Kapitola 4

Grupy a tělesa

Tato kapitola je věnovaná základním algebraickým strukturám jako jsou grupy a tělesa. Jsou to abstraktní pojmy zobecňující dobře známé obory reálných (racionálních, komplexních aj.) čísel s operacemi sčítání a násobení.

Pro hlubší informace a souvislosti doplněné mnoha názornými vizualizacemi doporučuji knihu Carter [2009].

4.1 Grupy

Pojem grupy zavedl francouzský matematik Èvariste Galois (1811–1832) při budování teorie řešitelnosti hledání kořenů polynomů. Pro kořeny polynomů stupně alespoň 5 neexistuje obecně žádný vzoreček (viz poznámka 1.2), ale Galoisova teorie dává návod, jak to otestovat pro konkrétní polynom, tj. jestli kořeny daného polynomu jdou vyjádřit pomocí základních aritmetických operací a odmocnin. Příkladem situace, kdy to nelze, je polynom $x^5 - 2x - 1$.

Grupy mají však mnohem širší použití. Díky jejich obecnosti a abstraktnosti je můžeme najít v různých oborech: fyzika (Lieovy grupy), architektura (Friezovy grupy), geometrie a molekulární chemie (symetrické grupy) aj.

Definice 4.1 (Grupa)**.** Buď $\circ\colon G^2 \to G$ binární operace na množině G. Pak *grupa* je dvojice $(G, \circ)$ splňující:

(1) $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$ (asociativita),

(2) $\exists e \in G\ \forall a \in G : e \circ a = a \circ e = a$ (existence neutrálního prvku),

(3) $\forall a \in G\ \exists b \in G : a \circ b = b \circ a = e$ (existence inverzního prvku).

Abelova (komutativní) grupa je taková grupa, která navíc splňuje:

(4) $\forall a, b \in G\ a \circ b = b \circ a$ (komutativita).

Výše zmíněné podmínky se také občas nazývají axiomy. Poznamenejme, že implicitně je v definici grupy schovaná podmínka uzavřenosti, aby výsledek operace nevypadl ven z množiny G, tedy aby $\forall a, b \in G : a \circ b \in G$. Pokud je operací $\circ$ sčítání, většinou se značí neutrální prvek 0 a inverzní $-a$, pokud jde o násobení, neutrální prvek se označuje 1 a inverzní a^{-1}.

Poznámka 4.2 (Definice konstrukcí vs. axiomy)**.** Matematický objekt lze zavést buď konstrukcí z nějakých již vytvořených objektů, nebo specifikací vlastností (axiomů), které má splňovat. Definice grupy padá do druhé skupiny, podobně jako definice tělesa v sekci 4.3 či vektorových prostorů v kapitole 5. Grupou pak je jakýkoli objekt, který splňuje dané vlastnosti. Axiomatická definice má tu výhodu, že nás nesvazuje s jedním konkrétním objektem – jakoukoli vlastnost, kterou odvodíme pro axiomaticky definovaný objekt potom automaticky platí pro každý konkrétní případ. Mnoho konkrétních příkladů grup ukazujeme v následujícím odstavci.

Příklad 4.3. Příklady grup:

- Dobře známé obory celých čísel $(\mathbb{Z}, +)$, racionálních čísel $(\mathbb{Q}, +)$, reálných čísel $(\mathbb{R}, +)$ a komplexních čísel $(\mathbb{C}, +)$. Neutrálním prvkem je 0, inverzním prvkem k prvku a je $-a$. Komutativita a asociativita sčítání zjevně platí.
- Grupy matic $(\mathbb{R}^{m\times n}, +)$. Neutrálním prvkem je nulová matice 0 rozměru $m \times n$, inverzním prvkem k matici A je $-A$. Komutativita a asociativita sčítání platí s ohledem na tvrzení 3.5.
- Konečná grupa $(\mathbb{Z}_n, +)$, kde množina $\mathbb{Z}_n \coloneqq \{0, 1, \ldots, n-1\}$ a sčítání se provádí modulo n. Neutrálním prvkem je 0, inverzním prvkem k prvku a je $-a \bmod n$.
- Číselné obory s násobením, např. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$. Nulu musíme vynechat, protože nemá inverzní prvek. Neutrálním prvkem je nyní 1, inverzním prvkem k prvku a je a^{-1}.
- Množina reálných polynomů proměnné x se sčítáním.

Výše zmíněné grupy jsou Abelovy. Z určitého pohledu jsou důležitější neabelovské grupy. Dva důležité příklady neabelovských grup jsou:

- Zobrazení na množině s operací skládání, např. rotace v $\mathbb{R}^n$ podle počátku nebo později probírané permutace (sekce 4.2). Rotace v rovině $\mathbb{R}^2$ jsou ještě komutativní, ale ve vyšších dimenzích komutativitu ztrácíme. Neutrálním prvkem je otočení o nulový úhel, inverzním prvkem je otočení o opačný úhel zpět.
- Regulární matice pevného řádu n s násobením (tzv. maticová grupa). Neutrálním prvkem je I_n, inverzním prvkem k matici A je inverzní matice A^{-1}. Asociativita maticového součinu byla nahlédnuta ve tvrzení 3.9.

Příklady negrup:

- $(\mathbb{N}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{R} \setminus \{0\}, :)$, ... □

Tvrzení 4.4 (Základní vlastnosti v grupě)**.** *Pro prvky grupy $(G, \circ)$ platí následující vlastnosti.*

(1) $a \circ c = b \circ c$ *implikuje* $a = b$ *(tzv. krácení),*

(2) neutrální prvek e je určen jednoznačně,

(3) pro každé $a \in G$ je jeho inverzní prvek určen jednoznačně,

(4) rovnice $a \circ x = b$ má právě jedno řešení pro každé $a, b \in G$,

(5) $(a^{-1})^{-1} = a$,

(6) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Důkaz. Ukážeme jen několik vlastností.

