Bevezetés a számításelméletbe II.

13. gyakorlat, 2014. május 6. IB 134 Összeállította: Fleiner Tamás (fleiner@cs.bme.hu)

Tudnivalók

Def: A D_n *diédercsoport* elemei a szab n-szöget fixen hagyó egybevágóságok, művelet a $\circ$ (fvkompozíció).

Állítás: D_n-nek $2n$ eleme van: n forgatás (a helybenhagyást is beleértve) és n tükrözés.

Def: Az *n-edrendű szimmetrikus csoport* alaphalmaza az $\{1, 2, \ldots, n\}$ számok S_n permutációinak, azaz az $f : [n] \to [n]$ kölcsönösen egyértelmű leképezések halmaza. Az S_n szimmetrikus csoport művelete a $\circ$ kompozíció, azaz $(\sigma \circ \pi)(x) := \sigma(\pi(x))$. G *permutációcsoport*, ha $G \leq S_n$.

Példa: Ha például $\pi = \begin{array}{c|c|c|c|c} 1 & 2 & 3 & 4 & 5 \\ \hline 2 & 4 & 3 & 1 & 5 \end{array}$ és $\sigma = \begin{array}{c|c|c|c|c} 1 & 2 & 3 & 4 & 5 \\ \hline 3 & 2 & 1 & 5 & 4 \end{array}$ akkor $\pi \circ \sigma = \begin{array}{c|c|c|c|c} 1 & 2 & 3 & 4 & 5 \\ \hline 3 & 4 & 2 & 5 & 1 \end{array}$ adódik.

Def: Az $(i_1, i_2, \ldots, i_k)$ a $\sigma \in S_n$ permutáció *ciklusa*, ha $\sigma(i_j) = i_{j+1}$, ahol $i_{k+1} := i_1$. Az $(i_1, i_2, \ldots, i_k)$ *ciklus* olyan permutáció, melynek $(i_1, i_2, \ldots, i_k)$ ciklusa, az összes további elem fix pontja. Két ciklus *diszjunkt*, ha a benne szereplő elemek halmaza diszjunk. *Transzpozíció* a kételemű ciklus. Ha $\mathcal{T}$ az S_n transzpozícióinak egy halmaza, akkor a $\mathcal{T}$ *gráfja* $G_{\mathcal{T}} = ([n], \{ij : (i, j) \in \mathcal{T}\}$. **Megfigyelés:** $\mathcal{T}$ generálja S_n-t $\iff$ $G_{\mathcal{T}}$ öf.

Tétel: Minden permutáció előáll diszjunkt ciklusok szorzataként.

Megjegyzés: A fenti példában szereplő permutációk ciklusok szorzataként történő lehetséges felírása pl $\pi = (124)$, $\sigma = (13)(45)$ és $\pi \circ \sigma = (13245)$, ahol az egyes ciklusok a zárójeleken belül vannak, a triviális ciklusokat (fix pontokat) nem írjuk ki.

Megfigyelés: Az S_n egységeleme az identikus permutáció, amire $\pi(i) = i \ \forall i \in \{1, 2, \ldots, n\}$. Tetszőleges π permutáció inverze S_n-ben az inverz leképezés, amire $\pi^{-1}(j) = i$, ha $\pi(i) = j$.

Cayley tétel: Minden véges csoport alkalmas permutációcsoporttal izomorf.

Def: A $\langle R, \{+, \cdot\}\rangle$ algebrai struktúra *gyűrű*, ha $\langle R, +\rangle$ Abel-csoport, $\langle R, \cdot\rangle$ félcsoport, továbbá teljesülnek a *disztributív azonosságok*: $a(b + c) = ab + ac$ ill. $(a + b)c = ac + bc$ $(\forall a, b, c \in R)$. Ha röviden csak R gyűrűt mondunk, akkor konvenció szerint R két művelete $+$ és $\cdot$ a fentiek szerint.

Az R gyűrű *kommutatív*, ha a szorzás kommutatív. Az R gyűrű összeadásának egységelemét *nullelemnek* nevezzük, és 0-val jelöljük. Az R gyűrűben az $a \in R$ elem inverzét az összeadásra $-a$ jelöli. Az R gyűrű *egységelemes*, ha a szorzásműveletnek van egysége, melyet (ha van) 1 jelöl.

Megfigyelés: Ha R gyűrű, és $a, b \in R$, akkor $0a = a0 = 0$ ill. $(-a)b = -ab = a(-b)$.

