1. Teorie grup

• 1.1. Grupoid. Pologrupa

► 1.1.1. Definice. Algebru $G = (M, \omega)$ s binární operací ω nazýváme grupoid. Operaci ω obvykle značíme $\cdot$ a říkáme multiplikativní grupoid, nebo $+$ a říkáme aditivní grupoid.

► 1.1.2. Definice. Grupoid $G = (M, \cdot)$ je asociativní neboli pologrupa, platí-li asociativní zákon: $(\forall a, b, c \in M)((ab)c = a(bc))$.

► 1.1.3. Definice. Definujeme standardní součin: $(a_1) = a_1$; $(a_1 a_2) = a_1 \cdot a_2$; $(a_1 \dots a_n\, a_{n+1}) = (a_1 \dots a_n)a_{n+1}$.

► 1.1.4. Lemma. Platí-li asociativní zákon, pak platí i zobecněný asociativní zákon:

$$\big(\forall m, n \in \mathbb{N}\big)\big(\forall a_i \in M\big)\big((a_1 \dots a_m)(a_{m+1} \dots a_{m+n}) = (a_1 \dots a_{m+n})\big).$$

◦ *Důkaz.* Důkaz provedeme matematickou indukcí podle n.

$(n = 1)$ Plyne z definice standardního součinu.

$(n \to n+1)$ $(a_1 \dots a_m)(a_{m+1} \dots a_{m+n}\, a_{m+n+1}) = (a_1 \dots a_m)((a_{m+1} \dots a_{m+n})a_{m+n+1}) =$
$((a_1 \dots a_m)(a_{m+1} \dots a_{m+n}))a_{m+n+1} = (a_1 \dots a_{m+n})a_{m+n+1} = (a_1 \dots a_{m+n+1})$.

□

► 1.1.5. Definice. Grupoid $G = (M, \cdot)$ je komutativní grupoid, platí-li komutativní zákon: $(\forall a, b \in M)(ab = ba)$.

► 1.1.6. Definice. $\mathcal{S}_n$ je množina všech permutací množiny $\widehat{n}$.

► 1.1.7. Lemma. V komutativní pologrupě platí zobecněný komutativní zákon:

$$(\forall n \in \mathbb{N})(\forall \pi \in \mathcal{S}_n)(a_1 \dots a_n = a_{\pi(1)} \dots a_{\pi(n)})$$

◦ *Důkaz.* Platí, že každé $\pi \in \mathcal{S}_n$ je konečným složením sousedních transpozicí. □

► 1.1.8. Definice. V pologrupě definujeme pro $a \in M$ a $n \in \mathbb{N}_0$ přirozenou mocninu:

$$a^n := \underbrace{a \cdot a \cdot \dots \cdot a}_{n\text{-krát}}.$$

V aditivní pologrupě používáme označení $n \times a$.

► 1.1.9. Příklad.

(1) $G = (\mathbb{Q}, \oplus), x \oplus y = \frac{x+y}{2}$ není asociativní.

(2) $(\mathbb{C}^{n,n}, +)$ je komutativní pologrupa.

► 1.1.10. Příklad.

(1) Číselné pologrupy: nosičem je vždy podmnožina $\mathbb{C}$, operace jsou přirozené operace na číslech, tj. $(+)$ nebo $(\cdot)$.

(a) $(\mathbb{Z}, +)$ je komutativní pologrupa nazývaná aditivní pologrupa celých čísel.

(b) $(\mathbb{Z}, \cdot)$ je komutativní pologrupa nazývaná multiplikativní pologrupa celých čísel.

(c) $(\mathbb{N}, \cdot)$ je komutativní pologrupa.

(2) $(\mathbb{Z}, -)$ je grupoid.

(3) Nechť $A \neq \emptyset$ a $M = \{f : A \to A\}$ a $\omega = \circ$ je operace složení zorazení. Pak $(M, \circ)$ je pologrupa (nekomutativní) a nazývá se symetrická pologrupa na A.

(4) $(\mathbb{C}^{n,n}, \cdot)$ je pologrupa (nekomutativní).

► 1.1.11. Definice. Neutrálním prvkem grupoidu $G = (M, \cdot)$ rozumíme libovolný prvek $e \in M$ takový, že $(\forall a \in M)(ea = ae = a)$. Obyčejně značíme v multiplikativním grupoidu $e := 1$ a nazýváme jednotka a v aditivním $e := 0$ a nazýváme nula.

► 1.1.12. Lemma. Grupoid má nejvýše jeden neutrální prvek.

◦ *Důkaz.* Nechť e_1, e_2 jsou neutrální prvky. Pak $e_1 = e_1 e_2 = e_2$. □

► 1.1.13. Definice. Nechť $G = (M, \cdot)$ je grupoid s jednotkou. Inverzním prvkem k $a \in M$ je prvek a^{-1} takový, že $a^{-1}a = aa^{-1} = 1$.

► 1.1.14. Lemma. V pologrupě s jednotkou má každý prvek nejvýše jeden prvek inverzní.

◦ *Důkaz.* Nechť a_1 a a_2 jsou inverzní k a. Pak $a_1 = a_1 1 = a_1(aa_2) = (a_1 a)a_2 = a_2$. □

► 1.1.15. Definice. Prvky, ke kterým existuje inverzní prvek, se nazývají invertibilní nebo regulární. V aditivním grupoidu používáme název opačný prvek a značku $-a$.

► 1.1.16. Definice. Řekneme, že v grupoidu $G = (M, \cdot)$ lze dělit, platí-li, že

$$(\forall a, b \in M)(\exists x, y \in M)(ax = b \ \wedge \ ya = b).$$

► 1.1.17. Definice. Řekneme, že v grupoidu $G = (M, \cdot)$ lze krátit, platí-li, že

$$(\forall a, b, c \in M)\big((ac = bc \vee ca = cb) \Rightarrow a = b\big).$$

► 1.1.18. Příklad. V pologrupě $(\mathbb{N}, +)$ lze krátit, neboť $a + c = b + c \Rightarrow a = b$, ale nelze dělit, neboť $a + x = b$ nemá vždy řešení. Má tedy smysl pojmy zavádět nezávisle, neboť krácení a dělení ze sebe nevyplývají.

1.2. Grupa

▶ 1.2.1. Definice. Pologrupa G, ve které lze jednoznačně dělit, se nazývá grupa. Je-li navíc G komutativní, nazývá se Abelova grupa.

▶ 1.2.2. Věta. V libovolné grupě existuje jednotka a každý prvek má inverzní.

◦ *Důkaz.*

(existence jednotky) Víme, že $(\forall a, b)(\exists x, y)(ax = b \wedge ya = b)$. Tedy pro konkrétní a existuje e tak, že $ae = a$. Ukážeme, že e je jednotka. Mějme libovolné $b \in M$. Pak $(\exists y)(ya = b)$ a $be = (ya)e = y(ae) = ya = b$. Tedy e je univerzální pravá jednotka. Symetricky ukážeme existenci univerzální levé jednotky e'. Platí $e' = e'e = e =: 1$, tedy existuje jen jedna jednotka a je pravá i levá.

(invertibilita) Označme a_P řešení $ax = 1$ a a_L řešení $ya = 1$. Pak $a_L = a_L 1 = a_L(aa_P) = (a_L a)a_P = 1a_P = a_P$. Tedy existuje inverzní a je jeden.

□

▶ 1.2.3. Věta. Nechť G je pologrupa, ve které existuje pravá jednotka e a libovolný prvek a má zprava inverzní prvek a^{-1} vzhledem k e. Pak G je grupa (tj. lze v G dělit).

◦ *Důkaz.*

$$ea = eae = eaa^{-1}(a^{-1})^{-1} = ee(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a,$$

tedy e je i levou jednotkou. □

▶ 1.2.4. Definice. V grupě definujeme pro $a \in G^\bullet$ a pro $n \in \mathbb{Z}$ celou mocninu:

(1) a^n definované dříve;

(2) $a^0 := 1$;

(3) $a^{-n} := (a^{-1})^n = (a^n)^{-1}$.

V aditivní grupě $G = (G^\bullet, +)$ používáme pro $n \geq 1$ zápis $n \times a := \underbrace{a + \cdots + a}_{n\text{-krát}}$.

▶ 1.2.5. Lemma. V libovolné grupě platí $(a^n)^l = a^{nl}$, v Abelově grupě navíc $(ab)^n = a^n b^n$.

▶ 1.2.6. Příklad.

(1) $Z = (\mathbb{Z}; +)$ je aditivní grupa celých čísel a je Abelova.

(2) $(\mathbb{Q} \setminus \{0\}, \cdot)$ je multiplikativní grupa nenulových racionálních čísel a je Abelova.

(3) Obdobně pro $\mathbb{R} \setminus \{0\}$ a $\mathbb{C} \setminus \{0\}$.

(4) Nechť $A \neq \emptyset$, $M = \{f : A \xrightarrow{\text{bij.}} A\}$. Pak $(M, \circ)$ je grupa nazývaná symetrická grupa na A. Jednotkou je identické zobrazení a inverzním prvkem k f je f^{-1}.

(5) Symetrickou grupu na $\widehat{n}$ značíme $\mathcal{S}_n$.

(6) $E = (\{1\}, \cdot)$ je nejmenší možná grupa nazývaná triviální grupa.

(7) Pro $n \in \mathbb{N}$ a pro $k \in \widehat{n}$ definujeme $a_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ a nazýváme je komplexní n-té odmocniny z 1. Platí $a_k a_l = a_{k+l}$ (nebo $a_k a_l = a_{k+l-n}$ pokud $k+l > n$). Jednotka je $1 = a_n$ a $a_k^{-1} = a_{n-k}$. Označme $\sqrt[n]{1} = \{a_k \mid k \in \widehat{n}\}$. Pak $(\sqrt[n]{1}, \cdot)$ je Abelova grupa.

