29.11.

3. Booleovy algebry

3.1. Určete počet prvků konečné Booleovy algebry, která obsahuje 5 atomů.

Využijeme Větu z přednášky, která říká, že konečná Booleova algebra je izomorfní potenční algebře $(\mathcal{P}(A), \cap, \cup, ', \emptyset, A)$ všech podmnožin množiny všech atomů, To mimo jiné znamená, že obě algebry mají stejný počet prvků. Tedy Booleova algebra obsahující 5 atomů má právě $2^5 = 32$ prvků. □

3.2. Rozhodněte, zda existuje Booleova algebra o 8, 9, 63, 64 prvcích.

Opět uvážíme, že konečná Booleova algebra je izomorfní nějaké potenční algebře $(\mathcal{P}(A), \cap, \cup, ', \emptyset, A)$, tedy obsahuje právě $2^{|A|}$ prvků. Vidíme, že algebra o 8 a 64 prvcích existují (a jsou izomorfní algebře $(\mathcal{P}(\{1,2,3\}), \cap, \cup, ', \emptyset, \{1,2,3\})$, respektive $(\mathcal{P}(\{1,2,3,4,5,6\}), \cap, \cup, ', \emptyset, \{1,2,3,4,5,6\}))$ a že Booleovy algebry o 9 a 63 prvcích neexistují. □

3.3. V Booleově algebře $(\mathcal{P}(\{1,2,3,4,5\}), \cap, \cup, ', \emptyset, \{1,2,3,4,5\})$ najděte všechny atomy a rozhodněte, zda obsahuje podalgebru o 16 prvcích.

Atomem je prvek, který není roven nejmenšímu prvku Booleovy algebry, kterým je $\emptyset$, ale mezi ním a $\emptyset$ žádný prvek neleží. To znamená, že atomy dané Booleovy algebry jsou právě jednoprvkové množiny, tj. množiny $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{5\}$.

Zvolme množinu $\mathcal{X} = \mathcal{P}(\{1,2,3\}) \cup \{X \cup \{4,5\} |\ X \in P(\{1,2,3\})\}$, snadno přímočarou úvahou nahlédneme, že jde o množinu uzavřenou na průniky, sjednocení a komplementy a že $\emptyset, \{1,2,3,4,5\} \in \mathcal{X}$, tedy jde o podalgebru dané Booleovy algebry. Navíc zřejmě $|\mathcal{X}| = 2 \cdot 2^3 = 16$. □

3.4. Rozhodněte kolik obsahuje Booleova algebra o 2^{57} prvcích atomů, a zda obsahuje podalgebru o 2^{31} prvcích.

Stejnou úvahou jako v předchozích úlohách nahlédneme, že Booleova algebra o 2^{57} prvcích obsahuje 57 atomů a že její podalgebra o 2^{31} prvcích existuje (řešíme-li úlohu v algebře podmnožin 57-prvkové množiny, stačí vzít množinu podmnožin nějké 30-prvkové pomnožiny a jejich komplementy). □

6.12.

4. Grupy

4.1. Dokažte, že množina $10\mathbf{Z}_{180} = \{10 \cdot k |\ k \in \mathbf{Z}_{18}\}$ je podgrupou cyklické grupy $(\mathbf{Z}_{180}, +, -, 0)$.

Potřebujeme ověřit, že pro každé $x, y \in 10\mathbf{Z}_{180}$ platí, že $-x, x+y \in 10\mathbf{Z}_{180}$, zřejmě přitom $0 \in 10\mathbf{Z}_{180}$. Tedy, jestliže $x = 10r$ a $y = 10s$ pro $x, y \in 10\mathbf{Z}_{18}$ pak:

$$x + y = 10((r+s)\mathrm{mod}18) \text{ a } -x = 10((-r)\mathrm{mod}18).$$

Tedy vidme, že $10\mathbf{Z}_{180}$ je osmnáctiprvková podgrupa grupy $(\mathbf{Z}_{180}, +, -, 0)$. □

4.2. Kolik prvků obsahují podgrupy $\langle 6\rangle$, $\langle 34\rangle$, $\langle 49\rangle$, $\langle 178\rangle$ grupy $(\mathbf{Z}_{180}, +, -, 0)$?

