20. ALGEBRICKÉ ŠTRUKTÚRY

Na začiatku týchto učebných textov sme uvažovali operácie na množine celých čísel $\mathbb{Z}$, resp. na množine prirodzených čísel $\mathbb{N}$. V predchádzajúcej kapitole sme definovali operácie na množinách podstatne menších. Táto kapitola bude venovaná tomu, že nejaké operácie môžme definovať na ľubovoľnej množine, pričom mnoho ich vlastností je určených základnými vlastnosťami, ktoré nazývame *axiomy*.

Ak $\mathbb{M}$ je nejaká neprázdna množina, na ktorej sú definované operácie, potom hovoríme, že $\mathbb{M}$ s týmito operáciami tvorí *algebrickú štruktúru*. Označujeme ju zvyčajne symbolom $(\mathbb{M}, ...)$, pričom za čiarku píšeme symboly označujúce operácie. Ak nepotrebujeme tieto symboly zdôrazniť, píšeme iba $\mathbb{M}$. Množina $\mathbb{M}$ sa nazýva *nosič* algebrickej štruktúry.

Nech $(\mathbb{M}, \diamond)$ je algebrická štruktúra. Hovoríme, že prvok $e \in \mathbb{M}$ je *neutrálny prvok* operácie $\diamond$, ak pre $a \in \mathbb{M}$ platí

$$a \diamond e = a = e \diamond a. \tag{25}$$

Úloha 424. Nech $(\mathbb{M}, \diamond)$ je algebrická štruktúra. Potom operácia $\diamond$ má najviac jeden neutrálny prvok. Dokážte.

(Návod: Nech e_1, e_2 sú dva neutrálne prvky. Uvažujte prvky $e_1 \diamond e_2$ a $e_2 \diamond e_1$.)

Nech $(\mathbb{M}, \diamond)$ je algebrická štruktúra a operácia $\diamond$ má neutrálny prvok. Nech $a \in \mathbb{M}$. Hovoríme, že prvok a' je *inverzný prvok* k prvku a, ak platí

$$a \diamond a' = e = a' \diamond a.$$

Hovoríme, že operácia $\diamond$ je *asociatívna*, ak pre každé $a, b, c \in \mathbb{M}$ platí

$$(a \diamond b) \diamond c = a \diamond (b \diamond c).$$

Hovoríme, že algebrická štruktúra $(\mathbb{M}, \diamond)$ je *grupa*, ak operácia $\diamond$ je asociatívna, má neutrálny prvok a ku každému prvku z množiny $\mathbb{M}$ existuje inverzný prvok.

Úloha 425. Dokážte, že v grupe $(\mathbb{M}, \diamond)$ platí pre každé $a, b, c \in \mathbb{M}$:

$$a \diamond c = b \diamond c \Rightarrow a = b.$$

Úloha 426. Dokážte, že v grupe existuje ku každému prvku práve jeden inverzný prvok.

(Návod: Použite úlohu 425.)

Inverzný prvok k prvku a budeme označovať symbolom a^{-1}.

Úloha 427. Ak $(\mathbb{M}, \diamond)$ je grupa a $a, b \in \mathbb{M}$, potom $(a \diamond b)^{-1} = b^{-1} \diamond a^{-1}$. Dokážte.

Operácia $\diamond$ sa nazýva *komutatívna*, ak

$$a \diamond b = b \diamond a$$

pre každé dva prvky a, b.

Ak $(\mathbb{M}, \diamond)$ je grupa a operácia $\diamond$ je komutatívna, potom grupa $(\mathbb{M}, \diamond)$ sa nazýva komutatívna grupa.

Úloha 428. Nech $m \in \mathbb{N}$, $m > 1$. Dokážte:
a) $(\mathbb{Z}_m, +)$ je komutatívna grupa.
b) $(\mathbb{R}_m, .)$ je komutatívna grupa.

Ďalej sa budeme zaoberať iba komutatívnymi grupami. Tie sa nazývajú aj Abelove grupy na počesť švédskeho matematika Nielsa Henrika Abela.