(1)

$$\begin{aligned} a \circ c &= b \circ c && / \circ c^{-1} \text{ zprava} \\ a \circ (c \circ c^{-1}) &= b \circ (c \circ c^{-1}) \\ a \circ e &= b \circ e \\ a &= b \end{aligned}$$

(2) Existují-li dva různé neutrální prvky e_1, e_2, pak $e_1 = e_1 \circ e_2 = e_2$, což je spor.

(3) Existují-li k $a \in G$ dva různé inverzní prvky a_1, a_2, pak $a \circ a_1 = e = a \circ a_2$ a z vlastnosti krácení dostáváme $a_1 = a_2$, což je spor.

(4) Vynásobme rovnost $a \circ x = b$ zleva prvkem a^{-1} a dostaneme jediného kandidáta $x = a^{-1} \circ b$. Dosazením ověříme, že rovnost splňuje. □

Tak jako množiny doprovází pojem podmnožina, tak nelze mluvit o grupách a nezmínit podgrupy.

Definice 4.5 (Podgrupa)**.** *Podgrupa* grupy $(G, \circ)$ je grupa $(H, \diamond)$ taková, že $H \subseteq G$ a pro všechna $a, b \in H$ platí $a \circ b = a \diamond b$. Značení: $(H, \diamond) \leq (G, \circ)$.

Jinými slovy, se stejně definovanou operací splňuje H vlastnosti uzavřenost a existence neutrálního a inverzního prvku. To jest, pro každé $a, b \in H$ je $a \circ b \in H$, dále $e \in H$, a pro každé $a \in H$ je $a^{-1} \in H$.

Příklad 4.6.

- Každá grupa $(G, \circ)$ má dvě triviální podgrupy: sama sebe $(G, \circ)$ a $(\{e\}, \circ)$.
- $(\mathbb{N}, +) \not\leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$. □

Příklad 4.7. Ukažte, že podgrupy jsou uzavřené na průnik, ale ne na sjednocení. Jinými slovy, ukažte, že průnik dvou podgrup grupy $(G, \circ)$ je opět její podgrupa a najděte příklad, kdy sjednocení podgrup již podgrupa není. □

4.2 Permutace

Důležitým příkladem grup je takzvaná symetrická grupa permutací, proto si povíme něco více o permutacích. Připomeňme, že vzájemně jednoznačné zobrazení $f\colon X \to Y$ je zobrazení, které je prosté (žádné dva různé prvky se nezobrazí na jeden) a „na“ (pokryje celou množinu Y).

Definice 4.8 (Permutace)**.** *Permutace* na konečné množině X je vzájemně jednoznačné zobrazení $p\colon X \to X$.

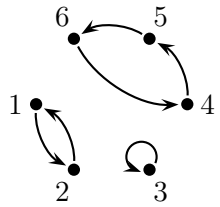
Většinou budeme uvažovat $X = \{1, \ldots, n\}$. Množina všech permutací na množině $\{1, \ldots, n\}$ se pak značí S_n.

Zadání permutace je možné například:

- Tabulkou, kde nahoře jsou vzory a dole jejich obrazy

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$$

- Grafem vyznačujícím kam se který prvek zobrazí



- Rozložením na cykly

$$p = (1, 2)(3)(4, 5, 6),$$

kde každá závorka uvádí seznam prvků v jednom cyklu. Tedy $(a_1, \ldots, a_k)$ znamená, že a_1 se zobrazí na a_2, a_2 se zobrazí na a_3, atd. až a_{k-1} se zobrazí na a_k. Z definice je patrné, že každou permutaci lze rozložit na disjunktní cykly. V následujícím textu budeme nejčastěji používat redukovaný zápis

$$p = (1, 2)(4, 5, 6),$$

ve kterém vynecháváme cykly délky 1.

Příkladem jednoduché, ale důležité, permutace je *transpozice*, což je permutace $= (i, j)$ s jedním cyklem délky 2 prohazující dva prvky. Jednodušší už je jenom identita id zobrazující každý prvek na sebe.

Inverzní permutace a skládání permutací je definováno stejně jako pro jiná zobrazení:

Definice 4.9 (Inverzní permutace)**.** Buď $p \in S_n$. *Inverzní permutace* k p je permutace p^{-1} definovaná $p^{-1}(i) = j$, pokud $p(j) = i$.

Příklad 4.10. $(i, j)^{-1} = (i, j)$, $(i, j, k)^{-1} = (k, j, i)$, ... □

Definice 4.11 (Skládání permutací)**.** Buďte $p, q \in S_n$. *Složená permutace* $p \circ q$ je permutace definovaná $(p \circ q)(i) = p(q(i))$.

Příklad 4.12. $id \circ p = p \circ id = p$, $p \circ p^{-1} = p^{-1} \circ p = id$, ... □

Skládání permutací je asociativní (jako každé zobrazení), ale komutativní obecně není. Např. pro $p = (1, 2)$, $q = (1, 3, 2)$ máme $p \circ q = (1, 3)$, ale $q \circ p = (2, 3)$.

Významná charakteristika permutace je tzv. znaménko.

Definice 4.13 (Znaménko permutace)**.** Nechť se permutace $p \in S_n$ skládá z k cyklů. Pak *znaménko permutace* je číslo $\operatorname{sgn}(p) = (-1)^{n-k}$.