Díky Eukleidovu algoritmu víme, že $\langle k\rangle = \langle NSD(k, 180)\rangle$ a podobně jako v předchozí úloze nahlédneme, že $|\langle k\rangle| = |\langle NSD(k, 180)\rangle| = \frac{180}{\langle NSD(k,180)\rangle}$. Tedy $|\langle 6\rangle| = 30$, $|\langle 34\rangle| = |\langle 178\rangle| = 90$, a $|\langle 49\rangle| = 180$. □

4.3. Kolik podgrup obsahuje grupa $(\mathbf{Z}_{33}, +, -, 0)$?

Stačí uvážit, že všechny podgrupy cyklické grupy $(\mathbf{Z}_{33}, +, -, 0)$ jsou opět cyklické, tedy tvaru $n\mathbf{Z}_{33} = \{(k \cdot n)\mathrm{mod}33|\ k \in \mathbf{Z}_{33}\}$. Díky Eukleidovu algoritmu máme $n\mathbf{Z}_{33} = NSD(n, 33)\mathbf{Z}_{33}$, tudíž statčí spočítat dělitele čísla 33, které je právě 4. Tedy v grupě $(\mathbf{Z}_{33}, +, -, 0)$ leží 4 podgrupy. □

4.4. Dokažte, že každý homomorfismus f grupy $(\mathbf{Z}_n, +, -, 0)$ do sebe je tvaru $f(a) = k \cdot a$, kde $k \in \mathbf{Z}_n$ a $\cdot$ je násobení modulo n.

Vezměme nějaký homomorfismus f grupy $\mathbf{Z}_n(+, -, 0)$ do sebe a položme $k = f(1)$. Potom zjevně $f(1 + 1) = k + k = 2 \cdot k$, $f(1 + 1 + 1) = k + k + k = 3 \cdot k$, atd. Indukcí snadno dostáváme, že $f(a) = k \cdot a$. Potřebujeme ještě ukázat, že každé zobrazení f_k dané předpisem $f_k(a) = k \cdot a$ je grupový homomorfismus. Podle Tvrzení 14.4(1) ze skript stačí ověřit slučitelnost f_k s binární operací $+$. Protože $f_k(a+b) = k\cdot(a+b) = k\cdot a+k\cdot b = f_k(a)+f_k(b)$, tvoří $\{f_k|k \in \mathbf{Z}_n\}$ množinu všech endomorfismů grupy $\mathbf{Z}_n(+, -, 0)$. □

4.5. Dokažte, že homomorfismus $f_k(a) = k \cdot a$ z předchozího příkladu je izomorfismem právě tehdy, když jsou k a n nesoudělná.

Protože je f_k zobrazení konečné množiny do sebe, je f_k bijekce, právě když je to zobrazení na, tj. $\langle k\rangle = \langle f_k(1)\rangle = f_k(\mathbf{Z}_n) = \mathbf{Z}_n$. To zřejmě nastává právě tehdy, když je k generátor cyklické grupy $\mathbf{Z}_n(+, -, 0)$, což platí právě tehdy, když je $NSD(k, n) = 1$. □

4.6. Najděte aspoň 3 izomorfismy grupy $(\mathbf{Z}_{100}, +, -, 0)$ do sebe.

Podle předchozí úlohy potřebujeme najít 3 čísla z množiny $\mathbf{Z}_{100}$, která jsou nesoudělná s číslem 100, vezmeme například, 1, 3, 7 a potom zobrazení $f_1 = Id$, f_3 a f_7 jsou hledané izomorfismy. □

4.7. Rozhodněte, zda existuje izomorfismus f grupy $(\mathbf{Z}_{30}, +, -, 0)$ do sebe, aby platilo a) $f(1) = 8$ b) $f(1) = 17$, c) $f(7) = 3$, c) $f(7) = 17$.

