Rozbor cvičného kurzu

Martin Holoubek (holoumar@fit.cvut.cz)

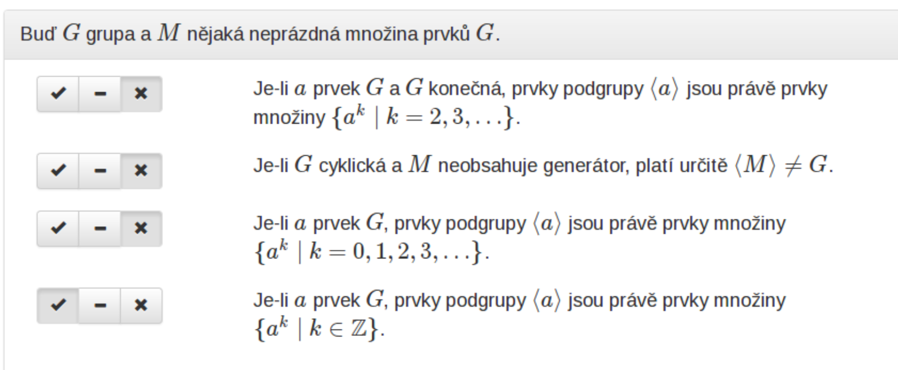
November 5, 2016

1 Prohlášení

Tento materiál je určen pouze ke studijním účelům, je založen na otázkách získaných ze serveru marast.fit.cvut.cz. Je možné, že od té doby došlo v systému ke změně. Pokud naleznete chybu, či sporné vysvětlení napište email a já materiál upravím.

Autor se tímto zbavuje zodpovědnosti za případné chyby. Všechny odpovědi jsou platné k datu 2.11.2016.

2 Otázka



Buď G grupa a M nějaká neprázdná množina prvků G.

Je-li a prvek G a G konečná, prvky podgrupy $\langle a \rangle$ jsou právě prvky množiny $\{a^k \mid k = 2, 3, \ldots\}$.

Je-li G cyklická a M neobsahuje generátor, platí určitě $\langle M \rangle \neq G$.

Je-li a prvek G, prvky podgrupy $\langle a \rangle$ jsou právě prvky množiny $\{a^k \mid k = 0, 1, 2, 3, \ldots\}$.

Je-li a prvek G, prvky podgrupy $\langle a \rangle$ jsou právě prvky množiny $\{a^k \mid k \in \mathbb{Z}\}$.

✗ ~~Tímto způsobem bychom nevygenerovali samotný prvek, ani inverze.~~

✓ Grupa je konečná, podgrupa je také konečná, vždy proto po dostatečném počtu kroků doiteruje až na začátek a proto nám nevadí chybějící indexy.

✗ Množina M může obsahovat více prvků, každý generuje část a ve výsledku celou grupu G

✗ Pokud by G byla cyklická a nekonečná a a její generátor, tak by generovaná množina neobsahovala inverze.

✓ Nyní už lze generovat všechny prvky až do ∞.

3 Otázka

S jakou operací tvoří množina $\{n \in \mathbb{Z} \mid n > 3\}$ monoid?

- $(n, m) \mapsto \min(n, m)$
- $(n, m) \mapsto n + m - 4$
- $(n, m) \mapsto n + m$
- $(n, m) \mapsto gcd(n, m)$

✗ Chybí neutrální prvek (globální maximum)

✓ Uzavřená je, asociativní také, a neutrální prvek je 4

✗ Chybí neutrální prvek (0)

✗ Není uzavřená, např. gdc(5, 7) je 1.

4 Otázka

Buďte G a H konečné grupy řádu n a f homomorfizmus G do H. Buď G cyklická a g její generátor.

- Grupy G a H jsou izomorfní, právě když je H cyklická.
- Jsou-li G a H cyklické, jsou izomorfní a existuje mezi nimi $\varphi(n)$ různých izomorfizmů (φ je Eulerova funkce.)
- Je-li f izomorfizmus, musí platit, že $f(g)$ je generátor H.
- Je-li $\langle f(g) \rangle$ vlastní podgrupa H, není f izomorfizmus.

✓ Tohle tvrzení platí na obě strany

✓ Ano platí, zafixujeme si generátor první grupy a počet generátorů té druhé je $\varphi(n)$.

✓ Ano, platí, že generátor se zobrazí na generátor

✓ Pokud by $\langle f(g) \rangle$ byla vlastní podgrupa, pak by tyto dvě grupy nemohly mít stejný řád, tzn. nemohl by mezi nimi existovat izomorfismus. Jiný pohled na věc je, že f zobrazí generátor na negenerující prvek, proto zobrazení nemůže být izomorfimus.

