פתרון מבחן תשעה מועד ב

1 בפברואר 2016

.1

(א) איבר g הוא יוצר של חבורה G אם $\langle g\rangle = \left\{g^k : k \in \mathbb{Z}\right\} = G$

(ב) תהא G חבורה ציקלית עם n איברים ו g יוצר. נסמן $o(g) = m$ צריך להוכיח $m = n$.

i. טענה $\langle g\rangle = \left\{g.g^2, \dots g^m = g^0 = e\right\}$
הוכחה: יהא $g^k \in \langle g\rangle$ צריך להוכיח כי $g^k \in \left\{g.g^2, \dots g^m = g^0 = e\right\}$ [ההכלה השניה מיידית].
כיוון ש $g^m = e$ ומקיים $g^{k+sm} = g^k \left(g^m\right)^s = g^k$ ניתן להניח כי $k > 0$ בה"כ (אחרת, נחליף את k נבחר s כלשהוא כך ש $k + sm > 0$)
נבצע חילוק מספרים $k = mq + r$ כאשר $0 \leq r < m$ וכמו מקודם מתקיים

$$g^k = g^{mq+r} = g^r \left(g^m\right)^q = g^r e^q = g^r$$

ו $g^r \in \left\{g.g^2, \dots g^m = g^0 = e\right\}$.

ii. טענה: בקבוצה $\left\{g.g^2, \dots g^m = g^0 = e\right\}$ יש mאיברים (כלומר כל האיברים שונים)
הוכחה: נניח שלא, אזי קיימים $0 \leq i < j < m$ כך ש $g^i = g^j$. נכפיל ב g^{-i} את השיוון ונקבל $e = g^{j-i}$ כאשר $0 < j - i < m$ זה סתירה להגדרה הסדר של g.

iii. מסקנה: $o(g) = m = \left|\left\{g.g^2, \dots g^m = g^0 = e\right\}\right| = |\langle g\rangle| = |G| = n$

(ג) ב $\mathbb{Z}_3$ גם 1וגם 2 יוצרים אבל $1 + 2 = 0$ אינו יוצר

.2

(א) פונקציה $\phi : G_1 \to G_2$ בין שתי חבורות תקרא הומורפיזים אם

$$\forall x, y \in G_1 : \ \phi(xy) = \phi(x)\phi(y)$$

(ב) נשים לב שכל מספר מרוכב z מקיים

$$z \in T \iff |z| = 1$$

כאשר $|z|$ זה הערך המוחלט המרוכב. כעת נוכיח ש T תת חבורה:

i. איבר היחידה $1 \in G$ אכן נמצא על מעגל היחידה $1 \in T$

ii. קיבוציות - נובע מקיבוציות של G

iii. סגירות: יהיו $z_1, z_2 \in T$ (ואז $|z_1| = |z_2| = 1$) אזי

$$|z_1 z_2| = |z_1| \cdot |z_2| = 1 \cdot 1 = 1$$

ולכן $z_1 z_2 \in T$

iv. הופכי: יהי $z \in T$ אז $|z| = 1$ בפרט $z \neq 0$ ולכן קיים לו הופכי במרוכבים. כלומר קיים $w = z^{-1}$ נוכיח כי $w \in T$ אכן $zw = 1$ ולכן (נשים ערך מוחלט על שני האגפים):

$$1 = |1| = |zw| = |z||w| = 1|w| = w$$

(ג) נגדיר $\phi : G \to \mathbb{R}_+$ ע"י $\phi(z) = |z|$ לכל $z \in G$ (שימו לב ש $|z|$ תמיד חיובי כי $z = 0 \iff |z| = 0$ אבל $0 \notin G$) . טענה: זהו הומומורפיזם על. הוכחה:

$$\phi(z_1 z_2) = |z_1 z_2| = |z_1||z_2| = \phi(z_1)\phi(z_2)$$

לכל $z_1, z_2 \in G$ ולכן זהו המומורפיזם. הוא על כי: יהא $x \in \mathbb{R}_+$ אזי בפרט $x \in G$ ובנוסף $\phi(x) = |x| = x$ ולכן הוא המקור של עצמו. נחשב את הגרעין של ϕ ואז נשתמש במשפט האיזומורפיזם הראשון.

$$\ker \phi = \{z \in G : \ \phi(z) = 1\} = \{z \in G : \ |z| = 1\} = T$$

ולכן

$$G/T \cong \mathbb{R}_+$$

.3

(א) Hתקרא תת חבורה נורמאלית של חבורה G אם

i. H תת חבורה של G

ii. לכל $g \in G$ מתקיים $gH = Hg$

(ב) כעת נתון בשאלה כי $|H| = \frac{|G|}{2}$ולכן גם $|G - H| = \frac{|G|}{2}$. יהא $g \in G$. אם $g \in H$ אז $gHg^1 = gH = H$ כי Hסגורה לכפל והופכי. אחרת: $g \in G - H$ ואז $gh \in G - H$ (כי אחרת $gh \in H$ ואז בהכפלה ב $h^{-1} \in H$ נקבל ש $g \in H$ סתירה). מאותו נימוק $hg \in G - H$. כיוון ש

$$|gH| = |H| = \frac{|G|}{2} = |G - H|$$

ובנוסף $gH \subseteq G - H$ נקבל שיוון $gH = G - H$ באופן דומה נקבל ש $Hg = G - H$ ולכן $gH = Hg$

