Poznámky - Algebra I

Petr Chmel, ZS 2019/20

Definice 1 (n-ární operace)**.** Buď A množina, $n \in \mathbb{N}_0$. Potom zobrazení $f : A^n \to A$ nazveme n-ární operací na A.

Pozorování (O dělení se zbytkem)**.** Buďte $a, b \in \mathbb{Z}, b > 0$. Pak existují jednoznačně určené $q \in \mathbb{Z}, r \in \mathbb{Z}_b$: $a = qb + r$ - $q = a$ div $b, r = a \mathrm{mod} b$.

Definice 2 (Slučitelnost s operacemi, uzavřenost na operaci)**.** Buďte $*, ', c$ po řadě binární, unární a nulární operace na A, $\circ, ^{-1}, d$ téže na B. Pak řekneme, že zobrazení $f : A \to B$ je slučitelné s operacemi $*$ a $\circ$ (resp $', ^{-1}; c, d$), pokud $f(a * b) = f(a) \circ f(b)$, resp. $f(a') = f(a)^{-1}$, resp $f(c) = d$.

Buď $*$ binární operace na A, $\sim$ binární relace na A. Řekneme, že $\sim$ je slučitelná s $*$, pokud $\forall a_1, a_2, b_1, b_2 \in A : a_1 \sim b_1 \wedge a_2 \sim b_2 \Rightarrow (a_1 * a_2) \sim (b_1 * b_2)$.

Poznámka (Rozšířený Euklidův algoritmus)**.** $a_0, a_1 := a, b; x_0, x_1 := 1, 0; y_0, y_1 := 0, 1; i := 1$

While $(a_i > 0) : a_{i+1} := a_{i-1} \mod a_i; q_i := a_{i-1} \mathrm{div} a_i; x_{i+1} := x_{i-1} - x_i q_i, ; y_{i+1} := y_{i-1} - y_i q_i; i := i + 1$

Věta 1 (Základní věta aritmetiky)**.** Každé přirozené číslo větši než jedna lze až na pořadí jednoznačně rozložit na součin prvočísel.

Důkaz. Zaprvé: každé číslo lze zapsat jako součin prvočísel: buď je samo prvočíslo, nebo je složené a použijeme IP.

Jednoznačnost: je-li n prvočíslo, je jednoznačnost zjevná. Nyní nechť platí tvrzení pro všechna $k < n$ a $n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ má dva prvočíselné rozklady. Pak existuje $q_i : p_1 | q_i$, búno $i = 1$, a tedy $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s < n$ a máme spor s IP. ⊞

Důsledek 1 (GCD a lcm)**.** $lcm(a, b) = \frac{a \cdot b}{GCD(a,b)}$ a lcm, GCD jsou určeny jednoznačně.

Věta 2 (Čínská věta o zbytcích)**.** Nechť $n_1, \ldots, n_k$ jsou kladná celá čísla a $n = n_1 \cdot \cdots \cdot n_k$. Potom je zobrazení $H : Z_n \to \prod \mathbb{Z}_{n_i} : H(a) \mapsto (a \mod n_1, \ldots, a \mod n_k)$ sluitelné s operacemi $+$ a $\cdot$. Navíc H je bijekce, právě když $n_1, \ldots, n_k$ jsou po dvou nesoudělná.

Důkaz. Slučitelnost triviální.

„$\Leftarrow$“: Máme-li čísla po dvou nesoudělná, pak stačí ukázat, že H je prosté. Nechť není: pak $a \leq b \in \mathbb{Z}_n$: $H(a) = H(b)$ – tedy $H(b - a) = o$, a tedy $n_i | b - a$ pro $i \in [k]$. Potom z nesoudělnosti po dvou získáváme, že $n | b - a$. Ale $0 \leq b - a \leq n - 1$, a tedy $b = a$.

„$\Rightarrow$“: Nepřímo: nechť existují indexy $i \neq j$ tak, že $c = GCD(n_i, n_j) > 1$. Potom $n/c \in \mathbb{Z}_n \setminus \{0\}$ a $\forall r \in [k] : n_r | \frac{n}{c}$. Pak $H(0) = o = H(\frac{n}{c})$, a tedy H není prosté. ⊞

Definice 3 (Neutrální, invertibilní prvek)**.** Buď A množina, $*$ binární operace na A. Prvek $e \in A$ je neutrální, jestliže $\forall a \in A : a * e = e * a = a$.

Buď $*$ binární operace na A. Řekneme, že $a \in A$ je invertibilní vzhledem k $*$, pokud $\exists b \in A : a * b = b * a = e$, kde e je neutrální prvek.

Definice 4 (Grupoid, pologrupa, monoid, grupa, komutativní)**.**

1. Buď G množina, $\cdot$ binární operace na G. Pak dvojici $(G, \cdot)$, psáno občas $G(\cdot)$ nazveme grupoid.
2. Je-li navíc $\cdot$ asociativní na G, pak $(G, \cdot)$ nazveme pologrupa.
3. Má-li pologrupa neutrální prvek, mluvíme o monoidu.
4. Je-li každý prvek monoidu invertibilní, mluvíme o grupě.
5. Pokud je v $G(\cdot)$ operace $\cdot$ komutativní, přidáme přívlastek komutativní.

Definice 5 (Grupa invertibilních prvků monoidu)**.** Buď $G(\cdot)$ monoid. Pak $G^* := \{g \in G : g \text{ je invertibilní}\}$.

Tvrzení 1 (Vlastnosti)**.** $s, t \in G^* \Rightarrow st \in G^*, s^{-1} \in G, (st)^{-1} = t^{-1}s^{-1}, (s^{-1})^{-1} = s$.

Důkaz. Snadno rozepsáním. ⊞

Příklad 1 (Symetrická grupa, zobecněná lineární grupa)**.** Symetrická grupa S_n je grupa permutací na n prvcích.

Zobecněná lineární grupa je $GL_n(T)$ - grupa všech regulárních matic $n \times n$ na tělesem T.

Definice 6 (Podgrupa, normální podgrupa)**.** Pro grupu $G(\cdot)$ její podgrupou rozumíme podmnožinu H takovou, že $1 \in H, \forall a, b \in H : a \cdot b \in H$.