(8) Nechť V je vektorový prostor. Pak $(V, +)$ je Abelova grupa.

► 1.2.7. Definice. Pologrupa s jednotkou se nazývá monoid.

► 1.2.8. Příklad. Monoid slov. Nechť $\mathbb{A} \neq \emptyset$ je abeceda. Pak $\alpha = a_1 \dots a_n$ je slovo. Označme $\mathbb{A}^+$ množinu všech neprázdných slov, ε prázdné slovo a $\mathbb{A}^* = \mathbb{A}^+ \cup \{\varepsilon\}$ množinu všech slov. Definujme operaci zřetězení $\circ$ tak, že $\alpha \circ \beta = a_1 \dots a_n b_1 \dots b_m$. Pak $(\mathbb{A}^+, \circ)$ je pologrupa a $(\mathbb{A}^*, \circ)$ je monoid.

1.3. Podgrupa

► 1.3.1. Definice. Nechť $G = (M, \cdot)$ je grupa. Řekneme, že množina $N \subseteq M$, $N \neq \emptyset$ je uzavřená v G, platí-li:

$$(\forall a, b \in N)(ab^{-1} \in N).$$

► 1.3.2. Lemma. Je-li N uzavřená v $G = (M, \cdot)$, pak je $H = (N, \cdot)$ grupa.

◦ *Důkaz.* Ukážeme, že H splňuje základní vlastnosti grupy:

(existence jednotky) Vezmu libovolné pevné $a \in N$ a položím $b := a$. Pak vím, že $aa^{-1} = 1 \in N$.

(invertibilita) K libovolnému $b \in N$ položím $a := 1$. Pak vím, že $1b^{-1} = b^{-1} \in N$.

(uzavřenost vůči operaci) K libovolným $a, c \in N$ položím $b := c^{-1}$. Pak vím, že $ac^{-1} = ab \in N$.

□

► 1.3.3. Definice. H definované v předchozím lemmatu nazýváme podgrupa grupy G a značíme $H \Subset G$.

► 1.3.4. Lemma. $G \Subset G$, $E \Subset G$.

► 1.3.5. Definice. Netriviální podgrupa je taková $H \Subset G$, že platí $H \neq G$ a $H \neq E$.

► 1.3.6. Věta. Buď $G = (M, \cdot)$ grupa a pro $i \in I$ buď $H_i = (N_i, \cdot)$ systém jejích podgrup. Potom $H := \bigcap_{i \in I} H_i = \left(\bigcap_{i \in I} N_i, \cdot\right) \Subset G$.

◦ *Důkaz.* Nezbytně $1 \in H_i$ tedy $H \neq \emptyset$. $(\forall a,b \in H)(\forall i \in I)(a,b \in H_i) \Rightarrow (\forall a,b \in H)(ab^{-1} \in H_i) \Rightarrow ab^{-1} \in H$. □

► 1.3.7. DEFINICE. Mějme $G = (M,\cdot)$ a $a \in M$. Pak označujeme $\langle a \rangle$ nejmenší podgrupu (ve smyslu inkluze) grupy G obsahující a, tj. $\langle a \rangle = \bigcap_{\substack{H \leqslant G \\ a \in H,}} H$. Podgrupu $\langle a \rangle$ nazýváme cyklická podgrupa grupy G.

► 1.3.8. LEMMA. $\langle a \rangle^\bullet = \left\{ a^k \;\middle|\; k \in \mathbb{Z} \right\}$.

◦ *Důkaz.* Je uzavřená vůči testovací podmínce, je podgrupou a je zjevně nejmenší. □

► 1.3.9. DEFINICE. Nechť $G = (M,\cdot)$ je grupa, $N \subseteq M$ libovolná její podmnožina. Pak definujeme podgrupu generovanou N jako $\langle N \rangle = \bigcap \{ H \leqslant G \mid N \subseteq H^\bullet \}$. Množinu N nazýváme generátor $\langle N \rangle$.

► 1.3.10. LEMMA. $\langle N \rangle^\bullet = \left\{ a_1^{k_1} \cdots a_n^{k_n} \;\middle|\; n \in \mathbb{N}_0, a_i \in N, k_i \in \mathbb{Z} \right\} =: K$.

◦ *Důkaz.* Zjevně nemůže být $\langle N \rangle^\bullet$ menší, stačí tedy ukázat, že K je podgrupou: Nechť $a = a_1^{k_1} \cdots a_n^{k_n} \in K$ a $b = b_1^{\ell_1} \cdots b_m^{\ell_m} \in K$ a potom $ab^{-1} = a_1^{k_1} \cdots a_n^{k_n}\, b_m^{-\ell_m} \cdots b_1^{-\ell_1}$. □

► 1.3.11. DEFINICE.

(1) Nechť $H, K \leqslant G$. Pak definujeme součin podgrup $H \cdot K = \langle H^\bullet \cup K^\bullet \rangle$.

(2) Nechť pro všechna $i \in I$ je $H_i \leqslant G$. Pak definujeme $\prod_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i^\bullet \right\rangle$.

► 1.3.12. PŘÍKLAD.

(1) Nechť S je množina sudých celých čísel. Pak $(S,+) \leqslant (\mathbb{Z},+)$ je netriviální podgrupa. Ověříme uzavřenost: $(\forall a,b \in S)(a-b \in S)$, což ale zjevně platí.

(2) $\mathcal{S}_n$ je grupa permutací $\widehat{n}$, nechť $\mathcal{A}_n$ je množina všech sudých permutací (přesná definice dále). Pak všechna $\pi, \sigma \in \mathcal{A}_n$ jsou složením sudého počtu transpozicí a inverze vznikne přečtením transpozic pozpátku. Tedy $(\mathcal{A}_n, \circ) \leqslant (\mathcal{S}_n, \circ)$, kterou nazýváme alternující grupa. $|\mathcal{S}_n| = n!$; pro $n \geq 2$ je $|\mathcal{A}_n| = n!/2$.

(3) $(\sqrt[n]{1}, \cdot) \leqslant (\mathbb{C}, \cdot)$.

• 1.4. ŘÁD PRVKU GRUPY

► 1.4.1. DEFINICE. Buď $G = (M,\cdot)$ grupa, $a \in M$.

(1) a má nekonečný řád, pokud $(\forall k, \ell \in \mathbb{Z}, k \neq \ell)(a^k \neq a^\ell)$.

(2) Nemá-li a nekonečný řád, pak má konečný řád a řádem prvku a rozumíme $\min \{ r \in \mathbb{N} \mid a^r = 1 \}$.

► 1.4.2. LEMMA. Nechť $a \in G$ má řád r a pro nějaké $k \in \mathbb{Z}$ je $a^k = 1$. Pak $r \mid k$.

◦ *Důkaz.* V celých číslech platí princip dělení se zbytkem (důkladně probereme níže):

$$(\forall k, r \in \mathbb{Z}, r \neq 0)(\exists \ell, R \in \mathbb{Z}, 0 \leq R < r)(k = r\ell + R).$$

Platí $a^R = a^k(a^r)^{-\ell} = 1$, tedy $R \in \mathbb{N}$ a $R < r$, což je spor s tím, že r je řád a. Tedy $R = 0$ a $r \mid k$. □

► 1.4.3. Definice. Buď $G = (M, \cdot)$ grupa. Řekneme, že G je

(1) periodická/torzní, má-li libovolný její prvek konečný řád;

(2) bez torze, pokud má každý prvek různý od 1 nekonečný řád;

(3) smíšená v ostatních případech.

► 1.4.4. Lemma. Libovolná konečná grupa je periodická.

► 1.4.5. Příklad. Ukážeme, že nekonečné grupy mohou být periodické, bez torze i smíšené.

(1) Označme $G_n = (\sqrt[n]{1}, \cdot)$ a $M = \bigcup_{n\in\mathbb{N}} G_n = \{\cos 2q\pi + i \sin 2q\pi \mid q \in \mathbb{Q}\}$. Pak M je uzavřená v $(\mathbb{C}, \cdot)$: $a, b \in M$, $a \in G_k$, $b \in G_\ell$. $(ab^{-1})^{kl} = (a^k)^\ell (b^\ell)^{-k} = 1 \cdot 1 = 1$, tedy $ab^{-1} \in G_{k\ell}$. Zjevně $(M, \cdot)$ je nekonečná grupa a řád prvku $a \in G_k$ je nejvýše roven k. Tedy $(M, \cdot)$ je nekonečná a periodická.

(2) $(\mathbb{Z}, +)$ je zjevně bez torze, neboť pro $z \in \mathbb{Z}$ je $k \times n = 0 \Leftrightarrow z = 0$.

(3) $(\mathbb{C}, \cdot)$ je smíšená, neboť $(M, \cdot) \Subset (\mathbb{C}, \cdot)$ je periodická a např. číslo $2 \in \mathbb{C}$ má nekonečný řád.

► 1.4.6. Věta (algoritmus dělení, o dělení se zbytkem).

$$(\forall k, \ell \in \mathbb{Z}, \ell \neq 0)(\exists_1 q, r \in \mathbb{Z})(k = q\ell + r \ \wedge \ 0 \leq r < |\ell|).$$

◦ *Důkaz.*

(existence) Položme $q' := \left\lfloor \frac{k}{|\ell|} \right\rfloor$, tedy $q' \leq \frac{k}{|\ell|} < q' + 1$. Pak $q'|\ell| \leq k < q'|\ell| + |\ell|$, tedy pro $r := k - q'|\ell|$ platí $0 \leq r < |\ell|$. Položme $q := q' \operatorname{sgn} \ell$, pak platí $q\ell + r = q'\ell \operatorname{sgn} \ell + r = q'|\ell| + k - q'|\ell| = k$.

