מבנים אלגבריים (89-214), מועד ב' תשע"ו

1. תהי G חבורה ונניח $H,K\leq G$ שתי תת-חבורות כך שאף אחת מהן לא מכילה את השנייה. הוכח כי האיחוד $H\cup K$ אינו תת-חבורה של G.

<u>פתרון</u> כיוון ש- $H\nsubseteq K$, קיים איבר $h\in H$ כך ש- $h\notin K$. וכן $K\nsubseteq H$, לכן קיים $k\in K$ כך ש- $k\notin H$.

נניח בשלילה כי $H\cup K$ כן תת-חבורה. אז היא סגורה תחת הפעולה של G. בפרט, $k,h\in H\cup K$, ולכן $h*k\in H\cup K$ זה אומר כי $h*k\in H$ או $h*k\in K$.

נניח כי $h*k\in H$. כיוון ש- H סגורה תחת הפכים, גם $h^{-1}\in H$, ולכן $k=h^{-1}*(h*k)\in H$, בסתירה להנחה כי $k\notin H$.
וכן אם $h*k\in K$, אז $h=(h*k)*k^{-1}\in K$, כי $k^{-1}\in K$, וזה סותר את ההנחה כי $h\notin K$.

לכן $H\cup K$ אינה סגורה תחת הפעולה של G, ולא ייתכן שהיא תת-חבורה.

2.א) מיין את החבורות האבליות מסדר 90. כלומר, הצג רשימה של חבורות
כך שכל חבורה מסדר 90 תהיה איזומורפית לאחת, ורק אחת, מן החבורות
ברשימה.

<u>פתרון</u> למדנו בהרצאה שכל חבורה אבלית מסדר n איזומורפית לאחת, ורק אחת, מן החבורות מן הצורה

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$$

כאשר $d_1 | d_2, \dots, d_{r-1} | d_r$, $1 < d_1$, וגם $d_1 d_2 \cdots d_r = n$.

במקרה של $n = 90 = 2 \cdot 5 \cdot 3^2$, הפירוקים $d_1 = 90$ הם היחידים
$d_1 = 3,\ d_2 = 30$
שעונים על הדרישות הנ"ל. לכן כל חבורה מסדר 90 איזומורפית
ל- $\mathbb{Z}_{90}$ או $\mathbb{Z}_3 \times \mathbb{Z}_{30}$.

ב) לפי משפט מן התרגול, אם $\gcd(m,n)=1$ <u>(שהצגנו גם בשיעור)</u> אזי $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

i) כיוון ש- $(5,18)=1$, נקבל $\mathbb{Z}_5 \times \mathbb{Z}_{18} \cong \mathbb{Z}_{90}$ לפי המשפט הנ"ל.

ii) כיוון ש- $(3,10)=1$, נקבל $\mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_{30}$, ולכן $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_3 \times \mathbb{Z}_{30}$

iii) כיוון ש- $(9,10)=1$, נקבל $\mathbb{Z}_{10} \times \mathbb{Z}_9 \cong \mathbb{Z}_{90}$.

<u>הערות</u> בסעיף א', אפשר לתת הרבה רשימות שקולות לרשימה הנ"ל, כל תשובה נכונה התקבלה.

בסעיף ב', מי שלא נימק את התשובה לא קיבל ציון מלא. אפשר גם להבדיל בין שני האופציות בשימוש באקספוננטה, אך יש לנמק איך מחשבים אותה:

$$\exp(\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}) = \mathrm{lcm}(d_1, \dots, d_r).$$

3. א) נסח הגדרה של מספר מדין ראשוני.

<u>פתרון</u> מספר שלם $n>1$ נקרא מדין ראשוני אם $a^{n-1}\equiv 1 \mod n$ לכל $a\in\mathbb{Z}$ כך ש- $(a,n)=1$.

ב) יהי k מספר טבעי כך ששלושת המספרים $6k+1,\ 12k+1,\ 18k+1$ כולם ראשוניים. הוכח כי $(6k+1)(12k+1)(18k+1)$ הינו מספר קרמייקל.

<u>פתרון</u> יהי $n=(6k+1)(12k+1)(18k+1)$. אזי n לא ראשוני, כי הוא מכפלה של שלושה גורמים ראשוניים. נשאר להוכיח כי n מדין ראשוני. נפתח את הסוגריים ונראה כי

$$n=(6\cdot12\cdot18)k^3+(18^2+72)k^2+36k+1$$

בפרט, $n-1=(36\cdot36)k^3+(36\cdot11)k^2+36k$ מתחלק ב- $36k$, ולכן $n-1$ מתחלק ב- $6k$, ב- $12k$, וב- $18k$.

