(\frac{100}{13}\right) = 7\,,\ E\left(\frac{100}{17}\right) = 5\,,$$

$$E\left(\frac{100}{19}\right) = 5\,,\ E\left(\frac{100}{23}\right) = 4\,,\ E\left(\frac{100}{29}\right) = 3\,,\ E\left(\frac{100}{31}\right) = 3\,,$$

$$E\left(\frac{100}{37}\right) = 2\,,\ E\left(\frac{100}{41}\right) = 2\,,\ E\left(\frac{100}{43}\right) = 2\,,\ E\left(\frac{100}{47}\right) = 2.$$

Pro ostatní prvočísla $p < 100$ je $E\left(\frac{100}{p}\right) = 1$.

Podle (3,16) je

$$\omega(100!;\,2) = 50 + 25 + 12 + 6 + 3 + 1 = 97,$$
$$\omega(100!;\,3) = 33 + 11 + 3 + 1 = 48,$$
$$\omega(100!;\,5) = 20 + 4 = 24,$$
$$\omega(100!;\,7) = 14 + 2 = 16$$

a pro $11 \leqq p < 100$ je $\omega(100!;\,p) = E\left(\frac{100}{p}\right)$.

Tedy

$$100! = 2^{97} \cdot 3^{48} \cdot 5^{24} \cdot 7^{16} \cdot 11^{9} \cdot 13^{7} \cdot 17^{5} \cdot 19^{5} \cdot 23^{4} \cdot 29^{3} \cdot$$
$$\cdot 31^{3} \cdot 37^{2} \cdot 41^{2} \cdot 43^{2} \cdot 47^{2} \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot$$
$$\cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 .$$

Je-li n podstatně větší než 100, je velmi mnoho prvočísel menších než n, která se vesměs vyskytují v rozkladu na prvočinitele čísla $n!$, takže tento rozklad je složitý. Přes to je snadné i pro n mnohem větší než 100 stanovit pro každé jednotlivé prvočíslo $p \leqq n$, v jaké mocnině se vyskytuje toto prvočíslo v rozkladu čísla $n!$ na prvočinitele. Budiž na př. $n = 2100$, $p = 7$. Jest

$$E\left(\frac{2100}{7}\right) = 300\,,\; E\left(\frac{2100}{7^2}\right) = E\left(\frac{300}{7}\right) = 42\,,$$

$$E\left(\frac{2100}{7^3}\right) = E\left(\frac{42}{7}\right) = 6\,,\; E\left(\frac{2100}{7^r}\right) = 0 \quad \text{pro } r \geqq 4\,,$$

$$300 + 42 + 6 = 348\,,$$

takže prvočíslo 7 se vyskytuje v rozkladu čísla 2100! na prvočinitele v mocnině 7^{348}.

§ 4. Počet uspořádání konečné množiny

Už v I § 1 (str. 10) jsme poznamenali, že nalezení počtu prvků konečné množiny mnohdy vyžaduje použití početních výkonů a jejich vlastností. V tomto a v následujícím paragrafu probereme některé případy tohoto druhu, důležité pro mnohé matematické úvahy.

Nejprve se budeme zabývat vyšetřením počtu všech možných uspořádání neprázdného konečného souboru, který označíme M_n,

kde n značí počet jeho prvků. Je patrné, že počet všech uspořádání závisí pouze na čísle n; označíme jej P_n. Tedy číslo P_n udává, kolika způsoby lze zapsat jeden po druhém všecky prvky souboru M_n tak, aby každý prvek byl zapsán právě jednou. Soubor M_2 o dvou prvcích a, b lze zřejmě uspořádat dvěma způsoby ab, ba, takže $P_2 = 2$. Je-li M_3 soubor o třech prvcích a, b, c, rozdělíme všecka jeho uspořádání na skupiny tak, že do první skupiny přijdou ta uspořádání, která začínají prvkem a, do další ta, která začínají prvkem b, do poslední ta, která začínají prvkem c; celkem máme tři skupiny po dvou uspořádáních, takže $P_3 = 3 \,.\, 2 = 6$. Všech 6 uspořádání souboru M_3 je

$$abc,\ acb;\ bac,\ bca;\ cab,\ cba;$$

jednotlivé skupiny jsme oddělili středníky. Přejděme k souboru M_4 čtyř prvků a, b, c, d, jehož uspořádání rozdělíme na čtyři skupiny podle toho, zda prvním prvkem je a, b, c či d. Máme 4 skupiny po 6 uspořádáních, takže $P_4 = 4 \,.\, 6 = 24$. Všech 24 uspořádání souboru M_4 je

$$\begin{aligned} &abcd,\ abdc;\ acbd,\ acdb;\ adbc,\ adcb;\\ &bacd,\ badc;\ bcad,\ bcda;\ bdac,\ bdca;\\ &cabd,\ cadb;\ cbad,\ cbda;\ cdab,\ cdba;\\ &dabc,\ dacb;\ dbac,\ dbca;\ dcab,\ dcba. \end{aligned}$$

Každá skupina vyplnila jeden řádek. Obecně můžeme pro každé n rozdělit všech P_{n+1} uspořádání souboru M_{n+1} o $n + 1$ prvcích na $n + 1$ skupin podle toho, který prvek je prvním; v každé skupině máme P_n uspořádání, takže

$$P_{n+1} = (n + 1)\, P_n \,. \tag{4,1}$$

Z toho plyne, že pro všecka přirozená čísla n je [viz (3,11)]

$$P_n = n! \,. \tag{4,2}$$

Neboť vzorec (4,2) je zřejmý pro $n = 1$ a ze správnosti vzorce (4,2) při určitém n plyne podle (4,1) a (3,12), že $P_{n+1} = (n + 1) \,.\, n! = (n + 1)!$, čímž je obecná správnost vzorce (4,2) dokázána indukcí.

Předcházející úvahy můžeme zobecnit. Budiž dáno přirozené číslo n a mimo to budiž dán konečný soubor M_k složený z k prvků, které označíme

$$\alpha_1, \alpha_2, \ldots, \alpha_k \,; \tag{4,3}$$

při tom může být $k = n$, $k > n$, $k < n$. Každému z prvků (4,3) přiřaďme určité nezáporné celé číslo; tato čísla označme

$$r_1, r_2, \ldots, r_k ; \tag{4,4}$$

obecně tedy pro $1 \leqq s \leqq k$ je prvku α_s přiřazeno číslo r_s. Budeme se zajímat o takové n-tice

$$[a_1, a_2, \ldots, a_n] , \tag{4,5}$$

jejichž každý člen je prvkem souboru M_k, při čemž počet těch členů n-tice (4,5), které jsou rovny určitému prvku (4,3), je dán číslem (4,4) tomuto prvku přiřazeným. Je tedy v každé z uvažovaných n-tic r_1 členů rovných α_1, r_2 členů rovných α_2 atd., a protože všech členů ve (4,5) je n, musí být

$$\sum_{s=1}^{k} r_s = n . \tag{4,6}$$

Dokážeme, že počet všech takových n-tic je dán číslem

$$P_n^{(r_1, \ldots, r_k)} = \frac{n!}{r_1!\, r_2! \ldots r_k!} . \tag{4,7}$$

Poznámka 4,1. Jestliže všecka čísla (4,4) jsou rovna jedné, takže podle (4,6) je $k = n$, jsou uvažované n-tice totožné se všemi možnými uspořádáními souboru M_n, takže jejich počet je dán číslem (4,2). To souhlasí se vzorcem (4,7), neboť $1! = 1$.

Poznámka 4,2. Jestliže některé z čísel (4,4) je rovné nule, znamená to, že příslušný prvek (4,3) se vůbec nevyskytne mezi členy n-tice (4,5). Protože pořadí, ve kterém jsou prvky souboru M_k zapsány ve (4,3), můžeme libovolně zvolit, můžeme předpokládat, že je

$$r_s > 0 \quad \text{pro} \quad 1 \leqq s \leqq h ,$$
$$r_s = 0 \quad \text{pro} \quad h + 1 \leqq s \leqq k .$$

Označme M_h' soubor prvků

$$\alpha_1, \alpha_2, \ldots, \alpha_h$$

neboli soubor, který vznikne ze souboru M_k vynecháním těch prvků α_s, pro které je $r_s = 0$. Jinak řečeno, M_h' je soubor všech těch prvků, které se skutečně vyskytnou jako členy uvažovaných n-tic (4,5). Při přechodu od souboru M_k k souboru M_h' máme místo (4,6)

$$\sum_{s=1}^{h} r_s = n , \tag{4,6'}$$

což se liší jenom formálně od (4,6), neboť součet nalevo ve (4,6′) vznikne ze součtu nalevo ve (4,6) vynecháním sčítanců rovných nule, které (viz větu I 3,5) je bez vlivu na hodnotu součtu. Místo (4,7) máme při přechodu k M'_h

$$P_n^{(r_1, \ldots, r_h)} = \frac{n!}{r_1!\, r_2! \ldots r_h!} \qquad (4,7')$$

a to se opět liší jenom formálně od (4,7), neboť jelikož $0! = 1$, liší se součin ve jmenovateli ve (4,7′) od příslušného součinu ve (4,7) pouze vynecháním činitelů rovných jedné, a to (viz větu I 3,8) je bez vlivu na hodnotu součinu. Z toho všeho je patrné, že důkaz vzorce (4,7) stačí provést za předpokladu, že všecka čísla (4,4) jsou přirozená čísla. Poznamenejme, že potom podle (4,6) je nutně $k \geqq n$; přitom skutečně novým je pouze případ $k > n$, neboť pro $k = 1$ jsou všecka čísla (4,4) rovna jedné a vzorec (4,7) se redukuje (viz poznámku 4,1) na dokázaný už vzorec (4,2).

Než přejdeme k obecnému důkazu vzorce (4,7), probereme dva jednoduché příklady, ve kterých se neomezíme na stanovení *počtu* všech uvažovaných n-tic, nýbrž skutečně všecky ty n-tice jednu po druhé vyjmenujeme.

Příklad 4,1. Budiž $k = 2$, $r_1 = 2$, $r_2 = 2$, tedy $n = r_1 + r_2 = 4$. Prvky množiny $M_k = M_2$ označíme a, b. Jde tedy o takové čtveřice

$$[a_1, a_2, a_3, a_4], \quad \text{krátce} \quad a_1a_2a_3a_4,$$

ve kterých každý člen je buďto roven a, nebo je roven b, při čemž máme právě dva členy rovné a a právě dva členy rovné b. Rozdělíme uvažované čtveřice na dvě skupiny podle toho, zda *prvním* prvkem je a či b a každou z obou skupin rozdělíme na dvě menší „skupinky" podle toho, zda *druhým* prvkem je a či b; v každé skupince je buďto jediná čtveřice, nebo dvě. Všecky naše čtveřice jsou

$$aabb;\ abab,\ abba;$$
$$baab,\ baba;\ bbaa.$$

Každá skupina zaujímá jeden řádek a skupinky v každém z obou řádků jsou od sebe odděleny středníkem. Celkový počet čtveřic je

$$6 = \frac{24}{2 \cdot 2} = \frac{4!}{2!\, 2!},$$

a to je v souhlase s obecným vzorcem (4,7).