Příklad 4.14. $\operatorname{sgn}(id) = 1$, $\operatorname{sgn}((i, j)) = -1$, ... □

Znaménko je vždy 1 nebo -1. Podle toho se též rozdělují permutace na *sudé* (ty, co mají znaménko 1) a na *liché* (ty se znaménkem -1).

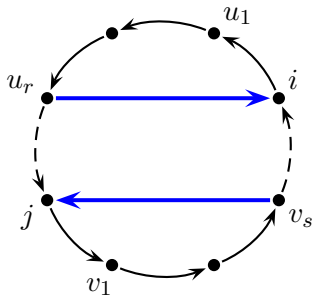
Věta 4.15 (O znaménku složení permutace a transpozice)**.** *Buď $p \in S_n$ a buď $t = (i, j)$ transpozice. Pak* $\operatorname{sgn}(p) = -\operatorname{sgn}(t \circ p) = -\operatorname{sgn}(p \circ t)$.

Důkaz. Dokážeme $\operatorname{sgn}(p) = -\operatorname{sgn}(t \circ p)$, druhá rovnost je analogická. Permutace p se skládá z několika cyklů. Rozlišme dva případy:

Nechť i, j jsou částí stejného cyklu, označme jej $(i, u_1, \ldots, u_r, j, v_1, \ldots, v_s)$. Pak

$$(i, j) \circ (i, u_1, \ldots, u_r, j, v_1, \ldots, v_s) = (i, u_1, \ldots, u_r)(j, v_1, \ldots, v_s),$$

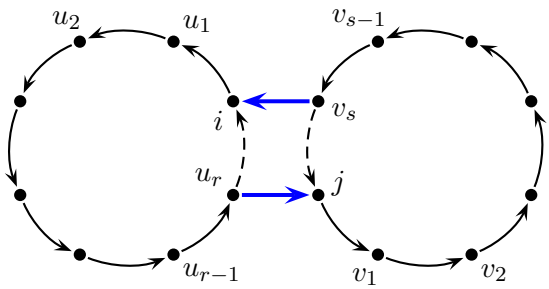
tedy počet cyklů se zvýší o jedna. Viz obrázek, kde černé šipky znázorňují původní cyklus a plné šipky nové dva cykly:



Nechť i, j náleží do dvou různých cyklů, např. $(i, u_1, \ldots, u_r)(j, v_1, \ldots, v_s)$. Pak

$$(i, j) \circ (i, u_1, \ldots, u_r)(j, v_1, \ldots, v_s) = (i, u_1, \ldots, u_r, j, v_1, \ldots, v_s),$$

tedy počet cyklů se sníží o jedna.



V každém případě se počet cyklů změní o jedna, a tudíž i výsledné znaménko. □

Věta 4.16. *Každou permutaci lze rozložit na složení transpozic.*

Důkaz. Rozložíme na transpozice postupně všechny cykly permutace. Libovolný cyklus $(u_1, \ldots, u_r)$ se rozloží

$$(u_1, \ldots, u_r) = (u_1, u_2) \circ (u_2, u_3) \circ (u_3, u_4) \circ \ldots \circ (u_{r-1}, u_r).$$ □

Poznamenejme, že rozklad na transpozice není jednoznačný, dokonce ani počet transpozic ne. Pouze jejich parita zůstane stejná.

Výše zmíněné vlastnosti mají řadu pěkných důsledků.

Důsledek 4.17. *Platí* $\operatorname{sgn}(p) = (-1)^r$*, kde* r *je počet transpozic při rozkladu* p *na transpozice.*

Důkaz. Je to důsledek věty 4.15. Vyjdeme z identity, která je sudá. Každá transpozice mění znaménko, tedy výsledné znaménko bude $(-1)^r$. □

Důsledek 4.18. *Buď* $p, q \in S_n$*. Pak* $\operatorname{sgn}(p \circ q) = \operatorname{sgn}(p)\operatorname{sgn}(q)$.

Důkaz. Nechť p se dá rozložit na r_1 transpozic a q na r_2 transpozic. Tedy $p \circ q$ lze složit z $r_1 + r_2$ transpozic. Pak $\operatorname{sgn}(p \circ q) = (-1)^{r_1+r_2} = (-1)^{r_1}(-1)^{r_2} = \operatorname{sgn}(p)\operatorname{sgn}(q)$. □

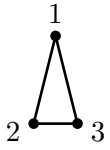
Důsledek 4.19. *Buď* $p \in S_n$*. Pak* $\operatorname{sgn}(p) = \operatorname{sgn}(p^{-1})$.

Důkaz. Platí $1 = \operatorname{sgn}(id) = \operatorname{sgn}(p \circ p^{-1}) = \operatorname{sgn}(p)\operatorname{sgn}(p^{-1})$, tedy p, p^{-1} musí mít stejné znaménko. □

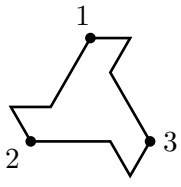
Poznámka 4.20. Kromě počtu cyklů a počtu transpozic jde znaménko permutace p zavést také např. pomocí počtu inverzí. Inverzí zde rozumíme uspořádanou dvojici (i, j) takovou, že $i < j$ a $p(i) > p(j)$. Označíme-li počet inverzí permutace p jako $I(p)$, pak platí $\operatorname{sgn}(p) = (-1)^{I(p)}$.