5 Otázka

Buď G grupa řádu $n \geq 2$.

- Je-li G cyklická a existuje-li v G právě jeden generátor, je n prvočíslo.
- Je-li G cyklická a a nějaký její prvek, pak jeho inverze je rovna prvku a^{n-1}.
- Je-li n prvočíslo, je G cyklická.
- Je-li G cyklická a a nějaký její generátor, je a^{-1} také generátor.

✓ Platí, je-li a generátor, pak každá mocnina nesoudělná s řádem grupy je generátorem. Pokud je řád prvočíslo, pak neexistuje soudělná mocnina.

Také platí, že je-li prvek generátor, jeho inverze je také generátor, proto musí platí, že $a = a^{-1}$, protože ale platí $a^2 = e$, tak víme, že grupa má minimálně jeden a maximálně dva elementy, to jsou prvočísla.

✓ V cyklické grupě platí, že $a^n = e$ a také existují inverze. $a^{n-1}a = e$ a to je definice inv. prvku.

✓ Víme, že grupa obsahuje pouze triviální podgrupy. To proto, že řád podgrupy dělí řád grupy. Každý prvek, který není e tvoří generátor celé grupy, protože žádná podgrupa nemůže existovat. Kromě triviální.

✓ V cyklické grupě platí, že inverze generátoru je generátor.

6 Otázka

Buď $(M, \oplus)$ struktura s jednou operací, kde $M = \{(a_1, a_2, a_3) \mid a_1, a_2, a_3 \in \{0, 1\}\}$, $\oplus_2$ je jiné značení pro operaci XOR a $\oplus$ je definováno následovně:

$$(a_1, a_2, a_3) \oplus (b_1, b_2, b_3) = (a_1 \oplus_2 b_1 \oplus_2 1, a_2 \oplus_2 b_2, a_3 \oplus_2 b_3).$$

Tato struktura je konečnou grupou.

Tato struktura je monoidem, ve kterém existuje inverze k prvku $(0, 0, 0)$.

Tato struktura je monoidem s neutrálním prvkem $(0, 0, 0)$.

Tato struktura je komutativní grupou.

✓ Ano je, operace na první souřadnici je XNOR, zbytek je XOR

✓ Ano, inverze je $(0, 0, 0)$

✗ Ne, neutrální prvek je $(1, 0, 0)$

✓ Ano, na poředí operací nazáleží.

7 Otázka

Buďte p a q prvočísla, u polynom stupně m ireducibilní nad $\mathbb{Z}_p$ a v polynom stupně n ireducibilní nad $\mathbb{Z}_q$. Označme těleso GF(p^m) s násobením modulo u jako T a těleso GF(q^n) s násobením modulo v jako S.

Multiplikativní grupa tělesa T je cyklická, právě když je m prvočíslo.

Jsou-li aditivní grupy těles T a S izomorfní, jsou izomorfní i tělesa T a S.

Jsou-li multiplikativní grupy těles T a S izomorfní, jsou izomorfní i tělesa T a S.

Jsou-li S a T izomorfní, musí být polynomy u a v totožné.

✗ Multiplikativita nezávisí na exponentu m, ale na základu p, který musí být prvočíselný.

✓ Izomorfismus aditivních grup platí, jen pokud jsou stejného řádu. Potom jsou stejného řádu i tělesa. Každá dvě tělesa stejného řádu jsou izomorfní.

✓ Stejné jako v předchozím případě.

✗ Tělesa jsou izomorfní pro libovolné polynomy.

8 Otázka

Které z následujících výroků jsou pravdivé? Symboly $+$, $-$ a $\cdot$ značí klasické aritmetické operace.

- $(\mathbb{Z} \setminus \{0\}, \cdot)$ je podgrupa grupy $(\mathbb{R} \setminus \{0\}, \cdot)$.
- Grupa $(\mathbb{R} \setminus \{0\}, \cdot)$ má nekonečně mnoho konečných podgrup.
- Grupa $(\mathbb{Z}, +)$ má pouze jedinou konečnou podgrupu.
- Existuje grupa řádu 11, která má tři různé podgrupy.

✗ Chybí inverze

✗ Má právě jednu konečnou podgrupu

✓ Její množinou je $\{0\}$

✗ 11 je prvočíslo a řád podgrupy dělí řád grupy. Tato grupa má pouze 2 triviální podgrupy.