Příklad 4,2. Budiž $k = 3$, $r_1 = 3$, $r_2 = 2$, $r_3 = 1$, tedy $n = r_1 +$

$+ r_2 + r_3 = 6$. Prvky množiny $M_k = M_3$ označíme a, b, c. Jde tedy o takové šestice

$$[a_1, a_2, a_3, a_4, a_5, a_6], \text{ krátce } a_1a_2a_3a_4a_5a_6 ,$$

ve kterých každý člen je roven některému ze tří prvků a, b, c, při čemž máme právě tři členy rovné a, právě dva členy rovné b, právě jeden člen rovný c. Rozdělíme uvažované šestice na tři skupiny podle toho, zda *prvním* prvkem je a, b či c; každou skupinu rozdělíme na menší „skupinky" podle toho, čemu se rovná *druhý* prvek šestice. (Každá skupina se dělí buďto na tři, nebo na dvě skupinky, neboť jestliže prvním prvkem je a nebo b, je druhým kterýkoli ze tří prvků a, b, c, je-li však první prvek roven c, je druhý buďto roven a, nebo b.) Každou skupinku rozdělíme ještě na „skupinečky" podle hodnoty *třetího* prvku šestice. (Počet skupineček ve skupince je roven dvěma nebo třem.) Všecky naše šestice jsou

$$\left\{\begin{array}{l} aaabbc,\ aaabcb,\ aaacbb;\ aababc,\ aabacb,\ aabbac,\ aabbca,\ aabcab, \\ aabcba;\ aacabb,\ aacbab,\ aacbba \mid abaabc,\ abaacb,\ ababac,\ ababca, \\ abacab,\ abacba;\ abbaac,\ abbaca,\ abbcaa;\ abcaab,\ abcaba,\ abcbaa \mid \\ acaabb,\ acabab,\ acabba;\ acbaab,\ acbaba,\ acbbaa \end{array}\right.$$

$$\left\{\begin{array}{l} baaabc,\ baaacb,\ baabac,\ baabca,\ baacab,\ baacba; \\ babaac,\ babaca,\ babcaa;\ bacaab,\ bacaba,\ bacbaa \mid \\ bbaaac,\ bbaaca,\ bbacaa;\ bbcaaa \mid bcaaab,\ bcaaba,\ bcabaa;\ bcbaaa \end{array}\right.$$

$$\left\{\begin{array}{l} caaabb,\ caabab,\ caabba;\ cabaab,\ cababa,\ cabbaa \mid \\ cbaaab,\ cbaaba,\ cbabaa;\ cbbaaa. \end{array}\right.$$

Při tom jsou od sebe odděleny jednotlivé skupiny svorkou {, skupinky svislou čarou |, skupinečky středníkem. Celkový počet všech šestic je roven

$$60 = \frac{720}{12} = \frac{6!}{3!\,2!\,1!}$$

a to je v souhlase s obecným vzorcem (4,7).

Přistupme k obecnému důkazu vzorce (4,7). Podle poznámky 4,2 můžeme předpokládat, že všecka čísla (4,4) jsou kladná neboli že každý z k prvků (4,3) se skutečně vyskytuje mezi prvky každé z uvažovaných n-tic (4,5). Zvolme nové prvky

$$\begin{array}{l} \alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r_1}, \\ \alpha_{21}, \alpha_{22}, \ldots, \alpha_{2r_2}, \\ \ldots\ldots\ldots\ldots \\ \alpha_{k1}, \alpha_{k2}, \ldots, \alpha_{kr_k} \end{array} \qquad (4,8)$$

tak, aby všecky tyto prvky byly navzájem různé. Počet všech prvků (4,8) je podle (4,4) roven n. Soubor všech n prvků (4,8) označme M_n^*. Je nám známo, že počet všech možných uspořádání M_n^* je roven číslu $n!$. To znamená, že $n!$ je počet všech těch n-tic (4,5), jejichž členy jsou rovny prvkům (4,8) souboru M_n^*, při čemž každý prvek souboru M_n^* je roven právě jednomu členu n-tice. Avšak z takových n-tic vzniknou ty n-tice, o jejichž počet x se zajímáme, tím, že pro $1 \leqq s \leqq k$ nahradíme každý z r_s prvků

$$\alpha_{s1}, \alpha_{s2}, \ldots, \alpha_{sr_s}$$

souboru M_n^* prvkem α_s původního souboru M_k. Dokážeme-li, že takovou náhradou vznikne každá z původních x n-tic celkem z $r_1!\,.\,r_2!\ldots r_k!$ nových n-tic, bude zjištěno, že

$$x\,.\,r_1!\,r_2!\ldots r_k! = n!\,,$$

t. j., bude proveden důkaz vzorce (4,7). Nyní každá nová n-tice N obsahuje v určitém pořadí všech n prvků a původní n-tice vznikne z N tím, že každý z prvků (4,8) nahradíme příslušným prvkem (4,3); při tom všecky prvky téhož řádku jsou nahrazeny jedním a týmž prvkem, ale prvky různých řádků jsou nahrazeny různými prvky. Jde tedy jenom o to, zjistit, že součin

$$r_1!\,r_2!\ldots r_k! \tag{4,9}$$

vyjadřuje počet těch n-tic (včetně n-tice N samé), které se liší od n-tice N pouze takovými změnami pořadí prvků (4,8), při kterém prvky každého jednotlivého řádku se pouze vyměňují mezi sebou. Ale prvky prvního řádku lze mezi sebou vyměnit $r_1!$ způsoby, prvky druhého řádku $r_2!$ způsoby atd., takže je přímým důsledkem definice součinu vyslovené v I § 3, že současná výměna je proveditelná (4,9) způsoby.

Poznámka 4,3. Levá strana vzorce (4,7) je podle svého významu celým číslem, takže totéž platí i o pravé straně. To znamená, že jsou-li n; $r_1, \ldots, r_k$ přirozená čísla taková, že platí (4,6), je číslo $n!$ dělitelné součinem $r_1!\,r_2!\ldots r_k!$. Při tom předpoklad (4,6) můžeme nahradit obecnějším předpokladem

$$\sum_{s=1}^{k} r_s \leqq n\,, \tag{4,10}$$

neboť platí-li (4,10), existuje takové nezáporné celé číslo r_{k+1}, že

$$\sum_{s=1}^{k+1} r_s = n\,;$$

pak podle předcházejícího výkladu je číslo $n!$ dělitelné součinem $r_1!\, r_2! \ldots r_{k+1}!$, který opět je dělitelný součinem $r_1!\, r_2! \ldots r_k!$, a tímto součinem je tedy podle věty 1,8 dělitelné také číslo $n!$. Výsledek, ke kterému jsme dospěli, t. j. že za předpokladu (4,10) je číslo $n!$ dělitelné součinem $r_1!\, r_2! \ldots, r_k!$, můžeme také odvodit přímo. Podle věty 2,8 a poznámky 2,6 stačí odvodit, že pro každé prvočíslo p je

$$\omega(n!;\, p) \geqq \sum_{s=1}^{k} \omega(r_s!;\, p)\,. \tag{4,11}$$

Avšak podle (3,16) je

$$\omega(n!;\, p) = \sum_{h} E\left(\frac{n}{p^h}\right), \tag{4,12}$$

$$\omega(r_s!;\, p) = \sum_{h} E\left(\frac{r_s}{p^h}\right) \quad \text{pro} \quad 1 \leqq s \leqq k\,,$$

kde každý ze součtů $\sum_h$ se vztahuje na všecka ta přirozená čísla h, pro která příslušné z čísel

$$E\left(\frac{n}{p^h}\right), \quad E\left(\frac{r_s}{p^h}\right) \qquad (1 \leqq s \leqq k) \tag{4,13}$$

je větší než nula; je však ovšem možné připojit další sčítance rovné nule, takže můžeme předpokládat, že sumační index h probíhá ve všech součtech (4,12) tytéž hodnoty; budou to ta přirozená čísla h, pro která aspoň jedno z čísel (4,13) je větší než nula, a chceme-li, ještě některé jiné hodnoty. Stačí tedy zjistit, že pro každé přirozené číslo h platí nerovnost

$$E\left(\frac{n}{p^h}\right) \geqq \sum_{s=1}^{k} E\left(\frac{r_s}{p^h}\right), \tag{4,14}$$

neboť sečtením takových nerovností, odpovídajících různým hodnotám čísla h, dostaneme podle (4,12) žádanou nerovnost (4,11). Zřejmě je však pro každé s a každé h

$$\frac{r_s}{p^h} \geqq E\left(\frac{r_s}{p^h}\right),$$

tedy též

$$\sum_{s=1}^{k} \frac{r_s}{p^h} \geqq \sum_{s=1}^{k} E\left(\frac{r_s}{p^h}\right).$$

Podle (4,10) je však

$$\frac{n}{p^h} \geqq \frac{\sum_{s=1}^{k} r_s}{p^h} = \sum_{s=1}^{k} \frac{r_s}{p^h},$$

takže

$$\frac{n}{p^h} \geq \sum_{s=1}^{k} E\left(\frac{r_s}{p^h}\right). \tag{4,15}$$

Na pravé straně nerovnosti (4,15) máme *celé číslo* a ze všech celých čísel x, pro která platí

$$\frac{n}{p^h} \geqq x,$$

je největší číslo $E\left(\frac{n}{p^h}\right)$, takže ze (4.15) plyne (4,14).

§ 5. Variace a kombinace

Úvahy provedené v § 4 můžeme zobecnit. Budiž dán neprázdný konečný soubor M_n složený z n prvků a budiž dáno přirozené číslo $m \leqq n$. Nazveme *variací m-té třídy* souboru M_n každou m-tici, složenou z navzájem různých prvků množiny M_n. Zřejmě počet všech variací m-té třídy souboru M_n závisí pouze na číslech m, n; označíme jej V_n^m. Tedy číslo V_n^m udává, kolika způsoby lze v určitém pořadí zapsat m různých prvků libovolně vybraných ze souboru M_n. Je-li $m = n$, je jasné, že variace n-té třídy souboru M_n není nic jiného než uspořádání souboru M_n, takže $V_n^n = P_n$.

Budiž na př. M_5 soubor pěti prvků a, b, c, d, e. Variace druhé třídy souboru M_5 rozdělíme na skupiny podle toho, kterým z prvků a, b, c, d, e začínají; celkem je pět skupin a je jasné, že v každé skupině jsou čtyři variace druhé třídy, takže $V_5^2 = 5 \cdot 4 = 20$. Všech dvacet variací druhé třídy souboru M_5 je

$$ab,\ ac,\ ad,\ ae;\ ba,\ bc,\ bd,\ be;\ ca,\ cb,\ cd,\ ce;$$
$$da,\ db,\ dc,\ de;\ ea,\ eb,\ ec,\ ed.$$

Jednotlivé skupiny jsme oddělili středníky. Všimněme si ještě variací třetí třídy našeho souboru M_5. Opět je rozdělíme na skupiny podle prvního prvku a každou skupinu ještě na menší skupinky podle druhého prvku. Je celkem 5 skupin, z nichž každá se rozpadá na 4 skupinky po třech variacích. Všech $V_5^3 = 5 \cdot 4 \cdot 3 = 60$ variací třetí třídy souboru M_5 je

abc, *abd*, *abe*; *acb*, *acd*, *ace*; *adb*, *adc*, *ade*; *aeb*, *aec*, *aed*;
bac, *bad*, *bae*; *bca*, *bcd*, *bce*; *bda*, *bdc*, *bde*; *bea*, *bec*, *bed*;
cab, *cad*, *cae*; *cba*, *cbd*, *cbe*; *cda*, *cdb*, *cde*; *cea*, *ceb*, *ced*;
dab, *dac*, *dae*; *dba*, *dbc*, *dbe*; *dca*, *dcb*, *dce*; *dea*, *deb*, *dec*;
eab, *eac*, *ead*; *eba*, *ebc*, *ebd*; *eca*, *ecb*, *ecd*; *eda*, *edb*, *edc*.

