Algebra — cvičení 10, řešení

V řešeních níže nebudeme obvykle explicitně zmiňovat použití Lagrangeovy věty. Když se zaobíráme možnými řády prvků v konečných grupách, užíváme tuto větu prakticky neustále.

1. (c) Najděte všechny generátory grupy $\mathbb{Z}_{11}^*$. Z přednášky víme, že $\mathbb{Z}_{11}^*$ je cyklická grupa, izomorfní s $\mathbb{Z}_{10}$. Nejprve zkusmo hledáme nějaký generátor grupy $\mathbb{Z}_{11}^*$. Začneme s prvkem 2. V $\mathbb{Z}_{11}^*$ dostáváme $2^2 = 4$ a $2^5 = 10$, takže 2 nemá řád ani 2, ani 5; dle Lagrangeovy věty proto musí mít řád 10, a tedy generuje grupu $\mathbb{Z}_{11}^*$.

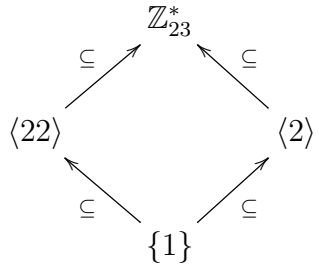
Grupa $\mathbb{Z}_{10}$ má čtyři generátory (neboť $\varphi(10) = 4$); stejné to musí být s grupou $\mathbb{Z}_{11}^*$, která je jí izomorfní. Jak jsme ukazovali na cvičení on-line, nalezením generátoru 2 grupy $\mathbb{Z}_{11}^*$ jsme mimo jiné také ukázali, že zobrazení $f : \mathbb{Z}_{10} \to \mathbb{Z}_{11}^*$, kde $f(n) = 2^n \mod 11$, je izomorfismus. Jelikož generátory grupy $\mathbb{Z}_{10}$ jsou $1, 3, 7, 9$, dostáváme, že generátory grupy $\mathbb{Z}_{11}^*$ jsou právě $2, 2^3 = 8, 2^7 = 7$ a $2^9 = 6$.

Alternativně lze místo izomorfismu f užít i vylučovací metodu. Víme, že 1 a $10 = -1$ nejsou generátory (coby prvky řádu 1, resp. 2). Dále všechny prvky řádu 5 leží v podgrupě $\langle 2^2 \rangle_{\mathbb{Z}_{11}^*} = \{1, 4, 5, 9, 3\}$, zbývají proto $2, 6, 7, 8$.

3. Napište všechny podgrupy zadané grupy. Jak jsou podgrupy uspořádány inkluzí?

(c) $\mathbb{Z}_{23}^*$;
(d) $\mathbb{Z}_{17}^*$.

Obě zadané grupy jsou cyklické, první z nich má 22 prvků, druhá 16. Začneme případem (c). Z věty o podgrupách cyklických grup víme, že $\mathbb{Z}_{23}^*$ má coby vlastní podgrupy pouze jednu dvouprvkovou a jednu 11prvkovou. Prvek řádu 2 je vždy $-1 = 22$. Spočteme-li $2^{11} = (2^5)^2 \cdot 2 = 9^2 \cdot 2 = 24 = 1$, vidíme, že 2 má řád 11. Všechny podgrupy grupy $\mathbb{Z}_{23}^*$ včetně upořádání inkluzí jsou na obrázku níže.



Co se týče grupy $\mathbb{Z}_{17}^*$, tam jsou všechny podrgupy uspořádány lineárně (opět využíváme větu o podgrupách cyklických grup): triviální je obsažena v dvouprvkové (generované prvkem 16), ta dále ve čtyřprvkové (generované prvkem 4), ta dále v osmiprvkové (generované prvkem 2) a ta nakonec v celé grupě $\mathbb{Z}_{17}^*$.

4. Rozložte dané grupy na direktní součin co nejvíce netriviálních cyklických grup:

(a) $\mathbb{Z}_{18}$;
(c) $\mathbb{Z}_{21}^*$.

Máme $\mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$, což už je hledaný rozklad. Dále $\mathbb{Z}_{21}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Druhý izomorfismus plyne z $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, který máme třeba z (důkazu) Čínské zbytkové věty. Co se prvního izomorfismu týče, grupa $\mathbb{Z}_{21}^*$ má řád $\varphi(21) = 12$, obsahuje prvek 2, který má řád 6, a prvek 20 (řádu 2), pro nějž $20 \notin \langle 2 \rangle_{\mathbb{Z}_{21}^*}$; je tudíž $\langle 2, 20 \rangle_{\mathbb{Z}_{21}^*} = \mathbb{Z}_{21}^*$. Můžeme proto definovat homomorfismus $f : \mathbb{Z}_2 \times \mathbb{Z}_6 \to \mathbb{Z}_{21}^*$ vztahem $f(1, 0) = 20$ a $f(0, 1) = 2$. Jelikož $2, 20 \in \mathrm{Im}(f)$, je $\mathrm{Im}(f) = \mathbb{Z}_{21}^*$. Homomorfismus f je tedy surjektivním homomorfismem mezi 12prvkovými grupami. Jako takový musí být rovněž prostý.