Využijeme-li úvahu úlohy 4.5, vidíme, že v případě a) $f = f_8$ a b) $f = f_{17}$. Protože číslo 8 je s číslem 30 soudělné, zatímco číslo 17 je s číslem 30 nesoudělné izomorfimus splňující podmínku a) neexistuje, ovšem izomorfimus splňující podmínku b) existuje. Uvážíme-li, že i případné homomorfismy z variant c), d) jsou tvaru f_k, stačí, abychom vyřešili rovnice

$$\text{c) } f_x(7) = (x \cdot 7)\mathrm{mod}30 = 3 \text{ a } \text{ d)} f_y(7) = (y \cdot 7)\mathrm{mod}30 = 17.$$

Například pomocí Euklidova algoritmu zjistíme, že $x = 9$ a $y = 11$. Tedy vidíme, že $\mathrm{NSD}(9, 30) \neq 1$ $\mathrm{NSD}(11, 30) = 1$, proto izomorfimus splňující podmínku c) neexistuje, ovšem izomorfimus splňující podmínku d) existuje. □

4.8. Dokažte, že je pro každé přirozené n relace $\equiv (\bmod n)$ daná předpisem $a \equiv b(\bmod n) \Leftrightarrow n/a-b$ krongruence na grupě $(\mathbf{Z},+,-,0))$.

Nejprve nahlédneme, že je $\equiv (\bmod n)$ reflexivní $(n/a-a=0)$, symetrická $(n/a-b \Leftrightarrow n/b-a)$ a tranzitivní relace (jestliže $n/a-b$ a $n/b-c$, pak $n/a-c = (a-b)+(b-c)$), tedy se jedná o ekvivalenci. Dále si vezměme $a,b,c,d \in \mathbf{Z}$, pro které $a \equiv b(\bmod n)$ a $c \equiv d(\bmod n)$. Potom $n/a-b$ a $n/c-d$, proto $n/(a+c)-(b+d) = (a-b)+(c-d)$ stejně jako $n/((-a)-(-b))$, tedy $a+c \equiv b+d(\bmod n)$ a $-a \equiv -b(\bmod n)$. Protože zřejmě $0 \equiv 0(\bmod n)$, je $\equiv (\bmod n)$ kongruence algebry $(\mathbf{Z},+,-,0))$. □

13.12.

4.9. Spočítejte počet izomorfismů grupy $(\mathbf{Z},+,-,0))$ do sebe.

Stačí si opět uvědomit, že obraz generátoru grupy musí být opět generátor. Protože grupu $(\mathbf{Z},+,-,0)$ generejí pouze čísla 1 a -1, existují právě dva izomorfismy grupy $(\mathbf{Z},+,-,0))$ do sebe. Prvním z nich je identita a druhý přiřazuje číslu z právě číslo $-z$. To, že se jedná o izomorfismus už ověříme zcela přímočaře. □

4.10. Nechť $p=(135)(4798)(26)$ a $q=(18)(247693)$ jsou dvě permutace z S_9. Určete permutace $p \circ q$, $q \circ p$.

Přímo použitím definice snadno zjistíme hodnoty (skládáme zprava doleva):

$$p \circ q = (1495)(27)(368), \quad q \circ p = (129)(3587)(46).$$

□

4.11. Napište permutace $p=(13475)$ a $q=(19)(267)(3548)$ z S_9 jako součin transpozic.

Připomeňme, že transpozice je permutace, která vyměňuje právě dva prvky, tj. můžeme ji v redukovaném cyklickém zápisu zapsat ve tvaru (ab). Řešení úlohy pro permutaci p je zřejmé z Věty 6.9, konkrétně

$$(13475) = (15)\circ(17)\circ(14)\circ(13) = (13)\circ(34)\circ(47)\circ(75).$$

Přímo z definice cyklického zápisu vidíme, že $(19)(267)(3548) = (19)\circ(267)\circ(3548)$, tedy nejprve úlohu vyřešíme pro každý z cyklů (19), (267) a (3548) pomocí Věty 6.9 a poté nalezené transpozice složíme, tedy

$$(19)(267)(3548) = (19)\circ(267)\circ(3548) =$$

$$= (19)\circ(27)\circ(26)\circ(38)\circ(34)\circ(35) = (19)\circ(26)\circ(67)\circ(35)\circ(54)\circ(48).$$

