Matematika IV – 2. přednáška
Základy teorie grup

Michal Bulant

Masarykova univerzita
Fakulta informatiky

25. 2. 2008

Obsah přednášky

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- *Předmětové záložky v IS MU*

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, *e*-text.
- *Předmětové záložky v IS MU*
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- Peter J. Cameron. *Introduction to algebra*, Oxford University Press, 2001, 295 s. (Dostupné v knihovně PřF).

Plán přednášky

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi
- **komutativní grupa** (grupoid, pologrupa, monoid apod.), je taková grupa (grupoid, ...), že operace $\cdot$ je komutativní. Často se v případě komutativních grup setkáte rovněž s pojmem **abelovská grupa**.

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi
- **komutativní grupa** (grupoid, pologrupa, monoid apod.), je taková grupa (grupoid, ...), že operace $\cdot$ je komutativní. Často se v případě komutativních grup setkáte rovněž s pojmem **abelovská grupa**.

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Opakování minulé přednášky

- **grupoid** $(G, \cdot)$ je množina G s binární operací $\cdot$
- **pologrupa** $(G, \cdot)$ je množina G s asociativní binární operací $\cdot$
- **monoid** $(G, \cdot)$ je pologrupa $(G, \cdot)$ s jednotkovým (neutrálním) prvkem[1]
- **grupa** $(G, \cdot)$ je monoid, ve kterém má každý prvek inverzi
- **komutativní grupa** (grupoid, pologrupa, monoid apod.), je taková grupa (grupoid, ...), že operace $\cdot$ je komutativní. Často se v případě komutativních grup setkáte rovněž s pojmem **abelovská grupa**.

Poznámka k nejednoznačnosti terminologie.

[1] Raději než jednotka používejme **jednotkový prvek** – důvod uvidíme později. Někdy se tomuto prvku rovněž říká jednička.

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií). Pro informatiky, kteří mají za sebou funkcionální programování (příp. prácí s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).
Pro informatiky, kteří mají za sebou funkcionální programování (příp. prácí s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.
Pro všechny *struktury* (pologrupy, grupy, okruhy, tělesa, svazy, atd.) lze definovat několik základních pojmů analogickým způsobem:

- **pod**struktury

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).
Pro informatiky, kteří mají za sebou funkcionální programování (příp. prácí s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.
Pro všechny *struktury* (pologrupy, grupy, okruhy, tělesa, svazy, atd.) lze definovat několik základních pojmů analogickým způsobem:

- **pod**struktury
- **homomorfismy** mezi strukturami stejného typu

Příliš stručná exkurze do univerzální algebry

Bystří studenti algebry si brzy povšimnou, že se mnohé pojmy a důkazy opakují pro různé situace. Skutečně se ukazuje, že základní pojmy a tvrzení je možné zavést a dokázat obecně pomocí univerzální algebry (příp. ještě obecněji v tzv. teorii kategorií).

Pro informatiky, kteří mají za sebou funkcionální programování (příp. prácí s objekty, metodami, šablonami apod.), by to možná mohl být přirozený postup, my však na to bohužel nemáme dostatek času.

Pro všechny *struktury* (pologrupy, grupy, okruhy, tělesa, svazy, atd.) lze definovat několik základních pojmů analogickým způsobem:

- **pod**struktury
- **homomorfismy** mezi strukturami stejného typu
- **součiny** struktur téhož typu

Podpologrupy a podgrupy

Definice

Je-li $(A, \cdot)$ grupa (případně pologrupa), pak její podmnožinu $B \subset A$, která je uzavřená vůči zúžení operace $\cdot$ a zároveň je spolu s touto operací grupou (resp. pologrupou) , nazýváme **podgrupa** (resp. podpologrupa) v $(A, \cdot)$.

Podpologrupy a podgrupy

Definice

Je-li $(A, \cdot)$ grupa (případně pologrupa), pak její podmnožinu $B \subset A$, která je uzavřená vůči zúžení operace $\cdot$ a zároveň je spolu s touto operací grupou (resp. pologrupou) , nazýváme **podgrupa** (resp. podpologrupa) v $(A, \cdot)$.

Definice

Zobrazení $f : (G, \cdot) \to (H, \circ)$ mezi dvěmi grupami $(G, \cdot)$ a $(H, \circ)$ se nazývá **homomorfismus grup**, jestliže respektuje násobení, tj. pro všechny prvky $a, b \in G$ platí

$$f(a \cdot b) = f(a) \circ f(b).$$

Povšimněme si, že násobení vlevo je uvnitř grupy G předtím, než zobrazujeme, zatímco vpravo jde o násobení v H poté, co zobrazujeme.