Niels Abel sa zaoberal otázkami riešiteľnosti rovníc 5. stupňa. Pokúšal sa nájsť univerzálny vzorec na riešenie týchto rovníc a dokonca ho aj našiel. Ukázalo sa však, že sa zmýlil a podarilo sa mu dokonca dokázať, že takýto vzorec neexistuje. Približne v tom istom čase sa podobnými otázkami zaoberal aj mladý francúz Galois, ktorý dokázal, že existuje rovnica 5. stupňa, ktorej riešenia sa nedajú vyjadriť pomocou odmocnín. Aby sme lepšie charakterizovali túto dobu, je potrebné povedať, že N. Abel mal veľké problémy s učiteľmi matematiky. Dokonca po absolvovaní strednej školy študoval herectvo a istý čas bol hercom. K matematike sa vrátil až neskôr.

Galoisov osud bol komplikovaný. Nikdy sa nedostal študovať na vysokú školu, kde ho neprijali pre údajnú neznalosť matematiky. Slávnu teóriu vymyslel úplne sám. Zahynul v dvadsiatich rokoch v súboji. Keď 30 rokov po jeho smrti vyšla najavo jeho sláva, jeho učitelia, ktorí ho prenasledovali, sa ním začali chváliť ako svojim bývalým žiakom.

Teraz si ukážeme inú charakterizáciu grúp.

Veta 27. Nech $\diamond$ je komutatívna a asociatívna operácia na $\mathbb{M}$. Potom $(\mathbb{M}, \diamond)$ je grupa práve vtedy, keď pre každé $a, b \in \mathbb{M}$ existuje taký prvok $x \in \mathbb{M}$, že

$$a \diamond x = b. \tag{26}$$

Je potrebné dokázať existenciu neutrálneho prvku a inverzných prvkov. Budeme predpokladať, že platí označenie a predpoklady z vety 27.

Úloha 429. Nech $a \in \mathbb{M}$. Nech $x \in \mathbb{M}$ je taký prvok, že $a \diamond x = a$. Dokážte, že pre $b \in \mathbb{M}$ platí $b \diamond x = b$.

(Návod: Vyjadrite $a \diamond y = b$.)

Úloha 430. Dokážte, že $\diamond$ má neutrálny prvok.

Úloha 431. Dokážte, že ku každému prvku $\mathbb{M}$ existuje inverzný prvok.

(Návod: Použite priamo vzťah (26).)

Úloha 432. Dokážte vetu 27.

Úloha 433. Nech $(\mathbb{M}, \diamond)$ je algebrická štruktúra a nech operácia $\diamond$ je komutatívna a asociatívna. Ak $\mathbb{M}$ je konečná množina, potom $(\mathbb{M}, \diamond)$ je grupa práve vtedy, keď pre $a, b, c \in \mathbb{M}$ platí

$$a \diamond c = b \diamond c \Rightarrow a = b.$$

Dokážte.

(Návod: Použite vetu 27.)

Ak $\mathbb{M}' \subset \mathbb{M}$ a $(\mathbb{M}, \diamond)$ je grupa, potom hovoríme, že $\mathbb{M}'$ je podgrupa grupy $(\mathbb{M}, \diamond)$ práve vtedy, keď $(\mathbb{M}', \diamond)$ je grupa.

Úloha 434. Dokážte, že $\mathbb{M}' \subset \mathbb{M}$ je podgrupa práve vtedy, keď neutrálny prvok patrí do $\mathbb{M}'$ a pre každé dva prvky $a, b \in \mathbb{M}'$ aj prvky $a^{-1} \in \mathbb{M}'$ a $a \diamond b \in \mathbb{M}'$.

Úloha 435. Dokážte, že $\emptyset \neq \mathbb{M}' \subset \mathbb{M}$ je podgrupa práve vtedy, keď pre všetky $a, b \in \mathbb{M}'$ $a \diamond b^{-1} \in \mathbb{M}'$.

Úloha 436. Nech $(\mathbb{M}, \diamond)$ je grupa. Nech $\mathbb{M}'$ je konečná a neprázdna podmnožina $\mathbb{M}$. Potom $\mathbb{M}'$ je podgrupa práve vtedy, keď pre všetky $a, b \in \mathbb{M}'$ platí $a \diamond b \in \mathbb{M}'$. Dokážte.

(Návod: Použite vetu 27.)

Úloha 437. Dokážte, že $(\mathbb{Z}_m \setminus \{0\}, \cdot)$ je grupa práve vtedy, keď m je prvočíslo.

