Algebra

MB104 - jaro 2011

1 Cvičení 1: Teorie čísel

Teorie: V prvním cvičení se budeme zabývat teorií čísel. Vše, co se naučíme, budeme využívat i v dalších cvičeních, proto je důležité porozumět základním pojmům. Ze střední školy byste již měli znát pojmy jako dělitelnost, největší společný dělitel, nejmenší společný násobek. Pro osvěžení si uveďme jejich definice.

Definice 1. Nechť $a, b \in \mathbb{Z}$. Řekneme, že celé číslo a dělí celé číslo b, píšeme $a|b$, jestliže existuje $k \in \mathbb{Z}$ tak, že $b = a \cdot k$.

S dělitelností souvisí věta o dělení celých čísel se zbytkem. Tuto větu považujeme za zcela zřejmou. V tomto předmětu si však ukážeme, že ne ve všech okruzích platí.

Věta 1 (O dělení celých čísel se zbytkem)**.** *Nechť $a, b \in \mathbb{Z}$. Potom existují $q, r \in \mathbb{Z}$ taková, že $a = b \cdot q + r$, kde $0 \leq r < |b|$.*

Definice 2. Nechť $a, b \in \mathbb{Z}$. Řekneme, že celé číslo d je největším společným dělitelem čísel a, b, píšeme $d = (a, b)$, jestliže platí dvě podmínky

1. $d|a,\ d|b$
2. Pokud existuje celé číslo c takové, že $c|a,\ c|b$, potom $c|d$.

Největší společný dělitel jste na střední škole určovali Euklidovým algoritmem. Toho budeme využívat i v našem předmětu. S největším společným dělitelem úzce souvisí Bezoutova identita.

Věta 2 (Bezoutova)**.** *Nechť $a, b \in \mathbb{Z}$. Potom existují celá čísla m, n taková, že $am + bn = (a, b)$.*

Definice 3. Nechť $a, b \in \mathbb{Z}$. Řekneme, že celé číslo n je nejmenším společným násobkem čísel a, b, píšeme $n = [a, b]$, jestliže platí dvě podmínky

1. $a|n,\ b|n$
2. Pokud existuje celé číslo m takové, že $a|m,\ b|m$, potom $n|m$.

Nyní se již dostáváme k pojmu kongruence. Tento pojem zřejmě neslyšíte poprvé. Využívali jste ho jistě už v Úvodu do Informatiky či Automatech a gramatikách.

Definujme tedy, kdy jsou spolu dvě celá čísla kongruentní modulo nějaké přirozené číslo.

Definice 4. Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Řekneme, že $a \equiv b \pmod{m}$, jestliže a i b dávají stejný zbytek po dělení m.

S definicí kongruence se můžete setkat v několika různých podobách, jak nám říká následující věta.

Věta 3. *Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Potom následující podmínky jsou spolu ekvivalentní:*

1. $a \equiv b \pmod{m}$
2. $m|(a-b)$
3. *Existuje celé číslo k takové, že $a = k \cdot m + b$*

To, jak můžeme s kongruencemi pracovat, nám poví následující věta.

Věta 4. *Nechť $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$. Nechť $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$. Potom platí*

1. $a + c \equiv b + d \pmod{m}$
2. $a \cdot c \equiv b \cdot d \pmod{m}$

Dále můžeme obě strany kongruence umocnit na stejné přirozené číslo, vynásobit stejným nenulovým celým číslem. Ovšem **pozor**, nemůžeme obě strany kongruence dělit.

Věta 5 (Malá Fermatova věta)**.** *Nechť $a \in \mathbb{Z}$, p je prvočíslo takové, že $(a, p) = 1$. Potom*

$$a^{p-1} \equiv 1 \pmod{m}.$$

Relace kongruence modulo přirozené číslo m je relací ekvivalence na množině celých čísel. Uvažme nyní rozklad příslušný této ekvivalenci. Jednotlivým třídám tohoto rozkladu říkámě zbytkové třídy modulo m.

Obsahuje-li zbytková třída modulo m celé číslo a, potom ji značíme $[a]_m$. Zbytkové třídy můžeme sčítat a násobit pomocí reprezentantů. Řekneme, že zbytková třída $[b]_m$ je inverzní ke zbytkové třídě $[a]_m$, jestliže $[a]_m \cdot [b]_m = [1]_m$. K výpočtu inverzních tříd využíváme Euklidova algoritmu.

Nyní si řekneme, co je to eulerova funkce.

Definice 5. Funkci $\varphi : \mathbb{N} \to \mathbb{N}$, která každému přirozenému číslu n přiřadí počet přirozených čísel, které jsou menší nebo rovny n a jsou s n nesoudělné, říkáme Eulerova funkce.

To, jak se hodnota Eulerovy funkce počítá, nám řekne další tvrzení.

Věta 6. *Nechť a, b jsou dvě **nesoudělná** přirozená čísla a nechť $n = p_1^{e_1} \cdot \cdots \cdot p_k^{e_k}$ je rozklad přirozeného čísla n na součin prvočísel. Potom*

1. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
2. $\varphi(n) = (p_1 - 1)p_1^{e_1 - 1} \cdot \cdots \cdot (p_k - 1)p_k^{e_k - 1}$

Věta 7 (Eulerova věta)**.** *Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$ takové, že $(a, m) = 1$. Potom*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Definice 6. Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$. Řekneme, že řád celého čísla a modulo m je n, jestliže n je nejmenší přirozené číslo takové, že $a^n \equiv 1 \pmod{m}$.

Pro řád daného čísla a modulo m platí, že dělí každé takové číslo k, pro které je $a^k \equiv 1 \pmod{m}$.

Příklad 1. Určete podíl q a zbytek r po dělení čísla a číslem b

1. $a = -47,\ b = 11$
2. $a = -47,\ b = -11$
3. $a = 47,\ b = -11$
4. $a = n^3 - 1,\ b = n + 1,\ n \in \mathbb{N}$

Výsledek.

1. $a = -5, b = 8$
2. $a = 5, b = 8$
3. $a = -4, b = 3$
4. $a = n^2 - n, b = n - 1$

Příklad 2. Určete největší společný dělitel čísel a, b a určete příslušné koeficienty v Bezoutově rovnosti

1. $a = 21,\ b = 98$
2. $a = 10175,\ b = 2277$

Výsledek.

1. $7 = 5 \cdot 21 + (-1) \cdot 98$
2. $11 = (-32) \cdot 10175 + 143 \cdot 2277$

Příklad 3. Nechť $a \in \mathbb{Z}$. Dokažte, že

1. a^2 dává po dělení čtyřmi zbytek 0 nebo 1.
2. a^4 dává po dělení osmi zbytek 0 nebo 1.

Řešení.

1. Uvažujme $a = 2k + 1$ a $a = 2k$. Po umocnění dostáváme požadované tvrzení.
2. Použijeme výsledek předchozího příkladu, tedy uvažujme $a^2 = 4k + 1$ a $a^2 = 4k$. Opět po umocnění dostaneme požadované tvrzení.

Příklad 4. Určete všechna celá čísla x tak, aby

1. $4x \equiv 1 \pmod 7$
2. $7x \equiv 3 \pmod{11}$

Výsledek.

