פתרון מטלה 05 — מבנים אלגבריים (2), 80446

10 במאי 2025

שאלה 1

סעיף א׳

נוכיח שחבורה אבלית סופית היא מכפלה ישרה של חבורות ה־p־סילו שלה.
נסיק שאם $n = p_1^{k_1} \cdots p_r^{k_r}$ פירוק לחזקות ראשוניים שונים אז $\mathbb{Z}_{/p_1^{k_1}} \times \cdots \times \mathbb{Z}_{/p_r^{k_r}} \simeq \mathbb{Z}_{/n}$, ואף שהאיזומורפיזם φ המעיד על כך מקיים,

$$\varphi(\{(x_1, \dots, x_r) \mid \forall 1 \le i \le r, \langle x_i \rangle = \mathbb{Z}_{/p_i^{k_i}}\}) = \{x \in \mathbb{Z}_{/n} \mid \langle x \rangle = \mathbb{Z}_{/n}\}$$

הוכחה. נניח ש־$p_1, \dots, p_n$ הראשוניים המחלקים את $|G|$, עבור חבורה אבלית סופית G. נניח גם ש־n_i מספר חבורות p_i־סילו של G. אנו יודעים שכל חבורות p_i־סילו הן צמודות אחת לשנייה ולכן אם $P, Q \le G$ חבורות p_i סילו שלה אז קיים $g \in G$ כך ש־$gPg^{-1} = Q$. אבל G אבלית ולכן לכל $h \in P$ נקבל $gpg^{-1} = p$ ונסיק ש־$P = Q$, כלומר $n_{p_i} = 1$. נגדיר $P_i \le G$ החבורה היחידה p_i־סילו של G לכל i.

נראה שאכן $G \simeq P_1 \times \cdots \times P_n$. אנו כבר יודעים שמתקיים $G = P_1 \cdots P_n$ מאבליות.
נניח ש־$i < j \le n$ ונבחן את $P_i \cap P_j$. אם קיים $e \ne g \in P_i \cap P_j$ נקבל שהסדר של g הוא p_i וגם p_j ולכן $p_i = p_j$ בסתירה להגדרתם, ולכן $P_i \cap P_j = \{e\}$ לכל $i \ne j$.
עוד נבחין כי ממשפט סילו השני $P_i \trianglelefteq G$ לכל $i \le n$.
נסיק מהאפיון למכפלות ישרות ש־$G \simeq P_1 \times \cdots \times P_n$.

מאפיון של חבורות $\mathbb{Z}_{/n}$ אנו יודעים ש־$H \le \mathbb{Z}_{/n}$ אם ורק אם $H \simeq \mathbb{Z}_{/d}$ עבור $n \mid d$, ולכן נסיק ש־$P_i = \mathbb{Z}_{p_i^{k_1}}$ לכל i וכאשר k_i מקסימלי בחלוקה $p_i^{k_i} \mid n$. נניח ש־$\varphi : \mathbb{Z}_{/p_1^{k_1}} \times \cdots \times \mathbb{Z}_{/p_r^{k_r}} \to \mathbb{Z}_{/n}$ האיזומורפיזם המעיד על כך. נניח ש־$(x_1, \dots, x_r)$ איברים כך ש־$\langle x_i \rangle = \mathbb{Z}_{p_i^{k_i}}$ לכל $i \le r$. אז הסדר של $(x_1, \dots, x_r)$ הוא n ולכן נוכל להסיק שגם $\varphi(x_1, \dots, x_r)$ מסדר n, כלומר בהכרח $\langle \varphi(x_1, \dots, x_r) \rangle = \mathbb{Z}_{/n}$ בלבד.
מהצד השני נניח ש־$x \in \mathbb{Z}_{/n}$ כך ש־$\langle x \rangle = \mathbb{Z}_{/n}$. נגדיר גם $x_i = \pi_i(x)$ עבור הומומורפיזם ההטלה $\pi_i : \mathbb{Z}_{/n} \to \mathbb{Z}_{/p_i^{k_i}}$ לכל i. משיקולי סדר דומים בהכרח $\langle x_i \rangle = \mathbb{Z}_{/p_i^{k_1}}$ ולכן נקבל שאכן מתקיים,

$$\varphi(\{(x_1, \dots, x_r) \mid \forall 1 \le i \le r, \langle x_i \rangle = \mathbb{Z}_{/p_i^{k_i}}\}) = \{x \in \mathbb{Z}_{/n} \mid \langle x \rangle = \mathbb{Z}_{/n}\}$$