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e_G \in G$ je jednotka v H*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e_G \in G$ je jednotka v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e_G \in G$ je jednotka v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*
3. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e_G \in G$ je jednotka v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*
3. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
4. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e_G \in G$ je jednotka v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*
3. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
4. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e_G \in G$ je jednotka v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*
3. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
4. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
5. *je-li f zároveň bijekcí, pak i inverzní zobrazení f^{-1} je homomorfismus.*

Přímo z definice se snadno ověří následující vlastnosti homomorfismů:

Věta

Pro každý homomorfismus $f : G \to H$ grup platí

1. *obraz jednotky $e_G \in G$ je jednotka v H*
2. *obraz inverze k prvku je inverzí obrazu, tj. $f(a^{-1}) = f(a)^{-1}$.*
3. *obraz podgrupy $K \subset G$ je podgrupa $f(K) \subset H$.*
4. *vzorem $f^{-1}(K) \subset G$ podgrupy $K \subset H$ je podgrupa.*
5. *je-li f zároveň bijekcí, pak i inverzní zobrazení f^{-1} je homomorfismus.*
6. *f je injektivní zobrazení právě tehdy, když $f^{-1}(e_H) = \{e_G\}$.*

Definice

Podgrupa, která je vzorem jednotkového prvku $e \in H$ (tj. $f^{-1}(e)$) se nazývá **jádro** homomorfismu f a značíme ji $\ker f$. Bijektivní homomorfismus grup G a H nazýváme **izomorfismus** (a značíme $G \cong H$).

Poznámka

Podobně jako v teorii grafů jsou i v algebře izomorfní objekty nerozlišitelné.

Definice

Podgrupa, která je vzorem jednotkového prvku $e \in H$ (tj. $f^{-1}(e)$) se nazývá **jádro** homomorfismu f a značíme ji $\ker f$. Bijektivní homomorfismus grup G a H nazýváme **izomorfismus** (a značíme $G \cong H$).

Poznámka

Podobně jako v teorii grafů jsou i v algebře izomorfní objekty nerozlišitelné.

Z předchozích tvrzení okamžitě vyplývá, že homomorfismus $f : G \to H$ s triviálním jádrem je izomorfismem G **na** obraz $f(G)$.

Příklad

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\mathrm{sgn} : (\Sigma_n, \circ) \to (\mathbb{Z}_2, +)$ přiřazující permutaci její paritu (lichá=1, sudá=0). Jde o homomorfismus grup $(\Sigma_n, \circ)$ a $(\mathbb{Z}_2, +)$. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.

Příklad

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\operatorname{sgn} : (\Sigma_n, \circ) \to (\mathbb{Z}_2, +)$ přiřazující permutaci její paritu (lichá=1, sudá=0). Jde o homomorfismus grup $(\Sigma_n, \circ)$ a $(\mathbb{Z}_2, +)$. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.

(2) Grupa symetrií rovnostranného trojúhelníka D_6 je izomorfní s grupou permutací Σ_3. Stačí zvolit realizaci Σ_3 tak, že za množinu tří prvků pro permutace vezmeme vrcholy trojúhelníka a jednotlivým symetriím přiřadíme permutace těchto vrcholů, které vyvolají.

Příklad

(1) Pro každou grupu permutací $G = \Sigma_n$ jsme definovali zobrazení $\text{sgn} : (\Sigma_n, \circ) \to (\mathbb{Z}_2, +)$ přiřazující permutaci její paritu (lichá=1, sudá=0). Jde o homomorfismus grup $(\Sigma_n, \circ)$ a $(\mathbb{Z}_2, +)$. Jádrem tohoto homomorfismu jsou permutace se sudou paritou.
(2) Grupa symetrií rovnostranného trojúhelníka D_6 je izomorfní s grupou permutací Σ_3. Stačí zvolit realizaci Σ_3 tak, že za množinu tří prvků pro permutace vezmeme vrcholy trojúhelníka a jednotlivým symetriím přiřadíme permutace těchto vrcholů, které vyvolají.
(3) Zobrazení $\exp : \mathbb{R} \to \mathbb{R}_+$ (nebo $\mathbb{C} \to \mathbb{C} \setminus 0$), je homomorfismus aditivní grupy reálných nebo komplexních čísel na multiplikativní grupu kladných reálných čísel, resp. na multiplikativní grupu všech nenulových komplexních čísel. V případě reálných čísel jde o izomorfismus (co je jeho inverzí?). Pro komplexní čísla dostáváme netriviální jádro $\{2k\pi i;\ k \in \mathbb{Z}\}$.