Podgrupa je normální, jestliže $\forall g \in G, \forall h \in H : g^{-1}hg \in H$.

Definice 7 (Relace rmod, lmod)**.** Pro H podgrupu G definujeme relace rmod H, lmod H tak, že: $(a, b) \in \text{rmod} \Leftrightarrow a \cdot b^{-1} \in H, (a, b) \in \text{lmod} \Leftrightarrow a^{-1} \cdot b \in H$

Tvrzení 2 (4.1: o vlastnostech rmod, lmod atd.)**.** Buď $G(\cdot)$ grupa, H její podgrupa, H_i podgrupy G pro $i \in I \neq \emptyset$. Pak

1. $\bigcap_{i \in I} H_i$ je podgrupa G, jsou li navíc všechny podgrupy normální, pak ji jejich průnik je normální
2. rmod, lmod jsou ekvivalence na G
3. rmod(H)=lmod(H)$\Leftrightarrow$ H je normální podgrupa G.
4. je-li H normální podgrupa, pak rmod(H) je slučitelná s $\cdot$

Důkaz. Rozepsat. ⊞

Definice 8 (Homomorfismus, monomorfismus, epimorfismus, izomorfismus)**.** Mějme $G(*), H(\cdot)$ grupy. $\varphi : G \to H$ zobrazení. Řekneme, že φ je homomorfismus, pokud je slučitelné s $*$ a $\cdot$.

Navíc, je-li prosté, mluvíme o monomorfismu, je-li na, mluvíme o epimorfismu a jedná-li se o bijekci, mluvíme o izomorfismu.

Definice 9 (Jádro zobrazení)**.** Jádrem zobrazení $\varphi : G \to H$ nazveme relaci $\ker\varphi = \{(a, b) \in G^2 : \varphi(a) = \varphi(b)\}$ a množinu $\text{Ker}\varphi = \{g \in G : \varphi(g) = 1_H\}$.

Tvrzení 3 (O grupách a homomorfismech)**.** Buďte G_1, G_2, G_3 grupy, $\varphi : G_1 \to G_2, \psi : G_2 \to G_3$ homomorfismy. Pak platí

1. $\varphi(1) = 1, \varphi(a^{-1}) = \varphi(a)^{-1} \forall a \in G$
2. $\psi \circ \varphi$ je homomorfismus
3. je-li φ bijekce, pak $\varphi^{-1} : G_2 \to G_1$ je homomorfismus
4. $H \leq G_2 \Rightarrow \varphi^{-1}(H) \leq G_1, \psi(H) \leq G_3$, navíc je-li H normální, pak i ostatní podgrupy jsou normální
5. Kerφ je normální podgrupou G_1 a kerφ =rmod=lmod.
6. φ je monomorfismus právě když Ker$\varphi = \{1\}$, což nastane právě když $\ker\varphi = \text{id}_{G_1}$.

Důkaz. Rozepisovat ⊞

Tvrzení 4 (Cayleyho věta (reprezentace))**.** Každá grupa je izomorfní podgrupě vhodné symetrické grupy.

Důkaz. Pro $G(\cdot)$ chci $\varphi(g) \mapsto L_g$, kde $L_g : G \to G : h \mapsto g \cdot h$. ⊞

Definice 10 (Rozkladové třídy)**.** Buď G grupa, H její podgrupa. Pak pro $g \in G$ je gH levá rozkladová třída a Hg pravá rozkladová třída.

Tvrzení 5 (O rozkladových třídách rmod, lmod)**.** Ať $G(\cdot)$ je grupa, $H \leq G$. Pak platí

1. $(a, b) \in \text{rmod}H \Leftrightarrow (a^{-1}, b^{-1}) \in \text{lmod}H \forall a, b \in G$
2. $|G/\text{lmod}H| = |G/\text{rmod}H|$

3. $[a]_{\text{lmod}} = aH, [a]_{rmod} = Ha \forall a \in G$

4. $|[a]_{\text{lmod}}| = |[a]_{\text{rmod}}| = |H|$

Důkaz. 1 rozepsat, 2 plyne z 1 za pomoci $[a]_{rmod} \mapsto [a]_{lmod}$ bijekcí mezi $G/rmod$ a $G/lmod$.

3 plyne z rozepsání třídy ekvivalence. 4 plyne z 3 tak, že nalezneme bijekci H a aH, např. $L_a : h \mapsto ah$ (levá translace). ⊞

Definice 11 (Řád grupy, index podgrupy)**.** Buďte $H \leq G$ grupa s podgrupou. Řádem grupy G myslíme $|G|$. Indexem podgrupy H v grupě G myslíme $[G : H] := |G/\text{lmod}H| = |G/\text{rmod}H|$.

Věta 3 (Lagrangeova)**.** Buď G grupa a H její podgrupa. Pak $|G| = |H| \cdot [G : H]$.

Důkaz. rmod H je ekvivalence na G, tedy $|G| = |\bigsqcup_{A \in G/rmod\, H} A| = \sum_{A \in G/rmod\, H} |A| = \sum_{A \in G/rmod\, H} |H| = |G| \cdot [G : H]$. ⊞

Důsledek 2. Řád podgrupy dělí řád celé grupy.

Definice 12 (Generovaná podgrupa grupy, cyklická grupa, řád prvku)**.** Buď G grupa, $X \subseteq G$. Pak $\langle X \rangle_G := \bigcup_{X \subseteq H \leq G} H$ nazýváme podgrupou grupy G generovanou množinou X.

Grupa G je cyklická, existuje-li $g \in G : \langle g \rangle = G$.

Řád prvku $g \in G$ je řád $\langle g \rangle$.

Tvrzení 6 ($\mathbb{Z}_n$ a generátory)**.** a je generátor $\mathbb{Z}_n$ právě když $GCD(a, n) = 1$.

Důkaz. Hlavní idea: neutrální prvek je generovatelný.

„⇒“: $\exists t \in \mathbb{Z}_n : 1 = tn$ v $\mathbb{Z}_n$, a tedy $1 \equiv ba \mod n$, a tedy $1 = ba + cn$ pro nějaké $c \in \mathbb{Z}$ - NSD dělí sčítance, tedy $NSD(a, n) = 1$.