כפי שרצינו להוכיח. $\square$

סעיף ב׳

נראה ש־$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, וכן שאם $n = p_1^{k_1} \cdots p_r^{k_r}$ פירוק לחזקות ראשוניים שונים אז,

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^\times$$

הוכחה. נגדיר את ההעתקה $\sigma : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times$, על־ידי $\sigma(\varphi) = \varphi(1)$. נבחין כי לכל $\varphi, \psi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$,

$$\sigma(\varphi \circ \psi) = \varphi(\psi(1)) = \varphi(\underline{k}) = k \cdot \varphi(1) = \varphi(1) \cdot \psi(1)$$

כאשר $\underline{k}$ הנמרטור המייצג את $\psi(1)$. נסיק ש־σ הומומורפיזם חבורות, נרצה להראות שהוא חד־חד ערכי ועל.
נניח ש־$\sigma(\varphi) = \sigma(\psi)$, אז $\varphi(1) = \psi(1)$ ונסיק ישירות ש־$\varphi = \psi$, לכן σ חד־חד ערכית.
יהי $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, אז נגדיר $\varphi(x) = k \cdot x$, זהו אוטומורפיזם פנימי וכן $\sigma(\varphi) = k$, ולכן σ על.
נסיק ש־$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

אנו יודעים שאם $G = H \times K$ אז $\mathrm{Aut}\, G \simeq \mathrm{Aut}\, H \times \mathrm{Aut}\, K$ ישירות מהגדרת אוטומורפיזם והרכבת איזומורפיזם עליו. נוכל להרחיב את המכפלה הזו לכל כמות סופית של מכפלות, ונסיק,

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Aut}(\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \cdots \times \mathrm{Aut}(\mathbb{Z}/p_r^{k_r}\mathbb{Z}) \simeq (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^\times$$

ואכן קיים איזומורפיזם. $\square$

סעיף ג׳

תהי $(A, +)$ חבורה אבלית סופית. נסיק שאם לכל p ראשוני כך ש־$p \mid |A|$ מתקיים,

$$A[p] = \{a \in A \mid \exists k \in \mathbb{N}, p^k a = 0\}$$

היא ציקלית, אז A ציקלית.

הוכחה. נתון כי $A[p]$ ציקלית לכל p, ונבחין כי $p^k = 0$ עבור k מקסימלי כלשהו, לכן $1 \in A[0]$, ונסיק ש־$|A[p]| = p^k$, כלומר זוהי חבורת p־סילו של A. אילו נבחר $(1, \ldots, 1)$ אז $x \in A$ $\varphi(1, \ldots, 1) = x$ עבור φ מסעיף א'. אבל מהמסקנה של אותו סעיף נובע ש־$A = \langle x \rangle$, כלומר x מעיד על הציקליות של A. $\square$

סעיף ד'

נראה שאם $(A, +)$ חבורה אבלית מסדר p^n עבור p ראשוני כלשהו, וגם של־A יש תת־חבורה ציקלית יחידה מסדר p, אז A ציקלית.

הוכחה. יהי $a \in A$, ונניח כי $a \notin \langle b \rangle$ עבור $b \in A$ כך ש־$o(b) = p$. אז $o(a) \neq p$, אחרת נקבל ש־$\langle a \rangle$ מסדר p ולכן $a \in \langle b \rangle$. אילו $o(a) = p^k$ עבור $1 < k < n$ אז נקבל $\langle a \rangle$ חבורה ציקלית מסדר p^k. אבל מאפיון חבורות־p אנו יודעים שקיימת $H \leq \langle a \rangle \leq A$ כך ש־$|H| = p$, ולכן H ציקלית, אבל $a \notin \langle b \rangle$ ולכן $H \neq \langle b \rangle$ וקיבלנו סתירה להנחה. לכן בהכרח $k = n$ ונובע ש־A עצמה ציקלית. $\square$

סעיף ה'

נראה שאם $(A, +)$ חבורה אבלית כך שלכל $p \mid A$ מתקיים ש־$A[p]$ אבלית, עם תת־חבורה ציקלית יחידה מסדר p, אז A ציקלית.

