Kapitola 1

Grupy

1.1 Množiny s jednou binární operací

Připomeňme několik pojmů.

1.1.1 Grupoid. Binární operace na množině S je každé zobrazení množiny všech uspořádaných dvojic $S \times S$ do množiny S. Binární operace budeme značit buď $\cdot$, nebo $+$, $\circ$, $*$ atd. (Prvkům x, y binární operace $\circ$ přiřazuje prvek $x \circ y$.)

Dvojice $(S, \circ)$, kde S je množina a $\circ$ je binární operace na S, se nazývá *grupoid*.

1.1.2 Pologrupy. Máme dánu binární operaci $\circ$ na množině S. Jestliže pro každé $x, y, z \in S$ platí

$$x \circ (y \circ z) = (x \circ y) \circ z \tag{1.1}$$

nazývá se množina S spolu s binární operací $\circ$ *pologrupa*.

Vlastnosti 1.1 říkáme asociativní zákon. Pologrupa je tedy každý grupoid, který splňuje asociativní zákon.

1.1.3 Jednotkový (neutrální) prvek. Máme dán grupoid $(S, \circ)$. Prvek $e \in \in S$ se nazývá *jednotkovým* (též *neutrálním*) prvkem právě tehdy, když

$$e \circ x = x = x \circ e \quad \text{pro každé } x \in S. \tag{1.2}$$

O neutrálním prvku mluvíme, jestliže se operace značí $+$ a říkáme jí sčítání. Značíme-li operaci podobně jako násobení, mluvíme častěji o jednotkovém prvku.

1.1.4 Monoidy. Pologrupa se nazývá *monoid*, má-li jednotkový prvek. Monoid obvykle značíme $(S, \circ, e)$, kde e je jednotkový prvek pologrupy $(S, \circ)$.

1.1.5 Invertibilní prvky. Mějme dán monoid $(S, \circ, e)$. Řekneme, že prvek $a \in S$ je *invertibilní*, jestliže existuje prvek $y \in S$ takový, že

$$a \circ y = e = y \circ a.$$

1.1.6 Inversní prvek. Je dán monoid $(S, \circ, e)$ a invertibilní prvek $a \in S$. Pak prvek y splňující 1.1.5 je určen jednoznačně a nazýváme jej *inversní prvek* k prvku a a značíme jej a^{-1}.

1.1.7 Grupy. Monoid $(S, \circ, e)$ se nazývá *grupa*, jestliže každý prvek je invertibilní; tj. ke každému prvku $a \in S$ existuje inversní prvek a^{-1}.

1.1.8 Tvrzení. V každém monoidu $(S, \circ, e)$ platí:

1. Jednotkový prvek e je invertibilní a $e^{-1} = e$.
2. Je-li a invertibilní prvek, pak také a^{-1} je invertibilní prvek a platí
$$(a^{-1})^{-1} = a.$$
3. Jsou-li $a, b \in S$ dva invertibilní prvky, pak také $a \circ b$ je invertibilní prvek a platí
$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

1.1.9 Podgrupa invertibilních prvků. Je dán monoid $(S, \circ, e)$. Označme N podmnožinu S tvořenou všemi invertibilními prvky monoidu $(S, \circ, e)$. Pak platí:

- N obsahuje e,
- $\circ$ je operace na množině N,
- $(N, \circ, e)$ je grupa.

1.2 Grupy

1.2.1 Tvrzení. Je dána grupa $(G, \circ, e)$. Pak pro každé dva prvky $a, b \in G$ existují jednoznačně prvky $x, y \in G$ takové, že

$$a \circ x = b \quad \text{a} \quad y \circ a = b.$$

Jinými slovy, každá rovnice tvaru $a \circ x = b$ a $y \circ a = b$ je jednoznačně řešitelná.

1.2.2 Věta. Pologrupa $(S, \circ)$ je grupou právě tehdy, když pro každé dva prvky $a, b \in S$ existují prvky $x, y \in S$ takové, že

$$a \circ x = b \quad \text{a} \quad y \circ a = b.$$

Jinými slovy, pologrupa je grupou právě tehdy, když každá rovnice tvaru $a \circ x = b$ a $y \circ a = b$ má řešení.

1.2.3 Komutativní pologrupa, monoid, grupa. Pologrupa, monoid, grupa se nazývá *komutativní*, jestliže platí tzv. *komutativní zákon*, tj. pro každé dva prvky x, y platí

$$x \circ y = y \circ x.$$

Komutativní grupa se též nazývá *Abelova grupa*.

1.2.4 Věta. Je dána konečná grupa $(G, \circ, e)$ s jednotkovým prvkem e taková, že G má n prvků. Pak pro každý prvek $a \in G$ platí

$$a^n = e,$$

kde $a^n = a \circ a \circ \ldots \circ a$ (prvek a „násobíme“ n-krát sám se sebou).

1.2.5 Zbytkové třídy modulo n. Je dáno přirozené číslo $n > 1$. Pro každé $i = 0, 1, \ldots, n-1$ označme

$$[i]_n = \{i + kn | k \in \mathbb{Z}\}.$$

Jinými slovy, množina $[i]_n$ je množina všech celých čísel, jejichž zbytek při dělení číslem n je i.

Poznamenejme, že množinám $[i]_n$ se říká *zbytkové třídy.*

Na množině $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ definujeme binární operace $\oplus$ a $\odot$ předpisem

$$[a]_n \oplus [b]_n = [c]_n,$$

kde c je zbytek při dělení čísla $a + b$ číslem n. Podobně

$$[a]_n \odot [b]_n = [d]_n,$$

kde d je zbytek při dělení čísla $a \cdot b$ číslem n.

1.2.6 Tvrzení.

- $(\mathbb{Z}_n, \oplus, [0]_n)$ je komutativní grupa.
- $(\mathbb{Z}_n, \odot, [1]_n)$ je komutativní monoid, který nikdy netvoří grupu, protože prvek $[0]_n$ není invertibilní.
- Jestliže n je prvočíslo, každá zbytková třida kromě $[0]_n$ je invertibilní prvek v $(\mathbb{Z}_n, \odot, [1]_n)$.

1.2.7 Podle 1.1.9 všechny invertibilní prvky monoidu $(\mathbb{Z}_n, \odot, [1]_n)$ tvoří grupu; tuto grupu značíme $(\mathbb{Z}_n^*, \odot, [1]_n)$ a nazýváme *grupou invertibilních prvků* $(\mathbb{Z}_n, \odot, [1]_n)$.

1.2.8 Eulerova funkce. Je dáno přirozené číslo n. Pak hodnota Eulerovy funkce $\varphi(n)$ je rovna počtu všech přirozených čísel i, $0 \leq i < n$, která jsou nesoudělná s číslem n.

Tedy např. $\varphi(6) = 2$, protože mezi 0 a 6 jsou pouze dvě nesoudělná čísla s 6 a to 1 a 5.

Poznamenejme, že grupa invertibilních prvků $(\mathbb{Z}_n^*, \odot, [1]_n)$ má přesně $\varphi(n)$ prvků.

1.2.9 Vlastnosti Eulerovy funkce.

1. Je-li p prvočíslo, pak $\varphi(p) = p - 1$.
2. Je-li p prvočíslo, pak $\varphi(p^k) = p^k - p^{k-1}$.
3. Jestliže n a m jsou nesoudělná přirozená čísla, pak $\varphi(n\,m) = \varphi(n) \cdot \varphi(m)$.

1.2.10 Euler - Fermatova věta. Je dáno přirozené číslo $n > 1$. Pak pro každé celé číslo a nesoudělné s n platí

$$a^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\, n).$$

Věta je přímým důsledkem 1.2.4, 1.2.7 a 1.2.8.

1.2.11 Poznámka. Jestliže číslo n je prvočíslo, pak $\varphi(n) = n-1$ a předchozí věta se nazývá Malá Fermatova věta.

1.3 Čínská věta o zbytcích

Připomeňme, že pracujeme-li se zbytkovými třídami modulo n, pracujeme vlastně s ekvivalencí *modulo* n, kterou jsme mohli definovat jedním z následujících způsobů: Je dáno přirozené číslo $n > 1$.

- $a \equiv b \,(\mathrm{mod}\, n)$, právě tehdy, když jejich rozdíl $a - b$ je dělitelný číslem n;
- $a \equiv b \,(\mathrm{mod}\, n)$, právě tehdy, když $a = b + kn$ pro nějaké celé číslo k;
- $a \equiv b \,(\mathrm{mod}\, n)$, právě tehdy, když a i b mají stejné zbytky při dělení n.

Uvědomme si, že dvě celá čísla a, b patří do stejné zbytkové třídy modulo n právě tehdy, když $a \equiv b \,(\mathrm{mod}\, n)$. Proto např. rovnice $[a]_n \cdot [x]_n = [b]_n$ odpovídá vztahu $a \cdot x \equiv b \,(\mathrm{mod}\, n)$.

1.3.1 Čínská věta o zbytcích. Jsou dána přirozená čísla $m_1, m_2, \ldots, m_k$ po dvou nesoudělná. Pak pro libovolná celá čísla $a_1, a_2, \ldots, a_k$ existuje celé číslo x takové, že

$$\begin{aligned} x &\equiv a_1 \,(\mathrm{mod}\, m_1) \\ x &\equiv a_2 \,(\mathrm{mod}\, m_2) \\ &\ldots \\ x &\equiv a_k \,(\mathrm{mod}\, m_k) \end{aligned} \tag{1.3}$$

Jestliže nějaké celé číslo y také splňuje 1.3, pak nutně $x \equiv y \,(\mathrm{mod}\, N)$, kde N je součin všech m_i, tj. $N = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

1.3.2 Nalezení x splňující 1.3. Stačí najít celá čísla $q_1, q_2, \ldots, q_k$ taková, že pro každé $i = 1, 2, \ldots, k$ platí

$$q_i \equiv 1 \,(\mathrm{mod}\, m_i) \text{ a } q_i \equiv 0 \,(\mathrm{mod}\, m_j) \text{ pro } j \neq i. \tag{1.4}$$

Pak námi hledané číslo x bude mít tvar:

$$x = a_1\, q_1 + a_2\, q_2 + \ldots + a_k\, q_k.$$

Čísla $q_1, q_2, \ldots, q_k$ nalezneme např. takto (pro jednoduchost ukážeme, jak najdeme číslo q_1, ostatní se hledají analogicky): Utvoříme číslo $M_1 = m_2 \cdot m_3 \cdot \ldots \cdot m_k$. Protože jsou čísla $m_1, m_2, \ldots, m_k$ po dvou nesoudělná, jsou nesoudělná i čísla m_1 a M_1. Proto (podle Bezoutovy věty) existují celá čísla t_1 a t_2 taková, že

$$m_1 \cdot t_1 + M_1 \cdot t_2 = 1.$$

Nyní číslo $q_1 = M_1 \cdot t_2$ má požadované vlastnosti. Ano, $M_1 \cdot t_2$ je dělitelné všemi m_i pro $i \neq 1$ a $M_1 \cdot t_2 \equiv 1 \,(\mathrm{mod} m_1)$.

(Uvědomte si, že číslo t_2 je vlastně inversní prvek k číslu M_1 v $(\mathbb{Z}_{m_1}, \odot)$).

1.3.3 Využití Čínské věty o zbytcích pro výpočet Eulerovy funkce. V 1.2.8 jsme si uvedli následující vlastnost Eulerovy funkce $\varphi(n)$:

Jestliže n a m jsou nesoudělná přirozená čísla, pak $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$. S využitím Čínské věty o zbytcích se o této vlastnosti můžeme přesvědčit.

Pro jednoduchost zjednodušíme značení zbytkových tříd: budeme psát $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ místo zdlouhavého $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ a dále budeme psát $+$ a $\cdot$ místo $\oplus$ a $\odot$. Přitom budeme mít na paměti, že mluvíme-li o sčítání a násobení v $\mathbb{Z}_n$ jedná se vždy o operace se zbytkovými třídami a ne operace s celými čísly.

Máme dáno přirozené číslo $n \cdot m$, kde n a m jsou nesoudělná čísla. Pak $\mathbb{Z}_{n \cdot m} = \{0, 1, \ldots, n \cdot m - 1\}$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ a $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. Čínská věta nám nyní dává jednoznačné přiřazení

$$a \longmapsto (a_n, a_m),$$

kde a_n je zbytek při dělení čísla a číslem n, a_m je zbytek při dělení čísla a číslem m. Jedná se tedy o vzájemně jednoznačné zobrazení

$$f : \mathbb{Z}_{n \cdot m} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m.$$

Z vlastností kongrunence modulo víme, že jestliže

$$\begin{array}{rcl} a & \longmapsto & (a_1, a_2, \ldots, a_k), \\ b & \longmapsto & (b_1, b_2, \ldots, b_k), \end{array}$$

pak také platí

$$a\,b \quad \longmapsto \quad (a_1\,b_1, a_2\,b_2, \ldots, a_k\,b_k). \tag{1.5}$$

Jedná se tedy o vzájemně jednoznačné zobrazení mezi invertibilními prvky $\mathbb{Z}_{n \cdot m}$ a dvojicemi invertibilních prvků $\mathbb{Z}_n$ a $\mathbb{Z}_m$, neboť $1 \mapsto (1, 1)$ a pro $a \cdot b = 1$ je $(a_n\,b_n, a_m\,b_m) = (1, 1)$. Proto dostáváme vzájemně jednoznačné zobrazení

$$f : \mathbb{Z}^*_{n \cdot m} \longrightarrow \mathbb{Z}^*_n \times \mathbb{Z}^*_m.$$

Navíc, počet prvků $\mathbb{Z}^*_{n\,m}$ je $\varphi(n \cdot m)$, obdobně počet prvků $\mathbb{Z}^*_n$ je $\varphi(n)$ a počet prvků $\mathbb{Z}^*_m$ je $\varphi(m)$. Proto

$$\varphi(n \cdot m) = \varphi(n)\,\varphi(m).$$

1.4 Podgrupy

Neformálně řečeno, podgrupa je podmnožina grupy, která je uzavřena na všechny tři operace: $\circ$, e a *tvorbu inverzních prvků.*

1.4.1 Značení. Pro jednoduchost budeme v dalším textu značit jednotkový prvek grupy jako 1. Grupa tedy bude trojice $(G, \circ, 1)$. Budeme-li mít na mysli celou trojici, budeme ji značit $\mathcal{G}$, množinu prvků grupy $\mathcal{G}$ vždy značíme G.

1.4.2 Podgrupa. Máme dánu grupu $(G, \circ, 1)$ (kde inversní prvek k prvku a značíme a^{-1}). Řekneme, že podmnožina $H \subseteq G$ spolu s operací $\circ$ tvoří *podgrupu* grupy $(G, \circ, 1)$ právě tehdy, když

1. Pro každé dva prvky $x, y \in H$ je $x \circ y \in H$, (tj. množina H je uzavřena na operaci $\circ$).

2. $1 \in H$, (tj. množina H je uzavřena na jednotkový prvek).

3. Pro každé $x \in H$ je $x^{-1} \in H$, (tj. množina H je uzavřena na tvorbu inversního prvku).

(V tomto případě množina $(H, \circ, 1)$ je také grupa.)

1.4.3 Příklady podgrup.

1. Množina všech sudých přirozených čísel S tvoří podgrupu grupy $(\mathbb{Z}, +, 0)$.

2. Množina všech čtvercových matic, jejichž determinant je roven 1, tvoří podgrupu grupy $(R_n, \cdot, \mathbf{E})$, kde R_n je množina všech regulárních čtvercových matic a $\cdot$ je násobení matic.

3. Množina všech kladných reálných čísel tvoří podgrupu grupy $(\mathbb{R} \setminus \{0\}, \cdot, 1)$ všech nenulových reálných čísel, kde $\cdot$ je násobení reálných čísel.

4. Množina všech komplexních čísel, jejichž velikost je 1, tvoří podgrupu grupy $(C, \cdot, 1)$, kde C je množina všech nenulových komplexních čísel a $\cdot$ je násobení komplexních čísel.

