Obsah

1. Základní algebraické pojmy 2
2. Monoidové okruhy a některé další základní konstrukce 4
3. Podgrupy a jiné podstruktury 7
4. Kvocientní struktury 9
5. Homomorfismy 12
6. Věta o homomorfismu 15
7. Uspořádané množiny, svazy a kvaziuspořádání 18
8. Dělitelnost v komutativních monoidech 21
9. Obory integrity 24
10. Cyklické grupy 28
11. Grupy a jejich reprezentace 30
12. Torzní součiny 33
13. Uzavěrové systémy, svazy a algebry 38
14. Modulární, distributivní a komplementární svazy 42
15. Booleovy algebry 44
16. Podílové okruhy a tělesa 45
17. Existence kořenových a rozkladových nadtěles 48
18. Algebraické prvky a minimální polynomy 51
19. Jednoznačnost kořenových a rozkladových nadtěles 53

Rejstřík 55

1. Základní algebraické pojmy

Devatenácté století přineslo do matematiky pojmy tělesa, vektorového prostoru a grupy. Tyto pojmy patří dodnes k základním stavebním kamenům matematického jazyka. Jejich zobecňováním a zjednodušováním vznikly mnohé další důležité pojmy, z nichž některé budeme nyní definovat.

Pologrupa bude pro nás množina, řekněme M, spolu s binární operací $\cdot$, která splňuje rovnost $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro všechna $a, b, c \in M$ (tj. je asociativní).

Jinými slovy, pologrupa není nic jiného nežli dvojice, která se skládá z množiny (například M) a z binární operace na M (tedy zobrazení $M \times M \to M$). Pokud chceme pologrupu nějak označit, řekněme S, používáme zápisu $S = M(\cdot)$. Často se však používá pro označení pologrupy i její nosné množiny stejného písmene a píše se například $M = M(\cdot)$. Takový zápis je formálně sice diskutabilní, leč hojně rozšířený.

Monoid $M(\cdot, 1)$ je dán množinou M, binární operací $\cdot$ a konstantou $1 \in M$, pro které platí, že

(i) operace $\cdot$ je asociativní (takže $M(\cdot)$ je pologrupa),

(ii) $a \cdot 1 = a = 1 \cdot a$ je splněno pro všechna $a \in M$ (říkáme, že 1 je *neutrální* prvek operace $\cdot$).

Grupa $G(\cdot, ^{-1}, 1)$ je dána množinou G, binární operací $\cdot$, unární operací $^{-1}$ a konstantou $1 \in G$, pro které platí, že

(i) operace $\cdot$ je asociativní a 1 je neutrální prvek (takže $G(\cdot, 1)$ je monoid),

(ii) $a \cdot a^{-1} = 1 = a^{-1} \cdot a$ je splněno pro všechna $a \in M$ (říkáme, že a^{-1} je prvek *inverzní* vůči prvku a).

Okruh $R(+, \cdot, -, 0, 1)$ je dán množinou R, binárními operacemi $+$ a $\cdot$, unární operací $-$ a konstantami $0, 1 \in R$, pro které platí, že

(i) $R(+, -, 0)$ je grupa, přičemž binární operace $+$ je komutativní (tedy platí $a + b = b + a$ pro všechna $a, b \in R$),

(ii) $R(\cdot, 1)$ je monoid,

(iii) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ a $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ je splněno pro všechna $a, b, c \in R$ (platí levý a pravý distributivní zákon).

Těleso $T(+, \cdot, -, 0, 1)$ je okruh, který navíc splňuje tyto dvě podmínky:

(i) prvky $0 \in T$ a $1 \in T$ jsou různé,

(ii) pro všechna $a \in T$ různé od 0 lze nalézt inverzní prvek (tedy pro všechna $a \in T$, $a \neq 0$, existuje $b \in T$ takové, že je $a \cdot b = 1 = b \cdot a$).

Modulem A nad okruhem R se rozumí grupa $A(+, -, 0)$ spolu s operací skalárního násobení $R \times A \to A$ (tu budeme značit rovněž $\cdot$), která splňuje podmínky

(i) $a + b = b + a$ pro všechna $a, b \in A$,

(ii) $r \cdot (a + b) = (r \cdot a) + (r \cdot b)$ pro všechna $r \in R$ a $a, b \in A$,

(iii) $r \cdot (s \cdot a) = (r \cdot s) \cdot a$ pro všechna $r, s \in R$ a $a \in A$,

(iv) $(r + s) \cdot a = (r \cdot a) + (s \cdot a)$ pro všechna $r, s \in R$ a $a \in A$,

(v) $1 \cdot a = a$ pro všechna $a \in A$.

Uvedenou algebraickou strukturu bychom přesněji měli nazývat *levý modul* nad R. Někdy se skalární násobení píše zprava, a pak se hovoří o *pravém modulu* nad R.

Modul nad tělesem se nazývá *vektorový prostor*.

Pokud je binární operace násobení (operace $\cdot$) komutativní (platí $a \cdot b = b \cdot a$ pro všechna a, b), tak hovoříme o *komutativní* pologrupě (monoidu, grupě, okruhu, tělesu). Pracujeme-li pouze s jednou asociativní operací, a ta je komutativní, používáme většinou pro vyjádření této operace symbol sčítání $+$. Nekomutativní operace se označují $+$ jen velmi zřídka. Při aditivním zápisu se inverzní prvky obvykle nazývají prvky *opačné*. Komutativní grupa v aditivní notaci se obvykle nazývá *Abelova*.

Je samozřejmé, že pro dobré porozumění uvedeným pojmům je vhodné se seznámit s větším počtem konkrétních příkladů. Postupně budeme takové příklady uvádět, avšak dříve než k tomu přistoupíme, uvedeme několik jednoduchých vlastností binárních operací.

Ať $\cdot$ je binární operace na množině M.

Prvek $e \in M$ se nazývá *zleva neutrální* (nebo levou jednotkou), jestliže pro všechna $a \in M$ platí $e \cdot a = a$. Prvek $f \in M$ se nazývá *zprava neutrální* (nebo pravou jednotkou), jestliže pro všechna $a \in M$ platí $a \cdot f = a$.

1.1 Lemma. *Je-li $e \in M$ zleva neutrální a $f \in M$ zprava neutrální, tak $e = f$.*

Důkaz. Platí $f = e \cdot f = e$. □

Prvek $e \in M$ se nazývá *neutrální* (jednotka), jestliže je současně zleva i zprava neutrální. (Pojem neutrálního prvku je zmíněn již u definice monoidu, zde však nutně nepředpokládáme asociativní operaci.)

1.2 Důsledek. *Ke každé binární operaci lze nalézt nanejvýš jeden neutrální prvek.* □

Ať 1 je neutrální prvek binární operace $\cdot$ na M.

Prvek $a \in M$ se nazývá *zleva invertibilní*, jestliže existuje prvek $b \in M$, který splňuje $b \cdot a = 1$. Každý takový prvek b se nazývá *zleva inverzní* (vůči a). Obdobně definujeme *zprava invertibilní* a *zprava inverzní*.

Prvek $a \in M$ se nazývá *invertibilní*, jestliže existuje $b \in M$, které splňuje $b \cdot a = 1 = a \cdot b$. Přitom každý takový prvek b se nazývá *inverzní* (vůči a).

1.3 Lemma. *Ať $M(\cdot, 1)$ je monoid a $a \in M$. Jsou-li $b, c \in M$ takové, že platí $1 = b \cdot a = a \cdot c$, tak je $b = c$.*

Důkaz. Máme $b = b \cdot 1 = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 1 \cdot c = c$. □

1.4 Důsledek. *V každém monoidu má každý prvek nanejvýš jeden prvek inverzní.* □

Vraťme se nyní k definici monoidu a k definici grupy. Mluvíme-li o monoidu $M(\cdot, 1)$, může se zdát zbytečné, že v závorkách výslovně uvádíme neutrální prvek 1, který, jak víme z Lemmatu 1.1, je určen jednoznačně danou binární operací. Zřejmě je pravda, že binární operace grupy $G(\cdot, {}^{-1}, 1)$ jednoznačným způsobem určuje jak neutrální prvek 1, tak inverzní prvky a^{-1}, kde $a \in G$ (viz 1.4). Mohli bychom tedy mluvit pouze o grupě $G(\cdot)$. Někdy se tak skutečně činí, jsou však vážné důvody pro to, aby se grupa (či monoid) definovaly námi uvedeným způsobem. V dalších kapitolách tyto důvody podrobněji vysvětlíme. Nicméně jde o důvody formální, a pokud si jich jsme vědomi, není třeba se tímto rozdílem příliš zatěžovat. Podle potřeby pak můžeme považovat pologrupu s neutrálním prvkem za monoid, a monoid, jehož všechny prvky jsou invertibilní, za grupu.

Je-li T těleso, tak množina všech jeho nenulových prvků se často označuje T^*. Pro každé $a \in T^*$ existuje jednoznačně určený inverzní prvek a^{-1}, a $T^*(\cdot, {}^{-1}, 1)$ je grupa.

1.5 Lemma. *Ať $M(\cdot, 1)$ je monoid a ať $a, b, c, d \in M$ jsou takové, že c je zleva inverzní vůči a a d zleva inverzní vůči b. Potom je dc zleva inverzní vůči ab.*

Důkaz. Stačí ověřit, že $(dc)(ab) = d(ca)b = d \cdot 1 \cdot b = db = 1$. □

1.6 Důsledek. *Ať $G(\cdot, {}^{-1}, 1)$ je grupa a ať $a, b \in G$. Potom $(ab)^{-1} = b^{-1}a^{-1}$.* □

1.7 Lemma. *Ať $R = R(+, \cdot, -, 0, 1)$ je okruh. Pak pro libovolné $a, b \in R$ platí $a \cdot 0 = 0 \cdot a = 0$, $(-a)b = -(ab) = a(-b)$ a $(-a)(-b) = ab$.*

Důkaz. Z $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ plyne $a \cdot 0 = 0$, neboť k oběma stranám lze přičíst $-(a \cdot 0)$. Podobně máme $0 \cdot a = 0$, a tedy $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$. Odsud $(-a)b = -(ab)$, a podobně $-(ab) = a(-b)$. Konečně $ab = -(-ab) = -(a(-b)) = (-a)(-b)$. □

V okruzích je zvykem psát $a - b$ namísto $a + (-b)$. Mezi další běžná pravidla pro zjednodušení zápisu patří, že symbol násobení $\cdot$ se často vynechává, a že při zápisu závorek se používají obvyklé vztahy precedence.

2. Monoidové okruhy a některé další základní konstrukce

Budeme se zabývat zejména grupami, okruhy a částečně také moduly. Nejprve připomeneme několik dobře známých algebraických struktur a pak zmíníme některé konstrukce, jež umožňují konstruovat z jednodušších objektů objekty složitější. Mnohé významné algebraické objekty se přirozeným způsobem vyskytují jako podobjekty nebo kvocientní objekty zde uvedených konstrukcí. Úvahám o podobjektech a kvocientních objektech se budeme věnovat ale až později.

Ať je Ω nějaká množina. Identické zobrazení $x \mapsto x$ množiny Ω na sebe budeme značit id_Ω. Množina všech zobrazení $\Omega \to \Omega$ tvoří *transformační monoid* $T_\Omega = T_\Omega(\circ, id_\Omega)$ a množina všech bijektivních zobrazení $\Omega \to \Omega$ tvoří *symetrickou grupu* $S_\Omega = S_\Omega(\circ, {}^{-1}, id_\Omega)$. (Přitom operace $\circ$ značí skládání zobrazení; klademe $(f \circ g)(x) = f(g(x))$, takže skládáme zprava doleva.)

Grupa, monoid nebo okruh se nazývají *triviální*, pokud mají jediný prvek. Nejzákladnějším netriviálním komutativním monoidem je monoid všech nezáporných čísel $\mathbb{N}_0(+, 0)$, kde $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$. Dále platí, že $\mathbb{Z}(+, -, 0)$, kde $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, je Abelovou grupou.

Racionální čísla $\mathbb{Q}$, reálná čísla $\mathbb{R}$ a komplexní čísla $\mathbb{C}$ jsou příklady komutativních těles. Každé těleso $T(+, \cdot, -, 0, 1)$ poskytuje jednak Abelovou grupu $T(+, -, 0)$, jednak *multiplikativní grupu* $T^*(\cdot, {}^{-1}, 1)$.

Každé těleso je okruhem, mnohé okruhy však tělesem nejsou. Nejjednodušším takovým příkladem je okruh celých čísel $\mathbb{Z}(+, \cdot, -, 0, 1)$.

Ať R je nějaký okruh (lze si představovat třeba $\mathbb{Z}$ nebo $\mathbb{R}$). Pak $R\big[[x]\big]$ bude značit množinu všech (formálních) mocninných řad. Každá posloupnost $a_i, i \geq 0$, prvků z R určuje právě jednu mocninnou řadu $\sum a_i x^i$. Dvě mocninné řady $a = \sum a_i x^i$ a $b = \sum b_i x^i$ lze sčítat, $a + b = \sum (a_i + b_i) x^i$, a násobit, $a \cdot b = \sum c_k x^k$, kde $c_k = \sum_{i+j=k} a_i \cdot b_j$ pro všechna $k \geq 0$. Každý prvek $r \in R$ lze ztotožnit s mocninnou řadou $r \cdot x^0 + 0 \cdot x^1 + 0 \cdot x^2 + 0 \cdot x^3 + \ldots$, takže R můžeme považovat za podmnožinu $R\big[[x]\big]$. Je zřejmé, že $0 \in R$ je neutrálním prvkem pro sčítání a $1 \in R$ je neutrálním prvkem pro násobení. Ověříme známý fakt:

2.1 Lemma. *Násobení v $R\big[[x]\big]$ je asociativní.*

Důkaz. Ať je $a = \sum a_i x^i$, $b = \sum b_j x^j$ a $c = \sum c_k x^k$. Pak $(a \cdot b) \cdot c = \Big(\sum_r \Big(\sum_{i+j=r} a_i b_j\Big) x^r\Big) \cdot$ $\cdot \Big(\sum_k c_k x^k\Big) = \sum_m \Big(\sum_{r+k=m} \Big(\sum_{i+j=r} a_i b_j\Big) c_k\Big) x^m = \sum_m \Big(\sum_{i+j+k=m} a_i b_j c_k\Big) x^m =$ $\sum_m \Big(\sum_{i+s=m} a_i \Big(\sum_{j+k=s} b_j c_k\Big)\Big) x^m = \Big(\sum_i a_i x^i\Big) \cdot \Big(\sum_s \Big(\sum_{j+k=s} b_j c_k\Big) x^s\Big) = a \cdot (b \cdot c)$. □

Ke každé mocninné řadě $a = \sum a_i x^i$ definujeme $-a = \sum (-a_i) x^i$. Pak je zjevně $R\big[[x]\big]$ Abelovou grupou vůči $(+, -, 0)$ a monoidem vůči $(\cdot, 1)$. Pro $a = \sum a_i x^i$, $b = \sum b_j x^j$ a $c = \sum c_j x^j$ je $a \cdot (b + c) =$ $= \sum_k a_k \Big(\sum_{i+j=k} (b_i + c_j)\Big) x^k = \sum_k \Big(\Big(\sum_{i+j=k} a_i b_j\Big) + \Big(\sum_{i+j=k} a_i c_j\Big)\Big) x^k = \sum_k \Big(\sum_{i+j=k} a_i b_j\Big) x^k +$ $+ \sum_k \Big(\sum_{i+j=k} a_i c_j\Big) x^k = (a \cdot b) + (a \cdot c)$. Podobně obdržíme $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$. Dokázali jsme:

2.2 Tvrzení. *Buď R okruh. Potom množina všech mocninných řad $R\big[[x]\big]$ spolu s výše definovanými operacemi tvoří okruh.* □

Mocninná řada $a = \sum a_i x^i \in R\big[[x]\big]$ se nazývá *polynomem* (nad R), jestliže existuje $k \geq -1$, že $a_i = 0$ pro všechna $i > k$. Nejmenší takové k se nazývá *stupeň* polynomu a značí se $\deg a$. Množina všech polynomů nad R se značí $R[x]$.

2.3 Lemma. *Ať a, b jsou polynomy nad okruhem R. Pak $a + b$ i $a \cdot b$ jsou rovněž polynomy a platí* $\deg(a + b) \leq \max\{\deg a, \deg b\}$, a $\deg(a \cdot b) \leq \deg a + \deg b$.

Důkaz. Ať $a = \sum a_i x^i$ a $b = \sum b_j k^j$. Prvá nerovnost je zřejmá. Mějme $a \cdot b = \sum c_k x^k$. Je-li $k > \deg a + \deg b$, $i \geq 0, j \geq 0$ a $i + j = k$, tak je nutně $i > \deg a$ nebo $j > \deg b$, a tedy $a_i b_j =$ $= 0$ a $c_k = 0$. □

Z Lemmatu 2.3 plyne, že součet polynomů je polynom a násobek polynomů je také polynom, takže $R[x]$ je rovněž okruh. Přitom $M = \{x^i; i \geq 0\}$ je podmnožinou $R[x]$, která je uzavřená na násobení. Tato množina je vlastně monoid s neutrálním prvkem $x^0 = 1$, a každý prvek $R[x]$ lze chápat jako $\sum_{m \in M} a_m m$, kde $a_m \neq 0$ jen pro konečně mnoho $m \in M$. Sčítání a násobení při tomto zápisu lze vyjádřit takto:

$$\Big(\sum_{m \in M} a_m m\Big) + \Big(\sum_{m \in M} b_m m\Big) = \sum_{m \in M} (a_m + b_m) m$$

$$\left(\sum_{m\in M} a_m m\right)\cdot\left(\sum_{n\in M} b_n n\right)=\sum_{k\in M}\left(\sum_{m\cdot n=k} a_m b_n\right)k$$

Ať je nyní $M=M(\cdot,1)$ libovolný monoid, a ať je $R=R(+,\cdot,-,0,1)$ opět okruh. Pokud budeme chtít odlišit jednotky v M a R, budeme psát 1_M a 1_R. Položme $RM=\{\sum_{m\in M} a_m m;\ a_m\in R \text{ a } a_m\neq 0$ jen pro konečně mnoho $m\in M\}$ a definujme na RM sčítání a násobení výše uvedenými vzorci. Pro $a=\sum a_m m\in RM$ ať dále $-a=\sum(-a_m)m$.

Zastavme se na chvíli u podvojného významu sčítání v definici monoidového okruhu. Na jednu stranu říkáme, že monoidový okruh RM je tvořen všemi možnými součty s konečným nosičem (jen konečně mnoho sčítanců je nenulových), na druhou stranu na těchto součtech definujeme operaci sčítání. Není to samozřejmě nic neobvyklého, bez nějakého hlubšího uvažování například píšeme $(x^2+3x+2)+(x+5)=$ $=x^2+4x+7$, aniž bychom přemýšleli, které plus je konstitutivní (vytváří prvek $\mathbb{Z}[x]$) a které je operativní (vyjadřuje operaci). Přirozené je každé plus vnímat jako naznačenou operaci. Jenže pak můžeme mít potíže, jak vůbec popsat množinu polynomů. Jistě, je tady alternativní způsob, jak definovat polynomy — místo o formálních součtech bychom mohli hovořit o zobrazeních $\mathbb{N}_0\to R$, která mají konečný nosič (to jest jen konečně mnoho čísel má nenulovou hodnotu v R). Při takovém pojetí je například x^2+3x+2 reprezentováno zobrazením $a\colon\mathbb{N}_0\to R$, kde $a(0)=2$, $a(1)=3$, $a(2)=1$ a $a(i)=0$ pro každé $i\geq 3$. Stejně bychom mohli definovat RM — ne jako množinu všech formálních součtů $\sum a_m m$ s konečným nosičem, ale jako množinu všech zobrazení $a\colon M\to R$ s konečným nosičem. Výhodou takové definice je, že není třeba zvlášť upozorňovat na komutativitu formálních součtů (dva formální součty považujeme za shodné, jsou-li napsány v jiném pořadí — například $2+3x+x^2$ je totéž co x^2+3x+2), nevýhodou je odtrženost od obvyklého způsobu zápisu.

Běžně se mezi operativním a konstitutivním plus nerozlišuje. Ve zbytku této kapitoly to však učiníme, abychom se zbavili pochybností o tom, v jakém významu je to které sčítání použito. Konstitutivní sčítání budeme značit $\oplus$ a RM ztotožníme s množinou $\{\bigoplus_{m\in M} r_m m; r_m\in R \text{ a } m\in M, r_m\neq 0_R$ jen pro konečně mnoho $m\in M\}$. Přitom $\bigoplus r_m m$ se shoduje s $\bigoplus s_m m$, jestliže jednu (formální) sumu mohu obdržet z druhé záměnou pořadí a přidáváním či vypouštěním členů s nulovým koeficientem.

Naše výchozí definice tedy jsou
$(\bigoplus_m a_m m)+(\bigoplus_m b_m m)=\bigoplus_m(a_m+b_m)m$ a
$(\bigoplus_m a_m m)\cdot(\bigoplus_n b_n n)=\bigoplus_k(\sum_{k=m\cdot n} a_m b_n)k$.

Uvedeme nyní s komentářem několik jednoduchých vztahů.

(i) $\bigoplus_m a_m m=\sum_m a_m m$.

Tento vztah říká, že každý prvek RM lze získat součtem prvků, které mají nejvýše jeden koeficient nenulový.

(ii) $(am)\cdot(bn)=(ab)(mn)$

Je-li totiž v každém činiteli nejvýše jeden nenulový koeficient, je v součinu nanejvýš jeden sčítanec s nenulovým koeficientem.

Z (ii) vyplývá, že když ztotožníme každý prvek $r\in R$ s $r1_M$, stane se R částí RM (je totiž $(r1_M)+(s1_M)=(r+s)1_M$ a $(r1_M)\cdot(s1_M)=(r\cdot s)1_M$). Snadno nyní nahlédneme, že $0_{RM}=0_R 1_M$ je neutrální prvek pro sčítání a $1_{RM}=1_R 1_M$ je neutrální prvek násobení. Okamžitě rovněž vidíme, že je $a+(-a)=0$ pro všechna $a\in M$.

(iii) $(\bigoplus_m a_m m)\cdot(\bigoplus_n b_n n)=\sum_{m,n}(a_m b_n)(m\cdot n)$.

Tento vztah získáme z definice pomocí (i), neboť pro každé $k\in M$ je
$(\sum_{k=m\cdot n} a_m b_n)k=\sum_{k=m\cdot n}(a_m b_n)k=\sum_{k=m\cdot n}(a_m b_n)(m\cdot n)$
a zbytek plyne z asociativity sčítání.

(iv) Mějme $a=\bigoplus a_m m$, $b=\bigoplus b_n n$ a $c=\bigoplus c_k k$. Pak $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ a $(b+c)\cdot a=(b\cdot a)+(c\cdot a)$.

Stačí ověřit pouze prvý z obou distributivních zákonů. Podle (iii) máme $a\cdot(b+c)=\sum_{m,n}(a_m\cdot(b_n+c_n))$ $(m\cdot n)=\sum(a_m\cdot b_n+a_m\cdot c_n)(m\cdot n)=\sum_{m,n}(a_m b_n)(m\cdot n)+\sum_{m,n}(a_m\cdot c_n)(m\cdot n)=a\cdot b+a\cdot c$. Podobně ověříme $(a+b)\cdot c=a\cdot c+b\cdot c$.

2.4 Lemma. *Násobení v RM je asociativní.*

Důkaz. Ať $a=\bigoplus a_m m$, $b=\bigoplus b_n n$ a $c=\bigoplus c_k k$. Pak $(a\cdot b)\cdot c=(\sum_{m,n}(a_m\cdot b_n)(m\cdot n))\cdot c=$ $=\sum_{m,n,k}(a_m b_n c_k)(m\cdot n\cdot k)=a\cdot((\sum_{n,k} b_n c_k)(n\cdot k))=a\cdot(b\cdot c)$. □

2.5 Důsledek. *RM spolu s výše definovanými operacemi tvoří okruh.* □

Pozorovali jsme, že konstrukce *monoidového okruhu* RM v sobě zahrnují i konstrukci okruhu polynomů. Velkého uplatnění došly *grupové okruhy*, kdy na místě monoidu je grupa.

Z okruhu R lze rovněž odvodit pro každé $n \geq 1$ *maticový okruh* $M_n(R)$. Jeho prvky jsou matice (a_{ij}), $1 \leq i, j \leq n$, kde a_{ij} jsou prvky R. Nulou je nulová matice, jednotkou diagonální jednotková matice, opačný prvek je definován vztahem $(a_{ij}) = (-a_{ij})$, sčítání vztahem $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$ a násobení vztahem $(a_{ij}) \cdot (b_{jk}) = (\sum_j a_{ij} b_{jk})$.

3. Podgrupy a jiné podstruktury

V definicích dosud uvedených algebraických struktur se vyskytují binární a unární operace a konstanty. Obecně je *n-ární operace*, $n \geq 0$, *na množině* A zobrazení z A^n do A. Přitom A^0 se definuje jako jednoprvková množina $\{\emptyset\}$, a to pro každou množinu A (k takové definici jsou dobré důvody, neboť A^n lze interpretovat jako množinu všech zobrazení množiny $\{1, 2, \ldots, n\}$ do A), takže nulární operace je vlastně zobrazení jednoho prvku (to jest $\emptyset$) do A, čili vybrání prvku z A. Uvádíme-li při definici algebraické struktury nějakou konstantu, můžeme tedy tuto konstantu považovat za nulární operaci.

Je-li α nějaká n-ární operace na množině A, $n \geq 0$, tak o $B \subseteq A$ řekneme, že je *uzavřená* na α, pokud pro všechna $b_1, \ldots, b_n \in B$ platí $\alpha(b_1, \ldots, b_n) \in B$. Je-li A nějaká algebraická struktura (pologrupa, monoid, grupa, okruh, modul nebo vektorový prostor), tak $B \subseteq A$ je podstruktura této struktury (*podpologrupa, podmonoid, podgrupa, podokruh, podmodul, vektorový podprostor)*, jestliže B je uzavřena na všechny operace, které se vyskytují v definici dané struktury.

Tak například $\mathbb{N} = \{1, 2, 3, \ldots\}$ je podpologrupa pologrupy $\mathbb{N}_0(+)$, ale $\mathbb{N}$ není podmonoidem monoidu $\mathbb{N}_0(+, 0)$ (množina $\mathbb{N}$ totiž neobsahuje 0, takže není uzavřena na nulární operaci 0).

Dále $\mathbb{N}_0$ je podmonoidem $\mathbb{Z}(+, 0)$, ale $\mathbb{N}_0$ není podgrupou Abelovy grupy $\mathbb{Z}(+, -, 0)$. Podgrupou $\mathbb{Z}(+, -, 0)$ je ovšem množina všech sudých čísel $2\mathbb{Z}$. Přitom $2\mathbb{Z}$ je podpologrupou $\mathbb{Z}(\cdot)$, ale $2\mathbb{Z}$ není podmonoid $\mathbb{Z}(\cdot, 1)$.

U těles je situace trochu odlišná, neboť inverzní operace $^{-1}$ je definována pouze pro nenulové hodnoty. Říkáme, že $S \subseteq T$ je *podtěleso* tělesa T, jestliže S je podokruh okruhu T a pro všechna $a \in S$, $a \neq 0$, je $a^{-1} \in S$.

Těleso racionálních čísel $\mathbb{Q}$ je podtělesem $\mathbb{R}$ a $\mathbb{R}$ je podtěleso $\mathbb{C}$. Dále platí, že $\mathbb{Z} = \mathbb{Z}(+, \cdot, -, 0, 1)$ je podokruh $\mathbb{Q}$, ale $\mathbb{Z}$ není podtěleso $\mathbb{Q}$.

Je-li R okruh, tak okruh polynomů $R[x]$ je podokruhem okruhu formálních mocninných řad $R\big[[x]\big]$ (viz kapitola 2).

Je-li M modul nad R, tak $N \subseteq M$ je podmodul, jestliže N je podgrupa (tedy N je uzavřeno na $+$, $-$ a 0) a je uzavřeno na skalární násobení. Tuto skutečnost lze užít v souladu s naší obecnou definicí, jestliže na M hledím jako na Abelovu grupu, na které je definováno tolik unárních operací, kolik má okruh R prvků (čili na M může být definováno nekonečně mnoho unárních operací $-$ u levých modulů má každá taková operace tvar $a \mapsto ra$ pro nějaké $r \in R$).

Pokud mluvíme o nějaké algebraické podstruktuře B struktury A (o podpologrupě, podmonoidu, atd.), předpokládáme, že B označuje podmnožinu množiny A spolu se všemi operacemi, které získáme zúžením operací z množiny A na tuto podmnožinu. Je tedy korektnější uvádět, že podmonoidem $\mathbb{Z}(+, 0)$ je $\mathbb{N}_0(+, 0)$, nikoliv pouze $\mathbb{N}_0$. Pokud ale nehrozí nedorozumění, tak se obvykle dává přednost kratšímu, byť diskutabilnímu, zápisu.

Ve zbytku této kapitoly se zaměříme na ekvivalence spojené s podgrupami dané grupy.

Připomeňme, že ekvivalence, řekněme ρ, na množině A je relace, která je reflexivní, symetrická a tranzitivní (tedy pro všechna $a, b, c \in A$ platí $a\rho a$, dále $a\rho b \Rightarrow b\rho a$ a $a\rho b, b\rho c \Rightarrow a\rho c$).

Je-li ρ ekvivalence na A, tak pro každé $a \in A$ klademe $[a]_\rho = \{b \in A; a\rho b\}$. Z vlastností ekvivalence plyne, že je jednak $A = \bigcup([a]_\rho; a \in A)$, jednak pro všechna $a, b \in A$ platí $[a]_\rho \cap [b]_\rho \neq \emptyset \iff [a]_\rho = [b]_\rho \iff a\rho b$. Každá množina $[a]_\rho$ se nazývá *blok* ekvivalence ρ, a množinu všech bloků $\{[a]_\rho; a \in A\}$ označíme A/ρ. Budeme potřebovat toto jednoduché lemma:

3.1 Lemma. *Ať λ je ekvivalence na A, ρ relace na B, $\varphi\colon A \to B$ bijektivní zobrazení, a ať pro všechna $a, b \in A$ platí*

$$a\lambda b \iff \varphi(a)\rho\varphi(b).$$

Potom ρ je ekvivalence na B, $[\varphi(a)]_\rho = \varphi([a]_\lambda)$ pro každé $a \in A$, a $[a]_\lambda \mapsto [\varphi(a)]_\rho$ je korektně definované zobrazení $A/\lambda \to B/\rho$. Toto zobrazení je bijektivní.

Důkaz. Každé $c \in B$ lze jediným způsobem zapsat jako $\varphi(a), a \in A$. Proto z $a\lambda a$ plyne $c\rho c$, a podobně se snadno ověří, že ρ je i symetrická a tranzitivní relace. Přitom $d = \varphi(b)$ padne do $[c]_\rho = [\varphi(a)]_\rho$ právě když je $d\rho c$, čili právě když $b\lambda a$, neboli $b \in [a]_\lambda$. Proto vskutku je $[\varphi(a)]_\rho = \varphi([a]_\lambda)$. To znamená, že pro $a\lambda b$ je $[\varphi(a)]_\rho = [\varphi(b)]_\rho$, takže zobrazení $\Phi\colon A/\lambda \to B/\rho$, které zobrazuje $[a]_\lambda$ na $[\varphi(a)]_\rho$, je korektně definované (jinými slovy hodnota $\Phi([a]_\lambda)$ vskutku závisí pouze na bloku $[a]_\lambda$, nikoliv na volbě reprezentanta tohoto bloku).

Položíme-li $\psi = \varphi^{-1}$, tak platí $c\rho d \iff \psi(c)\lambda\psi(d)$, takže podobně můžeme zkonstruovat zobrazení $\Psi\colon B/\rho \to A/\lambda$, které zobrazuje $[c]_\rho$ na $[\psi(c)]_\lambda$. Zbývá ověřit, že Ψ a Φ jsou vzájemně inverzní. To je však snadné, neboť $\Psi\Phi([a]_\lambda) = [\psi\varphi(a)]_\lambda = [a]_\lambda$ pro všechna $a \in A$, a $\Phi\Psi([c]_\rho) = [c]_\rho$ pro všechna $c \in B$. □

Je-li G grupa a A, B jsou její podmnožiny, tak klademe $AB = \{ab; a \in A \text{ a } b \in B\}$. Jsou-li a, b prvky G, tak místo $\{a\}B$ píšeme též aB a místo $A\{b\}$ píšeme též Ab. Zápisu A^{-1} používáme pro označení množiny $\{a^{-1}; a \in A\}$.

Uvažme nyní nějakou grupu G a její podgrupu H. Definujme relace λ a ρ na G tak, že pro $a, b \in G$ je $a\lambda b \iff a^{-1}b \in H$ a $a\rho b \iff ab^{-1} \in H$.

3.2 Lemma. *Relace λ je ekvivalence na G a pro každé $a \in G$ platí $[a]_\lambda = aH$.*

Důkaz. Mějme $a, b, c \in G$. Z $1 \in H$ plyne $a\lambda a$. Je-li $a\lambda b$, tak padne $a^{-1}b$ do H, a tedy i $(a^{-1}b)^{-1} = b^{-1}a \in H$. Proto $a\lambda b$ implikuje $b\lambda a$. Z $a\lambda b$ a $b\lambda c$, což znamená $a^{-1}b \in H$ a $b^{-1}c \in H$, dostáváme $(a^{-1}b) \cdot (b^{-1}c) = a^{-1}c \in H$, takže je $a\lambda c$. Dokázali jsme, že λ je ekvivalence. Je-li $b \in [a]_\lambda$, tak je b rovno $a \cdot (a^{-1}b) \in aH$. Naopak pro $b = ah$, $h \in H$, je jistě $a\lambda b$, a tedy $b \in [a]_\lambda$. Dokázali jsme $[a]_\lambda = aH$. □

3.3 Lemma. *Pro $a, b \in G$ platí $a\lambda b$ právě když je $a^{-1}\rho b^{-1}$.*

Důkaz. Máme $a\lambda b \iff a^{-1}b = a^{-1}(b^{-1})^{-1} \in H \iff a^{-1}\rho b^{-1}$. □

Označme nyní na chvíli zobrazení $a \mapsto a^{-1}$ jako φ. Je $\varphi: G \to G$ a $\varphi^2 = id_G$, takže φ je nutně bijekce. Podle 3.3 a 3.1 můžeme z 3.2 odvodit, že relace ρ je ekvivalence a pro každé $a \in G$ platí $[a]_\rho = [\varphi(\varphi(a))]_\rho = \varphi([\varphi(a)]_\lambda) = (a^{-1}H)^{-1} = (H^{-1})a = Ha$. Vlastnosti relace ρ lze samozřejmě odvodit přímo, stejným postupem jako v 3.2, bez užití 3.1. Co nám ale poskytuje 3.1 důležitého, je bijekce G/λ a G/ρ, která je dána (například) zobrazením $aH \mapsto Ha^{-1}$.

Společná mohutnost množin A/λ a A/ρ se nazývá *index* podgrupy H (v grupě G) a značí se $|G{:}H|$.

Bloky $[a]_\lambda = aH$ se nazývají *levé (rozkladové) třídy* H v G a bloky $[a]_\rho = Ha$ se nazývají *pravé (rozkladové) třídy* H v G.

Pro každé $a \in G$ definujeme zobrazeni $L_a: G \to G$ a $R_a: G \to G$ tak, že $L_a(b) = a \cdot b$ a $R_a(b) = b \cdot a$, pro každé $b \in G$. Zobrazení L_a se nazývá *levá translace* prvku a, zobrazení R_a je *pravá translace* prvku a.

3.4 Lemma. *Zobrazení L_a i R_a jsou permutace G.*

Důkaz. Dokažme, například, že L_a je permutace. Pro každé $b \in G$ je $L_a L_{a^{-1}}(b) = a(a^{-1}b) = b = a^{-1}(ab) = L_{a^{-1}} L_a(b)$ takže $L_a L_{a^{-1}} = id_G = L_{a^{-1}} L_a$, a odsud plyne $L_{a^{-1}} = (L_a)^{-1}$, takže L_a musí být permutace. □

Protože $aH = L_a(H)$ a L_a je bijekce, tak vidíme, že levá rozkladová třída aH má pro každé $a \in G$ stejnou mohutnost jako H.

Mohutnost grupy je zvykem nazývat *řád* a značit $|G|$, $|H|$ apod.

Vidíme, že v ekvivalenci λ je $|G{:}H|$ bloků, a každý z těchto bloků má mohutnost $|H|$. Proto řád grupy G musí být roven $|G{:}H| \cdot |H|$. Tento vztah je znám jako

3.5 Lagrangeova věta. *Pro každou podgrupu H grupy G platí $|G| = |H| \cdot |G{:}H|$.*

3.6 Důsledek. *Ať G je konečná grupa a H její podgrupa. Pak $|H|$ dělí $|G|$.* □

3.7 Tvrzení. *Buď G grupa a H její podgrupa. Následující podmínky jsou ekvivalentní:*
(i) $ghg^{-1} \in H$ pro každé $h \in H$ a $g \in G$,
(ii) $gH = Hg$ pro každé $g \in G$.

Důkaz. Prvou podmínku lze zapsat též jako $gHg^{-1} \subseteq H$ pro všechna $g \in G$. Jelikož g probíhá všechna $g \in G$, platí tedy i $g^{-1}Hg \subseteq H$, což však dává $H \subseteq gHg^{-1}$, takže prvá podmínka je ekvivalentní vztahu $gHg^{-1} = H$, což lze zapsat též jako $gH = Hg$, pro všechna $g \in G$. □

Podgrupa H grupy G se nazývá *normální*, jestliže splňuje podmínky Tvrzení 3.7. Vidíme, že H je normální, právě když ekvivalence λ a ρ splývají.

4. Kvocientní struktury

Na základní škole se děti učí zlomky. To budeme také dělat, ale o něco později. Zatím si ze zlomků vypůjčíme jenom tu nesamozřejmou zkušenost, že jeden a týž prvek může mít více jmen (například $\frac{2}{3}$, $\frac{4}{6}$ či $\frac{-12}{-18}$). Někdy se dá rozhodnout, které z těch jmen je nejlepší (a tak je tomu i u běžných číselných zlomků), ale lze si představit i takové systémy, kde chybí kritérium, podle kterého lze vybrat z mnoha možných označení to, jež by bylo nějak nejlepší. V takové situaci se dá postupovat tak, že nebudeme trvat na nějakém kanonickém zápisu, ale prostě prohlásíme všechna vyjádření za stejně dobrá. Prvkem v dané struktuře pak nebude nějaký privilegovaný zápis (například $\frac{2}{3}$), ale množina všech přípustných zápisů (tedy $\{\dots \frac{-4}{-6}, \frac{-2}{-3}, \frac{2}{3}, \frac{4}{6}, \dots\}$). U racionálních čísel tedy uvažujeme všechny jejich zápisy celočíselnými zlomky, což lze pokládat za množinu dvojic $\mathbb{Z} \times \mathbb{Z}^{\#}$, kde $\mathbb{Z}^{\#} = \mathbb{Z} \setminus \{0\}$, a tuto množinu rozdělíme do tříd, kde dvojice (r, s) a (u, v) padnou do téže třídy právě když $rv = su$.

Konstrukce podobného typu jsou v matematice zásadního významu. V mnoha případech spočívá nejefektivnější způsob konstrukce nějaké struktury v tom, že nejprve zkonstruujeme strukturu volnější, ve které je snazší dávat jména (tedy je snazší přesně popsat prvky takové struktury), a z této volnější struktury dostaneme strukturu novou ztotožněním některých jmen. Ztotožněním pak míníme, že volnější strukturu rozdělíme do tříd podle nějaké ekvivalence a za prvky nové struktury považujeme bloky této ekvivalence. Přitom každá třída této ekvivalence je určena svým libovolným reprezentantem, takže je třeba myšlenkově zvládnout přechod mezi ekvivalenčními třídami (bloky) a jejich reprezentanty. Například často se nějaké zobrazení nebo operace týkající se struktury tvořené bloky dané ekvivalence definuje pomocí reprezentantů těchto bloků. Přitom se obvykle musí ověřit, že tato definice je *korektní* — tedy, že hodnota zobrazení nebo výsledek operace bude stejný, jestliže nějaký reprezentant určitého bloku je nahrazen reprezentantem téhož bloku.

Nová struktura definovaná pomocí ekvivalence z volnější struktury se nazývá jejím *kvocientem*. Účelnost takové definice nové struktury je tím vyšší, čím více vlastností a operací mohu nějakým způsobem přenést z volnější struktury (kde se třeba tyto vlastnosti snáze ověřují a operace snáze definují). V této kapitole se budeme zejména zabývat přenosem operací na kvocientní struktury. (Kvocientním strukturám se říká také faktorstruktury, takže — jinými slovy — naším tématem je *faktorizace operací*.)