„⇐“: máme Bezoutovy koeficienty: $1 = xa + yn$ a tedy $1 \equiv a(x \mod n) \Rightarrow 1 \in \langle a \rangle \Rightarrow \langle a \rangle = \mathbb{Z}_n$. ⊞

Tvrzení 7 (Alternativní definice řádu)**.** Řád prvku $g \in G$ je nejmenší $n \in \mathbb{N}$ takové, že $g^n = 1$ pokud existuje. Jinak $\text{ord}(n) = \infty$.

Navíc, řád prvku vždy dělí libovolný takový exponent (je-li konečný).

Důkaz. Ať $g^l = 1$, mějme $n \in \mathbb{N}$ - $q := n \text{ div } l, r := n \bmod l$. Pak $g^n = g^{qk+r} = g^r \Rightarrow \langle g \rangle = \{g^r : r \in \mathbb{Z}_k\}$. Minimalita už pak vše zaručuje. ⊞

Věta 4 (Každá cyklická grupa je izomorfní $\mathbb{Z}$ nebo $\mathbb{Z}_n$)**.** Buď G cyklická grupa. Je-li G nekonečná, pak $G \simeq \mathbb{Z}(+)$, jinak $G \simeq \mathbb{Z}_{|G|}(+)$.

Důkaz. G nekonečná: máme homomorfismus $\varphi : \mathbb{Z} \to G : n \mapsto g^n$, kde $\langle g \rangle = G$. Dále je prosté z alternativní definice řádu, na je zjevně.

$|G| = n$: $\varphi : \mathbb{Z}_n \to G : n \mapsto g^n$, kde $\langle g \rangle = G$ Na je zjevně z generování n, stačí ověřit homomorfismus: $g^{x+y} = g^x \cdot g^y = \varphi(x) \cdot \varphi(y) = \varphi(x + y) = g^{x+y}$. ⊞

Důsledek 3. Podgrupy cyklických grup jsou cyklické.

Důkaz. Podgrupy $\mathbb{Z}$ jsou tvaru $n\mathbb{Z}$, a tedy cyklické. Uvažme $F_n : \mathbb{Z} \to \mathbb{Z}_n : x \mapsto x \mod n$. Máme grupový epimorfismus – je-li $H \leq \mathbb{Z}_n$, je $F_n^{-1}(H) \leq \mathbb{Z}$, a tedy je cyklická z výše zmíněného. ⊞

Tvrzení 8 (Podgrupy $\mathbb{Z}_n(+)$ podrobněji)**.** Buďte $k, n \in \mathbb{N}, k > 1, k|n$. Pak $\langle \frac{n}{k} \rangle_{\mathbb{Z}(+)}$ je jediná podgrupa $\mathbb{Z}_n$ řádu k. Navíc $\forall a \in \mathbb{Z}_n \setminus \{0\}$ platí, že $\langle a \rangle = \langle \frac{n}{k} \rangle \Leftrightarrow GCD(a, n) = \frac{n}{k}$.

Důkaz. Ať $d|n, d < n$. Pak $\{0, d, 2d, \ldots, (\frac{n}{d} - 1)d\} \leq \mathbb{Z}_n$ řádu n/d - máme existenci. Jednoznačnost: Ať $a \in \mathbb{Z}_n \setminus \{0\}, d := NSD(a, n)$. Ukážeme $\langle a \rangle = \langle d \rangle$. Jelikož $d|a$, máme $a \in \langle d \rangle \Rightarrow \langle a \rangle \subseteq \langle d \rangle$. Dále z Bezoutových koeficientů dostaneme $x, y \in \mathbb{Z} : d = xa + yn \Rightarrow x \in \langle a \rangle \Rightarrow \langle d \rangle \subseteq \langle a \rangle$. ⊞

Definice 13 (Eulerova funkce)**.** Eulerovou funkcí φ nazýváme zobrazení $\varphi : \mathbb{N} \to \mathbb{N} : \varphi(n) := |\mathbb{Z}_n^*(\cdot)| = |\{a \in \mathbb{Z}_n : GCD(a, n) = 1\}|$.

Věta 5 (Výpočet Eulerovy funkce)**.** Nechť $p_1 < p_2 < \ldots < p_k$ jsou prvočísla, $r_1, \ldots, r_k \in \mathbb{N}$.
Pak $\varphi(\prod p_i^{r_i}) = \prod (p_i - 1) \cdot p_i^{r_i - 1}$.

Důkaz. Pro $k = 1$ máme $p_1^{r_1 - 1}$ násobků p_1, a tedy $(p_1 - 1)p_1^{r_1 - 1}$ nenásobků (tj. nesoudělných čísel).

Pro $k > 1$ máme z Čínské věty o zbytcích bijekci $H : \mathbb{Z}_n \to \prod \mathbb{Z}_{p_i^{r_i}}$. Ihned z definice vidíme, že $(\prod \mathbb{Z}_{p_i^{r_i}})^*(\cdot) = \prod \mathbb{Z}^*_{p_i^{r_i}}(\cdot)$. Pro $a \in \mathbb{Z}_n : a \in \mathbb{Z}_n^* \Leftrightarrow \exists b \in \mathbb{Z}_n : ab = 1$ v $\mathbb{Z}_p \Leftrightarrow \exists c \in \prod \mathbb{Z}_{p_i^{r_i}} : H(a) \cdot c = H(1) = 1 \Leftrightarrow H(a) \in (\prod \mathbb{Z}_{p_i^{r_i}})^*$, tedy i po restrikci máme bijekci, a tedy $\varphi(n) = |\mathbb{Z}_n^*| = |\prod \mathbb{Z}^*_{p_i^{r_i}}| = \prod |\mathbb{Z}^*_{p_i^{r_i}}| = \prod (p_i - 1) p_I^{r_i - 1}$. ⊞

Věta 6 (Vnitřní charakterizace konečných cyklických grup)**.** Ať G je konečná grupa, $|G| = n$. Pak G je cyklická $\Leftrightarrow \forall d \in \mathbb{N} : G$ obsahuje nejvýše jednu d-prvkovou podgrupu.

Důkaz. „$\Rightarrow$“: Je cyklická, takže je izomorfní $\mathbb{Z}_n$, a v $\mathbb{Z}_n$ toto platí.