1.4.4 Triviální podgrupy. Každá grupa $(G, \circ, 1)$ má aspoň dvě podgrupy; jedna je tvořena množinou obsahující pouze jednotkový prvek $\{1\}$ a druhá celou množinou G. Těmto podgrupám se říká *triviální podgrupy.*

1.4.5 Poznámka. Často se říká, že množina $H \subseteq G$ *je podgrupa* grupy $\mathcal{G}$, místo přesného H *tvoří podgrupu* grupy $\mathcal{G}$. Je to v případě, kdy je z kontextu jasné o jaké operace se jedná. I my tuto konvenci budeme používat.

1.4.6 Věta. Je dána konečná grupa $(G, \circ, 1)$ a její podgrupa H. Pak počet prvků H dělí počet prvků G.

1.4.7 Nástin zdůvodnění věty 1.4.6. Označme $n = |G|$ a $k = |H|$. Pro každé $g \in G$ vytvoříme množinu $g \circ H = \{g \circ x \,|\, x \in H\}$. Pro různá $g_1, g_2 \in G$ jsou množiny $g_1 \circ H$ a $g_2 \circ H$ buď stejné nebo disjunktní. Protože $g \in g \circ H$ a tudíž každý prvek G leží v některé množině $g \circ H$, tvoří $\{g \circ H \,|\, g \in G\}$ rozklad množiny G.

Všechny množiny $g \circ H$ mají stejný počet prvků, navíc protože $1 \circ H = H$, je tento počet roven k. Je tedy množina G o n prvcích rozdělena na několik množin o k prvcích, proto k dělí n. (Uvědomte si, že různých množin $g \circ H$ je přesně n/k.)

1.4.8 Poznámka. Pro podpologrupy dané pologrupy podobná věta neplatí.

1.4.9 Řád grupy. Mějme konečnou grupu $\mathcal{G} = (G, \circ, 1)$. Pak počet prvků množiny G se nazývá *řád grupy* $\mathcal{G}$.

Věta 1.4.6 mohla znít také takto: Řád libovolné podgrupy dané grupy $\mathcal{G}$ dělí řád grupy $\mathcal{G}$.

1.4.10 Mějme konečnou grupu $(G, \circ, 1)$ a zvolme její prvek $a \in G$. Označme a^i součin i-krát prvku a sama se sebou, přesněji

$$a^0 = 1,\ a^1 = a,\ a^i = a^{i-1} \circ a.$$

Utvoříme množinu

$$\{a, a^2, a^3, \ldots, a^k, \ldots\}.$$

Protože G je konečná množina, musí existovat i, j takové, že $i \neq j$ a $a^i = a^j$. Můžeme předpokládat, že $i < j$, tj. že jsme jako i označili ten menší exponent. Protože pracujeme v grupě, existuje inversní prvek k prvku a, tj. existuje a^{-1} takové, že $a^{-1} \circ a = 1$. Tedy $a^i = a^j$ implikuje $a^{i-1} = a^{j-1}$, atd. až $1 = a^{j-i}$.

Označme $r(a)$ to nejmenší kladné přirozené číslo, pro které $a^{r(a)} = 1$.

1.4.11 Podgrupa generovaná prvkem. Mějme konečnou grupu $(G, \circ, 1)$ a její prvek $a \in G$. Množina

$$\{a, a^2, \ldots, a^{r(a)} = 1\}$$

kde $r(a)$ je definováno v 1.4.10 tvoří podgrupu, která se nazývá *podgrupa generovaná prvkem* a a značíme ji $\langle a \rangle$.

Číslo $r(a)$ se nazývá *řád prvku* a. Uvědomte si, že se vlastně jedná o řád podgrupy $\langle a \rangle$.

1.4.12 Tvrzení. Mějme konečnou grupu $(G, \circ, 1)$ o n prvcích. Pak řád každého prvku $a \in G$ dělí řád grupy $(G, \circ, 1)$.

1.4.13 Věta. Mějme konečnou grupu $(G, \circ, 1)$ o n prvcích. Pak pro každý její prvek $a \in G$ platí

$$a^n = 1.$$

1.4.14 Poznámka. I v případě nekonečné grupy $\mathcal{G} = (G, \circ, 1)$ definujeme podgrupu generovanou prvkem $a \in G$ a to takto:

$$\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}, \tag{1.6}$$

kde $a^0 = 1$ a $a^{-i} = (a^{-1})^i$. Není těžké se přesvědčit, že množina (1.7) je i v tomto případě podgrupou grupy $\mathcal{G} = (G, \circ, 1)$.

1.4.15 Generátor grupy. Je dána grupa $\mathcal{G} = (G, \circ, 1)$. Jestliže pro prvek $a \in G$ platí, že $\langle a \rangle = G$, pak se prvek a nazývá *generátor grupy* $\mathcal{G}$.

1.4.16 Cyklická grupa. Každá grupa, která má generátor se nazývá *cyklická grupa*.

Poznamenejme, že o cyklické grupě mluvíme i v případě, že se jedná o nekonečnou grupu.

1.4.17 Příklady.

1. Pro každé přirozené číslo $n > 1$ je grupa $(\mathbb{Z}_n, +, 0)$ cyklická grupa s generátorem 1.
2. Pro každé prvočíslo p je grupa $(\mathbb{Z}_p^\star, \cdot, 1)$ cyklická grupa. Najít její generátor není vždy jednoduché.
3. Grupa $(\mathbb{Z}_8^\star, \cdot, 1)$ není cyklická; skládá se ze čtyř prvků: $\mathbb{Z}_8^\star = \{1, 3, 5, 7\}$ a $3^2 = 1$, $5^2 = 1$ a $7^2 = 1$.
4. Grupa $(\mathbb{Z}, +, 0)$ všech celých čísel se sčítáním je nekonečná cyklická grupa s generátorem 1.

1.4.18 Pozorování. Konečná grupa $\mathcal{G} = (G, \circ, 1)$ řádu n (tj. o n prvcích) je cyklická právě tehdy, když v ní existuje prvek řádu n.

1.4.19 Tvrzení. Je dána konečná grupa $\mathcal{G} = (G, \circ, 1)$ a její prvek $a \in G$. Číslo r je řád prvku a právě tehdy, když platí následující dvě podmínky

1. $a^r = 1$
2. jestliže $a^t = 1$ pro nějaké kladné celé číslo t, pak r dělí t.

Toto tvrzení jsme mohli formulovat také takto: Řád prvku a je takové číslo $r > 0$, pro nějž platí:

$$a^t = 1 \quad \text{právě tehdy, když} \quad t = k \cdot r \ \text{ pro nějaké } \ k \in \mathbb{Z}.$$

1.4.20 Tvrzení. Mějme konečnou grupu $\mathcal{G} = (G, \circ, 1)$ a prvek $a \in G$ řádu $r(a)$. Pak prvek a^i má řád:

$$r(a^i) = \frac{r(a)}{\gcd(r(a), i)}$$

1.4.21 Podgrupa generovaná prvkem v obecných grupách. Pro konečné grupy $\mathcal{G}$ jsme definovali podgrupu generovanou prvkem $a \in G$. To můžeme udělat i v případě nekonečných grup. Je dána (obecná) grupa $\} = (G, \circ, 1)$ a prvek $a \in G$. Podgrupa generovaná prvkem a je

$$\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}, \tag{1.7}$$

kde $a^0 = 1$ a $a^{-i} = (a^{-1})^i$. Není těžké se přesvědčit, že tato množina také tvoří podgrupu grupy $\mathcal{G}$.

1.4.22 Poznámka. Jestliže pro prvek a existují celá čísla $i \neq j$ taková, že $a^i = a^j$, pak $\langle a \rangle$ je konečná a má tvar jaký je uveden v 1.4.11. Pro nekonečné grupy však taková celá čísla nemusí existovat a množna $\langle a \rangle$ je v takovém případě nekonečná. Stačí si uvědomit, že pro grupu $(\mathbb{Z}, +, 0)$ platí $\langle 1 \rangle = \mathbb{Z}$.

1.4.23 Pojmy generátor grupy a cyklická grupa se používají i pro nekonečné grupy. Tedy např. grupa $(\mathbb{Z}, +, 0)$ je cyklická a má generátor 1.

1.4.24 Věta. Je-li p prvočíslo, pak grupa $\mathbb{Z}_p^\star$ je cyklická grupa.

1.4.25 Tvrzení. Mějme konečnou grupu $\mathcal{G} = (G, \circ, 1)$ a prvek $a \in G$ řádu $r(a)$. Pak prvek a^i má řád:

$$r(a^i) = \frac{r(a)}{\gcd(r(a), i)}.$$

1.4.26 Pozorování. Předchozí věta nám dává návod, jak spočítat řády všech prvků b z podgrupy $\langle a \rangle$. O podgrupě $\langle a \rangle$ víme, že je cyklická a a je její generátor. Můžeme proto na každý prvek $b \in \langle a \rangle$ použít tvrzení 1.4.25. Speciálně, známe-li generátor cyklické grupy, můžeme spočítat řády všech prvků této grupy.

1.4.27 Důsledek. Mějme konečnou cyklickou grupu $\mathcal{G} = (G, \circ, 1)$ o n prvcích. Pak $\mathcal{G}$ má $\varphi(n)$ generátorů.

Důvod: Označme a některý generátor grupy $\mathcal{G}$. Pak a^i je také generátor $\mathcal{G}$ právě tehdy, když je i nesoudělné s n.

1.4.28 Tvrzení. Mějme konečnou cyklickou grupu $\mathcal{G} = (G, \circ, 1)$ o n prvcích. Pak pro každé číslo d, které dělí n existuje podgrupa $\mathcal{G}$ o d prvcích.

Důvod: Označme a některý generátor grupy $\mathcal{G}$. Pak hledaná podgrupa je podgrupa generovaná prvkem a^k, kde $k = \frac{n}{d}$; tj.

$$\langle a^k \rangle = \{a^k, a^{2k}, \ldots, a^{dk} = 1\}.$$

1.4.29 Poznámka. Konečná cyklická grupa má všechny podgrupy cyklické, a to výše uvedeného tvaru.

Důvod: Mějme cyklickou grupu s generátorem a. Vezměme dva prvky této grupy, řekněme a^i a a^j. Podgrupa, která tyto prvky obsahuje, obsahuje též všechny prvky tvary a^{ix+jy}, kde x a y jsou libovolná celá čísla. Z Bezoutovy věty víme, že rovnice $ix + jy = k$ má celočíselné řešení právě tehdy, když největší společný dělitel čísel i a j dělí číslo k. Odtud plyne, že nejmenší podgrupa obsahující prvky a^i a a^j je $\langle a^d \rangle$, kde d je největší společný dělitel čísel i a j.

1.4.30 Tvrzení. Pro každé přirozené číslo $n > 1$ platí

$$n = \sum_{d \mid n} \varphi(d), \quad \text{kde } \varphi(1) = 1.$$

1.5 Řešení rovnic $x^k = 1$

Využijeme znalosti, které máme o řádech prvků v konečné grupě, k řešení rovnic

$$x^k = 1 \tag{1.8}$$

1.5.1 Pozorování. Mějme konečný monoid $\mathcal{M} = (M, \circ, 1)$. Pak prvek $g \in M$ je řešením rovnice (1.8) právě tehdy, když je prvkem podgrupy $\mathcal{G}$ invertibilních prvků monoidu $\mathcal{M}$ a jeho řád v $\mathcal{G}$ dělí číslo k. Znamená to, že rovnici umíme vyřešit, jsme-li schopni najít všechny prvky podgrupy invertibilních prvků, jejichž řád dělí k.

My tento problém vyřešíme v konečných cyklických grupách (známe-li generátor této grupy) a v monoidech $(\mathbb{Z}_n, \cdot, 1)$ pro ta n, která jsou součinem různých prvočísel. (Poznamenejme, že takovým číslů se v angličtině říká „square free“.)

1.5.2 Řešení $x^k = 1$ v cyklické grupě. Mějme konečnou cyklickou grupu $\mathcal{G} = (G, \circ, 1)$ o n prvcích a označme a některý její generátor. Jestliže k dělí n, pak rovnice (1.8) má právě k řešení a totiž všechny prvky podgrupy $\langle a^d \rangle$, kde $n = k \cdot d$.

Jestliže k nedělí n, označme $d = \gcd(k, n)$. Nyní d dělí n a rovnice (1.8) má právě d řešení a to všechny prvky podgrupy $\langle a^l \rangle$, kde $n = l \cdot d$.

1.5.3 Poznámka. Řešit rovnice $x^k = 1$ jsme schopni i v konečných grupách, které nejsou cyklické. Řešením jsou všechny prvky grupy, jejichž rád dělí číslo k. V případě cyklických grup víme kolik řešení je a umíme všechna řešení snadněji najít.

1.5.4 Řešení $x^k = 1$ v $\mathbb{Z}_p$, kde p je prvočíslo. Protože pro každé prvočíslo p je grupa $(\mathbb{Z}_p^\star, \cdot, 1)$ cyklická (uvědomte si, že se jedná o podgrupu invertibilních prvků monoidu $(\mathbb{Z}_p, \cdot, 1)$), má každá rovnice (1.8) d řešení v $(\mathbb{Z}_p^\star, \cdot, 1)$, a tedy i v $(\mathbb{Z}_p, \cdot)$, kde

$$d = \gcd(p - 1, k).$$

Problém vyřešit tuto rovnici se tedy redukuje na problém nalezení některého prvku a grupy $(\mathbb{Z}_p^\star, \cdot, 1)$, řádu $r(a) = d$. Pak podgrupa $\langle a \rangle$ tvoří všechna řešení rovnice $x^k = 1$ v $(\mathbb{Z}_p, \cdot, 1)$.

1.5.5 Řešení $x^k = 1$ v $\mathbb{Z}_n$ pro n square free. Předpokládejme, že

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_m,$$

kde $p_1, p_2, \ldots, p_m$ jsou různá prvočísla. Pak z Čínské věty o zbytcích 1.3.1 máme vzájemně jednoznačný vztah

$$\mathbb{Z}_n \longleftrightarrow \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_m}.$$

Jestliže

$$\begin{aligned} x &\leftrightarrow (a_1, a_2, \ldots, a_m) \\ y &\leftrightarrow (b_1, b_2, \ldots, b_m) \end{aligned}$$

pak

$$x \cdot y \leftrightarrow (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_m \cdot b_m),$$

kde $a_1 \cdot b_1$ je součin v $\mathbb{Z}_{p_1}$, $a_2 \cdot b_2$ je součin v $\mathbb{Z}_{p_2}$, až $a_m \cdot b_m$ je součin v $\mathbb{Z}_{p_m}$.

Navíc,

$$1 \leftrightarrow (1, 1, \ldots, 1).$$

Proto invertibilnímu prvku x v $\mathbb{Z}_n$ odpovídá m-tice invertibilních prvků v jednotlivých $\mathbb{Z}_{p_i}$. Přesněji: jestliže x je invertibilní prvek v $\mathbb{Z}_n$, pak

$$x \leftrightarrow (a_1, a_2, \ldots, a_m),$$

kde a_1 je invertibilní prvek v $\mathbb{Z}_{p_1}$, a_2 je invertibilní prvek v $\mathbb{Z}_{p_2}$, až a_m je v invertibilní prvek v $\mathbb{Z}_{p_m}$.

A naopak, jestliže a_1 je invertibilní prvek v $\mathbb{Z}_{p_1}$, a_2 je invertibilní prvek v $\mathbb{Z}_{p_2}$, až a_m je v invertibilní prvek v $\mathbb{Z}_{p_m}$, pak prvek x, pro nějž

$$x \leftrightarrow (a_1, a_2, \ldots, a_m)$$

je invertibilní prvek v $\mathbb{Z}_n$.

Jedná se tedy též o vzájemně jednoznačný vztah

$$\mathbb{Z}_n^\star \longleftrightarrow \mathbb{Z}_{p_1}^\star \times \mathbb{Z}_{p_2}^\star \times \ldots \times \mathbb{Z}_{p_m}^\star.$$

Obdobně každé řešení rovnice $x^k = 1$ v $\mathbb{Z}_n$ jednoznačně odpovídá m-tici řešení rovnice $x^k = 1$ v $\mathbb{Z}_{p_1}$, $\mathbb{Z}_{p_2}$, až $\mathbb{Z}_{p_m}$.