Obecněji pro každé $n \geqq 2$ můžeme variace druhé třídy souboru M_n rozdělit na n skupin podle prvního prvku, takže v každé skupině je $n - 1$ variací, tedy $V_n^2 = n(n-1)$; podobně pro každé $n \geqq 3$ můžeme variace třetí třídy souboru M_n rozdělit na n skupin podle prvního prvku a každou z těchto skupin na $n - 1$ menších skupin podle druhého prvku; potom je v každé menší skupině $n - 2$ prvků, v každé větší skupině je $(n-1)(n-2)$ prvků a celkem máme $V_n^3 = n(n-1)(n-2)$. Dokážeme, že obecně pro $n \geqq m$ je počet V_n^m všech variací m-té třídy souboru M_n o n prvcích roven součinu m činitelů, z nichž první je roven n a každý následující činitel je o 1 menší než předcházející, tedy

$$V_n^m = n(n-1)\ldots(n-m+1) = \prod_{r=0}^{m-1}(n-r)\,. \qquad (5,1)$$

Důkaz vzorce (5,1) můžeme provést indukcí vzhledem k m. Pro $m = 1$ praví vzorec (5,1) prostě, že $V_n^1 = n$, což je nám známo. Nechť vzorec (5,1) je při určitém m už dokázán pro všecka $n \geqq m$ a nechť n je přirozené číslo, pro které platí nerovnost $n \geqq m + 1$. Rozdělme všecky variace $(m+1)$-ní třídy souboru M_n na n skupin podle prvního prvku. Je jasné, že každou variaci $(m+1)$-ní třídy určité skupiny dostaneme, jestliže ke společnému prvnímu prvku připojíme variaci m-té třídy toho souboru o $n - 1$ prvcích, který vznikne z M_{n-1} odstraněním prvního prvku; z toho plyne, že v každé skupině je V_{n-1}^m variací $(m+1)$-ní třídy, a jelikož máme n skupin, je celkem

$$V_n^{m+1} = n \,.\, V_{n-1}^m\,.$$

Podle předpokladu však platí vzorec (5,1), i když v něm číslo n nahradíme číslem $n - 1$; je tedy

$$V_{n-1}^m = \prod_{r=0}^{m-1}(n-1-r) \quad \text{neboli} \quad V_{n-1}^m = \prod_{r=1}^{m}(n-r)\,,$$

takže

$$V_n^{m+1} = n \,.\, V_{n-1}^m = n \,.\, \prod_{r=1}^{m}(n-r) = \prod_{r=0}^{m}(n-r)\,,$$

a to jsme měli dokázat.

Vzorec (5,1) můžeme dokázat také jinak. Všimli jsme si už, že $V_n^n = P_n$, takže v případě $m = n$ vzorec (5,1) plyne ze (4,2). Budiž tedy $m < n$. Každá variace třídy m množiny M_n se skládá z m prvků množiny M_n, vzatých v určitém pořadí; jestliže k těmto m prvkům připojíme zbývajících $n - m$ prvků množiny M_n ve kterémkoli z $(n - m)!$ možných pořadí, dostaneme jedno z $n!$ možných uspořádání množiny M_n a obráceně z každého uspořádání množiny M_n vznikne škrtnutím posledních $n - m$ prvků určitá variace třídy m množiny M_n. Z toho plyne, že $n! = (n - m)!\, V_n^m$; je tedy

$$V_n^m = \frac{n!}{(n-m)!} = \frac{n(n-1)\dots 1}{(n-m)(n-m+1)\dots 1} \tag{5,2}$$

a krácením dostaneme (5,1).

Budiž opět dán neprázdný konečný soubor M_n složený z n prvků a přirozené číslo $m \leqq n$. Nazveme *kombinací m-té třídy* souboru M_n každou část souboru M_n obsahující m prvků. Počet všech kombinací m-té třídy závisí pouze na číslech m, n; označme jej C_n^m. Rozdíl mezi pojmy kombinace a variace je v tom, že u variace záleží na pořadí m prvků, kdežto u kombinace na pořadí nezáleží. Jedna a táž kombinace třídy m dává tedy vznik $m!$ variacím třídy m, které vzniknou, jestliže prvky, ze kterých se kombinace skládá, píšeme jeden po druhém v kterémkoli z $m!$ možných pořadí. Z toho plyne, že je mezi počtem kombinací C_n^m a počtem variací V_n^m vztah

$$m!\, C_n^m = V_n^m .$$

Je tedy podle vzorce (5,1)

$$C_n^m = \frac{n(n-1)\dots(n-m+1)}{m!} \tag{5,3}$$

a podle vzorce (5,2) je

$$C_n^m = \frac{n!}{m!\,(n-m)!} . \tag{5,4}$$

Vzorec (5,3) vznikne ze vzorce (5,4) krácením.

Vzorec (5,4) můžeme odvodit také jinak. Výraz na pravé straně v (5,4) je totiž zvláštním případem $k = 2$ výrazu (4,7), ve kterém jsme měli podmínku (4,6), jež je zde splněna, neboť $m + (n - m) = n$. Podle známého nám významu výrazu (4,7) znamená tedy pravá strana počet takových n-tic

$$[a_1, a_2, \dots, a_n] , \tag{5,5}$$

ve kterých je m členů rovných jedné a $n - m$ členů rovných nule. (Místo čísel 1 a 0 jsme mohli zvolit kterékoli dvě navzájem různé věci.) K důkazu vzorce (5,4) je tedy pouze třeba zjistit, že počet právě popsaných n-tic je roven počtu kombinací třídy m libovolně zvoleného souboru M_n o n prvcích. To je snadné; jsou-li

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

prvky souboru M_n v libovolně zvoleném určitém pořadí a je-li (5,5) n-tice, jejíž každý člen je roven jednomu z čísel 1 a 0, přiřaďme n-tici (5,5) tu kombinaci třídy m souboru M_n, která se skládá z těch α_s ($1 \leqq s \leqq n$), pro něž je $a_s = 1$. Je patrné, že každá kombinace třídy m souboru M_n vznikne tímto způsobem z právě jedné n-tice (5,5), takže počet všech takových kombinací je roven počtu všech n-tic (5,5), a to jsme chtěli dokázat.

Výraz na pravé straně v (5,4) má smysl i pro $m = 0$ a dává

$$C_n^0 = 1$$

v souhlase s tím, že M_n má právě jednu část obsahující 0 prvků (prázdnou množinu).

Výrazy C_n^m, kde m, n jsou celá čísla, $0 \leqq m \leqq n$, nazývají se (z důvodu, který poznáme na str. 172) *binomické koeficienty* a vyskytují se ve velmi mnoha matematických vzorcích. Označení C_n^m pro binomické koeficienty je dosti časté ve světové literatuře, u nás se však odedávna užívá místo C_n^m označení $\binom{n}{m}$ [čteme n nad m], kterého i my budeme zpravidla užívat. Je tedy pro $1 \leqq m \leqq n$

$$\binom{n}{m} = \frac{n(n-1)\ldots(n-m+1)}{m!} \tag{5,3'}$$

a pro $0 \leqq m \leqq n$

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!}\,. \tag{5,4'}$$

Binomické koeficienty mají řadu zajímavých vlastností, jež však v této knize nebudeme probírat. Uveďme pouze, že pro $0 \leqq m \leqq n$ je podle (5,4)

$$C_n^m = C_n^{n-m} \quad \text{neboli} \quad \binom{n}{m} = \binom{n}{n-m}. \tag{5,6}$$

Vzorec (5,6) praví, že soubor M_n má týž počet kombinací třídy m jako třídy $n - m$; to je patrné z toho, že z každé kombinace třídy

m dostaneme kombinaci třídy $n - m$, do které patří ty prvky souboru M_n, které nepatří do uvažované kombinace třídy m.

Variace a kombinace, o kterých jsme dosud mluvili, jmenují se určitěji variace a kombinace *bez opakování* na rozdíl od *variací a kombinací s opakováním*, o kterých si nyní promluvíme. Budiž opět M_n konečný soubor n prvků a mimo to budiž dáno přirozené číslo m, při čemž tentokrát může být $m = n$, $m < n$, $m > n$. Nazveme *variací s opakováním třídy m* souboru M_n každou m-tici

$$[a_1, a_2, \ldots, a_n],$$

jejíž všecky členy jsou prvky souboru M_n, při čemž některý prvek množiny M_n se může rovnat i několika členům m-tice. Na př. soubor 4 prvků a, b, c, d má tyto variace třídy 3 s opakováním:

$$\left.\begin{array}{l} aaa,\ aab,\ aac,\ aad,\ aba,\ abb,\ abc,\ abd,\ aca,\ acb,\ acc,\ acd,\\ ada,\ adb,\ adc,\ add,\ baa,\ bab,\ bac,\ bad,\ bba,\ bbb,\ bbc,\ bbd,\\ bca,\ bcb,\ bcc,\ bcd,\ bda,\ bdb,\ bdc,\ bdd,\ caa,\ cab,\ cac,\ cad,\\ cba,\ cbb,\ cbc,\ cbd,\ cca,\ ccb,\ ccc,\ ccd,\ cda,\ cdb,\ cdc,\ cdd,\\ daa,\ dab,\ dac,\ dad,\ dba,\ dbb,\ dbc,\ dbd,\ dca,\ dcb,\ dcc,\ dcd,\\ dda,\ ddb,\ ddc,\ ddd. \end{array}\right\} \quad (5,7)$$

Z definice obecného součinu (I § 3) a z definice mocniny s přirozeným exponentem (I § 6) plyne přímo, že počet variací s opakováním třídy m souboru n prvků je roven n^m; v případě (5,7) je to $4^3 = 64$. Důležitější než variace s opakováním jsou kombinace s opakováním; k pojmu *kombinace s opakováním třídy m* dospějeme od pojmu variace s opakováním třídy m, jestliže nepřihlížíme k pořadí prvků, ze kterých se variace skládá. Tedy 64 variacím s opakováním třídy 3 souboru a, b, c, d odpovídají kombinace s opakováním třídy 3 téhož souboru:

$$\begin{array}{l} aaa,\ aab,\ aac,\ aad,\ abb,\ abc,\ abd,\ acc,\ acd,\ add, \\ bbb,\ bbc,\ bbd,\ bcc,\ bcd,\ bdd,\ ccc,\ ccd,\ cdd,\ ddd; \end{array} \quad (5,8)$$

je jich 20. Počet kombinací s opakováním se nedá odvodit z počtu variací s opakováním, je však možné, jak uvidíme, odvodit vzorec pro počet kombinací s opakováním ze známého nám vzorce pro počet kombinací bez opakování. Dokážeme, že počet kombinací s opakováním třídy m souboru M_n o n prvcích je roven číslu [viz (5,6)]

$$C^m_{n+m-1} = C^{n-1}_{n+m-1} \quad (5,9)$$

neboli

$$\binom{n+m-1}{m} = \binom{n+m-1}{n-1}; \quad (5,9')$$

pro $n = 4$, $m = 3$ je tento počet roven $\binom{6}{3} = \frac{6 \cdot 5 \cdot 4}{3!} = 5 \cdot 4 = 20$ [viz (4,8)].

Abychom dokázali vzorec (5,9), označme

$$\alpha_1, \alpha_2, \ldots, \alpha_n \tag{5,10}$$

prvky souboru M_n. Kombinace s opakováním třídy m souboru M_n je určena, známe-li čísla

$$r_1, r_2, \ldots, r_n , \tag{5,11}$$

která udávají, kolikrát se který z prvků (5,10) vyskytne v uvažované kombinaci. Čísla (5,11) jsou nezáporná celá čísla vyhovující podmínce

$$r_1 + r_2 + \ldots + r_n = m , \tag{5,12}$$

jinak však libovolná. Položme

$$s_1 = r_1;\ s_2 = r_1 + r_2;\ \ldots;\ s_n = r_1 + r_2 + \ldots + r_n . \tag{5,13}$$

Potom jsou

$$s_1, s_2, \ldots, s_n \tag{5,14}$$

nezáporná celá čísla vyhovující podmínkám

$$s_1 \leqq s_2 \leqq \ldots \leqq s_n = m . \tag{5,15}$$

Dále položme

$$t_1 = s_1 + 1;\ t_2 = s_2 + 2;\ \ldots;\ t_n = s_n + n . \tag{5,16}$$

Potom jsou

$$t_1, t_2, \ldots, t_n \tag{5,17}$$

přirozená čísla vyhovující podmínkám

$$t_1 < t_2 < \ldots < t_n = n + m . \tag{5,18}$$

Obráceně je patrné, že jsou-li dána přirozená čísla (5,17) vyhovující podmínkám (5,18), lze určit právě jedním způsobem nezáporná celá čísla (5,14) tak, aby platilo (5,16), načež (5,14) jsou nezáporná celá čísla splňující podmínky (5,15); potom lze určit právě jedním způsobem nezáporná celá čísla (5,11) tak, aby platilo (5,13); pak jsou (5,11) nezáporná celá čísla splňující podmínku (5,12). Z toho všeho je jasné, že počet všech kombinací s opakováním třídy m souboru M_n je dán číslem, které udává, kolik je takových $(n - 1)$-tic celých čísel $[t_1, t_2, \ldots, t_{n-1}]$, které splňují nerovnosti

$$1 \leqq t_1 < t_2 < \ldots < t_{n-1} \leqq n + m - 1 ,$$

t. j. uvažovaný počet je roven počtu všech kombinací (bez opakování) třídy $n - 1$ souboru $n + m - 1$ čísel

$$1, 2, \ldots, n + m - 1 ,$$

neboli je roven C_{n+m-1}^{n-1}.