(jednoznačnost) Mějme druhou dvojici $\tilde{q}, \tilde{r}$ splňující tvrzení věty a pro spor nejprve předpokládejme, že $q \neq \tilde{q}$. Potom $|\tilde{r} - r| = |(k - \tilde{q}\ell) - (k - q\ell)| = |q\ell - \tilde{q}\ell| = |\ell|\,|q - \tilde{q}| \geq |\ell| \cdot 1$. Ale $(\forall r_1, r_2 \in \mathbb{Z}, 0 \leq r_{1,2} \leq |\ell| - 1)(|r_1 - r_2| \leq |\ell| - 1)$, což je spor. Tedy $q = \tilde{q}$ a $r = k - q\ell = k - \tilde{q}\ell = \tilde{r}$.

□

► 1.4.7. Definice. Největší společný dělitel $k, \ell \in \mathbb{Z}$ je takové $d \in \mathbb{Z}$, že:

(1) $d \mid k$, $d \mid \ell$;

(2) $d' \mid k \wedge d' \mid \ell \Rightarrow d' \mid d$.

► 1.4.8. Poznámka. Je-li číslo d největší společný dělitel, pak i číslo $-d$ je největší společný dělitel.

► 1.4.9. Věta. K libovolným číslům $k, \ell \in \mathbb{Z}$ existuje největší společný dělitel d a existují $u, v \in \mathbb{Z}$ takové, že

$$d = uk + v\ell.$$

◦ *Důkaz.* Nechť $k, \ell \neq 0$. Označme $D := \{uk + v\ell \mid u, v \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Množina D je uzavřená na součty a $\mathbb{Z}$-násobky. Definujme $d := \min\{x \in D \mid x > 0\}$ a ukážeme, že je největší společný dělitel.

$k = dq + r$, kde $q \in \mathbb{Z}$ a $0 \leq r < d$. $r = k - dq$, kde $k \in D$ a $dq \in D$, tedy $r \in D$ a $r < d$, tedy musí $r = 0$, jinak by $r > 0 \wedge r < d$. Tedy $d \mid k$ a stejným postupem $d \mid \ell$.

Nechť $d' \mid k$ a $d' \mid \ell$. Z toho vyplývá, že d' dělí všechna čísla v D, tedy i $d' \mid d$. □

► 1.4.10. Definice. Nezáporný největší společný dělitel k a ℓ budeme značit $\delta(k, \ell)$. Řekneme, že k a ℓ jsou nesoudělná, když $\delta(k, \ell) = 1$.

► 1.4.11. Definice. Nejmenší společný násobek čísel k a ℓ označujeme $\nu(k, \ell)$ a je to nejmenší takové $m \in \mathbb{N}$, že $k \mid m$ a $\ell \mid m$.

• 1.5. Cyklické grupy

► 1.5.1. Definice. Řekneme, že grupa G je cyklická, je-li rovna některé ze svých cyklických podgrup, tedy $(\exists a \in G)(G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\})$. Prvek a nazýváme generátor grupy G.

► 1.5.2. Lemma.

(1) Každá cyklická grupa je Abelova.

(2) Každá cyklická grupa je nejvýše spočetná.

► 1.5.3. Příklad.

(1) $Z = (\mathbb{Z}, +)$ je nekonečná cyklická grupa generovaná prvkem 1 nebo -1:

$$Z = (\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle .$$

(2) Pro každé $n \in \mathbb{N}$ je $\sqrt[n]{1}$ konečná cyklická grupa s řádem n, generátorem je např. $a_1 = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.

► 1.5.4. Věta. Libovolná podgrupa cyklické grupy je cyklická.

◦ *Důkaz.* $G = \langle a \rangle$, $H \leqslant G$. Pro $H = E$ je generátorem jednotka. Označme $p = \min\{i \in \mathbb{N} \mid a^i \in H\}$. Ukážeme, že $\langle a^p \rangle = H$.

(⊆) Zřejmé.

(⊇) Vezměmě libovolné $x \in H$. Pak $(\exists q \in \mathbb{Z})(x = a^q)$. Označme $d = \delta(p, q) = up + vq$. Potom $a^d = a^{up+vq} = (a^p)^u \cdot (a^q)^v \in H$. p je nejmenší, tedy $d \geq p$, ale $d \mid p$, tedy $d \leq p$, což dohromady dává $p = d$. Současně $d \mid q$, tedy $q = pr$ a $a^q = (a^p)^r \in \langle a^p \rangle$.

□

► 1.5.5. LEMMA. Nekonečná cyklická grupa $\langle a \rangle$ má právě 2 generátory, a to a a a^{-1}.

► 1.5.6. VĚTA. Buď $G = \langle a \rangle$ cyklická grupa řádu n a nechť $1 \leq k < n$. Potom a^k generuje G právě tehdy, když jsou k a n nesoudělná.

◦ *Důkaz.*

(⇒) $G = \langle a^k \rangle$. Tedy $a = \left(a^k\right)^u$. Z toho vyplývá, že $a^{ku-1} = 1$. Každý generátor má řád n, tedy a má řád n, tedy $ku - 1 = vn$, tedy $uk - vn = 1$, tedy $\delta(k, n) = 1$.

(⇐) Z nesoudělnosti existují u, v tak, že $uk + vn = 1$. Dále $a = a^1 = a^{uk+vn} = \left(a^k\right)^u (a^n)^v = \left(a^k\right)^u 1^v = \left(a^k\right)^u$. Tedy pro libovolné $x \in G$ je $x = a^r = \left(a^{uk}\right)^r$.

□

► 1.5.7. DEFINICE. Definujeme Eulerovu funkci $\phi : \mathbb{N} \to \mathbb{N}$, kde $\phi(n)$ je počet čísel z $\widehat{n}$ nesoudělných s n.

► 1.5.8. LEMMA. n je prvočíslo právě tehdy, když $\phi(n) = n - 1$.

• **1.6.** KONGRUENCE

► 1.6.1. DEFINICE. Mějme grupoid $G = (M, \cdot)$ a mějme ekvivalenci $\equiv$ na M. Pak pro libovolné $x \in M$ definujeme T_x jako třídu ekvivalence podle $\equiv$, která obsahuje x, tedy $x \in T_x \in M / \equiv$ (korektnost je zajištěna disjunktností tříd ekvivalence).

► 1.6.2. DEFINICE. Buďte $G = (M, \cdot)$ grupoid a $\equiv$ ekvivalence na G. Řekneme, že $\equiv$ je kongruence na G, platí-li, že

$$\big(\forall a, b, c, d \in M\big)\big((a \equiv b \wedge c \equiv d) \Rightarrow ac \equiv bd\big).$$

► 1.6.3. DEFINICE. Buďte $G = (M, \cdot)$ grupoid a $\equiv$ kongruence na G. Pak definujeme součin tříd ekvivalence $M / \equiv$ jako $T_a \cdot T_b = T_{ab}$. (Korektnost definice je zajištěna definující vlastností kongruence.)

► 1.6.4. DEFINICE. Buďte $G = (M, \cdot)$ grupoid a $\equiv$ kongruence na M. Pak definujeme faktorgrupoid G jako $G / \equiv := (M / \equiv, \cdot)$

► 1.6.5. VĚTA. Buďte $G = (M, \cdot)$ grupoid a $\equiv$ kongruence na M. Pak $G / \equiv$ je pologrupa, resp. je komutativní, resp. má jednotkou, resp. je grupa, má-li odpovídající vlastnost i G.

◦ *Důkaz.* Všechny body jsou obdobné, ukážeme asociativitu (pologrupa). Nechť $T_a, T_b, T_c \in M / \equiv$. Pak $(T_a T_b)T_c = T_{ab}T_c = T_{(ab)c} = T_{a(bc)} = T_a T_{bc} = T_a(T_b T_c)$. □

► 1.6.6. DEFINICE. Mějme $Z = (\mathbb{Z}, +)$ a libovolné $m \in \mathbb{Z}$. Pak definujeme kongruenci modulo m (značíme $\equiv_m$) následovně:

$$a \equiv_m b \iff (\exists s \in \mathbb{Z})(a - b = sm).$$

Třídy $Z / \equiv_m$ se nazývají zbytkové třídy po dělení m. Faktorgrupu $Z / \equiv_m$ označujeme Z_m.

► 1.6.7. Lemma. Relace $\equiv_m$ je kongruence na Z.

○ *Důkaz.* Ukážeme, že $\equiv_m$ je ekvivalence a splňuje definiční podmínku kongruence.

(reflexivita) Platí $a - a = 0 = 0m$.

(symetrie) Nechť $a - b = sm$. Pak $b - a = -sm = (-s)m$.

(tranzitivita) Nechť $a-b = sm$ a $b-c = tm$. Pak $a-c = (a-b)+(b-c) = sm+tm = (s+t)m$.

(kongruence) Nechť $a - b = sm$ a $c - d = tm$. Pak $(a + c) - (b + d) = sm + tm = (s + t)m$.

□

► 1.6.8. Příklad.

$(m = 0)$ $a \equiv_0 b \Leftrightarrow 0 \mid a - b \Leftrightarrow a = b$, tedy každý prvek má svou jednoprvkovou třídu.

$(m = 1)$ $a \equiv_1 b \Leftrightarrow 1 \mid a - b$, tedy všechny prvky leží ve stejné třídě.

► 1.6.9. Lemma. Pro $m \geq 1$ platí, že dvě celá čísla jsou v jedné třídě $\mathbb{Z} / \equiv_m$ právě tehdy, když dávají stejný zbytek po dělení m. Tedy tříd ekvivalence podle $\equiv_m$ je m.