Proto řešíme rovnici $x^k = 1$ nejprve ve všech $\mathbb{Z}_{p_i}$ pro $i = 1, 2, \ldots, m$. Jestliže existuje d_1 řešení $x^k = 1$ v $\mathbb{Z}_{p_1}$, d_2 řešení v $\mathbb{Z}_{p_2}$, až d_m řešení v $\mathbb{Z}_{p_m}$, pak počet řešení této rovnice v $\mathbb{Z}_n$ je $d_1 \cdot d_2 \cdot \ldots \cdot d_m$.

Všechna řešení v $\mathbb{Z}_n$ najdeme např. postupem popsaným v důkaze Čínské věty o zbytcích.

1.5.6 Obdobně můžeme řešit i jiné rovnice, např. $x^k = x$ v $\mathbb{Z}_n$, kde n je square free.

1.5.7 Millerův test prvočíselnosti. Uvedeme pravděpodobnostní algoritmus, který pro dané velké liché číslo zjišťuje, zda se jedná o prvočíslo nebo o číslo složené.

Vstup: Velké liché číslo n.

Výstup: Odpověď „prvočíslo“ nebo „složené číslo“.

1. Vypočteme $n-1 = 2^l m$, kde m je liché.
2. Vybereme náhodně číslo $a \in \{1, \dots, n-1\}$.
3. Spočítáme $a^m \pmod n$. Jestliže
$$a^m \equiv 1 \pmod n, \quad \text{stop, výstup „prvočíslo“.}$$
4. Opakovaným povyšováním na druhou počítáme $a^{2m} \pmod n$, $a^{2^2 m} \pmod n$, $\dots$, $a^{2^l m} \pmod n$. Jestliže
$$a^{2^l m} \not\equiv 1 \pmod n, \quad \text{stop, výstup „složené“.}$$
5. Označme k nejmenší číslo takové, že $a^{2^k m} \equiv 1 \pmod n$. Jestliže
$$a^{2^{k-1} m} \equiv -1 \pmod n \quad \text{stop, výstup „prvočíslo“.}$$
Jestliže
$$a^{2^{k-1} m} \not\equiv -1 \pmod n \quad \text{stop, výstup „složené“.}$$

1.5.8 Tvrzení. Jestliže Millerův test prvočíselnosti dá výstup „složené“, pak je n složené číslo. Jestliže Millerův test prvočíselnosti dá výstup „prvočíslo“, je n prvočíslo s pravděpodobností alespoň 50 procent.

1.5.9 Není těžké ukázat, že Millerův test prvočíselnosti nemůže pro prvočíslo dát odpověď složené.

Předpokládejme, že n je prvočíslo. Pak $\varphi(n) = n-1$ a každé a vybrané v kroku 2 je invertibilní. Tedy $a^{n-1} = 1$ v $\mathbb{Z}_n$ a algoritmus nemohl skončit v kroku 4.

V kroku 5 má číslo $b = a^{2^{k-1} m}$ tu vlastnost, že $b^2 = 1$. V grupě $(\mathbb{Z}_n^\star, \cdot, 1)$ existují pouze dva prvky, které povýšené na druhou dají jedničku — a to 1 a -1.

1.5.10 Ověřit druhou část tvrzení, tj. že v případě, že n je složené číslo pro alespoň polovinu čísel a z kroku 2 dostaneme správnou odpověď, není obtížné pro všechna složená čísla kromě tzv. pseudoprvočísel (někdy též nazývaných Carmichaelova čísla). Složené číslo je pseudoprvočíslo, jestliže pro každé $a \in \mathbb{Z}_n^\star$ platí $a^{n-1} = 1$.

Důvod: Špatnou odpověď „prvočíslo“ můžeme dostat pouze v případě, kdy pro náhodně zvolené číslo a v kroku 2 platí $a^{n-1} \equiv 1 \pmod n$ (a to ještě ne vždy). Všechna taková čísla a tvoří podgrupu K grupy $(\mathbb{Z}_n^\star, \cdot, 1)$. Jestliže $K \neq \mathbb{Z}_n^\star$, pak řád K dělí řád $\mathbb{Z}_n^\star$, tj.
$$|K| \leq \frac{1}{2} |\mathbb{Z}_n^\star| < \frac{1}{2} |\mathbb{Z}_n|.$$

Tedy těch čísel a v kroku 2, pro která dostaneme špatnou odpověď, je méně než polovina.

Pro Carmichaelova složená čísla tento argument není možné použít, protože pro každé $a \in \mathbb{Z}_n^\star$ platí $a^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$ a tedy $K = \mathbb{Z}_n^\star$.

Kapitola 2

Struktury nad zbytkovými třídami

Připomeňme, že pro všechna přirozená čísla n, $n > 1$, je $(\mathbb{Z}_n, +, 0)$ komutativní grupa; $(\mathbb{Z}_n, \cdot, 1)$ je komutativní monoid a $(\mathbb{Z}_n^\star, \cdot, 1)$ je jeho grupa invertibilních prvků. Jestliže p je prvočíslo, pak invertibilní je každý nenulový prvek $\mathbb{Z}_p$ (tj. $\mathbb{Z}_p^\star = \mathbb{Z}_p \setminus \{0\}$).

Navíc, mezi sčítáním a násobením platí distributivní zákon, tj.

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{pro všechny} \quad a, b, c \in \mathbb{Z}_p. \tag{2.1}$$

Uvědomme si, že se jedná o všechny vlastnosti, které známe z počítání s reálnými čísly.

Pro jednoduchost budeme místo dlouhého $(\mathbb{Z}_n, +, \cdot, 0, 1)$ psát pouze $\mathbb{Z}_n$ všude tam, kde bude jasné, že na množině zbytkových tříd $\mathbb{Z}_n$ pracujeme se dvěma binárními operacemi a to sčítáním a násobením.

2.1 Polynomy nad $\mathbb{Z}_p$

V dalším textu studujeme polynomy pouze nad $\mathbb{Z}_p$, kde p je prvočíslo. Poznamenejme, že polynomy můžeme vytvářet také nad $\mathbb{Z}_n$ pro n složené. Ovšem v tomto případě neplatí věta o dělení a tudíž nemůžeme použít Eukleidův algoritmus. K vlastnostem polynomů nad $\mathbb{Z}_n$ pro n složené se vrátíme později.

2.1.1 Polynomy nad $\mathbb{Z}_p$. *Polynomem* nad $\mathbb{Z}_p$ rozumíme každý výraz

$$a_0 + a_1\, x + a_2\, x^2 + \ldots + a_n\, x^n, \tag{2.2}$$

kde všechny koeficienty a_i jsou ze $\mathbb{Z}_p$. Symbol x nazýváme *proměnná*. Jsou-li všechny koeficienty a_i nulové, mluvíme o *nulovém* polynomu. Jestliže alespoň jeden z koeficientů a_i je nenulový, mluvíme o *nenulovém* polynomu. Množinu všech polynomů nad $\mathbb{Z}_p$ značíme $\mathbb{Z}_p[x]$.

2.1.2 Stupeň polynomu. *Stupeň* nulového polynomu je roven -1, *stupeň* nenulového polynomu je roven největšímu n takovému, že a_n je nenulové. Stupeň polynomu $f(x)$ značíme $\mathrm{st}(f)$.

2.1.3 Rovnost polynomů. Dva polynomy jsou si *rovny*, rovnají-li se všechny jejich odpovídající koeficienty, tj. mají-li stejný stupeň a koeficienty u stejných mocnin jsou stejné.

2.1.4 Funkce odpovídající polynomu. Každému polynomu $f(x)$ ze $\mathbb{Z}_p[x]$ můžeme přiřadit zobrazení z $\mathbb{Z}_p$ do sebe a to tímto způsobem: Je-li $f(x) = a_0 + + a_1\,x + a_2\,x^2 + \ldots + a_n\,x^n$, pak jemu odpovídající zobrazení ze $\mathbb{Z}_p$ do $\mathbb{Z}_p$ je definováno: pro každé $b \in \mathbb{Z}_p$

$$b \mapsto a_0 + a_1\,b + a_2\,b^2 + \ldots + a_n\,b^n.$$

(Všechny operace sčítání a násobení jsou operace v $\mathbb{Z}_p$.)

Např. polynomu $f(x) = 1 + x^2$ nad $\mathbb{Z}_2$ odpovídá zobrazení $\mathbb{Z}_2$ do $\mathbb{Z}_2$, kde $0 \mapsto 1$, $1 \mapsto 1 + 1^2 = 0$. Uvědomte si, že se jedná o stejné zobrazení jako to zobrazení, které odpovídá polynomu $g(x) = 1 + x$. Není tedy pravda, že různým polynomům odpovídají vždy různá zobrazení. (Tento fakt je způsoben tím, že pro každý prvek $a \in \mathbb{Z}_p$ platí $a^p = a$.)

2.1.5 Poznámka. Poznamenejme, že polynomy nad reálnými nebo komplexními čísly se často definují jako funkce (reálné nebo komplexní) dané výrazem (2.2) pro reálné, nebo komplexní koeficienty a_i. To je možné proto, že v případě reálných polynomů platí, že dva polynomy jsou si rovny jakožto funkce právě tehdy, když jsou si rovny jako formální výrazy.

2.1.6 Sčítání a odčítání polynomů. Máme dány polynomy nad $\mathbb{Z}_p$: $f(x) = = a_0 + a_1\,x + a_2\,x^2 + \ldots + a_n\,x^n$ a $g(x) = b_0 + b_1\,x + b_2\,x^2 + \ldots + b_m\,x^m$ stupně n a m, $n \geq m$, pak jejich *součtem* je polynom

$$(a_0 + b_0) + (a_1 + b_1)\,x + \ldots + (a_m + b_m)\,x^m + a_{m+1}\,x^{m+1} + \ldots + a_n\,x^n,$$

rozdílem $f(x)$ mínus $g(x)$ je polynom

$$(a_0 - b_0) + (a_1 - b_1)\,x + \ldots + (a_m - b_m)\,x^m + a_{m+1}\,x^{m+1} + \ldots + a_n\,x^n.$$

Pro stupeň součtu nebo rozdílu dvou polynomů platí

$$\mathrm{st}(f \pm g) \leq \max(\mathrm{st}(f), \mathrm{st}(g)).$$

2.1.7 Násobení polynomů. *Součinem* polynomů $f(x)$ a $g(x)$ je polynom $h(x) = c_0 + c_1\,x + c_2\,x^2 + \ldots c_{n+m}\,x^{n+m}$, kde koeficienty $c_0, c_1, \ldots, c_{n+m}$ dostaneme tak, že polynomy „vynásobíme jako mnohočleny“, tedy např. $c_0 = = a_0\,b_0$, $c_1 = a_0\,b_1 + a_1\,b_0$, $\ldots$, $c_{n+m} = a_n\,b_m$.

Platí $\mathrm{st}(f \cdot g) = \mathrm{st}(f) + \mathrm{st}(g)$ kdykoli jsou oba polynomy nenulové, v opačném případě je $\mathrm{st}(f \cdot g) = -1$.

2.1.8 Věta o dělení polynomů. Mějme dva polynomy $f(x)$ a $g(x)$ ze $\mathbb{Z}_p[x]$, kde $g(x)$ je nenulový. Pak existují polynomy $r(x)$ a $z(x)$ v $\mathbb{Z}_p[x]$ takové, že

$$f(x) = r(x)\,g(x) + z(x) \quad \text{a} \quad \mathrm{st}(z) < \mathrm{st}(g).$$

Tyto polynomy jsou určeny jednoznačně.

Polynomu $r(x)$ z věty o dělení se říká *částečný podíl*, polynom $z(x)$ je *zbytek při dělení* polynomu $f(x)$ polynomem $g(x)$.

2.1.9 Věta o dělení polynomů. Mějme dva polynomy $f(x)$ a $g(x)$ ze $\mathbb{Z}_p[x]$, kde $g(x)$ je nenulový. Pak existují polynomy $r(x)$ a $z(x)$ v $\mathbb{Z}_p[x]$ takové, že

$$f(x) = r(x)\,g(x) + z(x) \quad \text{a} \quad \mathrm{st}(z) < \mathrm{st}(g).$$

Tyto polynomy jsou určeny jednoznačně.

Polynomu $r(x)$ z věty o dělení se říká *částečný podíl*, polynom $z(x)$ je *zbytek při dělení* polynomu $f(x)$ polynomem $g(x)$.

2.1.10 Algoritmus dělení polynomů. Polynomy $r(x)$ a $z(x)$ ze znění věty najdeme stejným způsobem jako v při dělení reálných polynomů, pouze místo „dělení prvkem“ používáme „násobení inverzním prvkem“. Ukažme si podrobněji jeden krok dělení:

Máme $f(x) = a_0 + a_1\,x + \ldots a_n\,x^n$, $g(x) = b_0 + b_1\,x + \ldots b_m\,x^m$, $\mathrm{st}(f) = n$, $\mathrm{st}(g) = m$. Jestliže $n < m$, pak platí

$$f(x) = 0\,g(x) + f(x) \quad \text{a} \quad \mathrm{st}(f) < \mathrm{st}(g).$$

Tedy polynomy $r(x) = 0$ a $z(x) = f(x)$ jsou hledané polynomy.

Předpokládejme, že $n \geq m$. Vezmeme členy polynomů $f(x)$ a $g(x)$ s největší mocninou, tj. $a_n\,x^n$ a $b_m\,x^m$. Vydělíme $a_n\,x^n$ členem $b_m\,x^m$; podíl je roven $a_n\,b_m^{-1}\,x^{n-m}$. Polynom $a_n\,b_m^{-1}\,x^{n-m} \cdot g(x)$ je polynom stupně n a má koeficient u nejvyšší mocniny a_n. Položme

$$h(x) = f(x) - a_n\,b_m^{-1}\,x^{n-m} \cdot g(x).$$

Polynom $h(x)$ má stupeň ostře menší než n.

Nyní buď $\mathrm{st}(h) < \mathrm{st}(g)$ a jsme hotovi; částečný podíl je $r(x) = a_n\,b_m^{-1}\,x^{n-m}$, zbytek při dělení je $z(x) = h(x)$.

Nebo $\mathrm{st}(h) \geq \mathrm{st}(g)$ a částečný podíl při dělení polynomu $f(x)$ polynomem $g(x)$ je roven součtu $a_n\,b_m^{-1}\,x^{n-m}$ a částečného podílu při dělení polynomu $h(x)$ polynomem $g(x)$. Zbytek při dělení $f(x)$ polynomem $g(x)$ je stejný jako zbytek při dělení $h(x)$ polynomem $g(x)$.

2.1.11 Dělitelnost polynomů. Jestliže zbytek při dělení polynomu $f(x)$ polynomem $g(x)$ je nulový polynom, říkáme, že polynom $g(x)$ *dělí* polynom $f(x)$, nebo že polynom $f(x)$ *je dělitelný* polynomem $g(x)$, nebo také, že polynom $g(x)$ *je dělitelem* polynomu $f(x)$.

2.1.12 Kořen polynomu. Prvek $a \in \mathbb{Z}_p$ se nazývá *kořen* polynomu $f(x) \in \in \mathbb{Z}_p[x]$, jestliže platí $f(a) = 0$.

2.1.13 Tvrzení. Prvek $a \in \mathbb{Z}_p$ je kořenem polynomu $f(x) \in \mathbb{Z}_p[x]$ právě tehdy, když polynom $(x - a)$ dělí polynom $f(x)$.

2.1.14 Ireducibilní polynomy. Polynom $f(x)$ ze $\mathbb{Z}_p[x]$ se nazývá *ireducibilní* (nad $\mathbb{Z}_p$), jestliže se polynom $f(x)$ nedá napsat jako součin dvou polynomů menšího stupně než je $f(x)$.

Jinými slovy, jestliže z rovnosti $f(x) = g(x) \cdot h(x)$ plyne buď $\mathrm{st}(g) = \mathrm{st}(f)$ (a $h(x)$ je polynom stupně 0, tj. konstanta) nebo $\mathrm{st}(h) = \mathrm{st}(f)$ (a $g(x)$ je polynom stupně 0, tj. konstanta).