Ať α je n-ární operace na množině A, $n \geq 0$, a ať ρ je ekvivalence na A. Převést operaci α na A/ρ je zjevně možné jenom tehdy, jestliže „blok výsledku operace závisí pouze na blocích argumentů“.

Tuto vlastnost nyní symbolicky popíšeme a pojmenujeme. Ekvivalence ρ se nazývá *slučitelná* s operací α, jestliže pro všechna $a_1, \dots, a_n \in A$ a pro všechna $b_1, \dots, b_n \in A$ z $a_1 \rho b_1, \dots, a_n \rho b_n$ plyne $\alpha(a_1, \dots, a_n) \rho \alpha(b_1, \dots, b_n)$.

Je-li ρ slučitelné s α, definujeme operaci α na A/ρ (přitom pro lepší srozumitelnost použijeme označení $\alpha_{A/\rho}$ a α_A) pro všechna $a_1, \dots, a_n \in A$ takto: $\alpha_{A/\rho}([a_1]_\rho, \dots, [a_n]_\rho) = [\alpha_A(a_1, \dots, a_n)]_\rho$.

4.1 Lemma. *Je-li α operace na A a ρ ekvivalence na A, která je slučitelná s α, tak výše uvedený vztah poskytuje korektní definici operace α na A/ρ.*

Důkaz. Ať $A_1, \dots, A_n$ jsou bloky ρ, přičemž je $a_1 \in A_1, \dots, a_n \in A_n$ a $b_1 \in A_1, \dots, b_n \in A_n$. Definice bude korektní, jestliže $[\alpha_A(a_1, \dots, a_n)]_\rho$ je v takové situaci vždy rovno $[\alpha_A(b_1, \dots, b_n)]_\rho$. To je však právě podmínkou slučitelnosti, kterou předpokládáme. □

Je-li dána nějaká algebraická struktura, která pracuje s jistými operacemi, tak ekvivalenci na této struktuře, jež je slučitelná se všemi těmito operacemi, nazýváme její *kongruencí*.

Ať G je grupa. Je-li N normální podgrupa G, je zvykem ekvivalenci určenou rozkladovými třídami N značit $\bmod N$. Místo $(a, b) \in \bmod N$ se často píše $a \equiv b \bmod N$.

4.2 Tvrzení. *Buď $G = G(\cdot, {}^{-1}, 1)$ grupa. Je-li N normální podgrupa G, tak $\bmod N$ je kongruence G. Naopak, je-li ρ kongruence G, tak $N = [1]_\rho$ je normální podgrupa G a ρ se shoduje s $\bmod N$.*

Důkaz. Ať N je normální podgrupa a ať je $a \equiv b \bmod N$ a $c \equiv d \bmod N$ pro nějaká $a, b, c, d \in G$. Je tedy $h = a^{-1}b \in N$ a $k = c^{-1}d \in N$. Protože N je normální podgrupa G, je i $h' = c^{-1}hc \in N$. To znamená, že $(ac)^{-1}(bd) = c^{-1}a^{-1}bd = c^{-1}hcc^{-1}d = h'k \in N$, takže $\bmod N$ je slučitelné s násobením. Protože je i $ab^{-1} \in N$, je také $a^{-1} \equiv b^{-1} \bmod N$, takže $\bmod N$ je slučitelné s unární operací ${}^{-1}$. Vidíme, že $\bmod N$ je vskutku kongruence.

Naopak, ať ρ je kongruence grupy G. Položme $N = [1]_\rho$. Je-li $a, b \in N$, tak z $a \rho 1$ a $b \rho 1$ plyne $(a \cdot b) \rho (1 \cdot 1)$, tedy $ab \in N$. Podobně též $(a^{-1}) \rho (1^{-1})$ dává $a^{-1} \in N$, takže vidíme, že N je podgrupa. Jsou-li $g \in G$ a $h \in N$, je $(g \cdot h \cdot g^{-1}) \rho (g \cdot 1 \cdot g^{-1})$, a z $g \cdot 1 \cdot g^{-1} = 1$ plyne $ghg^{-1} \in N$. Dokázali jsme, že N

je normální podgrupa grupy G. Z $a \equiv b \bmod N$ plyne $ab^{-1} \in N$, tedy $(ab^{-1})\rho 1$ a $(ab^{-1}b)\rho(1 \cdot b)$, což znamená $a\rho b$. Naopak, z $a\rho b$ máme $(ab^{-1})\rho 1$, odkud $a \equiv b \bmod N$. □

Je-li ρ kongruence nějakého algebraického systému, řekněme A, tak na kvocientní struktuře A/ρ je možné definovat všechny operace systému A. Splňují-li operace na A jisté identity (asociativní zákon, distributivní zákon a podobně), budou tytéž identity splněny i v kvocientní struktuře. Faktorizací podle kongruence z grupy dostaneme opět grupu (říkává se jí *faktorgrupa*), z okruhu *faktorokruh*, z modulu *faktormodul* a podobně.

Protože kongruence, řekněme ρ, grupy G je jednoznačně určena blokem $N = [1]_\rho$, který je normální podgrupou, píšeme místo G/ρ obvykle G/N. Prvky G/N jsou rozkladové třídy $aN = Na$, přičemž platí $(aN) \cdot (bN) = (ab)N$, $(aN)^{-1} = a^{-1}N$ a $1_{G/N} = 1 \cdot N = N$.

Ať $R = R(+, \cdot, -, 0, 1)$ je okruh. O množině $I \subseteq R$ řekneme, že je *levý ideál* okruhu R, jestliže
(i) $I(+, -, 0)$ je podgrupa $R(+, -, 0)$ a
(ii) pro každé $r \in R$ a každé $a \in I$ je $ra \in I$.

Pokud místo (ii) požadujeme
(ii′) pro každé $r \in R$ a každé $a \in I$ je $ar \in I$,

tak mluvíme o *pravém ideálu*. Je-li $I \subseteq R$ současně levý a pravý ideál, tak se nazývá (oboustranný) *ideál*.

V Abelově grupě je každá podgrupa normální, proto je ekvivalence $\bmod N$ definovaná pro každé $N \subseteq R$, které je podgrupou $R(+, -, 0)$. Přitom $a \equiv b \bmod N$ právě když $a - b \in N$.

4.3 Tvrzení. *Buď $R = R(+, \cdot, -, 0, 1)$ okruh. Je-li $I \subseteq R$ ideál, tak $\bmod I$ je kongruence okruhu R. Naopak, je-li ρ kongruence R, tak $I = [0]_\rho$ je ideál R a ρ se shoduje s $\bmod I$.*

Důkaz. Ať I je ideál. Z 4.2 plyne, že $\bmod I$ je slučitelné s operacemi $+$ a $-$. Zbývá ukázat, že pro $a \equiv b \bmod I$ a $c \equiv d \bmod I$ je $ac \equiv bd \bmod I$. Ovšem $ac - bd = a(c - d) + (a - b)d$, přičemž $a - b \in I$ a $c - d \in I$. Protože I je ideál, jsou i oba sčítance v I, takže vskutku je $ac \equiv bd \bmod I$.

Ať je naopak ρ kongruence R. Položme $I = [0]_\rho$. Protože ρ je také kongruence $R(+, -, 0)$, musí být ρ rovno $\bmod I$, dle 4.2. Zbývá ukázat, že I splňuje podmínky (ii) a (ii′). Dokažme například (ii). Je-li $a \in I$ a $r \in R$, tak z $a\rho 0$ a $r\rho r$ plyne $ra\rho 0$, neboť $0 = r \cdot 0$, takže je $ra \in I$. □

4.4 Lemma. *Ať I a J jsou ideály okruhu R. Pak $I + J = \{a + b; a \in I \text{ a } b \in J\}$ je nejmenší ideál okruhu R, který obsahuje $I \cup J$.*

Důkaz. Součet prvků z $I + J$ leží v $I + J$ díky komutativitě sčítání. Je-li $a \in I$ a $b \in J$, je $r \cdot (a + b) = = ra + rb \in I + J$ pro každé $r \in R$. Podobně pro násobení zprava. □

Vidíme, že Lemma 4.4 platí také pro jednostranné ideály, ať už levé nebo pravé. Rovněž je zřejmé, že pro každé $a \in R$ je $aR = \{ar; r \in R\}$ pravý ideál a Ra levý ideál. Takové ideály se nazývají *hlavní*. V komutativním okruhu levé a pravé ideály splývají. Okruh R se nazývá *okruhem hlavních ideálů*, jestliže je komutativní a každý jeho ideál je hlavní. V okruhu R lze nalézt vždy ideál R a ideál $\{0\}$; ten se většinou píše pouze 0. Ideálům R a 0 se říká *nevlastní*, ostatní ideály jsou *vlastní*.

4.5 Tvrzení. *Každý ideál I okruhu $\mathbb{Z}$ je roven hlavnímu ideálu $n\mathbb{Z}$ pro nějaké $n \geq 0$.*

Důkaz. Je-li $I = 0$, položíme $n = 0$. Ať je I nenulový ideál a ať m je nejmenší kladné číslo obsažené v I. Potom je jistě $m\mathbb{Z} \subseteq I$. Dokážeme i opačnou inkluzi. Ať je $a \in I$. Pak existují celá q a r, která splňují $a = mq + r$ a $0 \leq r < m$. Z $a \in I$ a $mq \in I$ plyne $r = a - mq \in I$. Z definice m vyplývá, že nemůže být $0 < r < m$, a proto je $r = 0$, takže a vskutku patří do $n\mathbb{Z}$. □

Jednostranný ideál okruhu R, který obsahuje 1, je zřejmě roven R. Prvek a okruhu R je tudíž zleva (nebo zprava) invertibilní, právě když platí $R = Ra$ (nebo $R = aR$). Vidíme, že těleso lze charakterizovat jako okruh, který není triviální a nemá vlastní jednostranný ideál.

Je-li I ideál okruhu R a ρ je kongruence $\bmod I$, tak — podobně jako v grupách — faktorokruh R/ρ označujeme R/I. Ideál I se nazývá *maximální*, je-li různý od R a není-li vlastní podmnožinou nějakého vlastního ideálu.

4.6 Tvrzení. *Buď R komutativní okruh a ať I je jeho maximální ideál. Potom je R/I komutativní těleso.*

Důkaz. Okruh R/I je tvořen množinami $a + I$, kde $a \in R$, přičemž množina I má roli nulového prvku. Je třeba dokázat, že $a + I$ je invertibilní pro každé $a \notin I$. Podle 4.4 je $Ra + I$ ideál, a z maximality I plyne

$Ra + I = R$. Znamená to, že $1 = ba + c$ pro nějaké $b \in R$ a $c \in I$, takže $(b + I)(a + I) = ba + I = 1 + I$. Jelikož $1 + I$ je jednotkovým prvkem R/I, je důkaz u konce. □

Pro celá čísla $n \geq 0$ a $m \geq 0$ zjevně platí $n\mathbb{Z} \subseteq m\mathbb{Z}$ právě když m dělí n, čili $n\mathbb{Z}$ je maximální ideál $\mathbb{Z}$ právě když n je prvočíslo. Podle 4.6 je $\mathbb{Z}/p\mathbb{Z}$ těleso.

Místo $\bmod n\mathbb{Z}$ se tradičně píše pouze $\bmod n$ a blokům ekvivalence $\bmod n$ se říká *zbytkové třídy*. Pokud je z každé zbytkové třídy vybrán právě jeden prvek, mluví se často o *úplné soustavě reprezentantů*. Zde použijeme kratší označení *transversála* (česky by se mohlo říkat příčnice). Obecně vzato, transversálou ekvivalence ρ na množině A je každá podmnožina T množiny A, která má jednobodový průnik s každým blokem B ekvivalence ρ. Označme tento prvek $\sigma_T(B)$. Pak σ_T je bijekcí A/ρ na T.

Je-li α nějaká n-ární operace na A/ρ a T je transversála ρ, tak můžeme na T definovat operaci α vztahem $\alpha(t_1, \ldots, t_n) = \sigma_T(\alpha(\sigma_T^{-1}(t_1), \ldots, \sigma_T^{-1}(t_n)))$, pro všechna $t_1, \ldots, t_n \in T$. Jinými slovy, výsledek operace α na T je ten prvek T, který leží v tom bloku ρ, jenž je výsledkem operace α aplikované na bloky obsahující $t_1, \ldots, t_n$. Právě definované operaci α na T se říká operace *indukovaná* transversálou T. Je-li A nějaký algebraický systém (například okruh nebo grupa) a ρ je kongruence A, která má transversálu T, tak veškeré operace A se promítají do operací A/ρ, a ty indukují operace na T. Algebraické systémy A/ρ a T se liší jen pojmenováním (můžeme si to představovat tak, že každý blok B ekvivalence ρ se stáhne do bodu $\sigma_T(B)$). Je-li A grupa, bude tedy T rovněž grupa, je-li A okruh, bude T okruh, a podobně.

Nejčastěji používanou transversálou $\bmod n$ je $\{0, 1, 2 \ldots, n-1\}$. Okruh indukovaný touto transversálou budeme značit $\mathbb{Z}_n$. (Například v $\mathbb{Z}_7$ platí $5 + 3 = 1 = 5 \cdot 3$.)

Na závěr této kapitoly ještě zmíníme faktorizaci modulů. Je-li A (levý) modul okruhu R a ρ je kongruence A (to jest ρ je kongruence Abelovy grupy $A(+, -, 0)$ a pro všechna $a, b \in A$ a všechna $r \in R$ z $a \rho b$ plyne $ra \,\rho\, rb$), tak jistě $B = [0]_\rho$ je podgrupa $A(+, -, 0)$ a $\rho = \bmod B$. Pro $b \in B$ a $r \in R$ máme $r \cdot b \,\rho\, r \cdot 0$, a tedy $rb \in B$. To znamená, že B musí být podmodul A. Je-li naopak B podmodul A, tak pro všechna $r \in R$ a $a, b \in A$ z $a - b \in B$ plyne $r(a - b) = ra - rb \in B$, a tedy $ra \equiv rb \bmod B$.

Vidíme, že kongruence modulů jsou charakterizovány jejich podmoduly, a že tedy pro každý podmodul B modulu A lze sestrojit faktormodul A/B. Všimněte si, že konstrukce je stejná jako ta, kterou znáte z vektorových prostorů.

5. Homomorfismy

Ať A a B jsou množiny, a ať α je n-ární operace, $n \geq 0$, která je zadána jak na A, tak na B. O zobrazení $f\colon A \to B$ řekneme, že je *slučitelné* s α, jestliže pro libovolná $a_1, a_2, \ldots, a_n \in A$ platí

$$\alpha_B(f(a_1), \ldots, f(a_n)) = f(\alpha_A(a_1, \ldots, a_n)).$$

Jinými slovy, výsledek operace na obrazech argumentů se shoduje s obrazem výsledku operace. A ještě jinak: pokud operaci α aplikuji v B pouze na hodnotách z $\operatorname{Im} f = \{f(a); a \in A\}$, tak operaci mohu použít nejprve v A a teprve poté zobrazit její výsledek.

5.1 Lemma. *Ať α je n-ární operace definovaná na množinách A, B, C a ať $f\colon A \to B$ a $g\colon B \to C$ jsou zobrazení slučitelná s α. Potom $g \circ f\colon A \to C$ je rovněž zobrazení slučitelné s α.*

Důkaz. Buďte $a_1, \ldots, a_n \in A$. Pak $\alpha_C(g(f(a_1)), \ldots, g(f(a_n))) = g(\alpha_B(f(a_1), \ldots, f(a_n))) = (g \circ f)(\alpha_A(a_1, \ldots, a_n))$. □

5.2 Lemma. *Ať α je n-ární operace definovaná na množinách A a B, a ať $f\colon A \to B$ je bijektivní zobrazení slučitelné s α. Potom $f^{-1}\colon B \to A$ je rovněž zobrazení slučitelné s α.*

Důkaz. Ať jsou $b_1, \ldots, b_n$ nějaké prvky B. Pak existují (jednoznačně určené) prvky $a_1, \ldots, a_n$ množiny A, že $b_1 = f(a_1), \ldots, b_n = f(a_n)$. Přitom platí $f(\alpha_A(f^{-1}(b_1), \ldots, f^{-1}(b_n))) = f(\alpha_A(a_1, \ldots, a_n)) = \alpha_B(f(a_1), \ldots, f(a_n)) = \alpha_B(b_1, \ldots, b_n)$, což znamená $f^{-1}(\alpha_B(b_1, \ldots, b_n)) = \alpha_A(f^{-1}(b_1), \ldots, f^{-1}(b_n))$. □

Je-li $f\colon A \to B$ zobrazení, tak definujeme na A relaci $\ker f$ tak, že $(a, b) \in \ker f$ právě když $f(a) = f(b)$. Relace $\ker f$ je zjevně ekvivalence, a nazývá se *jádro* f. Všimněte si, že zobrazení je *injektivní* (t.j. prosté) právě když $\ker f = id_A$. Připomeňme zde také, že zobrazení je *surjektivní* (na) právě když $\operatorname{Im} f = B$.

5.3 Lemma. *Je-li $f\colon A \to B$ zobrazení slučitelné s n-ární operací α, tak je $\ker f$ ekvivalence slučitelná s α.*

Důkaz. Ať je $(a_1, b_1) \in \ker f, \ldots, (a_n, b_n) \in \ker f$.

To znamená $f(a_1) = f(b_1), \ldots, f(a_n) = f(b_n)$ a ze slučitelnosti f s α plyne $f(\alpha(a_1, \ldots, a_n)) = \alpha(f(a_1), \ldots, f(a_n)) = \alpha(f(b_1), \ldots, f(b_n)) = f(\alpha(b_1, \ldots, b_n))$. □

Je-li ρ ekvivalence na množině A, tak zobrazení $a \mapsto [a]_\rho$ se nazývá *přirozené* a značí se nat_ρ (někdy též mluvíme o projekci podle ρ a značíme π_ρ).

5.4 Lemma. *Ať α je n-ární operace na A a ať ρ je ekvivalence na A slučitelná s α. Potom přirozené zobrazení $\operatorname{nat}_\rho\colon A \to A/\rho$ je slučitelné s α.*

Důkaz. Operace α je na A/ρ definována tak, že pro $a_1, \ldots, a_n \in A$ platí $\alpha_{A/\rho}([a_1]_\rho, \ldots, [a_n]_\rho) = \alpha(\operatorname{nat}_\rho(a_1), \ldots, \operatorname{nat}_\rho(a_n)) = [\alpha(a_1, \ldots, a_n)]_\rho = \operatorname{nat}_\rho(\alpha(a_1, \ldots, a_n))$. Vidíme tedy, že definice α na A/ρ je přesně taková, aby nat_ρ bylo zobrazení slučitelné s ρ. □

Jsou-li A a B dvě algebraické struktury (grupy, okruhy, množiny, apod.), tak zobrazení $f\colon A \to B$ nazveme *homomorfismus*, jestliže je slučitelné se všemi operacemi, jež vystupují v definici dané struktury.

Homomorfismus $f\colon A \to B$ se nazývá *izomorfismus*, jestliže f je bijektivní. Homomorfismus $f\colon A \to A$ se nazývá *endomorfismus*, a bijektivní endomorfismus je *automorfismus*. Z Lemmat 5.1 až 5.4 vyplývá několik pouček, jež můžeme shrnout ve stručném přehledu takto:

$f\colon A \to B$ a $g\colon B \to C$ homomorfismy	$\Longrightarrow g \circ f\colon A \to C$ homomorfismus
$f\colon A \to B$ izomorfismus	$\Longrightarrow f^{-1}\colon B \to A$ izomorfismus
$f\colon A \to B$ homomorfismus	$\Longrightarrow \ker f$ je kongruence
ρ kongruence A	$\Longrightarrow \operatorname{nat}_\rho\colon A \to A/\rho$ homomorfismus

5.5 Lemma. *Ať $G = G(\cdot, ^{-1}, 1)$ a $H = H(\cdot, ^{-1}, 1)$ jsou grupy a ať $f\colon G \to H$ je zobrazení, jež je slučitelné s násobením v obou grupách (je tedy $f(a \cdot b) = f(a) \cdot f(b)$ pro všechna $a, b \in G$). Potom je f homomorfismus grup.*

Důkaz. Zvolme libovolné $a \in G$. Máme $f(a) = f(a \cdot 1_G) = f(a) \cdot f(1_G)$, takže $f(1_G) = 1_H$. Dále $1_H = f(1_G) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$, takže $f(a^{-1}) = (f(a))^{-1}$. □

Je-li $f\colon G \to H$ homomorfismus grup, tak $\ker f$ je kongruence grupy. Víme, že každá kongruence grupy G je jednoznačně určena blokem této kongruence, který obsahuje neutrální prvek (řekněme 1), a že tento

blok, řekněme N, je normální podgrupou grupy G. V případě grup je zvykem tuto podgrupu N nazývat *jádrem homomorfismu* a značit ji $\operatorname{Ker} f$ (takže alespoň ve značení nedochází ke dvojznačnosti — je $\operatorname{Ker} f = [1]_{\ker f}$).

Dobrým příkladem netriviálního homomorfismu je logaritmus $\log\colon \mathbb{R}^+(\cdot, {}^{-1}, 1) \to \mathbb{R}(+, -, 0)$. Je to izomorfismus mezi multiplikativní grupou kladných reálných čísel a aditivní grupou všech reálných čísel. Inverzním izomorfismem je pak exponenciela.

V předchozím případě šlo o homomorfismus mezi grupami, ve kterých se odpovídající operace značily různě. Shodou okolností tomu bude tak i v případě následujícím. U homomorfismů jde, obecně vzato, o to, aby bylo jasné, které operace si vzájemně odpovídají, nikoliv o formální shodu zápisu.

5.6 Tvrzení. *Zobrazení $f\colon n \mapsto a^n$ je homomorfismus ve všech následujících případech:*
(i) $f\colon \mathbb{N}(+) \to A$, *kde* $A = A(\cdot)$ *je pologrupa;*
(ii) $f\colon \mathbb{N}(+, 0) \to A$, *kde* $A = A(\cdot, 1)$ *je monoid;*
(iii) $f\colon \mathbb{Z}(+, -, 0) \to A$, *kde* $A = A(\cdot, {}^{-1}, 1)$ *je grupa.*

Důkaz. Pro jistotu uveďme, že a^n, $n > 0$, chápeme jako součin $a \cdots a$, kde a se opakuje n-krát, že a^0 definujeme jako 1, a a^{-n}, $n > 0$, jako $(a^{-1})^n$.

Uvedené tvrzení je velmi intuitivní, formální důkaz však vyžaduje jistou péči, neboť je třeba postupovat indukcí. Přitom vyjdeme z rekurzivní definice $a^{n+1} = a^n \cdot a$.

(i) Indukcí dle m dokážeme $a^{n+m} = a^n \cdot a^m$. Případ $m = 1$ se shoduje s rekurzivní definicí. Abychom dokázali $a^{m+n+1} = a^n \cdot a^{m+1}$, položíme $a^{n+m+1} = a^{n+m} \cdot a$ dle rekurzívní definice, a odsud z indukčního předpokladu máme $a^{n+m+1} = a^n \cdot a^m \cdot a \ = a^n \cdot a^{m+1}$.

(ii) Je-li 1 neutrální prvek, tak jistě $a^{n+0} = a^n = a^n \cdot 1 = a^n a^0$, a podobně $a^0 \cdot a^n = a^{0+n}$. Zbytek plyne z (i).

(iii) Je-li $n = 0$ nebo $m = 0$, tak $a^{n+m} = a^n a^m$ dostaneme stejně jako v (ii). Je-li $n > 0$ a $m > 0$, stačí použít (i). Je-li $n < 0$ a $m < 0$, tak $a^n a^m = (a^{-1})^{-n} \cdot (a^{-1})^{-m} = (a^{-1})^{-n-m} = a^{n+m}$ dle (i). Ať je $n < 0$ a $m > 0$. Případ $m = 1$ plyne z $a^n a = (a^{-1})^{-n} a = (a^{-1})^{-(n+1)} a^{-1} a = (a^{-1})^{-(n+1)} = a^{n+1}$, a dále lze postupovat indukcí dle m stejně jako v (i). Případ $n > 0$ a $m < 0$ je obdobný. □

Je-li G grupa a $a \in G$, tak z 5.6(iii) plyne, že $A = \{a^n; n \in \mathbb{Z}\}$ je podgrupa G. Každá podgrupa, kterou lze vyjádřit jako množinu mocnin nějakého prvku, se nazývá *cyklická*, a takový prvek je její *generátor* (cyklická grupa ovšem může mít více různých generátorů). Množina A je tedy cyklickou podgrupou G, která je generována prvkem a. Podgrupa A je zjevně nejmenší podgrupou G, jež obsahuje a.

Řádem prvku a se rozumí řád podgrupy tímto prvkem generované (řád a je tedy roven $|A|$).

Jestliže pracujeme s aditivní notací, používáme místo exponenciálního zápisu zápis multiplikativní. Je-li tedy například $A(+, -, 0)$ Abelovská grupa, tak na znamená $a + \ldots + a$, kde a se (pro $n > 0$) opakuje n-krát.

S touto konvencí se dostáváme do drobných obtíží, pokud pracujeme s okruhy, zvláště s číselnými. V zápise na totiž není jasné, zda míníme násobení v okruhu nebo iterované sčítání. Obvykle se předpokládá (a často tak budeme činit i zde), že rozlišení je patrné z kontextu. Pro pohodlí čtenáře však místy budeme iterované sčítání v okruhu značit místo na též $n \times a$.

Je-li $R = R(+, \cdot, -, 0, 1)$ okruh, tak podle 5.6(iii) je zobrazení $n \mapsto n \times a$, pro pevně vybrané $a \in R$, homomorfismem Abelových grup $\mathbb{Z}(+, -, 0)$ a $R(+, -, 0)$. Dokážeme, že v případě $a = 1$ běží dokonce o homomorfismus okruhů.

K tomu stačí ověřit, že $n \mapsto n \times 1$ je zobrazení slučitelné s násobením, tedy že $(nm) \times 1 = (n \times 1) \cdot (m \times 1)$ platí pro všechna $n, m \in \mathbb{Z}$. Je-li $n = 0$ nebo $m = 0$, je tento vztah zřejmý, stejně tak tomu je i pro případ $m = 1$. Indukcí ověříme rovnost pro $m > 0$. Ať vztah platí pro nějaké $m \geq 1$. Pak $(n \times 1) \cdot ((m+1) \times 1) = (n \times 1) \cdot ((m \times 1) + 1) = (n \times 1) \cdot (m \times 1) + (n \times 1) = ((nm) \times 1) + (n \times 1) = (nm + n) \times 1 = (n(m+1)) \times 1$ vyplývá z 5.6(iii) a indukčního předpokladu.

Z 5.6(iii) také plyne, že $(n \cdot (-m)) \times 1 = (-nm) \times 1$ je prvek opačný k $(nm) \times 1$, a podobně ověříme, že $(n \times 1) \cdot (m \times 1)$ je prvek opačný vůči $(n \times 1) \cdot ((-m) \times 1)$. Proto dokázaný vztah platí i pro $m < 0$, a můžeme vyslovit:

5.7 Tvrzení. *Ať $R = R(+, \cdot, -, 0, 1,)$ je okruh. Pak zobrazení $\mathbb{Z} \to R$, $n \mapsto n \times 1$ je homomorfismus okruhů.* □

Je-li $f\colon R \to S$ homomorfismus okruhů, tak $\operatorname{Ker} f = f^{-1}(0) = [0]_{\ker f}$ je ideál, který je zvykem také nazývat *jádro homomorfismu*. Protože známe všechny ideály $\mathbb{Z}$ (viz 4.5), tak víme, že jádro homomorfismu, který je popsán v 5.7, je rovno $n\mathbb{Z}$ pro nějaké jednoznačně určené $n \geq 0$. Toto n se nazývá

charakteristika okruhu R a značí se $\operatorname{char} R$. Vidíme, že charakteristika n okruhu R je nenulová právě když lze iterovaným sčítáním 1 dostat 0. V takovém případě je rovna nejmenšímu možnému počtu sčítanců ve výrazu $1 + \cdots + 1$, který je v okruhu R roven 0.

Je dobré si uvědomit následující vztah:

5.8 Tvrzení. *Ať $f\colon A \to B$ je homomorfismus grup (nebo okruhů). Pak f je injektivní právě když* $\operatorname{Ker} f$ *je triviální (tj. má pouze jeden prvek).*

Důkaz. Z definice $\ker f$ plyne, že f je injektivní právě když každý blok $\ker f$ je jednobodový. To ovšem nastane právě když $\operatorname{Ker} f$ má jediný bod. □

Je-li A nějaká algebraická struktura, tak množinu $\operatorname{End}(A)$ všech endomorfismů lze považovat za monoid vzhledem ke skládání zobrazení a identitě, neboť složení dvou endomorfismů je vždy opět endomorfismus.

Invertibilní endomorfismy jsou automorfismy, jejich množinu označíme $\operatorname{Aut}(A)$. Protože zobrazení inverzní k automorfismu je opět automorfismus, vidíme, že $\operatorname{Aut}(A)$ je grupa.

Poznamenejme, že $\operatorname{End}(A)$ je podmonoid transformačního monoidu T_A a $\operatorname{Aut}(A)$ je podgrupa symetrické grupy S_A.

Automorfismy lze samozřejmě uvažovat i u struktur, jež nejsou po výtce algebraické. Lze například mluvit o automorfismech grafů, designů nebo geometrií.

Význam teorie grup plyne právě z toho, že nic nevyjadřuje tak jasně symetrie dané struktury (čili — obrazněji — úhly pohledu, ze kterých se jeví struktura stejně) jako její grupa automorfismů.

Je proto pochopitelné, že pro nějakou oblast matematiky mají grupy tím větší význam, čím více se tato oblast zabývá objekty, jež vykazují vysoký stupeň pravidelnosti, tedy symetrie.

Injektivní homomorfismy (někdy se jim říká též vložení nebo vnoření), jsme již několikrát použili. Nejjednodušší případ je zobrazení $A \to B$, $a \mapsto a$, v případě, že A je podstruktura (například podgrupa nebo podokruh) struktury B.

Jiný příklad je zobrazení $r \mapsto r \cdot x^0$, které přiřazuje prvku okruhu R prvek $R\big[[x]\big]$. U injektivních homomorfismů, které jsou tak přirozeně definovány jako tento, často říkáme, že ztotožňujeme prvky vzoru s prvky obrazu. Takovému obratu každý rozumí, a proto se mu nebudeme vyhýbat ani v budoucnu. Je dobré si ale uvědomit, že se za takovýmto obratem vlastně vždy skrývá nějaký injektivní homomorfismus, který jsme se kvůli přehlednosti a jednoduchosti rozhodli v zápisech neuvádět.

6. Věta o homomorfismu

6.1 Lemma. *Ať $f\colon A \longrightarrow B$ je zobrazení a ať ρ je ekvivalence na A. Zobrazení $g\colon A/\rho \to B$, které splňuje $g \circ \mathrm{nat}_\rho = f$, existuje právě když $\rho \subseteq \ker f$. V takovém případě je g určeno jednoznačně a platí $g([a]_\rho) = f(a)$ pro každé $a \in A$. Přitom g je surjektivní právě když f je surjektivní, a g je injektivní právě když $\ker f = \rho$. Je-li navíc dána n-ární operace α jak na A, tak na B, přičemž f i ρ jsou slučitelné s α, tak je i g (pokud existuje) slučitelné s α.*

Důkaz. Je-li $f = g \circ \mathrm{nat}_\rho$ a platí $a\rho b$ pro nějaká $a, b \in A$, tak je $f(a) = g \circ \mathrm{nat}_\rho(a) = g \circ \mathrm{nat}_\rho(b) = f(b)$, a proto musí být $\rho \subseteq \ker f$. Předpokládejme, že tomu tak je. Pak pro každé $a \in A$ nutně musí být $g([a]_\rho) = g \circ \mathrm{nat}_\rho(a) = f(a)$. Je-li $a\rho b$, tak z $\rho \subseteq \ker f$ plyne $f(a) = f(b)$, a proto je taková definice g korektní. Přitom je zjevně $\mathrm{Im}\, g = \mathrm{Im}\, f$, takže g je surjektivní právě když je f surjektivní. Pro všechna $a, b \in A$ z $g([a]_\rho) = g([b]_\rho)$ plyne $[a]_\rho = [b]_\rho$ právě když pro všechna $a, b \in A$ z $f(a) = f(b)$ plyne $a\rho b$, čili právě když je $\ker f \subseteq \rho$. Odtud část o injektivitě. Konečně ať na A i B je dána n-ární operace α, přičemž jsou splněny předpoklady slučitelnosti jak pro f, tak pro ρ. Pak pro všechna $a_1, \ldots, a_n \in A$ máme $g(\alpha_{A/\rho}([a_1]_\rho, \ldots, [a_n]_\rho)) = g([\alpha_A(a_1, \ldots, a_n)]_\rho) = (g \circ \mathrm{nat}\,\rho)(\alpha_A(a_1, \ldots, a_n)) = f(\alpha_A(a_1, \ldots, a_n)) = \alpha_B(f(a_1), \ldots, f(a_n)) = \alpha_B(g([a_1]_\rho), \ldots, g([a_n]_\rho))$. □

6.2 Lemma. *Ať α je n-ární operace na množinách A i B a ať $C \subseteq A$ je uzavřené na α a $D \subseteq B$ je také uzavřené na α. Je-li $f\colon A \to B$ zobrazení slučitelné s α, tak množiny $f(C) \subseteq B$ a $f^{-1}(D) \subseteq A$ jsou rovněž uzavřené na α.*

Důkaz. Ať jsou $b_1, \ldots, b_n \in f(C)$. Pak $b_1 = f(c_1), \ldots, b_n = f(c_n)$ pro nějaké $c_1, \ldots, c_n \in C$, takže $\alpha(b_1, \ldots, b_n) = \alpha(f(c_1), \ldots, f(c_n)) = f(\alpha(c_1, \ldots, c_n))$ padne rovněž do $f(C)$.

Ať jsou $a_1, \ldots, a_n \in f^{-1}(D)$. Pak $f(\alpha(a_1, \ldots, a_n)) = \alpha(f(a_1), \ldots, f(a_n))$ leží v D, neboť $f(a_1) \in D, \ldots$ $\ldots, f(a_n) \in D$, a proto $\alpha(a_1, \ldots, a_n)$ se nachází v $f^{-1}(D)$. □

Nyní definujeme pojem, který nám umožní jednotným způsobem popisovat algebraické struktury s více operacemi. Důvod, že jsme ho nezavedli dříve, je dvojí. Z hlediska didaktického se jeví být rozumnější některé pojmy nejprve si ujasnit na konkrétních strukturách (grupách, okruzích apod.); z vnitřního hlediska matematiky pak platí, že některé speciální pojmy (např. grupy, okruhy) jsou nepoměřitelně důležitější nežli jejich zobecnění. Smysl některých zobecnění často totiž bývá spíše v tom, že nám jednotným způsobem dovolují vyjádřit určité základní vztahy a vazby, a ne v tom, že by se definicí nové, zobecněné struktury podařilo objevit nové významné objekty.

Obecný pojem, o který nám nyní půjde, je *algebra signatury* σ, kde $\sigma\colon \Sigma \to \mathbb{N}_0$ je zobrazení, jež množině operačních symbolů přiřazuje jejich aritu (četnost). Například u grup by bylo $\Sigma = \{\cdot, {}^{-1}, 1\}$, $\sigma(\cdot) = 2$, $\sigma({}^{-1}) = 1$ a $\sigma(1) = 0$.

Slovo algebra se používá v mnoha významech. Algebry dané signatury se někdy nazývají universální algebry. V této kapitole budeme algebrou rozumět algebru (nějak pevně dané) signatury σ.

Jsou-li A, B dvě algebry, tak $f\colon A \to B$ je jejich homomorfismus, je-li f slučitelné se všemi operacemi $\alpha \in \Sigma$. Ekvivalence ρ na A je kongruencí algebry A, je-li slučitelná se všemi $\alpha \in \Sigma$. O $C \subseteq A$ řekneme, že je to podalgebra A, je-li C uzavřená na všechna $\alpha \in \Sigma$.

V (universálních) algebrách samozřejmě platí všechny obecné vztahy o homomorfismech a kongruencích, které jsme uvedli v předchozích kapitolách. K nim můžeme přidat následující důsledky lemmat 6.2 a 6.1.

6.3 Tvrzení. *Ať $f\colon A \to B$ je homomorfismus algeber. Je-li C podalgebra A, je $f(C)$ podalgebra B. Je-li D podalgebra B, je $f^{-1}(D)$ podalgebra A. Speciálně je* $\mathrm{Im}\, f$ *podalgebra B.* □

6.4 Věta o homomorfismu. *Ať $f\colon A \to B$ je homomorfismus algeber a ať ρ je kongruence A. Homomorfismus $g\colon A/\rho \to B$ takový, že $f = g \circ \mathrm{nat}_\rho$, existuje právě když $\rho \subseteq \ker f$. V takovém případě $g([a]_\rho) = f(a)$ pro každé $a \in A$, g je surjektivní právě když f je surjektivní a g je injektivní právě když* $\ker f = \rho$. □

Vztáhneme-li Větu o homomorfismu na situaci, kdy $\rho = \ker f$, okamžitě obdržíme:

6.5 První věta o izomorfismu. *Ať $f\colon A \to B$ je homomorfismus algeber a $\rho = \ker f$. Pak $[a]_\rho \mapsto f(a)$ je izomorfismus $A/\rho \simeq \mathrm{Im}\, f$.* □

Předchozí věta se často uvádí jen pro případ, kdy f je surjektivní homomorfismus. Pak dostaneme izomorfismus $A/\rho \simeq B$. Jsou-li například A a B grupy a ρ se shoduje s $\mathrm{mod}\, N$, kde N je normální

podgrupa A, tak izomorfismus $A/N \simeq B$ je dán vztahem $aN \mapsto f(a)$. Podobně v případě, kdy A a B jsou okruhy a I je ideál A, který určuje ρ, máme izomorfismus $A/I \simeq B$, $a + I \mapsto f(a)$.

6.6 Tvrzení. *Každá podgrupa $\mathbb{Z}(+,-,0)$ je rovna $n\mathbb{Z}$ pro nějaké $n \geq 0$.*

Důkaz. Je-li A podgrupa $\mathbb{Z}(+,-,0)$, tak pro $a \in A$ a $m \in \mathbb{Z}$ je $m \times a = m \cdot a \in A$ (zde $m \times a$ označuje iterované sčítání). Každá podgrupa $\mathbb{Z}(+,-,0)$ je tedy současně ideálem okruhu $\mathbb{Z}$, takže lze použít 4.5. □

6.7 Tvrzení. *Ať $A = A(\cdot, ^{-1}, 1)$ je cyklická grupa s generátorem a. Je-li A nekonečná, je zobrazení $i \mapsto a^i$, $i \in \mathbb{Z}$, izomorfismus $\mathbb{Z}(+,-,0)$ a A. Je-li A řádu n, je $i \mapsto a^i$, $i \in \mathbb{Z}_n$, izomorfismem $\mathbb{Z}_n(+,-,0)$ a A.*

Důkaz. Máme $A = \{a^i;\ i \in \mathbb{Z}\}$. Zobrazení $f\colon \mathbb{Z}(+,-,0) \to A$, $f(i) = a^i$, je podle 5.6 (iii) surjektivní homomorfismus grup. Podle 6.6 je $\operatorname{Ker} f = n\mathbb{Z}$ pro nějaké $n \geq 0$. Přitom v případě $n = 0$ je A nekonečná a f je izomorfismus. Ať je $n > 0$. Podle 6.5 je $i + n\mathbb{Z} \mapsto a^i$ izomorfismus $\mathbb{Z}/n\mathbb{Z} \simeq A$. Označme ho g. Protože izomorfismus $h\colon \mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$ lze definovat tak, že $h(i) = i + n\mathbb{Z}$, je možno námi popsaný izomorfismus obdržet jako $g \circ h$. □

6.8 Tvrzení. *Ať $R = R(+,\cdot,-,0,1)$ je okruh. Pak $S = \{i \times 1;\ i \in \mathbb{Z}_n\}$, tvoří podokruh R, který je obsažen v každém jiném podokruhu R. Je-li R charakteristiky 0, je $i \mapsto i \times 1$, $i \in \mathbb{Z}$, izomorfismus okruhů $\mathbb{Z} \simeq S$. Je-li R charakteristiky $n > 0$, je $i \mapsto i \times 1$, $i \in \mathbb{Z}_n$, izomorfismus okruhů $\mathbb{Z}_n \simeq S$.*

Důkaz. Je-li T nějaký podokruh R, tak obsahuje prvek 1, a proto i prvek $i \times 1$ pro každé $i \in \mathbb{Z}$. Přitom S je obrazem okruhového homomorfismu $f\colon \mathbb{Z} \to R$ definovaného v 5.7, a proto je S, podle 6.3, podokruhem R. Přitom f je injektivní právě když $\operatorname{Ker} f = 0$, tedy právě když R je charakteristiky 0, a v takovém případě je $i \mapsto f(i) = i \times 1$ izomorfismus $\mathbb{Z} \simeq S$. Je-li charakteristika R rovna $n > 0$, tak $\operatorname{Ker} f = n\mathbb{Z}$, a $i + n\mathbb{Z} \mapsto i \times 1$ je izomorfismus $\mathbb{Z}/n\mathbb{Z} \simeq S$ podle 6.5. Zbytek důkazu je stejný jako v 6.7. □

6.9 Tvrzení. *Ať $f\colon G \to H$ je homomorfismus grup. Pak $|G| = |\operatorname{Ker} f| \cdot |\operatorname{Im} f|$.*

Důkaz. Pro každé $a \in \operatorname{Im} f$ je $f^{-1}(a)$ blokem ker f, čili prvkem $G/\operatorname{Ker} f$. Řád $G/\operatorname{Ker} f$ je roven indexu $|G\colon \operatorname{Ker} f|$, takže dokazovaný vztah plyne z Lagrangeovy věty. □

Z algeber signatury $\sigma\colon \Sigma \to \mathbb{N}_0$ lze vytvářet nové algebry faktorizací, nalezením podalgebry a také *kartézským součinem*. Protože kartézský součin je možno definovat i pro nekonečně mnoho činitelů, bude pro nás výhodnější, jestliže součin $\prod A_i;\ i \in I$, kde $I \neq \emptyset$, budeme chápat jako množinu všech zobrazení $f\colon I \to \bigcup (A_i;\ i \in I)$, pro která pro každé $i \in I$ platí $f(i) \in A_i$.

