TEL AVIV UNIVERSITY אוניברסיטת תל-אביב
RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES
SCHOOL OF MATHEMATICAL SCIENCES
הפקולטה למדעים מדויקים ע"ש ריימונד ובברלי סאקלר
בית הספר למדעי המתמטיקה

מבחן באלגברה ב' 1

0366.2132.01

לתלמידי דן הרן

כ"ד באדר ב', תשס"ח
31 במרץ 2008

משך המבחן: 3 שעות.
אין להשתמש בחומר עזר כלשהו.
ענה על ארבע (בלבד) מתוך שש השאלות הבאות.

שאלה 1: הגדר חבורת סילוב־p של חבורה סופית והוכח שלכל חבורה סופית יש חבורת סילוב־p.

פתרון: ראה בחוברת (ההגדרה בתחילת סעיף 13 והמשפט הוא משפט 13.2.).

שאלה 2: הגדר זוגיות $\mathrm{Sg}(\sigma)$ של תמורה σ והוכח שההעתקה $\mathrm{Sg}\colon S_n \to \{\pm 1\}$ היא הומומורפיזם.

פתרון: ראה בחוברת. (זוהי הערה 9.7 ומשפט 9.9).

שאלה 3: תהי G חבורת־p ותהי $\{1\} \neq N \triangleleft G$. הוכח שבפעולת ההצמדה של G על N יש לפחות p מסלולים בעלי אורך 1 והסק או הוכח אחרת כי $N \cap Z(G) \neq \{1\}$.

פתרון: לפי נוסחת המחלקות

$$|N| = \sum_{i \in I'} (G : G_{x_i}) + |M| . \tag{1}$$

באשר $\{x_i\}_{i\in I'}$ היא מערכת מיצגים של מסלולי־G בעלי אורך >1. ו־

$$M = \{x \in N |\ gxg^{-1} = x \quad g \text{ לכל } g \in G\} = \{x \in N |\ x \in Z(G)\} = N \cap Z(G)$$

אורך של המסלול של x_i הוא $(G : G_{x_i})$, שהינו חזקה של p (כי הוא מחלק את $|G|$ שהינו חזקה של p), ואם הוא >1, אז זו חזקה לא טריביאלית של p ובפרט מספר שמתחלק ב־p. לכן הסכום הראשון באגף ימין של (1) מתחלק ב־p. גם אגף שמאל מתחלק ב־p כי $|N|$ מחלק את $|G|$ ואינו 1. לכן $|M| = |N \cap Z(G)|$ מתחלק ב־p ובפרט יש בו לפחות שני איברים. אחד מהם הוא 1, לכן $N \cap Z(G) \neq \{1\}$.

שאלה 4: תהי G חבורה מסדר p^2q, באשר p,q ראשוניים שונים. הוכח שאחת מחבורות סילוב של G הינה נורמלית ב־G. (שים לב שאם $2 \neq p < q$ אז q אינו מחלק את $(p-1)(p+1)$.)

פתרון: תהי P חבורת סילוב־p ו־Q חבורת סילוב־q של G. נסמן ב־n_p את מספר חבורות סילוב־p וב־n_q את מספר חבורות סילוב־q של G. די להוכיח כי $n_p = 1$ או $n_q = 1$, כי אם חבורת סילוב מסוימת הינה יחידה, אז היא נורמלית.

מתקיים $n_p|(G:P) = p^2q/p^2 = q$, לכן $n_p = 1$ או $n_p = q$. אך לפי המשפט השלישי של סילוב, $n_p \equiv 1 \pmod p$. לכן אם $q < p$, אז לא יתכן $n_p = q$, כי $1 < q < p$. לכן תחת ההנחה $q < p$ מתקיים $n_p = 1$, כמבוקש.