9 Otázka

Buďte p prvočíslo a u ireducibilní polynom z okruhu $\mathbb{Z}_p[x]$ stupně $m > 1$. Označme těleso GF(p^m) s násobením modulo polynom u jako T.

- Multiplikativní grupa tělesa T má řád $p^m - 1$.
- Cyklické netriviální podgrupy aditivní grupy T mají všechny řád p.
- Každá vlastní podgrupa aditivní grupy T je cyklická.
- Aditivní grupa tělesa T je cyklická, pouze pokud je m prvočíslo.

✓ Ano, je to počet možných variací bez nulového polynomu

✓ Jde o klasickou grupu $\mathbb{Z}_p^+$

✗ Sice existují cyklické vlastní podgrupy, ale nejsou to všechny. Protipříklad např. v $GF(2^3)$ si vezmeme podgrupu $\{00, 01, 10, 11\}$

✗ ~~Aditivní grupa tělesa nikdy není cyklická.~~ Aditivní grupa je cyklická, pokud je její řád prvočíslo. U GF je to ale vždy mocnina prvočísla, proto u GF cyklická není.

10 Otázka

Které z následujících zobrazení je homomorfismem z grupy $(M, \cdot)$ do grupy $(\mathbb{R} \setminus \{0\}, \cdot)$? V grupě $(M, \cdot)$ je M je množina všech horních trojúhelníkových matic rozměru 1000×1000 a $\cdot$ je maticové násobení.

- $(a_{i,j})_{i,j \leq 1000} \mapsto \sum_{i \leq 1000} a_{i,i}$ (Zobrazení provede součet diagonály)
- $A \mapsto 3 \cdot \det(A)$ pro $A \in M$
- $(a_{i,j})_{i,j \leq 1000} \mapsto a_{5,1}$ (Zobrazení vybírá z matice hodnotu na poli "5,1", tedy $a_{5,1}$)
- $A \mapsto |\det(A)|$ pro $A \in M$

✗ $f(A \circ B) \neq f(A) \circ f(B) \leftrightarrow \sum_{i=1}^{1000} A_{i,i} B_{i,i} \neq \sum_{i=1}^{1000} A_{i,i} \sum_{i=1}^{1000} B_{i,i}$

✗ Ne, $3 * det(A \circ B) \neq 3 * det(A) \circ 3 * det(B)$

✗ Matice je horní trojúhelníková a zobrazení bere prvek $A_{5,1} = 0$. A zároveň platí, že součin horních trojúhelníkových matic je horní. troj. matice. Proto má i výsledná matice v pozici $(5, 1)$ nulu. Přesto je to špatně, protože nula není prvkem cílové grupy.

✓ Ano, platí, že $det(A * B) = det(A) * det(B)$

11 Otázka

Který prvek je generátorem grupy $\mathbb{Z}_{26}^{\times}$?

- $a = 15$
- $a = 2$
- $a = 3$
- $a = 5$

✓ Grupa má řád $\phi(26) = 12$, jejími prvky jsou pouze čísla nesoudělná s 26. Jinak by bylo možné najít kombinaci, která by vedla na nulu. Obsahuje čísla $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$. Víme, že řád podgrupy dělí řád grupy, možné řády podgrup jsou $\{1, 2, 3, 4, 6, 12\}$. Platí, že prvek grupy na její řád je neutrální prvek e. Proto zkoušíme potenciální generátory umocňovat na maximální řády podgrup a když dostaneme jedničku až pro číslo 12, víme, že je to generátor celé grupy.

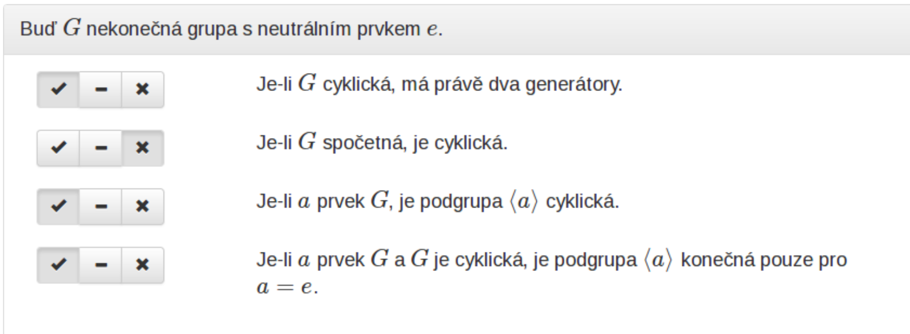
$|15^4|_{26} = 3$
$|15^6|_{26} = 25 = -1$
$|15^{12}|_{26} = |25^2|_{26} = |-1^2|_{26} = 1$

✗ $|2^4|_{26} = 16$
$|2^6|_{26} = 12$
$|2^{12}|_{26} = 14$

✗ $|3^4|_{26} = 3$
$|3^6|_{26} = 1$

✗ $|5^4|_{26} = 1$

12 Otázka



Buď G nekonečná grupa s neutrálním prvkem e.