2.1.15 Příklady.

1. Polynom $f(x) = x^2 + 1$ je ireducibilní nad $\mathbb{Z}_3$, protože se nedá napsat jako součin dvou lineárních polynomů; to by totiž musel mít kořen.
2. Polynom $f(x) = x^2 + 1$ není ireducibilní nad $\mathbb{Z}_2$; stačí si uvědomit, že v $\mathbb{Z}_2$ platí $(x^2 + 1) = (x + 1)(x + 1)$.
3. Polynom $g(x) = x^2 + x + 1$ je ireducibilní nad $\mathbb{Z}_2$, nemá totiž kořen.

2.1.16 Tvrzení. Polynom stupně 2 nebo 3 je ireducibilní právě tehdy, když nemá kořen.

Pro polynomy stupně většího než 3 už takové tvrzení neplatí; součin dvou ireducibilních polynomů stupně 2 je polynom stupně 4, který není ireducibilní a přesto nemá kořen. Samozřejmě, polynom, který kořen má, nikdy není ireducibilní (viz 2.1.13).

2.1.17 Tvrzení. Nad $\mathbb{Z}_p$ existují ireducibilní polynomy libovolného stupně.

2.1.18 Největší společný dělitel dvou polynomů. Mějme dva polynomy $f(x)$ a $g(x)$ ze $\mathbb{Z}_p[x]$. Polynom $h(x)$ ze $\mathbb{Z}_p[x]$ se nazývá *největší společný dělitel* polynomů $f(x)$ a $g(x)$, jestliže splňuje

1. $h(x)$ dělí oba polynomy $f(x)$ a $g(x)$;
2. kdykoli nějaký polynom $k(x)$ dělí oba polynomy $f(x)$ a $g(x)$, pak $k(x)$ dělí i $h(x)$.

Poznamenejme, že jsme také mohli definovat největší společný dělitel dvou polynomů jako společný dělitel, který má největší stupeň mezi všemi společnými děliteli.

2.1.19 Poznámka. Uvědomme si, že obecně není pouze jediný největší společný dělitel dvou polynomů. Jestliže je totiž polynom $h(x)$ největší společný dělitel polynomů $f(x)$ a $g(x)$, pak také polynom $b \cdot h(x)$, kde b je nenulový prvek $\mathbb{Z}_p$, je největší společný dělitel polynomů $f(x)$ a $g(x)$. Mezi všemi největšími společnými děliteli polynomů f a g je přesně jeden, který má u nejvyšší mocniny koeficient roven 1. (Polynomům, které mají koeficient u nejvyšší mocniny roven 1 se říká *monické*.) Někdy se za největší společný dělitel dvou polynomů považuje právě monický největší společný dělitel. V tomto případě je pak určen jednoznačně.

2.1.20 Nesoudělné polynomy. Dva polynomy nazýváme *nesoudělné*, jestliže $h(x) = 1$ je jejich největší společný dělitel.

2.1.21 Eukleidův algoritmus. Vstup: dva polynomy $f(x)$ a $g(x)$ ze $\mathbb{Z}_p[x]$. Výstup: polynom $h(x)$, který je jeden z největších společných dělitelů polynomů $f(x)$ a $g(x)$.

1. If $\mathrm{st}(f) \geq \mathrm{st}(g)$ then $t(x) := f(x), r(x) := g(x)$;
   else $t(x) := g(x)$, $r(x) := f(x)$

2. Vydělíme polynom $t(x)$ polynomem $r(x)$, tj. dostaneme

$$t(x) = q(x)\, r(x) + z(x),\ \mathrm{st}(z) < \mathrm{st}(r).$$

3. If $z(x) = 0$, položíme $h(x) := r(x)$, stop;
   else $t(x) := r(x)$, $r(x) := z(x)$, go to 2.

2.1.22 Bezoutova věta. Jsou-li $f(x)$ a $g(x)$ dva polynomy ze $\mathbb{Z}_p[x]$ a $h(x)$ je některý z jejich největších společných dělitelů, pak existují polynomy $a(x)$ a $b(x)$ ze $\mathbb{Z}_p[x]$ takové, že

$$h(x) = a(x)\, f(x) + b(x)\, g(x).$$

2.1.23 Poznámka. Jak správnost Eukleidova algoritmu, tak platnost Bezoutovy věty se dokazuje formálně úplně stejně jako obdobná tvrzení pro celá čísla.

2.1.24 Řešení polynomiálních rovnic. Jsou dány polynomy $a(x)$, $b(x)$ a $c(x)$ nad $\mathbb{Z}_p$, kde p je prvočíslo. Pak rovnice

$$y(x)\, a(x) + z(x)\, b(x) = c(x) \tag{2.3}$$

má řešení, tj. existují polynomy $y(x)$ a $z(x)$ které splňují rovnici (2.3), právě tehdy, když největší společný dělitel $d(x)$ polynomů $a(x)$ a $b(x)$ dělí polynom $c(x)$.

2.1.25 Poznámka. Jedno řešení rovnice (2.3) najdeme rozšířeným Eukleidovým algoritmem. Obecné řešení rovnice (2.3) je pak součtem jednoho řešení (nehomogenní) rovnice (2.3) a obecného řešení homogenní rovnice

$$a(x)\, y(x) + b(x)\, z(x) = 0. \tag{2.4}$$

Označme $a_0(x)$ ten polynom, pro který $a(x) = d(x)\, a_0(x)$ a $b_0(x)$ ten polynom, pro který $b(x) = d(x)\, b_0(x)$. (Jinými slovy, $a_0(x)$ je polynom, který dostaneme vydělením polynomu $a(x)$ největším společným dělitelem $d(x)$, obdobně $b_0(x)$.) Řešení homogenní rovnice (2.4) je tvaru:

$$y_0(x) = t(x)\, a_0(x),\ \text{a}\ z_0(x) = -t(x)\, b_0(x),$$

kde $t(x)$ je libovolný polynom z $\mathbb{Z}_p[x]$.

2.2 Konečné okruhy a tělesa

2.2.1 Definice okruhu. Trojice $(A, +, \cdot)$ se nazývá *okruh*, jestliže

- $(A, +)$ je komutativní grupa s neutrálním prvkem 0;
- $(A, \cdot)$ je pologrupa;
- a platí distributivní zákony, tj. pro všechna $a, b, c \in A$ platí

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{a také} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Je-li navíc pologrupa $(A, \cdot)$ komutativní, říkáme, že se jedná o *komutativní okruh*; má-li pologrupa $(A, \cdot)$ jednotkový prvek, mluvíme o *okruhu s jednotkou*.

2.2.2 Příklady.

1. $(\mathbb{Z}, +, \cdot)$ je komutativní okruh s jednotkou.
2. $(M_n(\mathbb{Z}), +, \cdot)$, kde M_n je množina všech čtvercových matic řádu n, je (nekomutativní) okruh s jednotkou, v tomto případě je jednotkový prvek jednotková matice řádu n.
3. $(M_n(\mathbb{Z}_p), +, \cdot)$, kde M_n je množina všech čtvercových matic řádu n s prvky v $\mathbb{Z}_p$, je (nekomutativní) okruh s jednotkou, v tomto případě je jednotkový prvek jednotková matice řádu n.
4. $(\mathbb{Z}_n, +, \cdot)$, $n > 1$, je komutativní okruh s jednotkou 1.
5. $(\mathbb{Z}_p[x], +, \cdot)$ je komutativní okruh s jednotkou, v tomto případě je jednotkovým prvkem polynom $q(x) = 1$ stupně 0.

2.2.3 Těleso. Těleso je okruh s jednotkou 1, kde každý nenulový prvek je invertibilni v monoidu $(A, \cdot, 1)$ a 1 není současně neutrálním prvkem 0 grupy $(A, +, 0)$.

2.2.4 Poznámka. Požadavek, aby $0 \neq 1$ v každém tělese znamená, že každé těleso musí mít alespoň dva prvky, a to 0 a 1. Nejmenší těleso se opravdu skládá pouze ze dvou prvků; jedná se o těleso $(\mathbb{Z}_2, +, \cdot)$.

2.2.5 Příklady.

1. $(\mathbb{Z}_p, +, \cdot)$, kde p je libovolné prvočíslo, je těleso.
2. $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ jsou tělesa, ovšem nekonečná.
3. $(\mathbb{Z}, +, \cdot)$ **není** těleso, invertibilní prvky tohoto okruhu jsou pouze 1 a -1.
4. $(\mathbb{Z}_n, +, \cdot)$, pro n složené, **není** těleso. Prvek $m \neq 1$, který dělí n, není invertibilní.
5. $(M_n(\mathbb{Z}_p), +, \cdot)$, kde M_n je množina všech čtvercových matic řádu n s prvky v $\mathbb{Z}_p$, **není** těleso. Matice A je invertibilní právě tehdy, když její determinant je invertibilní prvek v $\mathbb{Z}_p$.
6. $(\mathbb{Z}_p[x], +, \cdot)$ **není** těleso, invertibilní prvky tohoto okruhu jsou pouze polynomy stupně 0.

2.3 Faktorové okruhy polynomů

V dalším textu stále předpokládáme, že p je dané prvočíslo.

2.3.1 Kongruence modulo polynom. Je dán polynom $q(x) \in \mathbb{Z}_p[x]$. Na množině $\mathbb{Z}_p[x]$ definujeme relaci *modulo* $q(x)$ takto:

$$a(x) \equiv b(x) \,(\mathrm{mod}\, q(x)) \text{ iff polynom } (a(x) - b(x)) \text{ je dělitelný } q(x).$$

Poznamenejme, že se jedná o analogii ekvivalence modulo n na množině celých čísel $\mathbb{Z}$.

2.3.2 Tvrzení. Pro každé dva polynomy $a(x)$, $b(x)$ ze $\mathbb{Z}_p[x]$ platí:

$$a(x) \equiv b(x) \,(\mathrm{mod}\, q(x))$$

právě tehdy, když platí jedna z následujících podmínek:

1. $a(x) = b(x) + t(x)\, q(x)$ pro vhodný polynom $t(x) \in \mathbb{Z}_p[x]$;
2. $a(x)$ i $b(x)$ mají stejný zbytek při dělení polynomem $q(x)$.

2.3.3 Tvrzení. Relace modulo $q(x)$ je relace ekvivalence na množině $\mathbb{Z}_p[x]$, tj. tato relace je reflexivní, symetrická a tranzitivní.

Navíc, jestliže $a(x) \equiv b(x) \,(\mathrm{mod}\, q(x))$ a $c(x) \equiv d(x) \,(\mathrm{mod}\, q(x))$, pak také

$$(a(x) + c(x)) \equiv (b(x) + d(x) \,(\mathrm{mod}\, q(x))$$

$$a(x) \cdot c(x) \equiv b(x) \cdot d(x) \,(\mathrm{mod}\, q(x)).$$

2.3.4 Faktovový okruh. Označme k stupeň polynomu $q(x)$. Předchozí tvrzení umožňuje definovat množinu tříd modulo $q(x)$, budeme ji označovat $\mathbb{Z}_p[x]/q(x)$. Protože každá třída obsahuje přesně jeden polynom stupně menšího než je k, lze psát

$$\mathbb{Z}_p[x]/q(x) = \{[a(x)] \,|\, \mathrm{st}(a) < \mathrm{st}(q)\}.$$

Navíc, na množině $\mathbb{Z}_p[x]/q(x)$ definujeme dvě operace a to sčítání a násobení takto:

$$[a(x)] + [c(x)] = [a(x) + c(x)]$$

$$[a(x)] \cdot [c(x)] = [a(x) \cdot c(x)].$$

Díky tvrzení 2.3.3 jsou definice korektní.

2.3.5 Tvrzení. $(\mathbb{Z}_p[x]/q(x), +, \cdot)$ je komutativní okruh s jednotkou, kde jednotkový prvek je třída $[e(x)]$, kde platí $e(x) = 1$ je polynom stupně 0. Tento okruh má p^k prvků, (opět $k = \mathrm{st}(q)$).

2.3.6 Poznámka. Okruh z předchozího tvrzení nazýváme *faktorový okruh modulo* $q(x)$. Protože každá třída z faktorového okruhu je reprezentována právě jedním polynomem stupně menšího než k, můžeme také položit

$$\mathbb{Z}_p[x]/q(x) = \{a(x) \,|\, \mathrm{st}(a) < \mathrm{st}(q)\}.$$

Operace sčítání je pak obyčejné sčítání polynomů, protože součtem dvou polynomů stupně menšího než k dostaneme opět polynom stupně menšího než k. Násobení provádíme trochu složitěji, nejprve vynásobíme polynomy v $\mathbb{Z}_p[x]$ a jako jejich součin ve faktorovém okruhu vezmeme zbytek tohoto plynomu při dělení polynomem $q(x)$.

2.3.7 Úmluva. Protože budeme potřebovat odlišit polynomy nad $\mathbb{Z}_p$ od prvků faktorového okruhu, udělejme ještě jednu úmluvu. Proměnnou ve faktorovém okruhu budeme značit z a nikoli x. Píšeme tedy

$$\mathbb{Z}_p[x]/q(x) = \{a(z) \,|\, \mathrm{st}(a) < \mathrm{st}(q)\}.$$

2.3.8 Věta. Faktorový okruh $\mathbb{Z}_p[x]/q(x)$ je tělesem právě tehdy, když polynom $q(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$.

2.3.9 Příklady.

1. $\mathbb{Z}_3[x]/(x^2+1)$ je těleso, protože polynom x^2+1 je ireducibilní polynom nad $\mathbb{Z}_3$,
2. $\mathbb{Z}_2[x]/(x^2+1)$ **není** těleso, protože polynom x^2+1 není ireducibilní polynom nad $\mathbb{Z}_2$,
3. $\mathbb{Z}_2[x]/(x^2+x+1)$ je těleso, protože polynom x^2+x+1 je ireducibilní polynom nad $\mathbb{Z}_2$.

2.3.10 Tvrzení. Je dán ireducibilní polynom $q(x) \in \mathbb{Z}_p[x]$. Pak $\mathbb{Z}_p[x]/q(x)$ je těleso o p^k prvcích, kde $k = \mathrm{st}(q)$.

2.3.11 Jiný pohled na násobení v $\mathbb{Z}_p[x]/q(x)$. Označme $q(x) = a_0 + a_1x + \\ + a_2x^2 + \ldots + a_kx^k$. Pak v tělese $\mathbb{Z}_p[x]/q(x)$ platí $a_0 + a_1z + a_2z^2 + \ldots + a_kz^k = 0$, protože vydělíme-li polynom $q(x)$ sebou samým, dostaneme zbytek 0. Proto v $\mathbb{Z}_p[x]/q(x)$ platí

$$a_kz^k = -a_{k-1}z^{k-1} - \ldots - a_1z - a_0,$$

a odtud

$$z^k = a_k^{-1}(-a_{k-1}z^{k-1} - \ldots - a_1z - a_0). \tag{2.5}$$

Ze vztahu (2.5) dále dostáváme

$$\begin{aligned} z^{k+1} &= z \cdot [a_k^{-1}(-a_{k-1}z^{k-1} - \ldots - a_1z - a_0)] \\ z^{k+2} &= z^2 \cdot [a_k^{-1}(-a_{k-1}z^{k-1} - \ldots - a_1z - a_0)] \\ &\vdots \\ z^{2k-2} &= z^{k-2} \cdot [a_k^{-1}(-a_{k-1}z^{k-1} - \ldots - a_1z - a_0)]. \end{aligned}$$

Vyšší mocniny při součinu dvou prvků v daném tělese nevzniknou. Máme tedy $k-1$ pravidel pro násobení.

2.3.12 Poznámka. Výše uvedený postup je podobný tomu, jak jste vytvářeli z reálných čísel čísla komplexní.

Uvažujme polynom $q(x) = x^2 + 1$. Tento polynom je ireducibilní jako polynom nad reálnými čísly. Utvořme okruh všech polynomů s reálnými koeficienty $\mathbb{R}[x]$. Nyní $\mathbb{R}[x]/(x^2+1)$ se skládá ze všech $a + bz$, a a b jsou libovolná reálná čísla. Označme $z = i$, pak $i^2+1 = 0$ a $i^2 = -1$. Tedy i je dobře známá komplexní jednotka.