1. $x \equiv 2 \pmod 7$
2. $x \equiv 2 \pmod{11}$

Příklad 5. Určete inverzní zbytkové třídy k zadaným zbytkovým třídám

1. $[67]_{517}$
2. $[172]_{235}$
3. $[116]_{153}$
4. $[49]_{226}$

Výsledek.

1. $[463]_{517}$
2. $[138]_{235}$
3. $[62]_{153}$
4. $[143]_{226}$

Příklad 6. Určete

1. $\varphi(2010)$
2. $\varphi(1212)$

Výsledek.

1. 528
2. 400

Příklad 7. Určete všechna přirozená čísla n taková, že

1. $\varphi(n) = 6$
2. $\varphi(n) = 20$
3. $\varphi(n) = 11$

Výsledek.

1. $7, 9, 14, 18$
2. $25, 33, 44, 50, 66$
3. žádné neexistuje

Příklad 8. Určete všechna dvojciferná přirozená čísla n taková, že $9|\varphi(n)$

Výsledek. $19, 27, 37, 38, 54, 57, 63, 73, 74, 76, 81, 91, 95$

Příklad 9. Určete všechna přirozená čísla n taková, že

1. $\varphi(n) = \frac{n}{2}$
2. $\varphi(n) = \frac{n}{3}$

Nápověda: Napište n jako součin mocniny dvou (resp. tří) a čísla s dvojkou (resp. trojkou) nesoudělného.

Výsledek.

1. $n = 2^k$
2. $n = 2^k \cdot 3^l$

Příklad 10. Dokažte, že

1. je číslo $2^{60} + 7^{30}$ dělitelné 13.
2. pro libovolné $n \in \mathbb{N}$ je číslo $72^{2n+2} - 47^{2n} + 28^{2n-1}$ dělitelné číslem 25.

Příklad 11. Řešte soustavu kongruencí:

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 8 \pmod{11} \end{aligned}$$

Výsledek. $x \equiv 8 \pmod{55}$

Příklad 12. Řešte soustavu kongruencí:

$$\begin{aligned} 4x &\equiv 3 \pmod 7 \\ 5x &\equiv 4 \pmod 6 \end{aligned}$$

Výsledek. Nemá řešení.

Příklad 13. Určete zbytek po dělení čísla $2^{50} + 3^{50} + 4^{50}$ číslem 17.

Výsledek. 12

Příklad 14. Určete poslední cifru čísla

1. $3^{5^{7^9}}$
2. $37^{37^{37}}$

Výsledek.

1. 3
2. 7

Příklad 15. Určete poslední dvě cifry čísla

1. 7^{9^9}
2. $14^{14^{14}}$

Výsledek.

1. 07
2. 36

Příklad 16. Určete zbytek po dělení čísla $5^{33} + 7^{33}$ číslem 17.

Výsledek. 12

Příklad 17. Určete zbytek po dělení čísla $2^{181} + 3^{181} + 5^{181}$ číslem 37.

Výsledek. 10

Příklad 18. Dokažte, že je pro každé přirozené číslo n číslo $37^{n+2} + 16^{n+1} + 23^n$ dělitelné sedmi.

Příklad 19. Určete řád čísla 5 modulo 13.

Výsledek. 4

Příklad 20. Určete všechna přirozená čísla n, pro která je číslo $3^n + 4^n - 5^n$ dělitelné jedenácti.

Výsledek. $n \equiv 2 \pmod 5$

2 Cvičení 2: Základy teorie grup

Teorie: V tomto cvičení se budeme zabývat základními algebraickými strukturami. Na úvod několik základních pojmů:

Definice 7. Nechť G je libovolná neprázdná množina. Binární operací na množině G rozumíme libovolné zobrazení $\circledast : G \times G \to G$.

Dohodněme se, že místo $\circledast(a, b)$ budeme psát $a \circledast b$.

Definice 8. Řekneme, že je operace $\circledast$ komutativní na množině G, jestliže pro libovolné $a, b \in G$ platí $a \circledast b = b \circledast a$.

Nyní se dostáváme k sérii definic základních algebraických struktur jako je grupoid, pologrupa, monoid a grupa.

Definice 9. Libovolnou neprázdnou množinu s operací na této množině nazýváme grupoid.

Například tedy $(\mathbb{N}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Z}_5, +)$, $(\mathbb{C}, \cdot)$ jsou grupoidy. Naopak $(\mathbb{N}, -)$, $(\mathbb{N}, :)$ grupoidy nejsou.

Definice 10. Grupoid $(G, \circledast)$ nazýváme pologrupa, jestliže pro libovolné $a, b, c \in G$ platí, že $a \circledast (b \circledast c) = (a \circledast b) \circledast c$.

Například tedy $(\mathbb{N}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Z}_5, +)$, $(\mathbb{C}, \cdot)$ jsou pologrupy, ale $(\mathbb{N}, -)$, $(\mathbb{Z}, -)$ pologrupy nejsou.

Definice 11. Nechť $(G, \circledast)$ je pologrupa. Řekneme, že prvek $e \in G$ je neutrální prvek v pologrupě G, jestliže pro libovolné $a \in G$ platí

$$\begin{aligned} a \circledast e &= a \\ e \circledast a &= a \end{aligned}$$

Například $1 + 0i$ je neutrálním prvkem v pologrupě $(\mathbb{C}, \cdot)$, 0 je neutrálním prvkem v pologrupě $(\mathbb{Z}, +)$, $[0]_5$ je neutrálním prvkem v pologrupě $(\mathbb{Z}_5, +)$.

Pro počet neutrálních prvků v dané pologrupě platí následující tvrzení:

Věta 8. *V libovolné pologrupě existuje nejvýše jeden neutrální prvek.*

Definice 12. Pologrupu s neutrálním prvkem nazýváme monoid.

Definice 13. Nechť je dána pologrupa $(G, \circledast)$ s neutrálním prvkem e. Řekneme, že prvek $b \in G$ je inverzní (opačný) k prvku $a \in G$, jestliže platí:

$$\begin{aligned} a \circledast b &= e \\ b \circledast a &= e \end{aligned}$$

Definice 14. Monoid, ve kterém ke každému prvku existuje prvek inverzní, nazýváme grupa.

Například $(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Z}_7, +)$ jsou grupy. Oproti tomu $(\mathbb{R}, \cdot)$, $(\mathbb{Z}, \cdot)$ grupy nejsou.

Dále se můžeme podívat na podmnožiny grup. Pokud je sama podmnožina grupou, říkáme, že tvoří podgrupu dané grupy. Některé vlastnosti zdědí každá podmnožina (asociativitu, komutativitu), proto nemusíme pro podgrupy dokazovat všechny podmínky grupy.

Věta 9. *Nechť $(G, *)$ je grupa a nechť $\emptyset \neq H \subseteq G$. Potom H je podgrupa grupy G, jestliže platí*

1. *pro všechny $a, b \in H$ platí, že $a + b \in H$*
2. *pro všechny $a \in H$ platí, že $a^{-1} \in H$*

Příklad 21. Uveďte příklad:

1. Konečné komutativní grupy
2. Konečné nekomutativní grupy
3. Nekonečné komutativní grupy
4. Nekonečné nekomutativní grupy
5. Konečné komutativní pologrupy, která nebude monoidem.
6. Pětiprvkové komutativní grupy
7. Nekonečného monoidu, který nebude grupou

Řešení.