(ג) לא. למשל $G = S_3$ חבורה עם 6 איברים $H = \langle (1,2) \rangle = \{id, (1,2)\}$ תת חבורה עם $\frac{6}{3} = 2$ איברים. אבל Hאינה נומאלית כי עבור $g = (1,2,3)$ נקבל

$$gH = \{g, (3,1)\} \neq \{g, (2,3)\} = Hg$$

.4

(א) יהיו a, b שני פולינומים אזי אלגוריתם אוקלידיס (המוכלל) למציאת $\gcd(a,b)$ הוא אלגורתים הבא:

i. נגדיר באינדוקציה a_n, b_n פולינומים באופן הבא: $a_0 = a, r_0 = b_0 = b$ ושאר הפולינומים באידוקציה:
(נניח שהגדרנו פולינומים a_{n-1}, b_{n-1})
נבצע חילוק פולינומים ונקבל $a_{n-1} = q_{n-1}b_{n-1} + r_{n-1}$ כאשר $\deg r_{n-1} < \deg b_{n-1}$ או $r_{n-1} = 0$.
נגדיר $a_n = b_{n-1}$ ו $b_n = r_{n-1}$.

ii. $\gcd(a,b) = r_n$ כאשר $r_{n+1} = 0$ אך $r_n \neq 0$.

(ב) נשתמש בחילוק ארוך לקבל

$$\begin{aligned} x^5 + x^3 + x^2 + 1 &= \left(x^2 + x + 1\right)\left(x^3 + x^2 + x + 1\right) + \left(x^2 + x\right) \\ x^3 + x^2 + x + 1 &= x\left(x^2 + x\right) + (x + 1) \\ x^2 + x &= x \cdot (x + 1) + 0 \end{aligned}$$

ולכן $\gcd(x^5 + x^3 + x^2 + 1, x^3 + x^2 + x + 1) = x + 1$ נראה את הצירוף הלינארי המתאים:

$$\begin{aligned} x + 1 &= \left(x^3 + x^2 + x + 1\right) + x\left(x^2 + x\right) \\ &= \left(x^3 + x^2 + x + 1\right) + x\left(\left(x^5 + x^3 + x^2 + 1\right) + \left(x^2 + x + 1\right)\left(x^3 + x^2 + x + 1\right)\right) \\ &= \left(x^3 + x^2 + x + 1\right)\left(1 + x\left(x^2 + x + 1\right)\right) + x\left(x^5 + x^3 + x^2 + 1\right) \end{aligned}$$

(ג) נחשב הופכי $123^{-1} \mod 200$

$$\begin{aligned} 200 &= 23 \cdot 8 + 16 \\ 23 &= 1 \cdot 16 + 7 \\ 16 &= 2 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

ולכן

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3 \cdot (16 - 2 \cdot 7) = 7 \cdot 7 - 3 \cdot 16 \\ &= 7 \cdot (23 - 16) - 3 \cdot 16 = 7 \cdot 23 - 10 \cdot 16 \\ &= 7 \cdot 23 - 10 \cdot (200 - 23 \cdot 8) = 87 \cdot 23 - 10 \cdot 200 \end{aligned}$$

ולכן

$$23^{-1} = 87 \mod 200$$

ולכן פתרון המשוואה הוא

$$x = 23^{-1} \cdot 12 = 87 \cdot 12 = 44 \mod 200$$

.5

(א) I יקרא אידיאל של חוג קומטטבי R אם

i. I הוא תת חבורה (ביחס לחיבור) של $(R, +)$

ii. $\forall r \in R, i \in I : ri \in I$ ("בליעה" בכפל מ R)

(ב) נסמן $I = \{g(x) \in \mathbb{R}[x] : p(x)|g(x)\}$ נוכיח את שני התנאים:

i. תת חבורה של $\mathbb{R}[x]$: איבר הניטרלי $0 \in I$ כי $p(x)|0$. יש סגירות כי אם $g_1, g_2 \in I$ אזי $p|g_1, g_2$ ולכן מחלק גם את הסכום (סגירות) וההפרש (קיום הופכי) $p|g_1 \pm g_2$. (קיבוצויות נובע מקיבוצויות בחוג הפולינומים)

ii. יהא $h(x) \in \mathbb{R}[x], g(x) \in I$ צ"ל כי $h(x)g(x) \in I$ אכן כיוון ש $p(x)|g(x)$ אז זגם $p(x)|h(x)g(x)$.

(ג) לא קיים איבר שכזה. הוכחה: שדה $\mathbb{F}$ עם $27 = 3^3$ הוא ממאפין 3 בסימונים מקובלים $char(\mathbb{F}) = 3$ כלומר $1 + 1 + 1 = 0$. כעת יהא $x \in \mathbb{F}$ אזי

$$x + x + x = x(1 + 1 + 1) = x \cdot 0 = 0$$

ולכן $o(x) \leq 3$ בפרט $o(x) \neq 9$