Proto o okruzích $\mathbb{Z}_p[x]/(x^2+1)$ mluvíme též jako o komplexních číslech nad $\mathbb{Z}_p$. Je třeba si uvědomit, že tato komplexní čísla nad $\mathbb{Z}_p$ netvoří vždy těleso; např. nad $\mathbb{Z}_2$ nebo $\mathbb{Z}_5$ není polynom $x^2 + 1$ ireducibilní a proto $\mathbb{Z}_2[x]/(x^2+1)$ a $\mathbb{Z}_5[x]/(x^2+1)$ nejsou tělesa.

2.4 Řešení polynomiálních rovnic

2.4.1 Obdobně jako jsme v $\mathbb{Z}_n$ řešili rovnice tvaru $a\,x = b$, můžeme řešit i polynomiální rovnice

$$a(x)\,q(x) = b(x) \quad \text{v okruhu } \mathbb{Z}_p[x]/m(x) \tag{2.6}$$

(pro p prvočíslo a $m(x)$ pevně daný polynom nad $\mathbb{Z}_p$).

Víme, že $a(x)\,q(x) = b(x)$ v $\mathbb{Z}_p[x]/m(x)$ platí právě tehdy, když

$$a(x)\,q(x) \;\equiv\; b(x)\,(\mathrm{mod}\, m(x)).$$

A to nastává právě tehdy, když

$$a(x)\,q(x) + m(x)\,h(x) = b(x) \tag{2.7}$$

pro vhodný polynom $h(x) \in \mathbb{Z}_p[x]$.

2.4.2 Tvrzení. Rovnice 2.6 (a také 2.7) má řešení právě tehdy, když polynom $b(x)$ je dělitelný největším společným dělitelem polynomů $a(x)$ a $m(x)$.

2.4.3 Rovnice 2.7 je lineární rovnice pro neznámé polynomy, proto její řešení najdeme jako součet jednoho řešení nehomogenní rovnice (tj. rovnice 2.7) a obecného řešení homogenní rovnice, tj. rovnice

$$a(x)\,q(x) + m(x)\,h(x) = 0. \tag{2.8}$$

2.4.4 Jedno řešení nehomogenní rovnice. K tomu, abychom našli jedno řešení nehomogenní rovnice 2.7, můžeme postupovat dvěma způsoby.

1. Použijeme rozšířený Eukleidův algoritmus. Jedná se o analogický postup jako při řešení diofantických rovnic.
2. Využijeme přepisovací pravidla, která platí v okruhu $\mathbb{Z}_p[x]/m(x)$.

2.4.5 Obecné řešení homogenní rovnice. Postupujeme analogicky jako v případě diofantických rovnic: Polynomy $a(x)$ a $m(x)$ vydělíme některým z jejich největších společných dělitelů (nejčastěji to bývá ten monický největší společný dělitel). Tím dostaneme rovnici tvaru

$$a'(x)\,q(x) + m'(x)\,h(x) = 0,$$

kde $a'(x)$ a $m'(x)$ jsou nesoudělné polynomy. Tato rovnice má obecné řešení tvaru

$$q(x) = m'(x)\,k(x),\; h(x) = -a'(x)\,k(x),\;\; k(x) \in \mathbb{Z}_p[x].$$

2.5 Kódování

Připomeňme nejprve několik pojmů z kódování. Množinu všech slov délky n nad $\mathbb{Z}_p$ značíme $\mathbb{Z}_p^n$, jednotlivá slova označujeme $\overline{u}$. Tedy

$$\mathbb{Z}_p^n = \{\overline{u} = (u_1 u_2 \dots u_n) \,|\, u_i \in \mathbb{Z}_p\}.$$

O prvku $u_i \in \mathbb{Z}_p$ mluvíme jako o prvku na i-tém místě (i-té pozici) slova $\overline{u}$.

Na množině $\mathbb{Z}_p^n$ máme dány operace sčítání a násobení číslem $b \in \mathbb{Z}_p$. Jedná se o lineární prostor dimenze n nad $\mathbb{Z}_p$.

2.5.1 p-znakový blokový kód délky n. Každá podmnožina $K \subseteq \mathbb{Z}_p^n$ se nazývá *p-znakový blokový kód délky n*. Prvky množiny K nazýváme *kódová slova*.

2.5.2 Hammingova vzdálenost. Jsou dána dvě slova $\overline{u} = (u_1 u_2 \dots u_n)$ a $\overline{v} = (v_1 v_2 \dots v_n)$ ze $\mathbb{Z}_p^n$. Jejich *Hammingova vzdálenost* $d_H(\overline{u}, \overline{v})$ je rovna počtu míst, ve kterých se obě slova liší; tj. $d_H(\overline{u}, \overline{v}) = |\{i \mid u_i \neq v_i\}|$.

Hammingova vzdálenost kódu K je rovna

$$d_H(K) = \min\{d_H(\overline{u}, \overline{v}) \mid \overline{u}, \overline{v} \in K, \overline{u} \neq \overline{v}\}.$$

Hammingova váha $\|\overline{u}\|_H$ slova $\overline{u}$ je rovna počtu nenulových míst slova $\overline{u}$; tj. $\|\overline{u}\|_H = |\{i \mid u_i \neq 0\}|$. Též jsme mohli definovat Hammingovu váhu slova $\overline{u}$ jako Hammingovu vzdálenost slov $\overline{u}$ a $\overline{o}$, kde $\overline{o}$ je nulové slovo, tj. $\overline{o} = (00 \dots 0)$.

2.5.3 Objevování chyb. Řekneme, že kód K *objevuje t* chyb, jestliže pro každé kódové slovo $\overline{u} \in K$ a každé chybové slovo $\overline{e}$ váhy menší nebo rovno t slovo $\overline{u} + \overline{e}$ není kódové.

2.5.4 Opravování chyb. Řekneme, že kód K *opravuje t* chyb, jestliže pro každé kódové slovo $\overline{u} \in K$ a každé chybové slovo $\overline{e}$ váhy menší nebo rovno t platí: Slovo $\overline{u}$ je kódové slovo s nejmenší Hammingovou vzdáleností od slova $\overline{u} + \overline{e}$ mezi všemi kódovými slovy.

2.5.5 Tvrzení. Jestliže kód K má Hammingovu vzdálenost d, pak K objevuje $t_1 = d - 1$ chyb a opravuje $t_2 < \frac{d}{2}$ chyb.

2.6 Lineární kódy

Ukazuje se výhodné, má-li kód vnitřní algebraickou strukturu.

2.6.1 Lineární kód. Kód K, který je současně lineární podprostor prostoru $\mathbb{Z}_p^n$ se nazývá *lineární p-znakový kód délky n*.

2.6.2 Báze lineárního kódu. Je dán lineární p-znakový kód K délky n. Protože se jedná o lineární podprostor, má K bázi; tj. podmnožinu kódových slov, která je lineárně nezávislá a přitom generuje celý kód K.

2.6.3 (n, k)-kód. Má-li některá báze kódu K počet prvků roven k, tj. je rovna $\{\overline{g}_1, \overline{g}_2, \dots, \overline{g}_k\}$, říkáme, že kód K má *k informačních znaků* a *$n - k$ kontrolních znaků*. Kód K pak nazýváme *(n, k)-kód*.

Informační znaky $(u_1 \dots u_k)$ pak kódujeme např. podle předpisu

$$(u_1 \dots u_k) \longmapsto u_1 \overline{g}_1 + \dots + u_k \overline{g}_k.$$

2.6.4 Generující matice. Je dána báze $\{\overline{g}_1, \overline{g}_2, \ldots, \overline{g}_k\}$ lineárního kódu K. Matice, jejíž řádky jsou tvořeny slovy $\overline{g}_1, \overline{g}_2, \ldots, \overline{g}_k$, se nazývá *generující matice* kódu K a označujeme ji $\mathbf{G}$, tj.

$$\mathbf{G} = \begin{pmatrix} \overline{g}_1 \\ \overline{g}_2 \\ \vdots \\ \overline{g}_k \end{pmatrix}.$$

Vlastní kódování se pak provádí:

$$(u_1 \ldots u_k) \longmapsto (u_1 \ldots u_k) \cdot \mathbf{G}.$$

Uvědomme si, že pro stejný kód K může existovat více způsobů, jak jednotlivá informační slova zakódovat — stačí zvolit jinou generující matici kódu K.

2.6.5 Systematické kódování. Kódování se nazývá *systematické*, jestliže při kódování

$$(u_1\, u_2\, \ldots\, u_k) \to (v_1\, v_2\, \ldots\, v_n)$$

platí, že prvních k míst kódového slova jsou právě informační znaky; tj. $v_1 = u_1$, $v_2 = u_2$, …, $v_k = u_k$.

Používáme-li pro kódování generující matici $\mathbf{G}$, musí mít tvar

$$\mathbf{G} = \begin{pmatrix} \mathbf{E_k} & \mathbf{B} \end{pmatrix},$$

kde $\mathbf{E_k}$ je jednotková matice řádu k.

Při systematickém kódování je Je velmi jednoduché získat z kódového slova zpět informační znaky – stačí vzít prvních k míst kódového slova $\overline{v}$.

2.6.6 Tvrzení. Ke každému lineárnímu kódu K existuje systematický lineární kód K', který se od K liší pouze v pořadí znaků v kódových slovech.

2.6.7 Kontrolní matice. Každý lineární podprostor K prostoru $\mathbb{Z}_p^n$ je prostorem řešení některé homogenní soustavy rovnic nad $\mathbb{Z}_p$. Matici $\mathbf{H}$ takového soustavy nazýváme *kontrolní maticí* kódu K a značíme $\mathbf{H}$.

Pro kontrolní matici $\mathbf{H}$ kódu K tedy platí

$$\overline{u} \in K \quad \text{právě tehdy, když} \quad \mathbf{H} \cdot \overline{u}^T = \overline{o}^T.$$

2.6.8 Tvrzení. Je-li generující matice $\mathbf{G}$ tvaru

$$\mathbf{G} = \begin{pmatrix} \mathbf{E_k} & \mathbf{B} \end{pmatrix},$$

pak kontrolní matice $\mathbf{H}$ je rovna

$$\mathbf{H} = \begin{pmatrix} -\mathbf{B}^T & \mathbf{E_{n-k}} \end{pmatrix},$$

kde $\mathbf{E_l}$ je jednotková matice řádu l.

2.6.9 Tvrzení. Mějme lineární kód K s kontrolní maticí $\mathbf{H}$. Jestliže každých t sloupců matice $\mathbf{H}$ je lineárně nezávislých, pak K objevuje t chyb a opravuje $[\frac{t}{2}]$ chyb.

Jestliže existuje t lineárně závislých sloupců matice $\mathbf{H}$, pak K objevuje méně než t chyb.

2.6.10 Dekódování. Je dán lineární kód s kontrolní maticí $\mathbf{H}$. Předpokládejme, že kanál, kterým se kódová slova vysílají, má tu vlastnost, že dvě chyby jsou téměř vyloučené.

Přijali jsme slovo $\overline{v}$. Je-li $\overline{u}$ vyslané slovo, pak $\overline{v} = \overline{u} + \overline{e}$, kde $\overline{e}$ je tzv. *chybové* slovo. Za našich předpokladů má chybové slovo nejvýše jedno nenulové místo — jestliže nedošlo k chybě, je $\overline{e}$ nulové slovo, jestliže došlo k jedné chybě na i-tém místě, pak $\overline{e}$ má jedno nenulové místo a to i-té. Přitom platí:

$$\overline{s}^T = \mathbf{H} \cdot \overline{v}^T = \mathbf{H} \cdot \overline{u}^T + \mathbf{H} \cdot \overline{e}^T = \mathbf{H} \cdot \overline{e}^T.$$

Slovo $\overline{s}$ se nazývá *syndrom* slova $\overline{v}$.

Je-li syndrom $\overline{s}$ nulové slovo, je slovo $\overline{v}$ kódové a za našeho předpokladu je $\overline{v}$ vyslané slovo $\overline{u}$.

Je-li syndrom $\overline{s}$ nenulové slovo, pak došlo při přenosu k chybě. Předpokládejme, že chybové slovo má nenulový znak na i-tém místě, (tj. v místě, kde k chybě došlo). Označme hodnotu tohoto znaku e_i, pak

$$\mathbf{H} \cdot \overline{e}^T = e_i \cdot \overline{h}_i,$$

kde $\overline{h}_i$ je i-tý sloupec matice $\mathbf{H}$.

Je-li syndrom $\overline{s}$ roven a-násobku i-tého sloupce matice $\mathbf{H}$ a není-li roven násobku žádného jiného sloupce matice $\mathbf{H}$, dekódujeme slovo $\overline{v}$ jako kódové slovo, které dostaneme tak, že od slova $\overline{v}$ odečteme chybové slovo $\overline{e}$ (které má $e_i = a$ a $e_j = 0$ pro $j \neq i$). Tedy

$$\overline{w} = \overline{v} - \overline{e},$$

je dekódované slovo. Jestliže došlo k jediné chybě, je $\overline{w} = \overline{u}$.

Jestliže syndrom $\overline{s}$ je násobkem více než jednoho sloupce matice $\mathbf{H}$, víme, že při přenosu došlo k chybě, ale ani za našeho předpokladu nejsme schopni rozhodnout, které slovo bylo vysláno (tj. chybu opravit).

2.7 Cyklické kódy

2.7.1 Lieární blokový kód K nazveme *cyklický*, jestliže pro každé kódové slovo $\overline{u} = (u_0 u_1 \dots u_{n-1})$ kód K obsahuje také jeho cyklický posun $c(\overline{u}) = = (u_{n-1} u_0 u_1 \dots u_{n-2})$.

2.7.2 Pro popis cyklických posunů slov se ukazuje výhodné pracovat s n-ticemi znaků jako s polynomy. Proto zavedeme přiřazení

$$\overline{u} = (u_0 u_1 \dots u_{n-1}) \longmapsto u(z) = u_0 + u_1\, z + \dots + u_{n-1}\, z^{n-1}.$$

Cyklický posun je pak realizován vynásobením polynomu $u(z)$ proměnnou z s tím, že $z^n = 1$. Ano

$$\begin{aligned} z \cdot u(z) &= u_0\, z + u_1\, z^2 + \dots + u_{n-2}\, z^{n-1} + u_{n-1}\, z^n \\ &= u_{n-1} + u_0\, z + \dots + u_{n-2}\, z^{n-1}. \end{aligned}$$

Proto chápeme cyklický kód K jako lineární podprostor okruhu $\mathbb{Z}_p[x]/(x^n - 1)$. Pro jednoduchost textu budeme okruh $\mathbb{Z}_p[x]/(x^n - 1)$ značit $\mathbb{Z}_p^{(n)}$. (Poznamenejme také, že jako lineární prostory nad $\mathbb{Z}_p$ se $\mathbb{Z}_p^n$ a $\mathbb{Z}_p^{(n)}$ shodují.)

2.7.3 Tvrzení. Je dán cyklický (n, k)-kód K, $K \subseteq \mathbb{Z}_p^{(n)}$. Pak pro každý polynom $v(z) \in K$ a každý polynom $f(z) \in \mathbb{Z}_p^{(n)}$ platí $f(z) \cdot v(z)$ patří do K. (Uvědomte si, že se součin polynomů odehrává v okruhu $\mathbb{Z}_p^{(n)}$.)

2.7.4 Věta. Je dán cyklický (n, k)-kód K, $K \subseteq \mathbb{Z}_p^{(n)}$. Označme $g(z)$ jeho nenulový polynom nejmenšího stupně. Pak platí:

1. Polynom $v(z)$ leží v kódu K právě tehdy, když $v(z) = f(z) \cdot g(z)$ pro nějaký polynom $f(z) \in \mathbb{Z}_p^{(n)}$.
2. Množina $\{g(z), z\, g(z), z^2\, g(z), \dots, z^{k-1}\, g(z)\}$ tvoří bázi K. Stupeň polynomu $g(z)$ je $n - k$.
3. Polynom $x^n - 1$ je dělitelný polynomem $g(x)$ v okruhu $\mathbb{Z}_p[x]$.