1. $(\mathbb{Z}_5, +)$
2. $(\mathbb{S}_3, \circ)$
3. $(\mathbb{Z}, +)$

4. Množina všech regulárních matic spolu s násobením
5. $(\{a, b\}, \circledast)$, kde $a \circledast b = a$, $a \circledast a = a$, $b \circledast b = a$, $b \circledast a = a$.
6. $(\mathbb{Z}_5, +)$
7. $(\mathbb{Z}, \cdot)$

Příklad 22. Rozhodněte, zda daná množina $\mathbb{Z}$ tvoří spolu s operací $\heartsuit$ (komutativní) grupoid, (komutativní) pologrupu, (komutativní) monoid, (komutativní) grupu:

1. $a \heartsuit b = (a, b)$
2. $a \heartsuit b = a^{|}b|$
3. $a \heartsuit b = 2a + b$
4. $a \heartsuit b = |a|$
5. $a \heartsuit b = a + b + a \cdot b$
6. $a \heartsuit b = a + b - a \cdot b$
7. $a \heartsuit b = a + (-1)^a b$

Výsledek.

1. Daná množina s operací tvoří komutativní pologrupu, která není monoidem.
2. Daná množina s operací tvoří nekomutativní grupoid, který není pologrupou.
3. Daná množina tvoří nekomutativní grupoid, který není pologrupou.
4. Daná množina tvoří nekomutativní pologrupu, která nemá neutrální prvek.
5. Daná množina tvoří komutativní monoid, který není grupou.
6. Daná množina tvoří komutativní monoid, který není grupou.
7. Daná množina tvoří nekomutativní grupu.

Příklad 23. Rozhodněte, zda množina $G = \mathbb{R} \setminus \{0\} \times \mathbb{R}$ s operací $\triangle$ tvoří grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní, jestliže je operace $\triangle$ definována takto: $(x, y) \triangle (u, v) = (xu, xv + y)$, pro libovolná $(x, y), (u, v) \in G$.

Výsledek. Jedná se o nekomutativní grupu.

Příklad 24. Nechť X je libovolná množina. Nechť $\mathcal{P}(X)$ značí systém všech podmnožin množiny X. Určete, zda množina $\mathcal{P}(X)$ tvoří s danou operací grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní.

1. průnik množin
2. sjednocení množin
3. symetrický rozdíl množin

Výsledek. Je-li množina X prázdná, potom tvoří $\mathcal{P}(X)$ se všemi operacemi komutativní grupu. V ostatních případech

1. S operací průnik tvoří daná množina komutativní pologrupu s neutrálním prvkem.
2. S operací sjednocení tvoří daná množina komutativní pologrupu s neutrálním prvkem.
3. S operací symetrický rozdíl tvoří daná množina komutativní grupu.

Příklad 25. Rozhodněte, zda podmnožina G komplexních čísel tvoří spolu s operací násobení komplexních čísel grupoid, pologrupu, pologrupu s neutrálním prvkem (monoid), grupu a zda je zadaná operace komutativní.

1. $G = \{a + bi \mid a, b \in \mathbb{Z}\}$
2. $G = \{a + bi \mid a, b \in \mathbb{R}, a^2 + b^2 = 1\}$
3. $G = \{a + b \cdot \sqrt{5} \mid a, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}$

Výsledek.

1. G tvoří monoid
2. G tvoří komutativní grupu
3. G tvoří komutativní grupu

Příklad 26. Dokažte, že v každé grupě o sudém počtu prvků existuje prvek, který je sám sobě inverzním a přesto to není neutrální prvek.

Řešení. Seřaďme prvky dané grupy do dvojic, přičemž ve dvojici bude vždy prvek a jeho inverze. Sám potom zůstane neutrální prvek. To je však celkem lichý počet prvků.

Příklad 27. Určete, kolika způsoby lze doplnit tabulka tak, aby $(\{a, b, c\}, \circledast)$ byl

1. grupoid
2. komutativní grupoid
3. grupoid s neutrálním prvkem
4. pologrupa s neutrálním prvkem
5. grupa

$\divideontimes$	a	b	c
a	c	b	a
b			b
c			

Výsledek.

1. 3^5
2. 9
3. 9
4. 1
5. 0

Příklad 28. Doplňte tabulku tak, aby $(\{a, b, c\}, \divideontimes)$ byla pologrupa.

$\divideontimes$	a	b	c
a	b	a	c
b			
c			

Příklad 29. Doplňte tabulku tak, aby $(\{a, b, c\}, \divideontimes)$ byla grupa.

$\divideontimes$	a	b	c
a			
b	c	a	
c			

Příklad 30. Nechť $(G, \circ)$ je grupa, nechť $a \in G$ je libovolný pevný prvek. Definujme na G operaci $\heartsuit$ následovně: $x \heartsuit y = x \circ a \circ y$ pro libovolné $x, y \in G$. Dokažte, že $(G, \heartsuit)$ tvoří grupu.

Příklad 31. Uveďte příklad:

1. Dvou disjunktních podgrup grupy $\mathbb{Z}$.
2. Dvou různých podgrup grupy $\mathbb{Z}$.

3. Grupy, která má právě jednu podgrupu.
4. Podgrupy $\mathbb{C}^*$, která má 17 prvků.
5. Čtyř různých podgrup grupy $\mathbb{Z}$, které obsahují číslo 45.

Příklad 32. Popište všechny podgrupy grupy $\mathbb{Z}_{30}$ a nakreslete, jak jsou v sobě vnořeny.

Výsledek. Je jich celkem 8.

Příklad 33. Dokažte, že $H = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ tvoří podgrupu grupy $(\mathbb{R}, +)$.

Příklad 34. Dokažte, že $H = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$ tvoří podgrupu grupy $(\mathbb{C}, +)$.

Příklad 35. Dokažte, že $H = \{c \in \mathbb{C} \mid |c| = 1\}$ tvoří podgrupu grupy $(\mathbb{C}^*, \cdot)$.

Příklad 36. Popište všechny konečné podgrupy grupy $(\mathbb{R}^*, \cdot)$

Výsledek. Dvě podgrupy: $\{1\}, \{-1, 1\}$.

Příklad 37. Dokažte, že průnikem dvou podgrup grupy G je opět podgrupa grupy G.

Příklad 38. Označme $Mat_n(T)$ množinu všech čtvercových matic řádu n s koeficienty z množiny T. Dokažte, že $G = (Mat_2(\mathbb{R}), +)$ tvoří komutativní grupu a rozhodněte, zda množina H tvoří podgrupu grupy G:

1. $H = Mat_2(\mathbb{Z})$
2. $H = Mat_2(\mathbb{N}_0)$
3. $H = \left\{ \begin{pmatrix} 0 & a \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$
4. $H = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$
5. $H = \left\{ \begin{pmatrix} b & a \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$

Výsledek.

1. Ano
2. Ne
3. Ano
4. Ne
5. Ano

Příklad 39. Označme $\mathcal{GL}_n(\mathbb{R})$ množinu všech regulárních čtvercových matic s reálnými koeficienty. Dokažte, že $G = \mathcal{GL}_2(\mathbb{R})$ tvoří grupu a rozhodněte, zda množina H tvoří podgrupu grupy G:

1. $H = \mathcal{GL}_2(\mathbb{Q})$
2. $H = \mathcal{GL}_2(\mathbb{Z})$
3. $H = \{A \in \mathcal{GL}_2(\mathbb{Z}) \mid |A| = 1\}$
4. $H = \left\{ \begin{pmatrix} 0 & a \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$
5. $H = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \mid a \in \mathbb{Z} \right\}$
6. $H = \left\{ \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$
7. $H = \left\{ \begin{pmatrix} 0 & a \\ b & c \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$
8. $H = \left\{ \begin{pmatrix} 1 & a \\ b & c \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$

Výsledek.