Poznámka 4.21 (Symetrická grupa)**.** Vraťme se zpět ke grupám. Množina permutací S_n s operací skládání $\circ$ tvoří nekomutativní grupu $(S_n, \circ)$, tzv. *symetrickou grupu*. Ta hraje důležitou roli v algebře, protože se dá ukázat, že každá grupa je isomorfní nějaké podgrupě symetrické grupy (tzv. Cayleyova reprezentace, dokonce platí i zobecnění na nekonečné grupy). Podobnou roli hrají maticové grupy, protože každá konečná grupa je isomorfní nějaké maticové podgrupě (lineární reprezentace) s tím, že těleso, nad kterým s maticemi pracujeme, si můžeme dopředu zvolit.

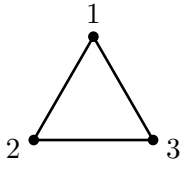
Grupa $(S_n, \circ)$ se nazývá symetrická, protože ona a její podgrupy popisují symetrie různých objektů. Kupříkladu rovnoramenný trojúhelník dole na obrázku je symetrický podle svislé osy, a této symetrii odpovídá permutace $(2, 3)$. Uvažujeme-li ještě základní symetrii danou podobností trojúhelníku se sebou samým, které odpovídá permutace id, potom symetrie trojúhelníku odpovídají podgrupě $\{id,\ (2, 3)\}$.



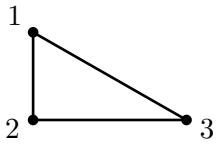
Symetrie následujícího objektu jsou rotace o 0°, 120° a o 240°. Tyto symetrie odpovídají permutacím id, $(1, 2, 3)$ a $(1, 3, 2)$. Tudíž symetrie tohoto objektu odpovídají podgrupě $\{id,\ (1, 2, 3),\ (1, 3, 2)\}$.



Symetrie rovnostranného trojúhelníku jsou souměrnosti podle těžnic, které odpovídají permutacím $(1, 2)$, $(2, 3)$ a $(1, 3)$, a dále otočení o 0°, 120° a o 240°. Všechny symetrie tedy představují celou grupu $(S_3, \circ)$.



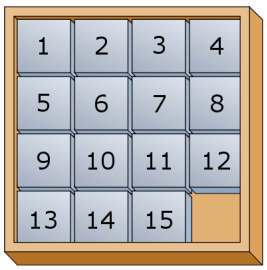
Naopak nesymetrickému trojúhelníku jako na obrázku dole přísluší pouze identita, a proto jeho symetrie představují grupu $\{id\}$.



Studium symetrií je důležité v mnoha vědních oborech. Například ve fyzice dokázaly předpovědět existenci několika elementárních částic ještě před tím, než se je podařilo objevit experimentálně. Známou ukázkou je predikce existence baryonu Ω^- americkým fyzikem Murray Gell-Mannem v roce 1962.

Loydova patnáctka

Symetrické grupy a znaménko permutace se využijí také při analýze hlavolamů jako je Loydova patnáctka nebo Rubikova kostka. Rubikova kostka vyžaduje trochu hlubší rozbor, proto nahlédneme pod pokličku pouze Loydova patnáctky.



Loydova patnáctka. Cílový stav. [zdroj: Wikipedia]

Loydova patnáctka je hra, která sestává z pole 4×4 a kachlíky očíslovanými 1 až 15. Jedno pole je prázdné a přesouváním sousedních kachlíků na prázdné pole měníme rozložení kachlíků. Cílem je dospět pomocí těchto přesunů k vzestupnému uspořádání kachlíků tak, jak je uvedeno na obrázku.

Otázka zní, které počáteční konfigurace jsou řešitelné a které ne. Jestliže očíslujeme 1 až 16 jednotlivá políčka, pak konfigurace kachlíků odpovídá nějaké permutaci $p \in S_{16}$ a přesun kachlíku odpovídá složení p s transpozicí. Označíme-li (r, s) pozici prázdného pole, pak hodnota $h = (-1)^{r+s} \operatorname{sgn}(p)$ zůstává po celou hru stejná, protože každý posun kachlíku změní o jedničku buď r nebo s, ale zároveň posun kachlíku odpovídá složení p s odpovídající transpozicí, čili i $\operatorname{sgn}(p)$ změní znaménko.

Cílová konfigurace má hodnotu $h = 1$, tedy počáteční konfigurace s $h = -1$ řešitelné být nemohou. Detailnější analýza [Výborný a Zahradník, 2002] ukáže, že všechny počáteční konfigurace s $h = 1$ už řešitelné jsou.

4.3 Tělesa

Algebraická tělesa zobecňují třídu tradičních číselných oborů jako je třeba množina reálných čísel na abstraktní množinu se dvěma operacemi a řadou vlastností. To nám umožní pracovat s maticemi (sčítat, násobit, invertovat, řešit soustavy rovnic, ...) nad jinými obory než jen nad $\mathbb{R}$.

Definice 4.22 (Těleso)**.** *Těleso* je množina $\mathbb{T}$ spolu se dvěma komutativními binárními operacemi $+$ a $\cdot$ splňující

(1) $(\mathbb{T}, +)$ je Abelova grupa, neutrální prvek značíme 0 a inverzní k a pak $-a$,

(2) $(\mathbb{T} \setminus \{0\}, \cdot)$ je Abelova grupa, neutrální prvek značíme 1 a inverzní k a pak a^{-1},

(3) $\forall a, b, c \in \mathbb{T}$: $a(b + c) = ab + ac$ (distributivita).

Z definice tělesa nutně vyplývá, že $0 \neq 1$.