Jsou-li A_i algebry signatury σ, tak $A = \prod A_i$ můžeme považovat za algebru téže signatury: je-li $\alpha \in \Sigma$ operace četnosti $n = \sigma(\alpha)$, tak pro $a_1, \ldots, a_n \in \prod A_i$ a $i \in I$ klademe

$$\alpha_A(a_1, \ldots, a_n)(i) = \alpha_{A_i}(a_1(i), \ldots, a_n(i)).$$

Jinými slovy, operace v $A = \prod A_i$ jsou definovány „po složkách“.

Je patrné, že součiny pologrup, monoidů, okruhů, nebo grup jsou opět odpovídající algebraické struktury. Ale pozor, součin alespoň dvou těles není těleso (proč?).

Jsou-li $R_i,\ i \in I$ okruhy, tak můžeme uvažovat množinu $S = \{a \in \prod R_i;\ a(i) \neq 0$ jen pro konečně mnoho $i \in I\}$. Okamžitě vidíme, že S je podokruh okruhu $\prod R_i$. Okruh S se označuje $\bigoplus S_i,\ i \in I$, a nazývá se *direktní suma* okruhů $S_i,\ i \in I$.

Podobně lze postupovat i u jiných algebraických struktur, ve kterých se vyskytují triviální podstruktury. Jsou-li například M_i, $i \in I$, (levé) moduly nad okruhem R, je jejich direktní suma $\bigoplus M_i$, $i \in I$, také rovna $\{a \in \prod R_i;\ a(i) \neq 0$ jen pro konečně mnoho $i \in I\}$.

Každý z modulů M_j, $j \in I$, lze chápat jako podmodul direktní sumy $M = \bigoplus_{i \in I} M_i$, pokud ztotožníme každý prvek $b \in M_j$ s takovým $a \in M$, že $a(j) = b$ a $a(i) = 0$ pro $i \neq j$. Při tomto ztotožnění je tak každý prvek $m \in M$ možno jediným způsobem vyjádřit jako $\sum_{i \in I} m_i$, kde $m_i \in M_i$.

Jsou-li $\varphi_i\colon M_i \to N$ homomorfismy modulů, $i \in I$, tak $\varphi = \bigoplus_i \varphi_i\colon \bigoplus M_i \to N$ je definováno tak, že $\varphi(\sum m_i) = \sum \varphi_i(m_i)$. Je snadné ověřit, že $\varphi\colon \bigoplus M_i \to N$ je rovněž homomorfismus modulů.

6.10 Lemma. *Ať B a C jsou podgrupy grupy G. Pak $(BC)^{-1} = CB$ a zobrazení $b(B \cap C) \mapsto bC$, $b \in B$, je bijekce množin $\{b \cdot (B \cap C),\ b \in B\}$ a $\{bC;\ b \in B\}$.*

Důkaz. Je-li $u \in BC$, tak existují $b \in B$ a $c \in C$, že je $u = bc$. Proto je $u^{-1} = c^{-1}b^{-1} \in CB$, a platí $(BC)^{-1} \subseteq CB$. Tudíž je také $(CB)^{-1} \subseteq BC$, a tedy i $CB \subseteq (BC)^{-1}$.

Položme $A = B \cap C$. Je-li b_1A rovno b_2A pro nějaká b_1, $b_2 \in B$, je $b_1^{-1}b_2 \in A \subseteq C$, a proto je $b_1C = b_2C$. Uvedené zobrazení, označme ho třeba γ, je tudíž korektně definováno.

Z definice je zřejmé, že γ je surjektivní. Předpokládejme nyní, že je b_1C rovno b_2C pro nějaká b_1, $b_2 \in B$. Pak je $b_1^{-1}b_2 \in C$. Protože současně i $b_1^{-1}b_2 \in B$, je nutně $b_1^{-1}b_2 \in A$, a tedy $b_1A = b_2A$. Vidíme, že γ je také injektivní. □

6.11 Tvrzení. *Ať B a N jsou podgrupy grupy G, přičemž N je normální podgrupa. Pak BN je také podgrupa grupy G a platí $BN = NB$.*

Důkaz. Je-li $BN = NB$, tak je $(BN)^{-1} = BN$ dle 6.10, a tak je BN uzavřené na násobení, neboť pro $u_i \in BN$, $i \in \{1, 2\}$, existují b_1, $b_2 \in B$ a n_1, $n_2 \in N$, že $u_1 = b_1n_1$, $u_2 = n_2b_2$, takže $u_1u_2 = b_1nb_2$, kde $n = n_1n_2 \in N$, přičemž $nb_2 = b_3n_3$ pro nějaká $b_3 \in B$ a $n_3 \in N$, odkud $u_1u_2 = (b_1 \cdot b_3) \cdot n_3 \in BN$.

Dokažme $BN = NB$. Inkluze $BN \subseteq NB$ plyne z toho, že pro dané $b \in B$ a $n \in N$ je $n\prime = bnb^{-1}$, takže $bn = n\prime b \in NB$. Podobně $nb \in NB$ je rovno $b \cdot (b^{-1}nb) \in BN$. □

6.12 Třetí věta o izomorfismu pro grupy. *Ať N a H jsou podgrupy grupy G, přičemž N je normální. Zobrazení $h \cdot (H \cap N) \mapsto hN$ je izomorfismus grup $H/H \cap N \simeq HN/N$.*

Důkaz. Grupa $H \cap N$ je zřejmě normální podgrupa grupy H. Podle 6.10 je uvedené zobrazení bijekce, takže vzhledem k 5.5 stačí ukázat, že je slučitelné s násobením, tedy že $(h_1h_2)N$, což je obraz $(h_1 \cdot \cdot (H \cap N)) \cdot (h_2 \cdot (H \cap N)) = (h_1h_2) \cdot (H \cap N)$, je rovno $(h_1N) \cdot (h_2N)$. To je ovšem samozřejmě pravda, neboť N je v G normální. □

Jsou-li H a K podgrupy grupy G, tak každá podgrupa G, jež obsahuje $H \cup K$, musí obsahovat HK. Pokud je HK podgrupa G, je to tedy nejmenší podgrupa G, jež obsahuje $H \cup K$. Je-li H nebo K normální podgrupa G, tak HK skutečně podgrupa je. Obecně však HK podgrupa být nemusí (z prvé části důkazu 6.11 vyplývá, že HK je podgrupa G právě když $HK = KH$.)

V abelovské grupě $A(+, -, 0)$ jsou všechny podgrupy, řekněme B a C, normální. Proto je $B + C$ podgrupa A a zobrazení $b + (B \cap C) \mapsto b + C$ je izomorfismus $B/B \cap C \simeq (B + C)/C$.

Je-li R okruh, S jeho podokruh a I ideál R, tak lze snadno ověřit, že $S \cap I$ je ideál S a že $S + I$ je podokruh R. Toho využijeme v následující větě:

6.13 Třetí věta o izomorfismu pro okruhy. *Ať R je okruhem, I jeho ideál a S podokruh R. Zobrazení $s + (S \cap I) \mapsto s + I$ je okruhový izomorfismus $S/S \cap I \simeq (S + I)/I$.*

Důkaz. Vzhledem k předchozímu stačí ukázat, že uvedené zobrazení je slučitelné s násobením, což však vede na rovnost $s_1s_2 + I = (s_1 + I)(s_2 + I)$, která je jistě splněna. □

Jsou-li A a B podmoduly (levého) modulu M nad okruhem R, je jistě $A + B$ nejmenší podmodul M, který obsahuje $A \cup B$.

6.14 Třetí věta o izomorfismu pro moduly. *Ať M je levý modul nad okruhem R a ať A a B jsou jeho podmoduly. Zobrazení $a + (A \cap B) \mapsto a + B$ je izomorfismus modulů $A/A \cap B \simeq (A + B)/B$.*

Důkaz. S ohledem na 6.12 stačí dokázat pouze slučitelnost se skalárním násobením. To však vede na zřejmou rovnost $r(a + B) = ra + B$, pro všechna $r \in R$ a $a \in A$. □

7. Uspořádané množiny, svazy a kvaziuspořádání

Relaci $\leq$ na množině M nazveme *uspořádáním* M, jestliže $\leq$ je reflexivní, tranzitivní a jestliže pro libovolná $a, b \in M$ z $a \leq b$ a $b \leq a$ plyne $a = b$.

Uspořádání, kde pro libovolné $a, b \in M$ platí $a \leq b$ nebo $b \leq a$, se nazývá *lineární*.

Poznámka. Často se používá jiné terminologie: relace uvedených vlastností se nazývá *částečné uspořádání*, přičemž uspořádáním se míní lineární uspořádání. Částečně uspořádané množiny se pak leckdy označují akronymem *poset* — z anglického "partially ordered set".

Dva prvky a, b uspořádané množiny $(M, \leq)$ se nazývají *porovnatelné*, je-li $a \leq b$ nebo $b \leq a$. V opačném případě jsou tyto prvky *neporovnatelné*. Prvek $a \in A \subseteq M$ se nazývá *nejmenší* prvek A, pokud $a \leq b$ pro každé $b \in A$. Dále $a \in A \subseteq M$ je *největší* prvek A, je-li $b \leq a$ pro všechna $b \in A$. Každá množina $A \subseteq M$ má zjevně nanejvýš jeden největší a nanejvýš jeden nejmenší prvek.

Prvek $a \in M$ je *dolní závorou* množiny $A \subseteq M$, jestliže $a \leq b$ pro každé $b \in A$. Prvek $a \in M$ je *horní závorou* množiny $A \subseteq M$, jestliže $b \leq a$ pro každé $b \in A$. Všimněte si, že každý prvek $a \in M$ je dolní i horní závorou prázdné množiny.

Buď $A \subseteq M$. Označme na chvíli B množinu horních závor A a C množinu jeho dolních závor. Nejmenší prvek B (pokud existuje) se nazývá *supremum* A (značíme $\sup_{\leq} A$). Podobně největší dolní závoru (pokud existuje) nazýváme *infimum* A ($\inf_{\leq} A$).

Řekneme, že $b \in M$ *pokrývá* $a \in M$, jestliže $a \leq b$, $a \neq b$ a pro $a \leq c \leq b$ je buď $a = c$, nebo $b = c$. Někdy se pak píše $a \lessdot b$.

Jestliže M obsahuje nejmenší prvek, řekněme e, tak $a \in M$ se nazývá *atomem* právě když a pokrývá e. Jestliže M obsahuje největší prvek, řekněme f, tak $a \in M$ se nazývá *koatomem* právě když f pokrývá a.

V $(\mathbb{Z}, \leq)$ je každé číslo k pokryté číslem $k + 1$. Naopak, v $(\mathbb{Q}, \leq)$ žádný prvek pokrytí nemá.

Je-li $(M, \leq)$ konečná uspořádaná množina, má v ní pokrytí každý prvek, ke kterému existuje alespoň jeden prvek větší. Grafické zachycení relace pokrytí (a a b spojíme úsečkou právě když $a \lessdot b$, přičemž b umístíme výše než a) se nazývá *Hasseův diagram*.

Definujeme-li na M relaci $\preccurlyeq$ tak, že $a \preccurlyeq b$ právě když $b \leq a$, dostaneme opět uspořádání. Tomuto uspořádání se říká *opačné*. Při přechodu od $\leq$ k $\preccurlyeq$ se z koatomů stanou atomy, z horních závor dolní závory, ze suprem infima, a naopak.

7.1 Lemma. *Buď M_i, $i \in I$ podmnožiny uspořádané množiny $(M, \leq)$. Ať pro každé $i \in I$ je $b_i \in M$ supremem množiny M_i. Potom $\sup_{\leq}\{b_i; i \in I\}$ existuje právě když existuje $\sup_{\leq}(\bigcup(M_i;\ i \in I))$. Přitom obě suprema, pokud existují, si jsou rovna.*

Důkaz. Ať $b = \sup_{\leq}\{b_i; i \in I\}$. Je-li $a \in \bigcup(M_i;\ i \in I)$, je $a \in M_i$ pro nějaké $i \in I$, a tedy $a \leq b_i \leq b$. Je-li c takové, že $a \leq c$ pro všechna $a \in \bigcup(M_i;\ i \in I)$, je též $b_i \leq c$ pro všechna $i \in I$, takže $b \leq c$. Naopak, ať $m = \sup(\bigcup(M_i;\ i \in I))$. Pak $m \geq b_i$ pro každé $i \in I$. Je-li $d \geq b_i$ pro všechna $i \in I$, je i $d \geq a$ pro všechna $a \in \bigcup(M_i;\ i \in I)$, takže $d \geq m$. □

Podobné lemma lze vyslovit a dokázat též pro infima. Ovšem infima jsou suprema v opačném uspořádání, takže takovéto duální lemma je zřejmé a není nutné ho výslovně uvádět.

Předpokládejme nyní, že $(M, \leq)$ je taková uspořádaná množina, že každé dva prvky z M mají supremum i infimum. Pak z 7.1 indukcí okamžitě vyplývá, že každá konečná neprázdná množina má supremum i infimum. Označíme-li $a \vee b = \sup_{\leq}\{a, b\}$ a $a \wedge b = \inf_{\leq}\{a, b\}$ pro každé $a, b \in M$, dostáváme dvě binární operace na M (nazývají se *spojení* a *průsek*). Pro tyto operace platí

komutativita	$a \wedge b = b \wedge a$ a $a \vee b = b \vee a$,
idempotence	$a \wedge a = a = a \vee a$,
asociativita	$(a \wedge b) \wedge c = a \wedge (b \wedge c)$ a $(a \vee b) \vee c = a \vee (b \vee c)$,
absorpce	$a \wedge (b \vee a) = a = a \vee (b \wedge a)$.

Ověřit uvedené identity je snadné — přitom asociativita vyplývá z 7.1, neboť $(a \vee b) \vee c = \sup_{\leq}\{a, b, c\} = a \vee (b \vee c)$.

Algebraický systém $M = M(\wedge, \vee)$, ve kterém jsou definovány binární operace $\wedge$ a $\vee$, jež splňují komutativní, idempotentní, asociativní a absorpční zákon, se nazývá *svaz*.

Ve svazu $M = M(\wedge, \vee)$ zaveďme relaci $\leq$ tak, že $a \leq b$ právě když $b = a \vee b$. Potom $a \leq a$ podle idempotentního zákona, $a \leq b$ a $b \leq c$ implikuje $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$ a z $a \leq b$, $b \leq a$ máme $b = a \vee b = b \vee a = a$. $(M, \leq)$ je tedy uspořádaná množina. Přitom pro každé $a, b \in M$ je

$a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$, takže $a \leq a \vee b$ a $b \leq a \vee b$. Je-li $c \geq a$ a $c \geq b$, je $c \vee (a \vee b) = (c \vee a) \vee b = c \vee b = c$, takže $a \vee b$ je supremum množiny $\{a, b\}$. Je-li $b = a \vee b$, je $a \wedge b = a \wedge (a \vee b) = a$. Naopak, je-li $a \wedge b = a$, je $a \vee b = b \vee (a \wedge b) = b$. To znamená, že $a \leq b$ platí právě když $a \wedge b = a$. Z této ekvivalentní definice uspořádání se analogicky dokáže, že $\inf\{a, b\} = a \wedge b$.

Z předchozího plyne, že svaz můžeme definovat ekvivalentně jako uspořádanou množinu, kde každé dva prvky mají supremum a infimum. Je zbytečné rozhodovat, zda prvotní by měla být tato definice, nebo definice vycházející z identit. V dalším budeme prostě předpokládat, že ve svazu máme definovány jak operace průseku a spojení, tak uspořádání.

Ve svazu může a nemusí existovat nejmenší a největší prvek. Pokud chceme existenci největšího a nejmenšího prvku algebraicky zachytit, definujeme „svaz s nulou a jedničkou“ $M = M(\wedge, \vee, 0, 1)$, kde navíc platí identity

$$a \wedge 1 = a = a \vee 0.$$

(Důsledkem absorpčního zákona pak je, že $a \vee 1 = 1$ a $a \wedge 0 = 0$.)

Svaz nazveme *úplný*, jestliže každá množina má supremum a infimum. V úplném svazu tedy existuje největší a nejmenší prvek (uvědomte si, že největší prvek je infimem prázdné množiny).

Množina všech podmnožin dané množiny s uspořádáním inkluzí a operacemi průniku a sjednocení je úplný svaz. Jeho podsvazem je svaz konečných množin. Sjednocení konečných množin nemusí být konečná množina, proto na nekonečné množině není podsvaz konečných množin úplný. Soustavu $\mathcal{P}(M)$ všech podmnožin dané množiny M bychom však mohli také chápat jako 0,1–svaz, ve kterém $0 = \emptyset$ a $1 = M$. Je-li M nekonečná množina, tak ovšem množina všech konečných podmnožin není podalgebra algebry $\mathcal{P}(M)(\cap, \cup, 0, 1)$, třebaže je podalgebrou algebry $\mathcal{P}(M)(\cap, \cup)$.

Jestliže v axiomech svazu zaměníme $\wedge$ a $\vee$, axiomy se nezmění. Proto, když ke svazu $L = L(\wedge, \vee)$ definujeme algebru $L^{op} = L(\wedge_{op}, \vee_{op})$ tak, že $a \wedge_{op} b = a \vee b$ a $a \vee_{op} b = a \wedge b$, dostaneme opět svaz, tento svaz se nazývá svazem *opačným*. Označíme-li uspořádání v L symbolem $\leq$ a uspořádání v L^{op} symbolem $\leq_{op}$, vidíme, že $a \leq_{op} b$ právě když $a = a \wedge_{op} b = a \vee b$, což platí právě když $a \geq b$. Uspořádání v opačném svazu je tedy opačné uspořádání.

Jsou-li $(A, \leq)$ a $(B, \leq)$ dvě uspořádané množiny, tak zobrazení $f\colon A \to B$ se nazývá *monotonní*, jestliže pro všechna $a, b \in A$ z $a \leq b$ plyne $f(a) \leq f(b)$.

7.2 Lemma. *Buďte $L = L(\wedge, \vee)$ a $M = M(\wedge, \vee)$ dva svazy. Je-li $f\colon L \to M$ homomorfismus svazů, je f monotonní zobrazení.*

Důkaz. Ať $a, b \in L$ a $a \leq b$. Pak $f(a) \wedge f(b) = f(a \wedge b) = f(a)$, takže je $f(a) \leq f(b)$. □

7.3 Tvrzení. *Buďte $L = L(\wedge, \vee)$ a $M = M(\wedge, \vee)$ dva svazy. Bijektivní zobrazení $f\colon L \to M$ je izomorfismus těchto svazů právě když f i f^{-1} jsou monotonní.*

Důkaz. Je-li f izomorfismus, jsou f a f^{-1} monotonní dle 7.2. Naopak, buďte f a f^{-1} monotonní a ať $a, b \in L$. Potom $f(a \wedge b) \leq f(a)$, $f(a \wedge b) \leq f(b)$ a pro $d \in M$ takové, že $d \leq f(a)$ a $d \leq f(b)$, existuje $c \in L$, že $f(c) = d$. Tudíž $c = f^{-1}(d) \leq f^{-1}(f(a)) = a$, a stejně tak $c \leq b$. Proto $c \leq a \wedge b$ a $f(c) = d \leq f(a \wedge b)$. Dokázali jsme $f(a \wedge b) = \inf\{f(a), f(b)\}$, takže nutně $f(a \wedge b) = f(a) \wedge f(b)$. Obdobně se ukáže $f(a \vee b) = f(a) \vee f(b)$. □

Reflexivní a tranzitivní relace na množině A se nazývá *kvaziuspořádání A*.

Buď $\leq$ kvaziuspořádání množiny A. Pro $a, b \in A$ pišme $a \sim b$, jestliže současně platí $a \leq b$ a $b \leq a$.

7.4 Lemma. *Relace $\sim$ je ekvivalence.*

Důkaz. $\sim$ je zjevně reflexivní a symetrická. Je-li $a \sim b$ a $b \sim c$, je $a \leq b \leq c$ a $c \leq b \leq a$, takže $a \sim c$. □

Relaci $\sim$ nazýváme *jádrem* kvaziuspořádání $\leq$.

7.5 Lemma. *Buď $\sim$ jádro kvaziuspořádání $\leq$ množiny A a ať $\beta, \gamma \in A/\sim$. Jestliže $b_0 \in \beta$, $c_0 \in \gamma$ jsou takové, že $b_0 \leq c_0$, tak $b \leq c$ pro libovolná $b \in \beta$, $c \in \gamma$.*

Důkaz. Je $b \leq b_0 \leq c_0 \leq c$. □

Na $A/\sim$ definujeme relaci $\preccurlyeq$ tak, že $\beta \preccurlyeq \gamma$ platí právě když existují $b \in \beta$ a $c \in \gamma$ taková, že je $b \leq c$. Z 7.5 vyplývá, že v takovém případě je $b \leq c$ pro všechna $b \in \beta$ a $c \in \gamma$. Můžeme tedy vyslovit následující lemma.

7.6 Lemma. *Buď $b, c \in A$. Pak $[b]_\sim \preccurlyeq [c]_\sim$ právě když $b \leq c$.* □

7.7 Tvrzení. *Relace $\preccurlyeq$ je na $A/\sim$ uspořádáním.*

Důkaz. Důkaz reflexivity a tranzitivity je okamžitý. Ať $\beta, \gamma \in A/\sim$ a $\beta \preccurlyeq \gamma$, $\gamma \preccurlyeq \beta$. Potom pro $b \in \beta$, $c \in \gamma$ máme $b \leq c$, $c \leq b$, takže $b \sim c$ a $\beta = \gamma$. □

Buď $\leq$ kvaziuspořádání A, $\sim$ jeho jádro a $\preccurlyeq$ uspořádání $A/\sim$. Kvaziuspořádání $\leq$ si můžeme představit tak, jakoby vzniklo z uspořádání $\preccurlyeq$ rozpadem jeho prvků do více exemplářů (prvek $\beta \in A/\sim$ se tedy jakoby rozpadá na všechna b obsažená v β, přičemž vztahy dané uspořádáním nijak narušeny nejsou). Pojmy definované pro uspořádání budeme používat i pro kvaziuspořádání, a to tímto způsobem:

Je-li $\mathcal{V}$ nějaká vlastnost prvků svazu, tak řekneme, že prvky $a_1, a_2, \ldots$ z A mají vlastnost $\mathcal{V}$ právě když ji mají prvky $[a_1]_\sim, [a_2]_\sim, \ldots$ svazu $(A/\sim, \preccurlyeq)$.

Tak například $a, b \in A$ jsou porovnatelné v $(A, \leq)$, jsou-li $[a]_\sim$ a $[b]_\sim$ porovnatelné v $(A/\sim, \preccurlyeq)$. Podobně definujeme v $(A, \leq)$ dolní a horní závory, infima a suprema, atomy a koatomy. Zápis $b = \inf_\leq B$ ovšem v kvaziuspořádání prvek b neurčuje jednoznačně, jednoznačně je určena pouze třída $[b]_\sim$ (je totiž $[b]_\sim = \inf_\preccurlyeq\{[c]_\sim;\, c \in B\}$).

Protože atomy kvaziuspořádání mají v dalším textu značný význam, uvedeme nyní výslovně podmínky, kdy $a \in A$ je atomem:

(i) A má (alespoň jeden) nejmenší prvek,

(ii) a není nejmenší prvek A,

(iii) je-li $c \in A$ a $c \leq a$, tak buď $c \sim a$, nebo je c nejmenší prvek A.

Kvaziuspořádání $\leq$ množiny A nazveme *noetherovské*, jestliže neexistuje nekonečná posloupnost prvků $a_1, a_2, a_3, \ldots$ z A taková, že pro každé $i \in \mathbb{N}$ je $a_i \geq a_{i+1}$, a současně neplatí $a_i \sim a_{i+1}$.

7.8 Tvrzení. *Buď $\leq$ noetherovské kvaziuspořádání množiny A a ať a je nejmenší prvek A. Potom pro každé $c \in A$ platí, že je buď $c \sim a$, nebo existuje atom $b \in A$ takový, že $b \leq c$.*

Důkaz. Předpokládejme, že není $c \sim a$. Položme $c_1 = c$ a ať $c_1, \ldots, c_n$ jsou takové prvky A, že pro $1 \leq i \leq n$ není $c_i \sim a$, a že pro $1 \leq i \leq n-1$ je $c_i \geq c_{i+1}$ a neplatí $c_i \sim c_{i+1}$. Jestliže c_n není atomem, existuje $c_{n+1} \in A$ takové, že $c_n \geq c_{n+1} \geq a$ a není ani $c_{n+1} \sim c_n$, ani $c_{n+1} \sim a$. Protože $\leq$ je noetherovské, lze takto zkonstruovat jen konečně mnoho členů posloupnosti $c_1, c_2, c_3, \ldots$ Proto musí existovat $n \in \mathbb{N}$, že c_n je atomem. □

8. Dělitelnost v komutativních monoidech

Buď $S = S(\cdot, 1)$ monoid. Řekneme, že $a \in S$ *dělí* (zleva) $b \in S$, jestliže existuje $c \in S$ takové, že $b = a \cdot c$. Symbolicky píšeme $a|b$ a a nazýváme *dělitelem* b.

8.1 Tvrzení. *Invertibilní prvky monoidu tvoří grupu.*

Důkaz. Podle 1.5 je součin dvou invertibilních prvků opět invertibilní. Je-li a invertibilní prvek a b je prvek k němu inverzní, tak je b také invertibilní. Podle 1.4 jsou inverzní prvky určeny jednoznačně. □

8.2 Tvrzení. *Relace dělitelnosti | v monoidu $S = S(\cdot, 1)$ je kvaziuspořádáním, přičemž 1 je jeho nejmenší prvek.*

Důkaz. Buď $a, b \in S$. Pak $1|a$, $a|a$, a z $a|b$ a $b|c$ plyne $a|c$. □

Jádro kvaziuspořádání | budeme, jak je obvyklé, značit ||. Je-li $a||b$, říkáme, že a a b jsou *asociovány*.

Uvědomte si, že z pouhého faktu, že | je kvaziuspořádání, plyne podle 7.6 několik důsledků. Jsou-li $a, b \in S$ asociovány, tak pro každé $c \in S$ například dostáváme $a|c \Leftrightarrow b|c$ a $c|a \Leftrightarrow c|b$.

Buď $B = \{b_1, \ldots, b_k\} \subseteq A$, $k \geq 1$. Místo $b = \inf_| B$ píšeme $b = \mathrm{NSD}(b_1, \ldots, b_k)$ a místo $b = \sup_| B$ píšeme $b = \mathrm{NSN}(b_1, \ldots, b_k)$. Přitom NSD znamená *největší společný dělitel* a NSN *nejmenší společný násobek*.

V každém kvaziuspořádání je $b \leq c$ právě když $b = \inf_{\leq}\{b, c\}$. Proto platí:

8.3 Lemma. *Buď $b, c \in S$. Pak $b = \mathrm{NSD}(b, c)$ právě když $b|c$.* □

Z 7.1, 7.6 a 7.7 okamžitě dostáváme:

8.4 Lemma. *Ať $b_1, \ldots, b_{n+1}$, kde $n \in \mathbb{N}$, jsou prvky monoidu S, a ať $c \in S$ je takové, že $c = \mathrm{NSD}(b_1, \ldots$ $\ldots, b_n)$. Potom $\mathrm{NSD}(b_1, \ldots, b_{n+1})$ existuje právě když existuje $\mathrm{NSD}(c, b_{n+1})$. Pokud tyto největší společní dělitelé existují, jsou asociovány.* □

V S tedy existují největší společní dělitelé, existuje-li $\mathrm{NSD}(b, c)$ pro libovolná $b, c \in S$. Totéž lze říci o největších společných násobcích. Z 7.7 plyne, že v S existují největší společní dělitelé a nejmenší společné násobky právě když uspořádaná množina $(S/||, |)$ je svaz.

Prvky $a, b \in S$ se nazývají *nesoudělné*, jestliže $1 = \mathrm{NSD}(a, b)$. Dělitel a prvku b se nazývá *vlastní*, jestliže neplatí ani $a||1$ ani $a||b$.

Budeme se zabývat především komutativními monoidy s krácením. Monoid S je *komutativní*, jestliže $b \cdot c = c \cdot b$ pro libovolná $b, c \in S$. Monoid S je *s krácením*, jestliže pro libovolná $a, b, c \in S$ z $a \cdot b = a \cdot c$ plyne $b = c$ a z $b \cdot a = c \cdot a$ rovněž plyne $b = c$.

Všimněte si, že prvek $a \in S$ je asociován s 1 (tedy je v kvaziuspořádání dělením nejmenší) právě když existuje $b \in S$ splňující $ab = 1$ (tedy právě když je a zprava invertibilní). V komutativním případě proto platí, že prvek je asociován s 1 právě tehdy, když je invertibilní, a že prvky asociované s 1 tvoří podmonoid monoidu $S(\cdot, 1)$ (který je podle 8.1 grupou).

8.5 Lemma. *Buď S komutativní monoid s krácením, a ať $a, b \in S$. Potom $a||b$ platí právě když existuje $u \in S$ invertibilní takové, že $b = a \cdot u$.*

Jestliže $a = bc$ pro nějaké $c \in S$, tak nastane jedna z následujících možností:

(i) b i c jsou vlastní dělitelé a,

(ii) b je invertibilní a $a||c$,

(iii) c je invertibilní a $a||b$.

Důkaz. Je-li $a||b$, existují $u, v \in S$ takové, že $a = bu$ a $b = av$. Tudíž $a = avu$, takže $vu = 1$. Jestliže $a = bu$ a u je invertibilní, lze nalézt $v \in S$ takové, že $uv = 1$, takže $b = buv = av$.

Je-li b (nebo c) invertibilní, tak $a||c$ (nebo $a||b$) platí podle prvé části lemmatu. Je-li $a||c$, tak existuje $u \in S$ takové, že $c = au$. Tudíž $a = bc = bau = abu$, a krácením dostáváme $1 = bu$, takže b je invertibilní. Podobně z $a||b$ plyne invertibilita c. □

Ve zbytku této kapitoly bude $S = S(\cdot, 1)$ vždy značit komutativní monoid s krácením, | kvaziuspořádání S dělitelností, a || jádro |.

Atomy kvaziuspořádání | budeme nazývat *ireducibilními* prvky.

8.6 Tvrzení. *Ať kvaziuspořádání | je noetherovské. Potom každý prvek S, který není invertibilní, lze vyjádřit jako součin ireducibilních prvků.*

Důkaz. Podle 7.8 má každý prvek S, který není invertibilní, ireducibilního dělitele. Ať $a = a_0$ není invertibilní. Budeme konstruovat posloupnost neinvertibilních prvků $a_0, a_1, \ldots$ a posloupnost ireducibilních prvků $p_1, p_2, \ldots$. Pokud a_i není ireducibilní, položíme $a_i = p_{i+1}a_{i+1}$ tak, aby p_{i+1} byl ireducibilní dělitel a_i. Potom je p_{i+1} vlastní dělitel a_i, takže podle 8.5 je i a_{i+1} vlastní dělitel a_i. Kdyby a_i nebyl ireducibilní pro žádné $i \in \mathbb{N}$, vznikla by nekonečná posloupnost $a_0, a_1, \ldots$, ve které by pro každé $i \in \mathbb{N}$ byl a_i vlastní dělitel a_{i-1}. Protože předpokládáme, že $|$ je noetherovské, existuje $n \in \mathbb{N}$ takové, že a_n je ireducibilní, takže $a = p_1 \ldots p_{n-1}a_n$. □

8.7 Lemma. *Buď $a, b, c \in S$ a ať $d = \mathrm{NSD}(a, b)$ a $e = \mathrm{NSD}(ac, bc)$. Potom $e||dc$.*

Důkaz. $dc|ac$ a $dc|bc$, takže $dc|e$ a $e = dcu$ pro nějaké $u \in S$. Ať $x, y \in S$ jsou takové, že $ac = ex$ a $bc = ey$. Pak $a = dux$, $b = duy$, a vidíme, že du je společný dělitel a a b. Proto $du|d$, takže $du||d$ a u je invertibilní podle 8.5. Proto $e||dc$. □

8.8 Lemma. *Buď $a, b, c \in S$ a ať a a b jsou nesoudělné. Jestliže $\mathrm{NSD}(ac, bc)$ existuje, tak z $a|bc$ plyne $a|c$.*

Důkaz. Podle 8.7 je $c = \mathrm{NSD}(a, b)c = \mathrm{NSD}(ac, bc)$. Odsud dostáváme $\mathrm{NSD}(a, c) = \mathrm{NSD}(a, ac, bc) = \mathrm{NSD}(a, bc) = a$, takže $a|c$. □

Prvek $p \in S$ se nazývá *prvočinitel*, jestliže není invertibilní, a pro každé $a, b \in S$ z $p|ab$ plyne, že $p|a$ nebo $p|b$.

8.9 Tvrzení. *Každý prvočinitel S je ireducibilní. Jestliže v S existují největší společní dělitelé, tak je každý ireducibilní prvek prvočinitel.*

Důkaz. Buď p prvočinitel, a ať $p = ab$. Z faktu, že p je prvočinitel, plyne $p|a$ (a pak $p||a$) nebo $p|b$ (a pak $p||b$). Ať naopak $p \in S$ je ireducibilní, $p|ab$, p nedělí a a $d = \mathrm{NSD}(p, a)$. Protože p nedělí a, není $d||p$. Protože p je ireducibilní a $d|p$, je $d||1$. Prvky p a a jsou tedy nesoudělné, a podle 8.8 z existence $\mathrm{NSD}(pb, ab)$ plyne $p|b$. □

8.10 Lemma. *Ať p je prvočinitel v S. Potom z $p|a_1 \ldots a_n$, kde $a_i \in S$, $1 \leq i \leq n$, plyne, že $p|a_j$ pro některé $1 \leq j \leq n$.*

Důkaz. Postupujme indukcí dle n. Pro $n = 2$ tvrzení vyplývá z definice prvočinitele. Položme $b = a_2 \ldots$ $\ldots a_n$. Pak p dělí $a_1 b$, čili p dělí a_1 nebo p dělí $a_2 \ldots a_n$. V druhém případě podle indukčního předpokladu existuje $2 \leq j \leq n$ takové, že $p|a_j$. □

Řekneme, že prvek $a \in S$ má *jednoznačný ireducibilní rozklad*, jestliže:
(i) existují $p_1, \ldots, p_r \in S$ ireducibilní a takové, že $a = p_1 \ldots p_r$,
(ii) kdykoliv $a = q_1 \ldots q_s \in S$, kdy $q_1, \ldots, q_s \in S$ jsou ireducibilní, tak $r = s$ a existuje permutace $\sigma \in S_r$, že $p_i||q_{\sigma(i)}$ pro $1 \leq i \leq r$.

(Jinými slovy ireducibilní rozklad je jednoznačný až na pořadí a $||$ ekvivalenci).

8.11 Tvrzení. *Jestliže v S je každý ireducibilní prvek prvočinitelem, tak jsou ireducibilní rozklady v S jednoznačné.*

Důkaz. Ať $p_1 \ldots p_n = q_1 \ldots q_m$, kde p_i, $1 \leq i \leq n$ a q_j, $1 \leq j \leq m$ jsou ireducibilní, a ať $n \leq m$. Z $q_1|p_1 \ldots p_n$ plyne podle 8.10, že můžeme předpokládat, že $q_1 = p_1 u$ pro u invertibilní. Je-li $n = 1$, dostáváme krácením $1 = uq_2 \ldots q_m$. Ovšem ireducibilní prvky nedělí 1, takže v tomto případě $m = 1$ a $p_1 = q_1$. Postupujme dále indukcí dle $n \geq 2$. Položme $q'_i = q_i$ pro $1 \leq i \leq n$, $i \neq 2$ a $q'_2 = up_2$. Pak $p_2 \ldots p_n = q'_2 \ldots q'_m$, a podle indukčního předpokladu $n = m$ a existuje $\sigma \in S_n$ takové, že $\sigma(1) = 1$ a $p_i||q'_{\sigma(i)}$. □

8.12 Tvrzení. *Ať každý neinvertibilní prvek má v S jednoznačný ireducibilní rozklad. Potom je každý ireducibilní prvek prvočinitel.*

Důkaz. Buď p ireducibilní prvek a ať $p|ab$. Pak existuje $c \in S$, tak že $cp = ab$. Použijeme 8.5, abychom vyjasnili případ, kdy některý z prvků a, b nebo c je invertibilní. Je-li invertibilní a, je $b||pc$, a proto p dělí b. Podobně dostáváme $p|a$, je-li b invertibilní. Je-li invertibilní c, je $p||ab$. Ovšem p nemá vlastního dělitele a oba prvky a a b nemohou být současně invertibilní (pak by totiž byl invertibilní i jejich součin, a tím i prvek p). Proto musí být $p||a$ nebo $p||b$. Předpokládejme nyní, že žádný z prvků a, b a c není

invertibilní, a ať jsou $a = a_1 \dots a_m$, $b = b_1 \dots b_s$ a $c = c_1 \dots c_t$ jejich ireducibilní rozklady. Potom $pc_1 \dots$ $\dots c_t = a_1 \dots a_r b_1 \dots b_s$ a z jednoznačnosti ireducibilních rozkladů plyne, že $p||a_i$ pro některé $1 \leq i \leq r$ (pak $p|a$) nebo $p||b_j$ pro některé $1 \leq j \leq s$ (pak $p|b$). □

8.13 Věta. *Buď $S = S(\cdot, 1)$ komutativní monoid s krácením, ve kterém každý neinvertibilní prvek má jednoznačný ireducibilní rozklad. Ať $P \subseteq S$ je taková množina ireducibilních prvků, že*

(i) kdykoliv $r \in S$ je ireducibilní, tak existuje $p \in P$, že $p||r$,

(ii) jsou-li $p_1, p_2 \in P$, tak $p_1||p_2$ právě pro $p_1 = p_2$.

Označme ještě I množinu všech invertibilních prvků. Potom platí:

(i) Každý prvek $a \in S$ lze (až na pořadí) jednoznačně vyjádřit ve tvaru $a = up_1^{k_1} \dots p_r^{k_r}$, kde $p_i \in P$, $k_i \in \mathbb{N}$ a $u \in I$ (přitom předpokládáme, že $p_i \neq p_j$ pro $1 \leq i < j \leq r$).

(ii) Je-li $a = up_1^{k_1} \dots p_r^{k_r}$ a $b = vp_1^{h_1} \dots p_r^{h_r}$, kde pro $1 \leq i \leq r$ je $p_i \in P$, $k_i \in \mathbb{N}_0$ a $h_i \in \mathbb{N}_0$, přičemž $u, v \in I$ a $p_i \neq p_j$ pro $1 \leq i < j \leq r$, tak $p_1^{\min(k_1,h_1)} \dots p_r^{\min(k_r,h_r)} = \mathrm{NSD}(a, b)$. Dále platí, že b dělí a právě když $h_i \leq k_i$ pro $1 \leq i \leq r$, přičemž b je vlastním dělitelem a, jestliže navíc existují $1 \leq s, t \leq r$ taková, že $h_s < k_s$ a $1 \leq h_t$.