„$\Leftarrow$“: obměnou: Zadefinujeme $p(d) = |\{g \in G : \mathrm{ord}_G(g) = d\}|$. Pak $n = |G| = \sum_{d|n} p(d)$ z Lagrangeovy věty. Ať G není cyklická. To nastane, právě když $p(n) = 0$. Také ovšem platí, že $\varphi(n) > 0$. Neboť $\sum_{d|n} p(d) = \sum_{d|n} \varphi(d)$, nutně existuje $1 < d < n$ tak, že $\varphi(d) < p(d) \geq 2$. Pro $g \in G$ řádu d. Pak v $\langle g \rangle_G$ je právě $\varphi(d)$ prvků řádu d. Máme-li tedy $h \in G \setminus \langle g \rangle_G$ řádu d, máme dvě různé podgrupy řádu d. ⊞

Tvrzení 9 (Prvek na velikost množiny)**.** Buď G konečná grupa, $g \in G$. Pak $g^{|G|} = 1$.

Důkaz. $n = \mathrm{ord}_G(g)$. Z Lagrangeovy věty $n||G|$. Pak $g^{|G|} = g^{n^{\frac{|G|}{n}}} = 1$. ⊞

Věta 7 (Eulerova)**.** Ať $a, n \in \mathbb{Z}, n > 1, GCD(a, n) = 1$. Potom $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$.

Důkaz. Bez újmy na obecnosti $a \in \mathbb{Z}_n$. Neboť $\mathrm{NSD}(a, n) = 1$, máme $a \in \mathbb{Z}_n^*(\cdot)$. Z předchozího tvrzení máme, že $a^{\varphi(n)} = a^{|\mathbb{Z}_n^*(\cdot)|} = 1$ v $\mathbb{Z}_n^*$. ⊞

Tvrzení 10 (Cosi pro RSA)**.** Buďte p, q dvě lichá prvočísla, $m = LCM(p - 1, q - 1)$. Pak $\forall a \in \mathbb{Z}_{pq}, u \in \mathbb{N} : a^{mu+1} \mod pq = 0$.

Tvrzení 11 (Vsuvka: něco jako základní věta algebry)**.** Buď T komutativní těleso. Pak $a \in T$ je kořen polynomu f právě když $(x - a)|f$ v $T[x](\cdot)$.

Důkaz. „$\Leftarrow$“: zjevně.

„$\Rightarrow$“: $f(a) = 0$. Vydělíme f polynomem $(x - a)$ se zbytkem. Máme $f = q(x - a) + r$, $\deg(r) < 1$. Dosadíme: $0 = f(a) = q(a) \cdot 0 + r(a) \Rightarrow r = 0$. ⊞

Věta 8 (Cykličnost konečné podgrupy invertibilních prvků tělesa)**.** Ať T je komutativní těleso, G konečná podgrupa grupy $T^*(\cdot)$. Pak G je cyklická.

Důkaz. Sporem: ať není cyklická. Pak existuje k takové, že G má dvě různé podgrupy řádu k. To ovšem znamená, že existuje více než d prvků g takových, že $g^d = 1$ v $GG \leq T^*$, což je ovšem spor s větou o počtu kořenů. ⊞

Důsledek 4. $\mathbb{Z}_p^*$ je cyklická pro p prvočíslo.

Definice 14 (Typ, algebra typu, univerzum, množina uzavřená na operaci, poduniverzum)**.** Buď I množina. Potom zobrazení $\Omega : I \to \mathbb{N}_0$ nazveme typem (na I), někdy signatura.

Dále řekneme, že $A(\alpha_i : i \in I)$ je algebra typu Ω, pokud $A \neq \emptyset, \forall i \in I : \alpha_i : A^{\Omega(i)} \to A$. Množinu A nazýváme univerzum (nosič) algebry.

Buď $B \subset A$ a α je n-ární operace na A. Řekneme, že B je uzavřená na α, pokud $\alpha(a_1, \ldots, a_n) \in B \forall a_1, \ldots, a_n \in B$.

Je-li $A(\alpha_i : i \in T)$ algebra, $B \subset A$, pak B nazveme poduniverzem univerza A, pokud je B uzavřené na všechny operace $\alpha_i : i \in I$. Je-li navíc $B \neq \emptyset$, říkáme, že B je podalgebra algebry B.

Definice 15 (Slučitelnost s operacemi, homomorfismus algeber)**.** Buďte α, β n-ární operace na A, B, buď $f : A \to B$ zobrazení. Řekneme, že f je slučitelné s α a β, jestliže $\forall a_1, \ldots, a_n \in A : f(\alpha(a_1, \ldots, a_n)) = \beta(f(a_1), \ldots, f(a_n))$.

Zobrazení $f : A \to B$, kde $\mathcal{A} = A(\alpha_i, i \in I), \mathcal{B} = B(\beta_i, i \in I)$ jsou algebry téhož typu se nazývá homomorfismus algeber $\mathcal{A}$ a $\mathcal{B}$, psáno $f : \mathcal{A} \to \mathcal{B}$, pokud je f slučitelné s α_i a β_i $\forall i \in I$.

Definice 16 (Slučitelná ekvivalence, kongruence)**.** Buď ρ ekvivalence nad A, α n-ární operace nad A. Pak ρ je slučitelné s α, jestliže $\forall a_1, \ldots, a_n, b_1, \ldots, b_n$ takové, že $(a_i, b_i) \in \rho \forall i \in [n]$ platí, že $(\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \rho$.

Je-li $\mathcal{A} = A(\alpha_i, i \in I)$ algebra typu Ω, ρ ekvivalence nad A, pak ρ nazveme kongruencí na α, je-li ρ slučitelné s $\alpha_i \forall i \in I$.

Definice 17 (Jádro zobrazení)**.** Pro libovolné zobrazení $f : A \to B$ (opět) definujeme relaci jádra zobrazení jako $\ker(f) = \{(a, b) \in A^2 : f(a) = f(b)\}$.