2.7.5 Generující polynom. Je dán cyklický (n, k)-kód K, $K \subseteq \mathbb{Z}_p^{(n)}$. Polynom $g(x)$ z věty 2.7.4 se nazývá *generující polynom* kódu K.

2.7.6 Kódování s generujícím polynomem. Je-li dán generující polynom $g(z)$ cyklického lineárního (n, k)-kódu K. Pak kódování probíhá takto: Máme-li dány informační znaky $(u_0 u_1 \dots u_{k-1})$. Vytvoříme polynom $u(z) = u_0 + u_1\, z + + \dots + u_{k-1}\, z^{k-1}$. Pak

$$u(z) \longmapsto u(z) \cdot g(z).$$

Jestliže polynom $u(z) \cdot g(z)$ je roven $v_0 + v_1\, z + \dots + v_{n-1}\, z^{n-1}$, pak kódování bude

$$(u_0 u_1 \dots u_{k-1}) \longmapsto (v_0 v_1 \dots v_{n-1}).$$

2.7.7 Z předchozího odstavce je jednoduché odvodit generující matici cyklického kódu ze znalosti generujícího polynomu $g(z)$. Generující matice kódu je rovna

$$\mathbf{G} = \begin{pmatrix} g(z) \\ z\,g(z) \\ \vdots \\ z^{k-1}\,g(z) \end{pmatrix}.$$

Přesněji, je-li

$$g(z) = g_0 + g_1\,z + \ldots + g_{n-k}\,z^{n-k},$$

pak generující matice má tvar

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & g_2 & \ldots & g_{n-k} & 0 & \ldots & 0 & 0 \\ 0 & g_0 & g_1 & \ldots & g_{n-k-1} & g_{n-k} & \ldots & 0 & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & 0 & \ldots & 0 & g_0 & \ldots & g_{n-k-1} & g_{n-k} \end{pmatrix},$$

kde v prvním řádku máme $k-1$ nul na konci, v posledním řádku $k-1$ nul na začátku.

2.7.8 Kontrolní polynom. Je dán cyklický (n,k)-kód K, $K \subseteq \mathbb{Z}_p^{(n)}$, s generujícím polynomem $g(x)$ (chápán jako polynom nad $\mathbb{Z}_p$). Z věty 2.7.4 víme, že generující polynom dělí polynom $x^n - 1$. Označme $h(x)$ podíl $x^n - 1$ a $g(x)$, tj. $(x^n - 1) = h(x) \cdot g(x)$ v $\mathbb{Z}_p[x]$. Polynom $h(x)$ se nazývá *kontrolní polynom* kódu K.

2.7.9 Tvrzení. Jestliže $h(x)$ je kontrolní polynom cyklického (n,k)-kódu K, pak jeho stupeň je roven k a platí:

$$v(z) \in K \quad \text{právě tehdy, když} \quad v(z) \cdot h(z) = 0,$$

součin se odehrává v okruhu $\mathbb{Z}_p^{(n)}$.

2.7.10 Poznámka. Z kontrolního polynomu $h(x)$ můžeme jednoduše získat kontrolní matici cyklického lineárního kódu K. Je-li $h(z) = h_0 + h_1\,z + \ldots + h_k\,z^k$, pak kontrolní matice je rovna

$$\mathbf{H} = \begin{pmatrix} 0 & \ldots & 0 & 0 & h_k & h_{k-1} & \ldots & h_1 & h_0 \\ 0 & \ldots & 0 & h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & 0 \\ \vdots & & & & & & & & \\ h_k & h_{k-1} & \ldots & h_1 & h_0 & 0 & 0 & \ldots & 0 \end{pmatrix},$$

kde v prvním řádku máme $n-k-1$ nul na začátku a v posledním řádku $n-k+1$ nul na konci.

2.7.11 Dekódování. Předpokládejme opět, že kanál, kterým se kódová slova vysílají, má tu vlastnost, že dvě chyby jsou téměř vyloučené. Obdobně jako pro lineární kódy, můžeme kontrolní polynom využít k tomu, abychom zjistili, zda přijaté slovo je kódové nebo ne. Jestliže $v(z) \cdot h(z) = 0$, pak slovo $\overline{v}$ je kódové, v opačném případě kódové není.

Je-li $v(z)$ kódové slovo, pak je dělitelné generujícím polynomem $g(z)$ a informaci, která byla zakódována, získáme vydělením polynomu $v(z)$ polynomem $g(z)$.

Pro zjištění, kolik chyb kód objevuje a kolik chyb opravuje, využíváme kontrolní matici a tvrzení, která platí pro lineární kódy. To můžeme, protože každý cyklický kód je lineární.

2.7.12 Systematické kódování. Je dán cyklický lineární (n, k)-kód K s generujícím polynomem $g(z)$, který je symetrický (tj. koeficient u nejvyšší mocniny je stejný jako koeficient u absolutního členu, koeficient u druhé nejvyšší mocniny je stejný jako u lineárního členu, atd.). Následující postup nám ke každému informačnímu slovu $(u_0u_1 \dots u_{k-1})$ přiřadí kódové slovo $(v_0v_1 \dots v_{n-1})$ a to tak, že prvních k míst kódového slova bude vždy rovno k informačním znakům; přesněji

$$v_0 = u_0, v_1 = u_1, \dots, v_{k-1} = u_{k-1}.$$

Nejprve informačnímu slovu přiřadíme polynom stupně $n-1$ takto:

$$(u_0u_1 \dots u_{k-1}) \longmapsto u(z) = u_0\, z^{n-1} + u_1\, z^{n-2} + \dots + u_{k-1}\, z^{n-k}.$$

Nyní vydělíme polynom $u(z)$ generujícím polynomem $g(z)$, dostaneme

$$u(z) = h(z)\, g(z) + r(z) \quad \text{kde} \quad st(r) < st(g) = n - k.$$

Proto

$$u(z) - r(z) = h(z)\, g(z)$$

je polynom z kódu K. Navíc

$$u(z) - r(z) = {}_0\, z^{n-1} + u_1\, z^{n-2} + \dots + u_{k-1}\, z^{n-k} - r_{n-k-1}\, z^{n-k-1} - \dots - r_1\, z - r_0.$$

Vlastní kódování je nyní

$$(u_0u_1 \dots u_{k-1}) \longmapsto (u_0u_1 \dots u_{k-1}v_k \dots v_{n-2}v_{n-1}),$$

kde $v_k = -r_{n-k-1}, \dots, v_{n-2} = -r_1, v_{n-1} = -r_0$.

2.7.13 Poznámka. Kdyby generující polynom nebyl symetrický, k tomu, aby výsledné slovo patřilo do kódu K, bychom museli výsledný polynom „číst odzadu“, tj. od nejnižší mocniny. Dostali bychom tedy slovo, ve kterém by informační znaky byly na konci a v opačném pořadí. Přesněji, dostali bychom slovo $(v_{n-1}v_{n-2} \dots v_k u_{k-1} \dots u_1u_0)$.

2.8 Galoisova tělesa

Ukázali jsme si, jak lze sestrojit konečná tělesa pomocí polynomů nad $\mathbb{Z}_p$. Nyní si ukážeme několik vlastností, které má každé konečné těleso.

2.8.1 Máme dáno konečné těleso $(F, +, \cdot, 0, 1)$. Připomeňme, že $(F, +, 0)$ je komutativní grupa, $(F, \cdot, 1)$ je komutativní monoid, platí distributivní zákony a $0 \neq 1$.

Vezměne prvek $1 \in F$ a utvořme prvky

$$1, 1+1, 1+1+1, \ldots, \underbrace{1+1+\ldots+1}_{i-\text{krát}}, \ldots$$

Protože F je konečná množina, musí existovat i, j, $i < j$, tak že

$$\underbrace{1+1+\ldots+1}_{i-\text{krát}} = \underbrace{1+1+\ldots+1}_{j-\text{krát}}.$$

Pak

$$0 = \underbrace{1+1+\ldots+1}_{(j-i)-\text{krát}}$$

2.8.2 Tvrzení. Označme n nejmenší kladné přirozené číslo, pro které

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

Pak n je prvočíslo.

2.8.3 Charakteristika tělesa. Prvočíslo p z tvrzení 2.8.2 se nazývá *charakteristika* tělesa $(F, +, \cdot, 0, 1)$.

2.8.4 Poznámka. Uvědomte si, že charakteristika p je vlastně řád prvku 1 v grupě $(F, +, 0)$.

2.8.5 Tvrzení. Je dáno konečné těleso $(F, +, \cdot, 0, 1)$ charakteristiky p. Pak pro každé $a, b \in F$ platí

$$(a+b)^p = a^p + b^p.$$

2.8.6 Důsledek. Je dáno konečné těleso $(F, +, \cdot, 0, 1)$ charakteristiky p. Pak

1. Pro každé $a, b \in F$ a $m \geq 0$ platí
$$(a+b)^{p^m} = a^{p^m} + b^{p^m}.$$
2. Pro každý polynom $f(x) \in \mathbb{Z}_p[x]$ a každé $a \in F$ platí
$$(f(a))^p = f(a^p).$$

2.8.7 Tvrzení. Je dáno konečné těleso $(F, +, \cdot, 0, 1)$. Označme $F^\star$ množinu všech nenulových prvků tělesa $(F, +, \cdot, 0, 1)$. Pak grupa invertibilních prvků $(F^\star, \cdot, 1)$ tělesa je cyklická grupa.

Toto tvrzení uvádíme bez důkazu.

2.8.8 Primitivní prvek tělesa. Generátor grupy $(F^\star, \cdot, 1)$ všech nenulových prvků se nazývá *primitivní prvek* tělesa $(F, +, \cdot, 0, 1)$.

2.8.9 Důsledek. Je dáno konečné těleso $(F, +, \cdot, 0, 1)$ o m prvcích. Pak těleso $(F, +, \cdot, 0, 1)$ má $\varphi(m-1)$ primitivních prvků, kde φ je Eulerova funkce definovaná v 1.2.8.

2.8.10 Uveďme ještě dvě základní tvrzení, obě bez důkazu, které nám dávají charakterizaci všech konečných těles. Dříve než tato tvrzení vyslovíme, uveďme definici isomorfismu dvou těles. Zhruba řečeno, dvě tělesa jsou isomorfní, jestliže se liší pouze v pojmenování prvků a výsledky všech operací „si odpovídají“. Přesněji:

Dvě tělesa $(F_1, +_1, \cdot_1, 0_1, 1_1)$ a $(F_2, +_2, \cdot_2, 0_2, 1_2)$ jsou isomorfní, jestliže existuje vzájemně jednoznačné zobrazení ψ množiny F_1 na množinu F_2 takové, že pro každé $a, b \in F_1$ platí

- $\psi(a +_1 b) = \psi(a) +_2 \psi(b)$, tj. je jedno jestli dva prvky nejprve v prvním tělese sečteme a pak je zobrazíme, nebo je napřed zobrazíme a pak v druhém tělese sečteme.
- $\psi(a \cdot_1 b) = \psi(a) \cdot_2 \psi(b)$, tj. je jedno jestli dva prvky nejprve v prvním tělese vynásobíme a pak je zobrazíme, nebo je napřed zobrazíme a pak v druhém tělese vynásobíme.
- $\psi(0_1) = 0_2$ a $\psi(1_1) = 1_2$, tj. odpovídají si nulové a jednotkové prvky obou těles.

2.8.11 Věta. Pro každé konečné těleso $(F, +, \cdot, 0, 1)$ existují prvočíslo p a ireducibilní polynom $q(x) \in \mathbb{Z}_p[x]$ takové že $(F, +, \cdot, 0, 1)$ je isomorfní $(\mathbb{Z}_p[x]/q(x), +, \cdot, 0, 1)$.

2.8.12 Věta. Pro každé prvočíslo p a každé přirozené číslo $k \geq 1$ existuje těleso o p^k prvcích. Toto těleso je až na isomorfismus určeno jednoznačně.

2.8.13 Galoisovo těleso. Těleso z věty 2.8.12 nazýváme *Galoisovo těleso* a značíme ho $GF(p^k)$.

2.8.14 Důsledek. Pro každé $k \geq 1$ a pro každé prvočíslo p existuje v $\mathbb{Z}_p[x]$ ireducibilní polynom stupně k.

2.8.15 Využití primitivního prvku pro cyklické kódy. Chceme vytvořit binární cyklický $(7, 4)$-kód K. Využijeme k tomu těleso $GF(2^3)$; tj. těleso $GF(8)$. Z věty 2.8.11 víme, že toto těleso je isomorfní s $\mathbb{Z}_2[x]/x^3 + x + 1$. S prvky tělesa $\mathbb{Z}_2[x]/x^3 + x + 1$ budeme pracovat jako s polynomy a proměnnou α, pro níž platí

$\alpha^3 + \alpha + 1 = 0$ tj. těleso $\mathbb{Z}_2[x]/x^3 + x + 1$ je vlastně $\{a\,\alpha^2 + b\,\alpha + c \,|\, a, b, c \in \in \mathbb{Z}_2, \alpha^3 = \alpha + 1\}$.

Každé těleso má primitivní prvek (viz 2.8.7). V tělese $\mathbb{Z}_2[x]/x^3 + x + 1$ je primitivním prvkem α. Ano, všechny nenulové prvky tělesa jsou $\alpha^0 = 1$, $\alpha^1 = \alpha$, α^2, $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$ a $\alpha^6 = \alpha^2 + 1$.

Aby náš kód K opravoval jednu chybu, musí mít kontrolní matice $\mathbf{H}$ tohoto kódu různé nenulové sloupce (protože pracujeme nad $\mathbb{Z}_2$, tento fakt nám stačí k tomu, aby každé dva sloupce byly lineárně nezávislé). Potřebujeme tedy matici se sedmi lineárně nezávislými sloupci, z nichž každý sloupec má tři složky (to vyplývá z faktu, že se jedná o $(7, 4)$-kód). Navíc kód K je prostor řešení homogenní soustavy s maticí $\mathbf{H}$. Slovo $\overline{u} = (u_0\, u_1\, \ldots\, u_6)$ je kódovým slovem právě tehdy, když

$$\mathbf{H} \cdot \overline{u}^T = \overline{o}^T. \tag{2.9}$$

Proto položíme

$$\mathbf{H} = (1\, \alpha\, \alpha^2\, \ldots\, \alpha^6), \tag{2.10}$$

(kde každý sloupec odpovídá polynomu stupně nejvýše 2 v proměnné α z $GF(8)$). Volba v 2.10 zaručuje, že matice $\mathbf{H}$ má různé nenulové sloupce o třech složkách.

Nyní podle 2.9 a 2.10 víme, že slovo $\overline{u}$ je kódové právě tehdy, když

$$u(\alpha) = 0, \quad \text{kde} \quad u(z) = u_0 + u_1 z + \ldots + u_6 z^6. \tag{2.11}$$

Vztah 2.11 zaručuje, že kód K je cyklickým kódem; ano, jestliže pro polynom $u(z)$ platí $u(\alpha) = 0$, pak pro polynom $v(z) = z\,u(z)$ také platí $v(\alpha) = \alpha\,u(\alpha) = = 0$. Abychom našli generující polynom kódu K potřebujeme najít nenulový polynom nejmenšího stupně takový, že α je jeho kořen. Žádný polynom stupně 2 nemá α jako kořen. Proto takovým polynomem je $g(z) = z^3 + z + 1$, protože $\alpha^3 + \alpha + 1 = 0$ v $GF(8)$.

Kontrolní polynom dostaneme vydělením polynomu $x^7 - 1$ polynomem $x^3 + + x + 1$. Tedy $h(z) = x^4 + x^2 + x + 1$. Generující matice $\mathbf{G}$ je

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Jiná kontrolní matice, kontrolní matice, kterou dostaneme z kontrolního polynomu má tvar

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Dekódování v případě, kdy došlo k nejvýše jedné chybě. je velmi jednoduché. Předpokládejme, že jsme přijali slovo $\overline{v} = (v_0\, v_1\, \ldots\, v_6)$, tj. $v(z) = v_0 + v_1 z + + \ldots + v_6 z^6$. Pak hodnota $v(\alpha)$ je buď 0, v tomto případě je $\overline{v}$ kódové slovo, nebo $v(\alpha) = \alpha^i$ pro některé $i \in \{0, 1, \ldots, 6\}$. V druhém případě slovo $\overline{v}$ kódové není, ale za předpokladu jediné chyby došlo k chybě v koeficientu u z^i.