Příklad

(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár z $\mathbb{K}$ (pracovali jsme s $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Cauchyova věta o determinantu součinu čtvercových matic $\det(A \cdot B) = (\det A) \cdot (\det B)$ je tvrzením, že pro grupu $G = GL(n, \mathbb{K})$ invertibilních matic je $\det : G \to \mathbb{K} \setminus \{0\}$ multiplikativním homomorfismem grup.

Příklad

(4) Determinant matice je zobrazením, které každé matici skalárů z $\mathbb{K}$ přiřazuje nějaký skalár z $\mathbb{K}$ (pracovali jsme s $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Cauchyova věta o determinantu součinu čtvercových matic $\det(A \cdot B) = (\det A) \cdot (\det B)$ je tvrzením, že pro grupu $G = GL(n, \mathbb{K})$ invertibilních matic je $\det : G \to \mathbb{K} \setminus \{0\}$ multiplikativním homomorfismem grup.
(5) Grupy zbytkových tříd $(\mathbb{Z}_k, +)$ jsou izomorfní grupám komplexních k–tých odmocnin z jedničky, což jsou zároveň izomorfní obrazy konečných grup otočení v rovině o celé násobky úhlu $\frac{2\pi}{k}$.
(6) Multiplikativní grupa invertibilních zbytkových tříd $(\mathbb{Z}_p^\times, \cdot)$ je izomorfní aditivní grupě $(Z_{p-1}, +)$ (plyne z cykličnosti grupy – později snad dokážeme).

(Přímý) součin grup

Definice

Pro každé dvě grupy $(G, \cdot)$, $(H, \circ)$ definujeme **součin grup** $(G \times H, *)$ takto: Jako množina je $G \times H$ skutečně (kartézský) součin, na kterém definujeme grupové násobení po složkách, tj. $(a, x) * (b, y) = (a \cdot b, x \circ y)$.

Poznámka

Rozmyslete si, že jde o grupu a že součin komutativních grup je zase komutativní!

(Přímý) součin grup

Definice

Pro každé dvě grupy $(G, \cdot)$, $(H, \circ)$ definujeme **součin grup** $(G \times H, *)$ takto: Jako množina je $G \times H$ skutečně (kartézský) součin, na kterém definujeme grupové násobení po složkách, tj. $(a, x) * (b, y) = (a \cdot b, x \circ y)$.

Poznámka

Rozmyslete si, že jde o grupu a že součin komutativních grup je zase komutativní!

Zobrazení

$$p_G : G \times H \ni (a, x) \mapsto a \in G, \;\; p_H : G \times H \ni (a, x) \mapsto x \in H$$

jsou surjektivní homomorfismy (tzv. **projekce**) s jádry

$$\ker p_G = \{(e_G, x);\;\; x \in H\} \qquad \ker p_H = \{(a, e_H); a \in G\}.$$

Příklad

(7) Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Toto lze nahlédnout buď geometrickou úvahou (prostřednictvím grup symetrií v rovině) nebo přímou konstrukcí izomorfismu.

Příklad

(7) Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_3$.
Toto lze nahlédnout buď geometrickou úvahou (prostřednictvím grup symetrií v rovině) nebo přímou konstrukcí izomorfismu.
V aditivní notaci vypadá izomorfismus takto:

$$\begin{aligned}
[0]_6 &\mapsto ([0]_2, [0]_3), \quad [1]_6 \mapsto ([1]_2, [2]_3) \\
[2]_6 &\mapsto ([0]_2, [1]_3), \quad [3]_6 \mapsto ([1]_2, [0]_3) \\
[4]_6 &\mapsto ([0]_2, [2]_3), \quad [5]_6 \mapsto ([1]_2, [1]_3)
\end{aligned}$$

Příklad

(7) Grupa $\mathbb{Z}_6$ je izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_3$.
Toto lze nahlédnout buď geometrickou úvahou (prostřednictvím grup symetrií v rovině) nebo přímou konstrukcí izomorfismu.
V aditivní notaci vypadá izomorfismus takto:

$$\begin{aligned} [0]_6 &\mapsto ([0]_2,[0]_3), & [1]_6 &\mapsto ([1]_2,[2]_3) \\ [2]_6 &\mapsto ([0]_2,[1]_3), & [3]_6 &\mapsto ([1]_2,[0]_3) \\ [4]_6 &\mapsto ([0]_2,[2]_3), & [5]_6 &\mapsto ([1]_2,[1]_3) \end{aligned}$$

(8) Dihedrální grupa D_8 (tj. grupa symetrií čtverce, $\langle r,s|r^4=1,s^2=1,srs=r^{-1}\rangle$) **není** izomorfní součinu $\mathbb{Z}_2 \times \mathbb{Z}_4$, přestože mají stejný počet prvků (D_8 není komutativní).