Tvrzení 12 (Algebry a homomorfismy)**.** Ať $\mathcal{A}_1 = A_1(\alpha_i, i \in I), \mathcal{A}_2 = A_2(\alpha_i, i \in I), \mathcal{A}_3 = A_3(\alpha_i, i \in I)$ jsou algebry typu Ω a $f : \mathcal{A}_1 \to \mathcal{A}_2, g : \mathcal{A}_2 \to \mathcal{A}_3$ jsou homomorfismy, $\mathcal{B}$ je podalgebra $\mathcal{A}_2$. Pak

1. $g \circ f$ je homomorfismus
2. je-li f izomorfismus, pak f^{-1} je rovněž izomorfismus
3. $g(\mathcal{B})$ je podalgebra $\mathcal{A}_3$, $f^{-1}(\mathcal{B})$ je podalgebra $\mathcal{A}_1$
4. $\ker(f)$ je kongruence na $\mathcal{A}_1$.

Důkaz. Rozepsat ⊞

Tvrzení 13 (Algebra a podalgebra)**.** Nechť $\mathcal{A} = A(\alpha_i, i \in I)$ je algebra typu Ω, $A_j, j \in J$ jsou podalgebry, $\rho_k, k \in K$ koungruence na $\mathcal{A}$.

1. $\bigcap_{j \in J} A_j$ je podalgebra, pokud $\bigcap_{j \in J} A_j \neq \emptyset$
2. $\bigcap_{k \in K} \rho_k$ je opět kongruence na $\mathcal{A}$.

Důkaz. Rozepsat ⊞

Definice 18 (Faktorizace, kanonická projekce, faktoralgebra)**.** Buď A množina, ρ ekvivalence na A. Pak rozkladem (faktorizací) podle ρ myslíme $A/\rho = \{[a]_\rho : a \in A\}$, kde $[a]_\rho$ je třída ekvivalence. Zobrazení $\pi_\rho : a \mapsto [a]_\rho$ nazveme přirozenou (kanonickou) projekcí.

Buď A množina, α n-ární operace na A, ρ ekvivalence na A sluičtelná s A. Pak definujeme n-ární operaci α na A/ρ vztahem $\alpha([a_1], \ldots, [a_n]) = [\alpha(a_1, \ldots, a_n)]$.

Tvrzení 14 (Kongruence a faktorizace podle kongruence dává smysl)**.** Je-li ρ kongruence ma algebře $\mathcal{A} = A(\alpha_i, i \in I)$, pak je definice operací v algebře $\mathcal{A}/\rho$ korektní a zobrazení $\pi_\rho : a \mapsto [a]_\rho$ je epimorfismus algeber.

Důkaz. Rozepsat ⊞

Definice 19 (Faktorkongruence)**.** Ať $\rho \subset \sigma$ jsou dvě ekvivalence na A. Pak σ/ρ definovaná vztahem $([a]_\rho, [b]_\rho) \in \sigma/\rho \overset{\text{def}}{\Leftrightarrow} (a, b) \in \sigma$ je ekvivalence na A/ρ.

Tvrzení 15 (O faktorkongruenci)**.** Buď ρ kongruence na $\mathcal{A} = A(\alpha_i : i \in I)$.

1. Je-li σ kongruence na $\mathcal{A}$, že $\rho \subseteq \sigma$, pak je σ/ρ dobře definovaná kongruence.
2. Je-li μ kongruence na A/ρ, pak existuje právě jedna kongruence σ na $\mathcal{A}$ taková, že $\rho \subset \sigma$ a $\sigma/\rho = \mu$.

Důkaz. 1 rozepsat

2: Zadefinujeme $\sigma : (a, b) \in \sigma \overset{\text{def}}{\Leftrightarrow} ([a]_\rho, [b]_\rho)$. Ověříme, že se jedná o kongruenci, $(a, b) \in \rho \Rightarrow ([a], [b]) \in \mu \Rightarrow (a, b) \in \sigma$. ⊞

Věta 9 (O homomorfismu, 1. věta o izomorfismu)**.** Ať $f : \mathcal{A} \to \mathcal{B}$ je homomorfismus algeber, kde $\mathcal{A}, \mathcal{B}$ jsou algebry stejného typu.

1. Je-li ρ kongruence na $\mathcal{A}$, pak existuje $g : \mathcal{A}/\rho \to \mathcal{B}$ takové, že $g \circ \pi_\rho = g$ právě tehdy, když $\rho \subseteq \ker(f)$. Navíc, pokud g existuje, pak g je izomorfismus právě když f je na $\mathcal{B}$ a $\ker(f) = \rho$.

2. Je-li f epimorfismus, pak $B \simeq A/\ker(f)$.

Důkaz. 1: $\Rightarrow$: $\ker\pi_\rho = \rho$ z definice - ker $(g \circ \pi_\rho) = \ker(f)$
$\Leftarrow$: položme $g([a]_\rho) := f(a)$: $[a]_\rho = [a']_\rho \Leftrightarrow (a, a') \in \rho \subseteq \ker(f) \Rightarrow f(a) = f(a')$. Z definice ihned $g \circ \pi_\rho = f$. Navíc, f je na, právě když g je na.
2: Aplikujeme 1 pro $\rho = \ker(f)$. ⊞

Věta 10 (2. věta o izomorfismu)**.** Nechť $\rho \subseteq \sigma$ jsou dvě kongruence na $\mathcal{A}$. Pak $\mathcal{A}/\sigma \simeq (\mathcal{A}/\rho)/(\sigma/\rho)$.

Důkaz. $\pi_\sigma : \mathcal{A} \to \mathcal{A}/\sigma, \pi_\rho : \mathcal{A} \to \mathcal{A}/\rho$ epimorfismy. Položíme $f : \pi_\sigma$ a z věty o homomorfismu dostanu epimorfismus $g : \mathcal{A}/\rho \to A/\sigma$. Dále na g použiji první větu o isomorfismu, tedy $\mathcal{A}/\sigma \simeq \mathcal{A}/\rho/\ker(g) = \mathcal{A}/\rho/\rho/\sigma$. ⊞

Věta 11 (Kongruence a normální podgrupy)**.** Ať G je grupa, ρ binární relace na G. Pak následující tvrzení jsou ekvivalentní:

1. ρ je kongruence algebry $G(\cdot)$

2. ρ je kongruence algebry $G(\cdot, ^{-1}, 1)$

3. $H = [1]_\rho$ je normální podgrupa a $\rho = \mathrm{rmod}\, H$.