Důkaz. (i) Jestliže a je invertibilní, tak nutně $u = a$, $r = 0$. Pokud a není invertibilní, existuje vyjádření $a = q_1 \dots q_s$, kde q_i, $1 \leq i \leq s$ jsou ireducibilní. Ovšem $q_i = u_i p_i$, kde $p_i \in P$ a $u_i \in I$, takže každý prvek lze jistě zapsat v požadovaném tvaru. Ať $a = up_1^{k_1} \dots p_r^{k_r} = vp_1^{h_1} \dots p_r^{h_r}$, kde $u, v \in I$, $p_i \in P$ a $k_i, h_i \in \mathbb{N}_0$. Ať přitom $p_i \neq p_j$ pro $1 \leq i < j \leq r$. Kdyby bylo například $k_1 < h_1$, tak $up_2^{k_2} \dots$ $\dots p_r^{k_r} = vp_1^{h_1 - k_1} p_2^{h_2} \dots p_r^{h_r}$, takže podle 8.2 a 8.10 $p_1||p_j$ pro některé $2 \leq j \leq r$. To však odporuje předpokládaným vlastnostem množiny P, a proto $k_i = h_i$ pro $1 \leq i \leq r$. Krácením dostáváme $u = v$, čímž je důkaz jednoznačnosti vyjádření uzavřen.
(ii) Ať $vp_1^{h_1} \dots p_r^{h_r} = b$ dělí $a = up_1^{k_1} \dots p_r^{k_r}$ a ať je například $h_1 \geq k_1$. Potom $vp_1^{h_1 - k_1} p_2^{h_2} \dots p_r^{h_r}$ dělí $up_2^{k_2} \dots p_r^{k_r}$ a z 8.2 a 8.10 plyne, že $h_1 - k_1 = 0$, čili $h_1 = k_1$. Proto $h_i \leq k_i$ pro $1 \leq i \leq r$. Hledejme nyní $\mathrm{NSD}(a, b)$, kde $a = up_1^{k_1} \dots p_r^{k_r}$ a $b = vp_1^{h_1} \dots p_r^{h_r}$. Buď $m_i = \min(k_i, h_i)$ pro $1 \leq i \leq r$. Z předchozího plyne, že $d = p_1^{m_1} \dots p_r^{m_r}$ dělí a i b. Ať c dělí rovněž a i b. Pak $c = wp_1^{c_1} \dots p_r^{c_r}$, kde $w \in I$ a $c_i \leq k_i$ a $c_i \leq h_i$ pro $1 \leq i \leq r$. Proto c dělí d, takže $d = \mathrm{NSD}(a, b)$.

Zkoumejme ještě, kdy $b = vp_1^{h_1} \dots p_r^{h_r}$ je vlastní dělitel $a = up_1^{k_1} \dots p_r^{k_r}$. Víme, že pak $h_i \leq k_i$ pro $1 \leq i \leq r$. Je-li $h_i = k_i$ pro všechna $1 \leq i \leq r$, je $a = uv^{-1}b$, takže $a||b$. Naopak, z $a||b$ plyne $h_i = k_i$ pro $1 \leq i \leq r$. Dále platí, že b je invertibilní právě když $h_1 = \dots = h_r = 0$. Proto je b vlastní dělitel a jedině tehdy, jestliže existují $1 \leq s, t \leq r$ taková, že $h_s < k_s$ a $1 \leq h_t$. □

8.14 Věta. *Buď $S = S(\cdot, 1)$ komutativní monoid s krácením. Pak následující podmínky jsou ekvivalentní.*

(i) V S má každý neinvertibilní prvek jednoznačný ireducibilní rozklad.

(ii) V S existují největší společní dělitelé a současně platí, že kvaziuspořádání dělitelností je noetherovské.

(iii) Každý ireducibilní prvek S je prvočinitelem a současně platí, že kvaziuspořádání dělitelností je noetherovské.

Důkaz. (ii) plyne z (i) podle 8.13.
(iii) plyne z (ii) podle 8.10.
(i) plyne z (iii) podle 8.6 a 8.11. □

8.15 Tvrzení. *Ať $S = S(\cdot, 1)$ je komutativní monoid s krácením, ve kterém existují největší společní dělitelé. Potom existují i nejmenší společné násobky, přičemž jsou-li $b, c, e, f \in S$ takové, že $e = \mathrm{NSD}(b, c)$ a $ef = bc$, je $f = \mathrm{NSN}(b, c)$. Uspořádání $S/||$ indukované dělitelností je v takovém případě svaz.*

Důkaz. Je-li $e = \mathrm{NSD}(b, c)$, tak $e|bc$, takže jistě existuje f takové, že $bc = ef$. Buď nejprve $e = 1$. Pak je třeba ukázat, že $bc = \mathrm{NSN}(b, c)$. Ať $b|h$, $c|h$ a $h = bg$. Potom $c|bg$, a podle 8.8 c dělí g. Tudíž $g = cx$, $h = bcx$, $bc|h$. Ať nyní $e \neq 1$, $b = eu$, $c = ev$. Pak $f = euv$ a pro $d = \mathrm{NSD}(u, v)$ platí, že $ed|e$. Proto $ed||e$ a $1 = \mathrm{NSD}(u, v)$. Ať $b|h$ a $c|h$. Pak $e|h$, a $h = ey$ pro nějaké $y \in S$. Krácením e dostáváme $u|y$, $v|y$, a podle prvé části důkazu platí $uv|y$. Tudíž $f = euv|ey = h$. □

9. Obory integrity

O prvku a komutativního okruhu $R = R(+,\cdot,-,0,1)$ řekneme, že je *dělitel nuly*, jestliže $a \neq 0$ a existuje $b \in R$, $b \neq 0$ takové, že $ab = 0$. Okruh $R = R(+,\cdot,-,0,1)$, který je komutativní, není triviální a je bez dělitelů nuly, se nazývá *obor integrity*. Všimněte si, že netriviální komutativní okruh R je oborem integrity právě když $R^{\#} = R \setminus \{0\}$ je podmonoid $R(\cdot,1)$.

Je-li R obor integrity a $a,b,c \in R^{\#}$, tak z $ab = ac$ plyne $a(b-c) = 0$, odkud $b - c = 0$, a tedy $b = c$. To znamená, že $R^{\#}(\cdot,1)$ je komutativní monoid s krácením.

9.1 Lemma. *Konečný obor integrity je komutativní těleso.*

Důkaz. Ať R je konečný obor integrity a $a \in R$, $a \neq 0$. Zobrazení $x \mapsto ax$ je injektivní, a protože R je konečné, je to permutace R. Proto existuje $b \in R$, že $ab = 1$. □

9.2 Lemma. *Buď R okruh. Potom $R[[x]]$ je obor integrity právě když R je obor integrity.*

Důkaz. Ať $a = \sum a_i x^i$ a $b = \sum b_j x^j$ jsou takové mocninné řady, že $a \neq 0 \neq b$. Položme $r = \min\{i;\ a_i \neq 0\}$ a $s = \min\{j; b_j \neq 0\}$. Ať $a \cdot b = \sum c_k x^k$. Pak $c_{r+s} = \sum_{i+j=r+s} a_i b_j = \sum_{i<r} a_i b_{r+s-i} + a_r b_s + + \sum_{s>j} a_{r+s-j} b_j = a_r b_s \neq 0$, takže $a \cdot b \neq 0$. □

Pro $a = \sum a_i x^i$ definujeme (formální) *derivaci* a'tak, že a' je mocninná řada $\sum (i+1) a_{i+1} x^i$. Všimněte si, že rovněž platí $a' = \sum_{i \geq 1} i a_i x^{i-1}$.

9.3 Tvrzení. *Buďte $a, b \in R[[x]]$ a $r \in R$. Pak $(a+b)' = a' + b'$, $(ab)' = a'b + ab'$ a $(ra)' = ra'$.*

Důkaz. Ať $a = \sum a_i x^i$, $b = \sum b_i x^i$. Pak $(a+b)' = \sum (i+1)(a_{i+1} + b_{i+1}) x^i = \sum (i+1) a_{i+1} x^i + + \sum (i+1) b_{i+1} x^i = a' + b'$. Dále $(ab)' = \sum_k ((k+1)(\sum_{i+j=k+1} a_i b_j)) x^k = \sum_k (\sum_{i+j=k+1} (i+j) a_i b_j) x^k = = \sum_k (\sum_{i+j=k+1} (i a_i) b_j) x^k + \sum_k (\sum_{i+j=k+1} a_i (j b_j)) x^k = \sum_k (\sum_{i+j=k} (i+1) a_{i+1} b_j) x^k + \sum_k (\sum_{i+j=k} a_i (j+ +1) b_{j+1}) x^k = a'b + ab'$. Konečně $(ra)' = r'a + ra' = ra'$, neboť $r' = 0$. □

9.4 Tvrzení. *Ať $a = \sum a_i x^i a\ b = \sum b_j x^j$ jsou nenulové polynomy nad oborem integrity R. Potom* $\deg(a \cdot b) = \deg a + \deg b$.

Důkaz. Ať $n = \deg a$ a $m = \deg b$ a $a \cdot b = \sum c_k x^k$. Podle 2.3 je $\deg(a \cdot b) \leq n + m$. Přitom $c_{n+m} = = \sum_{i+j=n+m} a_i b_j$ je rovno $a_n b_m$, neboť všechny ostatní sčítance ve vyjádření c_{n+m} jsou rovny nule. □

Připomeňme, že nenulové prvky okruhu R ztotožňujeme s polynomy nultého stupně.

9.5 Tvrzení. *Buď R obor integrity. Polynom $a \in R[x]$ je invertibilní právě když $\deg a = 0$ a a je invertibilní v R.*

Důkaz. Ať $a \cdot b = 1$. Pak $\deg a + \deg b = \deg 1 = 0$, takže $\deg a = \deg b = 0$. Zbytek je jasný. □

9.6 Věta. *Buďte R obor integrity a $a = \sum a_i x^i$ a $b = \sum b_i x^i$ dva polynomy nad R. Ať $m = \deg b \geq 0$ a b_m je invertibilní v R. Pak existují jednoznačně určené polynomy $q, r \in R[x]$ takové, že $a = bq + r$, kde* $\deg r < m$.

Důkaz. Dokažme nejprve, že uvedené polynomy skutečně existují. Položme $n = \deg a$. Je-li $m > n$, tak stačí položit $q = 0$ a $r = a$. Pro $n \geq m$ budeme postupovat indukcí dle $\delta = n - m$. Je-li $\delta = 0$, položíme $q = a_n b_n^{-1}$ a $r = a - qb$. Ať je $\delta > 0$. Položme $s = a_n b_m^{-1} x^{\delta}$ a $c = a - sb$. Pak $\deg c \leq \deg a = n$ a současně koeficient u x^n v c je roven $a_n - a_n b_m^{-1} b_m = 0$, takže $\deg c \leq n-1$. Podle indukčního předpokladu existují polynomy t a r takové, že $c = bt + r$, $\deg r < \deg b$. Potom $a = c + sb = bt + r + bp = b(t+p) + r$, a stačí položit $q = t + p$.

Ať $a = bq_1 + r_1 = bq_2 + r_2$ a ať platí $\deg r_1 < m$ a $\deg r_2 < m$. Potom b dělí $r_1 - r_2$ a z $r_1 - r_2 \neq 0$ by podle 9.3(ii) plynulo $\deg b \leq \deg(r_1 - r_2) < m$. To je spor, takže musí platit $r_1 = r_2$, a tím i $q_1 = q_2$. □

Buď R obor integrity. Zobrazení $\nu\colon R^{\#} \to \mathbb{N}_0$ (kde $R^{\#} = R \setminus \{0\}$) se nazývá *eukleidovskou funkcí*, jestliže pro libovolné $a, b \in R$ platí:

(i) pokud $a|b$ a $b \neq 0$, tak $\nu(a) \leq \nu(b)$,

(ii) pokud $a \neq 0 \neq b$, tak existují $q, r \in R$ takové, že $a = bq + r$, kde $r = 0$ nebo $\nu(r) < \nu(b)$.

Obor integrity R, pro který lze definovat alespoň jednu eukleidovskou funkci, se nazývá *eukleidovským oborem integrity* .

9.7 Věta. *Jestliže R je komutativní těleso, tak $R[x]$ je eukleidovský obor integrity, přičemž stupeň polynomu je eukleidovskou funkcí.*

Důkaz. Použij 9.4(ii) a 9.6. □

Obor integrity R se nazývá *oborem hlavních ideálů*, jestliže každý ideál R je hlavní ideál. Jinými slovy, obor hlavních ideálů je okruh hlavních ideálů, který je oborem integrity.

9.8 Tvrzení. *Každý eukleidovský obor integrity je oborem hlavních ideálů.*

Důkaz. Buď $\nu\colon R^\# \to \mathbb{N}_0$ eukleidovská funkce a ať I je nenulový ideál v R. Položme $t = \min\{\nu(b); 0 \neq b \in I\}$ a zvolme $a \in I$ tak, aby $\nu(a) = t$. Pak $aR \subseteq I$. Naopak, je-li $b \in I$, tak $b = aq + r$, kde $r = 0$ nebo $\nu(r) < \nu(a) = t$. Protože $r \in I$, tak z minimality t dostáváme $r = 0$, takže $b \in aR = I$. □

Obor integrity R se nazývá *Gaussův*, jestliže v $R^\#(\cdot, 1)$ má každý neinvertibilní prvek jednoznačný ireducibilní rozklad. (Ve Větě 8.14 jsou formulovány další ekvivalentní podmínky.)

Podle 4.4 je nejmenší ideál obsahující ideály I a J okruhu R roven $I + J$. Jsou-li $I_1, \ldots, I_k$ ideály okruhu R, tak podle 4.4 je nejmenší ideál obsahující $\bigcup(I_i, 1 \leq i \leq k)$ roven $\sum I_i = \{b_1 + \cdots + b_k; b_i \in I_i, 1 \leq i \leq k\}$. Je-li R komutativní a $I_i = a_iR$, tak $\sum I_i$ je nejmenší ideál obsahující prvky $a_1, \ldots, a_k$, přičemž tento ideál je tvořen všemi možnými součty $\sum u_ia_i, u_i \in R$. Mluvíme o ideálu *generovaném* prvky $a_1, \ldots, a_k$.

9.9 Tvrzení. *Buď R obor hlavních ideálů a $a_1, \ldots, a_n \in R$. Pak existují $u_1, \ldots, u_n \in R$ takové, že $\sum u_ia_i = \mathrm{NSD}(a_1, \ldots, a_n)$.*

Důkaz. Ať I je ideál generovaný prvky $a_1, \ldots, a_n$. Pak existuje $d \in R$, že $I = dR$, takže $d = \sum a_iu_i$. Současně $d|a_i$ pro $1 \leq i \leq n$. Jestliže $t|a_i$ pro $1 \leq i \leq n$, tak také $t|\sum a_iu_i = d$. □

9.10 Lemma. *Buď R obor hlavních ideálů. Pak kvaziuspořádání R dělitelností je noetherovské.*

Důkaz. Ať $a_0, a_1, \ldots$ je nekonečná posloupnost vlastních dělitelů. Potom pro $i \in \mathbb{N}_0$ je $a_iR \subsetneqq a_{i+1}R$. Snadno ověříme, že $I = \bigcup_i a_iR$ je ideál, a tedy existuje $d \in R$, pro které je $I = dR$. To ovšem znamená, že $d \in a_jR$ pro některé $j \in \mathbb{N}_0$, takže $a_jR = dR = a_{j+1}R$, spor. □

9.11 Důsledek. *Obory hlavních ideálů jsou Gaussovy.*

Důkaz. Použij 8.14, 9.9 a 9.10. □

9.12 Tvrzení. *Buď R obor hlavních ideálů. Potom $a \in R$ je prvočinitel právě když aR je maximální ideál v R.*

Důkaz. Prvek a je prvočinitel právě když je ireducibilní, tj. právě když není invertibilní a nemá vlastní dělitele. Buď I ideál, $R \supsetneqq I \supseteq aR$. Pak existuje $b \in R$, že $I = bR$. Ovšem $bR \supsetneqq aR$ jedině tehdy, jestliže b je vlastní dělitel a. □

Víme, že v eukleidovských oborech integrity existují největší společní dělitelé. Tyto obory integrity dostali svůj název podle prastarého algoritmu, který umožňuje největší společné dělitele účinně nacházet.

9.13 Tvrzení. (Eukleidův algoritmus.) *Buď R obor integrity a $\nu\colon R^\# \to \mathbb{N}_0$ eukleidovská funkce a ať a_0, a_1 jsou prvky $R^\#$. Budeme definovat posloupnost $a_0, a_1, \ldots$ takovýmto způsobem:*

(i) Je-li $i \geq 1$ a a_i nedělí a_{i-1}, tak zvolíme a_{i+1} tak, že pro nějaké $q_i \in R$ je $a_{i-1} = a_iq_i + a_{i+1}$ a $\nu(a_{i+1}) < \nu(a_i)$.

(ii) Je-li $i \geq 1$ a a_i dělí a_{i-1}, tak položíme $n = i$ a posloupnost ukončíme.

Takto vytvořená posloupnost je vždy konečná a $a_n = \mathrm{NSD}(a_0, a_1)$.

Důkaz. Konečnost posloupnosti plyne z toho, že $\nu(a_i) > \nu(a_{i+1})$. $\mathrm{NSD}(a_n, a_{n-1}) = a_n$, takže stačí ukázat, že pro každé $1 \leq i \leq n-1$ je $d||t$, kde $d = \mathrm{NSD}(a_{i-1}, a_i)$ a $t = \mathrm{NSD}(a_i, a_{i+1})$. Vidíme, že d dělí $a_{i+1} = a_{i-1} - a_iq$, takže $d|t$. Naopak, t dělí $a_{i-1} = a_iq + a_{i+1}$, takže $t|d$. □

Aplikujme nyní dosažené výsledky na eukleidovský obor integrity $T[x]$, kde T je komutativní těleso. Přitom na T hledíme jako na podokruh $T[x]$. Multiplikativní grupu tělesa T budeme označovat T^*. (Pro

těleso T je tedy T^* rovno $T^\#$; obecně pro okruhy tato rovnost však neplatí, neboť R^* označuje množinu (grupu) invertibilních prvků okruhu R.)

Invertibilní prvky $T[x]$ jsou nenulové prvky tělesa T (viz 9.5). Obor integrity $T[x]$ je eukleidovský (9.7), tedy obor integrity hlavních ideálů (9.8), tedy Gaussův (9.11).

Polynom $a = \sum a_i x^i \in T[x]$ nazveme *monický*, jestliže $a_{\deg a} = 1$ a $a \neq 0$. Každý nenulový polynom je zjevně asociován právě s jedním monickým polynomem. Z 8.13 plyne, že každý polynom $a \in T[x]$ stupně alespoň 1 lze napsat až na pořadí jediným způsobem jako $cp_1^{k_1} \dots p_r^{k_r}$, kde $p_1, \dots, p_r$ jsou navzájem různé monické ireducibilní polynomy, $k_1, \dots, k_r$ jsou přirozená čísla a $c \in T^*$ (přitom $c = a_{\deg a}$ a $\deg a = \sum k_i(\deg p_i)$).

Pro $a, b \in T[x]$ platí $aT[x] = bT[x]$ právě když jsou polynomy a, b v $T[x]$ asociovány (viz 7.6). Protože invertibilní prvky okruhu $T[x]$ se shodují s nenulovými prvky tělesa T (viz 9.5) a protože prvky jsou asociovány tehdy, liší-li se o invertibilní prvek (viz 8.10), vidíme, že $aT[x] = bT[x]$ platí právě když polynom a je roven tb pro nějaké $t \in T$. To znamená, že hlavní ideál $aT[x]$, $a \neq 0$, lze jediným způsobem vyjádřit jako $mT[x]$ tak, aby m byl polynom monický. Tudíž každý monický polynom obsažený v $aT[x]$ je buď roven m, nebo má stupeň vyšší než $\deg a = \deg m$. V okruhu $T[x]$ jsou všechny ideály hlavní, takže jsme dokázali, že každý nenulový ideál je jednoznačně charakterizován monickým polynomem, který ho generuje.

Prvek $\alpha \in T$ nazveme *kořenem* polynomu $a \in T[x]$, jestliže polynom $x - \alpha$ dělí a. Přitom $x - \alpha$ je podle 9.3(ii) a 9.5 ireducibilní prvek $T[x]$ pro každé $\alpha \in T$. Je-li $a = cp_1^{k_1} \dots p_r^{k_r}$ rozklad nenulového polynomu a na ireducibilní polynomy, tak ty z nich, které jsou tvaru $x - \alpha$, nazýváme *kořenovými* činiteli a. Jsou-li všechna $p_1, \dots, p_r$ stupně 1, říkáme, že a se *rozkládá na kořenové činitele*. Je-li p_i, $1 \leq i \leq r$, kořenový činitel, $p_i = x - \alpha$, tak číslo k_i nazýváme *násobností* kořenu α. Jestliže se a rozkládá na kořenové činitele, tak $\deg a = \sum k_i$. Počet kořenů, počítáme-li každý tolikrát, kolik činí jeho násobnost, je tedy menší nebo roven stupni polynomu, přičemž rovnost nastává právě když se polynom rozkládá na kořenové činitele. (Je třeba si uvědomit, že tyto výroky se týkají pouze nenulového polynomu.)

Komutativní těleso T, ve kterém se každý polynom $a \in T[x]$, $\deg a \geq 1$, rozkládá na kořenové činitele, se nazývá *algebraicky uzavřené*. Příkladem algebraicky uzavřeného tělesa je těleso komplexních čísel $\mathbb{C}$.

9.14 Tvrzení. *Buď T těleso, $0 \neq a \in T[x]$ a ať α je kořen a. Potom α je násobnosti alespoň 2 právě když je také kořenem a'.*

Důkaz. Ať je $a = (x - \alpha)b$ pro vhodné $b \in T[x]$. Máme $a' = b + (x - \alpha)b'$, takže $x - \alpha$ dělí a' právě když $x - \alpha$ dělí b. □

9.15 Důsledek. *Buď T těleso, $a \in T[x]$ a ať $\mathrm{NSD}(a, a') = 1$. Potom a nemá vícenásobné kořeny.* □

9.16 Tvrzení. *Buď $n \in \mathbb{N}$, T těleso a ať $\mathrm{char}\, T$ nedělí n. Pak polynomy $x^n - 1$ a $x^{n+1} - x$ nemají vícenásobné kořeny.*

Důkaz. Polynom $(x^n - 1)' = nx^{n-1} = (n \cdot 1)x^{n-1}$ je asociován s polynomem x^{n-1}, neboť z toho, že $\mathrm{char}\, T$ nedělí n, plyne $n \cdot 1 \neq 0$. Je $x^n - 1 = x \cdot x^{n-1} - 1$, a proto $\mathrm{NSD}(x^n - 1, x^{n-1}) = 1$.

Polynom $x^{n+1} - x = x \cdot (x^n - 1)$ má za kořeny nulu a všechny kořeny polynomu $x^n - 1$. Protože nula není kořenem polynomu $x^n - 1$, nemůže mít ani polynom $x^{n+1} - x$ jakýkoliv vícenásobný kořen. □

Jsou-li $S \supseteq R$ do sebe vřazené komutativní okruhy a α je prvek S, definujeme *dosazovací homomorfismus* $j_\alpha \colon R[x] \to S$ tak, že $j_\alpha(\sum a_i x^i) = \sum a_i \alpha^i$ pro každé $a = \sum a_i x^i \in R[x]$.

9.17 Lemma. *$j_\alpha \colon R[x] \to S$ je homomorfismus okruhů.*

Důkaz. Pro polynomy $a = \sum a_i x^i$ a $b = \sum b_j x^j$ jistě platí $j_\alpha(a + b) = j_\alpha(a) + j_\alpha(b)$. Podobně pro $a \cdot b = c = \sum c_k x^k$ je $j_\alpha(c) = \sum_k (\sum_{i+j=k} a_i b_j)\alpha^k = (\sum a_i \alpha^i)(\sum b_j \alpha^j) = j_\alpha(a) j_\alpha(b)$. □

Místo $j_\alpha(a)$ se většinou píše $a(\alpha)$. Ale označení j_α budeme pro dosazovací homomorfismus dále používat také.

9.18 Tvrzení. *Buď T komutativní těleso, $a \in T[x]$ a $\alpha \in T$. Pak α je kořen polynomu a právě když $a(\alpha) = 0$.*

Důkaz. Ať $a = (x - \alpha)b$ pro $b \in T[x]$. Podle 9.17 je $f_\alpha(a) = a(\alpha) = (\alpha - \alpha)b(\alpha) = 0$. Naopak, ať $a(\alpha) = 0$ a $a = (x - \alpha)q + r$, kde $\deg r \leq 0$ (čili $r \in T$). Potom $0 = a(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r$. □

Buď T komutativní těleso a ať $a \in T[x]$ je nenulový polynom. Podle 9.6 pro každé $b \in T[x]$ existuje jediné $r \in T[x]$, že $b \equiv r \bmod aT[x]$ a $\deg r < \deg a$. Jinými slovy, množina $U = \{u \in T[x]; \deg u < \deg a\}$ tvoří transversálu kongruence $\bmod aT[x]$. Je-li T konečné, $|T| = q$, $\deg a = n$, pak má U q^n prvků.

Okruh indukovaný transversálou U budeme značit $\big(T[x]\big)_a$. Sčítání v $\big(T[x]\big)_a$ odpovídá sčítání v $T[x]$, ale násobení je třeba počítat jako zbytek součinu v $T[x]$ po dělení polynomem a. Přitom $u \mapsto u + aT[x]$ poskytuje izomorfismus $\big(T[x]\big)_a \cong T[x]/aT[x]$. Je-li $aT[x]$ maximální ideál, je podle 4.6 okruh $\big(T[x]\big)_a$ komutativním tělesem. Přitom podle 9.12 je $aT[x]$ maximální ideál právě tehdy když a je ireducibilní.

Představme si, že T je rovno $\mathbb{Z}_p$, kde p je prvočíslo. Vidíme že stačí nalézt ireducibilní polynom stupně n, abychom uměli sestrojit těleso řádu p^n. Později ukážeme, že takový polynom vždy existuje a že všechna tělesa řádu p^n jsou vzájemně izomorfní.

9.19 Tvrzení. *Ať R je komutativní okruh a $a, b \in R$. Pak pro každé $n \in \mathbb{N}$ platí $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.* □

Uvedené tvrzení je známé jako binomická věta a jeho důkaz zde není třeba uvádět, neboť ho lze provést stejným postupem, jaký se používá při běžném důkazu binomické věty pro reálná čísla.

Je-li p prvočíslo a platí $1 \leq i < p$, tak je $\binom{p}{i}$ dělitelné číslem p (neboť $\binom{p}{i}$ lze zapsat ve tvaru zlomku, jehož jmenovatel není dělitelný p a čitatel je dělitelný p.) Činitele $\binom{p}{i} a^i b^{n-i}$ v zápisu binomické věty mají charakter iterovaného sčítání. (Zapisovali jsme je též ve tvaru $\binom{p}{i} \times a^i b^{n-i}$ — viz kapitola 5). Proto podle 5.7 platí

9.20 Důsledek. *Ať R je komutativní okruh charakteristiky p. Pak pro všechna $a, b \in R$ platí $(a+b)^p = a^p + b^p$.* □

9.21 Důsledek. *Ať R je komutativní okruh charakteristiky p. Pak zobrazení $a \mapsto a^p$ je endomorfismem tohoto okruhu.* □

Endomorfismus $a \mapsto a^p$ se nazývá často *Frobeniův endomorfismus.* Jestliže toto zobrazení iterujeme k-krát, dostaneme zobrazení $a \mapsto a^{p^k}$. To je v případě okruhů charakteristiky p samozřejmě také endomorfismem.

9.22 Tvrzení. *Ať T je komutativní těleso charakteristiky p a ať je $k \in \mathbb{N}_0$. Pak $U = \{a \in T;\ a^{p^k} = a\}$ je podtěleso T.*

Důkaz. Skutečnost, že U je uzavřeno na sčítání a násobení plyne z faktu, že $a \mapsto a^{p^k}$ je endomorfismus U. Je-li $a + b = 0$ (nebo $a \cdot b = 1$), je i $a^{p^k} + b^{p^k} = 0$ (nebo $a^{p^k} \cdot b^{p^k} = 1$). Protože opačné a inverzní prvky jsou určeny jednoznačně, plyne v těchto případech z $a \in U$ také $b \in U$. □

10. Cyklické grupy

Ať G je cyklická grupa generovaná prvkem g. Je-li $f: G \to H$ homomorfismus grup, tak z hodnoty $f(g) \in H$ můžeme odvodit hodnotu $f(a)$ pro každé $a \in G$. Musí totiž být $a = g^i$ pro nějaké $i \in \mathbb{Z}$, takže $f(a) = (f(g))^i$. Homomorfismus z cyklické grupy je tedy plně určen hodnotou obrazu svého generátoru.

Tuto skutečnost použijeme k popisu grupy endomorfismů cyklické grupy. Protože každá cyklická grupa je izomorfní $\mathbb{Z}(+,-,0)$ nebo $\mathbb{Z}_n(+,-,0), n \geq 1$, tak stačí popsat endomorfismy těchto grup.

10.1 Tvrzení.
(i) Zobrazení $a \mapsto ma$, kde m probíhá všechna celá čísla, jsou právě všechny endomorfismy $\mathbb{Z}(+,-,0)$.
(ii) Zobrazení $a \mapsto ma$, kde m probíhá $\mathbb{Z}_n, n \geq 0$, jsou právě všechny endomorfismy $\mathbb{Z}_n(+.-,0)$.

Důkaz. Daná zobrazení jsou jistě endomorfismy (například proto, že uvažované grupy lze pokládat za okruhy). Prvek 1 je v každé z uvažovaných grup generátorem. V již popsaném souboru endomorfismů existuje tedy pro každý prvek m dané grupy endomorfismus, jenž zobrazuje 1 na m. Proto nemohou žádné další endomorfismy existovat. □

Buď $n > 0$. Je-li $d > 0$ dělitel čísla n, $n = qd$, pak $d\mathbb{Z}_n = \{0, d, \ldots, (q-1)d\}$ je jistě jak podgrupa $\mathbb{Z}_n(+,-,0)$, tak ideál okruhu $\mathbb{Z}_n(+,\cdot,-,0,1)$. Přitom $d\mathbb{Z}_n$ má q prvků a je to cyklická grupa, přičemž d je její generátor.

10.2 Tvrzení. *Buď $n > 0$.*
(i) Je-li $a \in \mathbb{Z}_n, a \neq 0$, tak podgrupa $\mathbb{Z}_n(+,-,0)$, která je generována prvkem a, je rovna $d\mathbb{Z}_n$, kde $d = \mathrm{NSD}(a,n)$.
(ii) Je-li A netriviální podgrupa grupy $\mathbb{Z}_n(+,-,0)$, pak $A = d\mathbb{Z}_n$ pro nějaké $d > 0$, kde d dělí n.

Důkaz. Ať je $a \in \mathbb{Z}_n, a \neq 0$, a ať $d = \mathrm{NSD}(a,n)$. Ať $A = \{i \times a; i \in \mathbb{Z}\}$ označuje cyklickou podgrupu $\mathbb{Z}_n(+,-,0)$ generovanou prvkem a. Protože $d\mathbb{Z}_n$ i A jsou cyklické grupy, stačí k důkazu jejich rovnosti ověřit $d \in A$ a $a \in d\mathbb{Z}_n$. Podle 9.9 existují celá čísla u, v taková, že $d = au + nv$. Proto je $au \equiv d \bmod n$ a $d = u \times a \in A$. Naopak $a = qd$ pro nějaké $q > 0$, takže $a \in d\mathbb{Z}_n$.

Ať je nyní A nějaká netriviální podgrupa $\mathbb{Z}_n$. Položme $d = \min\{a \in A, a \neq 0\}$. Je-li $a \in A, a \neq 0$, pak $a = dq + r$ pro nějaká celá čísla q a r, $0 \leq r < d$. Pak $r = a - (q \times d)$ leží v A, takže je $r = 0$ a A je rovno $d\mathbb{Z}_n$. □

10.3 Důsledek. *Pro $A \subseteq \mathbb{Z}_n$, $n > 0$, jsou následující podmínky ekvivalentní:*
(i) A je podgrupa,
(ii) A je cyklická podgrupa,
(iii) A je ideál,
(iv) A je hlavní ideál,
(v) $A = d\mathbb{Z}_n$, kde $d = 0$ nebo d dělí n, $d > 0$. □

10.4 Důsledek. *Cyklická grupa G konečného řádu n obsahuje pro každé $d|n$ právě jednu podgrupu řádu d.* □

10.5 Tvrzení. *Buď $n > 1$. Pro $a \in \mathbb{Z}_n$ je ekvivalentní:*
(i) prvek a generuje $\mathbb{Z}_n(+,-,0)$,
(ii) a je invertibilní prvek okruhu $\mathbb{Z}_n$,
(iii) endomorfismus $i \mapsto ai$ grupy $\mathbb{Z}_n(+,-,0)$ je automorfismus.

Důkaz. Z $a\mathbb{Z}_n = \mathbb{Z}_n$ plyne $ab = 1$ pro nějaké $b \in \mathbb{Z}_n$. Proto (i) implikuje (ii).

Je-li $\varphi: i \mapsto ai$, tak $\mathrm{Im}\,\varphi$ je podgrupa $\mathbb{Z}_n$. To znamená, že φ je surjektivní (a tím i bijektivní — jde o konečné množiny) právě když $1 \in \mathrm{Im}\,\varphi$. To je ovšem splněno pokud je a invertibilní. Proto (ii) implikuje (iii).

Je-li φ automorfismus, musí a generovat $\mathbb{Z}_n(+,-,0)$, neboť automorfismus zobrazí generátor (kterým je například prvek 1) opět na generátor (kterým musí být prvek a). □

Buď $n > 1$. Počet invertibilních prvků okruhu $\mathbb{Z}_n$ je podle 10.5 a 10.2 roven počtu přirozených čísel k, $0 < k \leq n$, jež jsou nesoudělná s n. Tento počet se označuje $\varphi(n)$, přičemž φ se nazývá *Eulerova funkce*. Pro p prvočíslo je zjevně $\varphi(p) = p - 1$, $\varphi(1)$ je rovno 1.

Označme nyní na chvíli pro každé $a \in \mathbb{Z}_n$ a $n > 0$ prvek $b \in \mathbb{Z}_n$, $b \equiv a \bmod n$ jako $a \bmod n$.

Buď $n, m \in \mathbb{N}$ nesoudělná. Pak pro každé $a \in \mathbb{N}_0$ platí, že

(i) $\mathrm{NSD}(a,n) = \mathrm{NSD}(a \bmod n, n)$ a $\mathrm{NSD}(a,m) = \mathrm{NSD}(a \bmod m, m)$,

(ii) $\mathrm{NSD}(a, nm) = 1$ právě když $\mathrm{NSD}(a, n) = 1$ a $\mathrm{NSD}(a, m) = 1$.

Můžeme tedy říci, že $\mathrm{NSD}(a, nm) = 1$ právě když a mod n je invertibilní v $\mathbb{Z}_n$ a a mod m je invertibilní v $\mathbb{Z}_m$.

10.6 Lemma. *Ať $n, m \in \mathbb{N}$ jsou nesoudělná čísla. Pak $\varphi(nm) = \varphi(n)\varphi(m)$.*

Důkaz. Uvažme zobrazení $a \mapsto (a \bmod n, a \bmod m)$ ze $\mathbb{Z}_{nm}$ do $\mathbb{Z}_n \times \mathbb{Z}_m$. Ať $a, b \in \mathbb{Z}_{nm}$ se zobrazí stejně a $b \geq a$. Pak $(b-a) \bmod n = 0 = (b-a) \bmod m$, takže nm dělí $b-a$, a tudíž $a = b$. Zobrazení je injektivní, a proto i bijektivní. Počet invertibilních prvků $\mathbb{Z}_{nm}$ je tedy roven počtu dvojic $(u, v) \in \mathbb{Z}_n \times \mathbb{Z}_m$ takových, že u je invertibilní v $\mathbb{Z}_n$ a v je invertibilní v $\mathbb{Z}_m$. Takových dvojic je ovšem právě $\varphi(n)\varphi(m)$. □

10.7 Lemma. *$\varphi(p^r) = (p-1)p^{r-1}$ pro každé prvočíslo p a každé $r \in \mathbb{N}$.*

Důkaz. $a \in \mathbb{Z}_{p^r}$ není invertibilní právě když $p|a$. V $\mathbb{Z}_{p^r}$ je právě p^{r-1} násobků p. □

Z 10.6 a 10.7 okamžitě plyne:

10.8 Tvrzení. *Ať $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} \in \mathbb{N}$, kde $p_1 < p_2 < \dots < p_k$ jsou prvočísla a $r_i > 0$, $1 \leq i \leq k$. Pak $\varphi(n) = p_1^{r_1-1} p_2^{r_2-1} \dots p_k^{r_k-1}(p_1-1)(p_2-1)\dots(p_k-1)$.* □

Invertibilní prvky $\mathbb{Z}_n$, $n > 1$, tvoří multiplikativní grupu. Tato grupa má řád $\varphi(n)$. Řád každého jejího prvku proto musí dělit $\varphi(n)$ a $a^{\varphi(n)} = 1$ pro každé a z této grupy. Dokázali jsme:

10.9 Tvrzení. *Ať $a, n \in \mathbb{N}$ jsou nesoudělná čísla. Pak $a^{\varphi(n)} \equiv 1 \bmod n$.* □

(Pro n prvočíslo je vztah 10.9 známý jako Malá Fermatova věta.)

10.10 Tvrzení. *Buď $n \in \mathbb{N}$. Jestliže $k|n$, tak $\mathbb{Z}_n(+, -, 0)$ obsahuje právě $\varphi(k)$ prvků řádu k.*

Důkaz. Ať $r = \frac{n}{k}$. Podle 10.2 a 10.4 má $a \in \mathbb{Z}_n$ řád k právě když a generuje $r\mathbb{Z}_n \simeq \mathbb{Z}_k$. Ovšem $\mathbb{Z}_k$ má právě $\varphi(k)$ generátorů. □

10.11 Důsledek. *Buď $n \in \mathbb{N}$. Pak $n = \sum_{k|n} \varphi(k)$.* □

10.12 Tvrzení. *Buď T komutativní těleso a $G \subseteq T^*$ nějaká podgrupa (tj. G je množina uzavřená na násobení a inverzní prvky). Je-li G konečná, tak je cyklická.*

Důkaz. Položme $n = |G|$ a připomeňme, že řád každého prvku G dělí n (Lagrangeova věta). Pro dělitel k čísla n označme t_k počet prvků řádu k. Protože každý prvek má nějaký řád, musí platit $n = \sum t_k$. Grupa G bude cyklická, je-li $t_n \geq 1$ (a pak je $t_n = \varphi(n)$, kde φ označuje Eulerovu funkci). Podle 8.14 máme $n = \sum \varphi(k)$. Není-li G cyklická, je $0 = t_n < \varphi(n)$, takže pro nějaký vlastní dělitel k čísla n musí platit $t_k > \varphi(k)$. Předpokládejme, že tomu tak je, zvolme prvek $a \in G$ řádu k, a označme A podgrupu tímto prvkem generovanou. Ta má k prvků, z nichž $\varphi(k)$ má řád k. Z $t_k > \varphi(k)$ plyne, že musí existovat alespoň jeden prvek $b \in G$, jenž je řádu k, ale neleží v A. Každý prvek A je kořenem polynomu $x^k - 1$. Ale i prvek b je kořenem tohoto polynomu. To znamená, že polynom $x^k - 1$ má přinejmenším $|A| + 1 = k + 1$ různých kořenů. To je ovšem spor, takže grupa G skutečně musí být cyklická. □

11. Grupy a jejich reprezentace

Teorie Abelových grup a obecných nekomutativních grup se dosti odlišuje — například všechny konečné Abelovy grupy lze poměrně snadno popsat jako součin grup cyklických, avšak teorie konečných grup je velmi obsáhlá a složitá. Přitom je patrné, že počet a rozmanitost konečných grup je takového stupně, že nelze uvažovat o jejich popisu nějakým výčtem. Proto je důležité vybudovat takové pojmy, které by dovolovaly alespoň hrubou klasifikaci (konečných) grup.

Ať $A(+,-,0)$ je Abelova grupa. Prvek $g \in A$ se nazývá *torzní*, jestliže je $ng = 0$ pro nějaké $n > 0$. Jinými slovy, prvek je torzní, je-li konečného řádu. Sama grupa A se pak nazývá *torzní*, jsou-li torzní všechny její prvky. Množině všech torzních prvků grupy A se říká její *torzní část*. Je-li $na = 0 = mb$ pro $a, b \in A$ a $n, m \in \mathbb{N}$, je $nm(a+b) = 0$, takže vidíme, že torzní část tvoří podgrupu A.

Ať je $p > 0$ nějaké prvočíslo a položme $A_{(p)} = \{a \in A;\ p^k a = 0 \text{ pro nějaké } k \geq 0\}$. Je-li $p^r a = 0 = p^s b$, je $p^{\max(r,s)}(a+b) = 0$, takže $A_{(p)}$ je podgrupa A. Této podgrupě se říká *p-primární komponenta*.

