מטלה מס' 4 אלגברה מודרנית
להגשה: עד יום ג' 25 בדצמבר
פתרונות

1. (40 נק') יהי a יוצר של G ויהי $H \neq \{\mathbf{e}\}$ תת חבורה של G. לכל איבר h כאשר $e \neq h \in H \subseteq G = \langle a \rangle$ ניתן לכתוב $h = a^t$ כאשר $0 \neq t \in \mathbb{Z}$. יהי $S = \{k \in \mathbb{N} \mid a^k \in H\}$. מכיוון ש $H \neq \{\mathbf{e}\}$, קיים $0 \neq k \in \mathbb{Z}$ כך ש $a^k \in H$. אם $k < 0$ אז גם ההופכי $a^{-k} \in H$. נובע ש S אינה ריקה ולכן (לפי עקרון הסדר הטוב) קיים איבר מינימלי $k_0 \in S$. מכיוון ש H סגורה ביחס לפעולה והיא מכילה את ההופכי של כל איבר, נובע ש $\langle a^{k_0} \rangle \subseteq H$. יהי $e \neq h \in H$. ניתן לכתוב $h = a^m$ כאשר $m \in \mathbb{Z}$. לפי הלמה של אוקלידס קיימים $q, r \in \mathbb{Z}$ כך ש $m = qk_0 + r$ ו $0 \leq r \leq k_0 - 1$. נובע ש $a^m a^{-qk_0} \in H \Longleftarrow a^r \in H$. אם $r \neq 0$, אז קיבלנו ש $r \in S$ כאשר $r < k_0$. זאת סתירה לכך ש k_0 האיבר המינימלי של S. נובע ש $r = 0$. קיבלנו ש $h = a^m = a^{qk_0} \in \langle a^{k_0} \rangle$. נובע ש $H \subseteq \langle a^{k_0} \rangle$ לכן $H = \langle a^{k_0} \rangle$ ו H ציקלית. נציין שהאיברים a^{sk_0}, a^{tk_0} שונים לכל $s \neq t$ לפי טענה שהוכחנו בקורס (כי G ציקלית אינסופית). נובע ש $H = \langle a^{k_0} \rangle$ אינסופית.

2. (60 נק')

(א) (30 נק') נוכיח ש G נוצרת על ידי $(1,1)$. מכיוון שהסדר של G שווה mn מספיק להראות ש $\mathrm{ord}(1,1) = mn$. ברור ש $mn(1,1) = (0,0)$ כי $mn1 = 0$ ב $(\mathbb{Z}/m\mathbb{Z})$ וגם $mn1 = 0$ ב $(\mathbb{Z}/n\mathbb{Z})$. יהי $a \in \mathbb{N}$ כך ש $a(1,1) = (a,a) = (0,0)$. נובע ש a כפולה של m וגם a כפולה של n. ניתן לכתוב $a = mk$ ואז התנאי השני הוא ש $n|mk$. מכיוון ש $\gcd(m,n) = 1$ נובע ש $n|k$ לכן $mn|mk \iff mn|a$. בפרט, לכל $a = 1, \ldots, mn-1$ מתקיים ש $a(1,1) \neq (0,0)$. נובע ש $\mathrm{ord}(1,1) = mn$ לפי הנדרש.

(ב) (20 נק') מכיוון ש $t = \mathrm{lcm}(m,n)$ קיימים $x, y \in \mathbb{N}$ כך ש $t = xm = yn$. נובע שלכל $(a,b) \in G$ מתקיים

$$t(a,b) = (ta, tb) = (xma, ynb) = (0,0)$$

כי $m = 0$ ב $\mathbb{Z}/m\mathbb{Z}$ ו $n = 0$ ב $\mathbb{Z}/n\mathbb{Z}$.

(ג) (10 נק') נכתוב $\gcd(m,n) = d > 1$. לפי תרגיל שפרתנו בתרגול, $t = \mathrm{lcm}(m,n) = \frac{mn}{d} < mn$. לפי הסעיף הקודם, לכל $(a,b) \in G$ מתקיים $t(a,b) = (0,0)$ לכן $\mathrm{ord}(a,b) \leq t < mn$. אילו G הייתה ציקלית, היה קיים איבר $(a,b) \in G$ כך ש $\mathrm{ord}(a,b) = |G| = mn$. לכן G אינה ציקלית.

3. (בונוס 50 נק') נתאים לכל צבע איבר מהחבורה

$$G = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}.$$

יהי $a_i \in G$ האיבר ב G שמותאם לצבע הכובע של האדם שעומד במיקום i בתור, כאשר a_1 מותאם למי שעומד בראש התור ו a_r מותאם למי שעומד בסוף התור. האדם האחרון בתור מתרגם את כל

הכובעים שהוא רואה לפניו לאיברים ב G ומחשב את הסכום שלהם $a_{r-1}+\cdots+a_1$ ב G. הוא מתרגם את התוצאה בחזרה לצבע ואומר את הצבע הזה. האדם שעומד לפניו מתרגם את כל הכובעים שהוא רואה לאיברים ב G ומחשב את הסכום $a_{r-2}+\cdots+a_1$. הוא כבר יודע את הסכום $a_{r-1}+\cdots+a_1$ לכן הוא מחסר את התוצאות ומקבל את a_{r-1}, האיבר ב G שמותאם לצבע הכובע שלו. ואז כמובן הוא אומר את הצבע הזה. באופן כללי, כולם שומעים בהתלחה (תרגום של הסכום $a_{r-1}+\cdots+a_1$. אדם במיקום j שומע את הסכום הזה וגם את האיברים $a_{r-1}, a_{r-2}, \ldots, a_{j+1}$ ולכן הוא מחשב

$$(a_{r-1}+\cdots+a_1)-a_{r-1}-\cdots-a_{j+1}=a_j+\cdots+a_1.$$

לפי מה שהוא רואה הוא מחשב את $a_{j-1}+\cdots+a_1$ ואז הוא מחסר את התוצאות ומקבל את a_j. בצורה כזאת, כל אחד בתור (חוץ אולי מהאדם בסוף) יצליח לחשב את האיבר ב G שמותאם לצבע של הכובע שלו.