Důkaz. $1 \Rightarrow 2$: ověřování
$2 \Rightarrow 3$: a) $H := [1]_\rho$ je normální podgrupa $G : \forall a, b \in [1]_\rho : (1, a), (1, b) \in \rho \Rightarrow (1, ab) \in \rho$. $\forall g \in G, \forall a \in [1]_\rho : (g1g^{-1}, gag^{-1}) = (1, gag^{-1}) \in \rho \Rightarrow gag^{-1} \in [1]_\rho$.
b) $(a, b) \in \rho \Leftrightarrow (a, b) \in \mathrm{lmod}\, H : (a, b) \in \rho \Leftrightarrow (a^{-1}a, a^{-1}b) = (1, a^{-1}, b) \in \rho \Leftrightarrow a^{-1}b \in H \Leftrightarrow (a, b) \in \mathrm{lmod}\, H$.
$3 \Rightarrow 1 : \rho = \mathrm{rmod}\, H$, H normální podgrupa $G \Rightarrow \rho$ je ekvivalence slučitelná s $\cdot$. ⊞

Důsledek 5 (Bijekce mezi kongruencemi a normálními podgrupami)**.** Existuje vzájemně jednoznačná korespondence mezi normálními podgrupami grupy $G(\cdot)$ a jejími kongruencemi.

Definice 20 (Okruh, komutativní, obor, těleso)**.** Okruhem rozumíme algebru $R(+, -, 0, \cdot, 1)$, kde $+, \cdot$ jsou binární, $-$ je unární a $0, 1$ jsou konstanty splňující následující:

- $R(+)$ je komutativní grupa s neutrálním prvkem 0 a inverzním prvkem $-a + a = 0$.
- $R(\cdot)$ je monoid s neutrálním prvkem 1
- distributivita: $\forall a, b, c \in R : a(b + c) = ab + ac, (a + b)c = ac + bc$

Dále řekneme, že okruh je

- komutativní, pokud $R(\cdot)$ je komutativní monoid
- obor, pokud $0 \neq 1$ a pro každé $a, b \in R : a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$
- těleso, pokud $\forall a \neq O : a \in R \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1$ a současně $0 \neq 1$
- komutativní těleso, pokud se jedná o komutativní okruh a těleso zároveň

Tvrzení 16 (Vlastnosti okruhu)**.** Buď $R(+, -, 0, \cdot, 1)$ okruh. Pak $\forall a, b \in R$ platí

1. $0 \cdot a = a \cdot 0 = 0$
2. $(-a)b = a(-b) = -(ab)$

3. $0 \neq 1 \Leftrightarrow |R| > 1$.

Důkaz. Rozepsat ⊞

Definice 21 (Levý, pravý, oboustranný ideál)**.** Ať $R(+,-,0,\cdot,1)$ je okruh, $I \subseteq R$. I nazveme pravým ideálem v R, pokud I je podgrupa $R(+)$ a $\forall r \in R, \forall a \in I : a \cdot r \in I$.

I nazveme levým ideálem v R, pokud I je podgrupa $R(+)$ a $\forall r \in R, \forall a \in I : r \cdot a \in I$.

I nazveme ideálem v R, pokud je zároveň levým i pravým ideálem.

Definice 22 (Jednoduchý ideál)**.** Okruh, který má pouze nevlastní oboustranné ideály a splňuje $0 \neq 1$ nazveme jednoduchým.

Tvrzení 17 (O okruzích a ideálech)**.** Buď $R(+,-,0,\cdot,1)$ okruh, I levý nebo pravý ideál v R. Potom $I = R \Leftrightarrow I$ obsahuje nějaký invertibilní prvek okruhu R (tj. invertibilní prvek monoidu $R(\cdot)$).

Důkaz. $\Rightarrow$: $1 \in R$

$\Leftarrow$: I obsahuje nějaký invertibilní prvek a: $aa^{-1} = 1 \in I \Rightarrow \forall r \in R : 1r = r \in I$. ⊞

Věta 12 (Tělesa a vlastní jednostranné ideály)**.** Buď $R(+-,0\cdot,1)$ okruh, $0 \neq 1$. Pak následující tvrzení jsou ekvivalentní:

1. R je těleso
2. R neobsahuje vlastní pravé ideály (tj. jediné pravé ideály jsou $\{0\}, R$)
3. R neobsahuje vlastní levé ideály

Důkaz. $1 \Rightarrow 2 \wedge 3$: $0 \neq a \in R \Rightarrow a$ je invertibilní, tedy $aR = R, Ra = R$. Tedy $I = \{0\} \vee I = R$.

$2 \Rightarrow 1$: $0 \neq a \in R$ libovolné. Z 2 plyne, že $aR = R \Rightarrow \exists b \in R : ab = 1 \Rightarrow b \neq 0 \rightarrow bR = R \Rightarrow \exists c \in R : bc = 1 \Rightarrow a = c$ z jednoznačnosti inverzu, tedy b je oboustranný invers k a a naopak a R je těleso. ⊞

Tvrzení 18 (Okruhy a rmod ideálu, jádro homomorfismu)**.** Buďte $R(+,-,0,\cdot,1), S(+,-,0,\cdot,1)$ okdruhy, I ideál okruhu R, $\varphi : \mathcal{R} \to \mathcal{S}$ homomorfismus. Pak

1. rmod I je kongruence algebry $\mathcal{R}$. Označíme-li $R/I := R/\text{rmod } I$, pak je $R/I(+,-,[0],\cdot,[1])$ a přirozená projekce je epimorfismus.
2. Ker φ je ideál okruhu $\mathcal{R}$.

Důsledkem je, že ideály vzájemně jednoznačně odpovídají jádrům homomorfismů.

Důkaz. 1)Víme, že rmod I je kongruence algebry $R(+)$. Stačí ukázat slučitelnost s násobením: $(a,b),(c,d) \in$ rmod I, tedy $a-b, c-d \in I$, také z ideality $(a-b)c, b(c-d) \in I$, načež $ac - bd \in I \Rightarrow (ac, bd) \in$ rmod I.

2) Víme, že Kerφ je (normální) podgrupa $R(+)$. Buď $r \in R, s \in$ Kerφ. $\varphi(rs) = \varphi(r)\varphi(s) = \varphi(r) \cdot 0 = 0 \Rightarrow rs \in$ Ker, sr obdobně. Tedy Ker φ je oboustranný ideál. ⊞

Definice 23 (Maximální ideál)**.** Ať R je komutativní okruh, I ideál v R. Řekneme, že I je maximální ideál v R, pokud $I \neq R$ a $\forall$ ideál J v R platí, že $I \subset J \subseteq R \Rightarrow J \subseteq R$.