1. Ano
2. Ne
3. Ano
4. Ne
5. Ano
6. Ano
7. Ne
8. Ano

Příklad 40.

1. Rozhodněte, zda množina $H = \{a \in \mathbb{R}^* \mid a^2 \in \mathbb{Q}\}$ tvoří podgrupu grupy $(\mathbb{R}^*, \cdot)$
2. Rozhodněte, zda množina $H = \{a \in \mathbb{R} \mid a^2 \in \mathbb{Q}\}$ tvoří podgrupu grupy $(\mathbb{R}, +)$

Výsledek.

1. Ano
2. Ne

Příklad 41. Nechť G je komutativní grupa. Označme $H = \{g \in G \mid g^2 = e_G\}$. Dokažte, že H tvoří podgrupu grupy G a zdůvodněte, proč je důležitá komutativita grupy G.

3 Cvičení 3: Grupa permutací a podgrupy generované množinou

Teorie: V tomto cvičení se budeme zabývat permutacemi. Na závěr si ještě ukážeme několik příkladů na podgrupy generované danou množinou.

Definice 15. Libovolné bijektivní zobrazení na konečné neprázdné množině nazýváme permutace.

BÚNO můžeme předpokládat danou konečnou množinu ve tvaru $\{1, 2, \ldots, n\}$.

Díky tomu, že složením dvou bijekcí je opět bijekce, můžeme dané permutace skládat. Skládání zobrazení je navíc asociativní. Dále identické zobrazení je zřejmě také permutace a chová se jako neutrální prvek vzhledem ke skládání permutací. Navíc ke každému bijektivnímu zobrazení existuje zobrazení inverzní, které je také bijekcí. Odvodili jsme tak, že množina všech permutací na konečné neprázdné množině tvoří grupu.

Permutaci můžeme zadat několika způsoby:

1. Obrazem každého prvku, tzv. dvouřádkovým zápisem
2. Jako součin nezávislých cyklů (až na pořadí jednoznačný zápis)
3. Jako součin transpozic (nejednoznačný zápis)

Dále můžeme definovat tzv. grupu symetrií. Jedná se o množinu shodných zobrazení, které nechají daný útvar na místě.

V minulém cvičení jsme si dokázali, že průnikem podgrup je podgrupa. Můžeme tedy pro libovolnou podmnožinu dané grupy definovat podgrupu generovanou danou množinou jako průnik všech podgrup obsahujících danou množinu.

Příklad 42. Jsou dány permutace ρ, σ

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 6 & 5 & 7 & 8 \end{pmatrix}, \ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 4 & 2 & 3 & 8 & 6 & 7 \end{pmatrix}.$$

1. Zapište permutace ρ, σ jako součin nezávislých cyklů.
2. Rozložte permutace ρ, σ na součin transpozic a podle počtu transpozic určete jejich paritu.
3. Určete počet inverzí permutací ρ, σ a podle počtu inverzí určete jejich paritu.
4. Určete $\sigma \circ \rho$ a $\rho \circ \sigma$.

5. Určete σ^{-1}.
6. Určete ρ^{2011} a σ^{2011}.
7. Určete $(\rho^{-6} \circ \sigma^3)^{77}$.
8. Určete permutaci π tak, aby $\sigma \circ \pi = \rho$.

Příklad 43. Jsou dány permutace ρ, σ

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 2 & 5 & 7 & 6 & 1 & 3 \end{pmatrix}, \ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 7 & 1 & 6 & 4 & 3 \end{pmatrix}.$$

1. Zapište permutace ρ, σ jako součin nezávislých cyklů.
2. Rozložte permutace ρ, σ na součin transpozic a podle počtu transpozic určete jejich paritu.
3. Určete počet inverzí permutací ρ, σ a podle počtu inverzí určete jejich paritu.
4. Určete $\sigma \circ \rho$ a $\rho \circ \sigma$.
5. Určete σ^{-1}.
6. Určete ρ^{2010} a σ^{2010}.
7. Určete $(\rho^{-77} \circ \sigma^{81})^{-2}$.
8. Určete permutaci π tak, aby $\sigma^2 \circ \pi = \rho^3$.

Příklad 44. Jsou dány permutace $f, g \in \mathbb{S}_6$, $f = (5, 8, 7, 6) \circ (1, 4, 2)$, $g = (1, 5, 2, 6) \circ (2, 4, 7, 9, 5)$. Určete f^{-1}, g^{21}, $(f^{11} \circ g^{-3})^{20}$. Rozložte f na součin transpozic a určete počet transpozic této permutace.

Příklad 45. Určete všechny permutace $\pi \in \mathbb{S}_7$ tak, aby

1. $\pi^4 = (1, 2, 3, 4, 5, 6, 7)$
2. $\pi^2 = (1, 2, 3) \circ (4, 5, 6)$
3. $\pi^2 = (1, 2, 3, 4)$

Výsledek.

1. $(1, 3, 5, 7, 2, 4, 6)$
2. $(1, 3, 2) \circ (4, 6, 5), (1, 4, 2, 5, 3, 6), (1, 5, 2, 6, 3, 4), (1, 6, 2, 4, 3, 5)$

3. Neexistuje

Příklad 46. Určete všechny permutace $\rho \in \mathbb{S}_9$ taková, že

$$(\rho \circ (1,2,3))^2 \circ (\rho \circ (2,3,4))^2 = (1,2,3,4).$$

Řešení. Žádná taková neexistuje, na levé straně je totiž vždy sudá permutace, na pravé straně je permutace lichá.

Příklad 47. Určete všechny permutace $\rho \in \mathbb{S}_9$ taková, že

$$\rho^2 \circ (1,2) \circ \rho^2 = (1,2) \circ \rho^2 \circ (1,2).$$

Řešení. Žádná taková neexistuje, opět díky paritě.

Příklad 48. Určete znaménka daných permutací

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3n-2 & 3n-1 & 3n \\ 2 & 3 & 1 & 5 & 6 & 4 & \dots & 3n-1 & 3n & 3n-2 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & \dots & 2n \\ 2 & 4 & 6 & \dots & 2n & 1 & 3 & \dots & 2n-1 \end{pmatrix}$

Výsledek.

1. 1
2. $(-1)^{\frac{n\cdot(n-1)}{2}}$

Příklad 49. Napište permutace $f = (2,3,4,5)\circ(1,3,6,8)$ a $g = (1,4,6)\circ(2,7,4,8,3)\circ(1,5)$ jako součin 10 transpozic.

Příklad 50. Popište grupu symetrií čtverce a určete všechny její podgrupy.