§ 6. Binomická a polynomická věta

Název *polynomická věta* dáváme vzorci

$$(a_1 + a_2 + \ldots + a_k)^n = \sum_{r_1, \ldots, r_k} \frac{n!}{r_1!\, r_2! \ldots r_k!}\, a_1^{r_1} a_2^{r_2} \ldots a_k^{r_k} , \quad (6,1)$$

kde napravo $[r_1, \ldots, r_k]$ probíhá všecky ty k-tice nezáporných celých čísel, pro které je

$$r_1 + r_2 + \ldots + r_k = n . \quad (6,2)$$

Přitom jsou k, n libovolná přirozená čísla, $a_1, a_2, \ldots, a_k$ jsou libovolná reálná čísla.

Důkaz. Levá strana v (6,1) se rovná součinu

$$\sum_{\lambda=1}^{k} a_\lambda \cdot \sum_{\mu=1}^{k} a_\mu \cdot \sum_{\nu=1}^{k} a_\nu \ldots ,$$

kde počet činitelů se rovná n. Tento součin je podle nejobecnějšího distributivního zákona (věta I 4,6) roven součtu

$$\sum_{\lambda, \mu, \nu, \ldots} a_\lambda a_\mu a_\nu \ldots , \quad (6,3)$$

ve kterém každý z n indexů $\lambda, \mu, \nu, \ldots$ nezávisle na ostatních probíhá hodnoty $1, 2, \ldots, k$. Každý sčítanec v (6,3) je součinem n činitelů; rozdělíme je na skupiny tak, že do každé skupiny přijdou součiny lišící se navzájem pouze pořadím činitelů; potom je

$$a_\lambda a_\mu a_\nu \ldots = a_1^{r_1} a_2^{r_2} \ldots a_k^{r_k} ,$$

kde $r_1, r_2, \ldots, r_k$ jsou nezáporná celá čísla splňující podmínku (6,2); tato čísla jsou v celé skupině stále táž. Jelikož je jasné, že počet členů skupiny je vyjádřen číslem (4,7), dostáváme vzorec (6,1).

Důležitý zvláštní případ vzorce (6,1) dostáváme pro $k = 2$. Zde máme dva sumační indexy r_1, r_2, jež jsou nezáporná celá čísla vyhovu-

jící podmínce $r_1 + r_2 = n$. Tedy r_1 nabývá hodnot $0, 1, \ldots, n$; každému r_1 přísluší právě jedna hodnota $r_2 = n - r_1$. Podle (5,4′) je

$$\frac{n!}{r_1!\, r_2!} = \binom{n}{r_1}.$$

Píšeme-li ještě a, b místo a_1, a_2; r místo r_1, máme konečně

$$(a + b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}\ ; \tag{6,4}$$

vzorec (6,4) se nazývá *binomická věta*. Pro $n = 2, 3, 4$ zní binomická věta

$$(a + b)^2 = a^2 + 2ab + b^2\ ,$$
$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3\ ,$$
$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4\ .$$

Polynomické věty se užívá nejčastěji pro $n = 2$; zní v tomto případě

$$(a_1 + a_2 + \ldots + a_k)^2 = \sum_{r=1}^{k} a_r^2 + 2 \sum_{r,s} a_r a_s\ ,$$

kde v součtu $\sum_{r,s}$ probíhá $[r, s]$ kombinace (bez opakování) druhé třídy indexů $1, 2, \ldots, k$; je jich

$$\binom{k}{2} = \frac{k(k-1)}{2}\ .$$

Pro $k = 3$ máme

$$(a_1 + a_2 + a_3)^2 = a_1^2 + a_2^2 + a_3^2 + 2(a_1a_2 + a_1a_3 + a_2a_3)\ ,$$

pro $k = 4$ máme

$$(a_1 + a_2 + a_3 + a_4)^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2 + \\ + 2(a_1a_2 + a_1a_3 + a_1a_4 + a_2a_3 + a_2a_4 + a_3a_4)\ .$$

§ 7. Mnohočleny jedné proměnné

Budiž dáno celé číslo $n \geqq 0$ a reálná čísla $a_0, a_1, \ldots, a_n$, která můžeme zvolit libovolně až na podmínku, že

$$a_0 \neq 0\ . \tag{7,1}$$

Výraz

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \qquad (7,2)$$

se nazývá *mnohočlen* neboli *polynom*. Písmeno x zde neznamená určitým způsobem dané číslo, nýbrž *proměnnou*, za kterou můžeme dosadit libovolné reálné číslo. Jestliže za x dosadíme do výrazu (7,2) libovolně zvolené reálné číslo, dostaneme jako výsledek dosazení určité reálné číslo, které nazveme *hodnotou* mnohočlenu (7,2) ve zvoleném čísle. Označíme-li mnohočlen (7,2) třeba $P(x)$, označíme jeho hodnotu v číslech 1, -2, $-\frac{1}{2}$ atd.: $P(1)$, $P(-2)$, $P(-\frac{1}{2})$ atd. Číslo n se jmenuje [za předpokladu (7,1)] *stupeň* mnohočlenu (7,2). Čísla $a_0, a_1, \ldots, a_n$ se nazývají *koeficienty* mnohočlenu (7,2); a_0 se nazývá *nejvyšší koeficient*, a_n se nazývá *prostý člen* mnohočlenu (7,2). Je patrné, že prostý člen mnohočlenu je totožný s hodnotou tohoto mnohočlenu v čísle 0. O nejvyšším koeficientu mnohočlenu (7,2) jsme učinili předpoklad (7,1); pouze za tohoto předpokladu nazýváme číslo n stupněm mnohočlenu (7,2).

Jestliže ve výraze (7,2) je koeficient a_0 roven nule, jsou dvě možnosti. Buďto jsou *všecky* koeficienty rovny nule a pak je hodnota výrazu (7,2) v *každém* čísle rovna nule; v tomto případě říkáme, že (7,2) je *nulový mnohočlen*, kterému nepřisuzujeme žádný stupeň. Druhý případ je ten, že ačkoli $a_0 = 0$, je aspoň jeden koeficient různý od nuly; je-li k *nejmenší* index, pro který je $a_k \neq 0$, je výraz (7,2) pouze formálně různý od výrazu

$$a_kx^{n-k} + \ldots + a_{n-1}x + a_n ,$$

t. j. výraz (7,2) je ve vyšetřovaném případě mnohočlen stupně $n - k$ s nejvyšším koeficientem rovným a_k.

Poznámka 7,1. Přídavné jméno proměnná (v ženském rodě) má v matematice často význam podstatného jména; myslíme si je doplněno slovem veličina. (Stejně je tomu se slovem neznámá; viz poznámku I 7,1.) Místo písmena x můžeme pro proměnnou užít kteréhokoli písmena; podobně můžeme užít místo písmena P kteréhokoli jiného písmena při označení $P(x)$ mnohočlenu (7,2).

Poznámka 7,2. Poznali jsme, že výraz tvaru (7,2) je buďto nulový mnohočlen (jestliže všecky koeficienty jsou rovny nule), nebo je to mnohočlen určitého stupně, který je roven n v případě $a_0 \neq 0$ a je menší než n v případě $a_0 = 0$. Je účelné vyjadřovat se tak, že *každý* výraz tvaru (7,2) nazveme *mnohočlenem stupně nejvýš* n, t. j. mezi mnohočleny stupně nejvýš n řadíme také nulový mnohočlen pro každé $n = 0, 1, 2, 3, \ldots$, ačkoli nulový mnohočlen nemá žádný stupeň.

Číslo α nazveme *kořenem* mnohočlenu $P(x)$, je-li kořenem rovnice $P(x) = 0$ s neznámou x, neboli jestliže hodnota mnohočlenu $P(x)$ v čísle α je rovna nule. *Každé* reálné číslo je kořenem nulového mnohočlenu. Jestliže však nejsou všecky koeficienty mnohočlenu (7,2) rovny nule, může mít tento mnohočlen jenom konečný počet kořenů, neboť platí:

Věta 7,1. *Mnohočlen stupně n nemůže mít více než n kořenů.*

Důkaz. Věta je jasná pro $n = 0$, neboť hodnota mnohočlenu stupně 0 v každém čísle je rovna jednomu a témuž číslu (7,1). Důkaz dokončíme indukcí vzhledem k n způsobem, který byl vysvětlen v poznámce 2,2. Budeme předpokládat, že při určitém $n > 0$ je věta dokázána pro všecky mnohočleny stupňů menších než n a za tohoto předpokladu dokážeme, že věta je správná také pro mnohočlen (7,2) stupně n, který označíme $P(x)$; jeho nejvyšší koeficient je tedy (7,1). Jestliže daný mnohočlen $P(x)$ nemá žádný kořen nebo jestliže sice kořeny má, ale má jich celkem méně než n, není co dokazovat. Předpokládejme tedy, že existuje n navzájem různých čísel $\alpha_1, \alpha_2, \ldots, \alpha_n$, z nichž každé je kořenem mnohočlenu $P(x)$, a utvořme výraz

$$Q(x) = a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) = a_0 \prod_{r=1}^{n} (x - \alpha_r) . \qquad (7,3)$$

Z nejobecnějšího distributivního zákona (t. j. z věty I 4,6) plyne, že $Q(x)$ je mnohočlen stupně n s nejvyšším koeficientem (7,1) stejným jako u $P(x)$, takže

$$P(x) - Q(x) = R(x)$$

je buďto nulový mnohočlen, nebo je to mnohočlen stupně k menšího než n. Druhý případ je však nemožný, neboť je jasné, že každé z $n > k$ navzájem různých čísel $\alpha_1, \alpha_2, \ldots, \alpha_n$ je kořenem mnohočlenu $R(x)$, kdežto podle předpokladu mnohočlen stupně $k < n$ nemůže mít n různých kořenů. Tudíž $R(x)$ je nulový mnohočlen, t. j. mnohočlen $P(x)$ je totožný s mnohočlenem (7,3), který v důsledku (7,1) nemůže podle věty I 3,10 mít žádný další kořen různý od n kořenů $\alpha_1, \alpha_2, \ldots, \alpha_n$. Tím je naše věta dokázána.

Věta 7,2. *Je-li $P(x)$ mnohočlen stupně n, $Q(x)$ mnohočlen stupně m, je $P(x) \cdot Q(x)$ mnohočlen stupně $n + m$.*

Důkaz. Jest

$$\begin{aligned} P(x) &= a_0x^n + a_1x^{n-1} + \ldots + a_n , \\ Q(x) &= b_0x^m + b_1x^{m-1} + \ldots + b_m . \end{aligned} \qquad (7,4)$$

Podle zobecněného distributivního zákona je

$$P(x)\,Q(x) = c_0x^{n+m} + c_1x^{n+m-1} + \ldots + c_{n+m}\,,$$

kde $c_0 = a_0b_0$. Podle předpokladu je $a_0 \neq 0$, $b_0 \neq 0$, tedy také $c_0 \neq 0$, takže $P(x)\,.\,Q(x)$ má stupeň $n + m$.

Poznámka 7,3. Z věty 7,2 plyne indukcí vzhledem ke k: Jsou-li $P_1(x)$, $P_2(x)$, ..., $P_k(x)$ mnohočleny, při čemž pro $1 \leqq s \leqq k$ stupeň mnohočlenu $P_s(x)$ je roven r_s, pak $\prod_{s=1}^{k} P_s(x)$ je mnohočlen stupně $\sum_{s=1}^{k} r_s$.