Je-li G cyklická, má právě dva generátory.

Je-li G spočetná, je cyklická.

Je-li a prvek G, je podgrupa $\langle a \rangle$ cyklická.

Je-li a prvek G a G je cyklická, je podgrupa $\langle a \rangle$ konečná pouze pro $a = e$.

- ✓ Pokud je cyklická, pak má generátor, zároveň je generátorem i inverze. Předpokládejme dva různé generátory a a b. Pak $a = b^n$ a $b = a^m$, $a = b^n = (a^m)^n = a^{mn}$. V celých číslech a nekonečné grupě má tato rovnice pro m a n dvě řešení 1 a -1. Toto je přímý důkaz pro existenci přesně dvou generátorů
- ✗ Stačí si představit multiplikativní grupu $\langle\{2, 3\}\rangle$. Je generována ze spočené množiny, proto je spočetná. Přesto nemá jeden generátor, proto není cyklická.
- ✓ Máme jeden element, který generuje grupu, proto je to generátor.
- ✓ Podgrupa bude mít tvar $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$, pro každý prvek kromě e vidíme, že množina bude nekonečná, protože jinak nikdy nedoiteruje k nulovému prvku.

13 Otázka

Nechť $+$ a $\cdot$ značí klasické sčítání a násobení reálných čísel.

- Neexistuje konečná podmnožina $\mathbb{R}$ taková, že $(M, +, \cdot)$ je těleso.
- Množina $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ tvoří těleso.
- $(\mathbb{Z}, +, \cdot)$ je těleso.
- $(\{0, 1\}, +, \cdot)$ je těleso.

✓ S klasickým sčítáním a násobením by jakákoliv podmnožina $\mathbb{R}$ nebyla uzavřená. Případně víme, že nejmenší těleso je $\mathbb{Q}$.

✓ Ano, množina je uzavřená, operace je asociativní, neutrálním prvkem je $\{0\}$ pro sčítání a $\{1\}$ pro násobení, aditivní inverze existují intuitivně.

Inverze pro násobení:
$(a + b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$
Oba koeficienty jsou z $\mathbb{Q}$ a tvar odpovídá prvkům grupy, proto ke každému prvku existuje inverze. Pro nulu ($a == b$) rovnice nedává smysl, ale to nevadí, protože z multiplikativní je nula vyjmuta.

× Od podhledu v $\mathbb{Z}$ chybí inverze v multiplikativní grupě.

× Množina není uzavřena na sčítání.

14 Otázka

Uvažujme grupu $\mathbb{Z}_n^\times$, φ zančí Eulerovu funkci.

- Je-li tato grupa cyklická, má $\varphi(n)$ generátorů.
- Je-li n rovno prvočíslu 263, je prvek 87 generátor.
- Tato grupa je cyklická, pouze když je n prvočíslo.
- Je-li n rovno prvočíslu 263, je prvek 68 generátor.

✗ Ne číslo $\varphi(n)$ odpovídá řádu grupy, počet generátorů je $\varphi(\varphi(n))$.

✓ Řád grupy je 262, rozklad je $\{1, 2, 131, 262\}$

$|87^2|_{263} = 205$
$|87^{131}|_{263} = 262 = |-1|_{263}$
$|87^{262}|_{263} = 1$

✗ Ne, multiplikativní grupa je cyklická pro $n \in \{2, 4, p^k, 2p^k\} : k \in \mathbb{Z}_0^+$

✗ Ne

$|68^2|_{263} = 153$
$|68^{161}|_{263} = 1$

15 Otázka

Buďte p prvočíslo a u polynom z okruhu $\mathbb{Z}_p[x]$ stupně $m > 1$. Označme $M \subset \mathbb{Z}_p[x]$ množinu všech polynomů stupně ostře menšího než m.

- Množina M s operací sčítání polynomů (z okruhu $\mathbb{Z}_p[x]$) tvoří grupu.
- Není-li u ireducibilní, tvoří množina M s operací násobení polynomů (z okruhu $\mathbb{Z}_p[x]$) modulo polynom u pologrupu.
- Počet prvků M je p^m.
- Není-li u ireducibilní, tvoří množina M s operací násobení polynomů (z okruhu $\mathbb{Z}_p[x]$) modulo polynom u monoid.

