School of Mathematical Sciences
The Raymond and Beverly Sackler
Faculty of Exact Sciences
Tel Aviv University

בית הספר למדעי המתמטיקה
הפקולטה למדעים מדויקים
ע״ש ריימונד ובברלי סאקלר
אוניברסיטת תל אביב

מבחן באלגברה ב׳ 1

0366.2132.01

לתלמידי דן הרן
מועד א׳

י״א בשבט, תשע״ז
7 בפברואר 2017

משך המבחן: 3 שעות.
אין להשתמש בחומר עזר כלשהו.
ענו על ארבע (בלבד) מתוך שש השאלות הבאות. (כל השאלות הן שוות ערך.)
שתי השאלות הראשונות הן משפטים שהיו בהרצאה.

שאלה 1: הוכיחו: תהי $\langle g\rangle$ חבורה מעגלית מסדר סופי n. לכל מחלק d של n קימת ל־$\langle g\rangle$ בדיוק חבורה חלקית אחת מסדר d, היא $\langle g^{\frac{n}{d}}\rangle$. כמו כן, אלה כל החבורות החלקיות של $\langle g\rangle$.

פתרון: $\langle g^{\frac{n}{d}}\rangle$ הינה מסדר $\operatorname{ord} g^{\frac{n}{d}}$ ואיבר זה הינו מסדר $\frac{n}{\gcd(n,n/d)} = \frac{n}{n/d} = d$. לכן $\langle g^{\frac{n}{d}}\rangle$ אכן מסדר d.
תהי H תת חבורה מסדר d, באשר d מחלק את n. נראה כי $H = \langle g^{\frac{n}{d}}\rangle$. בגלל שוויון הסדרים די להראות $H \subseteq \langle g^{\frac{n}{d}}\rangle$.
יהי $h \in H$; אז $h = g^m$, באשר $0 \le m < n$. מתקיים $\operatorname{ord} h \mid |H|$, כלומר $n/\gcd(n,m) \mid d$, מכאן $n \mid \gcd(n,m)d$, ולכן $\frac{n}{d} \mid \gcd(n,m)$, ובפרט $\frac{n}{d} \mid m$. לכן $h = g^m \in \{(g^{\frac{n}{d}})^k \mid k \in \mathbb{Z}\} = \langle g^{\frac{n}{d}}\rangle$.
מכאן $H \subseteq \langle g^{\frac{n}{d}}\rangle$.

לבסוף, לפי משפט לגרנז׳ כל חבורה חלקית של $\langle g\rangle$ היא מסדר שמחלק את n. ∎

שאלה 2: תהי G חבורה, תהי $N \lhd G$ ותהי $A \le G$. הוכיחו: $AN = NA = \langle A, N\rangle \le G$, $A \cap N \lhd A$, ו־$A/A\cap N \cong AN/N$ על ידי $a(A\cap N) \mapsto aN$.

פתרון: כיוון ש־$N \lhd G$, מתקיים $aN = Na$ לכל $a \in G$. לכן $AN = \bigcup_{a\in A} aN = \bigcup_{a\in A} Na = NA$.
ברור ש־$N, A \subseteq NA \subseteq \langle A, N\rangle$ לכן אם נוכיח ש־AN תת חבורה של G, אז, מכיוון ש־$\langle A, N\rangle$ היא התת חבורה הקטנה ביותר של G שמכילה את A, N, נקבל $\langle A, N\rangle \le AN$ ומכאן $AN = \langle A, N\rangle$.
ואכן, $1 \in AN$, $(AN)(AN) = (AA)(NN) = AN$, $(AN)^{-1} = N^{-1}A^{-1} = NA = AN$. לכן AN תת חבורה של G.
יהי $\pi\colon G \to G/N$ האפימורפיזם הטבעי. גרעינו N. צמצומו $\theta\colon A \to G/N$ ל־A הוא הומומרפיזם. תמונתו [שאמורה לפי משפט האיזומרפיזם השלישי להיות מהצורה H/N באשר $N \le H \le A$] היא

$$\operatorname{Im}\theta = \{\pi(a) \mid a \in A\} = \{\pi(a)\pi(n) \mid a \in A, n \in N\} = AN/N.$$

כמו כן $\operatorname{Ker}\theta = \{a \in A |\ \pi(a) = e\} = A \cap \operatorname{Ker}\pi = A \cap N$. לפי משפט האיזומורפיזם הראשון יש איזומורפיזם $\theta_{A\cap N}\colon A/A\cap N \to AN/N$ הנתון על ידי $a(A\cap N) \mapsto \theta(a) = aN$. ∎

שאלה 3: הוכיחו ש־S_4 מכילה 3 תת חבורות איזומורפיות ל־D_4.