Buďtež opět dány dva mnohočleny (7,4). Můžeme předpokládat, že je $n \geqq m$, neboť kdyby tomu tak původně nebylo, docílili bychom toho prostou výměnou obou mnohočlenů. Oba mnohočleny jsou tedy stupně nejvýš n ve smyslu poznámky 7,2. Mnohočleny $P(x)$, $Q(x)$ považujeme za totožné, jestliže rozdíl $P(x) - Q(x)$ je nulový mnohočlen; v případě $n = m$ neboli $n - m = 0$ to znamená, že

$$a_0 = b_0\,,\ a_1 = b_1,\ \ldots,\ a_n = b_n\,,$$

kdežto v případě $n > m$, položíme-li $n - m = k > 0$, znamená totožnost mnohočlenů $P(x)$, $Q(x)$, že je

$$a_0 = \ldots = a_{k-1} = 0,\ a_k = b_0,\ a_{k+1} = b_1,\ \ldots,\ a_n = b_m\,,$$

t. j. $P(x)$ se liší od $Q(x)$ pouze o členy tvaru $0\,.\,x^r$, jejichž hodnota v každém čísle je rovna nule. Dva totožné mnohočleny mají ovšem v každém čísle touž hodnotu. Jestliže však mnohočleny $P(x)$, $Q(x)$ nejsou totožné ve smyslu právě podrobně popsaném, je $P(x) - Q(x)$ mnohočlen, který má určitý stupeň; tento stupeň zřejmě nemůže být větší než n, takže podle věty 7,1 je nejvýš n takových čísel x, pro která platí $P(x) - Q(x) = 0$ neboli $P(x) = Q(x)$. Tím jsme dokázali, že platí:

Věta 7,3. *Jsou-li $P(x)$, $Q(x)$ dva různé mnohočleny stupně nejvýš n, existuje nejvýš n takových čísel x, ve kterých je $P(x) = Q(x)$.*

Věta 7,4. *Budiž n nezáporné celé číslo a budiž dáno $n + 1$ různých reálných čísel $\alpha_0, \alpha_1, \ldots, \alpha_n$ a $n + 1$ reálných čísel $c_0, c_1, \ldots, c_n$, která nemusí* (ale mohou) *být navzájem různá. Potom existuje právě jeden mnohočlen $P(x)$ stupně nejvýš n takový, že*

$$P(\alpha_0) = c_0,\ P(\alpha_1) = c_1,\ \ldots,\ P(\alpha_n) = c_n\,.$$

Důkaz. Z věty 7,3 je patrné, že více než jeden mnohočlen se žádanými vlastnostmi existovat nemůže. Je tedy třeba dokázat, že existuje *aspoň jeden* mnohočlen se žádanými vlastnostmi. Nyní

$$P_0(x) = \prod_{r=1}^{n} \frac{x - \alpha_r}{\alpha_0 - \alpha_r}$$

je mnohočlen stupně n, pro který platí

$$P_0(\alpha_0) = 1,\ P_0(\alpha_r) = 0 \quad \text{pro} \quad 1 \leqq r \leqq n\,.$$

Stejně se však zjistí, že pro každé s $(0 \leqq s \leqq n)$ existuje takový mnohočlen $P_s(x)$ stupně n, že

$$P_s(\alpha_s) = 1,\ P_s(\alpha_r) = 0 \quad \text{pro} \quad 0 \leqq r \leqq n,\ r \neq s\,.$$

Je patrné, že

$$P(x) = \sum_{s=0}^{n} c_s P_s(x)$$

je mnohočlen se žádanými vlastnostmi.

Příklad 7,1. Hledejme takový mnohočlen $P(x)$ stupně nejvýš 4, pro který je

$$P(1) = \tfrac{1}{2},\ P(2) = -\tfrac{1}{2},\ P(3) = \tfrac{1}{3},\ P(4) = -\tfrac{1}{3},\ P(5) = 1\,.$$

Zde je

$$P_0(x) = \frac{(x-2)(x-3)(x-4)(x-5)}{(1-2)(1-3)(1-4)(1-5)} = \frac{1}{24}(x-2)(x-3)(x-$$

$$-4)(x-5) = \frac{1}{24}(x^4 - 14x^3 + 71x^2 - 154x + 120)\,,$$

$$P_1(x) = \frac{(x-1)(x-3)(x-4)(x-5)}{(2-1)(2-3)(2-4)(2-5)} = -\frac{1}{6}(x-1)(x-$$

$$-3)(x-4)(x-5) = -\frac{1}{6}(x^4 - 13x^3 + 59x^2 - 107x + 60)\,,$$

$$P_2(x) = \frac{(x-1)(x-2)(x-4)(x-5)}{(3-1)(3-2)(3-4)(3-5)} = \frac{1}{4}(x-1)(x-2)(x-$$

$$-4)(x-5) = \frac{1}{4}(x^4 - 12x^3 + 49x^2 - 78x + 40)\,,$$

$$P_3(x) = \frac{(x-1)(x-2)(x-3)(x-5)}{(4-1)(4-2)(4-3)(4-5)} = -\frac{1}{6}(x-1)(x-$$

$$-2)(x-3)(x-5) = -\frac{1}{6}(x^4 - 11x^3 + 41x^2 - 61x + 30),$$

$$P_4(x) = \frac{(x-1)(x-2)(x-3)(x-4)}{(5-1)(5-2)(5-3)(5-4)} = \frac{1}{24}(x-1)(x-2)(x-$$

$$-3)(x-4) = \frac{1}{24}(x^4 - 10x^3 + 35x^2 - 50x + 24),$$

a jelikož pro hledaný mnohočlen $P(x)$ platí

$$P(x) = \tfrac{1}{2}P_0(x) - \tfrac{1}{2}P_1(x) + \tfrac{1}{3}P_2(x) - \tfrac{1}{3}P_3(x) + P_4(x),$$

vyjde po výpočtu, který čtenář sám snadno provede, že

$$P(x) = \frac{41x^4 - 490x^3 + 2047x^2 - 3470x + 1944}{144}.$$

Budiž dán mnohočlen (7,2) stupně nejvýš n, který označíme $P(x)$ a budiž dáno reálné číslo α. Odvodíme si t. zv. *Ruffiniovo pravidlo*, podle kterého lze počítat hodnotu $P(\alpha)$ našeho mnohočlenu způsobem, který je zejména při větším n výhodnější než přímé dosazení. Ruffiniovo pravidlo záleží v tom, že počítáme postupně čísla

$$c_0 = a_0,\ c_1 = c_0\alpha + a_1,\ c_2 = c_1\alpha + a_2,\ \ldots,\ c_n = c_{n-1}\alpha + a_n$$

neboli

$$c_0 = a_0,\ c_r = c_{r-1}\alpha + a_r \quad \text{pro} \quad 1 \leqq r \leqq n. \tag{7,5}$$

Jest

$$c_1 = a_0\alpha + a_1,$$
$$c_2 = (a_0\alpha + a_1)\,\alpha + a_2 = a_0\alpha^2 + a_1\alpha + a_2,$$
$$c_3 = (a_0\alpha^2 + a_1\alpha + a_2)\,\alpha + a_3 = a_0\alpha^3 + a_1\alpha^2 + a_2\alpha + a_3$$

atd.; obecně máme

$$c_r = a_0\alpha^r + a_1\alpha^{r-1} + \ldots + a_r \quad \text{pro} \quad 1 \leqq r \leqq n,$$

takže $c_n = P(\alpha)$. Prakticky počítáme čísla (7,5) podle schematu

$$\begin{array}{c|cccccc} & a_0 & a_1 & a_2 & \ldots & a_{n-1} & a_n \\ \hline \alpha & c_0 & c_1 & c_2 & \ldots & c_{n-1} & c_n = P(\alpha) \end{array}, \tag{7,6}$$

které sestavujeme takto: V prvním řádku schematu jsou koeficienty mnohočlenu $P(x)$. Do druhého řádku napíšeme nejprve pod nejvyšší koeficient a_0 číslo $c_0 = a_0$. Potom postupně pro $r = 1, 2, \ldots, n$ vypočteme a zapíšeme pod koeficient a_r číslo c_r, které se vypočte tak, že předcházející číslo c_{r-1} znásobíme číslem α a k součinu přičteme a_r.

Příklad 7,2. Je-li $P(x) = 41x^4 - 490x^3 + 2047x^2 - 3470x + 1944$, máme

	41	− 490	2047	− 3470	1944
$\alpha = 1$	41	− 449	1598	− 1872	72
$\alpha = 2$	41	− 408	1231	− 1008	− 72
$\alpha = 3$	41	− 367	946	− 632	48
$\alpha = 4$	41	− 326	743	− 498	− 48
$\alpha = 5$	41	− 285	622	− 360	144

Tedy $P(1) = 72, P(2) = -72, P(3) = 48, P(4) = -48, P(5) = 144$, což souhlasí s výsledkem příkladu 7,1, neboť

$$\frac{72}{144} = \frac{1}{2}, \quad \frac{-72}{144} = -\frac{1}{2}, \quad \frac{48}{144} = \frac{1}{3},$$

$$\frac{-48}{144} = -\frac{1}{3}, \quad \frac{144}{144} = 1.$$

Má-li $P(x)$, $c_0, c_1, c_2, \ldots, c_n$ týž význam jako dosud, položme

$$P_1(x) = c_0x^{n-1} + c_1x^{n-2} + c_2x^{n-3} + \ldots + c_{n-1}$$

neboli

$$P_1(x) = \sum_{r=0}^{n-1} c_r x^{n-r-1},$$

takže

$$(x - \alpha) P_1(x) = xP_1(x) - \alpha P_1(x) = \sum_{r=0}^{n-1} c_r x^{n-r} - \alpha \sum_{r=1}^{n} c_{r-1} x^{n-r} =$$

$$= c_0x^n + \sum_{r=1}^{n-1} (c_r - \alpha c_{r-1}) x^{n-r} + (c_n - \alpha c_{n-1}) - c_n;$$

podle (7,5) je tedy

$$(x - \alpha) P_1(x) = a_0x^n + \sum_{r=1}^{n-1} a_r x^{n-r} + a_n - c_n,$$

a jelikož $c_n = P(\alpha)$, vyjde

$$P(x) = (x - \alpha) P_1(x) + P(\alpha). \qquad (7,7)$$

Poznámka 7,4. Je-li dán mnohočlen $P(x)$ a číslo α, je mnohočlen $P_1(x)$ jednoznačně určen. Neboť jestliže vedle (7,7) platí také

$$P(x) = (x - \alpha)\, Q(x) + P(\alpha)\,,$$

je

$$(x - \alpha)[P_1(x) - Q(x)] \qquad (7,8)$$

nulový mnohočlen, takže také $P_1(x) - Q(x)$ je nulový mnohočlen, neboť jinak by podle věty 7,2 mnohočlen (7,8) měl určitý stupeň a nebyl by nulový.

Poznámka 7,5. Je-li $P(x)$ mnohočlen stupně $n > 0$, je $P_1(x)$ mnohočlen stupně $n - 1$ a oba mnohočleny mají společný nejvyšší koeficient $a_0 = c_0 \neq 0$.

Je-li dán mnohočlen $P(x)$ stupně $n > 0$ a reálné číslo α, existuje takový mnohočlen $P_1(x)$ stupně $n - 1$, že platí (7,7) neboli, píšeme-li A_0 místo $P(\alpha)$,

$$P(x) = A_0 + (x - \alpha)\, P_1(x)\,.$$

Je-li $n - 1 > 0$, vyjdeme od mnohočlenu $P_1(x)$ stupně $n - 1$ a najdeme mnohočlen $P_2(x)$ stupně $n - 2$ a číslo A_1 tak, že

$$P_1(x) = A_1 + (x - \alpha)\, P_2(x)\,.$$

Je-li $n - 2 > 0$, postupujeme týmž způsobem dále, až skončíme mnohočlenem $P_n(x) = A_n$ stupně 0. Ostatně z poznámky 7,5 soudíme, že nejvyšší koeficient a_0 mnohočlenu $P(x)$ je zároveň nejvyšším koeficientem všech mnohočlenů $P_1(x)$, $P_2(x)$ atd., takže $A_n = a_0$. Vcelku máme

$$\begin{aligned}
P(x) &= A_0 + (x - \alpha)\, P_1(x)\,,\\
P_1(x) &= A_1 + (x - \alpha)\, P_2(x)\,,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
P_{n-2}(x) &= A_{n-2} + (x - \alpha)\, P_{n-1}(x)\,,\\
P_{n-1}(x) &= A_{n-1} + (x - \alpha)\, P_n(x)\,,\\
P_n(x) &= A_n\,,
\end{aligned}$$

takže

$$P(x) = A_0 + (x - \alpha)\, P_1(x) = A_0 + A_1(x - \alpha) + (x - \alpha)^2\, P_2(x) = \\ = A_0 + A_1(x - \alpha) + A_2(x - \alpha)^2 + (x - \alpha)^3\, P_3(x) \quad \text{atd.},$$

a nakonec

$$P(x) = A_0 + A_1(x - \alpha) + A_2(x - \alpha)^2 + \ldots + A_n(x - \alpha)^n\,, \qquad (7,9)$$

kde čísla $A_0, A_1, A_2, \ldots, A_n$ počítáme podle t. zv. *Hornerova schematu*, které záleží v tom, že se n-krát za sebou užije Ruffiniova pravidla. Podrobněji si to vyložíme na příkladě.