□

4.12. Dokažte, že je grupa S_n generována množinou všech transpozic.

V předchozí úloze jsme si uvědomili, jak libovolnou permutaci získat jako složení nějaké posloupnosti transpozic. To znamená, že nejmenší podgrupa obsahující všechny transpozice je rovna celé grupě S_n. □

4.13. Spočítejte řád permutací $(12)(4578)(396), (12457)(396) \in S_9$.

Stačí využít Tvrzení 17.1 ze skript, které říká, že řád permutace je právě nejmenší společný násobek délek cyklů dané permutace, tedy řád prvku $(12)(4578)(396)$ je $\mathrm{NSN}(2,4,3) = 12$ a řád prvku $(12457)(396)$ je $\mathrm{NSN}(5,3) = 15$. □

4.14. Určete počet prvků podgrupy generované permutací $(12458)(7396) \in S_9$.

Uvážíme-li , že řád prvku je přesně roven velikosti cyklické podgrupy tím prvkem generované, vidíme, že $|\langle(12458)(7396)\rangle| = \mathrm{NSN}(5,4) = 20$. □

4.15. Obsahuje grupa S_{35} prvek řádu 31, 62, 155, 270?

Opět využijeme Tvrzení 17.1. Nejprve nahlédneme, že v grupě najdeme permutaci obsahující cyklus délky 31 a dále čtyři cykly délky 1 (například $(1\,2\,3\,\ldots\,30\,31)$), a dále, že najdeme rovněž permutaci obsahující cyklus délky 31, jeden cyklus délky 2 a dále dva cykly délky 1 (například $(1\ 2)(3\ 4\ 5\ \ldots\ 32\ 33)$), pak podle Tvrzení 17.1 jsou tyto permutace řádu 31 resp. 62. Naopak pro permutaci řádu $155 = 31 \cdot 5$ bychom podle Tvrzení 17.1 mezi permutacemi grupy S_{35} potřebovali buď cyklus dély 155 nebo dva nezávislé cykly, z nichž jeden má délku 31 a druhý 5. Protože $155 > 31$ i $31 + 5 > 35$, permutace řádu 155 v grupě S_{35} neexistuje. Konečně $270 = 27 \cdot 2 \cdot 5 = \mathrm{NSN}(27,2,5)$ a $27 + 2 + 5 \leq 35$, ze stejného důvodu jako výše vidíme, že například permutace $(1\ 2)(3\ 4\ 5\ 6\ 7)(8\ 9\ \ldots\ 34\ 35)$ je řádu 270. □

4.16. Spočítejte $((135)(4798)(26))^{-1}$ a $((18)(247693))^{-1}$ pro permutace z S_9.

Při hledání inverzních permutací si uvědomme, že stačí cykly (redukovaného) cyklického zápisu původních permutací „zrcadlově převrátit", tedy

$$((135)(4798)(26))^{-1} = (531)(8974)(62), \quad ((18)(247693))^{-1} = (81)(396742).$$

□

4.17. Nechť p a s jsou permutace z grupy S_n a nechť $p(a) = b$, kde $a, b \in \{1, \ldots, n\}$. Dokažte, že $[sps^{-1}](s(a)) = s(b)$.

Důkaz tvrzení je zcela přímočarý. Důležitým důsledkem je ovšem pozorování, že permutace p a sps^{-1} mají stejný počet stejných cyklů, neboť jsme právě dokázali, že

$$s \circ [\ldots(\ldots ab \ldots)\ldots] \circ s^{-1} = \ldots(\ldots s(a)s(b)\ldots)\ldots.$$

□

4.18. Mějme $p = (1346)(27)(589)$ a $q = (16)(29)(345)$ dvě permutace z grupy S_9. Spočítejte hodnoty pqp^{-1} a qpq^{-1}.