Těleso se občas zavádí bez komutativity násobení a tělesu s komutativním násobením se pak říká komutativní těleso nebo pole, ale pro naše účely budeme komutativitu automaticky předpokládat. Podobně jako podgrupy můžeme zavést i pojem podtěleso jako podmnožinu tělesa, která se stejně definovanými operacemi tvoří těleso.

Příklad 4.23. Příkladem nekonečných těles je např. $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$. Množina celých čísel $\mathbb{Z}$ ale těleso netvoří, protože chybí inverzní prvky pro násobení, (např. když invertujeme hezkou celočíselnou matici, tak často vycházejí zlomky a tím pádem se dostáváme mimo obor $\mathbb{Z}$). Těleso netvoří ani čísla reprezentovaná na počítači v aritmetice s pohyblivou desetinnou čárkou – jednak nejsou operace sčítání a násobení uzavřené (pokud by výsledkem bylo hodně velké či hodně malé číslo), a jednak nejsou ani asociativní (díky zaokrouhlování). Konečná tělesa prozkoumáme později. □

Příklad 4.24 (Kvaterniony)**.** Oblíbeným příkladem těles jsou *kvaterniony*. Jedná se o zobecnění komplexních čísel přidáním dalších dvou imaginárních jednotek j a k, jejichž druhá mocnina je -1, a které jsou navíc svázány vztahem $ijk = -1$. Zatímco sčítání se definuje přirozeně, násobení je trochu komplikovanější a neplatí už pro něj komutativita. Kvaterniony pak tudíž tvoří nekomutativní těleso. Pomocí kvaternionů se dobře popisují rotace ve třírozměrném prostoru a našly využití i ve fyzikální kvantové teorii. □

Řadu pěkných vlastností zdědí těleso z vlastností příslušných grup $(\mathbb{T}, +)$ a $(\mathbb{T} \setminus \{0\}, \cdot)$. Např. distributivita zprava $(b + c)a = ba + ca$ plyne z levé distributivity a komutativity násobení. Některé specifické vlastnosti uvádíme v následující větě.

Tvrzení 4.25 (Základní vlastnosti v tělese)**.** *Pro prvky tělesa platí následující vlastnosti.*

(1) $0a = 0$,

(2) $ab = 0$ *implikuje, že* $a = 0$ *nebo* $b = 0$,

(3) $-a = (-1)a$.

Důkaz.

(1) Odvodíme

$$\begin{aligned} 0a = (0+0)a &= 0a + 0a && / + (-0a) \\ (-0a) + 0a = (0+0)a &= (-0a) + 0a + 0a \\ 0 &= 0 + 0a \\ 0 &= 0a \end{aligned}$$

(2) Je-li $a = 0$, pak věta platí. Je-li $a \neq 0$, pak existuje a^{-1}. Pronásobením obou stran rovnice $ab = 0$ zleva prvkem a^{-1} dostaneme $a^{-1}ab = a^{-1}0$, neboli $1b = 0$.

(3) Máme $0 = 0a = (1-1)a = 1a + (-1)a = a + (-1)a$, tedy $-a = (-1)a$. □

Druhá vlastnost (a její důkaz) předchozí věty mj. říkají, že při rozhodování, zda nějaká struktura tvoří těleso, nemusíme ověřovat uzavřenost násobení na množině $\mathbb{T} \setminus \{0\}$ (žádné dva nenulové prvky se nevynásobí na nulu), tato vlastnost vyplývá z ostatních. Stačí tedy jen uzavřenost na $\mathbb{T}$, což bývá snáze vidět.

Podívejme se teď na konečná tělesa. Zaveďme množinu $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ a operace $+$ a $\cdot$ modulo n. Snadno nahlédneme, že $\mathbb{Z}_2$ a $\mathbb{Z}_3$ jsou tělesy, ale $\mathbb{Z}_4$ už není, neboť prvek 2 nemá inverzi 2^{-1}. Tento výsledek můžeme zobecnit.

Lemma 4.26. *Buď n prvočíslo a buď $0 \neq a \in \mathbb{Z}_n$. Pak*

$$\{0, 1, \ldots, n-1\} = \{0a, 1a, \ldots, (n-1)a\},$$

kde prvky v množině napravo se počítají modulo n.

Důkaz. Sporem předpokládejme, že $ak = a\ell$ pro nějaké $k, \ell \in \mathbb{Z}_n$, $k \neq \ell$. Pak dostáváme $a(k-\ell) = 0$, tudíž buď a nebo $k-\ell$ je dělitelné n. To znamená buď $a = 0$ nebo $k - \ell = 0$. Ani jedna možnost ale nastat nemůže, což je spor. □

Věta 4.27. *$\mathbb{Z}_n$ je těleso právě tehdy, když n je prvočíslo.*

Důkaz. Je-li n složené, pak $n = pq$, kde $1 < p, q < n$. Kdyby $\mathbb{Z}_n$ bylo těleso, pak $pq = 0$ implikuje podle tvrzení 4.25 buď $p = 0$ nebo $q = 0$, ale ani jedno neplatí.

Je-li n prvočíslo, pak se snadno ověří všechny axiomy z definice tělesa. Jediný pracnější může být existence inverze a^{-1} pro libovolné $a \neq 0$. To ale nahlédneme snadno z lemmatu 4.26. Protože $\{0, 1, \ldots, n-1\} = \{0a, 1a, \ldots, (n-1)a\}$, musí být v množině napravo prvek 1, a tudíž existuje $b \in \mathbb{Z}_n \setminus \{0\}$ takové, že $ba = 1$. Proto $b = a^{-1}$. □

Příklad 4.28 (Těleso $\mathbb{Z}_5$)**.** Pro ilustraci uvádíme v tabulkách dole explicitní vyjádření obou operací nad tělesem $\mathbb{Z}_5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

V tabulkách se odráží některé základní vlastnosti těles: komutativita se projevuje jako symetrie tabulek, neutrální prvek kopíruje záhlaví tabulky do příslušného řádku a sloupce, a násobení nulou dává nulu. Vlastnost inverzního prvku se pak projevuje tak, že v každém řádku a sloupci (kromě násobení nulou) je uveden každý prvek tělesa právě jednou.