Příklad 51. Určete podgrupu grupy $\mathbb{S}_6$ generovanou množinou M

1. $M = \{(1,2,4,5)\}$
2. $M = \{(1,2),(5,6)\}$
3. $M = \{(1,2)\circ(4,5),(1,2)\}$
4. $M = (1,2)(3,4),(2,3)(4,5).$
5. $M = \{(1,2,3),(4,5)\}.$
6. $M = \{(1,2)\circ(3,4),\circ(5,6),(24)\}$

Příklad 52. Popište podgrupu grupy G generovanou množinou M

1. $G = \mathbb{Z}$, $M = \{36, 42\}$
2. $G = \{\mathbb{Z}_{30}\}$, $M = \{[15]_{30}, [21]_{30}\}$
3. $G = \mathbb{C}^*$, $M = \{-i\}$
4. $G = \mathbb{C}^*$, $M = \{\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\}$
5. $G = \mathbb{Z}_{12}^{\times}$, $M = \{[5]_{12}\}$
6. $G = \mathbb{Z}_{18}^{\times}$, $M = \{[7]_{18}\}$

Příklad 53. V grupě $\mathcal{GL}_2(\mathbb{Z}_2)$ určete podgrupu generovanou množinou M.

1. $M = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$
2. $M = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$

4 Cvičení 4: Homomorfismy a další vlastnosti grup

Teorie: Nyní se budeme zabývat zobrazeními mezi grupami. Budeme navíc požadovat, aby toto zobrazení zachovávalo danou operaci. Je proto důležité rozumět pojmům jako injektivní zobrazení, surjektivní zobrazení a umět obě vlastnosti dokazovat.

Definice 16. Nechť $(G, *)$, $(H, \odot)$ jsou grupy. Řekneme, že zobrazení $\varphi : G \to H$ je homomorfismus, jestliže pro všechna $a, b \in G$ platí, že

$$\varphi(a * b) = \varphi(a) \odot \varphi(b).$$

Je-li navíc toto zobrazení injektivní, mluvíme o injektivním homomorfismu (neboli o vnoření). Je-li surjektivní, říkáme danému zobrazení surjektivní homomorfismus. Jedná-li se o bijektivní homomorfismus, potom mluvíme o izomorfismu grup, nebo též říkáme, že dané grupy jsou izomorfní.

Definice 17. Nechť $(G, *)$, $(H, \odot)$ jsou grupy, $\varphi : G \to H$ homomorfismus. Potom množinu $\operatorname{Ker} \varphi = \{g \in G \mid \varphi(g) = e_H\}$ nazýváme jádro homomorfismu φ.

Jádro homomorfismu je podgrupa grupy G (ověřte si) a má důležitou vlastnost:

Věta 10. *Nechť $(G, *)$, $(H, \odot)$ jsou grupy, $\varphi : G \to H$ homomorfismus. Potom φ je injektivní (vnoření) právě tehdy, když* $\operatorname{Ker} \varphi = \{e_G\}$.

Definice 18. Nechť $(G, *)$, $(H, \odot)$ jsou grupy, $\varphi : G \to H$ homomorfismus. Potom množinu $\operatorname{Im} \varphi = \{h \in H \mid \exists g \in G : \varphi(g) = h\}$ nazýváme obraz homomorfismu φ.

Obraz homomorfismu je podgrupa grupy H (opět si prosím ověřte) a má také důležitou vlastnost:

Věta 11. *Nechť $(G, *)$, $(H, \odot)$ jsou grupy, $\varphi : G \to H$ homomorfismus. Potom φ je surjektivní právě tehdy, když* $\operatorname{Im} \varphi = H$.

Na závěr povídání o algebraických strukturách s jednou operací si uveďme ještě několik důležitých pojmů a vlastností.

Definice 19. Řekneme, že je grupa cyklická, jestliže je generovaná nějakým svým prvkem.

Definice 20. Počet prvků konečné grupy budeme nazývat řád dané grupy.

Definice 21. Nechť G je grupa, $a \in G$. Potom nejmenší přirozené číslo n takové, že $a^n = e_G$, nazýváme řád prvku a v grupě G. Pokud takové přirozené číslo neexistuje, říkáme, že daný prvek je řádu nekonečno.

Pro řád prvku a grupy platí řada zajímavých tvrzení. My si uveďme jen dvě:

Věta 12. *Řád libovolného prvku konečné grupy dělí řád celé grupy.*

Věta 13. *Řád libovolné podgrupy dané konečné grupy dělí řád celé grupy.*

Příklad 54. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi(([a]_4, [b]_3)) = [a - b]_{12}$
2. $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi(([a]_4, [b]_3)) = [6a + 4b]_{12}$
3. $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$, $\varphi(([a]_4, [b]_3)) = [0]_{12}$

Výsledek.

1. Není zobrazení
2. Je homomorfismus, který není ani injektivní ani surjektivní
3. Je homomorfismus, který není ani injektivní ani surjektivní

Příklad 55. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*$, $\varphi\left(\frac{p}{q}\right) = \frac{q}{p}$
2. $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*$, $\varphi\left(\frac{p}{q}\right) = \frac{p^2}{q^2}$
3. $\varphi : \mathbb{Q}^* \to \mathbb{Q}^*$, $\varphi\left(\frac{p}{q}\right) = \frac{p^2+q^2}{pq}$

Výsledek.

1. Je izomorfismus
2. Je homomorfismus, který není surjektivní ani injektivní.
3. Není homomorfismus

Příklad 56. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*$, $\varphi([a]_4) = i^a$
2. $\varphi : \mathbb{Z}_5 \to \mathbb{C}^*$, $\varphi([a]_4) = i^a$
3. $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*$, $\varphi([a]_4) = (-i)^a$
4. $\varphi : \mathbb{Z} \to \mathbb{C}^*$, $\varphi(a) = i^a$

Výsledek.

1. Je homomorfismus, který není injektivní ani surjektivní.
2. Není zobrazení.
3. Je homomorfismus, který není injektivní ani surjektivní.
4. Je homomorfismus, který není ani injektivní ani surjektivní.

Příklad 57. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*$, $\varphi(A) = |A|$
2. $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*$, $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a^2 + b^2$.
3. $\varphi : \mathcal{GL}_2(\mathbb{R}) \to \mathbb{R}^*$, $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ac + bd$.

Výsledek.

1. Je surjektivní homomorfismus, který není injektivní.
2. Není homomorfismus.
3. Není homomorfismus.

Příklad 58. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z} \to \mathbb{Z}_3$, $\varphi(a) = [a]_3$
2. $\varphi : \mathbb{Z} \to \mathbb{Z}_3$, $\varphi(a) = [|a|]_3$
3. $\varphi : \mathbb{Z} \to \mathbb{Z}_2$, $\varphi(a) = [a]_2$

4. $\varphi : \mathbb{Z} \to \mathbb{Z}_2$, $\varphi(a) = [|a|]_2$

Výsledek.

1. Je surjektivní homomorfismus, který není injektivní.
2. Není homomorfismus.
3. Je surjektivní homomorfismus, který není injektivní.
4. Je surjektivní homomorfismus, který není injektivní.

Příklad 59. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z}_3 \to \mathbb{A}_4$, $\varphi([a]_3) = (1,2,4) \circ (1,3,2)^a \circ (1,4,2)$
2. $\varphi : \mathbb{Z}_3 \to \mathbb{A}_4$, $\varphi([a]_3) = (1,2) \circ (1,3,2)^a$

Výsledek.