Postupujeme podle předchozího pozorování:

$$[(1346)(27)(589)] \circ [(16)(29)(345)] \circ [(1346)(27)(589)]^{-1} = (31)(75)(468)$$

a

$$[(16)(29)(345)] \circ [(1346)(27)(589)] \circ [(16)(29)(345)]^{-1} = (6451)(97)(382).$$

□

4.19. Mějme permutace $p_1 = (126)(37)(458)$ a $p_2 = (12)(345)(678)$ z grupy S_8. Rozhodněte, zda jsou permutace p_1 a p_2 konjugované, tj. zda existuje permutace $q \in S_8$ s vlastností $qp_1q^{-1} = p_2$ a případně takovou permutaci q najděte.

Využijeme opačný postup k postupu v předchozím příkladu. Obě permutace jsou stejného typu (což je zřejmě nutná podmínka, aby permutace q existovala). Seřaďme stejnými n-cykly pod sebe, například:

$$(126)(37)(458)$$
$$(345)(12)(678)$$

Zřejmě potom permutace $q = (13)(24657)(8)$ splňuje podmínku $qp_1q^{-1} = p_2$. □

20.12.

4.20. Dokažte, že je grupa S_n generována všemi permutacemi tvaru $(kk+1)$, kde $k < n$.

Díky 4.12, kde jsme ověřili, že $S_n = \langle\{(ab)|\ 0 \leq a < b \leq n, a, b \in \mathbf{N}\}\rangle$ stačí dokázat, že každou transpozici dostaneme složením vhodné posloupnosti transpozic tvaru $(kk+1)$. Vezmeme-li $a < b+1$, pak s využtím pozorování 4.17 snadno spočítáme, že

$$(ab) = (b-1b)(ab-1)(b-1b)^{-1} = (b-1b)(ab-1)(b-1b).$$

Indukčním argumentem tedy zjistíme, že $(ab) \in \langle\{(kk+1)|\ 0 \leq k < n\}\rangle$, a proto $\langle\{(kk+1)|\ 0 \leq k < n\}\rangle = S_n$. □

4.21. Dokažte, že je grupa S_n generována dvojicí permutací (12) a $(12\ldots n)$.

Podobně jako v 4.20 stačí díky 4.20 libovolnou transpozici tvaru $(kk+1)$ složit pomocí permutací (12) a $(12\ldots n)$. Opět snadno spočítáme, že

$$(kk+1) = (12\ldots n)^{k-1}(12)(12\ldots n)^{-k+1}.$$

čímž jsme dokázali, že $\langle(12),(12\ldots n)\rangle = \langle\{(kk+1)|\ 0 \leq k < n\}\rangle = S_n$. □

4.22. Dokažte, že je grupa sudých permutací A_n generována množinou všech trojcyklů.

Vezměme libovolnou sudou permutaci σ. Díky 4.12 víme, že existuje posloupnost transpozic $T_1, \ldots, T_{2k}$ sudé délky, pro níž

$$\sigma = T_1 \circ T_2 \cdots \circ T_{2k} = \sigma = (T_1 \circ T_2) \circ (T_3 \circ T_4) \cdots \circ (T_{2k-1} \circ T_{2k}).$$

Tedy stačí nahlédnout, že každé složení dvojice transpozic $T_{2i-1} \circ T_{2i}$ dostaneme jako složení trojcyklů. Proveďme tedy diskusi. Jakmile $T_{2i-1} = T_{2i}$, pak $T_{2i-1} \circ T_{2i} = Id$ a tvrzení zřejmě platí. Jestliže $T_{2i-1} = (ab)$ a $T_{2i} = (bc)$ jsou různé závislé transpozice, pak $T_{2i-1} \circ T_{2i} = (abc)$. Konečně, pokud $T_{2i-1} = (ab)$ a $T_{2i} = (cd)$ jsou nezávislé transpozice, potom snadno spočítáme, že $T_{2i-1} \circ T_{2i} = (abc) \circ (bcd)$. □

4.23. Popište množinu generátorů cyklické grupy $(\mathbf{Z}_n, +, -, 0)$.

Uvědomme si, že číslo k je generátorem právě tehdy, když podgrupa $\langle k \rangle$ obsahuje prvek 1 a to nastává právě tehdy, když je $\mathrm{NSD}(k, n) = 1$. □

