פתרון מבחן תשעה מועד א

1 בפברואר 2016

.1

(א) חבורה G תקרא קומטטיבית אם לכל $x,y\in G$ מתקיים $xy=yx$

(ב) יהיו $x,y\in G$ אזי לפי הנתון מתקיים כי

$$xyxy=(xy)^2=x^2y^2=xxyy$$

ע"י הכפלה ב x^{-1} משמאל ו y^{-1} מימין נקבל $yx=xy$.

(ג) לא. למשל $G=S_3$ חבורה לא קומטטבית. בנוסף $|S_3|=3!=6$ ולכן לפי משפט לגרנז לכל $\sigma\in S_3$ מתקיים $\sigma^6=id$ ולכן $\sigma^7=\sigma$בפרט מתקיים לכל σ_1,σ_2 כי

$$(\sigma_1\sigma_2)^7=\sigma_1\sigma_2=\sigma_1^7\sigma_2^7$$

.2

(א) H תת חבורה של Gאם היא חבורה ביחס לפעולה של G.

(ב) נוכיח קריטריון של חבורה

i. מוגדרות: יהיו $x,y\in G_1\cap G_2$ אזי $x,y\in G_1,G_2$ בגלל שאלו תת חבורות מתקיים כי $xy\in G_1,G_2$ ולכן גם $xy\in G_1\cap G_2$

ii. קיבוציות: מתקיים כתת קבוצה של G

iii. איבר נטרלי: כיוון ש G_1,G_2 תת חבורות אזי $e\in G_1,G_2$ ולכן גם בחיתוך

iv. הופכי: יהא $g\in G_1\cap G_2$ אזי $g\in G_1,G_2$ כיוון שאלו תת חבורות g^{-1} קיים בכל אחת מהן ולכן גם בחיתוך.

(ג) נניח בשלילה כי אף אחת לא מכילה את השניה. אזי קיים $g_1\in G_1\backslash G_2$ וגם $g_2\in G_2\backslash G_1$ כיוון שנתון שהאיחוד הוא תת חברה אזי בפרט הוא סגור לפעולה ולכן $g_1g_2\in G_1\cup G_2$ מהגדרת האיחוד $g_1g_2\in G_1$ או $g_1g_2\in G_2$. אם $g_1g_2\in G_1$: כיוון ש $g_1\in G_1$ ו G_1 חבורה אזי קיים $g_1^{-1}\in G_1$. בנוסף יש סגירות ב G_1 ולכן גם $g_2=g_1^{-1}(g_1g_2)\in G_1$ אבל $g_2\notin G_1$ סתירה. באופן דומה המקרה ש $g_1g_2\in G_2$.

.3

(א) תהא G חבורה סופית $H\leq G$ תת חבורה אזי $|H|$ מחלק את $|G|$.

(ב) יהא $g\in G$ שונה מאיבר היחידה אזי $|\langle g\rangle|$ מחלק את $|G|=p$ אזי $|\langle g\rangle|$ שווה 1 או p (כי p ראשוני). כיוון ש $e,g\in\langle g\rangle$ 2 איברים שונים אזי בהכרח $|\langle g\rangle|=p$ כיוון ש $\langle g\rangle\subseteq G$ מאותו גודל הם שוות. בפרט g יוצר ו G ציקלית

(ג) נגדיר את החוג $G=\{1,2,\dots,72\}$ חבורה ביחס לכפל מודולו 73 (זה חבורה כי 73 ראשוני). חבורה זאת בת 72 ולכן לפי משפט לגרנז $2^{72}=1$ בחבורה (כלומר מודלו 73) ולכן $2^{76}=2^{72}2^4=2^4=16$ מודלו 73 בפרט $2^{76}-16=0$ מדולו 73 כלומר מתחלק ב 73.

4.

(א) עבור שני פולינומים f,g המחלק המשותף המקס' הוא הפולינום $d=\gcd(f,g)$ כך ש

i. d מתוקן

ii. d מחלק את f וגם את g

iii. אם פולינום d' מקיימים מחלק את f וגם את g אזי $\deg d'\leq\deg d$

(ב) נבצע חילוק פולינומים בכמה שלבים

$$x^5-1 = \left(x^3-x^2+x-1\right)\left(x^2+x\right)+(x-1)$$

$$x^3-x^2+x-1 = (x-1)\left(x^2+1\right)+0$$

ולכן המחלק המשותף המקס הוא $x-1$ והוא שווה ל $x-1=\left(x^5-1\right)-\left(x^3-x^2+x-1\right)\left(x^2+x\right)$

(ג) רוצים לפתור (ע"י העברת אגף)

$$22x=32 \mod 120$$

טענה: זה שקול לפתור

$$11x=16 \mod 60$$

הוכחה: אם $22x=32 \mod 120$ אזי $22x-32=120k$ עבור k שלם שזה גורר כי $11x-16=60k$ שזה גורר $11x=16 \mod 60$. מצד שני אם $11x=16 \mod 60$ אזי $11x-16=60k$ עבור k מסוים שזה גורר $22x-32=120k$ שזה גורר $22x=32 \mod 120$.

נפתור את המשוואה השניה: תחילה נמצא $11^{-1} \mod 60$

$$60 = 5\cdot 11+5$$

$$11 = 2\cdot 5+1$$

ולכן

$$1=11-2\cdot 5=11-2\cdot(60-5\cdot 11)=11\cdot 11-2\cdot 60$$

ולכן $11^{-1}=11$ (אתם מוזמנים לבדוק ישירות)

לכן

$$x=11^{-1}\cdot 16=11\cdot 16=176=56 \mod 60$$

וזה הפתרון היחיד.

5.

(א) מחלק אפס הוא $a \neq 0$ כך שקיים $b \neq 0$ המקיים $ab = 0$

(ב) יש מחלקי אפס. למשל: $f(x) = (x-1) + \left\langle x^3 - 1 \right\rangle, g(x) = \left(x^2 + x + 1\right) + \left\langle x^3 - 1 \right\rangle$ יקימו

$$f(x) \cdot g(x) = x^3 - 1 + \left\langle x^3 - 1 \right\rangle = 0_R$$

כאשר Rהוא החוג שמוגדר בשאלה.

(ג) זהו שדה. מספיק לבדוק שהפולינום $p(x) = x^4 + x + 1$ הוא אי פריק מעל $\mathbb{Z}_2$. אכן אם הוא היה פריק היה לו גורם מדרגה 1 או 2 או 3

i. אם יש לו גורם מדרגה 1 אזי יש לו שורש אבל $p(1) = 1, p(0) = 1$ כלומר אין לו שורש

ii. אם יש לו גורם מדרגה 2 אזי זהו גורם אי פריק (כי אחרת שוב היה ל $p(x)$ שורש). הפולינום היחידה מדרגה 2 שהוא אי פריק זה הפולינום $x^2 + x + 1$ אבל פולינום זה אינו מחלק את $p(x)$ [בידקו והוכיחו!]

iii. אם היה לו גורם מדרגה 3 אזי הגורם השני בחלוקה היה מדרגה 1. שוב, לא יכול להיות.