Példa: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ gyűrűk. $\mathbb{N}$ nem gyűrű, $n\mathbb{Z}, \mathbb{Z}_m$ gyűrű. Tetszőleges H halmazra $\langle \mathcal{P}(H), \{\triangledown, \cap\}\rangle$ a H halmaz *Boole gyűrű*je, ahol $\triangledown$ a szimmetrikus különbséget jelöli: $A \triangledown B := (A \setminus B) \cup (B \setminus A)$. Itt a nullelem az $\emptyset$, az egység pedig a H.

Def: Az R gyűrűben a $a \neq 0$ elem *nullosztó*, ha létezik olyan $0 \neq b \in R$, melyre $ab = 0$. Az R gyűrű *nullosztómentes*, ha R-ben nincs nullosztó. Az R gyűrű *integritási tartomány*, ha kommutatív és nullosztómentes.

Megfigyelés: Ha $n \in \mathbb{Z}$, akkor $n\mathbb{Z}$ a $\mathbb{Z}$ részgyűrűje. A $\mathbb{Z}$ gyűrű minden részgyűrűje $n\mathbb{Z}$ alakú.

Def: A T gyűrű *ferdetest*, ha $\langle T \setminus \{0\}, \cdot\rangle$ csoport. Ha a szorzás kommutatív, akkor T *test*.

Példa: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ testek. Test még a $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in Q\}$ is.

Feladatok

1. Írjuk fel D_{2n} szorzótábláját!
2. Mutassuk meg, hogy ha G csoport és $a, b \in G$, akkor ab és ba rendjei megegyeznek: $o_G(ab) = o_G(ba)$.
3. Az S_n szimmetrikus csoportnak részcsoportját alkotják-e a páros inverziószámú permutációk?
4. Igazoljuk, hogy S_n-et generálják az $(1, 2)$ és $(1, 2, \ldots, n)$ permutációk.
5. Legkevesebb hány transzpozíció szükséges ahhoz, hogy a teljes S_n csoportot generálja?
6. Hogyan lehet meghatározni egy π permutáció rendjét a a π ciklusaiból?
7. Mutassunk példát arra, hogy két másodrendű permutáció kompozíciójának a rendje 7.
8. Gyűrűt alkotnak-e az invertálható $n \times n$ méretű valós mátrixok? Hát $\mathbb{Z}_m^*$ gyűrű-e vajon?
9. Tegyük fel, hogy R gyűrű és $\langle R, \cdot\rangle$ csoport. Bizonyítsuk be, hogy R egyelemű.
10. Mik a $\mathbb{Z}_m$ gyűrű nullosztói? Gyűrűt alkot-e $\mathbb{Z}^{n\times m}$? Ha igen, mik a nullosztói?
11. Tegyük fel, hogy az R gyűrű nullosztómentes, és $r^2 = r$ teljesül a gyűrű egy elemére. Bizonyítsuk be, hogy $r = 0$ vagy $r = 1$. Mutassunk példát olyan nem nullosztómentes gyűrűre, és annak egy r elemére $(1 \neq r \neq 0)$, amire $r^2 = r$ teljesül.
12. Testet alkot-e a $\{p + q\sqrt[3]{2} : p, q \in \mathbb{Q}\}$ halmaz a szokásos szorzásra és összeadásra?
13. Mutassuk meg, hogy ha T test, $a, x \in T$ és $a + a = 0$, akkor $x + x = 0$.
14. Határozzuk meg a kvaterniótestben az $x = 2 - j$ ill. az $y = 2 - i + j - k$ elemek inverzeit. Számítsuk ki a $\mathbb{Q}(\sqrt{2})$ testben a $(2 + 5\sqrt{2}) \cdot (3 - 2\sqrt{2})^{-1} = \frac{2+5\sqrt{2}}{3-2\sqrt{2}}$ elemet.
15. Bizonyítsuk be, hogy $\{a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} : a, b, c, d \in \mathbb{Q}\}$ test és egyúttal 2-dimenziós vektortér a $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ test felett!
16. Ha R gyűrű, és $\mathbb{Z} \cap R = \emptyset$, akkor gyűrűt alkot e a $\{(r, z) : r \in R, z \in \mathbb{Z}\}$ halmaz, ahol $(r, z) + (r', z') := (r + r', z + z')$ illetve $(r, z) \cdot (r', z') := (r \cdot r' + z \cdot r' + z' \cdot r, z \cdot z')$ definiálják a műveleteket, a $nr := r + r + \ldots + r$ $[n]$-szer konvencióval?