Ať $a \in A$ je prvek řádu $n = p_1^{k_1} \dots p_r^{k_r}$, kde $2 \leq p_1 < \dots < p_r$ jsou prvočísla a $k_i \geq 1, 1 \leq i \leq r$. Položme $q_i = n/p_i^{k_i}$ a ať h_i jsou taková, že $1 = \sum h_i q_i, 1 \leq i \leq r$. Existence čísel h_i plyne z 9.9, neboť $\mathrm{NSD}(q_1, \dots, q_r) = 1$. Pak a je rovno $\sum (q_i h_i)a$, přičemž $p_i^{k_i}(q_i h_i)a = (nh_i)a = h_i(na) = 0, 1 \leq i \leq r$. Vidíme, že každý prvek $a \in A$ je možno vyjádřit jako součet konečně mnoha prvků, z nichž každý patří do nějaké p-primární komponenty, p prvočíslo. Množinu všech prvočísel označíme $\mathbb{P}$.

11.1 Tvrzení. *Ať $A(+,-,0)$ je torzní Abelova grupa. Definujme zobrazení $f\colon \bigoplus_{p\in\mathbb{P}} A_{(p)} \to A$ tak,že $f(a) = \sum_{p\in\mathbb{P}} a(p)$. Pak f je izomorfismus grup.*

Důkaz. Podle předchozího je možné každý prvek vyjádřit jako součet prvků z p-primárních komponent. Proto je f surjektivní. Jsou-li $a, b \in \bigoplus A_{(p)}$, je $f(a+b) = \sum (a+b)(p) = \sum a(p) + \sum b(p) = f(a) + f(b)$. Zbývá tedy ukázat, že je $\mathrm{Ker}\, f = 0$. Ať jsou $a \in \mathrm{Ker}\, f$, $p \in \mathbb{P}$, $Q = \mathbb{P} \setminus \{p\}$ a $b = f(a) - a(p)$. Pak $b = \sum_{q\in Q} a(q)$ a je-li n součin řádů prvků $a(q)$, $q \in Q$, je $nb = 0$, přičemž p nedělí n. Pak $n \cdot a(p)$ je podle 10.5 stejného řádu jako $a(p)$, přičemž $a(p) = -b$ implikuje $n \cdot a(p) = 0$. Je tedy $a(p) = 0$, a tedy i $a = 0$. □

O prvcích g, h grupy $G = G(\cdot, {}^{-1}, 1)$ řekneme, že jsou *konjugované*, jestliže existuje $a \in G$, že $h = aga^{-1}$. Pišme $h \backsim g$, je-li h konjugované s g.

11.2 Lemma. *Relace $\backsim$ je ekvivalence na G.*

Důkaz. Volbou $a = 1$ dostáváme $g \backsim g$ a přechodem k a^{-1} ověříme $h \backsim g \iff g \backsim h$. Ať $h = aga^{-1}$ a $k = bhb^{-1}$. Pak $k = (ba)g(ba)^{-1}$. □

Ke každé permutaci $\alpha \in S_n$ s (úplným) cyklickým zápisem $(a_{11} \dots a_{1k_1}) \dots (a_{m1} \dots a_{mk_m})$ se definuje její typ $t_1, t_2, t_3, \dots$ tak, že t_j udává počet cyklů délky j (tedy počet $i, 1 \leq i \leq m$, že $k_i = j$). (Například permutace $(12)(34)$ z S_4 má typ $0, 2, 0, \dots$).

Je-li $\varphi \in S_n$, je $\varphi\alpha\varphi^{-1}$ rovno $(\varphi(a_{11}) \dots \varphi(a_{1k_1})) \dots (\varphi(a_{m1}) \dots \varphi(a_{mk_m}))$. Vidíme, že dvě permutace mají stejný typ právě tehdy, jsou-li v S_n konjugované.

Je-li N normální podgrupa S_n, tak s každým $\alpha \in N$ musí v N ležet všechny permutace téhož typu. Ukazuje se, že pro $n \neq 4$ může být N rovno buď jedné ze dvou nevlastních normálních podgrup (tj. S_n nebo 1), nebo alternující grupě $A_n = \mathrm{Ker}\,\mathrm{sgn}$, kde $\mathrm{sgn}\colon S_n \to \{+1, -1\}$ je zobrazení, jež udává znaménko permutace (v základním kurzu lineární algebry se ukazuje, že sgn je homomorfismus grup).

Grupa, která nemá vlastní normální podgrupu a která není triviální se nazývá *jednoduchá*. Grupa sudých permutací A_n je jednoduchá pro každé $n \geq 2$, $n \neq 4$.

Pro $n = 4$ tvoří *Kleinova grupa* $\{(1)(2)(3)(4), (12)(34), (13)(24), (14)(23)\}$ normální podgrupu jak S_n, tak A_n. Důkaz je snadný. Nejprve ověříme, že uvedený systém permutací je uzavřený na skládání a poté si všimneme, že obsahuje všechny permutace z S_4 typu $(0, 2, 0 \dots)$.

V mnoha aplikacích je velmi důležité vědět o způsobech, kterými lze danou grupu vnořit do nějaké významné grupy — například S_Ω, kde Ω je určitá množina, nebo do grupy $M_n^*(T)$ invertibilních (tj. regulárních) matic řádu n nad tělesem T.

Každý homomorfismus $G \to S_\Omega$ se nazývá *působení (akce)* G na Ω, každý homomorfismus $G \to M_n^*(T)$ se nazývá (maticovou) *reprezentací*. Je-li jádro uvedených homomorfismů triviální, mluvíme o *věrném působení* a *věrné reprezentaci* G.

Působení na množině i maticové reprezentace lze samozřejmě definovat i pro monoidy a pologrupy (pak jde o homomorfismy do T_Ω a do monoidu $M_n(T)(\cdot, 1)$).

Připomeňme, že pro binární operaci $\cdot$ na S značí L_a, $a \in S$, levou translaci $x \mapsto ax$.

11.3 Tvrzení. *Ať $M(\cdot, 1)$ je monoid. Pak zobrazení $a \mapsto L_a$ je věrným působením monoidu M na množině M.*

Důkaz. Pro $a, b \in M$ je $L_{ab}(x) = (ab)x = a(bx) = L_a(L_b(x))$ pro každé $x \in M$, takže $L_{ab} = L_a L_b$. Odtud vidíme, že jde o působení. Z $L_a = L_b$ plyne $a = L_a(1) = L_b(1) = b$, takže jde o působení věrné. □

Působení uvedené v předchozím tvrzení se nazývá *regulární*. Je-li G grupa, tak je L_a permutace G pro každé $a \in G$ podle 3.4. Pro každou grupu proto existuje alespoň jedno věrné působení na množině. Nyní zkonstruujeme pro každou podgrupu H grupy G jisté působení (které však již nemusí být vždy věrné) tak, aby regulární působení odpovídalo volbě $H = 1$.

11.4 Tvrzení. *Ať G je grupa a H její podgrupa. Položme $\Omega = \{bH, b \in G\}$; a definujme $\varphi: G \to S_\Omega$ tak, že $\varphi(a)(bH) = (ab)H$ pro všechna $a, b \in G$. Potom φ je působení G na Ω.*

Důkaz. Ať $a, b, c \in H$. Je-li $bH = cH$ je $(ab)H = (ac)H$, takže zobrazení $\varphi(a) \in T_\Omega$ je definováno korektně. Dále $(\varphi(a)\varphi(b))(cH) = \varphi(a)(\varphi(b)(cH)) = (ab)(cH) = \varphi(ab)(cH)$ poskytuje $\varphi(ab) = \varphi(a)\varphi(b)$ pro všechna $a, b \in H$. Protože platí $\varphi(a)\varphi(a^{-1}) = \varphi(a^{-1})\varphi(a) = \mathrm{id}_\Omega = \varphi(1)$, je $\varphi(a) \in S_\Omega$, takže φ je homomorfismus podle 5.5. □

11.5 Důsledek (Poincarého věta). *Ať H je podgrupa grupy G a platí $|G{:}H| = n$, $n \in \mathbb{N}$. Pak existuje $N \subseteq H$ normální podgrupa G, jež splňuje $|G{:}N| \leq n!$.*

Důkaz. Množina Ω má n prvků, takže je $|\operatorname{Im}\varphi| \leq |S_\Omega| = n!$. Položme $N = \operatorname{Ker}\varphi$. Pro $a \in N$ je $\varphi(a) = \mathrm{id}_\Omega$, takže speciálně platí $aH = H$, a tedy $a \in H$. Obecně platí, že pro každé $\alpha \in \operatorname{Im}\varphi$ je $\varphi^{-1}(\alpha)$ rovno nějakému bloku $\ker f$, a tedy vlastně prvku G/N, takže $|\operatorname{Im}\varphi| = |G{:}N|$. □

Uvažme nyní permutaci $\alpha \in S_n$ a definujme k ní 0,1-matici $M(\alpha)$ řádu n tak, že $M(\alpha)_{i,j} = 1$ právě když $\alpha(j) = i$. Je-li $\beta \in S_n$ nějaká další permutace, tak $M(\alpha)M(\beta)$ má na místě (i, j) hodnotu různou od 0 jen tehdy, existuje-li k tak, že $M(\alpha)_{i,k} \neq 0$ a $M(\beta)_{k,j} \neq 0$. Tyto podmínky lze vyjádřit jako $\alpha(k) = i$ a $\beta(j) = k$. Přičemž vidíme, že takové k může existovat nanejvýš jedno, a jeho existenci lze vyjádřit jako $(\alpha \circ \beta)(j) = i$. To znamená , že $M(\alpha \circ \beta) = M(\alpha)M(\beta)$ pro všechna $\alpha, \beta \in S_n$. Přitom $M(1) = M(1_{S_n})$ je rovno jednotkové matici, $M(\alpha)M(\alpha^{-1}) = M(1) = M(\alpha^{-1})M(\alpha)$ platí pro každé $\alpha \in S_n$. Vidíme, že $M(\alpha)$ je matice regulární (lze také snadno ukázat, že je $\det M(\alpha) = \operatorname{sgn}(\alpha)$). Můžeme tedy vyslovit

11.6 Tvrzení. *Ať T je těleso a $n \in N$. Pak $\alpha \mapsto M(\alpha)$ je věrnou reprezentací S_n nad T.* □

Z libovolného působení grupy G na nějaké n-prvkové množině $\Omega = \{\omega_1, \ldots, \omega_n\}$ můžeme ztotožněním ω_i a i dostat reprezentaci $g \mapsto M(\varphi(g))$. Vyjdeme-li přitom z regulárního působení, dostaneme tak takzvanou *regulární reprezentaci*. To ovšem nejsou reprezentace jediné. Například přiřazení $i \mapsto \cos(\frac{i}{n}2\pi) + \mathrm{i}\sin(\frac{i}{n}2\pi)$ je věrná reprezentace $\mathbb{Z}_n$, $n \in \mathbb{N}$, maticemi řádu 1 v tělese $\mathbb{C}$. Jiný, trochu složitější příklad uvedeme níže.

11.7 Lemma. *Ať $A = (a_{ij})$, $B = (b_{ij})$ a $C = (c_{ij})$ jsou čtvercové matice řádu n nad komutativním tělesem T. Předpokládejme, že B je regulární a že $C = BAB^{-1}$. Pak $\sum_{i=1}^n a_{ii} = \sum_{i=1}^n c_{ii}$.*

Důkaz. Položme $B^{-1} = (b'_{ij})$. Pak $\sum_j b'_{kj} b_{ji} = \delta_{ik}$ pro všechna i a k, kde $1 \leq i \leq n$ a $1 \leq k \leq n$. Vyjdeme-li ze vzorce pro násobení matic, tak platí $\sum_i c_{ii} = \sum_{i,j,k} b_{ij} a_{jk} b'_{ki} = \sum_{j,k} a_{jk}(\sum_i b'_{ki} b_{ij}) =$ $= \sum_j a_{jj}$. □

Je-li $A = (a_{ij})$ čtvercová matice řádu n, tak $\sum_{i=1}^n a_{ii}$ se nazývá *stopa* matice A a značí se $\operatorname{Tr} A$. Z 11.7 plyne, že podobné matice mají stejnou stopu.

Je-li nyní $\varphi: G \to M_n^*(T)$ reprezentace a T je komutativní těleso, nazývá se zobrazení $\chi = \chi_\varphi$, $\chi(g) =$ $= \operatorname{Tr}(\varphi(g))$ pro každé $g \in G$, *charakterem* grupy G. Charakterem je tedy každé zobrazení $G \to T$, které je rovno χ_φ pro nějakou reprezentaci φ.

11.8 Lemma. *Ať T je komutativní těleso G grupa a $\chi: G \to T$ charakter. Jsou-li g a h konjugované prvky G je $\chi(g) = \chi(h)$.*

Důkaz. Ať $\chi = \chi_\varphi$ pro reprezentaci φ. Existuje $a \in G$, že $g = aha^{-1}$, takže matice $\varphi(g) = \varphi(a)\varphi(h)\varphi(a^{-1})$ je podobná matici $\varphi(h)$. Zbytek plyne z 11.7. □

Vidíme, že charaktery lze chápat jako zobrazení z $G/\backsim$ do T, kde $\backsim$ značí ekvivalenci konjugace. Studiem takových zobrazení lze poměrně rychle získat mnoho hlubokých poznatků o reprezentacích grup. To by však přesahovalo rámec úvodního kurzu obecné algebry.

Ještě ukážeme souvislost reprezentací grup a modulů nad grupovými okruhy.

11.9 Tvrzení. *Ať T je komutativní těleso, $n \in \mathbb{N}$ a $\varphi: G \to M_n^*(T)$ reprezentace grupy G. Označme písmenem V standardní vektorový prostor nad T dimenze n. Pak V lze chápat jako levý modul grupového okruhu TG, jestliže pro každé $a = \sum a_g g \in TG$ a $u = (u_1, \dots, u_n) \in V$ položíme $a \cdot u = \sum a_g(\varphi(g) \cdot u^T)$ (kde u^T je sloupcová matice tvořená hodnotami $u_1, \dots, u_n$).*

Důkaz. Zobrazení $\varphi: G \to M_n^*(T)$ můžeme rozšířit na zobrazení $\psi: TG \to M_n^*(T)$ tak, že $\psi(\sum a_g g) = \sum a_g \varphi(g)$. Je zřejmé, že ψ je slučitelné se sčítáním. Dokážeme, že pro $a = \sum a_g g$ a $b = \sum b_h h$, kde g i h probíhají G, je $\psi(a)(\psi(b)(u^T)) = \psi(ab)(u^T)$ pro všechna $u \in V$. Vskutku $\psi(a)(\psi(b)(u^T)) = \psi(a)\sum_h (b_h \varphi(h))(u^T) = \sum_{g,h} a_g b_h \varphi(g)(\varphi(h)(u^T)) = \sum_k \big(\sum_{gh=k} a_g b_h\big)\varphi(k)(u^T) = \psi(a \cdot b)(u^T)$. Tím je dokázána rovnost $a \cdot (b \cdot u) = (a \cdot b) \cdot u$. Ostatní vztahy se ověří zcela přímočaře. □

Na závěr této kapitoly uvedeme jako příklad reprezentace a charaktery symetrické grupy S_3 nad $\mathbb{C}$. V této grupě má ekvivalence $G/\backsim$ tři bloky — označme je I (identita), D (dva dvojcykly) a T (tři transpozice). Každý charakter lze podle 11.8 chápat jako zobrazení z $\{I, D, T\}$ do $\mathbb{C}$.

Existují tři (takzvané ireducibilní) charaktery, označme je χ_0, χ_1 a χ_2. Jsou definovány tak, že $\chi_0(I) = \chi_0(D) = \chi_0(T) = 1$, $\chi_1(I) = \chi_1(D) = 1$ a $\chi_1(T) = -1$ a $\chi_2(I) = 2$, $\chi_2(D) = -1$ a $\chi_2(T) = 0$.

Tyto charaktery jsou lineárně nezávislé, takže každou lineární funkci $\varphi: V \to \mathbb{C}$, kde V je vektorový prostor s bazí $\{I, D, T\}$, lze zapsat jako jejich lineární kombinaci. Lze dokázat, že tomu tak je vždy — totiž, že pro každou konečnou grupu existují jakési charaktery (říká se jim, jak jsme již uvedli, ireducibilní), kterých je stejně jako bloků ekvivalence $\backsim$, a které jsou lineárně nezávislé. Existují metody, jak tyto charaktery počítat bez toho, že by se počítaly jim odpovídající reprezentace. Jejich popis by však byl mimo rámec tohoto úvodního kurzu.

Charakter χ_0 lze získat z triviální reprezentace $\varphi_0: S_3 \to M_1^*(\mathbb{C}) = \mathbb{C}^*$, kde $\varphi_0(g) = 1$ pro všechna $g \in G$.

Za φ_1 můžeme vzít znaménko permutace sgn, když sgn interpretujeme jako zobrazení z S_3 do $\mathbb{C}^*$. (Je $\operatorname{Im}\operatorname{sgn} = \{-1, 1\}$ a $\operatorname{Ker}\operatorname{sgn} = A_3 = I \cup T$.)

Teprve χ_2 vyžaduje maličko náročnější konstrukci. Zvolme za A matici $\begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix}$, kde $\alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2}$ (takže $\bar{\alpha} = -\frac{1}{2} - \frac{\sqrt{3}}{2}$), a za U matici $\begin{pmatrix} 0 & b^{-1} \\ b & 0 \end{pmatrix}$, kde b je libovolné nenulové číslo. Označme jeden z prvků D jako a a jeden z prvků T jako u, a definujme φ_2 tak, že $\varphi_2(a^{\pm 1}) = A^{\pm 1}$, $\varphi_2(u) = U$, $\varphi_2(au) = AU$ a $\varphi_2(ua) = UA$. Identita se samozřejmě musí zobrazit na jednotkovou diagonální matici. Ověřit, že φ_2 je (věrná) reprezentace S_3 s charakterem χ_2 je nyní již snadné.

12. Torzní součiny

Ať R je okruh. Hovoříme-li o modulu ${}_RM$, míníme tím levý modul M nad okruhem R. Podobně se N_R vztahuje k pravému modulu N nad R.

Pro každou Abelovu grupu A lze definovat skalární násobení $\mathbb{Z} \times A \to A$ vztahem $n \cdot a = n \times a$ pro všechna $n \in \mathbb{Z}$ a $a \in A$. Lze snadno ověřit, že každé takto definované skalární násobení splňuje požadavky kladené na levý modul A nad $\mathbb{Z}$ (rovnost $(n+m) \cdot a = n \cdot a + m \cdot a$ je dokázána v 5.6 (iii), z ní indukcí plyne $n \cdot (ma) = (nm) \cdot a$; rovnost $n \cdot (a+b) = n \cdot a + m \cdot b$ je okamžitý důsledek komutativity sčítání). Proto A můžeme považovat za modul ${}_{\mathbb{Z}}A$. Jelikož u komutativních okruhů není mezi levými a pravými moduly rozdíl, tak lze mluvit i o modulu $A_{\mathbb{Z}}$.

(Je-li totiž R komutativní okruh a M je levý modul nad R, tak skalární násobení $\circ$ definované vztahem $a \circ r = r \cdot a$ poskytuje strukturu pravého modulu. Klíčovou rovností při ověřování je vztah $a \circ (r \cdot s) = = (r \cdot s) \cdot a = (s \cdot r) \cdot a = s \cdot (r \cdot a) = (r \cdot a) \circ s = (a \circ r) \circ s$.)

Vedle okruhu R budeme uvažovat ještě okruh S. Mluvíme o *bimodulu* ${}_RM_S$ (nebo R,S-bimodulu M), jestliže

(i) M je levý modul nad R,
(ii) M je pravý modul nad S, a
(iii) $(r \cdot m) \cdot s = r \cdot (m \cdot s)$ pro všechna $r \in R$, $s \in S$ a $m \in M$.

Je zřejmé, že každý modul nad komutativním okruhem R lze považovat za bimodul ${}_RM_R$. Je-li R obecný okruh a M pravý modul nad R, tak pro všechna $n \in \mathbb{Z}$, $r \in R$ a $m \in M$ máme $n \times (m \cdot r) = = (n \times m) \cdot r$, takže M_R je též bimodul ${}_{\mathbb{Z}}M_R$. Podobně lze ${}_RM$ považovat za bimodul ${}_RM_{\mathbb{Z}}$. Ať jsou nyní R, S a T okruhy a ať jsou dány bimoduly ${}_RM_S$ a ${}_SN_T$. Naším cílem bude zkonstruovat bimodul ${}_R(M \otimes N)_T$, který se nazývá *torzním součinem* (bi)modulů M a N.

Pro každé $m \in M$ a $n \in N$ označíme $U_{m,n}$ Abelovu grupu definovanou na množině $\{i(m,n);\ i \in \mathbb{Z}\}$ tak, že $i(m,n)+j(m,n) = (i+j)(m,n)$ pro všechna celá i a j. Zobrazení $i \mapsto i(m,n)$ je tedy izomorfismus $\mathbb{Z}$ a $U_{m,n}$.

Položíme $U = \bigoplus_{(m,n) \in M \times N} U_{m,n}$. Grupa U je izomorfní direktní sumě takového počtu kopií $\mathbb{Z}(+,-,0)$, kolik je velikost (mohutnost) množiny $M \times N$. Její prvky můžeme zapisovat ve tvaru $\sum c_{m,n}(m,n)$, přičemž jen konečně mnoho koeficientů $c_{m,n}$ je nenulových. Místo $1 \cdot (m,n)$ a $(-1) \cdot (m,n)$ píšeme pouze (m,n) a $-(m,n)$.

Na U definujeme skalární násobení zleva tak, že $r \cdot (\sum c_{m,n}(m,n)) = \sum c_{m,n}(r \cdot m, n)$ pro každý prvek U a každé $r \in R$. Je-li $u \in U$, tak jistě platí $(r_1 + r_2) \cdot u = r_1 \cdot u + r_2 \cdot u$ a $r_1 \cdot (r_2 \cdot u) = (r_1 \cdot r_2) \cdot u$ pro libovolná $r_1, r_2 \in R$. Podobně je zřejmé $r \cdot (u_1 + u_2) = r \cdot u_1 + r \cdot u_2$, kde $r \in R$ a $u_1, u_2 \in U$, takže vidíme, že U je levý modul nad R.

Analogicky vztah $(\sum c_{m,n}(m,n)) \cdot t = \sum c_{m,n}(m, n \cdot t)$ poskytuje na U strukturu pravého modulu nad T. Je-li $u = \sum c_{m,n}(m,n) \in U$, $r \in R$ a $t \in T$, tak $(r \cdot u) \cdot t = (\sum c_{m,n}(r \cdot m, n)) \cdot t = \sum c_{m,n}(r \cdot m, n \cdot t) = = r \cdot (\sum c_{m,n}(m, n \cdot t)) = r \cdot (u \cdot t)$, takže vidíme, že můžeme mluvit o bimodulu ${}_RU_T$.

Definujme nyní podmnožiny A_R, A_S a A_T Abelovy grupy $U(+,-,0)$ tak, že

$$A_R = \{(m_1,n) + (m_2,n) - (m_1+m_2,n);\ m_1, m_2 \in M \text{ a } n \in N\},$$
$$A_S = \{(m \cdot s, n) - (m, s \cdot n);\ m \in M,\ n \in N \text{ a } s \in S\},$$
$$A_T = \{(m,n_1) + (m,n_2) - (m,n_1+n_2);\ m \in M \text{ a } n_1, n_2 \in N\},$$

a položme $A = A_R \cup A_S \cup A_T$.

Ať V označuje podmnožinu U tvořenou všemi hodnotami $i_1a_1 + \cdots + i_ka_k$, kde $i_1, \ldots, i_k$ jsou celá čísla a $a_1, \ldots, a_k$ jsou prvky A. Je-li k rovno nule, tak hodnotou součtu je 0_U. Vidíme, že V je podgrupa $U(+,-,0)$. Přitom pro všechna $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ a $s \in S$ platí

$$(m_1,n) + (m_2,n) \equiv (m_1+m_2,n) \bmod V,$$
$$(m \cdot s, n) \equiv (m, s \cdot n) \bmod V, \text{ a}$$
$$(m, n_1+n_2) \equiv (m,n_1) + (m,n_2) \bmod V.$$

Je zřejmé, že každá podgrupa V grupy U, která by splňovala předcházející tři vztahy, musí obsahovat námi definovanou podgrupu V. Můžeme tedy říci, že V je nejmenší podgrupa U, která je splňuje.

Nyní ověříme, že V je uzavřená i na skalární násobení. K tomu stačí nahlédnout, že pro všechna $a \in A$, $r \in R$ a $t \in T$ je $r \cdot a \in A$ a $a \cdot t \in A$.

Vskutku, $r\cdot((m_1,n)+(m_2,n)-(m_1+m_2,n))=(r\cdot m_1,n)+(r\cdot m_2,n)-(r\cdot m_1+r\cdot m_2,n)\in A_R$, $r\cdot((m\cdot s,n)-(m,s\cdot n))=(r\cdot(m\cdot s),n)-(r\cdot m,s\cdot n)=((r\cdot m)\cdot s,n)-(r\cdot m,s\cdot n)\in A$ a $r\cdot((m,n_1)+(m,n_2)-(m,n_1+n_2))=(r\cdot m,n_1)+(r\cdot m,n_2)-(r\cdot m,n_1+n_2)\in A$. Podobně se ukáže uzavřenost na skalární násobení zprava.

Torzní součin $M\otimes N={}_RM_S\otimes{}_SN_T$ se definuje jako U/V. Protože U i V jsou (R,T)-bimoduly, je $M\otimes N$ také (R,T)-bimodul. Roli okruhu S lze zdůraznit tak, že se místo $M\otimes N$ píše $M\otimes_S N$.

Prvky $M\otimes N$ jsou podle definice tvořeny množinami $(\sum c_{m,n}(m,n))+V$. Pro všechna $c\in\mathbb{Z}$ a $(m,n)\in M\times N$ z definice A_R a A_T plyne $c(m,n)\equiv(c\times m,n)\equiv(m,c\times n)\bmod V$, takže každý prvek $M\otimes N$ lze získat jako (konečný) součet prvků $(m,n)+V$, kde $m\in M$ a $n\in N$. Přitom $(m,n)+V$ se obvykle značí $m\otimes n$.

12.1 Lemma. *Ať $m=\sum_i r_im_i\in M$ a $n=\sum_j n_jt_j\in N$. Pak $m\otimes n=\sum_{i,j}r_i(m_i\otimes n_j)t_j$ a pro každé $s\in S$ platí $ms\otimes n=m\otimes sn$.*

Důkaz. Budeme upravovat modulo V. Z definice A_R a A_T plyne $(\sum r_im_i,\sum n_jt_j)\equiv\sum_i(r_im_i,\sum_j n_jt_j)\equiv\sum_i(\sum_j(r_im_i,n_jt_j))=\sum_{i,j}(r_im_i,n_jt_j)\equiv\sum_{i,j}r_i(m,n_j)t_j$. Druhý vztah lemmatu plyne z definice A_S. □

12.2 Důsledek. *Ať m_i, $i\in I$, a n_j, $j\in J$, jsou po řadě takové prvky M a N, že každé $m\in M$ a každé $n\in N$ lze s použitím vhodných $a_i\in R$ a $b_j\in T$ po řadě vyjádřit jako $\sum a_im_i$ a $\sum n_jb_j$. Potom každý prvek $M\otimes N$ lze vyjádřit ve tvaru $\sum_{i\in I,\ j\in J}r_i(m_i\otimes n_j)t_j$, kde $r_i\in R$ a $t_j\in T$.* □

Jsou-li R a T tělesa, lze za m_i, $i\in I$ a n_j, $j\in J$, zvolit prvky bází. Přirozená otázka je, zda pak i $m_i\otimes n_j$ budou tvořit bázi. Je-li navíc R komutativní a $R=S=T$, tak je odpověď kladná. Přímý formální důkaz tohoto faktu však není příliš příjemný, a proto nejprve vysvětlíme vztah torzních součinů a bilineárních zobrazení, který nám pak dovolí úspornější metodu důkazu.

Ať jsou dány bimoduly ${}_RM_S$, ${}_SN_T$ a ${}_RA_T$. (Zde je A nějaký modul, který nemá vztah k výše uváděným množinám A_R, A_S a A_T.) Zobrazení $\varphi\colon M\times N\to A$ nazveme *bilineární*, jestliže pro všechna $m,m_1,m_2\in M$, $n,n_1,n_2\in N$, $r\in R$, $s\in S$ a $t\in T$ platí:

$$\begin{aligned}\varphi(m_1+m_2,n)&=\varphi(m_1,n)+\varphi(m_2,n),\\ \varphi(m,n_1+n_2)&=\varphi(m,n_1)+\varphi(m,n_2),\\ \varphi(rm,n)&=r\varphi(m,n),\\ \varphi(m,nt)&=\varphi(m,n)t\quad\text{a}\\ \varphi(ms,n)&=\varphi(m,sn).\end{aligned}$$

Množinu všech popsaných bilineárních zobrazení označíme $\mathrm{Bln}(M\times N,A)$, nebo ${}_R\,\mathrm{Bln}_T(M\times N,A)$.

Vraťme se nyní k definici torzního součinu $M\otimes N$. Tento modul byl definován jako faktor U/V, kde $U=\bigoplus U_{m,n}$, přičemž (m,n) probíhá $M\times N$, a V je podmodul tvořený lineárními kombinacemi prvků množin A_R, A_T a A_S. Přitom v ${}_RU_T$ je skalární násobení odvozeno ze vztahu $r(m,n)t=(rm,nt)$. Označme $\pi=\mathrm{nat}_V$ přirozenou projekci $U\to U/V=M\otimes N$. Prvky U obsahují konečné sumy dvojic $(m,n)\in M\times N$, a proto můžeme chápat $M\times N$ jako podmnožinu U, nikoliv však jako podmodul! — sčítání v U je jiné než sčítání v $M\times N$. Zúžení zobrazení $\pi\colon U\to M\otimes N$ na $M\times N\subseteq U$ označíme τ. Všimněte si, že $m\otimes n$ jsme definovali jako $\tau(m,n)$.

12.3 Lemma. *Ať $f\colon M\otimes N\to A$ je homomorfismus (R,T)-bimodulů. Pak $f\tau$ padne do $\mathrm{Bln}(M\times N,A)$.*

Důkaz. Všechny potřebné vztahy plynou z 12.1:

$$\begin{aligned}f\tau(m_1+m_2,n)&=f((m_1+m_2)\otimes n)=f(m_1\otimes n+m_2\otimes n)=\\ &=f(m_1\otimes n)+f(m_2\otimes n)=f\tau(m_1,n)+f\tau(m_2,n),\\ f\tau(m,n_1+n_2)&=f(m\otimes(n_1+n_2))=f(m\otimes n_1+m\otimes n_2)=\\ &=f(m\otimes n_1)+f(m\otimes n_2)=f\tau(m,n_1)+f\tau(m,n_2),\\ f\tau(rm,n)&=f((rm)\otimes n)=f(r(m\otimes n))=rf(m\otimes n)=rf(\tau(m,n)),\\ f\tau(m,nt)&=f(m\otimes(nt))=f((m\otimes n)t)=f(m\otimes n)t=(f\tau(m,n))t\quad\text{a}\\ f\tau(ms,n)&=f(ms\otimes n)=f(m\otimes sn)=f\tau(m,sn).\end{aligned}$$ □

Množina všech homomorfismů bimodulů ${}_RA_T \to {}_RB_T$ se obvykle značívá $\mathrm{Hom}(A,B)$ nebo, úplněji, ${}_R\mathrm{Hom}_T(A,B)$.

12.4 Tvrzení. *Ať jsou dány bimoduly ${}_RM_S$, ${}_SN_T$ a ${}_RA_T$. Ať $\tau\colon M\times N\to M\otimes N$ zobrazuje (m,n) na $m\otimes n$ pro všechna $(m,n)\in M\times N$. Pak zobrazení $f\mapsto f\tau$ je bijekcí* $\mathrm{Hom}(M\otimes N,A)$ a $\mathrm{Bln}(M\times N,A)$.

Důkaz. Protože každý prvek $M\otimes N$ lze vyjádřit jako součet prvků $m\otimes n$, je homomorfismus $f\colon M\otimes N\to A$ plně určen hodnotami $f(m\otimes n)$. Jelikož z $f\tau=g\tau$ plyne $f(m\otimes n)=g(m\otimes n)$ pro všechna $m\otimes n$, $n\in N$, musí být $f=g$. Vidíme, že zobrazení $f\mapsto f\tau$ je injektivní.

Ať nyní je $\varphi\in\mathrm{Bln}(M\times N,A)$. K dokončení důkazu potřebujeme nalézt homomorfismus $f\colon M\otimes N\to A$ takový, že $f\tau=\varphi$. Definujeme nejprve pomocné zobrazení $F\colon U\to A$, a to tak, že $F(\sum\limits_{m,n} c_{m,n}(m,n)) = \sum\limits_{m,n} c_{m,n}\varphi(m,n)$.

Protože je $\varphi(rm,n)=r\varphi(m,n)$ a $\varphi(m,nt)=\varphi(m,n)t$, pro všechna $m\in M$, $n\in N$, $r\in R$ a $t\in T$, vidíme, že F je vskutku homomorfismus. Z dalších vlastností φ vyplývá, že V leží v jádru F. Podle Věty o homomorfismu proto existuje $f\colon M\otimes N\to A$ takové, že $F=f\circ\pi$, kde $\pi=\mathrm{nat}_V$. To ale znamená $f\tau(m,n)=f\pi(m,n)=F(m,n)=\varphi(m,n)$ pro všechna $(m,n)\in M\times N$. □

Lemma 12.1 a Tvrzení 12.4 nám dovolují pracovat s tenzorovými součty bez toho, že bychom se stále vraceli k jejich definici faktorizací U/V.

Z definice $M\otimes_S N$ je však ještě třeba si uvědomit následující fakt: definice prvků $M\otimes_S N$ a definice operace sčítání na $M\otimes_S N$ nijak nesouvisí s tím, že na M je současně zadáno skalární násobení zleva a na N skalární násobení zprava. Jinými slovy, $M\otimes_S N$ lze vybudovat nezávisle na okruzích R a T, a násobení prvky R a T definovat dodatečně na (již definované) Abelově grupě $M\otimes_S N$. Pokud se tedy na M díváme jednou jako (R,S)-bimodul, a jindy jako na (K,S)-bimodul, kde K je nějaký okruh, tak i $M\otimes_S N$ lze současně interpretovat jednak jako R-modul, jednak jako K-modul.

12.5 Tvrzení. *Ať jsou dány bimoduly ${}_RM_S$, ${}_SN_T$ a ${}_TP_K$. Pak existuje právě jeden izomorfismus (R,K)-bimodulů $f\colon (M\otimes_S N)\otimes_T P\to M\otimes_S(N\otimes_T P)$ takový, že $f((m\otimes n)\otimes p)=m\otimes(n\otimes p)$.*

Důkaz. Nejprve pro každé $p\in P$ definujeme $\varphi_p\colon M\times N\to M\otimes(N\otimes P)$ tak, že je $\varphi_p(m,n)=m\otimes(n\otimes p)$. Je snadné ověřit, že φ_p padne do ${}_R\mathrm{Bln}_{\mathbb{Z}}(M\times N, M\otimes(N\otimes P))$ (modul N při definici φ_p chápeme jako $(R,\mathbb{Z})$-bimodul). Proto existuje (jednoznačně určený) homomorfismus $f_p\colon M\otimes N\to M\otimes(N\otimes P)$, který padne do ${}_R\mathrm{Hom}_{\mathbb{Z}}(M\otimes N, M\otimes(N\otimes P))$ a splňuje $f_p(m\otimes n)=m\otimes(n\otimes p)$ pro všechna $m\in M$, $n\in N$.

Ověříme nyní několik vlastností f_p. Přitom budeme porovnávat různá aditivní zobrazení vycházející z $M\otimes N$. Protože každý prvek $M\otimes N$ je součtem konečně mnoha prvků $m\otimes n$, bude pro důkaz shody porovnávaných aditivních zobrazení vždy postačovat jejich shoda na prvcích typu $m\otimes n$.

(i) Pro všechna $p_1,p_2\in P$ je $f_{p_1+p_2}=f_{p_1}+f_{p_2}$. Je totiž $f_{p_1+p_2}(m\otimes n)=m\otimes(n\otimes(p_1+p_2))=$ $=m\otimes((n\otimes p_1)+(n\otimes p_2))=(m\otimes(n\otimes p_1))+(m\otimes(n\otimes p_2))=f_{p_1}(m\otimes n)+f_{p_2}(m\otimes n)$.

(ii) Pro všechna $p\in P$ a $s\in S$ je $f_p(us)=f_{sp}(u)$ pro každé $u\in M\otimes N$. Vskutku, $f_p((m\otimes n)s)=$ $=f_p(m\otimes ns)=m\otimes(ns\otimes p)=m\otimes(n\otimes sp)=f_{sp}(m\otimes n)$.

(iii) Pro všechna $p\in P$ a $k\in K$ je $f_{pk}(u)=f_p(u)\cdot k$ pro každé $u\in M\otimes N$. Je totiž $f_{pk}(m\otimes n)=$ $=m\otimes(n\otimes pk)=m\otimes((n\otimes p)k)=(m\otimes(n\otimes p))k=(f_p(m\otimes n))k$.

Definujme nyní $\varphi\colon(M\otimes N)\times P\to M\otimes(N\otimes P)$ tak, že $\varphi(u,p)=f_p(u)$ pro všechna $u\in M\otimes N$ a $p\in P$. Ať u_1,u_2,u_3 jsou prvky $M\otimes N$, p_1,p_2,p_3 prvky P a ať je $r\in R$, $s\in S$, $k\in K$. Protože f_p jsou homomorfismy levých R-modulů, máme $\varphi(u_1+u_2,p)=\varphi(u_1,p)+\varphi(u_2,p)$ a $\varphi(ru,p)=r\varphi(u,p)$. Z (i) plyne $\varphi(u,p_1+p_2)=\varphi(u,p_1)+\varphi(u,p_2)$, z (ii) dostáváme $\varphi(us,p)=\varphi(u,sp)$ a (iii) dává $\varphi(u,pk)=$ $=\varphi(u,p)\cdot k$. Dokázali jsme, že φ padne do ${}_R\mathrm{Bln}_K((M\otimes N)\times P, M\otimes(N\otimes P))$.

To znamená, že existuje jediný homomorfismus $f\colon(M\otimes N)\otimes P\to M\otimes(N\otimes P)$ takový, že $f(u\otimes p)=$ $=\varphi_p(u)$ pro všechna $u\in M\otimes N$ a $p\in P$, tedy jediný homomorfismus $f\colon(M\otimes N)\otimes P\to M\otimes(N\otimes P)$ takový, že $f((m\otimes n)\otimes p)=m\otimes(n\otimes p)$ pro všechna $m\in M$, $n\in N$ a $p\in P$.

Podobně dokážeme existenci jediného homomorfismu $g\colon M\otimes(N\otimes P)\to(M\otimes N)\otimes P$ takového, že $g(m\otimes(n\otimes p))=(m\otimes n)\otimes p$ pro všechna $m\in M$, $n\in N$ a $p\in P$. Složení obou homomorfismů dá v každém směru identitu, a proto tyto homomorfismy jsou vzájemně inverzní izomorfismy. □

Izomorfismus z tvrzení 12.5 se běžně chápe jako ztotožnění modulů $(M\otimes N)\otimes P$ a $M\otimes(N\otimes P)$. Píšeme pouze $M\otimes N\otimes P$ a pro $m\in M$, $n\in N$, $p\in P$ také jen $m\otimes n\otimes p$. Okamžitě je patrné. že každý prvek $M\otimes N\otimes P$ je roven součtu konečně mnoha prvků $m\otimes n\otimes p$.

Podobně jako jinde, i zde se bez dalších komentářů asociativita používá i pro více činitelů než tři. Je-li M modul nad komutativním R, tak můžeme dokonce vytvářet tenzorové mocniny $M \otimes \ldots \otimes M$. Pokud se M opakuje k-krát, budeme místo $M \otimes \ldots \otimes M$ psát též $\bigotimes^k M$. Ukážeme, jak pro tento speciální, ale důležitý případ se zobecní naše úvahy o bilineárních zobrazeních.

Ať nyní R značí komutativní okruh a ať M a N jsou R-moduly. Zobrazení $\varphi\colon M^k \to N$ se nazývá k-lineární, jestliže

$$\varphi(m_1, \ldots, m_{i-1}, m + m', m_{i+1}, \ldots, m_k) = \varphi(m_1, \ldots, m_{i-1}, m, m_{i+1}, \ldots, m_k) + \varphi(m_1, \ldots, m_{i-1}, m', m_{i+1}, \ldots, m_k)$$

a také

$$\varphi(m_1, \ldots, m_{i-1}, rm, m_{i+1}, \ldots, m_k) = r\varphi(m_1, \ldots, m_{i-1}, m, m_{i+1}, \ldots, m_k)$$

platí pro všechna $m_1, \ldots, m_k \in M$, všechna $m, m' \in M$ a všechna $r \in R$, pro každé i, $1 \leq i \leq k$.