Inverzní prvky tělesa $\mathbb{Z}_5$ jsou pak:

x	0	1	2	3	4
$-x$	0	4	3	2	1

x	0	1	2	3	4
x^{-1}	–	1	3	2	4

□

Příklad 4.29 (Těleso $\mathbb{Z}_2$)**.** Těleso $\mathbb{Z}_2$ má pro informatiky obzvláště velký význam, protože pracuje se dvěma prvky 0 a 1, na které můžeme nahlížet jako na počítačové bity. Je snadné pak nahlédnout, že operace sčítání v $\mathbb{Z}_2$ odpovídá počítačové operaci XOR a násobení odpovídá operaci AND. □

Poznámka 4.30. Soustavy rovnic a operace s maticemi jsme zaváděli nad tělesem reálných čísel. Nicméně nic nám nebrání rozšířit tyto pojmy a pracovat nad jakýmkoli jiným tělesem. Je-li $\mathbb{T}$ těleso, pak $\mathbb{T}^{m\times n}$ bude značit matici řádu $m \times n$ s prvky v tělese $\mathbb{T}$. Jediné vlastnosti reálných čísel, který jsme používali, jsou přesně ty, které se vyskytují v definici tělesa; nepotřebovali jsme čísla odmocňovat ani mezi sebou porovnávat ani nic podobného. Proto veškeré postupy a teorie vybudovaná v předchozích kapitolách 2 a 3 zůstane v platnosti. Můžeme tak například řešit soustavy lineárních rovnic nad libovolným tělesem pomocí Gaussovy eliminace, hovořit o regularitě matice z $\mathbb{T}^{n\times n}$ či hledat její inverzi.

Příklad 4.31 (Výpočet inverzní matice nad $\mathbb{Z}_5$)**.**

$$(A \,|\, I_3) = \left(\begin{array}{ccc|ccc} 1&2&3&1&0&0\\ 2&0&4&0&1&0\\ 3&3&4&0&0&1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&2&3&1&0&0\\ 0&1&3&3&1&0\\ 0&2&0&2&0&1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&0&2&0&3&0\\ 0&1&3&3&1&0\\ 0&0&4&1&3&1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1&0&2&0&3&0\\ 0&1&3&3&1&0\\ 0&0&1&4&2&4 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1&0&0&2&4&2\\ 0&1&0&1&0&3\\ 0&0&1&4&2&4 \end{array}\right) = \left(I_3 \,|\, A^{-1}\right)$$

□

Poznámka 4.32 (Jak najít inverzi)**.** Přirozená otázka při počítání nad tělesem $\mathbb{Z}_p$ zní, jak najít inverzní prvek k $x \in \mathbb{Z}_p \setminus \{0\}$. Pro malé hodnoty p mohu zkusit postupně $1, 2, \ldots, p-1$ dokud nenarazím na inverzní prvek k x. Pokud p je hodně velké prvočíslo, tento postup už není efektivní a postupuje se tzv. *rozšířeným Eukleidovým algoritmem*, který najde $a, b \in \mathbb{Z}$ taková, že $ax + bp = 1$, z čehož vidíme, že hledanou inverzí x^{-1} je prvek a (resp. jeho zbytek po dělení p).

Nyní víme, že existují tělesa o velikostech odpovídajících prvočíslům. Existují však tělesa jiných velikostí?

Věta 4.33 (O velikosti konečných těles)**.** *Existují konečná tělesa právě o velikostech p^n, kde p je prvočíslo a $n \geq 1$.*

Důkaz vynecháme, ale ukážeme základní myšlenku, jak sestrojit těleso o velikosti p^n. Takové těleso se značí[1)] symbolem $\mathrm{GF}(p^n)$ a jeho prvky jsou polynomy stupně nanejvýš $n-1$ s koeficienty v tělese $\mathbb{Z}_p$. Sčítání je definováno analogicky jako pro reálné polynomy. Násobí se modulo ireducibilní polynom stupně n, kde ireducibilní znamená nerozložitelný na součin dvou polynomů stupně aspoň jedna (takový polynom vždy existuje).

Další zajímavá vlastnost je, že každé konečné těleso velikosti p^n je isomorfní s $\mathrm{GF}(p^n)$, to znamená, že taková tělesa jsou v zásadě stejná až na jiné označení prvků.

Příklad 4.34 (Těleso GF(8))**.** Množina má za prvky polynomy stupňů nanejvýš dva s koeficienty v $\mathbb{Z}_2$

$$\mathrm{GF}(8) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

Sčítání je definované

$$(a_2x^2 + a_1x + a_0) + (b_2x^2 + b_1x + b_0) = (a_2+b_2)x^2 + (a_1+b_1)x + (a_0+b_0),$$

např. $(x+1) + (x^2+x) = x^2+1$. Uvažme ireducibilní polynom, např. x^3+x+1. Pak násobíme modulo tento polynom, např. $x^2 \cdot x = -x-1 = x+1$, nebo $x^2 \cdot (x^2+1) = -x = x$. □

Definice 4.35 (Charakteristika tělesa)**.** *Charakteristika tělesa* $\mathbb{T}$ je nejmenší n takové, že

$$\underbrace{1+1+\ldots+1}_{n} = 0.$$

Pokud takové n neexistuje pak ji definujeme jako 0.