○ *Důkaz.*

$(\Rightarrow)$ $a_1, a_2 \in \mathbb{Z}$, $a_1 \equiv_m a_2$. Pak $a_1 = mq_1 + r_1$, $a_2 = mq_2 + r_2$ a $a_1 - a_2 = sm$. Odečtením prvních dvou máme $a_1 - a_2 = m(q_1 - q_2) + (r_1 - r_2) = sm$, $r_1 - r_2 = m(q_1 - q_2 - s)$, tedy $m \mid r_1 - r_2$, ale protože $0 \leq r_{1,2} < m$, je nutně $r_1 = r_2$.

$(\Leftarrow)$ Víme, že $r_1 = r_2$, tedy $a_1 - a_2 = m(q_1 - q_2)$, tedy $s = q_1 - q_2$ a $a_1 \equiv_m a_2$.

$(|\mathbb{Z} / \equiv_m| = m)$ Toto je zjevné z předchozího.

□

► 1.6.10. Lemma. Faktorgrupa Z_m grupy $Z = (\mathbb{Z}, +)$ podle $\equiv_m$ je cyklická s generátorem T_1, tedy $Z_m = \langle T_1 \rangle$.

• 1.7. Homomorfismus

► 1.7.1. Definice. Buďte $G_1 = (M_1, \cdot)$, $G_2 = (M_2, \cdot)$ grupoidy. Řekneme, že $h : M_1 \to M_2$ je homomorfismus grupoidů, pokud platí:

$$(\forall x, y \in M_1)\big(h(xy) = h(x)h(y)\big)$$

a budeme též značit $h : G_1 \to G_2$.

► 1.7.2. DEFINICE. Homomorfismus h se nazývá:

(1) monomorfismus, je-li prostý (injekce);

(2) epimorfismus, je-li na (surjekce);

(3) izomorfismus, je-li prostý a na (bijekce);

(4) endomorfismus, je-li $G_1 = G_2$.

(5) automorfismus, je-li izomorfní endomorfismus (bijekce $G \to G$).

► 1.7.3. DEFINICE. Existuje-li izomorfismus $h : G_1 \to G_2$, nazýváme grupoidy izomorfní a značíme $G_1 \cong G_2$.

► 1.7.4. PŘÍKLAD. $G_1 := (\mathbb{R}^+, \cdot)$, $G_2 := (\mathbb{R}, +)$. Definujeme $h : G_1^\bullet \to G_2^\bullet$ jako $h(x) = \ln x$. Zjevně $h(xy) = h(x) + h(y)$, tedy h je morfismus a z analýzy víme, že je bijekcí. Tedy $G_1 \cong G_2$.

► 1.7.5. DEFINICE. Mějme $G = (M, \cdot)$ grupu a kongruenci $\equiv$ na G. Definujeme přirozené zobrazení (přirozený epimorfismus) $h_{\text{nat}} : G \to G / \equiv$ jako $h_{\text{nat}}(x) = T_x$.

► 1.7.6. LEMMA. h_{nat} je epimorfismus.

◦ *Důkaz.* Platí $h_{\text{nat}}(xy) = T_{xy} = T_x T_y = h_{\text{nat}}(x) h_{\text{nat}}(y)$, tedy h je homomorfismus. Současně pro každou třídu T_x platí $T_x = h_{\text{nat}}(x)$, tedy je na. □

► 1.7.7. VĚTA. Libovolné 2 nekonečné cyklické grupy jsou izomorfní. Libovolné 2 cyklické grupy s počtem prvků $n \in \mathbb{N}$ jsou izomorfní.

◦ *Důkaz.* Mějme libovolnou $G = \langle a \rangle$ nekonečnou. Ukážeme, že $G \cong Z = (\mathbb{Z}, +)$. Definujeme $h : G \to Z$ jako $h(a^n) = n \times 1 = n$. Pak h je prosté zobrazení ($m \neq n \Leftrightarrow a^m \neq a^n$), a neboť je G nekonečná, je na. Operace $\cong$ na grupách je ekvivalencí, tedy pro libovolné G_1, G_2 je $G_1 \cong Z$ a $G_2 \cong Z$, tedy $G_1 \cong G_2$. □

► 1.7.8. DEFINICE. Nechť $G = (M, \cdot)$ je grupoid, $N \subseteq M$. Pak $H = (N, \cdot)$ nazveme podgrupoid grupoidu G, pokud je H grupoid, tedy $(\forall x, y \in H)(xy \in H)$. Značíme $H \Subset G$.

► 1.7.9. LEMMA. Buďte G_1, G_2 grupoidy, $h : G_1 \to G_2$ homomorfismus. Pak $h(G_1) \Subset G_2$.

► 1.7.10. VĚTA (O HOMOMORFISMU). Buďte G_1, G_2 grupoidy, $h : G_1 \to G_2$ homomorfismus. Pak existuje kongruence (označovaná $\equiv_h$) na G_1 taková, že $h(G_1) \cong G_1 / \equiv_h$, kde $h(G_1)$ značí obor hodnot h.

◦ *Důkaz.* Definujeme $\equiv_h$ jako $x \equiv_h y \Leftrightarrow h(x) = h(y)$, tedy $\equiv_h$ je zjevně ekvivalence (je definovaná pomocí rovnosti) Nechť $a \equiv_h b$ a $c \equiv_h d$. Pak $h(ac) = h(a)h(c) = h(b)h(d) = h(bd)$, tedy $ac \equiv_h bd$ a $\equiv_h$ je kongruence.

Definujeme $g : G_1 / \equiv_h \to h(G_1)$ jako $g(T_x) = h(x)$. Definice je korektní, neboť $T_x = T_y \Leftrightarrow h(x) = h(y)$, z toho též vyplývá, že g je prosté. Z definice g pomocí h plyne, že pokryje celé $h(G_1)$, tedy je na. Je homomorfismus, neboť $g(T_x T_y) = g(T_{xy}) = h(xy) = h(x)h(y) = g(T_x)g(T_y)$. □

► 1.7.11. Poznámka. Všimněme si, jak souvisí korektnost definice s prostotou. Pokud by bylo $T_x = T_y$ a zároveň $h(x) \neq h(y)$, pak definice není korektní. Pokud by bylo $h(x) = h(y)$ a zároveň $T_x \neq T_y$, pak zobrazení není prosté.

► 1.7.12. Věta. Nechť $h : G_1 \to G_2$ je homomorfismus grupoidů a buď g zobrazení definované v důkazu předchozí věty. Pak $h_{\text{nat}} = g^{-1}h$.

► 1.7.13. Věta. Buďte G_1, G_2 grupoidy, $h : G_1 \to G_2$ homomorfismus. Je-li G_1 pologrupa, resp. je komutativní, resp. má jednotku, resp. je grupa, má tutéž vlastnost i grupoid $h(G_1)$.

○ *Důkaz.* Důkaz všech bodů je obdobný, ukážeme přenos jednotky. Nechť $1 \in G_1$, pak $h(1)$ je jednotkou v $h(G_1)$. Neboť pro libovolné $y \in h(G_1)$ existuje $x \in G_1$ takové, že $y = h(x)$. Potom $yh(1) = h(x)h(1) = h(x1) = h(x) = y$. Podobně zleva. □

► 1.7.14. Definice. Buď $G = (M, \cdot)$ grupa, $A, B \subseteq M$. Pak definujeme součin podmnožin $A \cdot B$ jako $A \cdot B := \{ab \mid a \in A, b \in B\}$. (Vztah mezi součinem podmnožin a podgrup osvětlíme později.) Je-li $B = \{b\}$, pak značíme $AB = Ab = \{xb \mid x \in A\}$.

► 1.7.15. Definice. Buď $H \leqslant G$ podgrupa grupy, definujeme následující 2 relace:

(1) $a \ {}_H\!\equiv b \Leftrightarrow b^{-1}a \in H$;

(2) $a \equiv_H b \Leftrightarrow ab^{-1} \in H$;

které nazýváme levá, resp. pravá ekvivalence indukovaná podgrupou H.

► 1.7.16. Lemma. Indukované relace jsou ekvivalence.

○ *Důkaz.*

(reflexivita) $a \ {}_H\!\equiv a \Leftrightarrow a^{-1}a \in H^\bullet$, ale $a^{-1}a = 1$.

(symetrie) $a \ {}_H\!\equiv b \Leftrightarrow b^{-1}a \in H^\bullet \Leftrightarrow (b^{-1}a)^{-1} = a^{-1}b \in H^\bullet \Leftrightarrow b \ {}_H\!\equiv a$.

(tranzitivita) $a \ {}_H\!\equiv b \wedge b \ {}_H\!\equiv c \Leftrightarrow b^{-1}a, c^{-1}b \in H^\bullet \Rightarrow c^{-1}bb^{-1}a \in H^\bullet \Rightarrow c^{-1}a \in H^\bullet \Leftrightarrow a \ {}_H\!\equiv c$.

Podobně lze ukázat totéž pro $\equiv_H$. □

► 1.7.17. Příklad. Zvolme $b = 1$. Pak $a \ {}_H\!\equiv 1 \Leftrightarrow a \in H$ a současně $a \equiv_H 1 \Leftrightarrow a \in H$, tedy H je jedna ze tříd ekvivalence podle obou indukovaných ekvivalencí.

► 1.7.18. Lemma. Označme T_a^L resp. T_a^P třídu ekvivalence podle ${}_H\!\equiv$, resp. $\equiv_H$ obsahující $a \in G^\bullet$. Potom $T_a^L = aH^\bullet$ a $T_a^P = H^\bullet a$.

○ *Důkaz.* Opět lemma ukážeme pro levou ekvivalenci. T_a^L je třída ${}_H\!\equiv$ obsahující a. Mějme libovolné $x \in G$. Pak $x \in T_a^L \Leftrightarrow x \ {}_H\!\equiv a \Leftrightarrow a^{-1}x \in H^\bullet \Leftrightarrow (\exists h \in H^\bullet)(a^{-1}x = h) \Leftrightarrow (\exists h \in H^\bullet)(x = ah) \Leftrightarrow x \in aH^\bullet$. □

► 1.7.19. Věta.