Čínská zbytková věta (Chinese remainder theorem)

Předchozí příklad je speciálním případem tzv. *Čínské zbytkové věty*.

Věta

Jsou-li k, m nesoudělná, pak

$$(\mathbb{Z}_{km}, +) \cong (\mathbb{Z}_k, +) \times (\mathbb{Z}_m, +).$$

Čínská zbytková věta (Chinese remainder theorem)

Předchozí příklad je speciálním případem tzv. *Čínské zbytkové věty*.

Věta

Jsou-li k, m nesoudělná, pak

$$(\mathbb{Z}_{km}, +) \cong (\mathbb{Z}_k, +) \times (\mathbb{Z}_m, +).$$

a obecněji

Věta

Jsou-li $m_1, m_2, \cdots, m_k$ po dvou nesoudělná, pak

$$(\mathbb{Z}_{\prod m_i}, +) \cong (\mathbb{Z}_{m_1}, +) \times (\mathbb{Z}_{m_2}, +) \times \cdots \times (\mathbb{Z}_{m_k}, +).$$

Tento izomorfismus se často s výhodou využívá k reprezentaci velkých čísel při distribuovaných výpočtech pracujících s dělitelností, kdy na každém počítači stačí pracovat s jedním (relativně malým) modulem.

Důkaz CRT:

Sestrojíme požadovaný izomorfismus f . Označme $m = \prod_i m_i$ a pro libovolné $[a]_m \in \mathbb{Z}_m$ položme $f([a]_m) = ([a]_{m_1}, \dots, [a]_{m_k})$. Snadno se ověří, že jde o injektivní homomorfismus (co je jádrem?).

[2] A nešlo by to ještě šikovněji? Pokud nám stačí existence izomorfismu, tak stačí využít toho, že injektivní zobrazení mezi množinami o stejném počtu

Důkaz CRT:

Sestrojíme požadovaný izomorfismus f . Označme $m = \prod_i m_i$ a pro libovolné $[a]_m \in \mathbb{Z}_m$ položme $f([a]_m) = ([a]_{m_1}, \dots, [a]_{m_k})$. Snadno se ověří, že jde o injektivní homomorfismus (co je jádrem?). Zbývá dokázat, že jde i o surjekci, tedy, že libovolný prvek

$$([a_1]_{m_1}, \dots, [a_k]_{m_k}) \in (\mathbb{Z}_{m_1}, +) \times \cdots \times (\mathbb{Z}_{m_k}, +)$$

je obrazem nějakého $a \in \mathbb{Z}_m$. To je ale totéž jako najít $a \in \mathbb{Z}$ takové, že $a \equiv a_1 \pmod{m_1}, \dots a \equiv a_k \pmod{m_k}$, což se udělá malým (ale šikovným) trikem:[2]

[2] A nešlo by to ještě šikovněji? Pokud nám stačí existence izomorfismu, tak stačí využít toho, že injektivní zobrazení mezi množinami o stejném počtu

Důkaz CRT:

Sestrojíme požadovaný izomorfismus f . Označme $m = \prod_i m_i$ a pro libovolné $[a]_m \in \mathbb{Z}_m$ položme $f([a]_m) = ([a]_{m_1}, \ldots, [a]_{m_k})$. Snadno se ověří, že jde o injektivní homomorfismus (co je jádrem?). Zbývá dokázat, že jde i o surjekci, tedy, že libovolný prvek

$$([a_1]_{m_1}, \ldots, [a_k]_{m_k}) \in (\mathbb{Z}_{m_1}, +) \times \cdots \times (\mathbb{Z}_{m_k}, +)$$

je obrazem nějakého $a \in \mathbb{Z}_m$. To je ale totéž jako najít $a \in \mathbb{Z}$ takové, že $a \equiv a_1 \pmod{m_1}, \ldots a \equiv a_k \pmod{m_k}$, což se udělá malým (ale šikovným) trikem:[2]

Pro libovolné $1 \leq i \leq k$ položme $n_i = m/m_i$ a protože $(m_i, n_i) = 1$ (zde jsme využili *nesoudělnost po dvou*), najdeme podle Bezoutovy věty u_i a v_i tak, že $u_i m_i + v_i n_i = 1$, tj. $v_i n_i \equiv 1 \pmod{m_i}$.