Tvrzení 4.36. *Charakteristika tělesa je buď nula, nebo prvočíslo.*

Důkaz. Protože $0 \neq 1$, charakteristika nemůže být 1. Pokud by byla charakteristika složené číslo $n = pq$, pak

$$0 = \underbrace{1+1+\ldots+1}_{n=pq} = (\underbrace{1+\ldots+1}_{p})(\underbrace{1+\ldots+1}_{q}),$$

tedy součet p nebo q jedniček dá nulu, což je spor s minimalitou n. □

Příklad 4.37. Jestliže charakteristika tělesa $\mathbb{T}$ není 2, tak můžeme zavést něco jako průměr. Označme symbolem 2 hodnotu $1+1$ a pak pro libovolné $a, b \in \mathbb{T}$ má číslo $p = \frac{1}{2}(a+b)$ má vlastnost $a - p = p - b$, je tedy stejně „vzdálené“ od a jako od b. (Viz důkaz věty 7.4 či příklad 12.10.)

Těleso s charakteristikou 2 je $\mathbb{Z}_2$ nebo obecněji jakékoliv těleso $\mathrm{GF}(2^n)$, kde $n \in \mathbb{N}$. V těchto tělesech tedy průměr 0 a 1 nelze zadefinovat, zatímco například v tělese $\mathbb{Z}_5$ je průměr 0 a 1 číslo 3. □

Další užitečný výsledek je *Malá Fermatova věta*[2)], používá se např. pro pravděpodobnostní test prvočíselnosti velkých čísel. Často se uvádí ve znění, že $a^{p-1} \equiv 1 \bmod p$, tedy, že čísla a^{p-1} a 1 mají stejný zbytek při dělení číslem p. V jazyce konečných těles větu formulujeme takto:

Věta 4.38 (Malá Fermatova věta)**.** *Buď p prvočíslo a buď $0 \neq a \in \mathbb{Z}_p$. Pak $a^{p-1} = 1$ v tělese $\mathbb{Z}_p$.*

Důkaz. Podle lemmatu 4.26 je $\{0, 1, \ldots, p-1\} = \{0a, 1a, \ldots, (p-1)a\}$. Protože $0 = 0a$, tak dostáváme $\{1, \ldots, p-1\} = \{1a, \ldots, (p-1)a\}$. Tudíž $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = (1a) \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a$. Zkrácením obou stran čísly $1, 2, \ldots, p-1$ získáme požadovanou rovnost $1 = a \cdots a$. □

Příklad 4.39. Jaká je hodnota 2^{111} v tělese $\mathbb{Z}_{11}$? Podle Malé Fermatovy věty je $2^{10} = 1$, tudíž i $2^{110} = 1$. Proto $2^{111} = 2^{110+1} = 2^{110}2^1 = 2$. □

[1)] GF = Galois field, tedy Galoisovo těleso.

[2)] Malá Fermatova věta byla formulována francouzským právníkem a amatérským matematikem Pierre de Fermatem r. 1640. Pro srovnání, Velká Fermatova věta z r. 1637 pak říká, že neexistují přirozená čísla x, y, z splňující rovnici $x^n + y^n = z^n$ pro $n > 2$. Tato věta zůstávala dlouho jako otevřený problém bez důkazu až ji r. 1993 dokázal britský matematik Andrew Wiles.

4.4 Aplikace

Konečná tělesa se používají např. v kódování a šifrování. Na závěr této kapitoly ukážeme praktické využití těles právě v kódování, viz [Tůma, 2003, kap. 11]. Jinou ukázkou použití je tzv. „Secret sharing“, viz [Tůma, 2003, kap. 4].

Příklad 4.40 (Samoopravné kódy – Hammingův kód $(7,4,3)$)**.** Uvažujme problém přenosu dat, která jsou tvořena posloupností nul a jedniček. Zatímco úlohou šifrování je transformovat data tak, aby je nikdo nepovolaný nepřečetl, úlohou kódování je zlepšit jejich přenosové vlastnosti. Tím myslíme zejména umět detekovat a opravit chyby, které při přenosu přirozeně vznikají.

Kódování vesměs funguje tak, že odesílatel rozdělí binární posloupnost na úseky o délce k. Každý úsek pak určitou metodou přetransformuje na úsek délky k', který pak odešle. Příjemce dat pak transformuje každý úsek na původní hodnoty. Podle zvolené metody je pak schopen detekovat nebo i rovnou opravit určitý počet chyb, které v úseku vznikly.

Jednoduchý příklad. Pokud kódujeme tak, že zdvojíme každý bit, tedy např. úsek $v = 010$ zakódujeme na $v' = 001100$, tak jsme schopni detekovat maximálně jednu chybu v každém úseku. Nicméně, neumíme data opravit. Pokud budeme kódovat tak, že každý bit ztrojíme, tedy např. úsek $v = 010$ zakódujeme na $v' = 000111000$, tak už jsme schopni nejen detekovat, ale i opravit jednu chybu. Pokud příjemce dostane úsek 000111010, ví, že původní úsek byl 000111000, anebo došlo aspoň ke dvěma přenosovým chybám. Tento způsob kódování je značně neefektivní, ukážeme šikovnější způsob.