(1) Libovolné 2 třídy rozkladů dle ${}_H\!\equiv$ či $\equiv_H$ jsou (množinově) ekvivalentní. („Každá třída má stejně prvků.“)

(2) Levý rozklad je (množinově) ekvivalentní s pravým rozkladem. („Levých a pravých tříd je stejný počet.“)

◦ *Důkaz.*

(1) Libovolné 2 levé třídy $aH^\bullet$ a $bH^\bullet$. Definujme $f : aH^\bullet \to bH^\bullet$ jako $f(x) = ba^{-1}x$. Nechť $x = ah$, pak $f(x) = bh \in bH^\bullet$ tedy definice je korektní. Mějme $y = bh$, pak $y = f(x) \Leftrightarrow ba^{-1}x \Leftrightarrow h = a^{-1}x \Leftrightarrow x = ah \in aH^\bullet$. Podobně dokážeme, že všechny pravé jsou ekvivalentní. Z tranzitivity a z toho, že $H^\bullet$ je v obou faktorizacích, vyplývá, že všechny levé třídy jsou ekvivalentní se všemi pravými.

(2) Definujeme $g : M \,/\, {}_H\!\equiv \to M \,/\, \equiv_H$ jako $g(aH^\bullet) = H^\bullet a^{-1}$. Zjevně je na, neboť a^{-1} projde celé G právě tehdy, když a projde celé G. Platí: $g(aH^\bullet) = g(bH^\bullet) \Leftrightarrow H^\bullet a^{-1} = H^\bullet b^{-1} \Leftrightarrow a^{-1} \equiv_H b^{-1} \Leftrightarrow a^{-1}b \in H^\bullet \Leftrightarrow (a^{-1}b)^{-1} = b^{-1}a \in H^\bullet \Leftrightarrow a \;{}_H\!\equiv b \Leftrightarrow aH^\bullet = bH^\bullet$, tedy g je prosté (směr $\Rightarrow$) a definice je korektní (směr $\Leftarrow$).

□

► 1.7.20. Definice. Počtu rozkladových tříd podle indukovaných ekvivalencí se říká index podgrupy H.

► 1.7.21. Věta (Lagrange). Součin řádu a indexu libovolné podgrupy H konečné grupy G je roven řádu G.

◦ *Důkaz.* Všechny třídy mají počet prvků, jako je řád H, a je jich tolik, jako je index H. □

► 1.7.22. Důsledek.

(1) Řád libovolné podgrupy konečné grupy G dělí řád G.

(2) Řád libovolného prvku konečné grupy G dělí řád G.

► 1.7.23. Důsledek. Má-li grupa G prvočíselný řád, je cyklická a nemá žádné netriviální podgrupy. Všechny grupy s prvočíselným řádem p jsou izomorfní.

◦ *Důkaz.* Grupa není triviální (má řád nejméně 2). Vezmu $a \neq 1$. Pak řád prvku a je p, (jednotkový řád má jen jednotka), tedy a generuje G. □

► 1.7.24. Věta. Buď G cyklická grupa řádu n a nechť $k \mid n$. Potom existuje právě jedna podgrupa grupy G řádu k.

◦ *Důkaz.*

(existence) Nechť $a \in G$ je generátor grupy. Položme $H := \langle a^{n/k} \rangle$. Pak $\left(a^{n/k}\right)^k = 1$ a platí, že pokud $\left(a^{n/k}\right)^\ell = 1$, tak $n\ell/k = sn$, tedy $\ell = ks$ a $\ell \geq k$.

(jednoznačnost) Nechť $K \Subset G$ je řádu k. Pak $K = \langle a^\ell \rangle$ a $\left(a^\ell\right)^k = 1$ a $\ell k = sn = skn/k$ a tedy $\ell = sd$ a $a^\ell = \left(a^{n/k}\right)^s \in H$. Tedy $K \Subset H$ a z rovnosti počtu prvků plyne $K = H$.

□

► 1.7.25. Definice. Buď G grupa. Řekneme, že podgrupa $H \Subset G$ je normální (invariantní), pokud ${}_H\equiv$ a $\equiv_H$ splývají, a značíme $H \lhd G$.

► 1.7.26. Lemma. $E \lhd G$; $G \lhd G$.

◦ *Důkaz.*

(1) $a \ {}_E\equiv b \Leftrightarrow b^{-1}a = 1 \Leftrightarrow a = b$; $a \equiv_E b \Leftrightarrow ab^{-1} = 1 \Leftrightarrow a = b$.

(2) $a \ {}_G\equiv b \Leftrightarrow b^{-1}a \in G$, což platí pro libovolné a, b; stejně tak pro $\equiv_G$.

□

► 1.7.27. Lemma. Je-li grupa G Abelova, je libovolná její podgrupa $H \Subset G$ normální.

► 1.7.28. Věta. Rozklad grupy G je rozkladem podle kongruence právě tehdy, je-li rozkladem podle některé normální podgrupy $H \lhd G$.

◦ *Důkaz.*

(⇒) Nechť $\equiv$ je kongruence na grupě $G = (M, \cdot)$. Vezměme třídu T_1 a $a, b \in T_1$. Pak $a \equiv 1$ a $b \equiv 1$, tedy $ab \equiv 1$. Také $a^{-1} \equiv a^{-1}$, tedy $1 \equiv a^{-1}$.

Ukážeme, že $H = (T_1, \cdot) \Subset G$ je normální. Vezměme lib. $x \in M$. Pak $x \in T_a \Leftrightarrow x \equiv a \Leftrightarrow xa^{-1} \equiv 1 \Leftrightarrow xa^{-1} \in H^\bullet \Leftrightarrow (\exists h \in H^\bullet)(xa^{-1} = h) \Leftrightarrow (\exists h \in H^\bullet)(x = ha) \Leftrightarrow x \in H^\bullet a$. Budeme-li násobit a^{-1} zleva, dostaneme $x \in aH^\bullet$. Tedy $T_a = aH^\bullet = H^\bullet a$, což znamená, že $H \lhd G$ a $(\equiv) = ({}_H\equiv) = (\equiv_H)$

(⇐) Nechť $H \lhd G$, ukážeme, že $\equiv_H$ je kongruence. Mějme $a, b, c, d \in M$ takové, že $a \equiv_H b$ a $c \equiv_H d$. Potom $ac(bd)^{-1} = acd^{-1}b^{-1}$. Označme $h := cd^{-1} \in H^\bullet$, pak existuje $h' \in H^\bullet$ takové, že $ah = h'a$. Tedy celkově dostáváme $ac(bd)^{-1} = ahb^{-1} = h'ab^{-1} \in h'H^\bullet = H$.

□

• 1.8. Vnitřní automorfismy

► 1.8.1. Definice. Nechť $\mathcal{A}^\bullet_G$ je množina všech automorfismů na G. Pak definujme $\mathcal{A}_G = (\mathcal{A}^\bullet_G, \circ)$.

► 1.8.2. Lemma. Nechť G je grupa. Pak $\mathcal{A}_G$ je grupa a $\mathcal{A}_G \Subset \mathcal{S}_G$.

◦ *Důkaz.* Součin (složení) 2 automorfismů je automorfismus, existuje jednotka (identita) a každý automorfismus má inverzní. Nechť $x, y \in G^\bullet$, $\alpha \in \mathcal{A}_G^\bullet$, pak $\alpha^{-1}(xy) = \alpha^{-1}(\alpha(\alpha^{-1}(x))\alpha(\alpha^{-1}(y))) = \alpha^{-1}(\alpha(\alpha^{-1}(x)\alpha^{-1}(y))) = \alpha^{-1}(x)\alpha^{-1}(y)$, tedy inverzní je opět morfismem. □

► 1.8.3. Lemma. Nechť $a \in M$, $\alpha_a(x) = axa^{-1}$. Pak α_a je automorfismus.

◦ *Důkaz.*

(morfismus) Pro libovolné $x, y \in M$ platí $\alpha_a(x)\alpha_a(y) = axa^{-1}\,aya^{-1} = axya^{-1} = \alpha_a(xy)$.

(bijekce) Ukážeme, že $\alpha_{a^{-1}}$ je inverzní k α_a, tj. $(\forall x \in M)(\alpha_{a^{-1}}\alpha_a = \alpha_a\alpha_{a^{-1}} = \mathrm{id})$. Pro všechna $x \in M$ platí $(\alpha_{a^{-1}}\alpha_a)(x) = \alpha_{a^{-1}}(axa^{-1}) = a^{-1}axa^{-1}a = 1x1 = x$, obdobně $(\alpha_a\alpha_{a^{-1}})(x) = x$.

□

► 1.8.4. Definice. Automorfismus α na G je vnitřní, právě když $(\exists a \in G^\bullet)(\alpha(x) = axa^{-1})$. Takový automorfismus značíme α_a.

Označme $\mathcal{I}_G^\bullet$ množinu všech vnitřních automorfismů.

► 1.8.5. Lemma. $\mathcal{I}_G = (\mathcal{I}_G^\bullet, \circ) \Subset \mathcal{A}_G$ je grupa.

◦ *Důkaz.* Jednotkou je α_1, $\alpha_1(x) = 1x1^{-1} = x$. $(\alpha_a\alpha_b^{-1})(x) = ab^{-1}xba^{-1} = (ab^{-1})x(ab^{-1})^{-1} = \alpha_{ab^{-1}}(x)$ □

► 1.8.6. Věta. Podgrupa H grupy G je normální právě tehdy, je-li uzavřená vůči všem vnitřním automorfismům, tj.

$$H \lhd G \iff (\forall a \in G^\bullet)(\forall x \in H^\bullet)(\alpha_a(x) \in H^\bullet).$$

◦ *Důkaz.*

(⇒) Mějme $H \lhd G$ a libovolné $a \in G^\bullet$ a $x \in H^\bullet$. Pak $ax \in aH^\bullet = H^\bullet a \Rightarrow (\exists h \in H^\bullet)(ax = ha) \Rightarrow axa^{-1} \in H^\bullet$.