Symbol operácie $\diamond$ zvyčajne nahrádzame symbolom $\cdot$ alebo symbolom $+$. V prvom prípade hovoríme o multiplikatívnom zápise, v druhom prípade hovoríme o aditívnom zápise. Keď budeme používať multiplikatívny zápis, potom symbol $\cdot$ budeme často vynechávať. Teda $x \cdot y = xy$. Vhodnosť tejto symboliky uvidíme neskôr.

Teraz sa budeme zaoberať konečnými grupami. Grupu budeme označovať G a budeme používať multiplikatívny zápis. Aby sme videli, že okrem grúp $\mathbb{Z}, \mathbb{Z}_m, \ldots$ existujú aj iné grupy, uvedieme nasledujúce úlohy.

Úloha A. Nech pre $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ $(a_1,b_1)+(a_2,b_2) = (a_1+a_2 \bmod \mathrm{m}, b_1 + b_2 \bmod \mathrm{n})$. Dokážte, že $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$ je grupa.

Ak G je konečná grupa, potom počet jej prvkov nazývame *rád* grupy G a zvyčajne ho označujeme $|G|$. Dokážeme tvrdenie, ktoré tiež nazývame Lagrangeova veta, podobne ako tvrdenie vo vete 11. Avšak tieto tvrdenia spolu nesúvisia.

Veta 28. Nech G je konečná grupa a H je jej podgrupa. Potom rád podgrupy H delí rád grupy G.

Budeme predpokladať, že platí označenie a predpoklady z vety 28. Označme pre $b \in G$

$$bH = \{bh; h \in H\}.$$

Úloha 438. Dokážte, že pre $b \in G$ platí $|bH| = |H|$.

(Návod: Použite úlohu 425.)

Úloha 439. Dokážte, že pre $b_1, b_2 \in G$ platí $b_1H \cap b_2H = \emptyset$ alebo $b_1H = b_2H$.

Úloha 440. Dokážte, že

$$\bigcup_{b\in G} bH = G.$$

(Návod: Uvedomte si, že H obsahuje neutrálny prvok.)

Úloha 441 Nech k je počet rôznych prvkov množiny $\{bH; b \in G\}$. Dokážte, že $k \cdot |H| = |G|$.

(Návod: Použite úlohy 438, 439, 440.)

Úloha 442 Dokážte vetu 28.

Ak máme grupu G, potom môžeme obvyklým spôsobom pomocou operácie $\cdot$ definovať $n-$tú mocninu pre $n \in \mathbb{N}$. Ešte upozorňujeme, že v ďalšom texte budeme symbolom e označovať neutrálny prvok grupy G.

Označme pre $a \in G$

$$a^n = a \cdot \ldots \cdot a \ (n\times)$$

$$a^0 = e$$

a ak $n \in \mathbb{Z}$ a $n < 0$, potom

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

Úloha 443. Dokážte, že pre všetky $a \in G$, $m, n \in \mathbb{Z}$ platí

$$a^m \cdot a^n = a^{m+n}, (a^n)^m = a^{mn}.$$

Úloha 444. Ak G je konečná grupa a $a \in G$, potom existuje $n \in \mathbb{N}$ taký, že

$$a^n = e.$$

Dokážte.

(Návod: V postupnosti $1, a, a^2, ...$ sa aspoň dva prvky musia opakovať.)

Ak $a \in G$, potom najmenšie číslo k také, pre ktoré platí, že $a^k = e$, nazývame *rádom* prvku a v grupe G a označujeme ho $rad\ a$. Nasledujúca úloha nám objasní, prečo tým istým slovom označujeme rád prvku a aj počet prvkov grupy.

Úloha 445. Nech $a \in G$ a $n = rad\ a$. Potom
a) pre každé $k \in \mathbb{N}$ platí $a^k = a^{n+k}$,
b) množina $\{e, a, ..., a^{n-1}\}$ je podgrupou grupy G .
Dokážte.

(Návod: Použite úlohu 436.)

Podgrupu $\{e, a, ..., a^{n-1}\}$ označujeme v tomto prípade symbolom $[a]$ a nazývame ju podgrupou generovanou prvkom a.

Úloha 446. Nech G je konečná grupa a $a \in G$. Potom

$$|[a]| = rad\ a.$$

Úloha 447. Ak G je konečná grupa a $a \in G$, potom

$$rad\ a \Big| |G|.$$

Dokážte.

(Návod: Použite úlohu 446 a vetu 28.)

Úloha 448. Ak G je konečná grupa a $a \in G$, potom

$$a^{|G|} = e.$$

Dokážte.