Hammingův kód $(7,4,3)$ spočívá v rozdělení přenosových dat na úseky o čtyřech bitech, které zakódujeme na sedm bitů. Tento kód umí detekovat a opravit jednu přenosovou chybu. Kódování a dekódování jde elegantně reprezentovat maticovým násobením. Úsek čtyř bitů si představíme jako aritmetický vektor a nad tělesem $\mathbb{Z}_2$. Kódování probíhá vynásobením vektoru a takzvanou generující maticí $H \in \mathbb{Z}_2^{7\times 4}$,

$$\text{např.: } Ha = \begin{pmatrix} 1&1&0&1\\ 1&0&1&1\\ 1&0&0&0\\ 0&1&1&1\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix} \begin{pmatrix} \mathbf{0}\\ \mathbf{1}\\ \mathbf{1}\\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} 1\\ 1\\ \mathbf{0}\\ 0\\ \mathbf{1}\\ \mathbf{1}\\ \mathbf{0} \end{pmatrix} = b.$$

Příjemce obdrží úsek reprezentovaný vektorem b. Bity původních dat jsou na zvýrazněných pozicích b_3, b_5, b_6, b_7, ostatní bity b_1, b_2, b_4 jsou kontrolní. K detekci a opravě chyb používá příjemce detekční matici $D \in \mathbb{Z}_2^{3\times 7}$. Pokud $Db = 0$, nedošlo k žádné chybě v přenosu (nebo nastaly více než dvě chyby). V opačném případě nastala přenosová chyba a chybný bit je na pozici Db, bereme-li tento vektor jako binární zápis přirozeného čísla.

$$\text{např.: } Db = \begin{pmatrix} 0&0&0&1&1&1&1\\ 0&1&1&0&0&1&1\\ 1&0&1&0&1&0&1 \end{pmatrix} \begin{pmatrix} 1\\ 1\\ 0\\ 0\\ 1\\ 1\\ 0 \end{pmatrix} = \begin{pmatrix} 0\\ 0\\ 0 \end{pmatrix} \ldots \text{v pořádku.}$$

$$\text{např.: } Db = \begin{pmatrix} 0&0&0&1&1&1&1\\ 0&1&1&0&0&1&1\\ 1&0&1&0&1&0&1 \end{pmatrix} \begin{pmatrix} 1\\ 1\\ 0\\ 0\\ 1\\ \mathbf{0}\\ 0 \end{pmatrix} = \begin{pmatrix} 1\\ 1\\ 0 \end{pmatrix} \ldots \text{chyba na pozici } 110_2 = 6.$$

Jak to, že chybný bit najdeme tak snadno? Protože vektor $Db = (1,1,0)^T$ je obsažen v matici D v šestém sloupečku, stačí změnit šestý bit vektoru b a už bude platit rovnost $Db = 0$. Všimněme si, že matice D obsahuje ve sloupcích všechny nenulové vektory, tedy všechny možné výsledky součinu Db jsou pokryty. Navíc sloupce matice D vyjadřují v binárním zápisu čísla 1 až 7, proto určíme index pokaženého bitu pomocí dvojkového vyjádření vektoru Db.

Popsat obecnou konstrukci matic H a D by bylo na pokročilou přednášku šifrování. Nicméně ještě několik podrobností k matici D zmíníme v příkladu 5.69. □

Problémy

4.1. Buď G konečná grupa a H její podgrupa. Dokažte, že velikost G je dělitelná velikostí H. Při důkazu možná využijete následující mezikroky:

(a) označme $aH \coloneqq \{ah;\, h \in H\}$[3)],

(b) pro každé $a, b \in G$ platí buď $aH = bH$, anebo $aH \cap bH = \emptyset$,

(c) pro každé $a \in G$ platí, že velikost aH je stejná jako velikost H.

4.2. Pro permutaci $p \in S_n$ definujme matici $P \in \mathbb{R}^n$ tak, že $P_{ij} = 1$ pokud $p(i) = j$ a nula jinak. Ukažte, že tato definice je ekvivalentní definici permutační matice ze sekce 3.5.2. Dále zjistěte, jak vypadá permutační matice inverzní permutace a permutační matice složení dvou permutací.

4.3. Dokažte vlastnost z poznámky 4.20.

4.4. Spočítejte průměrný počet cyklů v n-prvkové permutaci.

4.5. Určete pravděpodobnost, že náhodně zvolená permutace $p \in S_n$ má cyklus obsahující prvek 1 dlouhý přesně k.

[3)] Tato množina se nazývá levý koset.

Shrnutí ke kapitole 4. Grupy a tělesa

Grupy představují první abstraktní pojem, se kterým jsme se setkali. Grupa je jakákoli množina, na které máme zavedenou operaci splňující několik základních vlastností (asociativita, neutrální a inverzní prvek, případně komutativita). Právě tato abstraktní definice umožňuje obsáhnout velkou řadu objektů a tak rozšiřuje pole působnosti. Jako význačný příklad nekomutativní grupy jsme probírali permutace s operací skládání.

Algebraická tělesa jsou oproti grupám bohatší o další operaci. Tělesem je tedy množina se dvěma operacemi, splňujícími určité vlastnosti. Maticové operace probírané v minulých kapitolách tak směle lze rozšířit a pracovat nad libovolným tělesem, nikoliv jen nad $\mathbb{R}$; veškeré výsledky zůstanou v zásadě v platnosti. Známe nekonečná tělesa jako například $\mathbb{R}$ či $\mathbb{C}$, a konečná tělesa jako například informatikům blízké dvojprvkové těleso $\mathbb{Z}_2$. Konečná tělesa existují právě o velikosti p^n, kde p je prvočíslo.