[2] A nešlo by to ještě šikovněji? Pokud nám stačí existence izomorfismu, tak stačí využít toho, že injektivní zobrazení mezi množinami o stejném počtu

Důkaz CRT:

Sestrojíme požadovaný izomorfismus f . Označme $m = \prod_i m_i$ a pro libovolné $[a]_m \in \mathbb{Z}_m$ položme $f([a]_m) = ([a]_{m_1}, \dots, [a]_{m_k})$.
Snadno se ověří, že jde o injektivní homomorfismus (co je jádrem?).
Zbývá dokázat, že jde i o surjekci, tedy, že libovolný prvek

$$([a_1]_{m_1}, \dots, [a_k]_{m_k}) \in (\mathbb{Z}_{m_1}, +) \times \cdots \times (\mathbb{Z}_{m_k}, +)$$

je obrazem nějakého $a \in \mathbb{Z}_m$. To je ale totéž jako najít $a \in \mathbb{Z}$ takové, že $a \equiv a_1 \pmod{m_1}, \dots a \equiv a_k \pmod{m_k}$, což se udělá malým (ale šikovným) trikem:[2]
Pro libovolné $1 \leq i \leq k$ položme $n_i = m/m_i$ a protože $(m_i, n_i) = 1$ (zde jsme využili *nesoudělnost po dvou*), najdeme podle Bezoutovy věty u_i a v_i tak, že $u_i m_i + v_i n_i = 1$, tj. $v_i n_i \equiv 1 \pmod{m_i}$.
Hledané a pak najdeme jako

$$a = \sum_i a_i v_i n_i.$$

[2] A nešlo by to ještě šikovněji? Pokud nám stačí existence izomorfismu, tak stačí využít toho, že injektivní zobrazení mezi množinami o stejném počtu

Cyklické grupy

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje[3].
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.

[3] Co znamenají ty mocniny?

Cyklické grupy

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje[3].
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.
Nejmenší k s touto vlastností nazýváme **řád prvku** a v G. Grupa G je **cyklická**, je-li celé G generované nějakým svým prvkem a výše uvedeným způsobem.

[3] Co znamenají ty mocniny?

Cyklické grupy

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje[3].
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.
Nejmenší k s touto vlastností nazýváme **řád prvku** a v G. Grupa G je **cyklická**, je-li celé G generované nějakým svým prvkem a výše uvedeným způsobem. Zjistit pro konkrétní cyklickou grupu generátor je obecně obtížný problém. I při znalosti generátoru $g \in G$ je ale obecně velkým problémem zjistit pro dané $a \in G$ číslo k, pro které $g^k = a$ (tzv. *problém diskrétního logaritmu* je základem mnoha kryptografických protokolů – ElGamal, Diffie-Hellman, DSA).

[3] Co znamenají ty mocniny?

Cyklické grupy

Libovolný prvek a v grupě G je obsažen v minimální podgrupě $\{e = a^0, a = a^1, a^2, a^3, \dots\}$, která jej obsahuje[3].
Je zjevné, že je tato podgrupa komutativní, a pokud je celá grupa G konečná, nutně musí jednou nastat případ $a^k = e$.
Nejmenší k s touto vlastností nazýváme **řád prvku** a v G. Grupa G je **cyklická**, je-li celé G generované nějakým svým prvkem a výše uvedeným způsobem. Zjistit pro konkrétní cyklickou grupu generátor je obecně obtížný problém. I při znalosti generátoru $g \in G$ je ale obecně velkým problémem zjistit pro dané $a \in G$ číslo k, pro které $g^k = a$ (tzv. *problém diskrétního logaritmu* je základem mnoha kryptografických protokolů – ElGamal, Diffie-Hellman, DSA). Z definice přímo vyplývá, že každá cyklická grupa je izomorfní buď grupě celých čísel $\mathbb{Z}$ (pokud je nekonečná) nebo některé grupě zbytkových tříd $\mathbb{Z}_k$ (když je konečná).

[3] Co znamenají ty mocniny?