Vidíme, že úlohu 448 by sme mohli nazvať Eulerovou vetou pre grupy.

Konečná grupa G sa nazýva cyklická, ak existuje $a \in G$ tak, že

$$[a] = G.$$

Prvok a v tomto prípade nazývame generátor grupy G.

Úloha 449. Dokážte, že grupa $(\mathbb{R}_m, \cdot)$ je cyklická iba ak $m = 2, 4, p^\alpha, 2p^\alpha$, kde p je nepárne prvočíslo.

(Návod: Použite vetu 15 a uvedomte si, ako súvisia generátor grupy a primitívny koreň.)

Úloha B. Dokážte, že grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ definovaná v úlohe A za úlohou 437 nie je nikdy cyklická.

Úloha 450. Grupa prvočíselného rádu je vždy cyklická. Dokážte.

(Návod: Použite úlohu 447.)

Úloha 451. Ak G je konečná grupa a $a, b \in G$, $(rad\ a, rad\ b) = 1$, potom $rad\ (ab) = rad\ a \cdot rad\ b$. Dokážte.

(Návod: Použite analogický postup ako pri dôkaze lemy 1.)

Dôkaz nasledujúceho tvrdenia bude ilustráciou súhry vyššie uvedených výsledkov o abstraktných grupách, primitívnych koreňoch a čínskej zvyškovej vety.

Tvrdenie 1. Nech $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Označme $r = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}$. Potom existuje prvok rádu r modulo m.

Úloha A. Nech p je prvočíslo a $\alpha > 0$. Nech g je primitívny koreň modulo p^α. Dokážte, že $g^{\frac{\varphi(p^\alpha)}{p^{\alpha-1}}}$ je prvok rádu $p^{\alpha-1}$ modulo p^α.

Úloha B. Nech $x_j^h \equiv 1 \pmod{p_j^{\alpha_j}}$ a $x \equiv x_j \pmod{p_j^{\alpha_j}}$ pre $j = 1, ..., k$. Dokážte, že $x^h \equiv 1 \pmod{m}$.

Úloha C. Nech $x \equiv g_j^{\frac{\varphi(p_j^{\alpha_j})}{\alpha_j - 1}} \pmod{p_j^{\alpha_j}}$ pre $j = 1, ..., k$. Dokážte, že $x^r \equiv 1 \pmod{m}$.

Úloha D. Nech x má rovnaký význam ako v predchádzajúcej úlohe. Nech $x^{r_0} \equiv 1 \pmod{m}$. Dokážte, že $p_j^{\alpha_j - 1} | r_0$ pre j=1, 2,..., k.

(Návod: V tomto prípade platí, že $\left(g_j^{\frac{\varphi(p_j^{\alpha_j})}{p_j^{\alpha_j - 1}}}\right)^{r_0} \equiv 1 \pmod{p_j^{\alpha_j}}$.)

Úloha E. Dokážte tvrdenie 1.

Tvrdenie 2. Nech p je prvočíslo a $m > 1$ je prirodzené číslo. Potom existuje také $x \in \{2, \ldots, m-1\}$, ktoré vyhovuje kongruencii

$$x^p \equiv 1 \pmod{m}$$

práve vtedy, keď $p | \varphi(m)$.

Úloha F. Ak $p | \varphi(m)$, potom $p | \varphi(p_j^{\alpha_j})$ pre vhodné j.

Úloha G. Ak G je konečná cyklická grupa a $p || G|$, potom v G existuje prvok rádu p.

Úloha H. Analogickým postupom ako pri tvrdení 1 dokážte tvrdenie 2.

Teraz se budeme zaoberať takými algebrickými štruktúrami, ktoré majú dve operácie. Budeme ich označovať symbolmi $+, \cdot$.

Nech $R \neq \emptyset$. Potom $(R, +, \cdot)$ nazývame *okruhom*, ak $(R, +)$ je komutatívna grupa, operácia $\cdot$ je asociatívna a pre všetky $a, b, c \in R$ platí

$$(a + b) \cdot c = a \cdot c + b \cdot c, c \cdot (a + b) = c \cdot a + c \cdot b.$$

Predchádzajúce dve rovnosti nazývame distributívny zákon.

Začali sme už používať aj aditívny zápis. Neutrálny prvok grupy $(R, +)$ budeme označovať 0. Inverzný prvok k prvku $a \in R$ v grupe $(R, +)$ budeme označovať $-a$. Namiesto $a + (-b)$ budeme písať iba $a - b$.