אם $(a,n)=1$, אזי בפרט a זר לראשוני $6k+1$, ולפי המשפט הקטן של פרמה, $a^{6k}\equiv 1 \mod 6k+1$. אך $n-1=6k\cdot m$ עבור m שלם כלשהו, ולכן $a^{n-1}=(a^{6k})^m\equiv 1^m=1$ מודולו $6k+1$.

כמו כן, נקבל $a^{n-1}\equiv 1 \mod 12k+1$ וגם $a^{n-1}\equiv 1 \mod 18k+1$. לכן, $a^{n-1}-1$ מתחלק ב- $(6k+1)$, ב- $(12k+1)$ וב- $(18k+1)$, לכן הוא מתחלק ב- lcm של שלושת המספרים האלה. אך כיוון שהם ראשוניים <u>שונים</u>, ה- lcm הינו המכפלה שלהם, כלומר n.

לכן $n\mid(a^{n-1}-1)$, כלומר $a^{n-1}\equiv 1 \mod n$, ולכל a זר ל- n. לכן, n מדין ראשוני.

<u>הערה</u> בשיעור הוכחנו כי $561=3\cdot11\cdot17$ הינו מספר קרמייקל. ההוכחה הנ"ל <u>זהה</u>.

4. נסמן ב- $\mathbb{F}_q$ את השדה בעל q איברים. יהי $P(x)=x^2+[2]x+[2]$ (כאן $[2]=1_{\mathbb{F}_q}+1_{\mathbb{F}_q}$).

א) הוכח כי $P(x)$ אי פריק מעל $\mathbb{F}_7$.

<u>פתרון</u> נניח בשלילה כי $P(x)$ אכן פריק, כלומר $P(x)=Q_1(x)Q_2(x)$ עבור שני פולינומים לינאריים $Q_1(x), Q_2(x)$.
יהי $Q_1(x)=ax+b$, כאשר $a,b\in F=\mathbb{F}_7$, ו- $a\neq 0_F$. אזי $P(x)=a(x+ba^{-1})Q_2(x)$, לכן $P(-ba^{-1})=a\cdot 0_F\cdot Q_2(-ba^{-1})=0_F$. לכן $-ba^{-1}$ (ב-$\mathbb{F}_7$) הינו שורש של $P(x)$. אך נוכל לבדוק ישירות כי ל- $P(x)$ אין שורשים, בסתירה להנחה ש- $P(x)$ פריק מעל $\mathbb{F}_7$.

$P([0])=[0]+[0]+[2]=[2]$

$P([1])=[1]+[2]+[2]=[5]$ $\qquad$ $P([4])=[16]+[8]+[2]=[26]=[5]$

$P([2])=[4]+[4]+[2]=[3]$ $\qquad$ $P([5])=[25]+[10]+[2]=[37]=[2]$

$P([3])=[9]+[6]+[2]=[3]$ $\qquad$ $P([6])=[36]+[12]+[2]=[50]=[1]$

<u>הערה</u> לא הוכחנו לא בשיעור ולא בתרגיל כי לפולינום יש שורש אם יש לו גורם לינארי, לכן מי שרצה להיעזר בטענה הזאת היה צריך להוכיח אותה. יותר מזה, לא הוכחנו שפולינום אי-פריק אם אין לו שורשים (וזה לא נכון אם המעלה גדולה מ-3).

ב) על ידי הצבה כנ"ל, מוצאים כי $[1]\in\mathbb{F}_5$ ו- $[2]\in\mathbb{F}_5$ הם שורשים של $P(x)$ מעל $\mathbb{F}_5$. הרעיון מן הסעיף א' גורם לנו לנחש כי $P(x)=(x-[1])(x-[2])$

ואכן,

$$(x-[1])(x-[2]) = x^2-[1]x-[2]x+[2] = x^2-[3]x+[2] = x^2+[2]x+[2] = P(x)$$

לכן $P(x)$ פריק מעל $\mathbb{F}_5$.

<u>הערה</u> לא הוכחנו שאם a הינו שורש של $P(x)$, אזי $P(x)=(x-a)Q(x)$ עבור פולינום $Q(x)$. מי שרצה להשתמש בטענה הזאת ולעבור בבדיקה של- $P(x)$ יש שורשים מעל $\mathbb{F}_5$, היה צריך להוכיח אותה (על ידי האלגוריתם של אוקלידס לחילוק פולינומים).

ג) למצוא q,q' נוספים כך ש- $P(x)$ פריק על $\mathbb{F}_q$ אך אי-פריק מעל $\mathbb{F}_{q'}$.

<u>פתרון</u> אם נימקנו כראוי בסעיפים הקודמים, אפשר לחפש, בהצבה ישירה, שדות בהם יש או אין שורשים ל- $P(x)$, ולעשות כמו קודם. (צריך לעבוד רק עם שדות $\mathbb{F}_q$ כאשר q ראשוני, כי אנחנו לא יודעים לתאר את האיברים של $\mathbb{F}_q$ אחרת — הם לא מחלקות שקילות מודולו q.)