Příklad 7,3. Budiž $n = 5$, $P(x) = 3x^5 - 4x^3 + x^2 - x - 7$, $\alpha = 2$. Hornerovo schema je

2	3	0	−4	1	−1	−7
	3	6	8	17	33	59
	3	12	32	81	195	
	3	18	68	217		
	3	24	116			
	3	30				
	3					

Ve schematu je v prvním řádku zapsáno číslo $\alpha = 2$ a koeficienty 3, 0, −4, 1, −1, −7 mnohočlenu $P(x)$. Pomocí Ruffiniova pravidla jsou vypočteny a zapsány do druhého řádku koeficienty 3, 6, 8, 17, 33 mnohočlenu $P_1(x)$ a číslo $A_0 = 59$. Na základě nalezených koeficientů mnohočlenu $P_1(x) = 3x^4 + 6x^3 + 8x^2 + 17x + 33$ jsou dále vypočteny pomocí Ruffiniova pravidla a zapsány do třetího řádku koeficienty 3, 12, 32, 81 mnohočlenu $P_2(x) = 3x^3 + 12x^2 + 32x + 81$ a číslo $A_1 = 195$. Podobně dostaneme ve čtvrtém řádku koeficienty 3, 18, 68 mnohočlenu $P_3(x) = 3x^2 + 18x + 68$ a číslo $A_2 = 217$, v pátém řádku koeficienty 3, 24 mnohočlenu $P_4(x) = 3x + 24$ a číslo $A_3 = 116$, v šestém řádku je jediný koeficient 3 mnohočlenu $P_5(x) = 3$ a číslo $A_4 = 30$, v posledním řádku pak je číslo $A_5 = 3$. Výsledek je

$$P(x) = 59 + 195(x - 2) + 217(x - 2)^2 + 116(x - 2)^3 + 30(x - 2)^4 + 3(x - 2)^5 . \tag{7,10}$$

O správnosti výsledku se můžeme přesvědčit pomocí binomické věty, která dává

$$\left.\begin{aligned} (x - 2)^2 &= x^2 - 4x + 4 , \\ (x - 2)^3 &= x^3 - 6x^2 + 12x - 8 , \\ (x - 2)^4 &= x^4 - 8x^3 + 24x^2 - 32x + 16 , \\ (x - 2)^5 &= x^5 - 10x^4 + 40x^3 - 80x^2 + 80x - 32 , \end{aligned}\right\} \tag{7,11}$$

neboť dosadíme-li ze (7,11) do (7,10), vyjde $P(x) = 3x^5 - 4x^3 + x^2 - x - 7$.

§ 8. Kořeny mnohočlenů

Říkáme, že mnohočlen $P(x)$ je *dělitelný* mnohočlenem $Q(x)$, jestliže existuje takový mnohočlen $R(x)$, že pro všecka x je

$$P(x) = Q(x) \,.\, R(x) \,. \tag{8,1}$$

Podle této definice je nulový mnohočlen $P(x)$ dělitelný každým mnohočlenem $Q(x)$, neboť jestliže $P(x)$ i $R(x)$ je nulový mnohočlen, platí (8,1) pro libovolný mnohočlen $Q(x)$; mnohočlen $P(x)$, který není nulový, nemůže být dělitelný nulovým mnohočlenem, neboť jestliže $Q(x)$ je nulový mnohočlen, platí (8,1) pouze tehdy, je-li také $P(x)$ nulový mnohočlen. Proto pojem dělitelnosti má zajímavost pouze v oboru *nenulových* mnohočlenů.

Poznámka 8,1. Jsou-li dány mnohočleny $P(x)$, $Q(x)$, při čemž $Q(x)$ není nulový, může (8,1) platit jen pro *jediný* mnohočlen $R(x)$. Neboť jestliže vedle (8,1) platí

$$P(x) = Q(x) \,.\, R_1(x) \,,$$

kde také $R_1(x)$ je mnohočlen, je

$$Q(x) \,.\, [R(x) - R_1(x)]$$

nulový mnohočlen, což by podle věty 7,2 nebylo možné, kdyby ani $Q(x)$, ani $R(x) - R_1(x)$ nebyl nulový mnohočlen. Je tedy $R(x) - R_1(x) = 0$ neboli $R(x) = R_1(x)$ pro všecka x.

Věta 8,1. *Je-li mnohočlen stupně n dělitelný mnohočlenem stupně m,* je $n \geqq m$. To je snadný důsledek věty 7,2.

Věta 8,2. *Je-li mnohočlen $P_1(x)$ dělitelný mnohočlenem $P_2(x)$ a je-li mnohočlen $P_2(x)$ dělitelný mnohočlenem $P_3(x)$, je mnohočlen $P_1(x)$ dělitelný mnohočlenem $P_3(x)$.* To je zřejmé z definice dělitelnosti.

Pojem kořenu mnohočlenu jsme zavedli už na str. 174 a o kořenech mnohočlenu jsme už dokázali větu 7,1.

Věta 8,3. *Číslo α je kořenem nenulového mnohočlenu $P(x)$ právě tehdy, jestliže $P(x)$ je dělitelný mnohočlenem $x - \alpha$.*

Důkaz. Věta je správná pro mnohočlen stupně nula, neboť je jasné, že mnohočlen stupně nula nemá kořen, a z věty 8,1 plyne, že mnohočlen stupně 0 nemůže být dělitelný mnohočlenem $x - \alpha$, jehož stupeň je roven 1. Je-li $P(x)$ mnohočlen stupně $n > 0$, víme, že existuje takový mnohočlen $P_1(x)$ stupně $n - 1$, že platí (7,7). Je-li číslo α kořenem mnohočlenu $P(x)$, je $P(\alpha) = 0$, takže (7,7)

dává $P(x) = (x - \alpha)\, P_1(x)$, t. j. mnohočlen $P(x)$ je dělitelný mnohočlenem $x - \alpha$. Obráceně, je-li mnohočlen $P(x)$ dělitelný mnohočlenem $x - \alpha$, plyne z definice dělitelnosti, že existuje takový mnohočlen $P_1(x)$, že $P(x) = (x - \alpha)\, P_1(x)$ pro všecka x. Dosadíme-li $x = \alpha$, vyjde $P(x) = 0$, t. j. číslo α je kořenem mnohočlenu $P(x)$.

Nechť číslo α je kořenem mnohočlenu $P(x)$ stupně n. Ptejme se, pro jaké hodnoty přirozeného čísla r je mnohočlen $P(x)$ dělitelný mnohočlenem $(x - \alpha)^r$. Z věty 8,1 plyne, že $P(x)$ není dělitelný mnohočlenem $(x - \alpha)^r$, je-li $r > n$, z věty 8,3 pak plyne, že $P(x)$ je dělitelný mnohočlenem $x - \alpha = (x - \alpha)^1$. Jsou-li r, s taková přirozená čísla, že $r < s$, je

$$(x - \alpha)^s = (x - \alpha)^r \,.\, (x - \alpha)^{s-r} ,$$

takže mnohočlen $(x - \alpha)^s$ je dělitelný mnohočlenem $(x - \alpha)^r$; z věty 8,2 pak plyne, že jestliže mnohočlen $P(x)$ je dělitelný mnohočlenem $(x - \alpha)^s$, je také dělitelný mnohočlenem $(x - \alpha)^r$. V důsledku všech těchto poznatků ke každému kořenu α mnohočlenu $P(x)$ stupně n existuje zcela určité přirozené číslo k s tou vlastností, že mnohočlen $P(x)$ je dělitelný mnohočlenem $(x - \alpha)^r$ pro každé přirozené číslo $r \leqq k$ a není dělitelný mnohočlenem $(x - \alpha)^r$ pro žádné přirozené číslo $r > k$; mimo to podle předchozího výkladu je $k \leqq n$. Toto přirozené číslo k se nazývá *násobnost* nebo také *řád* kořenu α mnohočlenu $P(x)$. Kořen α se nazývá *k-násobným*, pro $k = 1$ *jednoduchým*, pro $k > 1$ *vícenásobným*, pro $k = 2$ *dvojným*, pro $k = 3$ *trojným*. Připomeňme znovu, že pro násobnost k kořenu α mnohočlenu $P(x)$, jehož stupeň je roven n, platí nerovnost $k \leqq n$.

Věta 8,4. *Kořen α nenulového mnohočlenu $P(x)$ je k-násobný právě tehdy, jestliže pro všecka x*

$$P(x) = (x - \alpha)^k \,.\, Q(x) , \tag{8,2}$$

kde $Q(x)$ je takový mnohočlen, že $Q(\alpha) \neq 0$ [t. j. že α není kořenem mnohočlenu $Q(x)$].

Důkaz. Podle definice násobnosti kořenu α platí (8,2) právě tehdy, je-li α kořenem mnohočlenu $P(x)$ s násobností $s \geqq k$. Máme ukázat, že $Q(\alpha) = 0$ právě tehdy, je-li $s > k$. Je-li však $Q(\alpha) = 0$, pak podle věty 8,3 existuje takový mnohočlen $R(x)$, že pro všecka x je $Q(x) = (x - \alpha)\, R(x)$, takže podle (8,2) je $P(x) = (x - \alpha)^{k+1}\, R(x)$; z definice násobnosti s pak plyne $s \geqq k + 1$ neboli $s > k$. Obráceně, je-li $s > k$ neboli $s \geqq k + 1$, existuje takový mnohočlen $R(x)$, že pro všecka x je $P(x) = (x - \alpha)^{k+1} \,.\, R(x)$ neboli

$$P(x) = (x - \alpha)^k \,.\, (x - \alpha)\, R(x) .$$

Porovnáme-li tuto rovnost s (8,2), soudíme z poznámky 8,1, že pro všecka x je $Q(x) = (x - \alpha)\, R(x)$. Dosadíme-li $x = \alpha$, dostaneme $Q(\alpha) = 0$.

Poznámka 8,2. Větu 8,4 můžeme doplnit. Je zřejmé, že kořeny mnohočlenu $Q(x)$ jsou totožné s těmi kořeny mnohočlenu $P(x)$, které jsou různé od α. (Je-li α jediný kořen mnohočlenu $P(x)$, nemá $Q(x)$ žádný kořen.) Je-li β kořen mnohočlenu $P(x)$ různý od kořenu α, t. j. je-li β kořen mnohočlenu $Q(x)$, *má β stejnou násobnost i jako kořen mnohočlenu $P(x)$ i jako kořen mnohočlenu $Q(x)$*. Neboť je-li β h-násobným kořenem mnohočlenu $Q(x)$, je podle věty 8,4 pro všecka x

$$Q(x) = (x - \beta)^h\, R(x)\,,$$

kde mnohočlen $R(x)$ už nemá kořen β. Potom je však pro všecka x

$$P(x) = (x - \beta)^h \,.\, (x - \alpha)^k\, R(x)\,,$$

a protože $\beta \neq \alpha$, není β kořenem mnohočlenu $(x - \alpha)^k \,.\, R(x)$, takže podle věty 8,4 je β h-násobným kořenem mnohočlenu $P(x)$.

