Bevezetés a számításelméletbe II.

12. gyakorlat, 2014. április 29. IB 134

Összeállította: Fleiner Tamás (fleiner@cs.bme.hu)

Tudnivalók

Def: $\langle G, \cdot \rangle$ *csoport*, ha (1) G félcsoport, (2) létezik $e \in G$ egység, és (3) minden elemnek létezik inverze. A G csoport *Abel-csoport*, ha a $\cdot$ csoportművelet kommutatív. A $(G, \cdot)$ csoport *rendje* $|G|$.

Példa: Az $\mathbb{R}$ az összeadásra Abel-csoportot alkot. Hasonlóan, $\mathbb{Q}\setminus\{0\}$ (vagy $\mathbb{R}\setminus\{0\}$) is a szorzásra. A modulo n maradékosztályok $\mathbb{Z}_n$ halmaza Abel-csoport az összeadásra, az n-hez relatív prím modulo n maradékosztályok Z_n^* halmaza pedig a szorzásra.

Megfigyelés: Csoport műveleti táblájának minden sorában és minden oszlopában szerepel minden elem.

Konvenció: A $\langle G, \cdot \rangle$ csoportot, ha világos, hogy a művelet a $\cdot$, akkor G-vel jelöljük. Ebben az esetben értelmezzük a csoportelemek hatványait is: g^i jelöli a $g \cdot g \cdot \ldots \cdot g$ elemet, ahol g-t i-szer műveljük össze önmagával. A negatív kitevőket is értelmezhetjük: $g^{-i} := (g^{-1})^i$, sőt, $g^0 = e$ az egységelem.

Def: A $\langle G_1, \cdot \rangle$) és $\langle G_2, \star \rangle$ csoportok *izomorfak* ($G_1 \cong G_2$), ha van közöttük művelettartó bijekció, azaz $\exists \varphi : G_1 \to G_2$ bijekció úgy, hogy tetszőleges $u, v \in G_1$-re $\varphi(u \cdot v) = \varphi(u) \star \varphi(v)$.

Def: H a G csoport *részcsoportja* (jele $H \leq G$), ha $H \subseteq G$ és H csoport a G csoportműveletére.

Állítás: Ha $\langle G, \star \rangle$ csoport és $H \subseteq G$, akkor $(H \leq G) \iff (H$ zárt a $\star$ műveletre és az inverzképzésre).

Állítás: A G csoport tetszőlegesen sok részcsoportjának metszete részcsoport.

Def: A $H \subseteq G$ *által generált* $\langle H \rangle$ *részcsoport* a legszűkebb, H-t tartalmazó részcsoportja G-nek. Azaz $\langle H \rangle$ a G csoport H tartalmazó részcsoportjainak metszete.

Def: A G csoport *ciklikus*, ha egy elem generálja, azaz, ha van olyan $g \in G$, amire $\langle g \rangle = G$.

Megfigyelés: Ha g generálja G-t, akkor G minden eleme g^i alakú ($i \in \mathbb{Z}$), a művelet pedig $g^i \cdot g^j = g^{i+j}$.

Állítás: A $\langle \mathbb{Z}, + \rangle$ és $\langle \mathbb{Z}_n, + \rangle$ csoportok ciklikusak. Tetsz. ciklikus csoport izomorf ezen csoportok egyikével.

Állítás: Ciklikus csoport minden részcsoportja ciklikus.

Def: C_n jelöli (a $\langle \mathbb{Z}_n, + \rangle$ csoporttal izomorf) n elemű ciklikus csoport.

Def: Az $g \in G$ csoportelem $o_G(g)$-vel jelölt *rendje* a g által generált részcsoport rendje.

Állítás: (Szokásos def) $o_G(g)$ az a legkisebb pozitív i egész, amire $g^i = e$. Ha nincs ilyen i, akkor ∞.

Def: Ha G csoport és $H, K \subseteq G$, akkor $HK := \{hk : h \in H, k \in K\}$ jelöli a H és K *komplexusszorzatát*. Konvenció: $g \in G$ esetén $Hg := H\{g\}$ és $gH := \{g\}H$.

Def: Ha $H \leq G$ és $g \in G$, akkor gH ill. Hg a H *részcsoport* g *szerinti bal- ill jobboldali mellékosztálya*, g pedig a mellékosztály *reprezentánsa*.

Lagrange tétel: Ha G véges csoport és $H \leq G$ akkor $|H| \mid |G|$.

Köv.: $o_G(g) \mid |G|$ minden $g \in G$-re. $|G|$ prím $\Rightarrow G$ ciklikus.