או אפשר לפתח את הנתון כך: נניח שיש שורש $y \in \mathbb{F}_q = F$. אזי

$$P(y) = y^2 + [2]y + [2] = (y+[1])^2 + 1_F = 0_F$$

כלומר, אם $z = y + 1_F$, אזי $z^2 = -1_F$. אזי
כלומר $z^4 = 1_F$ אך אם $\operatorname{char} F \neq 2$, אזי $z^2 \neq 1_F$, כלומר $o(z) = 4$
כאשר מתייחסים ל-z כאיבר של החבורה F^*. אך F^* היא חבורה ציקלית מסדר $q-1$, לכן יש לה איבר מסדר 4 אם ורק אם $4 \mid (q-1)$.

כלומר, אם $4 \nmid (q-1)$ (כלומר $q \not\equiv 1 \mod 4$) וגם $\operatorname{char} F \neq 2$, אזי ל-$P(x)$ אין שורשים מעל $\mathbb{F}_q$, וכמו בסעיף א' מסיקים שהוא אי-פריק מעל $\mathbb{F}_q$.

אם $\operatorname{char} \mathbb{F}_q = 2$, אזי $P(x) = x^2 + [2]x + [2] = x^2 = x \cdot x$, כך שהוא גם פריק.

אם $\operatorname{char} F \neq 2$ וגם $q \equiv 1 \mod 4$, אזי קיים $z \in F^*$ כך ש- $o(z) = 4$.
אזי $o(z^2) = 2$. אך בחבורה ציקלית יש לכל היותר שני איברים מסדר שמחלק את 2. אנחנו יודעים על שני איברים כאלה ב-F^*: $\pm 1_F$. לכן -1_F הינו האיבר היחיד של F^* מסדר 2. לכן $z^2 = -1_F$. אם $y = z - 1_F$, אזי

$$z^2 = (y + 1_F)^2 = y^2 + [2]y + [1] = -[1]$$

כלומר y הינו שורש של $P(x)$. כלומר במקרה הזה ל- $P(x)$ יש שורשים.
כדי להוכיח שהוא פריק בלי להוכיח משפטים, צריך למצוא שני שורשים מפורשים ולפרק לפולינומים ליניאריים, כמו שעשינו בסעיף ב'.

5. נתונה G חבורה סופית, ותהי $H \trianglelefteq G$ תת-חבורה נורמלית. יהי $f: G \to G/H$ ההומומורפיזם המוגדר על ידי $f(g)=gH$ לכל $g\in G$. יהי $a\in G$ איבר כך ש- $o(a)$ זר ל- $|H|$. הוכח כי $o(a)=o(f(a))$.

<u>הוכחה</u> יהי $n=o(a)$. אזי $a^n=e_G$. כיוון ש-f הומומורפיזם, נקבל

$$(aH)^n = (f(a))^n = f(a^n) = f(e_G) = e_{G/H}$$

(או ישירות: $(aH)^n = a^nH = e_GH = e_{G/H}$).

מכאן מסיקים $o(f(a)) \mid o(a)$.

עכשיו יהי m מספר חיובי כך ש- $(aH)^m = e_{G/H}$ אזי $(aH)^m = (a^mH) = e_{G/H} = H$, כלומר $a^m\in H$.

כיוון ש- $a^m \in \langle a\rangle$, ואילו $\langle a\rangle$ הינה תת-חבורה של G, לפי לגרנז' נקבל כי $o(a^m)$ מחלק את $n=o(a)=|\langle a\rangle|$. מאידך, $a^m\in H$, ולכן שוב לפי לגרנז', $o(a^m) \mid |H|$. לכן $o(a^m)$ הינו מחלק משותף של n ושל $|H|$. אך לפי ההנחה, $(n,|H|)=1$. לכן $o(a^m)=1$, כלומר $a^m=e_G$, כלומר $o(a) \mid m$.

הנ"ל היה נכון עבור כל מספר m כך ש- $f(a)^m=(aH)^m=e_{G/H}$, ובפרט עבור $o(f(a))=m$. לכן $o(a) \mid o(f(a))$.

כבר הוכחנו כי $o(f(a)) \mid o(a)$, ולכן $o(a) = o(f(a))$ כנדרש.

<u>הערה</u> הרבה סטודנטים הגיעו ל- $f(a)^{o(f(a))} = a^{o(f(a))}H=H$, אך הסיקו בטעות כי $a^{o(f(a))}=e$. ניתן להסיק רק כי $a^{o(f(a))}\in H$.