4.24. Určete počet generátorů cyklické grupy $(\mathbf{Z}_{50}, +, -, 0)$.

Podle úvahy z 4.23 potřebujeme určit hodnotu Eulerovy funkce na prvku 50. Prvočíselný rozklad čísla 50 je $5^2 \cdot 2$ a využijeme-li tvrzení 3.9 ze skript dostáváme $\varphi(50) = (5-1) \cdot 5^1 \cdot (2-1) = 20$. □

4.25. Určete počet generátorů cyklické grupy řádu 81.

Uvážíme-li, že cyklická grupa řádu 81 je izomorfní grupě $(\mathbf{Z}_{81}, +, -, 0)$, postujpujeme stejně jako v předchozím příkladu: prvočíelný rozklad čísla 81 je 3^4, tedy počet generátorů cyklické grupy řádu 81 je $\varphi(81) = (3-1) \cdot 3^3 = 54$. □

4.26. Nechť G je konečná cyklická grupa, $|G| = n$, a nechť k dělí n. Ukažte, že existuje právě jedna podgrupa grupy G, která má k prvků.

K důkazu využijeme charakterizace cyklických grup, díky němuž stačí tvrzení dokázat pro (izomorfní) grupu $(\mathbf{Z}_n, +, -, 0)$ a následně budeme uvažovat stejně jako v úloze 4.1. Jestliže $k = 1$, je tvrzení triviální, předpokládejme tedy, že $k > 1$, a položme $a = \frac{n}{k}$. Potom snadno nahlédneme, že $\langle a \rangle = \{0, a, 2a, \ldots, (k-1)a\}$, tudíž $|\langle a \rangle| = k$. Mějme nyní nějakou podgrupu H řádu k grupy $\mathbf{Z}_n$. Podle Lagrangeovy věty řád grupy $\langle h \rangle$ dělí k pro každý prvek $h \in H$, proto $(k \cdot h) \mathrm{mod} n = 0$. Tudíž $k \cdot h = c \cdot n$ pro vhodné celé číslo c, tedy $h = \frac{c \cdot n}{k} = c \cdot a$. Tím jsme ověřili, že H je částí podgrupy $\langle a \rangle$. Protože se ovšem jedná o dvě konečné stejně velké množiny dostáváme, že $H = \langle a \rangle$, čímž jsme ověřili jednoznačnost volby. □

4.27. Kolik podgrup obsahuje cyklická grupa řádu 98?

Využijeme úvahu úlohy 4.26, budeme tedy postupovat jako v příkladu 4.1: každému děliteli řádu cyklické grupy odpovídá právě jedna její podgrupa. Potřebujeme tedy jen spočítat dělitele čísla 98, kterých je 6 (tj. $1, 2, 7, 14, 49, 98$). □

4.28. Kolik podgrup obsahuje cyklická grupa řádu 1000?

Opět uvažujeme jako v 4.26 a vidíme, že podgrup obsahuje cyklická grupa řádu 1000 právě tolik, kolik je dělitelů čísla $1000 = 2^3 \cdot 5^3$, množinu dělitelů přitom tvoří $\{2^i \cdot 5^j \mid (i, j) \in \mathbf{Z}_4 \times \mathbf{Z}_4\}$, tedy je jich $|\mathbf{Z}_4 \times \mathbf{Z}_4| = 4^2 = 16$. □

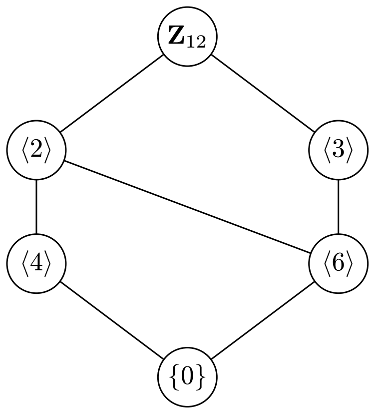
4.29. Kolik obsahuje cyklická grupa o tisíci prvcích prvků řádu 100?