Úloha 452. Ak R je okruh a $a, b, c \in R$, potom

$$a + c = b + c \Rightarrow a = b.$$

Dokážte.

(Návod: Je to iba aditívny prepis úlohy 425.)

Úloha 453. Dokážte, že pre všetky $a \in R$ platí, že

$$0 \cdot a = 0 = a \cdot 0.$$

(Návod: Vieme, že $0 = 0 + 0$. Použite distributívny zákon a úlohu 452.)

Ak je operácia $\cdot$ komutatívna, potom okruh $(R, +, \cdot)$ budeme nazývať komutatívnym okruhom. Ak má operácia $\cdot$ neutrálny prvok, potom tento prvok budeme nazývať jednotkou a označovať ho 1. Okruh $(R, +, \cdot)$ budeme v tomto prípade nazývať okruhom s jednotkou.

Úloha 454. Dokážte, že $(\mathbb{Z}_m, +, \cdot)$ je komutatívny okruh s jednotkou pre všetky $m \in \mathbb{N}$.

Úloha 455. Nech $(R, +, \cdot)$ je okruh s jednotkou a $|R| > 1$. Potom $1 \neq 0$. Dokážte.

Úloha 456. Nech $(R, +, \cdot)$ je okruh s jednotkou a $|R| > 1$. Potom 0 nemá v $(R, \cdot)$ inverzný prvok. Dokážte.

(Návod: Použite úlohu 453.)

Ak $(R, +, \cdot)$ je komutatívny okruh s jednotkou a $(R \setminus \{0\}, \cdot)$ je grupa, potom hovoríme, že $(R, +, \cdot)$ je *pole*. Inverzný prvok k prvku $a \in R \setminus \{0\}$ budeme označovať dvoma spôsobmi: $a^{-1} = \frac{1}{a}$.

Úloha 457. Dokážte, že $(\mathbb{Z}_m, +, \cdot)$ je teleso práve vtedy, keď m je prvočíslo.

Ak p je prvočíslo, potom teleso $(\mathbb{Z}_p, +, \cdot)$ budeme označovať $\mathbb{Z}_p$.

Budeme predpokladať, že máme daný komutatívny okruh s jednotkou, ktorý budeme označovať R.

Úloha 458. Dokážte, že pre každé $a \in R$ platí

$$(-1) \cdot a = -a.$$

Úloha 459. Dokážte, že pre každé $a \in R$ platí

$$-(-a) = a.$$

Úloha 460. Dokážte, že pre každé $a, b, c \in R$ platí

$$a(b - c) = ab - ac.$$

Okruh R budeme nazývať *oborom integrity*, ak pre každé $a, b \in R$ platí, že

$$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0.$$

Úloha 461. Dokážte, že $(\mathbb{Z}, +, \cdot)$ je obor integrity.

Úloha 462. Nech R je obor integrity. Dokážte, že pre všetky $a, b, c \in R, a \neq 0$ platí

$$ab = ac \Rightarrow b = c.$$

(Návod: Použite úlohu 460.)

Úloha 463. Dokážte, že konečný obor integrity je teleso.

(Návod: Použite úlohu 462 a 433.)

Vo všeobecnosti platí, že každý obor integrity je obsiahnutý v nejakom telese. Dôkaz tohto faktu je predmetom algebry a čitateľovi môžeme odporučiť napríklad monografiu [KOL].

Ak budeme hovoriť o bližšie neurčenom telese, budeme ho spravidla označovať písmenom F, ktoré pochádza z anglického termínu field.

Ak máme teleso $(F, +, \cdot)$, potom grupu $(F, +)$ nazývame aditívnou grupou telesa F a grupu $(F \setminus \{0\}, \cdot)$ nazývame multiplikatívnou grupou telesa F.

Úloha 464. Dokážte, že množina racionálnych čísel spolu s operáciami sčítania a násobenia je teleso.

Úloha 465. Dokážte, že množina reálnych čísel spolu s operáciami sčítania a násobenia je teleso.

Úloha 466. Nech F je konečné teleso. Potom pre každé $a \in F$, $a \neq 0$ platí

$$a^{|F|-1} = 1.$$

Dokážte.

(Návod: Použite úlohu 448.)

Úloha 467. Dokážte, že každé teleso je oborom integrity, ale nie každý obor integrity je telesom.