Feladatok

1. Hány olyan g eleme van a C_n ciklikus csoportnak, amire $\langle g \rangle = C_n$? (V '99)
2. A C_n csoport összes elemének négyzetét összeszorozzuk. Mit kapunk? Hát Abel csoportra? (V '99)
3. Állapítsuk meg, hogy izomorf-e a mod 4 maradékosztályok additív csoportja (azaz $\langle \mathbb{Z}_4, + \rangle$) a mod 8 redukált maradékosztályok multiplikatív csoportjával (azaz a $\langle \mathbb{Z}_8^*, \cdot \rangle$ csoporttal). (ZH '02)
4. Hány különböző részcsoportja van a C_{2002} ciklikus csoportnak? (V '00)
5. Bb: ha a G csoportnak nincs valódi részcsoportja és $|G| \geq 2$, akkor G prímrendű ciklikus csoport. (ZH '02)
6. Legyen $G = \{1, 5, 7, 11\}$, a művelet pedig a mod 12 szorzás. Csoport-e G? Ciklikus-e G? (V '01)
7. Bizonyítsuk be, hogy ha G csoport, $H, K \leq G$ és $HK = KH$, akkor $HK \leq G$. (V '01)
8. Mutassuk meg, hogy ha G csoport, $H, K \leq G$ és $H \cup K \leq G$, akkor $H \subseteq K$ vagy $K \subseteq H$. (V '01)
9. Tegyük fel, hogy G csoport, $H \leq G$ és $A \subseteq G$. Döntsük el minden egyes alábbi állításról, hogy biztosan igaz, biztosan hamis vagy lehet igaz és hamis is. (1) $|gA| = |A|$, (2) $hH = H$, (3) $ghH = gH$, (4) $hgH = gH$. (Ha biztosan igaz vagy biztosan hamis az állítás, bizonyítsuk ezt be, ha lehet igaz és hamis is adjunk ellenpéldát, egyébként adjunk példát arra is, hogy teljesül, és arra is, hogy nem.)
10. Határozzuk meg az alább megadott G csoportok H részcsoportjainak bal- és jobboldali mellékosztályait. (1) $G = \mathbb{Z}_{12}, H = \{0, 4, 8\}$, (2) $G = \langle \mathbb{R}^5, + \rangle, H = \{(x, y, z, 0, 0) : x, y, z \in \mathbb{R}\}$, (3) $G = \langle \mathbb{R} \setminus \{0\}, \cdot \rangle, H = \{\pm 1\}$, (4) $G = S_3, H = \{id, (12)\}$, (5) $\langle \mathbb{Z}, + \rangle, H = 2011\mathbb{Z}$.

Bevezetés a számításelméletbe II.

12. gyakorlat, 2014. április 29. IB 134

Összeállította: Fleiner Tamás (fleiner@cs.bme.hu)

Tudnivalók

Def: $\langle G, \cdot \rangle$ *csoport*, ha (1) G félcsoport, (2) létezik $e \in G$ egység, és (3) minden elemnek létezik inverze. A G csoport *Abel-csoport*, ha a $\cdot$ csoportművelet kommutatív. A $(G, \cdot)$ csoport *rendje* $|G|$.

Példa: Az $\mathbb{R}$ az összeadásra Abel-csoportot alkot. Hasonlóan, $\mathbb{Q}\setminus\{0\}$ (vagy $\mathbb{R}\setminus\{0\}$) is a szorzásra. A modulo n maradékosztályok $\mathbb{Z}_n$ halmaza Abel-csoport az összeadásra, az n-hez relatív prím modulo n maradékosztályok Z_n^* halmaza pedig a szorzásra.

Megfigyelés: Csoport műveleti táblájának minden sorában és minden oszlopában szerepel minden elem.

Konvenció: A $\langle G, \cdot \rangle$ csoportot, ha világos, hogy a művelet a $\cdot$, akkor G-vel jelöljük. Ebben az esetben értelmezzük a csoportelemek hatványait is: g^i jelöli a $g \cdot g \cdot \ldots \cdot g$ elemet, ahol g-t i-szer műveljük össze önmagával. A negatív kitevőket is értelmezhetjük: $g^{-i} := (g^{-1})^i$, sőt, $g^0 = e$ az egységelem.

Def: A $\langle G_1, \cdot \rangle$) és $\langle G_2, \star \rangle$ csoportok *izomorfak* ($G_1 \cong G_2$), ha van közöttük művelettartó bijekció, azaz $\exists \varphi : G_1 \to G_2$ bijekció úgy, hogy tetszőleges $u, v \in G_1$-re $\varphi(u \cdot v) = \varphi(u) \star \varphi(v)$.

Def: H a G csoport *részcsoportja* (jele $H \leq G$), ha $H \subseteq G$ és H csoport a G csoportműveletére.

Állítás: Ha $\langle G, \star \rangle$ csoport és $H \subseteq G$, akkor $(H \leq G) \iff (H$ zárt a $\star$ műveletre és az inverzképzésre).