I tentokrát stačí, abychom se zabývali cyklickou grupou $(\mathbf{Z}_{1000}, +, -, 0)$. Připomeňme, že prvek g grupy je řádu k právě tehdy, když $|\langle g \rangle| = k$. My ovšem víme, že existuje jediná podgrupa grupy $(\mathbf{Z}_{1000}, +, -, 0)$ řádu 100 (konkrétně se jedná o podgrupu $\langle 10 \rangle$), navíc se nutně jedná o cyklickou grupu, tedy potřebujeme spočítat její generátory. Postupujeme-li nyní stejmě jako v 4.25, vidíme, že generátorů pogrupy $\langle 10 \rangle$, tedy prvků řádu 100 v grupě $(\mathbf{Z}_{1000}, +, -, 0)$ je právě $\varphi(100) = (5-1) \cdot 5^1 \cdot (2 - 1 \cdot 2^1) = 40$. □

3.1.

4.30. Najděte Hasseův diagram svazu všech podgrup grupy $(\mathbf{Z}_{12}, +, -, 0)$.

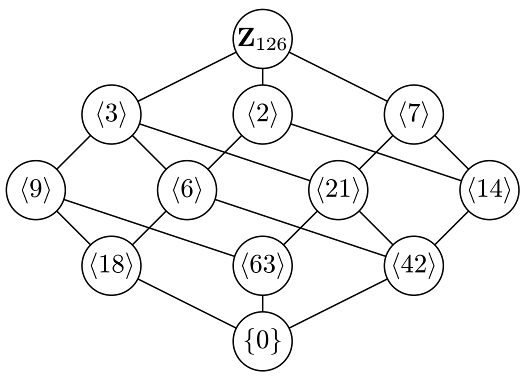
Připomeňme si, že podle Lagrangeovy věty existují v $(\mathbf{Z}_{12}, +, -, 0)$ jen podgrupy řádu, který dělí číslo 12, přičemž $12 = 2^2 \cdot 3$. Navíc podle Věty 5.11 v cyklické grupě pro každé k, které dělí řád grupy tj. 12, existuje právě jedna podgrupa řádu k, jež je generována právě prvkem $\frac{12}{k}$. Konečně si zbývá uvědomit, že každá podgrupa i faktorová grupa cyklické grupy je cyklická, proto jsou dvě podgrupy H_1 a H_2 spojeny v Hasseově diagramu hranou, právě když $|H_1|/|H_2|$ a $\frac{|H_2|}{|H_1|}$ je prvočíslo (to znamená, že mezi H_1 a H_2 neleží žádná další podgrupa). Uvědomíme-li si, že $H_1 = \langle k_1 \rangle = k_1\mathbf{Z}_{12}$ a $H_2 = \langle k_2 \rangle = k_2\mathbf{Z}_{12}$, pak H_1 a H_2 jsou spojeny hranou, přičemž H_1 leží pod H_2, právě když k_2 dělí k_1 a $\frac{k_1}{k_2}$ je prvočíslo (v našem případě tedy 2 nebo 3). Víme, že podgrupy grupy $\mathbf{Z}_{12}(+,-,0)$ jsou generovány prvky 1, 2, 3, 4, 6 a 0. Zbývá mezi příslušnými podgrupami nakreslit hrany a uspořádat je do Hasseova diagramu:



□

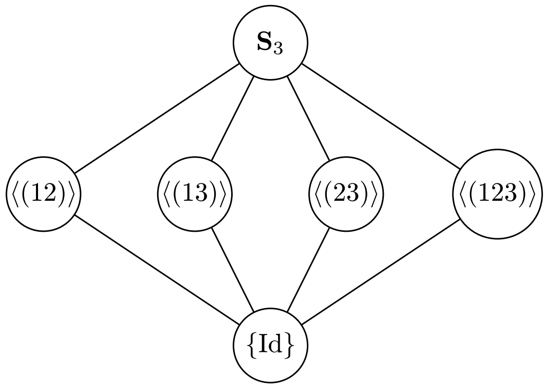
4.31. Najděte Hasseův diagram svazu všech kongruencí na cyklické grupě řádu 126.