פתרון: נסמן $\sigma = (1234)$, $\tau = (13)$ ו־$P = \langle \sigma, \tau \rangle$. אז $\operatorname{ord}\tau = 2$, $\operatorname{ord}\sigma = 4$, לכן $\langle \sigma \rangle \cong \mathbb{Z}/4\mathbb{Z}$, $\langle \tau \rangle \cong \mathbb{Z}/2\mathbb{Z}$. כמובן, $^{\sigma}\sigma = \sigma \in \langle \sigma \rangle$, ואילו

$$^{\tau}\sigma = \big(\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\big) = (3214) = \sigma^{-1} \in \langle \sigma \rangle,$$

לכן ו־$\langle \sigma \rangle \lhd P$. כיוון ש־$\tau \notin \langle \sigma \rangle$ (האיבר היחיד מסדר 2 של $\langle \sigma \rangle$ הוא $\sigma^2 = (13)(2,4)$), מתקיים $\langle \sigma \rangle \ \cap \langle \tau \rangle = 1$. לכן $P \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, כאשר $\mathbb{Z}/2\mathbb{Z}$ פועלת על $\mathbb{Z}/4\mathbb{Z}$ על ידי הכפלה ב־(-1). מכאן ש־$P \cong D_4$.

יהי n מספר חבורות סילוב־2 של S_4. אז $n \mid \frac{|S_4|}{|P|} = \frac{24}{8} = 3$, לכן $n = 1$ או $n = 3$. אילו היה $n = 1$, היו ב־S_4 בדיוק 8 איברים מסדרים שהם חזקה של 2. אבל ב־S_4 יש שישה חישוקים מאורך 4, שישה חישוקונים, שלוש מכפלות של שני חישוקונים, ואיבר היחידיה, סה"כ 16 איברים, סתירה. לכן $n = 3$.

לכן יש ב־S_4 בדיוק 3 חבורות מסדר 8, אחת מהן P. שתי האחרות צמודות ל־P, לכן איזומורפיות לה.

לכן יש ב־S_4 בדיוק 3 חבורות מסדר 8, כולן איזומורפיות ל־D_4. ∎

שאלה 4: תהי G חבורה ותהיינה H, K תת חבורות אופייניות שלה (ז.א., נשמרות על ידי האוטומורפיזמים של G) כך ש־$G = HK$ ו־$H \cap K = \{1\}$. הוכיחו ש־$\operatorname{Aut}(G) \cong \operatorname{Aut}(H) \times \operatorname{Aut}(K)$.

פתרון: [חזרה כמעט מילולית על ההוכחה של למה 10.4(ב).] יהי $\alpha \in \operatorname{Aut}(G)$. כיוון ש־$K$ אופיינית, $\alpha(K) = K$. לכן $\alpha|_K \in \operatorname{Aut}(K)$. באופן זהה $\alpha|_H \in \operatorname{Aut}(H)$.

נגדיר העתקה

$\varphi\colon \operatorname{Aut}(G) \to \operatorname{Aut}(H) \times \operatorname{Aut}(K)$ על ידי $\varphi(\alpha) = (\alpha|_H, \alpha|_K)$. אזי:

(1) φ **הומומורפיזם:** אכן, יהיו $\alpha, \beta \in \operatorname{Aut}(G)$. אז $(\alpha\beta)|_H = \alpha|_H\beta_H$, $(\alpha\beta)|_K = \alpha|_K\beta_K$, לכן $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

(2) φ **חח"ע:** אם $\varphi(\alpha) = (1,1)$ אז הצמצומים של α ל־H, K הם העתקות זהות ולכן α הינו זהות על $HK = G$.

(3) φ **על:** יהיו $\gamma \in \operatorname{Aut}(K)$, $\beta \in \operatorname{Aut}(H)$, נגדיר העתקה $\alpha\colon G \to G$ באופן הבא: $\alpha(hk) = \beta(h)\gamma(k)$, באשר $k \in K$, $h \in H$.

(א) זוהי הגדרה טובה: לכל $g \in G$ יש הצגה יחידה $g = hk, h \in H, k \in K$,

(ב) α הומומורפיזם: יהיו $g_1, g_2 \in G$. אז יש $k_1, k_2 \in K$, $h_1, h_2 \in H$, כך ש־$g_2 = h_2 k_2$, $g_1 = h_1 k_1$. אז $g_1 g_2 = h_1 h_2 k_1 k_2$, לכן

$$\alpha(g_1 g_2) = \beta(h_1 h_2)\gamma(k_1 k_2) = \beta(h_1)\beta(h2)\gamma(k_1)\gamma(k_2) =$$

$$\beta(h_1)\gamma(k_1)\gamma(h_2)\gamma(k_2) = \varphi(g_1)\varphi(g_2)$$

(ג) α חח"ע: יהיו h, k כך ש־$\alpha(hk) = 1$. אז $\beta(h)\gamma(k) = 1$. כיוון ש־$\beta(h) \in H, \gamma(k) \in K$ ול־1 יש הצגה יחידה כמכפלה של אברי H, K, יוצא $\beta(h) = 1, \gamma(k) = 1$). אבל β, γ חח"ע, לכן $h = 1, k = 1$ ומכאן $hk = 1$.