Poznámka 8,3. Z věty 8,4 je patrné, že číslo α je k-násobným kořenem mnohočlenu $P(x)$ právě tehdy, jestliže v (7,9) čísla A_0, $A_1, \ldots, A_{k-1}$ jsou rovna nule, ale $A_k \neq 0$. Z toho plyne, že násobnost kořenu α nenulového mnohočlenu $P(x)$ se dá určit pomocí Hornerova schematu.

Připomeňme si znovu, že podle věty 7,1 nenulový mnohočlen $P(x)$ má jen *konečný počet* kořenů.

Věta 8,5. *Jsou-li $\alpha_1, \alpha_2, \ldots, \alpha_m$ všecky kořeny nenulového mnohočlenu $P(x)$ a jsou-li $k_1, k_2, \ldots, k_m$ jejich násobnosti, existuje takový mnohočlen $Q(x)$, že pro všecka x je*

$$P(x) = \prod_{r=1}^{m} (x - \alpha_r)^{k_r} \,.\, Q(x) \qquad (8,3)$$

a že mnohočlen $Q(x)$ nemá žádný kořen. Obráceně, platí-li (8,3) *a nemá-li mnohočlen $Q(x)$ žádný kořen, jsou $\alpha_1, \alpha_2, \ldots, \alpha_m$ všecky kořeny mnohočlenu $P(x)$ a $k_1, k_2, \ldots, k_m$ jsou jejich násobnosti.*

Důkaz. Nechť nejprve jsou $\alpha_1, \alpha_2, \ldots, \alpha_m$ všecky kořeny mnohočlenu $P(x)$ a $k_1, k_2, \ldots, k_m$ jejich násobnosti. Podle věty 8,4 můžeme položit

$$P(x) = (x - \alpha_1)^{k_1} \,.\, P_1(x)\,, \qquad (8,4)$$

kde při přechodu od $P(x)$ k $P_1(x)$ se kořen α_1 ztratí, ale podle poznámky 8,2 ostatní kořeny $\alpha_2, \ldots, \alpha_m$ zůstanou zachovány i se svými

násobnostmi. (Pro $m = 1$ nemá ovšem $P_1(x)$ už žádný kořen.) Je-li $m > 1$, užijeme opětně věty 8,4 a položíme

$$P_1(x) = (x - \alpha_2)^{k_2} \cdot P_2(x) , \tag{8,5}$$

kde při přechodu od $P_1(x)$ k $P_2(x)$ se ztratí kořen α_2, ale kořeny $\alpha_3, \ldots, \alpha_m$ (je-li $m > 2$) zachovávají svoje násobnosti. Je-li $m > 2$, máme podobně dále

$$\left.\begin{aligned} P_2(x) &= (x - \alpha_3)^{k_3} P_3(x) , \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ P_{m-1}(x) &= (x - \alpha_m)^{k_m} P_m(x) , \end{aligned}\right\} \tag{8,6}$$

kde $P_m(x)$ už nemá žádný kořen. Stačí položit $P_m(x) = Q(x)$, abychom z (8,4), (8,5) a (8,6) dostali (8,3). Obráceně, platí-li (8,3), má $P(x)$ kořeny $\alpha_1, \ldots, \alpha_m$ a žádné další, jestliže $Q(x)$ nemá žádný další kořen. Máme ještě ukázat, že na př. α_1 je k_1-násobný kořen mnohočlenu (8,3). To plyne z věty 8,4, neboť podle (8,3) platí (8,4), kde

$$P_1(x) = \prod_{r=2}^{m} (x - \alpha_r)^{k_r} \cdot Q(x) ,$$

takže $P_1(\alpha_1) \neq 0$.

Poznámka 8,4. Z věty 8,5 plyne podle poznámky (7,3), že jestliže mnohočlen $P(x)$ stupně n má kořeny $\alpha_1, \alpha_2, \ldots, \alpha_k$ (navzájem různé) s násobnostmi $r_1, r_2, \ldots, r_k$, je $r_1 + r_2 + \ldots + r_k \leqq n$.

Poznámka 8,5. Jestliže mnohočlen $P(x)$ stupně n má n různých kořenů, plyne z poznámky 8,4, že všecky tyto kořeny jsou jednoduché.

Je jasné, že mnohočlen prvního stupně neboli *lineární mnohočlen*

$$P_1(x) = a_0 x + a_1 \quad (a_0 \neq 0)$$

má vždycky právě jeden kořen, jímž je číslo

$$\alpha = -\frac{a_1}{a_0};$$

jest

$$P_1(x) = a_0(x - \alpha)$$

pro všecka x; přitom kořen α je vždy jednoduchý. Naproti tomu mnohočlen druhého stupně neboli *kvadratický mnohočlen*

$$P_2(x) = a_0 x^2 + a_1 x + a_2 \quad (a_0 \neq 0) \tag{8,7}$$

nemusí vždycky mít kořen. Pro všecka x je jednak

$$4a_0P_2(x) = 4a_0^2x^2 + 4a_0a_1x + 4a_0a_2 ,$$

jednak

$$(2a_0x + a_1)^2 = 4a_0^2x^2 + 4a_0a_1x + a_1^2 ,$$

tedy také

$$4a_0P_2(x) = (2a_0x + a_1)^2 - D , \tag{8,8}$$

kde

$$D = a_1^2 - 4a_0a_2 . \tag{8,9}$$

Číslo D se nazývá *diskriminant* kvadratického mnohočlenu (8,7). Jelikož $a_0 \neq 0$, je patrné z (8,8), že číslo x je kořenem mnohočlenu $P_2(x)$ právě tehdy, jestliže x je kořenem rovnice

$$(2a_0x + a_1)^2 = D . \tag{8,10}$$

Jsou nyní tři možnosti. Jestliže *za prvé* diskriminant D je *záporný*, nemá mnohočlen $P_2(x)$ žádný kořen, neboť levá strana v (8,10) není záporná pro žádné x. Jestliže *za druhé* diskriminant D je *roven nule*, je číslo x kořenem mnohočlenu $P_2(x)$ právě tehdy, jestliže $2a_0x + a_1 = 0$, takže v tomto případě mnohočlen $P_2(x)$ má právě jeden kořen

$$\alpha = -\frac{a_1}{2a_0} ;$$

pro všecka x je potom

$$2a_0x + a_1 = 2a_0(x - \alpha) ,$$

tedy podle (8,8) také (jelikož $D = 0$)

$$P_2(x) = a_0(x - \alpha)^2 ,$$

takže číslo α je dvojným kořenem mnohočlenu $P_2(x)$. Jestliže *za třetí* diskriminant D je *kladný*, potom podle věty III 6,3 existuje kladné číslo $\sqrt{D}$ a rovnice (8,10) je splněna právě tehdy, je-li buďto

$$2a_0x + a_1 = \sqrt{D} ,$$

nebo

$$2a_0x + a_1 = -\sqrt{D} ,$$

t. j. je-li buďto $x = \alpha_1$, nebo $x = \alpha_2$, kde

$$\alpha_1 = \frac{-a_1 + \sqrt{D}}{2a_0} , \qquad \alpha_2 = \frac{-a_1 - \sqrt{D}}{2a_0} .$$

Z poznámky 8,5 plyne, že oba kořeny mnohočlenu $P_2(x)$ jsou jednoduché.

§ 9. Mnohočleny několika proměnných

Dosud jsme mluvili pouze o mnohočlenech jedné proměnné, kterou jsme označili x. Mnohočlen $P(x)$ proměnné x byl definován jako součet konečného počtu členů, z nichž každý má tvar $a_r x^r$, kde každý exponent r je určité nezáporné celé číslo a a_r je určité reálné číslo, zvané koeficient mnohočlenu $P(x)$ příslušný exponentu r. V tomto paragrafu si promluvíme zcela stručně o mnohočlenech k proměnných, které označíme $x_1, x_2, \ldots, x_k$; při tom je k libovolně dané přirozené číslo. Mnohočlen $P(x_1, x_2, \ldots, x_k)$ je součet

$$P(x_1, x_2, \ldots, x_k) = \sum_{r_1, r_2, \ldots, r_k} a_{r_1, r_2, \ldots, r_k} x_1^{r_1} x_2^{r_2} \ldots x_k^{r_k}, \qquad (9,1)$$

kde v každém členu exponenty $r_1, r_2, \ldots, r_k$ jsou určitá nezáporná čísla a $a_{r_1, r_2, \ldots, r_k}$ (stručněji, není-li obavy z nedorozumění, můžeme psát bez čárek $a_{r_1 r_2 \ldots r_k}$) je určité reálné číslo, zvané opět *koeficient* mnohočlenu $P(x_1, x_2, \ldots, x_k)$ příslušný exponentům $r_1, r_2, \ldots, r_k$ (při tom je podstatné také pořadí těchto exponentů).

Jsou-li všechny exponenty $r_1, r_2, \ldots, r_k$ rovny nule, nazveme příslušný koeficient $a_{00\ldots0}$ *prostým členem* mnohočlenu $P(x_1, x_2, \ldots, x_k)$.

Jsou-li $\alpha_1, \alpha_2, \ldots, \alpha_k$ určitá reálná čísla, dostaneme dosazením hodnot

$$x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_k = \alpha_k \qquad (9,2)$$

do mnohočlenu (9,1) určité reálné číslo, které označíme $P(\alpha_1, \alpha_2, \ldots, \alpha_k)$ a nazveme *hodnotou* mnohočlenu (9,1) v číslech $\alpha_1, \alpha_2, \ldots, \alpha_k$. Je jasné, že hodnota $P(0, 0, \ldots, 0)$ mnohočlenu (9,1) v číslech $0, 0, \ldots, 0$ je rovna prostému členu mnohočlenu (9,1).

Dva mnohočleny $P(x_1, x_2, \ldots, x_k)$ a $Q(x_1, x_2, \ldots, x_k)$ považujeme za *totožné*, liší-li se jeden od druhého pouze připojením nebo vynechání členů s koeficientem rovným nule. Je jasné, že jestliže mnohočleny $P(x_1, x_2, \ldots, x_k)$, $Q(x_1, x_2, \ldots, x_k)$ jsou v tomto smyslu totožné, nabývají oba téže číselné hodnoty při jakémkoli dosazení (9,2). Naproti tomu v opačném případě lze vždy za $x_1, x_2, \ldots, x_k$ dosadit taková čísla $\alpha_1, \alpha_2, \ldots, \alpha_k$, že

$$P(\alpha_1, \alpha_2, \ldots, \alpha_k) \neq Q(\alpha_1, \alpha_2, \ldots, \alpha_k); \qquad (9,3)$$

že tomu tak skutečně je, vyplývá z následující věty 9,1 (viz poznámku 9,1).

Mnohočlen $P(x_1, x_2, \ldots, x_k)$ nazveme *nulovým*, jsou-li všecky koeficienty rovny nule; jeho hodnota při libovolném dosazení je rovna 0. Předpokládejme však, že mnohočlen (9,1) není nulový a že $k \geqq 2$. Jestliže v (9,1) shrneme všecky ty členy, u kterých exponent při proměnné x_1 má touž hodnotu, uvedeme (9,1) na tvar

$$P(x_1, x_2, \ldots, x_k) = \sum_{r=0}^{n} p_r(x_2, \ldots, x_k)\, x_1^r , \tag{9,4}$$

kde při každém r je $p_r(x_2, \ldots, x_k)$ určitý mnohočlen $(k-1)$ proměnných $x_2, \ldots, x_k$; při tom se může stát, že pro některá r je $p_r(x_2, \ldots, x_k)$ nulový mnohočlen, je však zřejmé, že lze nezáporné celé číslo n právě jedním způsobem volit tak, že mnohočlen $p_n(x_2, \ldots, x_k)$, odpovídající nejvyšší hodnotě n indexu r, *není* nulový. Toto nezáporné celé číslo n nazveme *stupněm mnohočlenu* $P(x_1, x_2, \ldots, x_k)$ vzhledem k proměnné x_1.

Věta 9,1. *Budiž dán nenulový mnohočlen* $P(x_1, x_2, \ldots, x_k)$ *a budiž dána libovolná nekonečná množina* M *reálných čísel.* (Za M můžeme volit na př. množinu všech přirozených čísel, nebo množinu těch přirozených čísel, která jsou větší než libovolně dané přirozené číslo.) *Potom existují taková čísla*

$$\alpha_1 \in M,\ \alpha_2 \in M, \ldots, \alpha_k \in M ,$$

že $P(\alpha_1, \alpha_2, \ldots, \alpha_k) \neq 0$.