Položme $A = \bigotimes^k M$, $k \geq 1$. Je-li $f\colon A \to N$ homomorfismus R-modulů, tak zobrazení $\varphi\colon M^k \to N$ definované tak, že $\varphi(m_1, \ldots, m_k) = f(m_1 \otimes \cdots \otimes m_k)$, je zjevně k-lineární.

Ať naopak $\varphi\colon M^k \to N$ je nějaké k-lineární zobrazení. Indukcí podle k dokážeme, že φ je možno získat z nějakého $R-$homomorfismu $f\colon \bigotimes^k M \to N$ shora uvedeným způsobem.

Je-li $k = 1$, položme $f = \varphi$. Ať je $k > 1$ a ať $B = \bigotimes^{k-1} M$. Máme $A = B \otimes M$, přičemž pro každé $m \in M$ je $\varphi\colon M^{k-1} \to N$, $\varphi_m(m_1, \ldots, m_{k-1}) = \varphi(m_1, \ldots, m_{k-1}, m)$, nějaké $(k-1)$-lineární zobrazení, které je podle indukčního předpokladu možno získat z nějakého R-homomorfismu $f_m\colon B \to N$.

Definujme $\psi\colon B \times M \to N$ tak, že $\psi(b, m) = f_m(b)$ pro každé $b \in B$ a $m \in M$. Protože rf_m se musí shodovat s f_{rm} (je totiž $rf_m(m_1 \otimes \cdots \otimes m_{k-1}) = r\varphi(m_1, \ldots, m_{k-1}, m) = \varphi(m_1, \ldots, m_{k-1}, rm) = f_{rm}(m_1 \otimes \cdots \otimes m_{k-1})$) pro všechna $r \in R$ a $m \in M$, vidíme, že ψ je bilineární. Podle 12.4 tedy existuje $f\colon B \otimes M \to N$ takové, že $f(b \otimes m) = f_m(b)$ pro všechna $(b, m) \in B \otimes M$, takže vždy platí $f(m_1 \otimes \cdots m_{k-1} \otimes m) = f_m(m_1 \otimes \cdots \otimes m_{k-1}) = \varphi_m(m_1, \ldots, m_{k-1}) = \varphi(m_1, \ldots, m_{k-1}, m)$. Dokázali jsme:

12.6 Tvrzení. *Ať jsou M a N moduly nad komutativním okruhem R a ať je $k \geq 1$. Položme $A = \bigotimes^k M$ a definujme $\tau\colon M \times \cdots \times M \to A$ tak, že $\tau(m_1, \ldots, m_k) = m_1 \otimes \cdots \otimes m_k$. Potom zobrazení $f \mapsto f\tau$ je bijekce množiny $\mathrm{Hom}_R(A, N)$ a množiny všech k-lineárních zobrazení $M^k \to N$.* □

Nyní se budeme zabývat opět obecnými okruhy, bez předpokladu jejich komutativity.

12.7 Tvrzení. *Ať $M = \bigoplus M_i$, $i \in I$, je direktní suma (R, S)-bimodulů, a $N = \bigoplus N_j$, $j \in J$, je direktní suma (S, T)-bimodulů. Pak existuje jednoznačně určený izomorfismus $f\colon M \otimes N \to \bigoplus_{i,j}(M_i \otimes N_j)$ takový, že $f((\sum_i m_i) \otimes (\sum_j n_j)) = \sum_{i,j}(m_i \otimes n_j)$.*

Důkaz. Definujme $\varphi\colon M \times N \to \bigoplus_{i,j}(M_i \otimes N_j)$ tak, že $\varphi(\sum_i m_i, \sum_j n_j) = \sum_{i,j}(m_i \otimes n_j)$. Bezprostřední ověření bilinearity φ nečiní potíže, takže je $\varphi \in {}_R\mathrm{Bln}_T(M \times N, \bigoplus(M_i \otimes N_j))$, a existuje jediný homomorfismus f, který splňuje

$$f((\sum_i m_i) \otimes (\sum_j n_j)) = \sum_{i,j}(m_i \otimes n_j).$$

Pro pevné $i \in I$ a $j \in J$ definujme $\psi_{i,j}\colon M_i \times N_j \to M \otimes N$ tak, že $\psi_{i,j}(m, n) = m \otimes n$ pro všechna $m \in M_i$ a $n \in N_j$ (přitom M_i chápeme jako podmodul M a N_j jako podmodul N — viz definici direktní sumy modulů v kapitole 6). Protože $\psi_{i,j}$ jsou bilineární, odpovídá každému z nich (R, T)-homomorfismus $g_{i,j}\colon M_i \otimes N_j \to M \otimes N$. Položme $g = \sum_{i,j} g_{i,j}$. Pak g je homomorfismus $\bigoplus_{i,j}(M_i \otimes N_j) \to M \otimes N$, který zobrazuje $\sum_{i,j}(m_i \otimes n_j)$ na součet všech hodnot $m_i \otimes n_j$ chápaných jako prvky $M \otimes N$. Pokud v tomto součtu nejprve fixujeme n_j, vidíme, že je roven $\sum_j((\sum_i m_i) \otimes n_j)$, což je však rovno $(\sum m_i) \otimes (\sum n_j) \in M \otimes N$. Nyní je již zřejmé, že homomorfismy f a g jsou vzájemně inverzní izomorfismy. □

Okruh S lze samozřejmě chápat jako ${}_SS_S$-bimodul. Budeme zkoumat tenzorový součin bimodulů ${}_RM_S$ a ${}_SS_S$. Zobrazení $(m, s) \mapsto ms$ jistě padne do ${}_R\mathrm{Bln}_S(M \times S, M)$, a proto existuje podle 12.4 takový homomorfismus $f\colon M \otimes S \to M$, že je $f(m \otimes s) = ms$ pro všechna $m \in M$ a $s \in S$. Z toho, že pro všechna $m \in M$ a $s \in S$ je $m \otimes s = ms \otimes 1$, vyplývá, že $M \otimes S = \{m \otimes 1;\ m \in M\}$ a že $f\colon M \otimes S \to M$ je izomorfismus. Speciálně je $s_1 \otimes s_2 \mapsto s_1 s_2$ izomorfismus $S \otimes S \simeq S$.

Proto z 12.7 dostáváme následující důsledek (viz též 12.1):

12.8 Důsledek. *Ať T je komutativní těleso a ať V a W jsou vektorové prostory nad T s bázemi $v_1, \ldots, v_r$ a $w_1, \ldots, w_s$. Pak $V \otimes W$ je vektorový prostor dimenze rs s bází $\{v_i \otimes w_j;\ 1 \leq i \leq r \text{ a } 1 \leq j \leq s\}$.* □

Poznamenejme, že zápis $m \otimes n$ je jednoznačný teprve tehdy, když je uvedeno, do kterého modulu prvky m a n patří. Smyslem tvrzení 12.7 bylo ukázat, že tato nejednoznačnost není na závadu u direktních sum — tedy, že $m_i \otimes n_j$ v $M_i \otimes N_j$ lze ztotožnit s $m_i \otimes n_j \in (\bigoplus M_i) \otimes (\bigoplus N_j)$. Důsledku 12.8 je třeba rozumět právě ve smyslu tohoto ztotožnění. Přitom je zřejmé, že vzhledem k asociativitě je možné přejít i na více činitelů — jsou-li $V_1, \dots, V_k$ vektorové prostory s bázemi $\{v_1^{(1)}, \dots, v_{r_1}^{(1)}\}, \dots, \{v_1^{(k)}, \dots, v_{r_k}^{(k)}\}$, bude $V_1 \otimes \cdots \otimes V_k$ vektorový prostor dimenze $\prod r_i$, $1 \le i \le k$, který bude mít bázi tvořenou prvky $v_{a_1}^{(1)} \otimes \cdots \otimes v_{a_k}^{(k)}$, kde je $1 \le a_i \le r_i$ pro každé i, $1 \le i \le k$.

Při výpočtech ve vektorových prostorech jsou vždy důležitá zobrazení související se změnou báze. Obecněji jde vlastně o to, jak se homomorfismy modulů dají sloučit s tenzorovými součiny.

Uvažme homomorfismy bimodulů $f\colon {}_RM_S \to {}_RA_S$ a $g\colon {}_SN_T \to {}_SB_T$. Definujme zobrazení $\varphi\colon M \times N \to A \otimes B$ tak, že $\varphi(m,n) = f(m) \otimes g(n)$. Pro $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $r \in R$, $s \in S$ a $t \in T$ jistě platí $\varphi(m_1 + m_2, n) = f(m_1 + m_2) \otimes g(n) = (f(m_1) + f(m_2)) \otimes g(n) = (f(m_1) \otimes g(n)) + (f(m_2) \otimes g(n)) = \varphi(m_1, n) + \varphi(m_2, n)$, podobně $\varphi(m, n_1 + n_2) = \varphi(m, n_1) + \varphi(m, n_2)$, dále $\varphi(rm, n) = f(rm) \otimes g(n) = (r(f(m)) \otimes g(n) = r(f(m) \otimes g(n)) = r\varphi(m,n)$, podobně $\varphi(m, nt) = \varphi(m,n)t$, a konečně $\varphi(ms, n) = f(ms) \otimes g(n) = (f(m)s) \otimes g(n) = f(m) \otimes (sg(n)) = f(m) \otimes g(sn) = \varphi(m, sn)$. Ověřili jsme, že φ je bilineární, a proto můžeme podle 12.4 vyslovit:

12.9 Tvrzení. *Ať $f\colon {}_RM_S \to {}_RA_S$ a $g\colon {}_SN_T \to {}_SB_T$ jsou homomorfismy bimodulů. Pak existuje jediný homomorfismus $M \otimes N \to A \otimes B$ takový, že $m \otimes n$ se zobrazí na $f(m) \otimes g(n)$ pro všechna $(m,n) \in M \times N$.* □

Zobrazení z předchozího tvrzení se značí $f \otimes g$. Je zřejmé, že $\mathrm{id}_M \otimes \mathrm{id}_N$ se rovná $\mathrm{id}_{M \otimes N}$.

12.10 Tvrzení. *Ať $f\colon M \to A$ a $u\colon A \to U$ jsou (R,S)-homomorfismy a $g\colon N \to B$ spolu s $v\colon B \to V$ jsou (S,T)-homomorfismy. Pak $(u \circ f) \otimes (v \circ g)$ se rovná $(u \otimes v) \circ (f \otimes g)$.*

Důkaz. Stačí ověřit, že $(u \circ f) \otimes (v \circ g)(m \otimes n) = u(f(m)) \otimes v(g(n))$ se shoduje s $(u \otimes v) \circ (f \otimes g)(m \otimes n) = (u \otimes v)(f(m) \otimes g(n)) = u(f(m)) \otimes v(g(n))$ pro všechna $m \in M$ a $n \in N$. □

Jsou-li $f\colon M \to A$ a $g\colon N \to B$ izomorfismy, tak z 12.10 plyne, že inverzním homomorfismem k $f \otimes g$ je $(f^{-1}) \otimes (g^{-1})$, takže $f \otimes g$ je opět izomorfismus.

Jsou-li $f\colon A \to B$ a $g\colon U \to V$ lineární zobrazení, kde A, B, U a V jsou vektorové prostory nad komutativním tělesem T, které mají báze $\{a_1, \dots, a_m\}$, $\{b_1, \dots, b_m\}$, $\{u_1, \dots, u_n\}$ a $\{v_1, \dots, v_n\}$, bude $f \otimes g$ zobrazovat $a_j \otimes u_s$ na $f(a_j) \otimes f(u_s)$. Je-li M matice f a N matice g (tedy $f(a_j) = \sum_i m_{ij} b_j$ a $g(u_s) = \sum_r n_{rs} v_s$), bude $(f \otimes g)(a_j \otimes u_s)$ rovno $\sum_{i,r} m_{ij} n_{rs} (b_j \otimes v_r)$. Jestliže v matici odpovídající $f \otimes g$ budeme sloupce indexovat dvojicí (j,s) a řádky dvojicí (i,r), tak v buňce odpovídající průsečíku takového řádku a sloupce bude hodnota $m_{ij} n_{rs}$. Taková matice se značí obvykle též $M \otimes N$. Chceme-li ji umístit do roviny, můžeme si například představit, že každý prvek m_{ij} nahradíme blokem, který odpovídá matici $m_{ij}N$. Takto získané matice se také někdy říká *Kroneckerův součin matic* M a N.

13. Uzavěrové systémy, svazy a algebry

Ať $\mathcal{C}$ je systém podmnožin množiny A, který splňuje
(i) $A \in \mathcal{C}$,
(ii) jsou-li $B_i \in \mathcal{C}$, $i \in I \neq \emptyset$, je $\bigcap_{i\in I} B_i \in \mathcal{C}$.

Potom $\mathcal{C}$ nazýváme *uzávěrový systém nad* A.

Jinak řečeno, systém podmnožin $\mathcal{C}$ množiny A se nazývá uzávěrový systém nad A, jestliže je uzavřený na průniky a A je jednou z množin tohoto systému.

Je-li $\mathcal{C}$ uzávěrový systém nad A a B je nějaká podmnožina A, tak je množina $\mathcal{B} = \{C \in \mathcal{C};\ C \supseteq B\}$ jistě neprázdná, neboť je $A \in \mathcal{B}$. Položme $\overline{B} = \bigcap_{C\in\mathcal{B}} C$. Podle (ii) platí $\overline{B} \in \mathcal{C}$. Současně je $\overline{B} \supseteq B$ a $\overline{B} \subseteq C$ pro všechna $C \in \mathcal{B}$. Vidíme, že $\overline{B}$ je nejmenší množina ze systému $\mathcal{C}$, která obsahuje B.

Množině $\overline{B}$ se říká *uzávěr* B v $\mathcal{C}$ nebo též množina *generovaná* množinou B v $\mathcal{C}$. (Podle povahy uzávěrového systému se zpravidla používá jen jedno z možných vyjádření).

Matematické objekty poskytují množství přirozeně se vyskytujících uzávěrových systémů. Každá topologie například poskytuje uzávěrový systém všech svých uzavřených množin. Jiným přirozeným příkladem je množina všech ekvivalencí nějaké množiny, řekněme opět A. Snadno nahlédneme, že všechny ekvivalence na A (což jsou podmnožiny $A \times A$) tvoří uzávěrový systém nad $A \times A$ (uzávěr je pak nejmenší ekvivalence obsahující danou relaci).

Nás zde však budou zajímat uzávěrové systémy, které jsou spjaty s algebraickými strukturami. Ať A je nějaká algebra signatury $\sigma\colon \Sigma \to \mathbb{N}_0$. Je snadné ověřit, že všechny její podalgebry tvoří uzávěrový systém nad A. Podobně je snadné ověřit, že všechny kongruence tvoří uzávěrový systém nad $A \times A$.

Je-li T těleso, tak také všechna jeho podtělesa tvoří uzávěrový systém nad T.

Na každém uzávěrovém systému, jak za okamžik uvidíme, lze přirozeným způsobem definovat svaz. V tomto smyslu se pak mluví o *svazu podalgeber*, *svazu kongruencí* nebo *svazu podtěles*.

Pokud jsou kongruence jednoznačně určeny nějakými svými vybranými bloky (například u grup jsou kongruence určeny normálními podgrupami a u okruhů ideály), tvoří tyto bloky také uzávěrový systém. Obecně vztah kongruencí a jejich bloků zde formulovat nebudeme — ověřit, že všechny normální podgrupy dané grupy tvoří uzávěrový systém nebo že všechny ideály okruhu tvoří uzávěrový systém, je totiž velmi snadné přímo. Následně budeme proto moci hovořit o *svazu normálních podgrup* a *svazu ideálů*.

13.1 Tvrzení. *Ať $\mathcal{C}$ je uzávěrový systém nad množinou A. Potom $(\mathcal{C}, \subseteq)$ je úplný svaz, ve kterém pro $\mathcal{B} \subseteq \mathcal{C}$ platí $\inf \mathcal{B} = \bigcap_{C\in\mathcal{B}} C$ a $\sup \mathcal{B}$ je rovno nejmenší množině $\overline{B} \in \mathcal{C}$, která obsahuje $B = \bigcup_{C\in\mathcal{B}} C$.*

Důkaz. Každý prvek $E \in \mathcal{C}$, jenž je obsažen ve všech $C \in \mathcal{B}$, musí být obsažen i v $\bigcap_{C\in\mathcal{B}} C$. Proto je $\inf \mathcal{B}$ definováno správně. Prvek $F \in \mathcal{C}$ je horní závorou $\mathcal{B}$ právě když platí $F \supseteq B = \bigcup_{C\in\mathcal{B}} C$. Z $F \supseteq B$ ovšem plyne $F \supseteq \overline{B}$, takže i $\sup \mathcal{B}$ je správně definováno. □

Zde je na místě upozornit na určitou podvojnost v používání slov minimální a maximální. Je-li $(X, \leq)$ nějaká uspořádaná množina, je možno používat slovo minimální pro označení takového prvku $x \in X$, že pro žádné $y \in X$, $y \neq x$, neplatí $y \leq x$. V algebře se však většinou pracuje s uspořádáními, která mají nejmenší (a často i největší) prvek. V takových systémech je slovo minimální použité ve výše uvedeném smyslu pouze synonymem slova nejmenší.

Většinou se však slov minimální a maximální používá jinak — a to s ohledem na nějaký uzávěrový systém $\mathcal{C}$ (který bývá patrný z kontextu). *Minimální* je ten prvek $C \in \mathcal{C}$, který je atomem ve svazu $(\mathcal{C}, \subseteq)$ a *maximální* je ten prvek $C \in \mathcal{C}$, který je koatomem v tomto svazu. V uvedeném smyslu jsme již dříve definovali maximální ideál ve vztahu k uzávěrovému systému všech ideálů nějakého okruhu R.

Nyní se budeme zabývat kongruencemi kvocientních algeber a vztahem uzávěrových systémů daných kvocientní algebrou k uzávěrovým systémům určeným původní algebrou.

Jsou-li σ a ρ ekvivalence na množině A, přičemž σ obsahuje ρ (vztah $\sigma \supseteq \rho$ vlastně znamená, že každý blok σ lze vyjádřit jako sjednocení bloků ρ), tak definujeme relaci σ/ρ na A/ρ tak, že pro bloky B, C ekvivalence ρ, je

$$(B, C) \in \sigma/\rho \iff (b, c) \in \sigma \quad \text{platí pro všechna } b \in B \text{ a } c \in C.$$

13.2 Lemma.
(i) Pro $b, c \in A$ platí $([b]_\rho, [c]_\rho) \in \sigma/\rho$ právě když je $(b, c) \in \sigma$.
(ii) Relace σ/ρ je ekvivalence na A/ρ.

Důkaz.

(i) Ať je $(b,c) \in \sigma$ a ať $b' \in A$ patří do $[b]_\rho$ a $c' \in A$ do $[c]_\rho$. Je třeba dokázat $(b',c') \in \sigma$. Ovšem $(b',b) \in \rho$ a $(c',c) \in \rho$ implikují $(b',b) \in \sigma$ a $(c',c) \in \sigma$, neboť platí $\rho \subseteq \sigma$. Stačí tedy použít tranzitivitu ekvivalence σ.

(ii) Ať $B, C, D \in A/\rho$ jsou rozkladové třídy ekvivalence ρ. Vyberme prvky $b \in B$, $c \in C$ a $d \in D$. Je tedy $B = [b]_\rho$, $C = [c]_\rho$ a $D = [d]_\rho$. Předpokládejme, že platí $(B,C) \in \sigma/\rho$ a $(C,D) \in \sigma/\rho$. Podle definice musí být $(b,c) \in \sigma$ a $(c,d) \in \sigma$, takže je rovněž $(b,d) \in \sigma$. Ovšem to podle (i) implikuje $(B,D) \in \sigma/\rho$. Relace σ/ρ je tedy tranzitivní. Symetrie a reflexivita se dokáží podobně. □

13.3 Lemma. *Ať ρ je ekvivalence na množině A a ať η je ekvivalence na A/ρ. Pak existuje právě jedna ekvivalence $\sigma \supseteq \rho$ na A, pro kterou platí $\eta = \sigma/\rho$.*

Důkaz. Má-li být $\eta = \sigma/\rho$, tak podle 13.2 (ii) musí být $(b,c) \in \sigma$ právě když je $([b]_\rho, [c]_\rho) \in \eta$. Tento vztah σ jednoznačně určuje, takže ho lze použít jako definici. Je třeba ukázat, že takto definovaná relace σ je ekvivalence, obsahuje ρ a splňuje $\eta = \sigma/\rho$.

To, že σ je ekvivalence se odvodí přímo z faktu, že η je ekvivalence. Zbývá dokázat rovnost η a σ/ρ. Uvažme prvky b a c množiny A. Je-li $(b,c) \in \rho$, je $[b]_\rho$ rovno $[c]_\rho$, takže jistě platí $([b]_\rho, [c]_\rho) \in \eta$, a tedy i $(b,c) \in \sigma$.

Vztah $([b]_\rho, [c]_\rho) \in \eta$ podle definice σ znamená $(b,c) \in \sigma/\rho$. Tím je dokázáno, že ekvivalence η a σ/ρ se shodují. □

13.4 Lemma. *Ať ρ je ekvivalence na A, $f\colon A \to B$ zobrazení, které splňuje* $\ker f \supseteq \rho$ *a $g\colon A/\rho \to B$ zobrazení, které splňuje $g \circ \mathrm{nat}_\rho = f$. Potom* $\ker g = (\ker f)/\rho$.

Důkaz. Pro $a, b \in A$ platí $g([a]_\rho) = g([b]_\rho)$, tedy $([a]_\rho, [b]_\rho) \in \ker g$, právě když $f(a) = f(b)$, tedy $(a,b) \in \ker f$. □

Připomeňme, že každá n-ární operace α na A, která je slučitelná s ekvivalencí ρ na A, indukuje n-ární operaci α na A/ρ tak, že $\alpha([a_1]_\rho, \ldots, [a_n]_\rho) = [\alpha(a_1, \ldots, a_n)]_\rho$ — viz lemma 4.1.

13.5 Lemma. *Buď ρ ekvivalence na množině A, jež je slučitelná s operací $\alpha = \alpha_A$ na A. Buď $\sigma \supseteq \rho$ další ekvivalence na A. Pak σ je slučitelná s α_A právě když σ/ρ je slučitelná s $\alpha_{A/\rho}$.*

Důkaz. Označme n četnost operace α a ať $a_1, \ldots, a_n$ a $b_1, \ldots, b_n$ jsou prvky A. Podle 13.2 je $(a_i, b_i) \in \sigma$ právě když $([a_i]_\rho, [b_i]_\rho) \in \sigma/\rho$. Ať $(a_i, b_i) \in \sigma$ platí pro všechna i, $1 \leq i \leq n$. Pak ekvivalence σ je slučitelná s α_A právě když pro libovolnou takovou volbu prvků a_i a b_i platí $(\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \sigma$, zatímco ekvivalence σ/ρ je slučitelná s $\alpha_{A/\rho}$ právě když pro libovolné takové a_i a b_i platí $([\alpha(a_1, \ldots, a_n)]_\rho, [\alpha(b_1, \ldots, b_n)]_\rho) \in \sigma/\rho$. Poslední podmínka je ovšem, opět podle 4.1, shodná s podmínkou $(\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \sigma$. □

Z 13.5 nyní okamžitě plyne:

13.6 Tvrzení. *Buď ρ kongruence algebry A signatury $\tau\colon \Sigma \to \mathbb{N}_0$ a ať $\sigma \supseteq \rho$ je ekvivalence na A. Potom σ/ρ je kongruence algebry A/ρ právě když σ je kongruence algebry A.* □

13.7 Druhá věta o izomorfismu. *Ať A je algebra signatury $\tau\colon \Sigma \to \mathbb{N}_0$ a ať $\rho \subseteq \sigma$ jsou její kongruence. Pak $\big[[a]_\rho\big]_{\sigma/\rho} \mapsto [a]_\sigma$ je izomorfismus $A/\rho\big/\sigma/\rho \simeq A/\sigma$.*

Důkaz. Podle Věty o homomorfismu 6.4 lze $\mathrm{nat}_\sigma\colon a \mapsto [a]_\sigma$ faktorizovat přes ρ, přičemž věta říká, že $[a]_\rho \mapsto [a]_\sigma$ je homomorfismus $A/\rho \to A/\sigma$. Jádrem tohoto homomorfismu je podle 13.4 kongruence σ/ρ. Zbytek plyne použitím První věty o izomorfismu 6.5 na homomorfismus $[a]_\rho \mapsto [a]_\sigma$. □

Kongruence grup odpovídají normálním podgrupám. Jestliže $\sigma \supseteq \rho$ je kongruence grupy G, tak $\sigma = \mathrm{mod}\, M$ a $\rho = \mathrm{mod}\, N$ pro nějaké normální podgrupy N, M grupy G, přičemž $M = [1_G]_\sigma$ obsahuje $N = [1_G]_\rho$. Kongruence σ/ρ je pak rovna $\mathrm{mod} M/N$. Tvrzení 13.6 pro grupy říká, že všechny normální podgrupy G/N mají tvar M/N, kde M je normální podgrupa G, která obsahuje N. Přitom M je určené jednoznačně.

Podobně se ověří, že ideály okruhu R/I, kde I je ideál okruhu R, mají tvar J/I. přičemž $J \supseteq I$ je jednoznačně určený ideál R.

Konečně všechny moduly modulu K/N, kde N je podmodul modulu K, mají tvar M/N, přičemž $M \supseteq N$ je jednoznačně určený podmodul M.

Při použití stejného označení jako v předchozích třech odstavcích pak Druhá věta o izomorfismu poskytuje izomorfismy

$$\begin{aligned} G/N\Big/M/N &\to G/M, \qquad (aN)(M/N) \mapsto aM; \\ R/I\Big/J/I &\to R/J, \qquad (a+I)+(J/I) \mapsto a+J; \text{ a} \\ K/N\Big/M/N &\to K/M, \quad (a+N)+(M/N) \mapsto a+M. \end{aligned}$$

Svaz všech podalgeber algebry A se často značí $\mathrm{Sub}(A)$ a svaz všech jejich kongruencí se značí $\mathrm{Con}(A)$.

Je-li $L = L(\wedge, \vee)$ nějaký svaz, přičemž pro jeho prvky $a, b \in L$ platí $a \leq b$, tak se množina $[a, b] = \{c \in L;\ a \leq c \leq b\}$ nazývá jeho *interval*. Je zřejmé, že každý interval svazu L je jeho podsvaz.

Největší kongruencí algebry A (a tedy největším prvkem svazu $\mathrm{Con}(A)$) je *univerzální kongruence* $A^2 = A \times A$. Ať ρ je nějaká kongruence A. Budeme uvažovat interval $[\rho, A^2]$ ve svazu $\mathrm{Con}(A)$. Zobrazení $\sigma \mapsto \sigma/\rho$ je podle 13.3 a 13.6 bijekcí $[\rho, A^2]$ a $\mathrm{Con}(A/\rho)$. Protože pro $\sigma_1, \sigma_2 \in [\rho, A^2]$ je jistě $\sigma_1 \supseteq \sigma_2$ právě když je $\sigma_1/\rho \supseteq \sigma_2/\rho$, můžeme podle 7.3 vyslovit následující tvrzení.

13.8 Tvrzení. *Ať ρ je kongruence algebry A. Potom zobrazení $\sigma \mapsto \sigma/\rho$ je izomorfismem intervalu $[\rho, A^2]$ svazu $\mathrm{Con}(A)$ a svazu $\mathrm{Con}(A/\rho)$.* □

Tvrzení 13.8 lze vyslovit samozřejmě také ve formě, která vede na izomorfismus svazu normálních podgrup grupy G/N a intervalu normálních podgrup $[N, G]$ (resp. svazu ideálů v R/I a intervalu $[I, R]$, resp. svazu podmodulů K/N a intervalu $[N, K]$).

Je-li $\pi = \mathrm{nat}_\rho$ přirozená projekce $A \to A/\rho$ a B je podalgebra A/ρ, je $C = \pi^{-1}(B)$ podle 6.3 podalgebra A. Protože π je surjektivní, je B obrazem $\pi(C)$. Každá podalgebra B algebry A/ρ je tedy obrazem nějaké podalgebry C algebry A, která má tu vlastnost, že pro každé $c \in C$ platí $[c]_\rho \subseteq C$.

Speciálně tedy každá podgrupa G/N má tvar H/N, kde $H \supseteq N$ je podgrupa G, a každý podokruh R/I má tvar S/I, kde $S \supseteq I$ je podokruh R. Protože $H_1/N \supseteq H_2/N$ právě když $H_1 \supseteq H_2$, a $S_1/I \supseteq S_2/I$ právě když $S_1 \supseteq S_2$, můžeme podle 7.3 uvést:

13.9 Tvrzení.
(i) Ať N je normální podgrupa grupy G. Pak $H \mapsto H/N$ je izomorfismus intervalu $[N, G]$ svazu $\mathrm{Sub}(G)$ a svazu $\mathrm{Sub}(G/N)$.
(ii) Ať I je ideál okruhu R. Pak $S \mapsto S/I$ je izomorfismus intervalu $[P, R]$ svazu $\mathrm{Sub}(R)$ a svazu $\mathrm{Sub}(R/I)$, kde $P = \{n \cdot 1_R + c;\ n \in \mathbb{Z} \text{ a } c \in I\}$.

Důkaz. Zbývá ověřit, že P je nejmenší podokruh, který obsahuje I. V každém podokruhu, který obsahuje I, musí ležet 1_R, a tedy v něm musí ležet všechny prvky P. Naopak, pro $n, m \in \mathbb{Z}$ a $c, d \in I$ je $(n \cdot 1_R + c) + (m \cdot 1_R + d) = (n+m) \cdot 1_R + (c+d)$ a $(n \cdot 1_R + c) \cdot (m \cdot 1_R + d) = (nm) \cdot 1_R + f$, kde $f = n \cdot d + m \cdot d + c \cdot d \in I$. □

Závěrem této kapitoly budeme ještě věnovat pozornost otázce generování podalgeber. Ať A je opět algebra signatury $\tau\colon \Sigma \to \mathbb{N}_0$. Je-li $X \subseteq A$ nějaká množina, tak nejmenší podalgebře B, která obsahuje X, se říká podalgebra *generovaná* X. Je-li $B = A$, mluví se o X jako o *množině generátorů* A.

Je-li na A a G dána operace α a zobrazení $f\colon A \to G$ a $g\colon A \to C$ jsou slučitelná s α, tak množina $\{a \in A;\ f(a) = g(a)\}$ je zjevně uzavřená na α. Proto platí:

13.10 Tvrzení. *Ať A a C jsou algebry signatury $\tau\colon \Sigma \to \mathbb{N}_0$ a ať $f\colon A \to C$ a $g : A \to C$ jsou homomorfismy těchto algeber. Potom $\{a \in A;\ f(a) = g(a)\}$ je podalgebra A.* □

13.11 Důsledek. *Ať f je endomorfismus algebry A. Pak $\{a \in A;\ f(a) = a\}$ je podalgebra A.* □

13.12 Důsledek. *Ať $f\colon A \to C$ a $g\colon A \to C$ jsou homomorfismy algeber a ať X je množina generátorů A. Jestliže pro všechna $x \in X$ platí $f(x) = g(x)$, tak je $f = g$.* □

Z 13.12 tedy plyne, že homomorfismus $f\colon A \to C$ je plně určen svými hodnotami na nějakých generátorech A. Připomeňme si některé množiny generátorů, které se pro ověřování jednoznačnosti zadaných homomorfismů často používají (v některých případech jsme tak ostatně již učinili).

Monoidový okruh RM je generován množinou $R \cup M = \{r \cdot 1_R;\ r \in R\} \cup \{1_R \cdot m;\ m \in M\}$. Přitom místo R nebo M lze také uvažovat nějaké množiny jejich generátorů.

Grupa je cyklická, má-li jednobodovou množinu generátorů. Homomorfismy jsou určeny obrazem takového generátoru (to jsme použili v 10.1).

Tenzorový součin $M \otimes N$ je (jako Abelova grupa i jako modul) generován všemi prvky $m \otimes n$, kde $m \in M$ a $n \in N$.

Často bývá výhodné umět nějak popsat pomocí operací podalgebru B algebry A generovanou množinou $Y \subseteq A$.

Je-li A Abelova grupa, jsou to všechny sumy $\sum_i n_y y$, kde je $y \in Y$ a $n_y \in \mathbb{Z}$. Je-li A modul, jsou to — podobně — všechny lineární kombinace nad Y.

Je-li A obecná (multiplikativní) grupa, je B tvořena všemi hodnotami, které je možno vyjádřit jako posloupnost $y_1^{\epsilon_1} \cdots y_k^{\epsilon_k}$, kde $\epsilon_i \in \{-1, 1\}$ a $y_i \in Y$, $1 \leq i \leq k$.

Je-li R okruh, tak nejprve definujeme Z jako množinu všech součinů $y_1 \cdots y_k$, kde $y_i \in Y$, $1 \leq i \leq k$, a pak B je rovno množině všech součtů $z_1 + \cdots + z_r$, kde $z_j \in Z$, $1 \leq j \leq r$.

Obecně pak u algebry signatury $\tau\colon \Sigma \to \mathbb{N}_0$ lze postupovat tak, že nejprve položíme $M_0 = Y \cup \{\tau^{-1}(0)\}$ (tedy k množině Y přidáme všechny konstanty), a pro každé $i \geq 0$ definujeme M_{i+1} vztahem $M_{i+1} = M_i \cup \{\alpha(a_1, \ldots, a_k);\ a_j \in M_i$; pro každé j, $1 \leq j \leq k$, $\alpha \in \Sigma$ a $k = \tau(\alpha) \geq 1\}$. Pak $B = \bigcup_{i \leq 0} M_i$. (Jsou-li totiž $a_1, \ldots, a_k \in B$ a $\alpha \in \Sigma$, $\tau(\alpha) = k$, tak existuje takové $i \in \mathbb{N}$, že všechna $a_1, \ldots, a_k$ jsou obsažena v M_i. Podle definice M_{i+1} je pak $\alpha(a_1, \ldots, a_k) \in M_{i+1} \subseteq B$.)

Tím jsme dostali schéma, jak pomocí operací Σ popsat uzávěr množiny v uzavěrovém systému podalgeber dané algebry. Toto schéma lze aplikovat na výše uvedené případy grup, monoidů a okruhů — u nich však vztahy, které operace splňují, dovolují generovanou množinu popsat v zjednodušeném tvaru.

14. Modulární, distributivní a komplementární svazy

14.1 Lemma. *Buď $L = L(\wedge, \vee)$ svaz a ať jsou $a, b, c \in L$. Je-li $a \leq c$, je $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.*

Důkaz. $a \leq a \vee b$ a $a \leq c$, proto $a \leq (a \vee b) \wedge c$. Současně $b \wedge c \leq a \vee b$, $b \wedge c \leq c$, takže $b \wedge c \leq (a \vee b) \wedge c$. □

Poznámka. Zkusme získat duální nerovnost k nerovnosti $a \vee (b \wedge c) \leq (a \vee b) \wedge c$ ($\vee$ a $\wedge$ prohodíme a $\leq$ zaměníme za $\geq$). Ta bude znít, že z $a \geq c$ plyne $a \wedge (b \vee c) \geq (a \wedge b) \vee c$. Vyměníme-li a a c, dostaneme, že z $a \leq c$ plyne $c \wedge (b \vee a) \geq (c \wedge b) \vee a$. To ovšem je naše původní nerovnost, čili jsme neobdrželi žádný nový vztah. Uvedená nerovnost je samoduální.

14.2 Tvrzení. *Bud $L = L(\wedge, \vee)$ svaz. Potom jsou následující podmínky ekvivalentní.*
(i) $a \vee (b \wedge c) = (a \vee b) \wedge c$, *kdykoliv* $a, b, c \in L$ *a* $a \leq c$.
(ii) $(a \wedge c) \vee (b \wedge c) = ((a \wedge c) \vee b) \wedge c$ *pro všechna* $a, b, c \in L$.
(iii) $(a \vee c) \wedge (b \vee c) = ((a \vee c) \wedge b) \vee c$ *pro všechna* $a, b, c \in L$.

Důkaz. (i) $\iff$ (ii) : Položíme-li $a' = a \wedge c \leq c$, bude mít identita (ii) tvar $a' \vee (b \wedge c) = (a' \vee b) \wedge c$.
(i) $\iff$ (iii) : Položíme-li $c' = a \vee c \geq c = a'$, získá identita (iii) tvar $c' \wedge (b \vee a') = (c' \wedge b) \vee a'$. □

Svaz, který vyhovuje ekvivalentním podmínkám tvrzení 14.2, se nazývá *modulární*.

14.3 Lemma. *Buď a, b, c prvky svazu L, $a \leq c$. Je-li $a \leq b$ nebo $b \leq c$, platí $a \vee (b \wedge c) = (a \vee b) \wedge c$.*

Důkaz. Stačí ukázat $a \vee (b \wedge c) \geq (a \vee b) \wedge c$. Ať nejprve $b \geq a$. Pak $a \vee (b \wedge c) \geq b \wedge c = (a \vee b) \wedge c$. Pokud $b \leq c$, tak dostáváme $a \vee (b \wedge c) = a \vee b \geq (a \vee b) \wedge c$. □

Na množině $\{0, 1, u, v, w\}$ definujeme uspořádání tak, že u a v pokrývají 0, w pokrývá v a 1 pokrývá w a u. Takto definované uspořádání dává svaz, a ten se obvykle značí N_5. (Nakreslete si Hasseův diagram!).

14.4 Tvrzení. *Svaz L je modulární právě když neobsahuje podsvaz izomorfní svazu N_5.*

Důkaz. Svaz N_5 modulární není, neboť $v \vee (u \wedge w) = v$, zatímco $(v \vee u) \wedge w = w$. Proto L, je-li modulární, nemůže obsahovat podsvaz izomorfní s N_5.

Není-li L modulární, lze najít $a, b, c \in L$, že $a \leq c$ a $a \vee (b \wedge c) < (a \vee b) \wedge c$. Ukážeme, že $\{b \wedge c, a \vee (b \wedge c), (a \vee b) \wedge c, a \vee b, b\}$ tvoří podsvaz izomorfní s N_5. Z $b \wedge c = a \vee (b \wedge c)$ plyne $a \leq b \wedge c$, odkud $a \leq b$. Z $a \vee b = (a \vee b) \wedge c$ dostáváme $a \vee b \leq c$, takže $b \leq c$. Ovšem podle 14.3 neplatí ani $a \leq b$ ani $b \leq c$. Proto $b \wedge c < a \vee (b \wedge c) \leq (a \vee b) \wedge c < a \vee b$ a $b \wedge c < b < a \vee b$. Tím jsou dány operace $\wedge$ a $\vee$ na uvedených řetězcích. Zbývá určit $b \wedge x$ a $b \vee x$, kde $x \in \{a \vee (b \wedge c), (a \vee b) \wedge c\}$. Platí $b \wedge c \leq b \wedge (a \vee (b \wedge c)) \leq b \wedge ((a \vee b) \wedge c) = (b \wedge c) \wedge (a \vee b) \leq b \wedge c$, takže $b \wedge c = b \wedge (a \vee (b \wedge c)) = b \wedge ((a \vee b) \wedge c)$. Obdobně $b \vee a \geq b \vee ((a \vee b) \wedge c) \geq b \vee a \vee (b \wedge c) = b \vee a$. □

Modulární svazy jsou v matematice velmi důležité. Bez důkazu uvedeme jednu jejich typickou vlastnost: Jestliže $a = a_0 < \ldots < a_k = b$ a $c = c_0 < \ldots < c_r = d$ jsou dvě posloupnosti prvků modulárního svazu, kde každý člen posloupnosti pokrývá člen předchozí, tak z $a = c$ a $b = d$ plyne $r = k$. (V konečném modulárním svazu tedy platí, že každé dvě cesty v Hasseově diagramu mezi dvěma prvky jsou stejně dlouhé – pokud se ovšem pohybujeme pouze zdola nahoru nebo pouze zeshora dolů.)

14.5 Tvrzení. *Buď G grupa a A a B její podgrupy. Je-li A normální v G, tak podgrupa generovaná $A \cup B$ je rovna $AB = BA$. Svaz normálních podgrup G je modulární.*

Důkaz. První část tvrzení se shoduje s tvrzením 6.11. Dokažme tedy druhou část. Ať A, B, C jsou normální podgrupy G, $A \subseteq C$. Jetřeba ukázat $A \vee (B \cap C) \supseteq (A \vee B) \cap C$, čili $A(B \cap C) \supseteq (AB) \cap C$. Je-li $a \in A$, $b \in B$ a $ab \in C$, je $b = a^{-1}(ab) \in C$, takže $b \in B \cap C$. □

14.6 Tvrzení. *Buď L svaz. Potom jsou následující podmínky ekvivalentní.*
(i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ *pro všechna* $a, b, c \in L$.
(ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ *pro všechna* $a, b, c \in L$.
(iii) $(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$ *pro všechna* $a, b, c \in L$.