(ד) $\varphi(\alpha) = (\beta, \gamma)$: אכן, לכל $h \in H$ מתקיים $\alpha(h) = \beta(h)\gamma(1) = \beta(h)1 = \beta(h)$, לכן $\alpha|_H = \beta$. באופן דומה $\alpha|_K = \gamma$.

מתוך (א), (ב), (ג) נובע ש־$\alpha \in \mathrm{Aut}(G)$. זה, יחד עם (ד) מוכיח ש־φ על.

מתוך (1),(2), (3), נובע ש־φ איזומורפיזם. ∎

שאלה 5: תהי A חבורה אבלית חפשית ויהי $\{e_1, e_2, e_3\}$ בסיס שלה. יהי $a = 2e_1 + 7e_3$ ויהי $b = 3e_2 + 5e_3$. הוכיחו שקיים אוטומורפיזם φ של A כך ש־$\varphi(a) = b$.

פתרון: די להשלים את a לבסיס $a_1 = a, a_2, a_3$ ואת b_1 לבסיס $b_1 = b, b_2, b_3$ של A. אכן, אז קיימים הומומורפיזמים יחידים $\varphi, \psi\colon A \to A$ כך ש־$\varphi(a_i) = b_i$, $\psi(b_i) = a_i$, $i = 1, 2, 3$. ההרכבות $\varphi \circ \psi$ ו־$\psi \circ \varphi$ מעתיקות בסיס של A על עצמו, ולכן, לפי היחידות של הומומורפיזמים, הן שוות ל־id_A. בפרט ל־φ יש הופכי ψ ולכן הוא אוטומורפיזם.

כעת, e_1, e_2, e_3 בסיס, לכן, לפי תרגיל בהרצאה, לכל $\alpha, \beta \in \mathbb{Z}$, גם $e_1 + \alpha e_3, e_2, e_3$ בסיס, ואז גם $e_1 + \alpha e_3, e_2, e_3 + \beta(e_1 + \alpha e_3)$ בסיס. אם נקח $\beta = 2, \alpha = 3$ אז האיבר האחרון בבסיס זה הוא a.

אם נחליף בפסקה הקודמת בין e_1 ל־e_2, נקבל כי $e_2 + \alpha e_3, e_1, e_3 + \beta(e_2 + \alpha e_3)$ בסיס. (אך אין $\alpha, \beta \in \mathbb{Z}$ כך שהאיבר האחרון בבסיס זה הוא b, אחרת היה $\beta = 3$, ו־$\alpha\beta + 1 = 5$, כלומר, $3\alpha = 4$, סתירה. לכן:) נבצע עוד שינוי אחד של בסיס: $e_2 + \alpha e_3 + \gamma\big(e_3 + \beta(e_2 + \alpha e_3)\big), e_1, e_3 + \beta(e_2 + \alpha e_3)$ בסיס, לכל $\gamma \in \mathbb{Z}$. האיבר הראשון בבסיס זה הוא $(1 + \beta\gamma)e_2 + (\alpha + \gamma + \alpha\beta\gamma)e_3$. כדי שהוא יהיה שווה ל־$b$, צריך להתקיים $3 = 1 + \beta\gamma$, כלומר, $\beta\gamma = 2$, ואז $5 = \alpha + \gamma + \alpha\beta\gamma = 3\alpha + \gamma$. ניקח, למשל, $\gamma = 2$, $\alpha = 1$, $\beta = 1$, אז התנאים מתקיימים. ∎

שאלה 6: (א) הוכיחו שלכל חבורה מסדר $154 = 2 \cdot 7 \cdot 11$ יש תת חבורה מסדר $77 = 7 \cdot 11$.

(ב) מיינו, עד כדי איזומורפיזם, חבורות מסדר 154.

פתרון: (א) תהי G מסדר $2 \cdot 7 \cdot 11$. עבור $p = 2, 7, 11$ נסמן ב־n_p מספר חבורות סילוב־p של G ותהי P_p אחת מהן. לפי המשפט השלישי של סילוב, $n_{11} \equiv 1 \pmod{11}$ וגם $n_{11} | \frac{|G|}{|P_{11}|} = 2 \cdot 7$, לכן $n_{11} = 1$.