Kapitola 3

Svazy a Booleovy algebry

Ukážeme si další algebraické struktury, tentokrát vzniklé z uspořádaných množin.

3.1 Svazy

3.1.1 Uspořádané množiny, posety. Je dána množina A a na ní relace $\sqsubseteq$. Dvojice $(A, \sqsubseteq)$ se nazývá *částečně uspořádaná množina*, též *poset*, jestliže relace $\sqsubseteq$ je reflexivní, antisymetrická a tranzitivní.

Připomeňme, že relace $\sqsubseteq$ na množině A se nazývá

- *reflexivní*, jestliže pro každé $a \in A$ platí $a \sqsubseteq a$;
- *antisymetrická*, jestliže pro každé $a, b \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq a$, tak $a = b$;
- *tranzitivní*, jestliže pro každé $a, b, c \in A$ platí: je-li $a \sqsubseteq b$ a $b \sqsubseteq c$, tak $a \sqsubseteq c$.

3.1.2 Příklady uspořádaných množin.

1. $(\mathbb{R}, \leq)$, kde $\mathbb{R}$ je množina všech reálných čísel, $\leq$ je dobře známé uspořádání reálných čísel.
2. $(\mathcal{P}(U), \subseteq)$, kde U je pevně daná množina a $\mathcal{P}(U)$ je množina všech podmnožin množiny U, $\subseteq$ je relace býti podmnožinou.
3. $(\mathbb{N}, \mid)$, kde relace $\mid$ je relace dělitelnosti na množině přirozených čísel, tj. $n \mid m$ iff existuje $k \in \mathbb{N}$ tak, že $m = k \cdot n$.

3.1.3 Relace pokrývání. Máme dánu uspořádanou množinu $(A, \sqsubseteq)$ a v ní dva prvky a, b. Řekneme, že prvek b *pokrývá* prvek a, jestliže $a \sqsubseteq b$, $a \neq b$ a kdykoli $a \sqsubseteq c \sqsubseteq b$, tak buď $a = c$ nebo $b = c$.

3.1.4 Hasseho diagram. Máme dánu uspořádanou množinu $(A, \sqsubseteq)$. Do *Hasseho diagramu* $(A, \sqsubseteq)$ kreslíme pouze relaci pokrývání a to ještě tak, že prvek, který je níž je ten, který je menší.

3.1.5 Supremum množiny. Mějme uspořádanou množinu $(A, \sqsubseteq)$ a v ní nějakou podmnožinu $X \subseteq A$. Prvek $c \in A$ nazveme *supremum* množiny X, jestliže platí

- $a \sqsubseteq c$ pro každé $a \in X$, (tj. c je horní mez množiny X),
- jestliže také $a \sqsubseteq d$ pro každé $a \in X$, pak nutně $c \sqsubseteq d$ (tj. c je nejmenší horní mez množiny X).

3.1.6 Infimum množiny. Mějme uspořádanou množinu $(A, \sqsubseteq)$ a v ní nějakou podmnožinu $X \subseteq A$. Prvek $c \in A$ nazveme *infimum* množiny X, jestliže platí

- $c \sqsubseteq a$ pro každé $a \in X$, (tj. c je dolní mez množiny X),
- jestliže také $d \sqsubseteq a$ pro každé $a \in X$, pak nutně $d \sqsubseteq c$ (tj. c je největší dolní mez množiny X).

3.1.7 Tvrzení. Jestliže existuje supremum (infimum) některé množiny X v $(A, \sqsubseteq)$, pak je určeno jednoznačně.

Proto značíme $\sup(X)$ supremum množiny X a $\inf(X)$ infimum množiny X.

3.1.8 Svaz. *Svaz* je uspořádaná množina $(A, \sqsubseteq)$, kde pro každé $a, b \in A$ existuje $\sup(\{a, b\})$ a $\inf(\{a, b\})$.

3.1.9 Operace ve svazu. Je dána uspořádaná množina $(A, \sqsubseteq)$, která je svazem; t.j. existují suprema a infima každé dvojice prvků $a, b \in A$. Pak $\sup(\{a, b\})$ a $\inf(\{a, b\})$ jsou určeny jednoznačně a můžeme se proto na ně dívat jako na binární operace.

Označme

$$a \vee b = \sup(\{a, b\}), \quad a \wedge b = \inf(\{a, b\}).$$

Operace $\vee$ se někdy také nazývá spojení, operace $\wedge$ průsek.

3.1.10 Tvrzení. Je dán svaz $(A, \sqsubseteq)$. Pak pro operace $\vee$ a $\wedge$ platí:

(1) Pro každý prvek $a \in A$ platí

$$a \vee a = a \quad \text{a} \quad a \wedge a = a.$$

(2) Pro každé dva prvky $a, b \in A$ platí

$$a \vee b = b \vee a \quad \text{a} \quad a \wedge b = b \wedge a.$$

(3) Pro každé tři prvky $a, b, c \in A$ platí

$$a \vee (b \vee c) = (a \vee b) \vee c \quad \text{a} \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c.$$

(4) Pro každé dva prvky $a, b \in A$ platí

$$a \vee (b \wedge a) = a \quad \text{a} \quad a \wedge (b \vee a) = a.$$

3.1.11 Tvrzení. Je dán svaz $(A, \sqsubseteq)$. Pak pro každé dva prvky $a, b \in A$

$$a \vee b = b \quad \text{právě tehdy, když} \quad a \wedge b = a.$$

3.1.12 Věta. Je dána množina A spolu se dvěma binárními operacemi $\vee$ a $\wedge$, které splňují podmínky (1) – (4) z tvrzení 3.1.10. Definujme relaci $\sqsubseteq$ na množině A takto:

$$a \sqsubseteq b \quad \text{právě tehdy, když} \quad a \vee b = b \text{ (tj. } a \wedge b = a).$$

Pak relace $\sqsubseteq$ je uspořádání na množině A a navíc

$$a \vee b = \sup_{\sqsubseteq}(\{a, b\}) \quad \text{a} \quad a \wedge b = \inf_{\sqsubseteq}(\{a, b\}).$$

3.1.13 Poznámka. Předchozí věta vlastně říká, že na svaz se můžeme dívat dvěma různými způsoby: buď jako na uspořádanou množinu, kde každé dva prvky mají supremum a infimum, nebo jako na množinu spolu s dvěma binárními operacemi splňující podmínky (1) – (4) z 3.1.10. Budeme proto svaz značit jako čtveřici $(A, \vee, \wedge, \sqsubseteq)$ a pracovat nejen s binárními operacemi, ale i s odpovídajícím uspořádáním.

3.1.14 Suprema a infima ostatních množin. V libovolném svazu existuje supremum a infimum každé konečné neprázdné množiny. Ano, je-li $X = \{a_1, a_2, \ldots, a_n\}$, pak

$$\sup(X) = a_1 \vee a_2 \vee \ldots \vee a_n \quad \text{a} \quad \inf(X) = a_1 \wedge a_2 \wedge \ldots \wedge a_n.$$

Uvědomte si, že nemusíme psát závorky, protože v každém svazu pro operace suprema i infima platí asociativní zákon.

3.1.15 Supremum a infimum prázdné množiny. Máme dán libovolný svaz $(A, \vee, \wedge, \sqsubseteq)$. Pak každý prvek $a \in A$ je horní mez prázdné množiny. Ano, kdyby totiž některý prvek $a \in A$ nebyl horní mezí prázdné množiny $\emptyset$, tak by existoval prvek $x \in \emptyset$ takový, že neplatí $x \sqsubseteq a$. Ale $\emptyset$ žádný prvek nemá, takže to není možné.

Protože supremum je nejmenší horní mez, je $\sup(\emptyset) = c$, kde c je nejmenší prvek v uspořádání $(A, \sqsubseteq)$.

Obdobně se ukáže, že každý prvek svazu je dolní mez prázdné množiny $\emptyset$. Protože infimum je rovno největší dolní mezi, je $\inf(\emptyset)$ roven největšímu prvku uspořádané množiny $(A, \sqsubseteq)$.

3.1.16 Poznámka. Z 3.1.15 vyplývá, že ne v každém svazu existuje supremum a infimum prázdné množiny. Ano, existují svazy, které nemají nejmenší a/nebo největší prvek. Tyto svazy však musí být nekonečné, jak ukazuje následující tvrzení.

3.1.17 Tvrzení. Každý konečný svaz $(A, \vee, \wedge, \sqsubseteq)$ má největší a nejmenší prvek. Největší prvek je roven $\sup(A)$, nejmenší $\inf(A)$.

3.1.18 V dalším textu budeme nejmenší prvek ve svazu značit $\underline{0}$ a největší prvek $\underline{1}$. Uvědomte si, že pro $a \in A$ platí:

$$a \vee \underline{1} = \underline{1}, \quad a \wedge \underline{1} = a, \quad a \vee \underline{0} = a, \quad a \wedge \underline{0} = \underline{0}.$$

3.1.19 Úplný svaz. Svaz $(A, \vee, \wedge, \sqsubseteq)$ nazveme *úplný*, jestliže existuje supremum a infimum libovolné množiny $X \subseteq A$.

3.1.20 Poznámka. Každý konečný svaz je úplný. Existují i nekonečné svazy, které jsou úplné: např. $(\mathcal{P}(\mathbb{N}), \cup, \cap, \subseteq)$ je úplný svaz. Svaz $(\mathbb{R}, \leq)$ není úplný, nemá např. supremum prázdné množiny, nebo supremum množiny všech kladných reálných čísel.

3.1.21 Tvrzení. V každém svazu $(A, \vee, \wedge, \sqsubseteq)$ pro každé tři prvky $a, b, c \in A$ platí

$$a \vee (b \wedge c) \sqsubseteq (a \vee b) \wedge (a \vee c),$$

$$a \wedge (b \vee c) \sqsubseteq (a \wedge b) \vee (a \wedge c).$$

3.1.22 Distributivní svaz. Svaz $(A, \vee, \wedge, \sqsubseteq)$ nazveme *distributivní svaz*, jestliže pro každé tři prvky $a, b, c \in A$ platí

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c). \tag{3.1}$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c). \tag{3.2}$$

3.1.23 Příklady distributivních svazů.

1. Svaz $(\mathcal{P}(U), \cup, \cap, \subseteq)$ je distributivní.
2. Svaz $(\mathbb{N}, \mathrm{lcm}, \gcd, |\,)$ je distributivní.

3.1.24 Tvrzení. Ve svazu $(A, \vee, \wedge, \sqsubseteq)$ platí rovnost (3.1) právě tehdy, když platí rovnost (3.2).

Znamená to, že ve svazu stačí ověřit jednu z rovností (3.1) a (3.2). Platí-li jedna, platí i druhá, neplatí-li jedna, neplatí ani druhá.

3.1.25 Svaz $\mathcal{L}_3$. Označme $\mathcal{L}_3$ následující svaz s pěti prvky $a, b, c, \underline{0}, \underline{1}$:
Prvky a, b, c jsou po dvou nesrovnatelné, $\underline{0}$ je nejmenší prvek a $\underline{1}$ je největší prvek.

Svazu $\mathcal{L}_3$ se také říká diamond nebo třílapmionek.

3.1.26 Svaz $\mathcal{P}_5$. Označme $\mathcal{P}_5$ následující svaz s pěti prvky $a, b, c, \underline{0}, \underline{1}$:
Prvky a a c jsou nesrovnatelné, prvky b a c jsou nesrovnatelné, $a \sqsubseteq b$, $\underline{0}$ je nejmenší prvek, $\underline{1}$ je největší prvek.

Svazu $\mathcal{P}_5$ se též říká pentagon.

3.1.27 Ve svazu $\mathcal{L}_3$ platí

$$a \vee (b \wedge c) = a \vee \underline{0} = a \quad \text{a} \quad (a \vee b) \wedge (a \vee c) = \underline{1} \wedge \underline{1} = \underline{1}.$$

Ve svazu $\mathcal{P}_5$ platí

$$a \vee (b \wedge c) = a \vee \underline{0} = a \quad \text{a} \quad (a \vee b) \wedge (a \vee c) = b \wedge \underline{1} = b.$$

Tedy oba svazy $\mathcal{L}_3$ a $\mathcal{P}_5$ nejsou distributivní. Platí v nich však nerovnosti z 3.1.21.

To může pomoci při „zapamatování“ nerovnosti z 3.1.21; zkusíme jaká nerovnost platí ve svazu $\mathcal{L}_3$ pro prvky a, b, c a stejná nerovnost pak platí v každém svazu.

3.1.28 Podsvaz. K tomu, abychom mohli charakterizovat distributivní svazy, potřebujeme pojem podsvazu.

Máme dán svaz $(A, \vee, \wedge, \sqsubseteq)$. Množinu $B \subseteq A$ nazveme *podsvaz* svazu $(A, \vee \vee, \wedge, \sqsubseteq)$, jestliže platí

$$\text{je-li} \quad b, c \in B \quad \text{pak} \quad b \vee c,\ b \wedge c \in B.$$

Je tedy podsvazem taková podmnožina, která je „uzavřena“ na obě svazové operace.

3.1.29 Věta. Svaz je distributivní právě tehdy, když neobsahuje ani $\mathcal{L}_3$ ani $\mathcal{P}_5$ jako podsvaz.

3.1.30 Doplněk. Jedním z příkladů svazu, který jsme si ukázali, je svaz všech podmnožin dané množiny U – svaz $(\mathcal{P}(U), \cup, \cap, \subseteq)$. Víme, že tento svaz má nejmenší prvek $\underline{0} = \emptyset$ a největší prvek a to $\underline{1} = U$. V množinách známe ještě jednu operaci — a to doplněk. Dolněk množiny X je množina $U \setminus X$. Zobecníme dolněk i pro další svazy.

Je dán svaz $(A, \vee, \wedge, \sqsubseteq)$ s nejmenším prvkem $\underline{0}$ a největším prvkem $\underline{1}$. Prvek $b \in A$ nazveme *dopněk* prvku a, jestliže

$$b \vee a = \underline{1} \quad \text{a} \quad b \wedge a = \underline{0}.$$

3.1.31 Poznámka. Všimněte si, že dopněk množiny, tak jak jsme si ho připomněli v minulém odstavci, odpovídá doplňku ve svazu $(\mathcal{P}(U), \cup, \cap, \subseteq, \emptyset, U)$.

V obecném svazu nemusí být doplněk určen jednoznačně. Uvažujme např. svaz $\mathcal{L}_3$ z 3.1.25. Pak prvky b i c jsou dopňky prvku a. Ano, $a \vee b = \underline{1} = a \vee c$ a $a \wedge b = \underline{0} = a \wedge c$.

3.1.32 Tvrzení. Je-li svaz $(A, \vee, \wedge, \sqsubseteq, \underline{0}, \underline{1})$ distributivní, pak každý prvek má nejvýše jeden doplněk.

3.1.33 Poznámka. V distributivním svazu se dá dokázat i více.

Platí-li v distributivním svazu

$$a \vee b = a \vee c \quad \text{a} \quad a \wedge b = a \wedge c,$$

pak $b = c$.

3.1.34 Poznámka. Existují distributivní svazy, ve kterých některé prvky dolněk nemají. Uvažujme na příklad svaz skládající se ze tří prvků $\underline{0}, a, \underline{1}$, kde $\underline{0} \sqsubseteq a, a \sqsubseteq \underline{1}$; tj. $\underline{0}$ je nejmenší prvek, $\underline{1}$ je největší prvek, a a je „mezi nimi“. Pak prvek a nemá doplněk.

3.1.35 Komplementární svaz. Svaz $(A, \vee, \wedge, \sqsubseteq)$ s nejmenším prvkem $\underline{0}$ a největším prvkem $\underline{1}$ se nazývá *komplementární*, jestliže každý prvek $a \in A$ má doplněk.

3.1.36 Je dán distributivní, komplementární svaz $(A, \vee, \wedge, \sqsubseteq, \underline{0}, \underline{1})$. Pak doplněk každého prvku existuje a je určen jednoznačně. Můžeme se tedy na doplněk dívat jako na unární operaci na množině A. Budeme proto značit $\overline{a}$ doplněk prvku $a \in A$.