הוכחה. מסעיף ד' נובע ש־$A[p]$ ציקלית לכל $p \mid |A|$, ומסעיף ג' נובע ש־A ציקלית. $\square$

שאלה 2

נניח ש־$p_1, \dots, p_n$ ראשוניים זרים, נוכיח בסעיפים הבאים כי,

$$\mathbb{Q}(\sqrt{p_1} + \cdots + \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) = L$$

סעיף א'

נראה שאם $\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}$ אז יש אוטומורפיזם, φ_n, של L ששולח את $\sqrt{p_i}$ ל־$\epsilon_i \sqrt{p_i}$ לכל i.

הוכחה. נראה את הטענה באינדוקציה על n. עבור $n = 0$ הטענה טריוויאלית.

נניח שקיים אוטומורפיזם של $L_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ השולח את $\sqrt{p_i}$ ל־$\epsilon_i \sqrt{p_i}$ ונראה שעבור p_{n+1} ו־ϵ_{n+1} ניתן להרחיב את האוטומורפיזם הזה על,

$$L_{n+1} = L_n(\sqrt{p_{n+1}}) \simeq L_n[x]/(x^2 - p_{n+1})$$

כאשר האיזומורפיזם האחרון נובע מהעובדה שזהו הפולינום המינימלי של $\sqrt{p_{n+1}}$. נסיק אם כך ש־$L_n(\sqrt{-p_{n+1}}) \simeq L_n[x]/(x^2 - p_{n+1})$ ולכן נובע ש־$L_{n+1} \simeq L_n(\epsilon_i \sqrt{p_{n+1}})$. משאלה 3 במטלה 3 נוכל להסיק אף ש־$L_{n+1} = L_n(\epsilon_i \sqrt{p_{n+1}})$.

נגדיר $\varphi_{n+1} : L_{n+1} \to L_{n+1}$ על־ידי $\varphi_{n+1} \restriction L_n = \varphi_n$ וכן $\varphi_{n+1}(\sqrt{p_{n+1}}) = \epsilon_i \sqrt{p_{n+1}}$. זהו L_n־הומומורפיזם. מהעובדה שיש שוויון בין השדות, נוכל להסיק שבפרט קיים אוטומורפיזם, וזהו אוטומורפיזם כזה. $\square$

סעיף ב'

נראה שאם $\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}$ אז $\sum_{i=1}^n \epsilon_i \sqrt{p_i}$ צמוד של $\sum_{i=1}^n \sqrt{p_i}$ מעל $\mathbb{Q}$, ונסיק שיש להם את אותו הפולינום המינימלי.

הוכחה. אנו יודעים כי קיים אוטומורפיזם $\varphi : L \to L$ כך ש־$\varphi(\sqrt{p_i}) = \epsilon_i \sqrt{p_i}$ לכל i.

$$\varphi\left(\sum_{i=1}^n \sqrt{p_i}\right) = \sum_{i=1}^n \epsilon_i \sqrt{p_i}$$

מהגדרת φ. אבל מלמה מההרצאה נובע בהכרח שבשדות נורמליים איברים עוברים לצמודים שלהם בלבד. אנו טוענים ש־L נורמלית, זאת שכן נוכל לאפיין באותו אופן של סעיף א' את כל האוטומורפיזמים של L מעל $\overline{L}$, ונקבל שהתמונה תמיד זהה. נסיק אם כך שאכן שני האיברים צמודים, ולכן מהגדרת צמידות יש להם פולינום מינימלי משותף. $\square$

סעיף ג'

נחשב את דרגת הפולינום המינימלי, f, של $\sqrt{p_1} + \cdots + \sqrt{p_n}$ ונסיק את הטענה הראשית.

הוכחה. נבחין כי לכל בחירת ϵ_i נקבל ש־$\epsilon_1 \sqrt{p_1} + \cdots + \epsilon_n \sqrt{p_n}$ איבר צמוד של $\sqrt{p_1} + \cdots + \sqrt{p_n}$. נובע אם כך ש־$\deg_{\mathbb{Q}} f \ge 2^n$. אבל מתכונות של פולינום מינימלי שראינו בהרצאה ידוע גם כי $\deg_{\mathbb{Q}} f \le 2^n$, על־ידי שימוש בתכונות על חסמי פולינום מינימלי ביחס לפעולות החיבור והכפל, ולכן $\deg_{\mathbb{Q}} f = 2^n$.