מכאן ש־$G \triangleleft P_{11}$. לכן $H := P_7P_{11} \leq G$ (שאלה 2). כיוון ש־P_7, P_{11} מסדרים זרים, $P_7 \cap P_{11} = 1$. לכן $H = P_{11} \rtimes P_7$. אך כיוון ש־$7 \nmid 11-1$, לפי תרגיל בהרצאה [תרגיל 13.10], $H = P_7 \times P_{11}$. בפרט $H \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}/77\mathbb{Z}$. לכן $|H| = 77$.

(ב) כיוון ש־$(G:N) = 2$, מתקיים $H \triangleleft G$. לכן $HP_2 \leq G$. אבל P_2, H מסדרים זרים, לכן $H \cap P_2 = 1$, ולכן $HP_2 = H \rtimes P_2$. תת חבורה זו של G היא מסדר $|P_2| \cdot |H| = 2 \cdot 77 = |G|$, לכן $G = H \rtimes P_2$.

המבנה של G כמכפלה חצי ישרה נקבע על ידי הומומורפיזם $\psi\colon P_2 \to \operatorname{Aut}(H)$. יהי z היוצר של P_2; אז $P_2 = \{1, z\}$ ו־ψ כזה נתון על ידי $\varepsilon := \psi(z)$ המקיים $\varepsilon^2 = 1$ (ו־$\psi(1) = 1$). כיוון ש־P_7, P_{11} מסדרים זרים ו־$H = P_7 \times P_{11}$, לפי משפט בהרצאה [למה 10.4(ב)] יש איזומורפיזם $\operatorname{Aut}(H) \to \operatorname{Aut}(P_7) \times \operatorname{Aut}(P_{11})$ על ידי $\alpha \mapsto (\alpha|_{P_7}, \alpha|_{P_{11}})$; מתקיים $\alpha^2 = 1$ אם ורק אם $(\alpha|_{P_{11}})^2 = 1$, $(\alpha|_{P_7})^2 = 1$.

כעת, P_7 מעגלית מסדר 7, ויש לה אוטומורפיזם β מסדר 2, הנתון על ידי $h \mapsto h^{-1}$; זהו האוטומורפיזם היחיד מסדר 2 שלה, כי $\operatorname{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$ מעגלית ולכן יש לה תת חבורה יחידה מסדר 2. מתקיים $\beta(h) = h$ אם ורק אם $h = 1$. באותו אופן, יהי γ האוטומורפיזם היחיד מסדר 2 של P_{11}; גם הוא נתון על ידי $h \mapsto h^{-1}$ ומתקיים $\gamma(h) = h$ אם ורק אם $h = 1$.

לכן יש בדיוק 4 אוטומורפיזמים ε של H כך ש־$\varepsilon^2 = 1$:

(א) $\varepsilon := \varepsilon_1 = (1,1)$ הנתון על ידי ${}^{\varepsilon}(h_1, h_2) = (h_1, h_2)$, באשר $h_1 \in P_7, h_2 \in P_{11}$,

(ב) $\varepsilon := \varepsilon_2 = (\beta, 1)$ הנתון על ידי ${}^{\varepsilon}(h_1, h_2) = (h_1^{-1}, h_2)$,

(ג) $\varepsilon := \varepsilon_3 = (1, \gamma)$ הנתון על ידי ${}^{\varepsilon}(h_1, h_2) = (h_1, h_2^{-1})$,

(ד) $\varepsilon := \varepsilon_4 = (\beta, \gamma)$ הנתון על ידי ${}^{\varepsilon}(h_1, h_2) = (h_1^{-1}, h_2^{-1})$,

זה נותן 4 חבורות. עלינו להוכיח שאין ביניהן חבורות איזומורפיות.

נשים לב ש־H היא התת חבורה היחידה של G מאינדקס 2. אכן, אם $(G:N) = 2$ אז לפי משפט האיזומורפיזם השני $(H : (H \cap N)) = (NH : N) | (G:N) = 2$, אבל H מסדר אי זוגי, לכן גם $(H : (H \cap N))$ אי זוגי ולכן הוא 1. ומכאן $H = H \cap N$. בפרט $H \leq N$ ולכן $H = N$.

נבחר $c \in G \setminus H$ ונגדיר $C = \{h \in H |\ {}^{c}h = h\}$. הגדרה זו אינה תלויה בבחירת c, כי אם $c' \in G \setminus H$, יש $h' \in H$ כך ש־$c' = h'c$ ואז $h^{c'} = (h^{h'})^c = h^c$, לכל $h \in H$, כי H חילופית. לכן בלי הגבלת הכלליות $c = \psi(z) = \varepsilon$.

כעת C הוא, לפי המקרים לעיל, (א) $C = H$, (ב) $C = P_{11}$, (ג) $C = P_7$, (ד) $C = \{1\}$. כייון שחבורות אלה מסדרים שונים, החבורות בארבעת המקרים אינן איזומורפיות. ∎

בהצלחה!