3.2 Booleovy algebry

Jistě jste se již setkali s Booleovou algebrou a to buď v logice nebo v logických obvodech. Jednalo se o dva prvky $0, 1$ a na nich byly definovány operace $\vee$, $\wedge$ a $^-$ známým způsobem. Toto byl příklad jedné Booleovy algebry — totiž té nejmenší. Uspořádání bylo dáno $0 \leq 0$, $0 \leq 1$ a $1 \leq 1$, doplňky: $\overline{0} = 1$, $\overline{1} = 0$.

3.2.1 Booleova algebra. Každý svaz, který je distributivní a komplementární, nazveme *Booleova algebra*.

Booleovu algebru budeme značit jako sedmici $(B, \vee, \sqsubseteq, \wedge, \underline{0}, \underline{1}, ^-)$, kde první část, totiž $(B, \vee, \wedge)$, je distributivní svaz, $\underline{0}$ je nejmenší prvek, $\underline{1}$ je největší prvek tohoto svazu a $^-$ je operace doplňku.

3.2.2 Příklady Booleových algeber. Tak zvaná hyperkrychle (hypercube) je vlastně příklad Booleovy algebry. Máme dáno přirozené číslo $n \geq 1$. Označme $B_n = \{0,1\}^n$, tj.

$$B_n = \{(a_1, a_2, \ldots, a_n) \,|\, a_i \in \{0,1\}\}.$$

Na množině B_n definujeme binární operace $\vee$ a $\wedge$ takto:

$$(a_1, a_2, \ldots, a_n) \vee (b_1, b_2, \ldots, b_n) = (a_1 \vee b_1, a_2 \vee b_2, \ldots, a_n \vee b_n),$$

$$(a_1, a_2, \ldots, a_n) \wedge (b_1, b_2, \ldots, b_n) = (a_1 \wedge b_1, a_2 \wedge b_2, \ldots, a_n \wedge b_n).$$

Trojice $(B_n, \vee, \wedge)$ je distributivní svaz s nejmenším prvkem $(0, 0, \ldots, 0)$ a největším prvkem $(1, 1, \ldots, 1)$. Není obtížné nahlédnout, že v tomto distributivním svazu existuje doplněk každého prvku a to

$$\overline{(a_1, a_2, \ldots, a_n)} = (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}).$$

Uvědomte si, že se vlastně jedná o kartézský součin n exemplářů nejmenší Booleovy algebry.

3.2.3 Tvrzení. Je dána Booleova algebra $(B, \vee, \wedge, \sqsubseteq, \underline{0}, \underline{1}, ^-)$. Pak platí

1. $\overline{\underline{0}} = \underline{1}$, $\overline{\underline{1}} = \underline{0}$
2. $\overline{\overline{a}} = a$ pro každé $a \in B$
3. $\overline{a \vee b} = \overline{a} \wedge \overline{b}$, $\overline{a \wedge b} = \overline{a} \vee \overline{b}$ pro každé $a, b \in B$,
4. $a \sqsubseteq b$ právě tehdy, když $\overline{b} \sqsubseteq \overline{a}$.

3.2.4 Věta. Každá konečná Booleova algebra je až na přejmenování shodná (isomorfní) s Booleovou algebrou $(B_n, \vee, \wedge, (0, 0, \ldots, 0), (1, 1, \ldots, 1), ^-)$.

3.2.5 Důsledek. Je-li $(B, \vee, \wedge, \sqsubseteq, \underline{0}, \underline{1}, ^-)$ konečná Booleova algebra, pak množina B má 2^n prvků.

3.2.6 Poznámka. Mějme konečnou množinu o n prvcích $U = \{1, 2, \ldots, n\}$. Víme, že $(\mathcal{P}(U), \cup, \cap, \subseteq, ^-)$ je Booleova algebra, protože se jedná o distributivní a komplementární svaz. Podle věty 3.2.4 je tato Booleova algebra isomorfní s některou hyperkrychlí (v tomto případě se jedná o hyperkrychli B_n). Ukážeme si, jak si tyto dvě Booleovy algebry odpovídají:

Každá podmnožina $X \subseteq U$ je jednoznačně určena svojí charakteristickou funkcí $\chi_X : U \to \{0, 1\}$, kde

$$\chi_X(i) = \begin{cases} 1, & \text{pro} \quad i \in X \\ 0, & \text{pro} \quad i \notin X \end{cases}$$

Navíc, na zobrazení z množiny $\{1, 2, \ldots, n\}$ do množiny $\{0, 1\}$ se můžeme dívat jako na uspořádané n-tice nul a jedniček (v i-té složce je 1, je-li $\chi_X(i) = 1$ a 0, je-li $\chi_X(i) = 0$), Charakteristické funkce jsou tedy prvky hyperkrychle B_n.

Přiřazení je dáno

$$X \subseteq \{1, 2, \ldots, n\} \quad \longmapsto \quad (a_1\, a\, \ldots\, a_n)$$

kde $a_i = 1$ iff $i \in X$ a $a_i = 0$ iff $i \notin X$.

Tedy např. množině $\{1, 2, \ldots, n\}$ je přiřazena n-tice samých jedniček, prázdné množině pak n-tice samých nul.

Operaci sjednocení v $\mathcal{P}(U)$ odpovídá operace $\vee$ v B_n, operaci průniku odpovídá operace $\wedge$ v B_n, atd. Jedná se tedy o isomorfismus mezi booleovskými algabrami; víc o isomorfismu se dozvíte v následující kapitole.

Kapitola 4

Homomorfismy a volné algebry

4.1 Homomorfismy a isomorfismy

4.1.1 Ukázali jsme si řadu příkladů tzv. algeber, tj. množin, na kterých jsou dány operace a tyto operace splňují jisté rovnosti. Připomeňme si je:

1. Pologrupa je dvojice $(A, *)$, kde A je množina, $*$ je binární operace splňující asociativní zákon
$$a * (b * c) = (a * b) * c.$$

2. Monoid je trojice $(A, *, e)$, kde $(A, *)$ je pologrupa a prvek e splňuje
$$a * e = a, \quad e * a = a.$$
Prvku e říkáme jednotkový prvek.

3. Grupa je čtveřice $(A, *, e, ^{-1})$, kde $(A, *, e)$ je monoid, kde každý prvek $a \in A$ má inversní prvek a^{-1}, tj. platí
$$a * a^{-1} = e, \quad a^{-1} * a = e.$$

4. Okruh je pětice $(R, +, \cdot, 0.-)$, kde $(R, +, 0, -)$ je komutativní grupa (tj. $a+b = b+a$ pro všechny $a, b \in R$), $(R, \cdot)$ je pologrupa a platí distributivní zákony
$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

5. Svaz je trojice $(A, \vee, \wedge)$, kde $\vee$ a $\wedge$ jsou binární operace splňující rovnosti 1) až 4) z 3.1.10.

6. Booleova algebra je šestice $(A, \vee, \wedge, \underline{0}, \underline{1}, ^{-})$, kde $(A, \vee, \wedge)$ je distributivní svaz s nejmenším prvkem $\underline{0}$, největším prvkem $\underline{1}$, kde každý prvek má doplněk. Uvědomte si, že jak nejmenší, tak největší prvek je charakterizován rovnostmi, totéž platí o doplňku.

4.1.2 Typ algebry. *Typem* algebry nazveme soubor, který udává kolik a jakých operací se v dané algebře nachází.

Tedy pologrupa je algebra typu (2), protože obsahuje jednu binární operaci.

Monoid je algebra typu $(2, 0)$, protože kromě binární operace obsahuje ještě jednotkový prvek a ten považujeme za nulární operaci.

Grupa je algebra typu $(2, 0, 1)$, protože k binární a nulární operaci obsahuje též unární operaci — tvorba inversního prvku.

Okruh je algebra typu $(2, 2, 0, 1)$, jsou zde dvě binární operace a to sčítání a násobení, přitom pro sčítání máme neutrální prvek a můžeme odčítat — tj. máme opačné prvky.

Svaz je algebra typu $(2, 2)$, jsou zde definovány dvě binární operace.

Booleova algebra je algebra typu $(2, 2, 0, 0, 1)$, jsou zde definovány dvě binární operace, dvě nulární operace (nejmenší a největší prvek) a jedna unární operace (doplněk).

4.1.3 Poznámka. Pojem univerzální algebry je značně abstraktní. Uvádíme ho tady z toho důvodu, že řada struktur, které jsme do teď studovali, zapadá pod tento obecný pohled. Navíc, řada tvrzení platí pro univerzální algebry obecně a je zbytečné dokazovat každé z nich nezávisle.

Mezi vyjmenovanými chybí těleso. Je to proto, že přiřazení inverzního prvku v tělese není unární operací, protože inverzní prvek neexistuje pro všechny prvky tělesa, ale pouze pro ty nenulové.

4.1.4 Univerzální algebra. Univerzální algebra typu Δ je množina A spolu s operacemi, jejichž arity jsou předepsány právě typem Δ. Algebru značíme $\mathcal{A}$ a množinu A nazýváme *nosnou množinou* algebry.

Tedy pologrupa, monoid, grupa, okruh, svaz a Booleova algebra jsou příklady univerzálních algeber (různých typů). Co je pro jednotlivé algebry podstatné, jsou ještě rovnice, které tyto algebry splňují. Budeme proto mluvit a algebře typu Δ splňující rovnice E.

4.1.5 Podalgebra. Řekneme, že množina B je uzavřena na binární operaci $*$, jestliže pro každé dva prvky $a, b \in B$ je jejich vvýsledek $a * b$ také v množině B.

Řekneme, že množina B je uzavřena na unární operaci $^-$, jestliže pro každý dva prvek $b \in B$ je jejich vvýsledek $\overline{b}$ také v množině B.

Řekneme, že množina B je uzavřena na nulární operaci e, jestliže e leží v množině B.

Podalgebra algebry s nosnou množinou A je podmnožina $B \subseteq A$, která je uzavřena na všechny operace dané algebry.

4.1.6 Poznámka. Uvědomte si, že takto jsme definovali podpologrupu, podmonoid, podgrupu i podsvaz.

4.1.7 Tvrzení. Jestliže algebra $\mathcal{A}$ splňovala rovnice E, pak každá její podalgebra tyto rovnice splňuje také.

Takže podsvaz daného svazu je také svazem, podgrupa dané grupy je také grupou, atd.

4.1.8 Respektování operací. Mějme dány dvě algebry $\mathcal{A}$ a $\mathcal{B}$ s nosnými množinami A a B stejného typu. Řekneme, že zobrazení $f\colon A \to B$ *respektuje, zachovává* binární operaci $*$, jestliže pro každé $x, y \in A$ platí

$$f(x *_{\mathcal{A}} y = f(x) *_{\mathcal{B}} f(x).$$

Řekneme, že zobrazení $f\colon A \to B$ *respektuje, zachovává* unární operaci $^-$, jestliže pro každé $x \in A$ platí

$$f(\overline{x}) = \overline{f(x)}.$$

Řekneme, že zobrazení $f\colon A \to B$ *respektuje, zachovává* nulární operace e, jestliže platí

$$f(e_{\mathcal{A}}) = e_{\mathcal{B}}.$$

4.1.9 Homomorfismus algeber. Jsou dány dvě algebry $\mathcal{A}, \mathcal{B}$ stejného typu a splňující rovnice E; $\mathcal{A}$ má nosnou množinu A, $\mathcal{B}$ má nosnou množinu B.

Homomorfismus algebry $\mathcal{A}$ do algebry $\mathcal{B}$ je zobrazení $f\colon A \to B$, které respektuje všechny operace.

4.1.10 Poznámka. Uvědomte si, že takto jsme definovali pologrupový homomorfismus, tj. zobrazení, které respektuje binární operaci, monoidový homomorfismus, tj. zobrazení, které respektuje i jednotkový prvek, grupový homomorfismus, tj. zobrazení, které navíc respektuje inversní prvky, svazový homomorfismus, tj. zobrazení, které respektuje suprema a infima, atd.

Homomorfismus tělesa $\mathcal{F}_1$ do tělesa $\mathcal{F}_2$ je každý okruhový homomorfismus, který navíc respektuje jednotkové prvky, tj. $f(1_1) = 1_2$.

4.1.11 Tvrzení. Máme dány dvě grupy $(G, *, 1_G, ^{-1_G})$ a $(H, \circ, 1_H, ^{-1_H})$. Jestliže zobrazení $f\colon G \to H$ respektuje binární operaci, pak respektuje i zbývající operace.

Jinými slovy, je-li zobrazení mezi dvěma grupami pologrupovým homomorfismem, je i grupovým homomorfismem.

4.1.12 Isomorfismus. Homomorfismus f, který je bijektivním zobrazením, nazveme *isomorfismus*.

4.1.13 Příklady isomorfismů.

1. Funkce $\log_{10}$ je isomorfismus grupy $(\mathbb{R}^+, \cdot, 1, ^{-1})$ na grupu $(\mathbb{R}, +, 0, -)$, kde $\mathbb{R}^+$ značí množinu všech kladných reálných čísel.

2. Mějme dána dvě nesoudělná přirozená čísla n a m. Čínská věta o zbytcích dává isomorfismus $(\mathbb{Z}_{n\cdot m}, +, 0)$ na $(\mathbb{Z}_n, +, 0) \times (\mathbb{Z}_m, +, 0)$.

   Obdobně $(\mathbb{Z}_{n\cdot m}, \cdot, 1)$ je isomorfní s $(\mathbb{Z}_n, \cdot, 1) \times (\mathbb{Z}_m, \cdot, 1)$ a $(\mathbb{Z}^*_{n\cdot m}, \cdot, 1)$ je isomorvní s $(\mathbb{Z}^*_n, \cdot, 1) \times (\mathbb{Z}^*_m, \cdot, 1)$.

3. Existuje isomorfismus Booleovy algebry $(\mathcal{P}(U), \cup, \cap, \subseteq, ^-)$ na Booleovu algebru $(B_n, \vee, \wedge, (0, 0, \ldots, 0), (1, 1, \ldots, 1), ^-)$, viz 3.2.6.

4.1.14 Tvrzení. Je-li f homomorfismus algebry $\mathcal{A}$ do algebry $\mathcal{B}$, pak obraz $f(A)$ nosné množiny A algebry $\mathcal{A}$ je podalgebra algebry $\mathcal{B}$.

4.1.15 Poznámka. Tedy speciálně, je-li f homomorfismus pologrup, pak obraz $f(A)$ pologrupy $\mathcal{A}$ je podpologrupa pologrupy $\mathcal{B}$; je-li f grupový homomorfismus, pak obraz grupy je podgrupa, atd.

4.1.16 Tvrzení. Jou dány dvě grupy $\mathcal{G} = (G, *, 1_G, {}^{-1_G})$ a $\mathcal{H} = (H, \circ, 1_H, {}^{-1_H})$. Pak existuje homomorfismus $f\colon \mathcal{G} \to \mathcal{H}$ definovaný

$$f(x) = 1_H \quad \text{pro každé} \quad x \in G.$$

Tento homomorfismus se též nazývá *triviální homomorfismus*.

4.1.17 Volná algebra nad množinou generátorů. Uvažujme třídu $\mathcal{T}$ všech algeber typu Δ splňující rovnice E. Řekneme, že algebra $\mathcal{F}(X)$ je *volná algebra* v $\mathcal{T}$, jestliže pro každou algebru $\mathcal{A}$ ze třídy $\mathcal{T}$ lze libovolné zobrazení $f\colon X \to A$ jednoznačně rozšířit na homomorfismus z $\mathcal{F}(X)$ do $\mathcal{A}$.

4.1.18 Příklady.

1. Je dána abeceda A. Pak množina všech neprázdných slov A^+ spolu s operací zřetězení je volná pologrupa nad množinou generátorů A.
2. Je dána abeceda A. Pak množina všech slov $A^\star$ spolu s operací zřetězení je volný monoid nad množinou generátorů A.
3. $(\mathbb{Z}, +, 0)$ je volná grupa nad jedním generátorem, kterým je číslo 1.