אנו יודעים שדרגת L היא 2^n כמגדל הרחבות, וכן $\sqrt{p_1} + \cdots + \sqrt{p_n} \in L$, ולכן נוכל להסיק שמתקיים,

$$\mathbb{Q}(\sqrt{p_1} + \cdots + \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) = L$$

כפי שרצינו. $\square$

שאלה 3

בכל סעיף נגדיר $f \in \mathbb{Q}[x]$ ונוכיח ש־f אי־פריק. נניח ש־$\alpha \in \mathbb{C}$ שורש של f ונגדיר $K = \mathbb{Q}(\alpha)$, נבדוק האם K/A הרחבה נורמלית.

סעיף א׳

נגדיר $f(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5-1}{x-1}$.

פתרון f הוא הפולינום הציקלוטומי מסדר 5, זהו סדר ראשוני ולכן מטענה מהרצאה נובע שהוא אי־פריק.

השורשים של f מעל $\mathbb{C}$ הם ω^n עבור $\omega = \exp(\frac{2\pi i n}{5})$ ו־$1 \le n \le 4$. לכל $q \in \mathbb{Q}$ אנו יודעים כי $f_{q/\mathbb{Q}}$ מתפצל לחלוטין מעל $\mathbb{Q}(\alpha)$ ולכן עלינו לבדוק רק את ω. אנו יודעים כי $f_{\omega/\mathbb{Q}}(x) = x^5 - 1$, מעקרון שובך היונים והעובדה ש־$o(\alpha) = 5$ נסיק ש־$\omega \in \mathbb{Q}(\omega^n)$ ולכן $f_{\omega/\mathbb{Q}}$ מתפצל לחלוטין בשדה זה, ונסיק שהוא נורמלי.

סעיף ב׳

נגדיר $f(x) = x^4 - 7x^2 + 7$.

פתרון נבחין כי,

$$x^2 = \frac{7 \pm \sqrt{49-28}}{2} = \frac{7 \pm \sqrt{21}}{2}$$

ולכן,

$$x = \pm\sqrt{\frac{7 \pm \sqrt{21}}{2}}$$

מבדיקה ישירה נקבל שאף מכפלת שורשים של f היא לא רציונלית, ולכן נוכל להסיק ש־f אי־פריק מעל $\mathbb{Q}$.

יהי α שורש של f. נסמן $\beta = \alpha^2$, נסמן,

$$\beta_1 = \frac{7+\sqrt{21}}{2}, \quad \beta_2 = \frac{7-\sqrt{21}}{2}$$

ונניח בלי הגבלת הכלליות ש־$\alpha = \beta_1$ (אחרת ההוכחה זהה). נבדוק אם $\sqrt{\beta_2} \in \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\beta_1})$.

$$\sqrt{\beta_2} = \sqrt{7 - \beta_1}$$

ולכן נוכל להסיק $f_{\sqrt{\beta_2}/\mathbb{Q}(\alpha)} = x^2 - 7 + \sqrt{\alpha}$ וזהו פולינום אי־פריק ולכן לא כל שורשי f ב־$\mathbb{Q}(\alpha)$ ונובע שהוא לא נורמלי מעל $\mathbb{Q}$.

סעיף ג׳

נגדיר $f(x) = x^4 - x - 1$.

פתרון אילו f פריק ב־$\mathbb{Q}$ אז הוא פריק גם ב־$\mathbb{F}_2[x]$ (1.4.2). נבחין כי ב־$\mathbb{F}_2[x]$ גם $f(x) = x^4 + x + 1$. בהצבה נקבל $f(x) = 1$ לכל $x \in \mathbb{F}_2$, ולכן אם f פריק אז הוא מכפלת פולינומים מסדר 2. אבל הוא לא מכפלה של x^2, x^2+x, x^2+1 שכן להם יש שורש, ונשאר לבדוק את x^2+x+1. אבל ישירות מחלוקת פולינומים נקבל שפולינום זה לא מחלק את f ולכן f אי־פריק מעל $\mathbb{F}_2[x]$ ומהמשפט לא פריק ב־$\mathbb{Q}$.