1. Je homomorfismus.
2. Není homomorfismus.

Příklad 60. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{C} \to \mathbb{R}$, $\varphi(a + bi) = a + b$
2. $\varphi : \mathbb{C} \to \mathbb{R}$, $\varphi(a + bi) = a$
3. $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(a + bi) = a^2 + b^2$
4. $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(c) = 2|c|$
5. $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(c) = |c|^3$
6. $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(c) = 1/|c|$

Výsledek.

1. Není homomorfismus.
2. Je surjektivní homomorfismus.
3. Je surjektivní homomorfismus.
4. Je surjektivní homomorfismus.
5. Je surjektivní homomorfismus.
6. Je surjektivní homomorfismus.

Příklad 61. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = 2a$
2. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = a + 1$
3. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = 3|a|$
4. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = 1$

Výsledek.

1. Je injektivní homomorfismus.
2. Není homomorfismus.
3. Není homomorfismus.
4. Není homomorfismus.

Příklad 62. Rozhodněte, zda předpis φ zadává zobrazení. Pokud ano, rozhodněte, zda jde o homomorfismus a určete jádro a obraz. Rozhodněte o surjektivitě a injektivitě φ:

1. $\varphi : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}^*$, $\varphi((a, b, c)) = 2^a 3^b 12^c$
2. $\varphi : \mathbb{Z}_3^* \times \mathbb{Z}_5 \to \mathbb{Z}_5$, $\varphi((a, b)) = b^a$
3. $\varphi : \mathbb{Z}_2 \times \mathbb{Z} \to \mathbb{Z}$, $\varphi(([a]_2, b)) = b$

Výsledek.

1. Je homomorfismus.
2. Není homomorfismus.
3. Je surjekivní homomorfismus.

Příklad 63. Popište všechny homomorfismy φ

1. $\varphi : \mathbb{Z} \to \mathbb{Z}$
2. $\varphi : \mathbb{Z}_5 \to \mathbb{Z}$
3. $\varphi : \mathbb{Z} \to \mathbb{Z}_5$
4. $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_5$

Příklad 64. Popište všechny homomorfismy φ

1. $\varphi : \mathbb{Z}_{15} \to \mathbb{Z}_6$
2. $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_{15}$
3. $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$
4. $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$

Příklad 65. Určete dvě různá přirozená čísla m, n tak, aby byly grupy $\mathbb{Z}_m^\times$ a $\mathbb{Z}_n^\times$ izomorfní.

Výsledek. 3,4

Příklad 66. Nechť G je komutativní grupa. Nechť $\varphi : G \to G$, $\varphi(g) = g^2$. Dokažte, že φ je homomorfismus. Uveďte příklad grup G, kdy se jedná o izomorfismus a kdy se izomorfismus nejedná.

Příklad 67. Nechť G je grupa. Nechť $\varphi : G \to G$, $\varphi(g) = g^{-1}$. Dokažte, že φ je homomorfismus právě tehdy, když je G komutativní.

Příklad 68. Dokažte, že součin cyklických grup nemusí být cyklická grupa.

Řešení. Například $\mathbb{Z}_2 \times \mathbb{Z}_2$

Příklad 69. Určete řády všech prvků v grupě $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$. vyberte generátory těchto grup.

Příklad 70. Spočítejte řád prvku

1. 60 v grupě $\mathbb{Z}_{64}$.
2. 7 v grupě $\mathbb{Z}_{17}^*$.
3. $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ v grupě $\mathcal{GL}_2(\mathbb{Z}_2)$.

Příklad 71. Nechť G je grupa. Označme $Aut(G)$ množinu všech izomorfismů $\varphi : G \to G$. Dokažte, že $Aut(G)$ tvoří grupu. Určete, kolik prvků má $Aut(\mathbb{Z}_8^\times)$, $Aut(\mathbb{Z}_8)$.

5 Cvičení 5: Okruhy a polynomy

Teorie: V tomto cvičení se podíváme na algebraické struktury se dvěma operacemi.

Definice 22. Nechť $(R, \oplus)$ je komutativní grupa a $(R, \odot)$ pologrupa s neutrálním prvkem. Nechť pro libovolné $a, b, c \in R$ platí, že

$$\begin{aligned} a \odot (b \oplus c) &= a \odot b \oplus a \odot c \\ (b \oplus c) \odot a &= b \odot a \oplus c \odot a \end{aligned}$$

Potom $(R, \oplus, \odot)$ nazýváme okruh. Je-li navíc operace $\odot$ komutativní, potom dané struktuře říkáme komutativní okruh.

Například $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_6, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ a $(Mat_2(\mathbb{R}), +, \cdot)$ tvoří okruhy.

Definice 23. Nechť $(R, \oplus, \odot)$ je okruh, $a, b \in R$. Potom prvkům a, b říkáme dělitelé nuly, pokud platí, že $a, b \neq 0$ a $a \odot b = 0$.

Definice 24. Netriviální komutativní okruh bez dělitelů nuly nazýváme obor integrity.

Například $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_7, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ tvoří obory integrity, oproti tomu $(Mat_2(\mathbb{R}), +, \cdot)$ a $(\mathbb{Z}_6, +, \cdot)$ obory integrity nejsou.

Příklad 72. Obor integrity, kde ke každému nenulovému prvku existuje prvek inverzní, se nazývá těleso.

Například $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_7, +, \cdot)$ tvoří těleso, oproti tomu $(\mathbb{Z}_6, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ tělesa nejsou.

Definice 25. Libovolnou konečnou posloupnost prvků daného okruhu nazýváme polynom.

My jsme zvyklí psát polynom ve tvaru $a_n x^n + \cdots + a_1 x + a_0$. Protože můžeme polynomy sčítat a násobit, nabízí se otázka, co za strukturu tvoří množina všech polynomů s těmito operacemi. Platí následující věta.

Věta 14.

1. *Množina všech polynomů tvoří spolu se sčítáním a násobením okruh.*
2. *Okruh polynomů nad oborem integrity je obor integrity.*
3. *Okruh polynomů nad tělesem je obor integrity.*

Definice 26. Polynom $f \in R[x]$ nazýváme ireducibilní nad R, jestliže je nekonstantní a nelze ho rozložit na součin dvou nekonstantních polynomů.

Věta 15 (Eisensteinovo lemma)**.** *Nechť* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_+ x + a_0 \in \mathbb{Z}[x]$. *Pokud existuje prvočíslo* p *takové, že* $p|a_0, \ldots p|a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$, *potom je polynom* f *ireducibilní nad* $\mathbb{Z}$.

Nyní nás bude zajímat, jak určit kořeny polynomů:

Věta 16. *Nechť* $f \in \mathbb{Z}[x]$, $f = a_n x^n + \cdots + a_1 x + a_0$. *Pokud je racionální číslo* $\frac{p}{q}$ *kořenem polynomu* f, *potom* $p|a_0, q|a_n$.

Příklad 73. Uveďte příklad

1. Konečného okruhu, který nebude oborem integrity.
2. Nekonečného okruhu, který nebude oborem integrity.
3. Konečného oboru integrity, který nebude tělesem.
4. Nekonečného oboru integrity, který nebude tělesem.
5. Konečeného tělesa.
6. Nekonečného tělesa.

Příklad 74. Rozhodněte, zda množina R s operacemi $\oplus$, $\odot$ tvoří okruh, komutativní okruh, obor integrity či těleso.