Přitom svaz splňující tyto podmínky je modulární.

Důkaz. (i)$\Longrightarrow$(ii) : $(a \wedge b) \vee (a \wedge c) = ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) = a \wedge ((a \wedge b) \vee c) = a \wedge ((a \vee c) \wedge (b \vee c)) =$
$= (a \wedge (a \vee c)) \wedge (b \vee c) = a \wedge (b \vee c)$.
(ii)$\Longrightarrow$(i) : Identity (i) a (ii) jsou duální. V předchozím důkazu tedy stačí zaměnit $\wedge$ a $\vee$.

(i+ii)$\Longrightarrow$(iii) : $(a\wedge b)\vee(a\wedge c)\vee(b\wedge c)=(a\wedge(b\vee c))\vee(b\wedge c)=((a\wedge(b\vee c))\vee b)\wedge((a\wedge(b\vee c))\vee c)=$
$=((a\vee b)\wedge(b\vee c))\wedge((a\vee c)\wedge(b\vee c))=(a\vee b)\wedge(a\vee c)\wedge(b\vee c)$.

(iii)$\Longrightarrow$(i) : Nejprve ukážeme modularitu. Je-li $a\le c$, dostáváme $a\vee(b\wedge c)=(a\wedge b)\vee(a\wedge c)\vee(b\wedge c)=$
$=(a\vee b)\wedge(a\vee c)\wedge(b\vee c)=(a\vee b)\wedge c$. Buď nyní $a,b,c\in L$ libovolná. Položme $u=(a\wedge b)\vee(b\wedge c)\vee(a\wedge c)$.
Pak $a\wedge(b\vee c)=a\wedge u=(((a\wedge b)\vee(a\wedge c))\vee(b\wedge c))\wedge a=((a\wedge b)\vee(a\wedge c))\vee(b\wedge c\wedge a)=(a\wedge b)\vee(a\wedge c)$. □

Svazy, které splňují ekvivalentní podmínky tvrzení 14.6 se nazývají *distributivní* a vztahy (i) a (ii) se nazývají distributivními zákony.

Na množině $\{0,u,v,w,1\}$ definujme svaz tak, že 0 je nejmenší prvek, 1 největší prvek, $u\wedge v=u\wedge w=$
$=v\wedge w=0$ a $1=u\vee v=u\vee w=v\vee w$. Tento svaz se obvykle značí M_5. Často se mu říká ‚diamant'.

M_5 zjevně není distributivní. Proto žádný distributivní svaz neobsahuje podsvaz izomorfní N_5 nebo M_5. Platí i obrácené tvrzení.

14.7 Tvrzení. *Svaz L je distributivní právě když neobsahuje podsvaz izomorfní N_5 nebo M_5.*

Nástin důkazu. Potřebujeme ukázat, že pokud modulární svaz není distributivní, lze v něm nalézt M_5. Není-li L distributivní, lze najít $x,y,z\in L$ takové, že $r=(x\wedge y)\vee(x\wedge z)\vee(y\wedge z)\ne(x\vee y)\wedge(x\vee z)\wedge$
$(y\vee z)=s$. Pak $r<s$ a pro $a=(x\wedge s)\vee r$, $b=(y\wedge s)\vee r$, $c=(z\wedge s)\vee r$ lze s trochou počítání pomocí modulárního zákona ukázat, že $a\wedge b=r$ a $a\vee b=s$. Ze symetrie pak vyplyne, že $a\wedge c=r=b\wedge c$ a $a\vee c=s=b\vee c$. Zbytek je již snadný. □

Buď $L=L(\wedge,\vee,0,1)$ 0,1–svaz, a ať $a\in L$. Potom $b\in L$ nazveme *komplementem* (doplňkem), jestliže $a\wedge b=0$ a $a\vee b=1$. Z definice plyne, že je-li b komplementem a, je a komplement b.

14.8 Tvrzení. *Buď L distributivní 0,1–svaz. Potom má každý prvek nejvýše jeden komplement.*

Důkaz. Buď b a c komplementy a. Pak $b=b\wedge1=b\wedge(a\vee c)=(b\wedge a)\vee(b\wedge c)=b\wedge c$. Tudíž $b\ge c$. Obdobně dostaneme $b\le c$, a tedy $b=c$. □

V N_5 má každý prvek komplement, ale tento komplement nemusí být jednoznačný. Totéž platí o M_5. Představme si, že v distributivním 0,1–svazu L má každý prvek komplement. Pak je jednoznačně určena unární operace $'$ taková, že pro všechna $a\in L$ je $a\wedge a'=0$ a $a\vee a'=1$.

Algebra $L=L(\vee,\wedge,0,1,')$, kde $L(\vee,\wedge,0,1)$ je distributivní 0,1–svaz a $'$ je unární operace, která vyhovuje identitám $a\wedge a'=0$ a $a\vee a'=1$, se nazývá *Booleova algebra*.

14.9 Lemma. *Ať $L=L(\vee,\wedge,0,1,')$ je Booleova algebra. Potom*

(i) $(a')'=a$ *pro všechna* $a\in L$.

(ii) $0'=1$ *a* $1'=0$.

(iii) $(a\wedge b)'=a'\vee b'$ *a* $(a\vee b)'=a'\wedge b'$ *pro všechna* $a,b\in A$. *(De Morganovy zákony.)*

Důkaz.

(i) a je komplement a'. Podle 14.8 je komplement jednoznačně určen. Proto $a=(a')'$.

(ii) Toto jistě každý zvládne.

(iii) $(a\wedge b)\vee(a'\vee b')=(a\vee a'\vee b')\wedge(b\vee a'\vee b')=1\wedge1=1$. $(a\wedge b)\wedge(a'\vee b')=(a\wedge b\wedge a')\vee(a\wedge b\wedge b')=$
$=0\vee0=0$. Druhý zákon je k prvému duální. □

15. Booleovy algebry

Je-li $L = L(\wedge, \vee, 0, 1)$ 0,1–svaz, nazývá se $a \in L$ *atomem,* jestliže $a \neq 0$ a z $0 \leq b \leq a$ plyne $b = a$ pro každé $b \in L$. Je-li L konečný svaz a $0 \neq b$, tak jistě existuje alespoň jeden atom $a \in L$ takový, že $0 < a \leq b$.

15.1 Lemma. *Buď $S = S(\wedge, \vee, 0_S, 1_S, ')$ a $T = T(\wedge, \vee, 0_T, 1_T, ')$ dvě Booleovy algebry. Bijektivní zobrazení $\varphi: S$ toT je izomorfismem právě když pro všechna $a, b \in S$ platí, že $a \leq_S b$ tehdy a jen tehdy, je-li $\varphi(a) \leq_T \varphi(b)$.*

Důkaz. Připomeňme, že podle 7.3 je $\varphi: S(\wedge, \vee) \to T(\wedge, \vee)$ izomorfismus, pokud $a \leq_S b$ je ekvivalentní $\varphi(a) \leq_T \varphi(b)$ pro $a, b \in S$. Je proto třeba ukázat, že pro izomorfismus $\varphi: S(\wedge, \vee) \to T(\wedge, \vee)$ platí $\varphi(0_S) = 0_T$, $\varphi(1_S) = 1_T$ a $\varphi(a') = (\varphi(a))'$ pro všechna $a \in S$. Pro každé $b \in T$ existuje $c \in S$, že $\varphi(c) = b$. Protože $\varphi(0_S) \wedge b = \varphi(0_S \wedge c) = \varphi(0_S)$, je $\varphi(0_S)$ nejmenší prvek $T(\wedge, \vee)$. Ovšem $T(\wedge, \vee)$ může mít jen jeden nejmenší prvek, takže $\varphi(0_S) = 0_T$. Podobně $\varphi(1_S) = 1_T$. Zbývá ukázat, že $\varphi(a')$ je komplement $\varphi(a)$. Ovšem $\varphi(a') \wedge \varphi(a) = \varphi(a' \wedge a) = \varphi(0_S) = 0_T$ a $\varphi(a') \vee \varphi(a) = \varphi(a' \vee a) = \varphi(1_S) = 1_T$.

Typickým příkladem Booleových algeber je množina $\mathcal{P}(X)$ všech podmnožin množiny X s operacemi průniku, sjednocení a množinovým doplňkem. Konečné Booleovy algebry jsou dokonce vždy takové algebře izomorfní.

Je-li $M = \{u_1, \ldots, u_k\}$ nějaká neprázdná konečná podmnožina Booleovy algebry S, klademe $\bigwedge_M = m_1 \wedge \cdots \wedge m_k$ a $\bigvee_M = m_1 \vee \cdots \vee m_k$. Definitoricky $\bigwedge_\emptyset = 1$ a $\bigvee_\emptyset = 0$.

15.2 Věta. *Buď $S = S(\wedge, \vee, 0, 1, ')$ konečná Booleova algebra a A ať je množina jejích atomů. Definujme zobrazení $\varphi: \mathcal{P}(A) \to S$ tak, že $\varphi(B) = \bigvee_B$ pro všechna $B \subseteq A$. Potom φ je izomorfismus Booleových algeber.*

Důkaz. Definujme $\psi: S \to \mathcal{P}(A)$ tak, že $\psi(s) = \{a \in A;\ a \leq s\}$. Nejprve ukážeme, že $\varphi\psi(s) = s$. Položme $\psi(s) = T$ a $\varphi\psi(s) = \bigvee_T = t$. Pak $t \leq s$. Předpokládejme, že $t < s$. Pak $s = s \wedge 1 = s \wedge (t \vee t') = (s \wedge t) \vee (s \wedge t') = t \vee (s \wedge t')$. Z $s \neq t$ plyne $s \wedge t' \neq 0$. Tudíž existuje $a \in A$ takový, že $a \leq s \wedge t'$. Z $a \leq s$ plyne $a \in T$, takže $a \leq t$. Současně ale $a \leq t'$, takže dostáváme $a \leq t \wedge t' = 0$, a to je spor. Je tedy $s = t$ a $\varphi\psi(s) = s$ pro každé $s \in S$.

Nyní dokážeme, že $\psi\varphi(B) = B$ pro všechna $B \subseteq A$. Položme $b = \bigvee_B$ a $T = \psi(b) = \{a \in A;\ a \leq b\}$. Zjevně $T \supseteq B$. Ať $a \in T \setminus B$. Pak $a = a \wedge b = \bigvee_{c \in B}(a \wedge c)$. Ovšem $a \wedge c \leq c$, takže z $a \neq c$ plyne $a \wedge c = 0$, a tedy $a = 0$. Proto $T = B$.

Pro $B \subseteq C \subseteq A$ jistě $\varphi(B) \leq \varphi(C)$ a pro $s \leq t$ jistě $\psi(s) \subseteq \psi(t)$. Podle 15.1 je ψ izomorfismus Booleových algeber.

Okruh R se nazývá *idempotentní*, jestliže $a^2 = a$ pro každé $a \in R$.

15.3 Tvrzení. *Buď $B(\wedge, \vee, 0, 1, ')$ Booleova algebra. Definujeme na B operace $+, \cdot$ tak, že $a + b = (a \wedge b') \vee (a' \wedge b)$ a $a \cdot b = a \wedge b$. Položíme dále $-a = a$ pro každé $a \in B$. Potom je $B(+, \cdot, -, 0, 1)$ komutativní idempotentní okruh charakteristiky 2. Naopak, je-li $B(+, \cdot, -, 0, 1)$ komutativní idempotentní okruh charakteristiky 2, tak $B(\wedge, \vee, 0, 1, ')$, kde $a \wedge b = a \cdot b$, $a \vee b = a + b + a \cdot b$, $a' = 1 + a$, je Booleova algebra.*

Důkaz. Buď nejprve $B(\wedge, \vee, 0, 1, ')$ Booleova algebra. Pak zjevně $a + b = b + a$, $a + a = 0$, $a + 0 = a$. Zbývá ověřit $a + (b + c) = (a + b) + c$ a $a \cdot (b + c) = a \cdot b + a \cdot c$ pro $a, b, c \in B$. Je $a + (b + c) = a + ((b' \wedge c) \vee (c' \wedge b)) = (a \wedge ((b' \wedge c) \vee (c' \wedge b))') \vee (a' \wedge ((b' \wedge c) \vee (c' \wedge b)) = (a \wedge (b \vee c') \wedge (c \vee b')) \vee (a' \wedge b' \wedge c) \vee (a' \wedge c' \wedge b)$. Ovšem $a \wedge (b \vee c') \wedge (c \vee b') = ((a \wedge b) \vee (a \wedge c')) \wedge (c \vee b') = (a \wedge b \wedge c) \vee (a \wedge b' \wedge c')$. Je tedy $a + (b + c) = (a \wedge b \wedge c) \vee (a \wedge b \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c)$. V tomto výraze lze a, b i c vzájemně zaměnit, aniž by se změnila hodnota tohoto výrazu. Vyměníme-li a a c, dostaneme opačnými úpravami, že $a + (b + c)$ je rovno $c + (a + b) = (a + b) + c$. Dále $a \cdot (b + c) = a \wedge ((b \wedge c') \vee (b' \wedge c)) = (a \wedge b \wedge c') \vee (a \wedge b' \wedge c)$. Ovšem $(a \wedge b) \wedge (a \wedge c)' = a \wedge b \wedge c'$ a $(a \wedge b)' \wedge (a \wedge c) = a \wedge b' \wedge c$.

Na druhou stranu, ať $B(+, \cdot, -, 0, 1)$ je komutativní idempotentní okruh charakteristiky 2. Pak $a \vee a = a + a + a^2 = a$, $(a \vee b) \vee c = a + b + ab + c + ac + bc + abc = a + b + c + bc + ab + ac + abc = a \vee (b \vee c)$, $a \vee 1 = a + 1 + a = 1$, $a \vee 0 = a$, $a \wedge (b \vee a) = a + ab + ab = a$, $a \vee (b \wedge a) = a + ba + ba = a$, $a \wedge (b \vee c) = a \cdot (b + c + bc) = ab + ac + a^2bc = (a \wedge b) \vee (a \wedge c)$. Konečně $(a')' = 1 + 1 + a = a$, $a \vee a' = a + 1 + a + a + a^2 = 1$ a $a \wedge a' = a(1 + a) = a + a = 0$.

16. Podílové okruhy a tělesa

Ať $R = R(+,\cdot,-,0,1)$ je komutativní okruh a ať S je podmonoid $R(\cdot,1)$, který neobsahuje dělitele nuly. Na množině $F = R \times S$ budeme definovat algebru $F = F(+,\cdot,-,0,1)$. Pro přehlednost budeme uspořádané dvojice $(a,b) \in R \times S$ zapisovat $\frac{a}{b}$. Buď $a,c \in R$ a $b,d \in S$. Definujeme

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad -\frac{a}{b} = \frac{-a}{b}, \quad 0_F = \frac{0}{1}, \quad 1_F = \frac{1}{1}.$$

16.1 Lemma. *$F(+,0)$ a $F(\cdot,1)$ jsou komutativní monoidy.*

Důkaz. Komutativita je zřejmá přímo z definice. Buď $a \in R$ a $b \in S$. Pak $\frac{a}{b} + \frac{0}{1} = \frac{a\cdot 1 + b\cdot 0}{b\cdot 1} = \frac{a}{b}$ a $\frac{a}{b} \cdot \frac{1}{1} = \frac{a\cdot 1}{b\cdot 1} = \frac{a}{b}$, takže 0_F a 1_F jsou neutrálními prvky. Pro násobení asociativita plyne rovněž okamžitě z definice. Ověřme asociativitu sčítání. Buďte $a,c,e \in R$ a $b,d,f \in S$. Pak $(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+bcf+bde}{bdf} = \frac{a}{b} + \frac{cf+de}{df} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$. □

Na F definujeme ekvivalenci $\sim$ tak, že $\frac{a}{b} \sim \frac{c}{d}$ právě když $ad = bc$.

16.2 Lemma. *$\sim$ je kongruence F.*

Důkaz. Nejprve je třeba ověřit, že $\sim$ je vskutku ekvivalence. Reflexivita a symetrie je jasná. Ať $\frac{a}{b} \sim \frac{c}{d}$ a $\frac{c}{d} \sim \frac{e}{f}$. Pak $acf = ade = bce$, čili $af = be$. Nyní je třeba ověřit, že $\sim$ je kongruence. Buď $\frac{a}{b} \sim \frac{c}{d}$. Pak jistě $-\frac{a}{b} \sim -\frac{c}{d}$. Buď ještě $\frac{e}{f} \sim \frac{g}{h}$. Pak $\frac{a}{b} + \frac{e}{f} = \frac{af+be}{bf}$ a $\frac{c}{d} + \frac{g}{h} = \frac{ch+dg}{dh}$. Ovšem $afdh + bedh = adfh + bdeh = bcfh + bdfg = bfch + bfdg$, takže $\frac{a}{b} + \frac{e}{f} \sim \frac{c}{d} + \frac{g}{h}$. Podobně z $adeh = bcfg$ plyne $\frac{a}{b} \cdot \frac{e}{f} \sim \frac{c}{d} \cdot \frac{g}{h}$. □

Očividně platí

16.3 Lemma. *Buď $a \in S$. Potom $\frac{0}{a} \sim 0_F$ a $\frac{a}{a} \sim 1_F$.* □

16.4 Lemma. *$F/\sim$ je komutativní okruh.*

Důkaz. Podle 16.1 stačí ověřit, že unární minus poskytuje opačné prvky, a ověřit distributivní zákon. Buď $a \in R$ a $b \in S$. Pak $\frac{a}{b} + (-\frac{a}{b}) = \frac{ab-ab}{bb} \sim 0_F$. Buď ještě $c,e \in R$ a $d,f \in S$. Pak $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{acf+ade}{bdf} \sim \frac{abcf+abde}{bbdf} = \frac{ac}{bd} + \frac{ae}{bf}$. □

Z 16.3 dostáváme:

16.5 Lemma. *Buď $a,b \in S$. Pak $\frac{a}{b} \cdot \frac{b}{a} \sim 1_F$.* □

Formálně správnější (ale méně přehledné) by bylo v předchozím textu místo $\frac{a}{b}$ psát (a,b). Představme si, že jsme zvolili tento formálně korektnější postup a nyní definujeme $\frac{a}{b} = [(a,b)]_\sim$. Od této chvíle tedy zlomkem $\frac{a}{b}$ označujeme celý blok $[(a,b)]_\sim$ ekvivalence $\sim$. Není to nic, co je v rozporu s naším běžným užíváním zlomků, vždyť nikoho nepřekvapí zápis $\frac{2}{6} = \frac{1}{3}$.

Okruh F se značívá $R[S^{-1}]$ a říká se mu *podílový okruh* R vzhledem k S nebo také *okruh zlomků* R podle S. Procesu, kterým se okruh $R[S^{-1}]$ definuje, se říká *lokalizace*.

Jestliže $a \in R$ a $b \in R$ nejsou dělitelé nuly, není ani jejich součin ab dělitelem nuly. Proto všechny prvky komutativního okruhu R, které nejsou dělitelé nuly, tvoří podmonoid $R(\cdot,1)$. Za S lze tedy zvolit například tento podmonoid. Přitom komutativní okruh R je obor integrity právě když množina S všech prvků R, kteří nejsou dělitelé nuly, je rovna $R \setminus \{0\}$. V takovém případě se $R[S^{-1}]$ nazývá *podílové těleso* oboru integrity S. To, že jde vskutku o těleso, plyne z 16.5, neboť podle tohoto lemmatu je v $R[S^{-1}]$ invertibilní každý zlomek, který lze vyjádřit tak, že jeho čitatel leží v S (jmenovatel leží v S vždy).

16.6 Tvrzení. *Ať R je komutativní okruh, S podmonoid $R(\cdot,1)$, který neobsahuje dělitele nuly. Definujme zobrazení $\sigma\colon R \to R[S^{-1}]$ tak, že $\sigma(r) = \frac{r}{1}$ pro každé $r \in R$. Platí, že σ je injektivní homomorfismus okruhů.*

Důkaz. Zjevně $\frac{r}{1} + \frac{s}{1} = \frac{r+s}{1}$, $\frac{r}{1} \cdot \frac{s}{1} = \frac{rs}{1}$ atd., takže σ je homomorfismus. Přitom $\frac{r}{1} = \frac{s}{1}$ právě když $r = s$, a proto je σ prosté. □

Protože σ je injektivní, můžeme ztotožnit prvek $r \in R$ s prvkem $\frac{r}{1} \in R[S^{-1}]$. V dalším tedy budeme hledět na R jako na podokruh $R[S^{-1}]$.

16.7 Tvrzení. *Ať R je komutativní okruh a S podmonoid $R(\cdot,1)$. Předpokládejme, že $\sigma\colon R \to U$ je injektivní homomorfismus okruhů, přičemž každý prvek $\sigma(s)$, kde $s \in S$, je v U invertibilní. Potom*

existuje jediný homomorfismus $\psi\colon R[S^{-1}] \to U$ takový, že $\psi(a) = \sigma(a)$ pro každé $a \in R$. Přitom $\psi(\frac{a}{b}) = \sigma(a)(\sigma(b))^{-1}$ pro libovolné $\frac{a}{b} \in R[S^{-1}]$. Homomorfismus ψ je rovněž injektivní.

Důkaz. Žádný prvek $s \in S$ nemůže být dělitelem nuly, neboť v opačném případě by $\sigma(s)$ nemohlo být invertibilní v U. Protože pro každé $b \in S$ má být $1_U = \psi(1_{R[S^{-1}]}) = \psi(\frac{b}{b}) = \psi(b \cdot \frac{1}{b}) = \sigma(b) \cdot \psi(\frac{1}{b})$, musí být $\psi(\frac{1}{b}) = (\sigma(b))^{-1}$ pro každé $b \in S$, a tedy $\psi(\frac{a}{b}) = \psi(a \cdot \frac{1}{b}) = \sigma(a)(\sigma(b)^{-1})$ pro každé $\frac{a}{b} \in R[S^{-1}]$. Pro libovolná $a \in R$ a $b \in S$ je $\sigma(a)\sigma(b) = \sigma(ab) = \sigma(ba) = \sigma(b)\sigma(a)$, a proto i $\sigma(b)\sigma(a)^{-1} = \sigma(a)^{-1}\sigma(b)$. Tudíž pro $\frac{a}{b} = \frac{c}{d}$ máme $ad = bc$, $\sigma(a)\sigma(d) = \sigma(b)\sigma(c)$ a tedy i $\sigma(a)\sigma(b)^{-1} = \sigma(b)^{-1}\sigma(a) = \sigma(c)\sigma(d)^{-1}$. Tím je dokázána korektnost a jednoznačnost definice zobrazení ψ. Zbývá ověřit, že ψ je homomorfismus. Zjevně $\psi(0_{R[S^{-1}]}) = 0_U$, $\psi(1_{R[S^{-1}]}) = 1_U$, $\psi(-\frac{a}{b}) = -\psi(\frac{a}{b})$, $\psi(\frac{a}{b} \cdot \frac{c}{d}) = \psi(\frac{a}{b})\psi(\frac{c}{d})$, a konečně $\psi(\frac{a}{b} + \frac{c}{d}) = \psi(\frac{ad+bc}{bd}) = \sigma(ad + bc)\sigma(bd)^{-1} = \sigma(a)\sigma(b)^{-1} + \sigma(c)\sigma(d)^{-1} = \psi(\frac{a}{b}) + \psi(\frac{c}{d})$. Injektivita plyne ψ snadno z injektivity σ. □

16.8 Tvrzení. *Ať pro $i \in \{1, 2\}$ jsou R_i komutativní okruhy, přičemž S_i jsou podmonoidy $R_i(\cdot, 1)$, které neobsahují dělitele nuly. Ať $\sigma\colon R_1 \simeq R_2$ je okruhový izomorfismus, který splňuje $\sigma(S_1) = S_2$. Potom $\psi\colon R_1[S_1^{-1}] \to R_2[S_2^{-1}]$, $\psi(\frac{a}{b}) = \frac{\sigma(a)}{\sigma(b)}$ je také izomorfismus.*

Důkaz. Protože R_2 lze považovat dle 16.6 za podmnožinu $R_2[S_2^{-1}]$, můžeme σ chápat jako injektivní homomorfismus $R_1 \to R_2[S_2^{-1}]$. Proto lze použít pro definici ψ Tvrzení 16.7. Podobně ze $\sigma^{-1}\colon S_2 \to S_1$ lze odvodit existenci homomorfismu $\gamma\colon R_2[S_2^{-1}] \to R_1[S_1^{-1}]$ takového, že $\gamma(\frac{c}{d}) = \frac{\sigma^{-1}(c)}{\sigma^{-1}(d)}$. Pak ale $\gamma\psi(\frac{a}{b}) = \frac{a}{b}$ a $\psi\gamma(\frac{c}{d}) = \frac{c}{d}$, takže ψ je bijektivní. □

V konstrukci $R[S^{-1}]$ stojí za povšimnutí, že pokud $b \in S$ má inverzní prvek už v R (tedy $bc = 1$ pro nějaké $c \in S$) tak $\frac{a}{b} = \frac{ac}{bc} = ac$ leží v S pro každé $a \in R$. To znamená, že pokud každý prvek z $S \subseteq R$ je invertibilní v R, lze $R[S^{-1}]$ ztotožnit s R. To speciálně znamená, že $(R[S^{-1}])[S^{-1}]$ je vždy rovno $R[S^{-1}]$ a že podílové těleso komutativního tělesa T je opět jenom těleso T.

Je vhodné si uvědomit, že podle 16.7 lze každý injektivní homomorfismus $\sigma\colon R \to U$, kde R je obor integrity a U těleso, jednoznačně rozšířit na homomorfismus $\psi\colon T \to U$, kde T je podílové těleso R. Homomorfismus je podle 16.7 injektivní, což však ovšem plyne z následujícího obecnějšího pozorování.

16.9 Lemma. *Ať T je těleso a $\gamma\colon T \to R$ homomorfismus okruhů, přičemž R je netriviální okruh a rovněž $\gamma(T)$ je netriviální. Potom je γ injektivní.*

Důkaz. Je třeba dokázat, že pro žádné nenulové $a \in T$ není $a \in \operatorname{Ker}\gamma$ (viz 5.8). Předpokládejme opak. Pak $1_R = \gamma(aa^{-1} = \gamma(a)\gamma(a^{-1}) = 0_R \cdot \gamma(a^{-1}) = 0_R$, a odsud plyne, že $r = 0$ pro každé $r \in R$, takže R je triviální. (Bez výpočtu lze důkaz provést, pokud si uvědomíme, že $\operatorname{Ker}\gamma$ je ideál T, přičemž jediným netriviálním ideálem tělesa T je celé těleso T.) □

Vraťme se nyní opět k podílovým tělesům. Ať R je obor integrity a T jeho podílové těleso. Podle 16.8 dostáváme izomorfní podílová tělesa, vyjdeme-li z izomorfních oborů integrity. Předpokládejme, že R je obsaženo v nějakém tělese U. Pak $\{ab^{-1}; a \in R, b \in R - \{0\}\}$ zjevně tvoří podtěleso generované R v U. Následující tvrzení vyslovuje víceméně zřejmý fakt, že toto podtěleso je izomorfní podílovému tělesu T.

16.10 Tvrzení. *Buď U těleso, $R \subseteq U$ obor integrity a T podílové těleso R. Ať V označuje podtěleso U generované R. Potom $\sigma\colon T \to V$, kde $\sigma(\frac{a}{b}) = ab^{-1}$ pro každé $\frac{a}{b} \in T$, je izomorfismus.*

Důkaz. To, že $\frac{a}{b} \mapsto ab^{-1}$ pro každé $\frac{a}{b} \in T$ je injektivní homomorfismus $T \to U$, plyne z 16.7 rozšířením inkluze $R \to U$, $r \mapsto r$. Sestrojený homomorfismus zobrazuje těleso T na podtěleso U, které je jistě nejmenším podtělesem, jež obsahuje R. □

16.11 Důsledek. *Je-li T podílové těleso okruhu celých čísel $\mathbb{Z}$, tak zobrazení $\sigma\colon T \to \mathbb{Q}$, $\sigma(\frac{a}{b}) = ab^{-1}$ je izomorfismus těles.* □

Předchozí důsledek je však trochu zavádějící tvrzení. V teoretické aritmetice se odvozují racionální čísla z celých konstrukcí, která je shodná s konstrukcí podílového tělesa. Důsledek 16.11 je tedy spíše možno pokládat za definici tělesa racionálních čísel.

Víme, že každý okruh R obsahuje nejmenší podokruh, řekněme S, který je roven všem hodnotám $i \times 1$, kde i probíhá celá čísla, je-li R charakteristiky 0, a i splňuje $0 \leq i < n$, je-li R charakteristiky $n \geq 0$.

V případě, že je $n > 0$, je $S \simeq \mathbb{Z}_n$. Protože $\mathbb{Z}_n$ obsahuje dělitele nuly, když u je číslo složené, vidíme, že obory integrity musí mít buď charakteristiku nula, nebo prvočíselnou charakteristiku. V tom druhém případě je $S \simeq \mathbb{Z}_p$ podtěleso R. Vidíme tedy, že v případě nenulové charakteristiky p obsahuje každé těleso T nejmenší podtěleso $P = \{i \times 1_T; 0 \leq i < p\}$. Tomuto tělesu se říká *prvotěleso*.

Obecně vzato je prvotěleso vždy definované jako nejmenší podtěleso daného tělesa T. Tato definice je korektní, protože všechna podtělesa tvoří uzávěrový systém nad T. Strukturu prvotělesa jsme v případě nenulové charakteristiky již popsali. Předpokládejme, že $\operatorname{char} T = 0$. Pak T obsahuje nejmenší podokruh $S = \{i \times 1_T; i \in \mathbb{Z}\} \simeq \mathbb{Z}$ a $\sigma: i \mapsto i \times 1_T$ je injektivní okruhový homomorfismus $\mathbb{Z} \to T$. Podle 16.10 (a vzhledem k 16.11) lze tento homomorfismus rozšířit na homomorfismus těles $\mathbb{Q} \to T$, $\frac{a}{b} \mapsto (a \times 1_T)(b \times 1_T)^{-1}$. Obrazem tohoto homomorfismu je nejmenší podtěleso, které obsahuje S, a to je nejmenší podtěleso T vůbec, tedy prvotěleso P. Vidíme, že v každém tělese T charakteristiky 0 je prvotěleso $P = \{(a \times 1_T)(b \times 1_T)^{-1}; a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\}\}$ izomorfní tělesu racionálních čísel $\mathbb{Q}$.

17. Existence kořenových a rozkladových nadtěles

V této kapitole bude T označovat komutativní těleso a $p \in T[x]$ bude nějaký polynom stupně $n \geq 1$. Označme I hlavní ideál generovaný polynomem p, tj. $I = pT[x] = \{ap;\ a \in T[x]\}$ je množina všech násobků polynomu p, čili množina všech polynomů dělitelných polynomem p.

V kapitole 9 jsme si již všimli, že s každým nenulovým polynomem je asociován právě jeden monický polynom (polynomy jsou totiž asociovány, liší-li se jen o násobek invertibilního prvku, přičemž invertibilní prvky z $T[x]$ jsou právě všechny nenulové prvky tělesa T). Asociované polynomy generují shodné hlavní ideály, takže při vyšetřování struktury konkrétního kvocientního okruhu $T[x]/I$ můžeme vždy zvolit polynom p monický.

Ukážeme, že ke kvocientnímu okruhu $T[x]/I = T[x]/pT[x]$ lze přistupovat podobně jako ke kvocientnímu okruhu $\mathbb{Z}/n\mathbb{Z}$. Přitom na příkladech rozebereme postup popsaný v kapitole 9, za tvrzením 9.18.

Jsou-li $a, b \in T[x]$, tak $a \equiv b \bmod I$ znamená, že je $a - b \in I$, tedy že p dělí $a - b$. Proto je přirozené vedle $a \equiv b \bmod I$ psát také $a \equiv b \bmod p$.

17.1 Lemma. *Množina* $\{a \in T[x];\ \deg a < n\}$ *je transversálou kongruence* $\bmod p$.

Důkaz. Je-li $b = pq + r$, kde $b, q, r \in T[x]$ jsou polynomy, platí $b \equiv r \bmod p$. Proto každý polynom $b \in T[x]$ je modulo p kongruentní s nějakým polynomem $r \in T[x]$, $\deg r < n = \deg p$.

Jsou-li a, b dva polynomy stupně menšího než $n = \deg p$, tak je i $\deg(a - b) < p$, a proto v takovém případě z $a \equiv b \bmod p$ plyne $a - b = 0$, a tedy $a = b$. □

Zobrazení $a \mapsto a + I$ je tudíž bijekce mezi transversálou $\{a \in T[x];\ \deg a < n\}$ a okruhem $T[x]/I$. Na $\{a \in T[x];\ \deg a < n\}$ můžeme tudíž přenést strukturu okruhu $T[x]/I$. Takto vzniklý okruh budeme označovat $(T[x])_p$. (Vztah $(T[x])_p$ a $T[x]/pT[x]$ je tedy podobný jako vztah $\mathbb{Z}_n$ a $\mathbb{Z}/n\mathbb{Z}$. V obou případech jde o okruhy indukované transversálou ve smyslu definice v závěru 4. kapitoly.)

Pro $a, b \in (T[x])_p$, kde $a = \sum_{0 \leq i < k} a_i x^i$ a $b = \sum_{0 \leq i < k} b_i x^i$ je $a + b$ rovno $\sum_{0 \leq i < k} (a_i + b_i) x^i$, čili sčítání v $(T[x])_p$ se shoduje s běžným sčítáním v $T[x]$. (To plyne ze $\deg(a + b) \leq \max\{\deg a, \deg b\}$.) Všimněte si, že zde je jistý rozdíl proti sčítání v $\mathbb{Z}_n$, neboť součty v $\mathbb{Z}_n$ se nemusí shodovat se součty v $\mathbb{Z}$.

Pro $a, b \in (T[x])_p$ uvažme nyní jejich součin c v $T[x]$, tj. $c = \sum_k (\sum_{i+j=k} a_i b_j) x^k$. Hodnotou součinu ab v $(T[x])_p$ je ten polynom stupně menšího než n, který je s c kongruentní modulo p, čili je to ten (jednoznačně určený) polynom r, že $ab = pq + r$, kde $\deg r < n$. Podobně jako v $\mathbb{Z}_n$, je tedy i v $(T[x])_p$ hodnota součinu rovna zbytku po dělení příslušným generátorem hlavního ideálu (v $\mathbb{Z}_n$ je jím n, v $(T[x])_p$ je jím p).

Připomeňme nyní, že polynom p je ireducibilní, jestliže nelze vyjádřit jako součin dvou vlastních dělitelů, tedy jestliže pro žádná $a, b \in T[x]$ současně neplatí $p = ab$, $\deg a < n$ a $\deg b < n$. V kapitole 9 jsme ukázali, že $T[x]$ je eukleidovský obor integrity, tedy obor hlavních ideálů, a tedy Gaussův okruh. Proto je každý ireducibilní polynom prvočinitel, takže podle 9.12 je ideál $I = pT[x]$ maximální právě když je p ireducibilní. Připomeňme (viz 4.6), že $T[x]/I$ je těleso právě když I je v $T[x]$ maximální ideál. Dokázali jsme:

17.2 Tvrzení. *Okruh* $(T[x])_p$ *je tělesem právě když* p *je ireducibilní polynom.*

Vzhledem k závažnosti tohoto tvrzení uvedeme i přímý důkaz:

Důkaz. Pokud p není ireducibilní, pak $p = a \cdot b$, kde $\deg a < n$ a $\deg b < n$. V $(T[x])_p$ v takovém případě máme $a \neq 0 \neq b$, $ab = 0$, takže $(T[x])_p$ není ani obor integrity, natož těleso. Je-li p ireducibilní a $0 \neq a \in (T[x])_p$, tak polynomy a a p jsou v $T[x]$ nesoudělné. Proto podle 9.9 existují polynomy $u, v \in T[x]$ takové, že $ua + vp = 1$. To ale znamená $ua \equiv 1 \bmod p$, takže k a lze v $(T[x])_p$ nalézt inverzní prvek. □

Z důvodů, které brzy ozřejmíme, je někdy potřebné psát místo x nějaký jiný symbol, například y.

Snadno lze ukázat, že polynom $t = y^3 + y + 1$ je nad $\mathbb{Z}_2[y]$ ireducibilní. (Kdyby tomu tak nebylo, polynom t by musel mít vlastní dělitel stupně 1, a tím pádem by musel mít alespoň jeden kořen. Ovšem ani 0 ani 1 kořenem zjevně nejsou.) Sčítání v $(\mathbb{Z}_2[y])_{y^3+y+1}$ nečiní obtíže, a pro násobení sestrojíme multiplikační tabulku:

$\cdot$	0	1	y	$y{+}1$	y^2	$y^2{+}1$	$y^2{+}y$	$y^2{+}y{+}1$
0	0	0	0	0	0	0	0	0
1	0	1	y	$y{+}1$	y^2	$y^2{+}1$	$y^2{+}y$	$y^2{+}y{+}1$
y	0	y	y^2	$y^2{+}y$	$y{+}1$	1	$y^2{+}y{+}1$	$y^2{+}1$
$y{+}1$	0	$y{+}1$	$y^2{+}y$	$y^2{+}1$	$y^2{+}y{+}1$	y^2	1	y
y^2	0	y^2	$y{+}1$	$y^2{+}y{+}1$	$y^2{+}y$	y	$y^2{+}1$	1
$y^2{+}1$	0	$y^2{+}1$	1	y^2	y	$y^2{+}y{+}1$	$y{+}1$	$y^2{+}y$
$y^2{+}y$	0	$y^2{+}y$	$y^2{+}y{+}1$	1	$y^2{+}1$	$y{+}1$	y	y^2
$y^2{+}y{+}1$	0	$y^2{+}y{+}1$	$y^2{+}1$	y	1	$y^2{+}y$	y^2	$y{+}1$

Podle předchozího je $(\mathbb{Z}_2[y])_{y^3+y+1}$ těleso, takže jsme vlastně sestrojili těleso řádu 8. Zkonstruovali jsem tedy těleso neprvočíselného řádu. V této kapitole ukážeme, že pro každé $n \in \mathbb{N}$ a každé prvočíslo q existuje komutativní těleso řádu q^n. Později ještě ukážeme, že komutativní tělesa jiných řádů neexistují a že každá dvě komutativní tělesa shodného řádu jsou izomorfní. Platí také, že každé konečné těleso je komutativní; to však dokazovat nebudeme.

Předpokládejme nyní, že $p \in T[y]$ je ireducibilní polynom. Nad tělesem $(T[y])_p$ můžeme opět uvažovat polynomy, tedy můžeme pracovat s okruhem $(T[y])_p[x]$. Protože T je podtělesem tělesa $(T[y])_p$ (prvky tělesa T totiž ztotožňujeme s polynomy stupně 0 a -1), platí $T[x] \subseteq (T[y])_p[x]$.

Polynomem ze $(\mathbb{Z}_2[y])_{y^3+y+1}[x]$ tedy například je $(y^2{+}1)x^6 + yx^5 + x^2 + (y^2{+}y{+}1)$, ale také $x^3 + x + 1$.

Máme-li spočítat hodnotu polynomu $a \in (T[y])_p[x]$ v nějakém bodě $u \in (T[y])_p$, můžeme postupovat tak, že pomocí vytvořené tabulky násobení postupně vyhodnotíme všechny mocniny u^i, kde $i \leq \deg a$, a pak opět pomocí tabulky násobení spočítáme hodnotu $a_i u^i$ v $(T[y])_p$, a nakonec provedeme součet.

Je-li $a = (y^2{+}1)x^6 + yx^5 + x^2 + (y^2{+}y{+}1) \in (\mathbb{Z}_2[y])_{y^3+y+1}[x]$ a $u = y{+}1$, tak tímto způsobem zjistíme, že $u^2 = y^2 + 1$, $u^3 = y^2$, $u^4 = y^2 + y + 1$, $u^5 = y$, $u^6 = y^2 + y$, $(y^2 + 1)u^6 = y + 1$, a tedy $a(y + 1) = y + 1$, takže a se v bodě $y + 1$ chová jako identické zobrazení.