Poznámka. Ze Zornova lemmatu plyne, že každý ideál lze rozšířit do maximálního ideálu.

Věta 13 (Faktorokruh je těleso právě když je faktorizováno maximálním ideálem)**.** Ať $R(+,-,0,\cdot,1)$ je komutativní okruh, I ideál v R. Pak R/I je těleso, právě když I je maximální ideál v R.

Důkaz. Pomocné lemma: přiřazení $J \mapsto \pi(J), \overline{J} \to \pi^{-1}(\overline{J})$ jsou vzájemně iverzní bijekce mezi množinou $\mathcal{I}_I^R := \{J : J \text{ ideál v } R, I \subseteq J\}$ a $\mathcal{I}_\emptyset^{R/I} = \{\text{všechny ideály v } R/I\}$.

Důkaz pomocného lemmatu: Z grup víme, že $\pi(J)$ je podgrupa $R/I(+)$ a $\pi^{-1}(\overline{J})$ je podgrupa $R(+)$, dokonce jsou ideály, což se snadno ověří. Nyní ať $j \in \pi^{-1}(\overline{J}), r \in R, \pi(jr) = \pi(j)\pi(r) \in \overline{J} \Rightarrow jr \in \pi^{-1}(\overline{J})$ atd. Zbytek plyne z rozepsání $\pi^{-1}\pi(J) = J, \pi\pi^{-1}(\overline{J}) = \overline{J}$.

Nyní I je maximální ideál, což je z lemmatu právě když R/I nemá žádné vlastní ideály, což nastane právě když R/I je těleso. ⊞

Definice 24 (Polynom, okruh polynomů nad okruhem)**.** Buď r okruh. Pak $R[x] := \{p : \mathbb{N}_0 \to R : |\{n \in \mathbb{N}_0 : p(n) \neq 0\}| < \infty\}$. Prvek $p \in R[x]$ budeme psát jako $\sum p(n)x^n$. Na $R[x]$ pak definujeme $+, \cdot$, unární $-$, nulární $0, 1$: $p + q = \sum(p_n + q_n)x^n, -p = \sum(-p_n)x^n, 0 = \sum 0x^n, 1 = 1x^0 + \sum 0x^n$

Tvrzení 19 (Polynomy okruhu a jejich vlastnosti)**.** Ať $R(+, -, 0, \cdot, 1)$ je okruh, $p, q \in R[x]$

1. $R[x](+, -, 0, \cdot, 1)$ je okruh a množina $\{sx^0, s \in R\} \subseteq R[x]$ je jako podokruh izomorfní okruhu R.

2. $\deg(p + q) \leq \max(\deg p, \deg q)$, je-li $p, q \neq 0$, pak $\deg(pq) \leq \deg(p) + \deg(q)$. Pokud je R navíc obor, pak $\deg(pq) = \deg(p) + \deg(q)$

3. $R[x]$ je obor, právě když R je obor

4. $R[x]$ je komutativní okruh, právě když R je komutativní okruh

Důkaz. Rozepsat ⊞

Věta 14 (O dělení se zbytkem)**.** Buď $R(+, -, 0, \cdot, 1)$ komutativní obor, $a, b \in R[x]$. $b = \sum b_n x^n$. Ať $m = \deg b \geq 0$, b_m buď invertibilní v $R(\cdot)$. Pak existují jednoznačně určené polynomy $q, r \in R[x]$, že $a = qb + r$, kde $\deg r < \deg b$.

Důkaz. Existence: středoškolský algoritmus dělení polynomů se zbytkem.

Jednoznačnost: ať existují $q, r, q', r' : a = qb + r = q'b + r'$. Pak $b(q - q') = r' - r$. Víme, že $\deg(r' - r') < \deg b$, a neboť máme komutativní obor, máme $q - q' = 0 \Rightarrow r' - r = 0$. ⊞

Důsledek 6 (Komutativní těleso a ideály okruhu polynomů)**.** Ať $T(+, -, 0, \cdot, 1)$ je komutativní těleso. Pak je každý ideál okruhu $T[x](+, -, 0, \cdot, 1)$ hlavní (tj. generovaný jedním prvkem, tvaru aT nebo Ta).

Definice 25 (Dělení, asociace, ireducibilita v okruhu)**.** Buď R komutativní okdruh, $a, b \in R$. Pak řekneme, že a dělí b, pokud existuje $c \in R : ac = b$.

Dále řekneme, že a je asociováno s b $(a||b)$, pokud $(a|b \wedge b|a)$.

Pokud $a \in R$ není 0 ani invertibilní, nazveme a ireducibilní v R, pokud $\forall b, c \in R : a = b \cdot c \Rightarrow (a|b \vee a|c)$

Tvrzení 20 (Dělení a komutativní okruh)**.** Buď R komutativní okruh, $a, b \in R$. Pak $a|b \Leftrightarrow b \in aR \Leftrightarrow bR \subseteq aR$.

Důkaz. Plyne ihned z definice ⊞

Tvrzení 21 (Komutativní těleso a jeho maximální ideál)**.** Buď T komutativní těleso, I ideál v $T[x]$. Pak I je maximální, právě když existuje ireducibilní $f \in T[x]$ tak, že $I = fT[x]$.

Důkaz. Už víme, že každý ideál okruhu polynomů nad komutativním tělesem je hlavní, tedy existuje $f \in T[x] : I = fT[x]$ a všechny ideály mají tvar $gT[x]$ pro nějaké $g \in T[x]$. Platí $fT[x] \subset gT[x] \subset T[x] \Leftrightarrow g|f \wedge f \not/ |g \wedge g$ není invertibilní, což nastane právě když $0 < \deg g < \deg f \wedge g|f \Leftrightarrow f$ není ireducibilní. ⊞

Důsledek 7. $f \in T[x]$ - $T[x]/fT[x]$ je komutativní těleso, právě když f je ireducibilní v $T[x]$.