Poznamenejme, že cyklická grupa řádu 126 je izomorfní grupě $(\mathbf{Z}_{126}, +, -, 0)$, tedy stačí vyšetřit všechny podgrupy $(\mathbf{Z}_{126}, +, -, 0)$. Postupujeme stejně jako v úloze 4.30 a úloha se redukuje na nalezení dělitelů čísla 126. Dělitelé 126 jsou 1, 2, 3, 6, 7, 9, 14, 18, 21, 42, 63, 126. Zbývá vytvořit Hasseův diagram:



4.32. Najděte Hasseův diagram svazu všech podgrup grupy permutací $(S_3, \circ, ^{-1}, \mathrm{Id})$.

Nejprve najdeme všechny podgrupy grupy $(S_3, \circ, ^{-1}, \mathrm{Id})$. Zřejmě S_3 i $\{\mathrm{Id}\}$ jsou podgrupy. Uvědomme si, že velikost libovolné další podgrupy není 1 ani 6, ale podle Lagrangeovy věty číslo 6 dělí. To znamená, že zbývá, abychom vyšetřili podgrupy velikosti 2 a 3. Ty jsou nutně cyklické, tedy si stačí všimnout, které permutace jsou řádu 2 a které jsou řádu 3. Vše namalujeme do Hasseova diagramu:

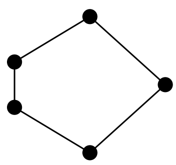


□

Další úlohy

(1) Dokažte, že svaz všech podmnožin $P(X)$ neprázdné množiny X je spolu s inkluzí modulární.

(2) Ověřte, že je svaz modulární právě tehdy, když jako podsvaz obsahuje svaz s Hasseovým diagramem



item Popište všechny grupy, které obsahují právě dvě podgrupy.

(3) Kolik existuje izomorfismů cyklické grupy řádu 44 do sebe?

(4) Kolik existuje izomorfismů grupy prvočíselného řádu p do sebe?

(5) Existuje izomorfismus $f : \mathbf{Z}_{10} \to \mathbf{Z}_{10}$ grupy $(\mathbf{Z}_{10}, +, -, 0)$ takový, že a) $f(1) = 6$, b) $f(1) = 9$, c) $f(2) = 6$, d) $f(2) = 9$, e) $f(9) = 7$?

(6) Rozhodněte, zda jsou izomorfní grupy $(\mathbf{Z}_4, +, -, 0)$ a $(\mathbf{Z}_2 \times \mathbf{Z}_2, +, -, 0)$.

(7) Rozhodněte, zda jsou izomorfní grupy $(\mathbf{Z}_6, +, -, 0)$ a $(\mathbf{Z}_2 \times \mathbf{Z}_3, +, -, 0)$.

(8) Rozhodněte, zda jsou izomorfní grupy $(\mathbf{S}_3, \circ, ^{-1}, Id)$ a $(\mathbf{Z}_2 \times \mathbf{Z}_3, +, -, 0)$.

(9) Rozhodněte, zda je grupa $(\mathbf{Z}_{20} \times \mathbf{Z}_{30}, +, -, 0)$ cyklická.

(10) Rozhodněte, zda je grupa $(\mathbf{Z}_{21} \times \mathbf{Z}_{31}, +, -, 0)$ cyklická.

(11) Rozhodněte, zda jsou permutace p_1 a p_2 konjugované v S_9, jestliže
a) $p_1 = (13)(259)$ a $p_2 = (247)(58)$,
b) $p_1 = (13)(259)$ a $p_2 = (13)(259)(48)$

(12) Rozhodněte, zda jsou permutace $(13)(259)$ a $(247)(58)$ konjugované v A_9.

(13) Spočítejte řád permutací $(357498)(126), (357498)(12), (35749)(126) \in S_9$.
(14) Obsahuje grupa S_{100} prvek řádu 80, 110, 111, 113, 5!, 6!, 7!?
(15) Kolik obsahuje cyklická grupa o 333 prvcích prvků řádu 3, 9, 33, 50, 111?
(16) Dokažte, že pro každé přirozené n existuje nekonečně neizomorfních konečných grup obsahujících právě n podgrup. Najděte Hasseův diagram svazu všech kongruencí na cyklické grupě řádu 1000, 1001, 1002.
(17) Najděte Hasseův diagram svazu všech podgrup grupy permutací $(S_4, \circ, ^{-1}, \mathrm{Id})$.