Pro výpočet $a(u)$, kde $a = \sum a_i x^i \in (T[y])_p[x]$ a $u \in (T[y])_p$ ovšem můžeme použít i jiný postup. Pokud koeficienty a_i chápeme jako prvky okruhu $T[y]$, tak namísto polynomu a můžeme uvažovat polynom $b = \sum a_i x^i \in T[y][x]$ (grafický zápis polynomů b a a je stejný, ale jsou to polynomy nad různými okruhy). Prvek $u = \sum_{0 \leq i < n} u_i y^i \in (T[y])_p$ můžeme chápat jako polynom $v = \sum u_i y^i \in T[y]$. Nyní $b(v)$ je prvek $T[y]$ a existuje jediný prvek $w \in T[y]$ takový, že je $w \equiv b(v) \bmod p$ a $\deg w < n$.

17.3 Lemma. *Platí $w = a(u)$.*

Důkaz. Hodnota $b(v)$ je rovna součtu členů $a_i v^i$, kde $a_i v^i$ počítáme v $T[y]$. Hodnota $a(u)$ je rovna součtu členů $a_i u^i$, kde $a_i u^i$ počítáme v $(T[y])_p$. Pokud na $a_i u^i \in (T[y])_p$ pohlédneme jako na prvek $T[y]$, tak z definice $(T[y])_p$ okamžitě vyplývá, že je $a_i u^i \equiv a_i v^i \bmod p$. To ale znamená i $\sum a_i u^i \equiv \sum a_i v^i \bmod p$, čili $a(u)$ je kongruentní s $b(w)$ modulo p, pokud $a(u) \in (T[y])_p$ chápeme jako prvek $T[y]$. Je tedy $w \equiv a(u) \bmod p$ a platí $\deg w < n$ a $\deg a(u) < n$, čili nutně $w = a(u)$. □

Použijeme-li předchozí lemma na polynom $a = (y^2{+}1)x^6 + yx^5 + x^2 + (y^2{+}y{+}1) \in (\mathbb{Z}_2[y])_{y^3+y+1}[x]$, a na $u = y{+}1$, tak obdržíme $b(v) = (y^2{+}1)(y{+}1)^6 + (y{+}1)^5 + (y{+}1)^2 + (y^2{+}y{+}1) = y^8 + y^6 + y^5 + y^4 + y^2 + 1 = (y^3{+}y{+}1)(y^5{+}y) + (y{+}1)$, takže vskutku platí $a(u) = y{+}1 \equiv b(v) \bmod y^3 + y + 1$.

Lemma 17.3 má jeden velmi významný důsledek:

17.4 Tvrzení. *Buďte T komutativní těleso a $a = \sum a_i x^i \in T[x]$ polynom ireducibilní nad T. Položme $p = \sum a_i y^i$ a uvažme těleso $(T[y])_p \supseteq T$. Pak $a = \sum a_i x^i$ má v $(T[y])_p[x]$ kořen y.*

Důkaz. Vyhodnotíme-li polynom $\sum a_i x^i$ v $T[y][x]$, dostaneme po dosazení y hodnotu $\sum a_i y^i = p$. Ovšem jistě je $p \equiv 0 \bmod p$, a proto je podle 17.3 hodnota polynomu $a \in (T[y])_p[x]$ v bodě $y \in (T[y])_p$ rovna 0. □

Předchozí tvrzení tedy například říká, že polynom $x^3 + x + 1 \in (\mathbb{Z}_2[y])_{y^3+y+1}[x]$ má v $(\mathbb{Z}_2[y])_{y^3+y+1}$ kořen y. Pokud se o této skutečnosti chceme přesvědčit přímo z multiplikační tabulky tělesa $(T[y])_p$, vidíme, že y^3 je rovno $y{+}1$, takže je $y^3 + y + 1 = (y{+}1) + y + 1 = 0$. Mohli bychom se také dále ptát (i když to v tuto chvíli není podstatné), zda se polynom $x^3{+}x{+}1$ rozkládá v $(\mathbb{Z}_2[y])_{y^3+y+1}[x]$ na kořenové činitele. Tak tomu skutečně je, a platí $x^3 + x + 1 = (x - y)(x - y^2)(x - (y^2{+}y))$.

Každý polynom stupně alespoň 1 je součinem ireducibilních polynomů, a proto 17.4 okamžitě implikuje:

17.5 Důsledek. *Buď T komutativní těleso a $a \in T[x]$ polynom stupně alespoň 1. Potom existuje komutativní těleso $U \supseteq T$ takové, že a má v U alespoň jeden kořen.* □

Nemalá péče, kterou jsme věnovali důkazu 17.5, byla motivována snahou po předložení snadno pochopitelného postupu, který by využíval analogií s počítáním dle celočíselných modulů. Existují samozřejmě daleko kratší důkazy, které nevyžadují definici tělesa $(T[y])_p$. Například následujícím důkazem 17.5 by bylo možno nahradit celou předcházející část této kapitoly.

Důkaz. Protože a je součinem polynomů ireducibilních v $T[x]$, lze předpokládat, že a je ireducibilní. Pak $I = a\,T[x]$ je maximální ideál a $U = T[x]/I$ je těleso. Zobrazení $t \mapsto t + I$ je homomorfismus těles $T \to U$, takže při ztotožnění t a $t + I$ můžeme T chápat jako podtěleso U. Pak máme $T[x] \subseteq U[x]$, a dosadíme-li do $a \in U[x]$ hodnotu $x + I$, dostaneme $a + I$. Ovšem a je prvek I, takže $a + I = I = 0_U$, a proto je $a(x + I) = 0_U$. □

Buď U komutativní těleso a T jeho podtěleso. Pro $S \subseteq U$ se podtěleso generované $T \cup S$ značí $T(S)$. Je-li $S = \{\alpha_1, \ldots, \alpha_k\}$, tak vedle $T(S)$ píšeme též $T(\alpha_1, \ldots, \alpha_k)$.

Je-li $a \in T[x]$ a $\alpha \in U$ je kořenem polynomu a, tak se těleso $T(\alpha)$ nazývá *kořenové nadtěleso* polynomu a. Jestliže se polynom $a \in T[x]$ v $U[x]$ rozkládá na kořenové činitele a $\alpha_1, \ldots, \alpha_k$ jsou všechny jeho kořeny, tak se těleso $T(\alpha_1, \ldots, \alpha_k)$ nazývá *rozkladové nadtěleso* polynomu a.

Z 17.5 plyne, že ke každému polynomu $a \in T[x]$ lze sestrojit kořenové nadtěleso. Indukcí nyní snadno dokážeme existenci rozkladových nadtěles.

17.6 Tvrzení. *Buď T komutativní těleso a $a \in T[x]$ ať je polynom stupně alespoň 1. Pak existuje komutativní těleso $U \supseteq T$ takové, že a se v $U[x]$ rozkládá na kořenové činitele.*

Důkaz. Postupujme indukcí podle $n = \deg a$. Je-li $n = 1$, stačí položit $U = T$. Ať je $n > 1$ a ať $V \supseteq T$ je kořenové nadtěleso polynomu a, přičemž $\alpha \in V$ je kořen a. Pak a je rovno $(x - \alpha)b$, kde $b \in V[x]$ je stupně $n - 1$. Podle indukčního předpokladu existuje komutativní těleso $U \supseteq V$, ve kterém se b (a tím pádem i a), rozkládá na kořenové činitele. □

17.7 Tvrzení. *Buď p prvočíslo a $n \in \mathbb{N}$. Rozkladové nadtěleso polynomu $x^{p^n} - x \in \mathbb{Z}_p[x]$ má právě p^n prvků.*

Důkaz. Ať U je nějaké rozkladové nadtěleso polynomu $x^{p^n} - x$. Z $U \supseteq \mathbb{Z}_p$ plyne, že charakteristika U je rovna p. Ať M označuje množinu všech kořenů polynomu $x^{p^n} - x$. Protože p nedělí $p^n - 1$, plyne z 9.16, že $x^{p^n} - x$ má vesměs různé kořeny, takže M má p^n prvků. Přitom $a \in U$ leží v M tehdy, je-li $a^{p^n} = a$. Z 9.22 vyplývá, že M je těleso, takže M obsahuje i prvotěleso $\mathbb{Z}_p$. Ovšem U má být nejmenší těleso, které obsahuje $\mathbb{Z}_p$ a M, a proto musí být rovno M. □

17.8 Tvrzení. *Ať U je nějaké komutativní těleso řádu p^n, kde p je prvočíslo a $n \in \mathbb{N}$. Ať $P \simeq \mathbb{Z}_p$ je prvotěleso tělesa U. Pak U je rozkladovým nadtělesem polynomu $x^{p^n} - x \in P[x]$.*

Důkaz. Řád grupy U^* je $p^n - 1$, takže $a^{p^n - 1} = 1$ platí pro každé nenulové $a \in U$. To znamená, že každé $a \in U$ splňuje $a^{p^n} = a$, a tedy U je tvořeno právě všemi kořeny polynomu $x^{p^n} - x$. □

V následujících kapitolách dokážeme, že
(i) každé konečné komutativní těleso charakteristiky p musí mít řád p^n, kde $n \in \mathbb{N}$, a že
(ii) dvě rozkladová tělesa nad týmž polynomem jsou vždy izomorfní.

Z 17.7 a 17.8 tudíž poté vyplyne, že konečné komutativní těleso řádu m existuje právě když $m = p^n$ je mocnina prvočísla, a že libovolná dvě komutativní tělesa stejného konečného řádu jsou navzájem izomorfní.

18. Algebraické prvky a minimální polynomy

V celé této kapitole ‚těleso' znamená ‚komutativní těleso'.

Jestliže $U \supseteq T$ jsou komutativní tělesa, tak U můžeme chápat jako vektorový prostor nad T (sčítání ve vektorovém prostoru je shodné se sčítáním v U, je–li $t \in T$ a $u \in U$, tak skalární násobení $t \cdot u$ definujeme jako součin $t \cdot u$ v tělese U). Dimenze $\dim_T U$ vektorového prostoru U se značí $[U : T]$ a nazývá se *stupeň* tělesa U (nad T). Je–li $[U : T] < \infty$, řekneme, že U je *rozšíření konečného stupně*.

Jako příklad můžeme uvést komplexní a reálná čísla. Je zřejmé, že $\mathbb{C}$ jako reálný vektorový prostor má dimenzi 2 (máme-li zvolit jeho bázi, tak nejpřirozenější je vybrat čísla 1 a i). Poznamenejme, že $\mathbb{C}$ je jak kořenové, tak rozkladové nadtěleso polynomu $x^2 + 1 \in \mathbb{R}[x]$.

18.1 Lemma. *Buď $T \subseteq U \subseteq V$ do sebe vřazená tělesa. Potom $[V : T] = [V : U] \cdot [U : T]$.*

Důkaz. Ať A je báze U nad T a B je báze V nad U. Stačí ukázat, že $C = \{ab;\ a \in A,\ b \in B\}$ je báze V nad T. Je-li $v \in V$, existují $u_b \in U$, že $v = \sum_{b\in B} u_b b$, a protože každé u_b lze zapsat jako $\sum_{a\in A} t_{a,b} a$, kde $t_{a,b} \in T$, tak $v = \sum t_{a,b} ab$. Naopak, ať $\sum t_{a,b} ab = 0$, kde $a \in A$, $b \in B$ a $t_{a,b} \in T$. Pak $\sum_{b\in B}(\sum_{a\in A} t_{a,b} a)b = 0$, takže pro každé $b \in B$ je $\sum_{a\in A} t_{a,b} a = 0$, a tedy $t_{a,b} = 0$ pro všechna $a \in A$, $b \in B$. □

18.2 Lemma. *Ať $S \supseteq R$ jsou komutativní okruhy a α ať je prvek S. Pak okruh $R[\alpha]$ je roven okruhu* $\operatorname{Im} j_\alpha = \{a(\alpha);\ a \in R[x]\}$.

Důkaz. $\{a(\alpha);\ a \in R[x]\} = \operatorname{Im} j_\alpha$ je podokruh S, a proto $R[\alpha] \subseteq \operatorname{Im} j_\alpha$. Pro $a = \sum a_i x^i \in R[x]$ je $a(\alpha) = \sum a_i \alpha^i$ jistě prvek $R[\alpha]$. □

Prvek $\alpha \in U$ se nazývá *algebraický* (nad T), jestliže $a(\alpha) = 0$ pro nějaké $a \in T[x]$, $a \neq 0$. Pokud takový polynom a neexistuje, nazýváme α *transcendentní* (nad T).

18.3 Tvrzení. *Nechť $T \subseteq U$ jsou tělesa a ať $\alpha \in U$ je prvek algebraický nad T. Pak existuje jediný monický polynom $m \in T[x]$ takový, že pro všechna $a \in T[x]$ je $a(\alpha) = 0$ právě když m dělí a. Polynom m je ireducibilní a hlavní ideál $mT[x]$ je jádrem dosazovacího homomorfismu $j_\alpha : T[x] \to U$. Zobrazení $a + mT[x] \mapsto a(\alpha)$ je izomorfismus okruhů $T[x]/mT[x]$ a $T[\alpha]$. Oba tyto okruhy jsou tělesa a platí $T[\alpha] = T(\alpha)$.*

Důkaz. Pro $a \in T[x]$ platí $a(\alpha) = 0$ právě když je $j_\alpha(a) = 0$. Jádro homomorfismu j_α je vlastní ideál, a z kapitoly 10 víme, že každý vlastní ideál lze jednoznačným způsobem vyjádřit jako hlavní ideál generovaný monickým polynomem.

Ať m dělí pq, kde $p, q \in T[x]$ jsou polynomy. Pak $0 = m(\alpha) = p(\alpha)q(\alpha)$, takže je $p(\alpha) = 0$ nebo $q(\alpha) = 0$. Čili m dělí p nebo q, takže vidíme, že m je prvočinitel, a tedy ireducibilní polynom.

Podle 18.2 je $\operatorname{Im} j_\alpha$ rovno $T[\alpha]$, takže j_α je surjektivní homomorfismus $T[x]$ na $T[\alpha]$. Podle první věty o izomorfismu je zobrazení $a + mT[x] \mapsto a(\alpha)$ izomorfismem okruhů $T[x]/mT[x]$ a $T[\alpha]$. Protože $mT[x]$ je maximální ideál (viz 9.12), tak je okruh $T[x]/mT[x]$ tělesem (viz 4.6), a proto je i okruh $T[\alpha]$ těleso. Protože $T(\alpha)$ je nejmenší podtěleso U, které obsahuje $T[\alpha]$, musí být $T(\alpha) = T[\alpha]$. □

Polynom m z Tvrzení 18.3 se nazývá *minimální polynom* prvku α (nad T) a značí se m_α.

18.4 Tvrzení. *Buď $\alpha \in U \supseteq T$. Pak α je algebraický nad T právě když $[T(\alpha) : T] < \infty$. Je-li α algebraický nad T, tak $T(\alpha) = T[\alpha]$ a $[T[\alpha] : T] = \deg m_\alpha$.*

Důkaz. Ať $[T(\alpha) : T] = n$. Je-li $n < \infty$, jsou $1, \alpha, \ldots, \alpha^n$ prvky nad T lineárně závislé, takže existují $c_0, c_1, \ldots, c_n$ prvky T takové, že $\sum c_i \alpha^i = 0$ a $c_j \neq 0$ pro alespoň jedno $0 \leq j \leq n$. Tudíž $c(\alpha) = 0$ pro $0 \neq c = \sum c_i x^i$, takže α je algebraický nad T.

Naopak, ať $\alpha \in U$ je algebraický nad T a $s = \deg m_\alpha$. Ukážeme, že $1, \alpha, \ldots, \alpha^{s-1}$ tvoří bázi $T[\alpha] = T(\alpha)$. Je-li $c \in T[x]$, $\deg c \leq s - 1$, tak $c(\alpha) = 0$ jedině pro $c = 0$. Proto jsou $1, \alpha, \ldots, \alpha^{s-1}$ lineárně nezávislé. Je-li $\beta \in T[\alpha]$, tak existuje $b \in T[x]$, že $\beta = b(\alpha)$. Ovšem $b = m_\alpha q + r$, kde $q, r \in T[x]$, $r = \sum r_i x^i$ a $\deg r < \deg m_\alpha = s$, takže $\beta = b(\alpha) = r(\alpha) = \sum_{1\leq i\leq s-1} r_i \alpha^i$. □

Ať $T \subseteq U$ jsou tělesa. U nazveme *algebraickým rozšířením* T, jestliže každý prvek $\beta \in U$ je algebraický nad T.

18.5 Důsledek. *Každé rozšíření konečného stupně U tělesa T je algebraické rozšíření.*

Důkaz. Buď $\beta \in U$. Podle 18.1 je $[U : T] = [U : T(\beta)] \cdot [T(\beta) : T]$, takže $[T(\beta) : T]$ je konečné číslo. Podle 18.4 je β algebraický prvek. □

18.6 Tvrzení. *Ať $T \subseteq U$ jsou tělesa a $\alpha_1, \ldots, \alpha_n \in U$ jsou algebraické nad T. Potom $V = T(\alpha_1, \ldots, \alpha_n)$ je konečné algebraické rozšíření T a $V = T[\alpha_1, \ldots, \alpha_n]$.*

Důkaz. Položme $T_0 = T$ a $T_i = T[\alpha_1, \ldots, \alpha_i]$, $1 \leq i \leq n$. Indukcí ukážeme, že T_i je těleso a že pro $i \geq 1$ je $[T_i : T_{i-1}]$ konečné. Pro $i = 0$ není co dokazovat, ať $0 \leq i \leq n-1$. Pak $T_{i+1} = T_i[\alpha_{i+1}]$, přičemž α_{i+1} je algebraický nad $T_i \supseteq T$. Podle 18.3 je T_{i+1} těleso a podle 18.4 je $[T_{i+1} : T_i]$ konečné.

Tudíž $V = T_n$, V je rozšíření konečného stupně, a to je podle 18.5 algebraické. □

18.7 Důsledek. *Ať $U \supseteq T$ je rozkladové nadtěleso polynom $a \in T[x]$ a ať $\alpha_1, \ldots, \alpha_n \in U$ jsou všechny kořeny a. Pak $U = T[\alpha_1, \ldots, \alpha_n]$.* □

Na závěr této kapitoly ještě zmíníme, jak lze dosažené výsledky využít pro konečná tělesa.

18.8 Lemma. *Buď T konečné těleso, a ať p je jeho charakteristika. Pak je $p > 0$ prvočíslo a $|T| = p^n$ pro nějaké $n \in \mathbb{N}$.*

Důkaz. T je vektorový prostor nad prvotělesem P. Protože P je konečné, je $P \simeq \mathbb{Z}_p$. T je nad P dimenze $[T : P]$, takže $|T| = |P|^{[T:P]}$. □

Podle 10.12 je multiplikativní grupa T^* každého konečného tělesa T cyklická. Má-li těleso $q = p^n$ prvků, tak T^* je řádu $q-1 = p^n - 1$, takže cyklická grupa T^* má $\varphi(p^n - 1)$ generátorů. Je zvykem každý takový generátor nazývat *primitivní prvek* tělesa T. Je-li $P \simeq \mathbb{Z}_p$, tak $T = P[\xi]$ jistě platí pro každý primitivní prvek ξ. Podle 18.4 tudíž dostáváme:

18.9 Tvrzení. *Ať T je konečné těleso řádu p^n a P jeho prvotěleso. Ať ξ je nějaký primitivní prvek tělesa T. Pak je $P \simeq \mathbb{Z}_p$ a $\deg m_\xi = n$.* □

Z 18.3 nyní okamžitě plyne:

18.10 Důsledek. *Pro každé $n \in \mathbb{N}$ a pro každé prvočíslo p existuje ireducibilní polynom $a \in \mathbb{Z}_p[x]$, který je stupně n.* □

Podle 18.10 je tedy vždy možné sestrojit těleso řádu p^n ve tvaru $\mathbb{Z}_p[x]_a$ (viz kapitola 17). V následující kapitole dokážeme, že libovolná dvě tělesa řádu p^n jsou izomorfní. To znamená, že ze strukturálního hlediska nezáleží na konkrétní volbě ireducibilního polynomu a.

Možná, že si někdo položí otázku po vztahu polynomu $x^{p^n} - x \in \mathbb{Z}_p[x]$ a ireducibilních polynomů stupně n. K tomu lze například uvést, že $x^{p^n} - x$ je roven součinu všech ireducibilních polynomů stupňů $m \leq n$, přičemž každý z těchto polynomů se v rozkladu polynomu $x^{p^n} - x$ vyskytuje právě jednou. Toto tvrzení ovšem leží mimo rámec výkladu, a dokazovat ho nebudeme.

19. Jednoznačnost kořenových a rozkladových nadtěles

19.1 Lemma. *Ať $f: R \simeq S$ je izomorfismus okruhů a ať $I \subseteq R$ a $J \subseteq S$ jsou ideály takové, že $f(I) = J$. Potom zobrazení $a + I \mapsto f(a) + J$ je korektně definované a je to izomorfismus $R/I \simeq S/J$.*

Důkaz. $\mathrm{nat}_J f: R \to S/J$ je surjektivní homomorfismus, který zobrazuje prvek $a \in R$ na $f(a) + J$. Jeho jádrem je ideál I, a proto podle 1. věty o izomorfismu (7.10) je $a + I \mapsto f(a) + J$ izomorfismus R/I a S/J. □

Je-li $f: R \to S$ homomorfismus okruhů, definujeme $f_x: R[x] \to S[x]$ tak, že pro $a = \sum a_i x^i \in R[x]$ je $f_x(a) = \sum f(a_i)x^i$. Všimněte si, že zobrazení f_x je rozšířením homomorfismu f.

19.2 Lemma. *$f_x: R[x] \to S[x]$ je okruhový homomorfismus.*

Důkaz. Ať $a = \sum a_i x^i$ a $b = \sum b_i x^i$ jsou polynomy z $R[x]$. Pak $f_x(a+b) = \sum f(a_i + b_i)x^i = \sum(f(a_i) + + f(b_i))x^i = f_x(a) + f_x(b)$ a $f_x(a \cdot b) = \sum_k f(\sum_{i+j=k} a_i b_j)x^k = \sum_k(\sum_{i+j=k} f(a_i)f(b_j))x^k = f_x(a)f_x(b)$. Zbytek je zřejmý. □

Okruh $R[x]$ je generován množinou $R \cup \{x\}$. Je-li A nějaký jiný okruh a h_1, h_2 jsou homomorfismy $R[x] \to A$, tak podle 13.12 musí být $h_1 = h_2$, pokud platí $h_1(x) = h_2(x)$ a pro každé $r \in R$ je $h_1(r) = = h_2(r)$. Tohoto pozorování využijeme v obou následujících lemmatech.

19.3 Lemma. *Buďte $f: R \to S$ a $g: S \to T$ homomorfismy okruhů. Pak $(gf)_x = g_x f_x$.*

Důkaz. Platí $(gf)_x(x) = g_x(f_x(x))$ a pro $r \in R$ je $g_x f_x(r) = gf(r) = (gf)_x(r)$. □

19.4 Důsledek. *Buď $f: R \simeq S$ izomorfismus okruhů. Pak $f_x: R[x] \to S[x]$ je rovněž izomorfismus.*

Důkaz. Podle 19.3 je $f_x(f^{-1})_x = (\mathrm{id}_S)_x = \mathrm{id}_{S[x]}$ a $(f^{-1})_x f_x = (\mathrm{id}_R)_x = \mathrm{id}_{R[x]}$. □

19.5 Lemma. *Buď $f: R \to S$ homomorfismus okruhů a ať $\alpha \in R$. Pak $f j_\alpha = j_{f(\alpha)} f_x$.*

$$\begin{array}{ccc} R[x] & \xrightarrow{f_x} & S[x] \\ {\scriptstyle j_\alpha}\downarrow & & \downarrow{\scriptstyle j_{f(\alpha)}} \\ R & \xrightarrow{f} & S \end{array}$$

Důkaz. $f j_\alpha(r) = f(r) = j_{f(\alpha)}(f(r)) = j_{f(\alpha)} f_x(r)$ pro $r \in R$, a $f j_\alpha(x) = f(\alpha) = j_{f(\alpha)}(x) = j_{f(\alpha)} f_x(x)$. □

19.6 Lemma. *Buď $f: T \simeq S$ izomorfismus komutativních těles a ať $I \subseteq T[x]$ a $J \subseteq S[x]$ jsou nenulové ideály, pro které platí $f_x(I) = J$. Jsou-li $a \in T[x]$ a $b \in S[x]$ ty (jednoznačně určené) monické polynomy, které splňují $I = aT[x]$ a $J = bS[x]$, tak platí $f_x(a) = b$.*

Důkaz. $bS[x] = J = f_x(I) = f_x(aT[x]) = f_x(a)f_x(T[x]) = f_x(a)S[x]$ a $f_x(a)$ je monický polynom. Víme (viz kapitola 9), že ideál J je generován právě jedním monickým polynomem. Proto se $f_x(a)$ musí rovnat b. □

19.7 Tvrzení. *Buďte $T \subseteq U$ a $S \subseteq V$ komutativní tělesa, $f: T \simeq S$ izomorfismus a ať $\alpha \in U$ je prvek algebraický nad T a $\beta \in V$ prvek algebraický nad S. Izomorfismus $g: T[\alpha] \simeq S[\beta]$ splňující $g(\alpha) = \beta$ a $g(t) = f(t)$ pro všechna $t \in T$ existuje právě když $f_x(m_\alpha) = m_\beta$.*

Důkaz. Předpokládejme nejprve, že platí $f_x(m_\alpha) = m_\beta$. S využitím 18.3 a 19.1 sestrojíme řadu izomorfismů

$$T[\alpha] \simeq T[x]/m_\alpha T[x] \simeq S[x]/m_\beta S[x] \simeq S[\beta].$$

Oba krajní izomorfismy vyjadřují skutečnost, že každé kořenové nadtěleso algebraického prvku je strukturálně shodné s kvocientem podle hlavního ideálu příslušného minimálního polynomu (toto pozorování je obsahem Tvrzení 18.3). Prostřední izomorfismus je pak přímou aplikací 19.1, kde se říká, že izomorfismus okruhů (zde je to izomorfismus f_x) lze přenést na izomorfismus kvocientních okruhů, jestliže faktorizujeme přes ideály, které si v daném izomorfismu jednoznačně odpovídají (zde to jsou hlavní ideály generované polynomy m_α a m_β).

Proveďme nyní naznačený postup podrobně. Podle Tvrzení 18.3 jsou zobrazení $u: T[x]/m_\alpha T[x] \to T[\alpha]$ a $v: S[x]/m_\beta S[x] \to S[\beta]$, jež jsou definována vztahy $u(a + m_\alpha T[x]) = a(\alpha)$ a $v(b + m_\beta S[x]) = = b(\beta)$, izomorfismy. Protože f_x je podle 19.4 izomorfismus $T[x]$ a $S[x]$ a protože podle předpokladu je

$f_x(m_\alpha T[x]) = m_\beta S[x]$, dostáváme z 19.1 izomorfismus $w\colon T[x]/m_\alpha T[x] \simeq S[x]/m_\beta S[x]$, $w(a+m_\alpha T[x]) = f_x(a) + m_\beta S[x]$.

Jako vhodný kandidát se na místo hledaného izomorfismu g se přímo nabízí vwu^{-1}. Stačí ověřit, že je $vwu^{-1}(\alpha) = \beta$ a že $vwu^{-1}(t) = f(t)$ pro každé $t \in T$. Z definic izomorfismů v, w a u ale skutečně dostáváme $vwu^{-1}(t) = vw(t + m_\alpha T[x]) = v(f(t) + m_\beta S[x]) = f(t)$. Protože $x(\alpha) = \alpha$ a $x(\beta) = \beta$, tak $vwu^{-1}(\alpha) = vw(x + m_\alpha T[x]) = v(x + m_\beta S[x]) = \beta$, a lze tedy položit $g = vwu^{-1}$.

Nyní naopak předpokládejme, že existuje izomorfismus $g\colon T[\alpha] \simeq S[\beta]$, který je rozšířením $f\colon T \simeq S$, a splňuje $g(\alpha) = \beta$. Uvažme dosazovací homomorfismy $j_\alpha\colon T[\alpha][x] \to T[\alpha]$ a $j_\beta\colon S[\beta][x] \to S[\beta]$. Podle 19.5 je $j_\beta g_x = g j_\alpha$:

$$\begin{array}{ccc} T[x] \subseteq T[\alpha][x] & \xrightarrow{\ g_x\ } & S[\beta][x] \supseteq S[x] \\ {\scriptstyle j_\alpha}\downarrow & & \downarrow{\scriptstyle j_\beta} \\ T \subseteq T[\alpha] & \xrightarrow{\ g\ } & S[\beta] \supseteq S \end{array}$$

Pro $a \in T[x]$ je jistě $f_x(a) = g_x(a)$, neboť g je rozšířením f. Pro $a \in T[x]$ tedy platí $a \in m_\alpha T[x] \Leftrightarrow a(\alpha) = 0 \Leftrightarrow j_\alpha(a) = 0 \Leftrightarrow g j_\alpha(a) = 0 \Leftrightarrow j_\beta g_x(a) = 0 \Leftrightarrow (g_x(a))(\beta) = 0 \Leftrightarrow (f_x(a))(\beta) = 0 \Leftrightarrow f_x(a) \in m_\beta S[x]$. Polynom a tedy patří do ideálu $m_\alpha T[x]$ právě když $f_x(a)$ patří do ideálu $m_\beta S[x]$, takže $f_x(m_\alpha T[x]) = m_\beta S[x]$. Podle 19.6 je $f_x(m_\alpha)$ rovno m_β. □

19.8 Věta. *Buď $f\colon T \simeq S$ izomorfismus komutativních těles, $a \in T[x]$, $\deg a \geq 1$, a ať $U \supseteq T$ je rozkladové nadtěleso polynomu $a \in T[x]$, zatímco $V \supseteq S$ je rozkladové nadtěleso polynomu $b = f_x(a)$. Ať $\alpha_1, \ldots, \alpha_m$ jsou kořeny a v U a $\beta_1, \ldots, \beta_n$ kořeny b ve V. Pak $m = n$ a existuje permutace $\sigma \in S_n$ a izomorfismus $g\colon U \simeq V$ tak, že $g(t) = f(t)$ pro všechna $t \in T$ a $g(\alpha_i) = \beta_{\sigma(i)}$ pro $1 \leq i \leq n$.*

Důkaz. Ať $a = p_1^{k_1} \ldots p_r^{k_r}$ je rozklad polynomu a na ireducibilní činitele v $T[x]$. Položme $q_i = f_x(p_i)$, $1 \leq i \leq k$. Pak $b = q_1^{k_1} \ldots q_r^{k_r}$ je podle 19.4 rozklad na ireducibilní činitele v $S[x]$. Důkaz provedem indukcí podle $[U : T]$. Je-li $U = T$, lze kořeny uspořádat tak, že $p_i = x - \alpha_i$ a $q_i = x - \beta_i$, $1 \leq i \leq r$, takže stačí položit $g = f$. Ať je $[U : T] = j > 0$ a ať věta platí pro každý stupeň menší než j. Kořeny a polynomy jistě můžeme uspořádat tak, aby α_1 byl kořen p_1 a β_1 kořen q_1, a aby $\deg p_1 = \deg q_1 > 1$. Podle 19.7 existuje izomorfismus $h\colon T(\alpha_1) \to S(\beta_1)$ takový, že $h(\alpha_1) = \beta_1$ a $h(t) = f(t)$ pro každé $t \in T$. Protože $[U : T] = [U : T(\alpha_1)] \cdot [T(\alpha_1) : T] = [U : T(\alpha_1)] \cdot \deg p_1$ (viz 18.1 a 18.3), je $[U : T(\alpha_1)] < j$. U je rozkladové nadtěleso polynomu $a \in T(\alpha_1)[x]$ a V je rozkladové nadtěleso polynomu $b \in S(\beta_1)[x]$. Podle indukčního předpokladu existuje izomorfismus $g\colon U \to V$, který má požadované vlastnosti a rozšiřuje h, a tím i f. □

19.9 Věta. *Ať je $q \in \mathbb{N}$. Pak konečné komutativní těleso řádu q existuje právě když q je rovno p^n pro některé prvočíslo p a $n \in \mathbb{N}$. Libovolná dvě komutativní tělesa téhož řádu q jsou izomorfní.*

Důkaz. Ať pro $i = 1, 2$ jsou T_i komutativní tělesa řádu q a ať P_i jsou jejich prvotělesa. Podle závěru kapitoly 16 a lemmatu 18.8 existuje prvočíslo p a $n \in \mathbb{N}$ takové, že je $P_i \simeq \mathbb{Z}_p$ a $q = p^n$. Podle 17.8 je T_i rozkladovým nadtělesem polynomu $x^{p^n} - x \in P_i[x]$, takže z 19.8 plyne $T_1 \simeq T_2$ z $P_1 \simeq P_2$. □

Těleso T řádu p^n se často značí $GF(p^n)$, kde GF je zkratka z ‚Galois field'. Lze se dohodnout, že $GF(p)$ je rovno $\mathbb{Z}_p$. Ovšem pro $n > 1$ se už žádný kanonický tvar $GF(p^n)$ nezavádí. Podle 10.10 je multiplikativní grupa $GF(p^n)$ cyklická řádu $p^n - 1$. Proto má $\varphi(p^n - 1)$ generátorů. Každý z těchto generátorů se nazývá *primitivní prvek*.

Rejstřík

symboly a značky
- $\bigoplus$, *5, 30*
- $\leq$, *18*
- $\preccurlyeq$, *18, 19*
- $\sim$, *19, 45*
- $\backsim$, *30*
- $\vee$, $\wedge$, *18*
- $|$, *21*
- $\|$, *21*
- a', *24*
- A/ρ, *7*
- $[a]_\rho$, *7, 12*
- $\frac{a}{b}$, *45*
- AB, Ab, aB, A^{-1}, *8*
- $a \equiv b \bmod N$, *9*
- $\mathrm{Aut}(A)$, *14*
- $\mathrm{Con}(A)$, *40*
- $\deg a$, *4*
- $\mathrm{End}(A)$, *14*
- G/N, *10*
- $GF(p^n)$, *54*
- $|G{:}H|$, *8*
- $\mathrm{char}\, R$, *14*
- $I + J$, *10*
- id_Ω, *4*
- $\ker f$, *12*
- $\mathrm{Ker}\, f$, *13*
- L_a, *8*
- $M_n(T)$, *6, 30*
- $M_n^*(T)$, *30*
- $n \times a$, *13*
- nat_ρ, *12*
- NSD, NSN, *21*
- $n\mathbb{Z}$, *10*
- $\mathbb{P}$, *30*
- $R\big[[x]\big]$, *4*
- $R^\#$, *24*
- $R[x]$, *4*
- R_a, *8*
- RM, *5*
- $R[S^{-1}]$, *45*
- S_Ω, *4, 30*
- sgn, *30*
- Σ, *15*
- $\mathrm{Sub}(A)$, *40*
- T^*, *3, 25*
- $\big(T[x]\big)_a$, *27*
- T_Ω, *4, 30*
- $\mathrm{Tr}\, A$, *31*
- $x - \alpha$, *26*

A
- Abelova grupa, *2*
- akce (působení) na množině, *30*
- algebra se signaturou, *15*
- algebraické rozšíření, *51*
- algebraický prvek, *51*
- algebraicky uzavřené těleso, *26*
- asociativita, *2*
- asociované prvky, *21*
- atom, *18, 44*
- automorfismus, *12*

B
- bilineární zobrazení, *34*
- bimodul, *33*
- binomická věta, *27*
- blok ekvivalence, *7*
- Booleova algebra, *43*

C
- cyklická grupa, *28*
- cyklická podgrupa, *13*

Č
- částečné uspořádání, *18*

D
- dělitel, *21*
- dělitel nuly, *24*
- derivace (formální), *24*
- direktní suma okruhů, *16*
- distributivita, *2*
- dolní závora, *18*
- dosazovací homomorfismus, *26*

E
- endomorfismus, *12*
- eukleidovská funkce, *24*
- eukleidovský obor integrity, *25*
- Eulerova funkce, *28*

F
- faktorgrupa, *10*
- faktorizace operací, *9*
- faktormodul, *10*
- faktorokruh, *10*
- faktorstruktura, *9*
- Frobeniův endomorfismus, *27*

G
- Galois field, *54*
- Gaussův obor integrity, *25*
- generátor cyklické podgrupy, *13*
- generovaná podalgebra, *40*
- generovaný ideál, *25*
- grupa, *2*
- grupový okruh, *6*

H
- Hasseův diagram, *18*
- hlavní ideál, *10*
- homomorfismus, *12*
- horní závora, *18*

Ch
- charakter grupy, *31*
- charakteristika okruhu, *14*

I
ideál, *10*
identické zobrazení, *4*
index podgrupy, *8*
indukovaná operace, *11*
infimum, *18*
injektivní zobrazení, *12*
interval svazu, *40*
invertibilní prvek, *3*
inverzní prvek, *2, 3*
ireducibilní charakter, *32*
ireducibilní prvky, *21*
iterované sčítání, *13*
izomorfismus, *12*
J
jádro, *12*
jádro homomorfismu, *13*
jádro kvaziuspořádání, *19*
jednoduchá grupa, *30*
jednoznačný ireducibilní rozklad, *22*
K
kartézský součin algeber, *16*
Kleinova grupa, *30*
koatom, *18*
komutativita, *2*
komutativní monoid, *21*
komutativní struktura, *2*
kongruence, *9*
konjugované prvky, *30*
kořen polynomu, *26*
kořenové nadtěleso, *50*
kořenový činitel, *26*
Kroneckerův součin matic, *37*
kvaziuspořádání, *19*
kvocient struktury, *9*
L
levá translace, *8*
levé (rozkladové) třídy, *8*
levý ideál okruhu, *10*
levý modul, *2*
lineární uspořádání, *18*
lokalizace, *45*
M
maticový okruh, *6*
maximální ideál, *10*
maximální prvek, *38*
minimální polynom, *51*
minimální prvek, *38*
množina generátorů, *40*
množina generovaná množinou, *38*
modul, *2*
monický polynom, *26*
monoid, *2*
monoid s krácením, *21*
monoidový okruh, *6*
monotonní zobrazení, *19*
multiplikativní grupa, *4*
N
n-ární operace, *7*
násobnost kořenu, *26*
nejmenší prvek, *18*
nejmenší společný násobek, *21*
největší prvek, *18*
největší společný dělitel, *21*
neporovnatelné prvky, *18*
nesoudělné prvky, *21*
neutrální prvek, *2, 3*
nevlastní ideály, *10*
noetherovské kvaziuspořádání, *20*
normální podgrupa, *8*
O
obor hlavních ideálů, *25*
obor integrity, *24*
okruh, *2*
okruh hlavních ideálů, *10*
okruh zlomků, *45*
opačné prvky, *2*
opačné uspořádání, *18*
opačný svaz, *19*
P
p-primární komponenta, *30*
podgrupa, *7*
podílové těleso, *45*
podílový okruh, *45*
podmodul, *7*
podmonoid, *7*
podokruh, *7*
podpologrupa, *7*
podtěleso, *7*
pokrývání prvkem, *18*
pologrupa, *2*
polynom, *4*
porovnatelné prvky, *18*
pravá translace, *8*
pravé (rozkladové) třídy, *8*
pravý ideál okruhu, *10*
pravý modul, *2*
primitivní prvek, *52*
průsek, *18*
prvočinitel, *22*
prvotěleso, *46*
přirozené zobrazení, *12*
působení (akce) na množině, *30*
R
regulární působení, *31*
regulární reprezentace, *31*
reprezentace (maticová), *30*
rozkladové nadtěleso, *50*
rozložení na kořenové činitele, *26*
rozšíření konečného stupně, *51*
Ř
řád grupy, *8*

řád prvku, *13*
S
skalární násobení, *2*
slučitelná ekvivalence, *9*
slučitelné zobrazení, *12*
spojení, *18*
stopa matice, *31*
stupeň, *51*
stupeň polynomu, *4*
supremum, *18*
surjektivní zobrazení, *12*
svaz, *18*
svaz ideálů, *38*
svaz kongruencí, *38*
svaz normálních podgrup, *38*
svaz podalgeber, *38*
svaz podtěles, *38*
svaz s nulou a jedničkou, *19*
symetrická grupa, *4*
T
těleso, *2*
torzní část, *30*
torzní grupa, *30*
torzní prvek, *30*
torzní součin, *33*
transcendentní prvek, *51*
transformační monoid, *4*
transversála, *11*
triviální okruh či monoid, *4*
U
univerzální kongruence, *40*
úplná soustava reprezentantů, *11*
úplný svaz, *19*
uspořádání množiny, *18*
uzávěr množiny, *38*
uzávěrový systém, *38*
uzavřená podmnožina, *7*
V
vektorový podprostor, *7*
vektorový prostor, *2*
věrná reprezentace, *30*
věrné působení na množině, *30*
vlastní dělitel, *21*
vlastní ideály, *10*
Z
zbytkové třídy, *11*
zleva invertibilní prvek, *3*
zleva inverzní prvek, *3*
zleva neutrální prvek, *2*
zprava invertibilní prvek, *3*
zprava inverzní prvek, *3*
zprava neutrální prvek, *2*