נניח, איפוא, $p < q$. מתקיים $n_q|(G:Q) = p^2q/q = p^2$, לכן $n_q = 1$ או $n_p = q$ או $n_q = p^2$. אך לפי המשפט השלישי של סילוב, $n_q \equiv 1 \pmod q$. לכן לא יתכן $n_q = p$, כי $1 < p < q$. אם $n_q = 1$, סיימנו. נניח אם כן כי $n_q = p^2$. אז $p^2 \equiv 1 \pmod q$ פירושו $q|p^2 - 1 = (p-1)(p+1)$, וכיון ש־q ראשוני, זה אומר $q|p-1$ או $q|p+1$. בפרט $q \leq p-1$ או $q \leq p+1$, כלומר, $q \leq p+1$. כיון ש־$p < q$ זה אומר $q = p+1$. כיון ש־p,q ראשוניים, זה אומר $p=2, q=3$.

במקרה זה G מסדר 12, יש לה $n_q = p^2 = 4$ חבורות סילוב־3. בכ"א מהן יש 2 איברים מסדר 3, וחיתוך כל שתי חבורות סילוב־3 הוא $\{1\}$, לכן יש בחבורות סילוב־3 בדיוק $4 \times 2 = 8$ איברים מסדר 3. מלבד האיברים האלה יש עוד קבוצה A בת 4 איברים ב־G. איברים בחבורות סילוב־2 אינם מסדר 3, לכן הם בתוך A. היות ובכל חבורות סילוב־2 יש ארבעה איברים, היא שווה ל־A. לכן יש חבורת סילוב־2 יחידה ב־G.

שאלה 5: כתוב הגדרה של חבורה פשוטה. הוכח שאם G_1, G_2 חבורות סופיות פשוטות אז כל תת חבורה נורמלית של $G = G_1 \times G_2$ השונה מ־G ומ־$\{1\}$ הינה איזומורפית ל־G_1 או ל־G_2.

פתרון: חבורה G הינה פשוטה אם אין לה תת חבורות נורמליות, מלבד $\{1\}$ ו־G.

נניח כי $G = G_1 \times G_2$, באשר G_1, G_2 סופיות פשוטות. אז $G \triangleright G_1 \triangleright \{1\}$ סדרת הרכב של G, כי $G/G_1 \cong G_2$, $G_1/\{1\} \cong G_1$ פשוטות. תהי $N \triangleleft G$ שונה מ־G ומ־$\{1\}$. אז $G \triangleright N \triangleright \{1\}$ סדרה נורמלית ללא חזרות מאורך 2. אפשר לעדן אותה לסדרת הרכב. לפי משפט Jordan-Hölder כל שתי סדרות הרכב שקולות, ובפרט יש להן אותו מספר של איברים. במקרה שלנו סדרת ההרכב הראשונה מאורך 2, לכן $G \triangleright N \triangleright \{1\}$ כבר סדרת הרכב וגורמיה הם כמו בסדרת הרכב הראשונה, עד כדי הסדר. לכן

(א) $N \cong G_1$, $G/N \cong G_2$; או

(ב) $N \cong G_2$, $G/N \cong G_1$.

בכל מקרה, $N \cong G_1$ או $N \cong G_2$.

שאלה 6: תהי A חבורה חילופית סופית. יהי m המספר הטבעי הקטן ביותר כך ש־$ma = 0$ לכל $a \in A$. הוכח שקיים $a \in A$ בעל סדר m.

פתרון: לפי המשפט היסודי של חבורות חילופיות נוצרות סופית אפשר להניח כי

$$A = \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\epsilon_k\mathbb{Z} \oplus \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{r}$$

באשר $\epsilon_1|\cdots|\epsilon_k$ מספרים טבעיים ו־$k, r \geq 0$. בגלל ש־A סופית, $r = 0$. לכן $A = \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\epsilon_k\mathbb{Z}$. יהי $1 \leq i \leq k$. כל $a_i \in \mathbb{Z}/\epsilon_i\mathbb{Z}$ הוא מסדר שמחלק את ϵ_i ו־$\epsilon_i|\epsilon_k$, לכן $\epsilon_k a_i = 0$. מכאן לכל $a = a_1 + \cdots + a_k \in \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\epsilon_k\mathbb{Z} = A$ מתקיים $\epsilon_k a = \epsilon_k a_1 + \cdots + \epsilon_k a_k = 0$. מצד שני, יש $b_k \in \mathbb{Z}/\epsilon_k\mathbb{Z} \leq A$ מסדר ϵ_k. מכאן ש־$m = \epsilon_k$. כאמור, b_k מסדר m.