Állítás: A G csoport tetszőlegesen sok részcsoportjának metszete részcsoport.

Def: A $H \subseteq G$ *által generált* $\langle H \rangle$ *részcsoport* a legszűkebb, H-t tartalmazó részcsoportja G-nek. Azaz $\langle H \rangle$ a G csoport H tartalmazó részcsoportjainak metszete.

Def: A G csoport *ciklikus*, ha egy elem generálja, azaz, ha van olyan $g \in G$, amire $\langle g \rangle = G$.

Megfigyelés: Ha g generálja G-t, akkor G minden eleme g^i alakú ($i \in \mathbb{Z}$), a művelet pedig $g^i \cdot g^j = g^{i+j}$.

Állítás: A $\langle \mathbb{Z}, + \rangle$ és $\langle \mathbb{Z}_n, + \rangle$ csoportok ciklikusak. Tetsz. ciklikus csoport izomorf ezen csoportok egyikével.

Állítás: Ciklikus csoport minden részcsoportja ciklikus.

Def: C_n jelöli (a $\langle \mathbb{Z}_n, + \rangle$ csoporttal izomorf) n elemű ciklikus csoport.

Def: Az $g \in G$ csoportelem $o_G(g)$-vel jelölt *rendje* a g által generált részcsoport rendje.

Állítás: (Szokásos def) $o_G(g)$ az a legkisebb pozitív i egész, amire $g^i = e$. Ha nincs ilyen i, akkor ∞.

Def: Ha G csoport és $H, K \subseteq G$, akkor $HK := \{hk : h \in H, k \in K\}$ jelöli a H és K *komplexusszorzatát*. Konvenció: $g \in G$ esetén $Hg := H\{g\}$ és $gH := \{g\}H$.

Def: Ha $H \leq G$ és $g \in G$, akkor gH ill. Hg a H *részcsoport* g *szerinti bal- ill jobboldali mellékosztálya*, g pedig a mellékosztály *reprezentánsa*.

Lagrange tétel: Ha G véges csoport és $H \leq G$ akkor $|H| \mid |G|$.

Köv.: $o_G(g) \mid |G|$ minden $g \in G$-re. $|G|$ prím $\Rightarrow G$ ciklikus.

Feladatok

1. Hány olyan g eleme van a C_n ciklikus csoportnak, amire $\langle g \rangle = C_n$? (V '99)
2. A C_n csoport összes elemének négyzetét összeszorozzuk. Mit kapunk? Hát Abel csoportra? (V '99)
3. Állapítsuk meg, hogy izomorf-e a mod 4 maradékosztályok additív csoportja (azaz $\langle \mathbb{Z}_4, + \rangle$) a mod 8 redukált maradékosztályok multiplikatív csoportjával (azaz a $\langle \mathbb{Z}_8^*, \cdot \rangle$ csoporttal). (ZH '02)
4. Hány különböző részcsoportja van a C_{2002} ciklikus csoportnak? (V '00)
5. Bb: ha a G csoportnak nincs valódi részcsoportja és $|G| \geq 2$, akkor G prímrendű ciklikus csoport. (ZH '02)
6. Legyen $G = \{1, 5, 7, 11\}$, a művelet pedig a mod 12 szorzás. Csoport-e G? Ciklikus-e G? (V '01)
7. Bizonyítsuk be, hogy ha G csoport, $H, K \leq G$ és $HK = KH$, akkor $HK \leq G$. (V '01)
8. Mutassuk meg, hogy ha G csoport, $H, K \leq G$ és $H \cup K \leq G$, akkor $H \subseteq K$ vagy $K \subseteq H$. (V '01)
9. Tegyük fel, hogy G csoport, $H \leq G$ és $A \subseteq G$. Döntsük el minden egyes alábbi állításról, hogy biztosan igaz, biztosan hamis vagy lehet igaz és hamis is. (1) $|gA| = |A|$, (2) $hH = H$, (3) $ghH = gH$, (4) $hgH = gH$. (Ha biztosan igaz vagy biztosan hamis az állítás, bizonyítsuk ezt be, ha lehet igaz és hamis is adjunk ellenpéldát, egyébként adjunk példát arra is, hogy teljesül, és arra is, hogy nem.)
10. Határozzuk meg az alább megadott G csoportok H részcsoportjainak bal- és jobboldali mellékosztályait. (1) $G = \mathbb{Z}_{12}, H = \{0, 4, 8\}$, (2) $G = \langle \mathbb{R}^5, + \rangle, H = \{(x, y, z, 0, 0) : x, y, z \in \mathbb{R}\}$, (3) $G = \langle \mathbb{R} \setminus \{0\}, \cdot \rangle, H = \{\pm 1\}$, (4) $G = S_3, H = \{id, (12)\}$, (5) $\langle \mathbb{Z}, + \rangle, H = 2011\mathbb{Z}$.