✓ Ano, tvrzení obecně platí.

✗ Ne, množina není uzavřená. Nyní obsahuje i polynomy, které jsou soudělné s polynomem. Tzn. neobsahuje pouze zbytky po dělení, ale i "něco navíc".

✓ Ano, je to počet variací

✗ Ne, množina není uzavřená. Nyní obsahuje i polynomy, které jsou soudělné s polynomem. Tzn. neobsahuje pouze zbytky po dělení, ale i "něco navíc".

16 Otázka

Nechť $+$ a $\cdot$ značí klasické sčítání a násobení reálných čísel.

- Buď $M \subset \mathbb{R}$ taková, že $(M, +, \cdot)$ je okruh, potom $\mathbb{Z} \subset M$.
- $(\{0\}, +, \cdot)$ je okruh.
- $(\{0, 1\}, +, \cdot)$ je okruh.
- $(\mathbb{Z}, +, \cdot)$ je okruh.

✗ Ne, existují i menší okrumy. Tzn. jejich podmnožinou není nutně $\mathbb{Z}$.

✓ Ano, množina je uzavřena na obě operace a dvojice splňuje požadované vlastnosti.

✗ Ne, množina není uzavřena na sčítání.

✓ Ano, množina splňuje požadované vlastnosti. To, že neexistují inverze pro ~~sčítání~~ násobení nevadí.

17 Otázka

Uvažujme grupu $\mathbb{Z}_{331}^{\times}$ (331 je prvočíslo).

- Prvek 85 je generátor.
- Prvek 55 je generátor.
- Tato grupa má 4 různé netriviální podgrupy.
- Tato grupa má 14 různých netriviálních podgrup.

✗ Ne, není.

✓ Ano, je.

✗ Zvláštní formulace.. člověk by řekl, že grupa, co má 14 podgrup má i 4. logicky.. chybí mi tam slovo právě.

✓ Platí, že konečná grupa má právě jednu podgrupu daného řádu, které dělí řád grupy. Řád grupy dělí čísla:

$$M = \{1, 2, 3, 5, 6, 10, 11, 15, 22, 33, 30, 55, 66, 110, 165, 330\}$$

$|M| = 16$, celkem je proto 14 různých netriviálních podgrup

18 Otázka

Buď G cyklická grupa řádu $n \in \mathbb{N}$, g nějaký její generátor a H nějaká její vlastní podgrupa.

- Grupa H nemusí být cyklická.
- Buď q nejmenší přirozené číslo takové, že $g^q \in H$, potom g^q je generátor H.
- Generátor g nemůže být prvkem H.
- Je-li k nesoudělné s n, platí $g^k \notin H$.

✗ Ne, každá podgrupa cyklické grupy je také cyklická

✓ Ano, toto tvrzení jsme dokazovali na přednášce.

✓ Ano, pokud by g byl generátor G a zároveň byl prvkem H, muselo by platit, že $G \subseteq H$, ale to je ve sporu s tím, že H je vlastní grupa ($H \subset G$).

✓ Ano, protože je-li k nesoudělné s n, tak je také generátorem G, proto nemůže být prvkem vlastní podgrupy.

19 Otázka

Buďte G a H konečné grupy řádů m resp. n a f homomorfizmus G do H.

- Je-li H vlastní podgrupa G, je f izomorfizmus.
- Je-li f prosté, je f^{-1} homomorfizmus H do G.
- Je-li f bijekce, platí $m = n$.
- Je-li f prosté, je G izomorfní s nějakou podgrupou H.

✗ Pokud je H vlastní podgrupa, tak má menší řád, proto nemůžou být izomorfní.

✗ Homoforfismus $f : G \to H$ musí být definován pro $\forall x \in G$. I když je zobrazení prosté, tak mohou existovat prvky H, které nikdy nebudou obrazem žádného prvku z G. Proto inverzní zobrazení sice bude surjektivní, ale nebude definováno pro $\forall x \in H$, což odporuje definici totálního zobrazení.

✓ Ano, pokud má být zobrazení injektivní a surjektivní, musí být mohutnosti obou množin stejné.

✓ Ano, pokud platí $(\forall x, y \in G : x \neq y) \to f(x) \neq f(y)$, tak jistě existuje podmnožina H, ke které existuje inverzní zobrazení, tj. izomorfismus. Zároveň platí, že homomorfismus vždy zobrazí grupu na grupu.