נבחין כי $f'(x) = 4x^3 - 1$ ולכן הנגזרת מונוטונית עולה ונסיק של־f יש אפס או שני שורשים בלבד, אבל בהצבה נקבל $f(0) = -1 < 0$ וכן $f(2) = 13 > 0$ ולכן יש בדיוק שני שורשים ל־f. שורשים אלה הם שניהם ממשיים, אבל משימוש במשפט רושה על תחום פתוח שלא כולל את הציר הממשי והפולינום $g(z) = z^4$ נוכל להסיק שיש לפחות שורש מרוכב אחד, ובהתאם למסקנה מהתרגול ההרחבה $\mathbb{Q}(\alpha)/\mathbb{Q}$ לא נורמלית.

שאלה 4

יהי K שדה כך ש־μ_∞ מתפצלת, ולכן לכל שורש יחידה $z \in \overline{K}$ גם $z \in K$. נסמן $p = \mathrm{char}(K)$ אם המציין של K חיובי ו־$p = 1$ אחרת.
נוכיח כי $\mu_\infty(K) \simeq \mathbb{Q}/(\mathbb{Z}[\frac{1}{p}])$.

הוכחה. במקרה $p = 1$ אנו רוצים להראות כי $\mu_\infty(K) \simeq \mathbb{Q}/\mathbb{Z}$. לכל $n \in \mathbb{N}$, כל $\mu_n \le \mu_\infty$ היא חבורה ציקלית, נקבע את אחד מהשורשים הפרימיטיביים ב־μ_n, נסמן ω_n, ונגדיר את $\varphi_n : \mu_n \to \mathbb{Q}/\mathbb{Z}$ על־ידי $\varphi_n(\zeta) = \frac{k}{n}$ כאשר $\zeta = \omega_n^k$. עתה נגדיר $\varphi : \mu_\infty(K) \to \mathbb{Q}/\mathbb{Z}$, לכל $\zeta \in \mu_\infty$ נבחר n כך ש־$\zeta \in \mu_n$ ונגדיר $\varphi(\zeta) = \varphi_n(\zeta)$. אנו יודעים כבר כמסקנה מהרצאה ש־φ כזו היא מוגדרת היטב, נשאר להראות שהיא איזומורפיזם. לכל $\zeta, \eta \in \mu_\infty$ קיים $n \in \mathbb{N}$ כך ש־$\zeta, \eta \in \mu_n$, זאת על־ידי בחירת $\mathrm{lcm}(m, l)$ עבור סדרים של שני האיברים. אז מתקיים,

$$\varphi(\zeta \cdot \eta) = \varphi_n(\zeta \cdot \eta) = \frac{k_1 + k_2}{n} = \frac{k_1}{n} + \frac{k_2}{n} = \varphi_n(\zeta) + \varphi_n(\eta) = \varphi(\zeta) + \varphi(\eta)$$

ונסיק ש־φ הומומורפיזם.
נניח ש־$\zeta, \eta \in \mu_\infty$ כך ש־$\zeta \ne \eta$, אז,

$$\varphi(\zeta) = \frac{k_1}{n} \ne \frac{k_2}{n} = \varphi(\eta)$$

ולכן נסיק חד־חד ערכיות.
לכל $\frac{k}{n}$ אנו יודעים ש־$1 \in K$ שורש יחידה מסדר n וכן שהוא מתפצל לחלוטין, ולכן נבחר $\zeta \in \mu_n$ מתאימה ונקבל $\varphi(\zeta) = \frac{k}{n}$ ונסיק על, לכן,

$$\mu_\infty(K) \simeq \mathbb{Q}/\mathbb{Z}$$

במקרה $p > 1$ ההוכחה דומה ומשתמשת בלמה 6.1.7. אנו יודעים ש־$\mu_n \simeq \mathbb{Z}/m\mathbb{Z}$ עבור $n = p^l m$ כך ש־$\gcd(m, p) = 1$. בהתאם גם $m = \frac{n}{p^l}$ ונוכל ליצור העתקה $\varphi_n : \mu_n \to \mathbb{Q}/(\mathbb{Z}[\frac{1}{p}])$. שאר ההוכחה זהה. $\square$