(⇐) Mějme libovolné $x \in aH^\bullet$, tedy $x = ah = aha^{-1}a = \alpha_a(h)a$ a neboť $\alpha_a(h) \in H^\bullet$, je $x \in H^\bullet a$ a $aH^\bullet \subseteq H^\bullet a$. Obrácenou inkluzi dokážeme obdobně, tedy $aH^\bullet = H^\bullet a$.

□

► 1.8.7. Poznámka. Věta dává návod, jako ověřit, že H je normální. Ale nesmíme opomenout ověřit, že H vůbec je podgrupou.

► 1.8.8. Definice. Buď G grupa. Řekneme, že $x, y \in G^\bullet$ jsou konjungované, existuje-li $a \in G^\bullet$ takové, že $y = \alpha_a(x)$. Značíme $x \equiv_K y$.

► 1.8.9. Lemma. Relace konjungovanosti je ekvivalence na G.

► 1.8.10. Důsledek. Podgrupa H grupy G je normální právě tehdy, je-li sjednocením nějakých tříd konjungovaných prvků.

► 1.8.11. Definice. Buďte G_1, G_2 grupy, $h : G_1 \to G_2$ homomorfismus. Jádrem homomorfismu h rozumíme množinu $\ker h := h^{-1}(\{1\}) = \{x \in G_1^\bullet \mid h(x) = 1\}$.

► 1.8.12. Lemma. Buďte G_1, G_2 grupy, $h : G_1 \to G_2$ homomorfismus. Pak $\ker h \lhd G_1$.

◦ *Důkaz.*

(je podgrupa) Mějme libovolné $x, y \in \ker h$, tj. $h(x) = h(y) = 1$. Pak $h(xy^{-1}) = h(x)h(y^{-1}) = h(x)h(y)^{-1} = 11^{-1} = 1$.

(je uzavřená vůči automorfismům) Nechť $a \in G_1^\bullet$, $x \in \ker h$. Pak $h(axa^{-1}) = h(a)h(x)h(a^{-1}) = h(a)h(a^{-1}) = h(aa^{-1}) = h(1) = 1$.

□

► 1.8.13. Lemma. Mějme $H \lhd G$, faktorgrupu $G \,/\, H$ a přirozený epimorfismus $h_{\text{nat}}(x) = T_x$. Pak $\ker h_{\text{nat}} = H$.

◦ *Důkaz.* $\ker h_{\text{nat}} = \{x \in G^\bullet \mid T_x = T_1\}$, ale $T_1 = H^\bullet$, tedy $\ker h_{\text{nat}} = H^\bullet$. □

► 1.8.14. Věta. Normální podgrupy grupy G jsou právě všechna jádra homomorfismů na G, tj.

$$H \lhd G \iff (\exists h, h \text{ je homomorfismus na } G)(H = \ker h).$$

◦ *Důkaz.* Věta shnuje předchozí 2 tvrzení. □

► 1.8.15. Lemma. Homomorfismus $h : G_1 \to G_2$ je prostý právě tehdy, je-li $\ker h = \{1\}$.

◦ *Důkaz.*

(⇒) Obrazem jednoprvkové množiny je nejvýše jednoprvková množina a 1 je v jádru pro všechny homomorfismy.

(⇐) Nechť $\ker h = \{1\}$. Mějme $x, y \in G_1$ takové, že $h(x) = h(y)$. Pak $1 = h(x)h(y^{-1}) = h(xy) \Rightarrow xy^{-1} \in \ker h \Rightarrow xy^{-1} = 1 \Rightarrow x = y$.

□

► 1.8.16. Lemma. Nechť $h : G_1 \to G_2$ je homomorfismus. Pak $a \equiv_{\ker h} b$ právě tehdy, je-li $h(a) = h(b)$.

◦ *Důkaz.* $a \equiv_{\ker h} b \Leftrightarrow ab^{-1} \in \ker h \Leftrightarrow h(ab^{-1}) = 1 \Leftrightarrow h(a) = h(b)$. □

► 1.8.17. Věta (o homomorfismu pro grupy). Nechť $h : G_1 \to G_2$ je homomorfismus grup. Potom $h(G_1) \cong G_1 \,/\, \ker h$.

◦ *Důkaz.* $h(G_1) \cong G_1 / \equiv_h = G_1 / \equiv_{\ker h}$. □

► 1.8.18. Věta. Buď G grupa a buďte $H_i \lhd G$ pro $i \in I$. Potom

$$A := \bigcap_{i\in I} H_i \lhd G \quad \text{a} \quad B := \prod_{i\in I} H_i \lhd G.$$

◦ *Důkaz.*

(průnik) Mějme libovolné $a \in G^\bullet$ a $x \in A$. Pak $(\forall i \in I)(x \in H^\bullet) \Rightarrow (\forall i)(\alpha_a(x) \in H_i) \Rightarrow \alpha_a(x) \in A$.

(součin) Mějme libovolné $a \in G^\bullet$ a $x \in B$. Platí $B = \langle \bigcup_I H_i^\bullet \rangle$. Pak $x = a_1^{k_1} \cdots a_n^{k_n}$, kde $k_j \in \mathbb{Z}$ a $(\forall j)(\exists i_j)(a_j \in H_{j_i}^\bullet)$. Protože H_{j_i} je podgrupa, je $a_i^{k_i} \in H_{j_i}^\bullet$ a protože, je normální, je $\alpha_a(a_i^{k_i}) \in H_{j_i}^\bullet$. A konečně $\alpha_a(x) = \alpha_a(a_1^{k_1} \cdots a_n^{k_n}) = \alpha_a(a_1^{k_1}) \cdots \alpha_a(a_n^{k_n})$. Tedy každý prvek součinu je ve sjednocení podgrup, tedy je i v produktu podgrup.

□

► 1.8.19. Lemma (o tečce). Buď G grupa, $A \lhd G$ a $B \Subset G$. Potom $(AB)^\bullet = A^\bullet B^\bullet$.

◦ *Důkaz.* $AB = \langle A^\bullet \cup B^\bullet \rangle$, ale $A^\bullet B^\bullet = \{ab \mid a \in A^\bullet, b \in B^\bullet\}$.

(⊆) Ukážeme, že $A^\bullet B^\bullet$ je uzavřená v grupě G. Platí $A \cup B \subseteq A^\bullet B^\bullet$ Zvolme libovolné $x, y \in A^\bullet B^\bullet$, $x = a_1 b_1$, $y = a_2 b_2$. Potom $xy^{-1} = a_1 b_1 (a_2 b_2)^{-1} = a_1 \underbrace{b_1 b_2^{-1} a_2^{-1} (b_1 b_2^{-1})^{-1}}_{\alpha_{b_1 b_2^{-1}}(a_2^{-1}) \in A^\bullet} b_1 b_2^{-1} = \tilde{a}\tilde{b}$,

kde $\tilde{a} \in A^\bullet$ a $\tilde{b} \in B^\bullet$. Tedy $A^\bullet B^\bullet$ je podgrupa obsahující $A^\bullet \cup B^\bullet$. Ale AB je nejmenší taková, tedy inkluze platí.

(⊇) V AB jsou všechny součiny $x_1 \cdots x_n$, kde $x_i \in A \cup B$ tedy i všechny součiny tvaru ab.

□

► 1.8.20. Definice. Buď G grupa. Pak $C_G := \{c \in G \mid (\forall x \in M)(cx = xc)\}$ nazveme centrum grupy (tedy centrum grupy obsahuje právě ty prvky grupy, které komutují s každým prvkem.)

► 1.8.21. Lemma. Buď G grupa, C_G její centrum. Pak:

(1) je-li G Abelova, je $C_G = G$;

(2) $C_G \lhd G$;

(3) $G / C_G \cong \mathcal{I}_G$.

◦ *Důkaz.*

(1) V Abelově grupě komutují každé 2 prvky.

(2) Ukážeme, že C_G je uzavřená vůči všem vnitřním automorfismům. Mějme libovolné $a \in G^\bullet$ a $c \in C_G$. Pak $\alpha_a(c) = aca^{-1} = caa^{-1} = c \in C_G$.

(3) Definujme $h : G \to \mathcal{I}_G$ jako $h(a) = \alpha_a$, h je epimorfismus. Pak $I_G = h(G) \cong G \,/\, \ker h$. Platí $x \in \ker h \Leftrightarrow h(x) = \alpha_1 = \mathrm{id}_G \Leftrightarrow (\forall y \in G^\bullet)(xyx^{-1} = y) \Leftrightarrow (\forall y \in G^\bullet)(xy = yx) \Leftrightarrow x \in C_G$, tedy $\ker h = C_G$ a $I_G \cong G \,/\, C_G$.

□

► 1.8.22. Věta (o izomorfismu). Buď $G = (M, \cdot)$ grupa, $A, B \Subset G$. Je-li $A \lhd AB$, potom $A \cap B \lhd B$ a $AB \,/\, A \cong B \,/\, (A \cap B)$.

◦ *Důkaz.* Třídy $AB \,/\, A$ jsou tvaru $A^\bullet c$, kde $c \in (AB)^\bullet = A^\bullet B^\bullet$. Tedy $(\exists a \in A^\bullet, b \in B^\bullet)(c = ab)$. Vezměme $f_{\mathrm{nat}} : AB \to AB \,/\, A$ a položme $f_B = f_{\mathrm{nat}}/B$. Ukážeme, že $f_B : B \to AB \,/\, A$ je epimorfismus, tedy, že v každé třídě $A^\bullet ab$ leží prvek z B. Tedy i $a^{-1}ab = b$ je v každé třídě. Podlě věty o homomorfismu je $AB \,/\, A \cong B \,/\, \ker f_B$, ale $\ker f_B = \{x \in B \mid f_B(x) = T_1 = A\} = \{x \in B \mid x \in A\} = A \cap B$. □

► 1.8.23. Definice. Grupa, která nemá netriviální normální podgrupy, tj. $H \lhd G \Rightarrow H = G \vee H = E$, se nazývá jednoduchá.