1. $R = \mathbb{Z}$, $a \oplus b = a + b + 3$, $a \odot b = -3$
2. $R = \mathbb{Z}$, $a \oplus b = a + b - 3$, $a \odot b = a \cdot b - 1$
3. $R = \mathbb{Z}$, $a \oplus b = a + b - 1$, $a \odot b = a + b - a \cdot b$
4. $R = \mathbb{Q}$, $a \oplus b = a + b$, $a \odot b = b$
5. $R = \mathbb{Q}$, $a \oplus b = a + b + 1$, $a \odot b = a + b + a \cdot b$
6. $R = \mathbb{Q}$, $a \oplus b = a + b - 1$, $a \odot b = a + b + a \cdot b$

Výsledek.

1. je okruh
2. není okruh
3. je obor integrity
4. není okruh
5. je těleso
6. není okruh

Příklad 75. Dokažte, že podmnožina komplexních čísel $\mathbb{Z}[i] = \{a+bi | a, b \in \mathbb{Z}\}$ tvoří obor integrity. Jedná se o těleso?

Výsledek. Ne

Příklad 76. Na množině $R = \mathbb{Q} \times \mathbb{Q}$ definujeme operace $\oplus$ a $\odot$ vztahem $(a, b) \oplus (c, d) = (a + c, b + d)$, $(a, b) \odot (c, d) = (ac + 2bd, ad + bc)$. Dokažte, že $(R, \oplus, \odot)$ tvoří těleso.

Příklad 77. Na množině $R = \mathbb{R} \times \mathbb{R}$ definujeme operace $\oplus$ a $\odot$ vztahem $(a, b) \oplus (c, d) = (a+c, b+d)$, $(a, b) \odot (c, d) = (ac+2bd, ad+bc)$. Dokažte, že $(R, \oplus, \odot)$ netvoří obor integrity.

Příklad 78. Nechť X je neprázdná množina. Rozhodněte, zda $(\mathcal{P}(X), \div, \cap)$ tvoří okruh, obor integrity, těleso, přičemž $A \div B = (A \setminus B) \cup (B \setminus A)$.

Příklad 79. Označme symbolem $\mathbb{R}^{\mathbb{R}}$ množinu všech reálných funkcí. Definujme $(f \oplus g)(x) = f(x) + g(x)$, $(f \odot g)(x) = f(x) \cdot g(x)$. Rozhodněte, zda $(\mathbb{R}^{\mathbb{R}}, \oplus, \odot)$ tvoří okruh, obor integrity, těleso.

Příklad 80. Označme $R = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} | a, b, c, d \in \mathbb{Q}\}$. Rozhodněte, zda $(R, +, \cdot)$ tvoří okruh, obor integrity, těleso.

Příklad 81. Uveďte příklad

1. Polynomu 2011-tého stupně s celočíselnými koeficienty, který je nad $\mathbb{Z}$ ireducibilní.
2. Polynomu s celočíselnými koeficienty, který je nad $\mathbb{Z}$ ireducibilní, přesto má celočíselný kořen.
3. Polynomu s celočíselnými koeficienty, který je nad $\mathbb{Z}$ ireducibilní, nemá celočíselný kořen, ale má kořen racionální.
4. Polynomu s celočíselnými koeficienty, který je ireducibilní nad $\mathbb{Z}$, přesto nesplňuje podmínky Eisensteinova lemmatu.
5. Polynomu pátého stupně s celočíselnými koeficienty, který není nad $\mathbb{Z}$ ireducibilní, přesto nemá celočíselný kořen.
6. Polynomu třetího stupně, který je nad $\mathbb{Z}_5$ ireducibilní.
7. Polynomu pátého stupně, který není nad $\mathbb{Z}_5$ ireducibilní, přesto nemá kořen.
8. Nenulového polynomu, který má více kořenů, než je jeho stupeň.

Příklad 82. Určete všechny kořeny polynomu

1. $x^8 + 3x^4 + 1 \in \mathbb{Z}_5[x]$.
2. $x^5 + 3x^3 + x - 3 \in \mathbb{Z}_5[x]$.

Příklad 83. Určete součet, rozdíl, součin a podíl polynomů $f, g \in \mathbb{Z}_5[x]$, $f(x) = 3x^3 + 2x^2 + 4x + 1$, $g(x) = x^2 + 2x + 2$.

Příklad 84. Určete, kolik je polynomů $f(x) \in \mathbb{Z}_5[x]$ takových, že $f(3) = 2$.

Výsledek. 100

Příklad 85. Uveďte příklad normovaného polynomu třetího stupně s koeficienty ze $\mathbb{Z}_3$, jehož jediné kořeny budou 1 a -1, oba jednonásobné.

Příklad 86. Uveďte příklad 2010 polynomů 2011-tého stupně s racionálními koeficienty, jejichž jediné racionální kořeny budou dvojnásobný kořen 1, trojnásobný kořen $-\frac{1}{3}$ a pětinásobný kořen 0.

Příklad 87. Určete všechna $a \in \mathbb{Z}_5$ tak, aby byl polynom $x^3 + 3x^2 + 4x + a$ ireducibilní nad $\mathbb{Z}_5$.

Příklad 88. Určete všechna $a \in \mathbb{Z}_5$ tak, aby byl polynom $x^5 + 4x^4 + 4x^3 + 4x^2 + ax + 4$ ireducibilní nad $\mathbb{Z}_5$.

Příklad 89. Určete všechny polynomy $f \in \mathbb{Z}_2[x]$, které jsou nad $\mathbb{Z}_2$ ireducibilní a jsou

1. druhého stupně.
2. třetího stupně.
3. čtvrtého stupně.
4. pátého stupně.

Příklad 90. Dokažte, že jsou dané polynomy ireducibilní nad $\mathbb{Z}$:

1. $3x^5 + 2x^4 + 6x^3 - 14x^2 + 8x - 10$
2. $x^7 + 35x^5 - 70x^3 + 140x - 175$

3. $x^2 + 5x - 8$
4. $x^3 + x^2 + x - 1$
5. $x^4 + 8x^3 + 24x^2 - 18x - 1$ *Nápověda: Uvažujte Taylorův rozvoj se středem v 1.*

Příklad 91. Určete všechny racionální kořeny polynomu $f \in \mathbb{Z}[x]$:

1. $f(x) = 6x^5 - 11x^4 - 19x^3 + 18x^2 + 28x + 8$
2. $f(x) = 5x^6 + 11x^5 - 28x^4 - 26x^3 + 61x^2 - 17x - 6$
3. $f(x) = 4x^5 - 8x^4 - 27x^3 + 29x^2 + 44x + 12$
4. $f(x) = 4x^5 - 24x^4 + 37x^3 + 9x^2 - 32x - 12$
5. $f(x) = 2x^6 - 7x^5 - 6x^4 + 26x^3 + 14x^2 - 27x - 18$

Řešení.

1. $f(x) = (x + 1)(2x + 1)(3x + 2)(x - 2)(x - 2)$
2. $f(x) = (x + 3)(5x + 1)(x + 2)(x - 1)(x - 1)(x - 1)$
3. $f(x) = (x + 2)(2x + 1)(2x + 1)(x - 3)(x - 2)$
4. $f(x) = (x - 2)(2x + 1)(2x + 1)(x - 3)(x - 2)$
5. $f(x) = (x + 1)(x + 1)(x + 1)(x - 3)(x - 2)(2x - 3)$

Příklad 92. Metodou neurčitých koeficientů rozložte polynom $x^4 - 3x^3 + 5x^2 - 4x + 2$ na ireducibilní faktory nad $\mathbb{Z}$.