Fakt 1. Pro každé p prvočíslo a $n \in \mathbb{N}$ existuje ireducibilní polynom $u \in \mathbb{Z}_p[x]$ stupně n. Navíc, v $\mathbb{Z}_p[x]$ platí $u|x^{p^n} - x$.

Věta 15 (Konstrukce konečných těles)**.**

1. Je-li $p, n \in \mathbb{N}$, p prvočíslo, pak existuje komutativní těleso s p^n prvky.

2. Ať $\mathbb{F}$ je konečné komutativní těleso. Pak existují $p, n \in \mathbb{N}, p$ prvočíslo tak, že $|\mathbb{F}| = p^n$

3. Jsou-li $\mathbb{F}, \mathbb{K}$ komutativní tělesa a $|\mathbb{F}| = |\mathbb{K}| < \infty$, pak $\mathbb{F} \simeq \mathbb{K}$ okruhově.

Důkaz. Fakt: máme u ireducibilní nad $\mathbb{Z}_p[x]$ stupně n.

1) Položme $\mathbb{F}_{p^n} := Z_p[x]/u\mathbb{Z}_p[x]$. Z důsledku věty o komutativních tělesech a maximálních ideálech máme, že se jedná o těleso podle ideálu $I := u\mathbb{Z}_p[x]$. Pro libovolné $f, g \in \mathbb{Z}_p[x] : f+I = g+I \Leftrightarrow f-g \in I \Leftrightarrow u|f-g$ v $\mathbb{Z}_p[x]$. Tedy $f+I = (f \mod n)+I$. Pro $g, h \in \mathbb{Z}_p[x]$, kde deg $g, h < n$ navíc ještě platí $g+I = h+I \Leftrightarrow g = h$. Tedy prvky v $\mathbb{F}_{p^n}$ lze jednoznačně reprezentovat polynomy stupně nižším než n z $\mathbb{Z}_p[x]$, a těchto polynomů je p^n.

2) Mějme $\mathbb{F}$ konečné komutativní těleso Ať G je podgrupa grupy $\mathbb{F}(+)$ generovaná prvkem 1. Prvky G jsou $0, 1, 1+1, \ldots, 1+\ldots+1$, kde dále následuje 0. A tedy $G \simeq \mathbb{Z}_p(+)$. Z distributivity máme dokonce podokruh. Potom p musí být prvočíslo, jinak by $\mathbb{F}$ nebyl obor – měli bychom $xy = 0, x \neq 0, y \neq 0$. Máme izomorfismus $L : \mathbb{Z}_p \to G : k \mapsto$ součet k jedniček. Neboť G je podtěleso $\mathbb{F}$, $\mathbb{F}$ je vektorový prostor nad G, tedy existuje $n = \dim_G(\mathbb{F}) \Rightarrow |\mathbb{F}| = |G|^n$.

3) Ať $\mathbb{F}$ je konečné komutativní těleso, víme, že $|\mathbb{F}| = p^n$. Označme $\mathbb{Z}_p$ prvotěleso tělesa $\mathbb{F}$. Ukážeme, že $\mathbb{F} \simeq \mathbb{F}_{p^n}$ z 1, kde $\mathbb{F}_{p^n} = \mathbb{Z}_p[x]/u\mathbb{Z}_p[x]$. Víme, že $u|x^{p^n} - x$ v $\mathbb{Z}_p[x]$. Potom $x^{p^n} - x$ má za kořeny právě všechny prvky tělesa $\mathbb{F}$ – 0 je kořen, $x^{p^n-1} - 1$. Mějme $F^*(\cdot)$ multiplikativní grupu tělesa, $|F^*| = p^n - 1$, a tedy $\forall a \in \mathbb{F}^* : a^{p^n-1} = 1$. Tedy existuje $g \in \mathbb{F}[x]$, že $ug = x^{p^n} - x$, kde $\deg(g) < p^n$. Pro každé $a \in \mathbb{F} : 0 = a^{p^n} - a = u(a)g(a)$ – existuje $a \in \mathbb{F}$, že $u(a) = 0$. Jinak řečeno, $u\mathbb{Z}_p[x]$ je částí jádra dosazovacího homomorfismu d_u.

Z věty o homomorfismu existuje jednoznačně určení homomorfismus okruhů $\psi : \mathbb{Z}_p[x]/u\mathbb{Z}_p[x] \mapsto \mathbb{F}$ takový, že $\psi \cdot \pi_{u\mathbb{Z}_p[x]} = d_u$. Neboť $\mathrm{Ker}\psi = \{0\}$, máme, že ψ je prostý, a tedy isomorfismus, neboť obě tělesa jsou stejně velká. ⊞

Definice 26 (Multiplikativní množina, algebra F)**.** Buď R komutativní obor. Pak $M \subseteq R$ nezveme multiplikativní množinou, pokud obsahuje 1, neobsahuje 0 a je uzavřená na násobení.

Definice 27 (Algebra F - podílové těleso)**.** Buď M multiplikativní v R, $F := R \times M$. Na F definujeme strukturu algebry pro jazyk $(+, -, 0, \cdot, 1)$ následovně:

- $0 := (0, 1)$
- $1 := (1, 1)$
- $-(a, b) = (-a, b)$
- $(a, b) \cdot (c, d) = (ac, bd)$
- $(a, b) + (c, d) = (ad + bc, bd)$

Dále řekneme, že $(a, b) \sim (c, d) \overset{\text{def}}{\Leftrightarrow} ad = bc$

Věta 16 (Algebra F a její vlastnosti)**.** Pro algebru $F(+, -, 0, \cdot, 1)$ platí:

1. $F(+), F(\cdot)$ jsou komutativní monoidy
2. $\sim$ je kongruence na $F(+, -, 0, \cdot, 1)$ a $\forall a \in M : (0, a) \sim 0, (a, a) \sim 1$
3. $F/\sim (+, -, [0], \cdot, [1])$ je komutativní obor, navíc je to těleso, pokud $M = R \setminus \{0\}$.
4. zobrazení $\sigma : R \to F/\sim$ dané $\sigma(r) := [(r, 1)]$ je prostý okruhový homomorfismus.

Důkaz. Rozepsat ⊞

Poznámka (Značení podílových těles)**.** Místo $[(a, b)]$ budeme psát $\frac{a}{b}$.

Seznam témat