► 1.8.24. Příklad.

(1) E je jednoduchá.

(2) G o $p \in P$ prvcích jsou jednoduché, současně jsou cyklické, tedy Abelovy.

► 1.8.25. Věta. Buď $G \neq E$ Abelova grupa. Potom G je jednoduchá právě tehdy, má-li prvočíselný řád p.

◦ *Důkaz.*

(G je cyklická) Nebyla-li by cyklická, obsahovala by netriviální podgrupu, která by byla normální, neboť všechny by byly normální (netriviální podgrupou by bylo libovolné $\langle a \rangle$, kde $a \neq 1$).

(G je konečná) Pokud není konečná, pak $G \cong Z = (\mathbb{Z}, +)$, ale např. $S = (\mathbb{S}, +) \lhd Z$ a S odpovídá nějaké netriviální podgrupa G.

(neex. $1 \neq q \mid p$) Podle předházející věty existuje podgrupa H řádu q, která je v Abelově normální, a tedy G není jednoduchá.

□

• 1.9. Grupy permutací

► 1.9.1. Definice. Buď A množina a M množina všech bijekcí $A \to A$. Pak $\mathcal{S}_A(M, \circ)$ je grupa nazývaná symetrická grupa. Označme ϵ identitu v $\mathcal{S}_A$.

► 1.9.2. Definice. Grupa permutací je libovolná podgrupa symetrické grupy $\mathcal{S}_A$.

► 1.9.3. Věta (Cayley). Libovolná grupa je izomorfní s nějakou grupou permutací.

○ *Důkaz.* Mějme $G = (M, \cdot)$, $a \in M$; definujeme $\pi_a : M \to M$ jako $\pi_a(x) = ax$. Pro libovolné $y \in M$ řešme $\pi_a(x) = ax = y$, dostaneme jedno řešení $x = a^{-1}y$, tedy π_a je bijekce (permutace).

Definujme $h : M \to \mathcal{S}_M$ jako $h(a) = \pi_a$ a ukážeme, že h je homomorfismus: Mějme $a, b, x \in M$; pak $h(ab)(x) = \pi_{ab}(x) = abx = \pi_a(bx) = \pi_a(\pi_b(x)) = (\pi_a\pi_b)(x) = (h(a)h(b))(x)$.

Ukážeme, že h je monomorfní (prostý): $\ker h = \{a \in M \mid h(a) = \epsilon\}$, $(\forall x \in M)(\epsilon(x) = x)$, $\pi_a(x) = \epsilon(x) = x$, $a = 1$.

Platí $G \cong h(G) \Subset \mathcal{S}_M$. Tedy $h(G)$ je grupa permutací. □

► 1.9.4. Poznámka. Cayleyova věta se dá formulovat i následovně: Libovolnou grupu lze izomorfně vnořit do symetrické grupy.

► 1.9.5. Poznámka. Pro $M = \widehat{n}$ se G izomorfně vnoří do $\mathcal{S}_{\widehat{n}} =: \mathcal{S}_n$.

► 1.9.6. Poznámka. $\pi \in \mathcal{S}_n$ zapisované $\pi = \begin{pmatrix} 1 & \cdots & n \\ p_1 & \cdots & p_n \end{pmatrix}$ je zobrazení.

► 1.9.7. Příklad. $\pi \in \mathcal{S}_8$, $\pi = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 2&4&5&1&3&7&6&8 \end{pmatrix}$ lze zapsat jako $1 \to 2 \to 4(\to 1); 3 \to 5(\to 3); 6 \to 7(\to 6); 8(\to 8)$, ale zkráceně jako $(124)(35)(67)(8)$. Zápis současně vyjadřuje složení cyklů a můžeme vynechat cykly s 1 prvkem. Tedy můžeme psát $\pi = (124)(35)(67)$.

► 1.9.8. Definice. Mějme $\pi \in \mathcal{S}_n$. Pak π je cyklus, pokud $\pi = (p_1p_2...p_k)$, $1 \leq k \leq n$, p_k jsou různá. Cykly jsou nezávislé, pokud neobsahují společný prvek.

► 1.9.9. Lemma. Libovolná permutace lze rozepsat jako součin nezávislých cyklů.

► 1.9.10. Lemma.

$$(k_1 \cdots k_p) = (k_1k_p)(k_1k_{p-1}) \cdots (k_1k_3)(k_1k_2).$$

○ *Důkaz.* Obrázkem. □

► 1.9.11. Důsledek. Transpozice generují $\mathcal{S}_n$. (Každá permutace lze zapsat jako součin transpozic.)

► 1.9.12. Poznámka. Lze ukázat, že i sousední transpozice generují $\mathcal{S}_n$. Dále lze ukázat, že pro jakékoli n existují 2 permutace, které generují $\mathcal{S}_n$, a to např. $\tau = (12)$ a $\pi = (123\ldots n)$.

► 1.9.13. Věta. Buď $n \in \mathbb{N}$ a $\sigma, \pi \in \mathcal{S}_n$, $\sigma = (k_1^1 \cdots k_{p_1}^1) \cdots (k_1^m \cdots k_{p_m}^m)$ je rozklad na (ne nutně nezávislé) cykly. Potom $\alpha_\pi(\sigma) = (\pi(k_1^1) \cdots \pi(k_{p_1}^1)) \cdots (\pi(k_1^m) \cdots \pi(k_{p_m}^m))$

◦ *Důkaz.*

($m = 1$) Máme $\sigma = (k_1 \dots k_p)$, označme $\sigma_\pi := (\pi(k_1) \dots \pi(k_p))$, tedy chceme $\alpha_\pi(\sigma) = \sigma_\pi$, což, protože π je bijekce, je ekvivalentní $\alpha_\pi(\sigma) \circ \pi = \sigma_\pi \circ \pi$.

Ukážeme, že $(\forall k \in \widehat{n})\,(\alpha_\pi(\sigma)(\pi(k)) = \sigma_\pi(\pi(k)))$. To jest $(\pi\sigma\pi^{-1})(\pi(k)) = \pi(\sigma(k))? = \sigma_\pi(\pi(k))$.

Nechť $k = k_i$, pak $\sigma(k) = k_{i+1}$ (položíme $k_{p+1} := k_1$), tedy $\pi(\sigma(k)) = \pi(k_{i+1})$. Současně $\sigma_\pi(\pi(k_i)) = \pi(k_{i+1})$, což jsme potřebovali.

Pro $k \neq k_i$ jsou obě strany rovny $\pi(k)$.

($m \in \mathbb{N}$) S využitím případu $m = 1$ dostaneme

$$\alpha_\pi\left(\left(k_1^1 \dots k_{p_1}^1\right) \dots \left(k_1^m \dots k_{p_m}^m\right)\right) = \alpha_\pi\left(k_1^1 \dots k_{p_1}^1\right) \dots \alpha_\pi\left(k_1^m \dots k_{p_m}^m\right) = \left(\pi(k_1^1) \dots \pi\left(k_{p_1}^1\right)\right) \dots \left(\pi(k_1^m) \dots \pi\left(k_{p_m}^m\right)\right).$$

□

► 1.9.14. Důsledek. $(\alpha_\pi(\sigma))(\pi(k)) = \pi(\sigma(k))$, $\sigma = \begin{pmatrix} 1 & \cdots & n \\ p_1 & \cdots & p_n \end{pmatrix}$, pak $\alpha_\pi(\sigma) = \begin{pmatrix} \pi(1) & \cdots & \pi(n) \\ \pi(p_1) & \cdots & \pi(p_n) \end{pmatrix}$.

► 1.9.15. Lemma. Libovolná podgrupa H grupy G, která má index 2, je normální. (Index je počet rozkladových tříd G / H).

◦ *Důkaz.* Jedna ze tříd je H, druhá tedy nutně $G \setminus H$. Rozklad je tedy jednoznačný. □

► 1.9.16. Definice. Označme $\mathcal{A}_n$ grupu sudých permutací (ověření, že je grupa, je triviální). Pak $\mathcal{A}_n$ nazýváme alternující (pod)grupa.

► 1.9.17. Důsledek. $\mathcal{A}_n \lhd \mathcal{S}_n$.

► 1.9.18. Lemma. Nechť $A \Subset B \Subset G$. Pak $A \lhd G \Rightarrow A \lhd B$.

◦ *Důkaz.* Lze jednoduše ukázat pomocí uzavřenosti na vnitřní automorfismy. □

► 1.9.19. Příklad.

($n = 1$) $\mathcal{A}_1 = \mathcal{S}_1 = E$.

($n = 2$) $\mathcal{A}_2 = E$.

($n \geq 3$) $\mathcal{A}_n$ je netriviální normální podgrupa.

($n = 3$) $\mathcal{S}_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$ a $\mathcal{A}_3 = \{\mathrm{id}, (123), (132)\}$ má prvočíselný počet prvků a je jednoduchá.

($n = 4$) $\mathcal{A}_4$ má řád 12 a není jednoduchá, neboť obsahuje např. $\mathcal{K}_4 := \{\mathrm{id}, (12)(34), (13)(24), (23)(14)\}$ a platí $\mathcal{K}_4 \lhd \mathcal{A}_4$. Předně je $\mathcal{K}_4$ uzavřená na skládání, součin 2 se vždy zobrazí na třetí, např. $(12)(34) \cdot (13)(24) = (23)(14)$. A každá permutace je sama sobě inverzní, tedy $\mathcal{K}_4$ je grupa.