Důkaz provedeme indukcí vzhledem ke k. Je-li nejprve $k = 1$, má nenulový mnohočlen $P(x_1)$ určitý stupeň n a správnost naší věty v případě $k = 1$ je důsledkem věty 7,1. Předpokládejme nyní, že při určitém $k \geqq 2$ naše věta je správná pro mnohočleny $(k-1)$ proměnných; máme odvodit, že věta je správná také pro mnohočleny k proměnných. Budiž tedy $P(x_1, x_2, \ldots, x_k)$ nenulový mnohočlen k proměnných a budiž n jeho stupeň vzhledem k proměnné x_1, takže platí (9,4), při čemž mnohočlen $p_n(x_2, \ldots, x_k)$ není nulový. Podle předpokladu existují taková čísla

$$\alpha_2 \in M, \ldots, \alpha_k \in M , \tag{9,5}$$

že $p_n(\alpha_2, \ldots, \alpha_k) \neq 0$. Dosaďme do mnohočlenu $P(x_1, x_2, \ldots, x_k)$ za proměnné $x_2, \ldots, x_k$ čísla (9,5), ponechávajíce proměnnou x_1 volnou. Dostaneme

$$P(x_1, \alpha_2, \ldots, \alpha_k) = \sum_{r=0}^{n} p_r(\alpha_2, \ldots, \alpha_k)\, x_1^r ,$$

při čemž $p_n(\alpha_2, \ldots, \alpha_k) \neq 0$, t. j. $P(x_1, \alpha_2, \ldots, \alpha_k)$ je mnohočlen stupně n proměnné x_1, takže podle věty 7,1 je počet takových čísel

x_1, pro která je $P(x_1, \alpha_2, \ldots, \alpha_k) = 0$, nejvýš rovný n, takže je konečný; jelikož množina M je nekonečná, existuje takové číslo $\alpha_1 \in M$, že $P(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$, a to jsme měli dokázat.

Poznámka 9,1. Jsou-li $P(x_1, x_2, \ldots, x_k)$, $Q(x_1, x_2, \ldots, x_k)$ dva mnohočleny k proměnných $x_1, x_2, \ldots, x_k$, které nejsou totožné ve smyslu vysvětleném na str. 186, je jasné, že

$$P(x_1, x_2, \ldots, x_k) - Q(x_1, x_2, \ldots, x_k)$$

je nenulový mnohočlen, takže podle věty 9,1 můžeme za proměnné $x_1, x_2, \ldots, x_k$ dosadit taková čísla (9,2), že platí (9,3).

Věta 9,2. *Jsou-li $P(x_1, x_2, \ldots, x_k)$, $Q(x_1, x_2, \ldots, x_k)$ nenulové mnohočleny, je také $P(x_1, x_2, \ldots, x_k) \cdot Q(x_1, x_2, \ldots, x_k)$ nenulový mnohočlen. Jestliže vzhledem k proměnné x_1 má mnohočlen P stupeň n a mnohočlen Q stupeň m, má mnohočlen $P \cdot Q$ vzhledem k x_1 stupeň $n + m$.*

Důkaz. Pro $k = 1$ je nám to známo (viz větu 7,2). Nechť tedy $k > 1$ a nechť

$$P(x_1, \ldots, x_k) = \sum_{r=0}^{n} p_r(x_2, \ldots, x_k)\, x_1^r ,$$

$$Q(x_1, \ldots, x_k) = \sum_{s=0}^{m} q_s(x_2, \ldots, x_k)\, x_1^s ,$$

kde p_r, q_s jsou mnohočleny $k - 1$ proměnných, při čemž mnohočleny $p_n(x_2, \ldots, x_k)$, $q_m(x_2, \ldots, x_k)$ jsou nenulové. Potom je však

$$P(x_1, \ldots, x_k) \cdot Q(x_1, \ldots, x_k) = \sum_{t=0}^{m+n} u_t(x_2, \ldots, x_k)\, x_1^t ,$$

kde také u_t jsou mnohočleny $k - 1$ proměnných, při čemž

$$u_{n+m}(x_2, \ldots, x_k) = p_n(x_2, \ldots, x_k) \cdot q_m(x_2, \ldots, x_k) .$$

Je třeba pouze zjistit, že u_{n+m} není nulový mnohočlen. To plyne z věty 9,1, neboť podle této věty je možné udat $k - 1$ čísel $\alpha_2, \ldots, \alpha_k$ tak, že $p_n(\alpha_2, \ldots, \alpha_k) \neq 0$, $q_m(\alpha_2, \ldots, \alpha_k) \neq 0$, a pak je nutně také $u_{n+m}(\alpha_2, \ldots, \alpha_k) \neq 0$.

Stejně jako jsme definovali stupeň nenulového mnohočlenu $P(x_1, x_2, \ldots, x_k)$ vzhledem k proměnné x_1, můžeme ovšem definovat také stupeň vzhledem k jiné z k proměnných $x_1, x_2, \ldots, x_k$. Vedle těchto stupňů vzhledem k jednotlivým proměnným má však nenulový mnohočlen $P(x_1, x_2, \ldots, x_k)$ ještě také *celkový stupeň*. Než

vyslovíme obecnou definici tohoto pojmu, všimněme si jednoho zvláštního případu. Říkáme, že mnohočlen

$$P(x_1, x_2, \ldots, x_k) = \Sigma\, a_{r_1 \ldots r_k} x_1^{r_1} \ldots x_k^{r_k} \tag{9,6}$$

je *homogenní*, jestliže buďto je to nulový mnohočlen, nebo ve všech členech $a_{r_1 \ldots r_k} x_1^{r_1} \ldots x_k^{r_k}$, jejichž koeficient $a_{r_1 \ldots r_k}$ je různý od nuly, je součet všech exponentů

$$r_1 + r_2 + \ldots + r_k$$

roven jednomu a témuž číslu m, které nazveme *stupněm nenulového homogenního mnohočlenu*. Jestliže nyní $P(x_1, x_2, \ldots, x_k)$ je libovolný nenulový mnohočlen, je jasné, že existuje takové nezáporné celé m, že

$$P(x_1, x_2, \ldots, x_k) = \sum_{r=0}^{m} P_r(x_1, \ldots, x_k)\,, \tag{9,7}$$

kde pro každé r je $P_r(x_1, \ldots, x_m)$ homogenní mnohočlen, který je buďto nulový, nebo má stupeň r, kdežto mnohočlen $P_m(x_1, \ldots, x_k)$ nulový není. Je-li dán nenulový mnohočlen $P(x_1, \ldots, x_k)$, je patrné, že číslo m je určeno jednoznačně a že jsou jednoznačně určeny také všecky homogenní mnohočleny, které se vyskytují na pravé straně v (9,7). Číslo m je celkový stupeň mnohočlenu P a vyjádření (9,7) nazveme *rozkladem nenulového mnohočlenu P na homogenní části*.

Věta 9,3. *Jsou-li $P(x_1, x_2, \ldots, x_k)$, $Q(x_1, x_2, \ldots, x_k)$ nenulové mnohočleny, takže podle věty* 9,2 *také*

$$P(x_1, x_2, \ldots, x_k) \,.\, Q(x_1, x_2, \ldots, x_k) \tag{9,8}$$

je nenulový mnohočlen, je celkový stupeň mnohočlenu (9,8) *roven součtu celkových stupňů mnohočlenů P a Q.*

Důkaz. Buďtež m, m' celkové stupně mnohočlenů P, Q a buďtež (9,7) a

$$Q(x_1, x_2, \ldots, x_k) = \sum_{s=1}^{m'} Q_s(x_1, \ldots, x_k)$$

jejich rozklady na homogenní části. Pro každé celé t, pro něž $0 \leqq t \leqq m + m'$, budiž

$$u_t(x_1, \ldots, x_k) = \sum_{r+s=t} P_r(x_1, \ldots, x_k) \,.\, Q_s(x_1, \ldots, x_k)\,,$$

kde součet napravo se vztahuje na všecky ty dvojice $[r, s]$ nezáporných celých čísel, pro které je $r + s = t$. Je patrné, že pro každé

t je u_t homogenní mnohočlen, který je buďto nulový, nebo má stupeň rovný t, při čemž však mnohočlen

$$u_{m+m'}(x_1, \ldots, x_k) = P_m(x_1, \ldots, x_k) \cdot Q_{m'}(x_1, \ldots, x_k)$$

nulový není. Potom je však

$$\sum_{t=0}^{m+m'} u_t(x_1, \ldots, x_k)$$

rozklad mnohočlenu (9,8) na homogenní části, a tím je vše dokázáno.

Jsou-li dána nezáporná celá čísla $n_1, n_2, \ldots, n_k$, zní obecný tvar mnohočlenu $P(x_1, x_2, \ldots, x_k)$, jehož stupně vzhledem k jednotlivým proměnným $x_1, x_2, \ldots, x_k$ jsou rovny daným číslům $n_1, n_2, \ldots, n_k$, takto:

$$P(x_1, x_2, \ldots, x_k) = \sum_{r_1, r_2, \ldots, r_k} a_{r_1 r_2 \ldots r_k} x_1^{r_1} x_2^{r_2} \ldots x_k^{r_k}, \qquad (9,9)$$

kde součet na pravé straně se vztahuje na všecky ty k-tice

$$[r_1, r_2, \ldots, r_k] \qquad (9,10)$$

nezáporných celých čísel, pro které je

$$0 \leqq r_1 \leqq n_1, \; 0 \leqq r_2 \leqq n_2, \ldots, \; 0 \leqq r_k \leqq n_k .$$

Koeficienty $a_{r_1 r_2 \ldots r_k}$ jsou vázány pouze podmínkou, že nejsou všecky rovny nule.

Je jasné, že počet všech našich k-tic (9,10) je roven součinu

$$\prod_{r=1}^{k} (n_k + 1) .$$

Je-li dáno nezáporné celé číslo m, je (9,9) obecný tvar nenulového homogenního mnohočlenu stupně m, kde součet na pravé straně se vztahuje na všecky takové k-tice (9,10) nezáporných celých čísel, pro které je

$$r_1 + r_2 + \ldots + r_k = m \qquad (9,11)$$

a koeficienty $a_{r_1 \ldots r_k}$ splňují pouze tu podmínku, že nejsou všecky rovny nule. Podmínka (9,11) se liší od (5,12) pouze tím, že místo písmena n máme nyní písmeno k. Z toho plyne, že počet všech k-tic splňujících podmínku (9,11) je dán číslem

$$\binom{m + k - 1}{m} = \binom{m + k - 1}{k - 1} . \qquad (9,12)$$

Je-li dáno nezáporné celé číslo m, je (9,9) obecný tvar nenulového mnohočlenu celkového stupně m, kde součet na pravé straně se vztahuje na všecky takové k-tice (9,10) nezáporných celých čísel, pro které je

$$r_1 + r_2 + \ldots + r_k \leqq m\,; \tag{9,13}$$

při tom koeficienty $a_{r_1 r_2 \ldots r_k}$ splňují pouze tu podmínku, že nejsou rovny nule všecky ty z nich, pro něž platí rovnost (9,11). Počet všech k-tic splňujících nerovnost (9,13) je dán číslem

$$\binom{m+k}{m} = \binom{m+k}{k}, \tag{9,14}$$

které se liší od čísla (9,12) pouze tím, že místo k máme nyní $k+1$. Abychom se o tom přesvědčili, stačí uvážit, že každé k-tici (9,10) splňující nerovnost (9,13) můžeme přiřadit nezáporné celé číslo

$$r_0 = m - (r_1 + r_2 + \ldots + r_k)\,,$$

takže počet k-tic (9,10) splňujících nerovnost (9,13) je roven počtu všech $(k+1)$-tic

$$[r_0, r_1, \ldots, r_k],$$

splňujících rovnost

$$r_0 + r_1 + \ldots + r_k = m\,,$$

která se liší od (9,13) pouze tím, že počet sčítanců, který dříve byl roven k, je nyní roven $k+1$.