Kratší možnost odvození 1. izomorfismu je (z ČZV): $\mathbb{Z}_{21}^* \cong (\mathbb{Z}_3 \times \mathbb{Z}_7)^* = \mathbb{Z}_3^* \times \mathbb{Z}_7^* \cong \mathbb{Z}_2 \times \mathbb{Z}_6$.

5. Rozhodněte, zda jsou následující grupy cyklické:

(b) $\mathbf{A}_3$;
(c) $\mathbb{Z}_{12}^*$;
(d) $\mathbb{Z}_{14}^*$.

Grupa $\mathbf{A}_3$ je 3prvková, a tedy cyklická. Grupa $\mathbb{Z}_{12}^*$ má $\varphi(12) = 4$ prvky, konkrétně $1, 5, 7, 11$. Všechny ovšem mají řád 1 nebo 2, nejedná se proto o cyklickou grupu.

Nakonec, grupa $\mathbb{Z}_{14}^*$ má $\varphi(14) = 6$ prvků, konkrétně $1, 3, 5, 9, 11, 13$. Jelikož $3^2 = 9$ a $3^3 = 27 = -1$, má prvek 3 řád 6, a proto generuje cyklickou grupu $\mathbb{Z}_{14}^*$.

6. Najděte všechny homomorfismy

(a) ze $\mathbb{Z}_7^*$ do $\mathbb{Z}_8$;
(b) ze $\mathbb{Z}_{11}$ do $\mathbb{Z}_{2021}$.

Případ (b) má coby řešení pouze nulový homomorfismus, jelikož $\mathrm{NSD}(11, 2021) = 1$. Každý homomorfismus v případu (a) je jednoznačně určen obrazem generátoru šestiprvkové grupy $\mathbb{Z}_7^*$, což — jak se snadno ověří — je například prvek 3. Obrazem prvku 3 (který má řád 6) při homomorfismu ovšem může být pouze prvek řádu dělícího 6. V (aditivní) grupě $\mathbb{Z}_8$ se jedná pouze o prvky 0 a 4 řádů 1, resp. 2. Kromě nulového homomorfismu máme tedy ještě právě jeden další, konkrétně $f : \mathbb{Z}_7^* \to \mathbb{Z}_8$, kde $f(3^n) = 4$ pro lichá $n \in \mathbb{Z}_6$ a $f(3^n) = 0$ pro sudá $n \in \mathbb{Z}_6$.

7. Buď $T = \mathbb{Z}_3[\alpha]/(\alpha^2+1)$. Najděte generátor grupy T^*. Kolik má tato grupa generátorů celkem? Polynom $\alpha^2 + 1$ je ireducibilní nad $\mathbb{Z}_3[\alpha]$. Víme tedy, že T je 9prvkové těleso a T^* je cyklická 8prvková grupa. Je proto izomorfní grupě $\mathbb{Z}_8$ a má právě $\varphi(8) = 4$ generátory. Jeden z nich je kupříkladu prvek $\alpha + 1$, jelikož v T^* máme $(\alpha + 1)^2 = 2\alpha$ a $(\alpha + 1)^4 = (2\alpha)^2 = 2$.

8. Pro jaká $m, n \in \mathbb{N}$ je grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ cyklická?

Jsou-li m, n nesoudělná, máme z (důkazu) Čínské zbytkové věty $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, pročež je zadaná grupa cyklická.

Pokud naopak $\mathrm{NSD}(m, n) > 1$, pak $N := \mathrm{NSN}(m, n) < mn$, a zřejmě pro libovolné $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ platí $\underbrace{(a, b) + \cdots + (a, b)}_{N\times} = 0$. Všechny prvky v grupě $\mathbb{Z}_m \times \mathbb{Z}_n$ tím pádem mají řád nejvýše N, a tato grupa proto není cyklická.

9. Ukažte, že pro komutativní okruh R nemůže mít grupa R^* pět prvků. Sporem: nechť R^* je 5prvková. Pak $R^* = \{1, a, a^2, a^3, a^4\}$ pro nějaké pevné $a \in R$. Jelikož $-1 \in R^*$, nesmí být -1 řádu 2, a proto $-1 = 1$. Jinak řečeno v R platí $1 + 1 = 0$ (tj. R má charakteristiku 2), a v důsledku potom $r + r = r(1 + 1) = 0$ pro všechna $r \in R$.

Pokud máme dojít ke sporu, měli bychom se pokusit objevit nějaký další invertibilní prvek. Kde ho ale vzít? O chování prvků mimo R^* toho moc nevíme. Budeme proto zkoušet sčítat různé kombinace prvků z R^* a zjišťovat, nejsou-li tyto prvky invertibilní.

Například pro $b := 1 + a + a^4$ máme $b^2 = 1 + a^2 + a^8 = 1 + a^2 + a^3$. Dále ovšem

$$b^3 = (1 + a + a^4)(1 + a^2 + a^3) = 1 + a^2 + a^3 + a + a^3 + a^4 + a^4 + a + a^2 = 1.$$

Musí proto být $b \in R^*$, a z Lagrangeovy věty dokonce dostaneme $b = 1$. To by ale znamenalo, že $a + a^4 = 0$, a tedy $a^4 = -a = a$, což je spor s předpokladem, že a, a^4 jsou dva různé prvky v pětiprvkové grupě R^*.