$\mathcal{K}_4$ jsou všechny $(ij)(k\ell)$, kde tato 4 čísla jsou různá. Ukážeme, že $\mathcal{K}_4$ je uzavřená vůči vnitřním automorfismům. $\alpha_\pi((ij)(k\ell)) = (\pi(i)\pi(j))(\pi(k)\pi(\ell))$, ale neboť π je bijekce, jsou to opět čísla $1, 2, 3, 4$, jenom případně přeházená.

$\mathcal{K}_4$ nazýváme Kleinova grupa (matracová grupa - podle otáčení matrace).

Všimněme si, že také $\mathcal{L}_2 := \{\mathrm{id}, (12)(34)\} \lhd \mathcal{K}_4$ (má polovinu prvků, tedy index rozkladu podle $\mathcal{L}_2$ je 2 a je normální). Ale $\mathcal{L}_2 \not\lhd \mathcal{A}_4$.

► 1.9.20. Věta. Alternující grupy $\mathcal{A}_n$ jsou pro $n \neq 4$ jednoduché (tedy nemají netriviální normální podgrupu).

○ *Důkaz.* Pro $n \leq 3$ jsme platnost ukázali v předchozím příkladě. Tedy nechť $n \geq 5$. Mějme libovolnou $H \lhd \mathcal{A}_n$, $H \neq E$. Ukážeme, že $H = \mathcal{A}_n$. Důkaz se rozpadá do 3 kroků.

(v H existuje 3cykl (u, v, w)) Vezměme $\pi \in H^\bullet$ takovou, která mění co nejmenší počet prvků a není identitou. Určitě není transpozice (ta je lichá). Sporem, nechť $\pi \neq (u, v, w)$. Pak rozklad na nezávislé cykly může vypadat následovně:

(1) $\pi = (pq)(rs)\cdots$. Pak existuje páté číslo, označme jej t.

(2) $\pi = (pqr\cdots)\cdots$ A mění ještě nejméně 2 další čísla s, t.

Mějme $\varrho := (rst) \in \mathcal{A}_n$ sudou permutaci. Pak $\alpha_\varrho(\pi) = \varrho\pi\varrho^{-1} \in H^\bullet$ (neboť H je normální). V prvním případě $\alpha_\varrho(\pi) = (pq)(st)\cdots \neq \pi$ a ve druhém $\alpha_\varrho(\pi) = (pqs)\cdots \neq \pi$. Definujeme $\sigma := \pi^{-1}(\varrho\pi\varrho^{-1}) \in H$ a není jednotková.

Ukážeme, že σ nechává na místě více prvků než π.

(2) Mějme libovolné $k \in \widehat{n}$ tak, že $\pi(k) = k$. Pak $k \notin \{p, q, r, s, t\}$ a $\varrho(k) = k$. Pak $\sigma(k) = k$, neboť žádná z permutací π, π^{-1}, ϱ a ϱ^{-1} nemění k. Ale $\pi(p) = q$ a $\sigma(p) = p$ TODO. Tedy σ mění nejméně o 1 méně čísel než π.

Obdobně pro (1). Tedy σ nechává na místě více čísel než π.

(je-li v H jeden 3cyklus (u, v, w), jsou tam všechny 3cykly) Zvolme libovolný 3cyklus (p, q, r). Položme $\pi := \left(\begin{smallmatrix} u & v & w & y & z \\ p & q & r & Y & Z \end{smallmatrix}\right)$. Nutně existují takové y, z, Y, Z, že π je sudá, tj. $\pi \in \mathcal{A}_n$. Potom $\alpha_\pi((u, v, w)) = (\pi(u), \pi(v), \pi(w)) = (p, q, r)$ a neboť H je normální, je $(p, q, r) \in H$.

(3cykly generují $\mathcal{A}_n$) Ukážeme, že součin π 2 libovolných transpozicí lze rozložit na 3cykly. Je-li $\pi = (p, q)(p, r) = (prq)$ je 3cyklus. Je-li $\pi = (p, q)(r, s) = (p, r, s)(p, q, s)$. Je-li $\pi = (p, q)(p, q) = (p, q, r)(r, q, p)$ pro libovolné r.

□

• 1.10. Kartézský a direktní součin grup

► 1.10.1. Definice. Mějme $G_1, \ldots, G_n$ grupy, $G_i = (M_i, \cdot)$. Označme $M := M_1 \times \cdots \times M_n$ a definujme operaci $\cdot\colon (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 b_1, \ldots, a_n b_n)$. Jednotkou bude $1_M = (1, \ldots, 1)$ a inverzním prvkem $(a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$. Grupu $G := (M, \cdot)$ nazýváme kartézský součin grup a značíme $G = \overset{n}{\underset{1}{\times}} G_i$..

► 1.10.2. Definice. Buďte G grupa a $A, B \Subset G$. Řekneme, že G je direktní součin podgrup A, B, je-li zobrazení $f : A \times B \to G$, $f(x, y) = xy$ izomorfismem grup. Značíme $G = A \odot B$.

► 1.10.3. Poznámka. Direktní součin lze přirozeně zobecnit na konečné i spočetné systémy podgrup.

► 1.10.4. Lemma. Zobrazení f z předchozí definice je homomorfismus právě tehdy, když $(\forall a \in A^\bullet, b \in B^\bullet)(ab = ba)$.

◦ *Důkaz.*

(⇒) $ab = f(\langle a, b\rangle) = f(\langle 1, b\rangle \langle a, 1\rangle) = f(1, b)f(a, 1) = ba$.

(⇐) $f(\langle a_1, b_1\rangle \langle a_2, b_2\rangle) = f(\langle a_1a_2, b_1b_2\rangle) = a_1a_2b_1b_2 = a_1b_1a_2b_2 = f(\langle a_1, b_1\rangle)f(\langle a_2, b_2\rangle)$.

□

► 1.10.5. Lemma. Zobrazení f z předchozí definice je „na“ právě tehdy, když $A^\bullet B^\bullet = G^\bullet$.

◦ *Důkaz.* $A^\bullet B^\bullet$ je z definice obor hodnot f. □

► 1.10.6. Lemma. Je-li f z předchozí definice homomorfismus, pak je f prostý právě tehdy, je-li $A^\bullet \cap B^\bullet = \{1\}$.

◦ *Důkaz.*

(⇒) Víme, že $\ker f = \{\langle 1, 1\rangle\}$. Nechť $c \in A \cap B$. Pak triviálně $c \in A$ a $c^{-1} \in B$ a $\langle c, c^{-1}\rangle \in A \times B$. A neboť $f(\langle c, c^{-1}\rangle) = cc^{-1} = 1$, je $\langle c, c^{-1}\rangle = \langle 1, 1\rangle$, tedy hlavně $c = 1$.

(⇐) Nechť $A^\bullet \cap B^\bullet = \{1\}$. Mějme libovolné $\langle a, b\rangle \in \ker f$. Pak $f(a, b) = ab = 1$, tedy $a = b^{-1}$ a nutně $a = b^{-1} \in A^\bullet \cap B^\bullet$ a tedy $a = b = 1$.

□

► 1.10.7. Věta. Platí $G = A \odot B$ právě tehdy, když platí:

(1) $(\forall a \in A^\bullet, b \in B^\bullet)(ab = ba)$;

(2) $A^\bullet B^\bullet = G^\bullet$;

(3) $A^\bullet \cap B^\bullet = \{1\}$.

► 1.10.8. Poznámka. V aditivní grupě používáme název direktní součet.

► 1.10.9. Věta. Je-li $G = A \odot B$, pak platí

(4) $A \lhd G$, $B \lhd G$;

(5) $AB = G$ (tedy A a B komutují);

(6) $(\forall x \in G^\bullet)(\exists_1 a \in A^\bullet, b \in B^\bullet)(x = ab = ba)$.

◦ *Důkaz.*

(4) Mějme $c \in G^\bullet$, $x \in A$, $y \in B$ a podle (2) je $c = ab$, $a \in A^\bullet$, $b \in B^\bullet$. Pak

$$\alpha_c(x) = cxc^{-1} = abxb^{-1}a^{-1} \overset{(1)}{=} axbb^{-1}a^{-1} = axa^{-1} \in A^\bullet$$

a

$$\alpha_c(y) = cyc^{-1} = a\overbrace{byb^{-1}}^{\in B^\bullet}a^{-1} = byb^{-1}aa^{-1} = byb^{-1} \in B^\bullet.$$

(5) Podle lemmatu o tečce je $G^\bullet = A^\bullet B^\bullet \subseteq (AB)^\bullet = G^\bullet$, tedy $AB = G$.

(6) Zobrazení f je bijekce, tedy existuje právě jedna dvojice a, b taková, že $f(a, b) = c$.

□

► 1.10.10. Věta. Buď G cyklická grupa řádu $p_1^{k_1} \cdots p_n^{k_n}$ – standardní rozklad na prvočísla. Pak $G = A_1 \odot \cdots \odot A_n$, kde A_i má řád p_i. (v roce 2010/2011 nedělal)

► 1.10.11. Příklad. Pro $Z_6 = Z / \equiv_6 = (\{0, 1, \ldots, 5\}, +)$ má řád $6 = 2 \cdot 3$ a lze ji napsat jako $Z_6 = A \oplus B$. Platí $A^\bullet = \{0, 3\}$ a $B^\bullet = \{0, 2, 4\}$.

► 1.10.12. Věta. Buď $G = A \odot B$. Pak $G / A \cong B$.

◦ *Důkaz.* Z věty o izomorfismu je $AB / A \cong B / A \cap B$, ale $AB = G$, $A \cap B = E$, tedy $B / E \cong B$, tedy $G / A \cong B$. □