Výsledek. $f(x) = (x^2 - x + 1)(x^2 - 2x + 2)$

Příklad 93. Uveďte příklad kubického polynomu f s celočíselnými koeficienty, který má jedničku za kořen a platí, že $f(2) = f(3) = f(4)$.

6 Cvičení 6: Polynomy s reálnými a komplexními koeficienty

Teorie: Zde pro nás bude teorie kraťoučká. Půjde o sérii tvrzení, která byla odvozena na přednášce. Než se do nich pustíme, uveďme jistou paralelu mezi polynomy a celými čísly. Také se zde můžeme bavit o dělitelnosti, stanovovat Euklidovým algoritmem největší společný dělitel a hledat koeficienty v Bezoutově rovnosti.

Věta 17. *Má-li polynom $f \in \mathbb{R}[x]$ komplexní kořen $a + bi$, potom má i kořen $a - bi$.*

Věta 18. *Každý polynom s reálnými koeficienty lichého stupně má reálný kořen.*

Věta 19. *Má-li polynom f s reálnými koeficienty vícenásobný kořen a, potom je a kořenem polynomu $f'(x)$ a tedy i polynomu $gcd(f, f')$.*

Věta 20. *Polynom s reálnými koeficienty je nad $\mathbb{R}$ ireducibilní právě tehdy, když je lineární nebo kvadratický se záporným diskriminantem.*

Věta 21. *Polynom s komplexními koeficienty je nad $\mathbb{C}$ ireducibilní právě tehdy, když je lineární.*

Příklad 94. Dokažte, že jsou dané polynomy $f, g \in \mathbb{R}[x]$ nesoudělné a nalezněte příslušné koeficienty v Bezoutově rovnosti.

1. $f(x) = x^4 + 2x^3 + 4^x + 2$, $g(x) = x^2 + 2x + 2$
2. $f(x) = 2x^3 + x + 1$, $g = x^2 + 1$
3. $f(x) = x^5 + 1$, $g = x^3 - 1$

Příklad 95. Určete největší společný dělitel polynomů $f, g \in \mathbb{R}[x]$ a nalezněte příslušné koeficienty v Bezoutově rovnosti.

1. $f(x) = x^4 + 4x^3 + 10x^2 + 12x + 9$, $g(x) = x^3 + 3x^2 + 5x + 3$.
2. $f(x) = x^6 + 9x^4 + 27x^2 + 27$, $g(x) = x^4 + 6x^2 + 9$.
3. $x^5 + x^4 - 2x^3 - 2x^2 + x + l, g = x^3 - 2x^2 - x + 2$

Příklad 96. Nalezněte všechny kořeny polynomu $f \in \mathbb{R}[x]$, víte-li, že má násobný kořen. Daný polynom rozložte na ireducibilní faktory nad $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.

1. $f(x) = x^4 - 40x + 400$
2. $f(x) = x^4 - 4x^3 - 26x^2 + 60x + 225$
3. $f(x) = x^6 + 6x^5 + 15x^4 + 20x^3 + 12x^2 - 4$
4. $f(x) = x^4 - 2x^3 - x^2 + 2x + 1$

Příklad 97. Určete všechny kořeny polynomu $f = x^7 - 4x^6 + 8x^5 - 7x^4 + 8x^2 - 8x + 4 \in \mathbb{C}[x]$, víte-li, že má dvojnásobný kořen $1 + i$. Rozložte tento polynom na ireducibilní faktory nad $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Příklad 98. Určete všechny kořeny polynomu $f = x^6 + 8x^5 + 24x^4 + 24x^3 - 27x^2 - 80x - 50 \in \mathbb{C}[x]$, víte-li, že má dvojnásobný kořen $2 + i$. Rozložte tento polynom na ireducibilní faktory nad $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Příklad 99. Určete všechny kořeny polynomu $f = x^4 - 2x^3 + x^2 + 2x - 2 \in \mathbb{C}[x]$, víte-li, že má kořen $1 + i$. Rozložte tento polynom na ireducibilní faktory nad $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Příklad 100. Mezi všemi normovanými polynomy s reálnými koeficienty nalezněte ten nejnižšího stupně, který má

1. dvojnásobný kořen $1 + i$ a jednoduchý kořen 2.
2. dvojnásobný kořen 1 a jednoduchý kořen $2 - 3i$.
3. trojnásobný kořen i a jednoduchý kořen $-1 - i$.
4. jednoduché kořeny $i + 1, 2 - i, i - 3$.

Rozložte tyto polynomy na ireducibilní faktory nad $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Příklad 101. Zjistěte násobnost kořene -1 polynomu $x^5 - ax^2 - ax + 1 \in \mathbb{C}[x]$ v závislosti na parametru $a \in \mathbb{C}$.

Příklad 102. Určete normované polynomy $f, g \in \mathbb{R}[x]$ čtvrtého stupně tak, aby $f(1+i) = 0$ a aby g měl dva dvojnásobné kořeny, přičemž $gcd(f, g) = x^2 + x + 1$.

Příklad 103. Rozložte polynom $x^4 - x^2 - 2$ na součin ireducibilních prvků v oborech $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_3[x]$.

Příklad 104. Určete všechny kořeny polynomů $f(x) = x^4 + 2x^3 + 2x^2 + 2x + 1$, $g(x) = x^3 - 2x^2 + x - 2$, víte-li, že mají společný kořen. Rozložte tyto polynomy na ireducibilní faktory nad $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Příklad 105. Určete všechny kořeny polynomů $f(x) = 2x^4 - 5x^3 - x^2 + 11x + 5$, $g(x) = 2x^4 - 11x^3 + 20x^2 - 7x - 10$, víte-li, že mají společný racionální kořen. Rozložte tyto polynomy na ireducibilní faktory nad $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Příklad 106. Určete všechny kořeny polynomů $f(x) = x^6 - 4x^5 + 9x^4 - 12x^3 + 12x^2 - 8x + 4$, $g(x) = x^5 - 3x^4 + 4x^3 - 4x + 4$, víte-li, že mají společný násobný kořen. Rozložte tyto polynomy na ireducibilní faktory nad $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Výsledek. $f(x) = (x-(1+i))^2(x-(1-i))^2(x-i)(x+i)$, $g(x) = (x-(1+i))^2(x-(1-i))^2(x+1)$

Příklad 107. Určete všechny kořeny polynomu

1. $f(x) = 6x^4 - 5x^3 - 38x^2 - 5x + 6$
2. $f(x) = 5x^4 - 26x^3 + 10x^2 - 26x + 5$

Příklad 108. Rozložte na ireducibilní faktory nad $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ polynom $x^6 + 27$.

Příklad 109. Polynom $f(x) = x^3 + ax^2 + bx - 15$ má kořen $2 + i$. Určete reálná čísla a, b a ostatní kořeny tohoto polynomu.

Příklad 110. Aniž byste počítali kořeny polynomu $x^3 - 4x^2 + 6x - 4$, určete polynom, který bude mít dvojnásobné kořeny.

Příklad 111. Aniž byste počítali kořeny polynomu $2x^3 - 5x^2 - x + 6$, určete polynom, který bude mít kořeny, které budou převrácenými hodnotami kořenů zadaného polynomu.