

# פתרון מבחן בקורס 88-311 שדות ותורת גלואה

מועד א', תשפ"ב

מרצה: פרופ' בוריס קוניאבסקי

מתרגל: גיא בלשר

**הוראות:** יש לענות על 4 מתוך 5 השאלות הבאות. לכל השאלות משקל שווה. ענו על כל שאלה שבחרתם פתרון מלא ומנומק. כתבו את תשובותיכם במחברת הבחינה. התחילו את התשובה לכל שאלה בעמוד נפרד, וציינו בתחילת כל עמוד את מספר השאלה המתאימה. משך המבחן: שעתיים וחצי. חומר עזר מותר: מחשבון פשוט בלבד.

בהצלחה!

---

**שאלה 1.** יהי  $F$  שדה, יהי  $p$  מספר ראשוני, יהי  $f \in F[x]$  פולינום ממעלה  $p$ , ויהי  $K$  שדה הפיצול של  $f$ . נניח כי  $[K : F] = tp$  לאיזשהו  $t > 1$  טבעי.

א. (12 נק') הוכיחו כי אי-פריק מעל  $F$ .

ב. (13 נק') הוכיחו כי ההרחבה  $K/F$  ספרבילית.

פתרון.

א. נניח בשלילה כי  $f$  פריק מעל  $F$ . נכתוב  $f = f_1 f_2$  כאשר  $f_1, f_2 \in F[x]$  פולינומים ממעלה קטנה מ- $p$ . נסמן על ידי  $K_1$  את שדה הפיצול של  $f_1$  מעל  $F$ ; אז  $K$  הוא שדה הפיצול של  $f_2$  מעל  $K_1$ . מכפלויות המימד,

$$[K : F] = [K : K_1] \cdot [K_1 : F]$$

$K_1$  הוא שדה הפיצול של  $f_1$  מעל  $F$ , ו- $\deg f_1 < p-1$ , לכן  $[K_1 : F] < p$  (אכן, נכתוב  $[F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})] \leq \deg f_1 < p$ , לכל  $i$ ;  $K_1 = F(\alpha_1, \dots, \alpha_m)$  ו- $[K_1 : F]$  הוא מכפלת כל המימדים האלו). בדומה,  $[K : K_1] < p$ . אבל  $[K : F] > p$ , בסתירה.

ב. בה"כ, נניח כי הפולינום  $f$  מתוקן (כי כפל בסקלר אינו משנה את שדה הפיצול). נסמן  $K = F(a_1, \dots, a_n)$ , כאשר  $a_1, \dots, a_n$  הם כל השורשים של  $f$ . מסעיף א', אי-פריק, ולכן  $f$  הוא הפולינום המינימלי של כל  $a_i$  מעל  $F$ . לכן  $K/F$  היא ספרבילית אם ורק אם  $a_1, \dots, a_n$  ספרביליים מעל  $F$ , אם ורק אם  $f$  ספרבילי מעל  $F$ . נניח בשלילה ש- $f$  אינו ספרבילי מעל  $F$ . ממשפט מההרצאה, בהכרח  $\text{char} F = p$  ו- $f(x) = x^p - b$  לאיזשהו  $b \in F$ . כיוון שאנחנו במאפיין  $p$ , מתקיים  $(x - a_1)^p = x^p - a_1^p = x^p - b = f(x)$ , כלומר ל- $f(x)$  יש שורש יחיד. אבל אז  $K = F(a_1)$ , ו- $[K : F] = p-1$ , בסתירה לנתון. לכן  $f$  ספרבילי מעל  $F$ , ומההסבר בתחילת הסעיף נקבל שההרחבה  $K/F$  ספרבילית.

**שאלה 2.** (25 נק') הוכיחו או הפריכו: יהי  $F$  שדה, ותהי  $E = F(\alpha)$  הרחבה סופית של  $F$ . נניח כי  $[E : F]$  אינו מתחלק ב-2 וב-3. אז  $E = F(\alpha^3)$ .

פתרון. הוכחה. נתנו במגדל השדות  $F \subseteq F(\alpha^3) \subseteq E = F(\alpha)$ . מכפלות המימד,

$$[E : F] = [E : F(\alpha^3)] \cdot [F(\alpha^3) : F] = [F(\alpha) : F(\alpha^3)] \cdot [F(\alpha^3) : F]$$

נשים לב כי  $[F(\alpha) : F(\alpha^3)] \leq 3$ , כי  $\alpha$  שורש של הפולינום  $f(x) = x^3 - \alpha^3$ . כיוון ש- $[E : F]$  אינו מתחלק ב-2 וב-3, נקבל ש- $[F(\alpha) : F(\alpha^3)] = 1$ , כלומר  $E = F(\alpha) = F(\alpha^3)$ .

**שאלה 3.** יהי  $f(x) = x^3 - 10 \in F[x]$ . חשבו את חבורת גלואה של שדה הפיצול של  $f$  מעל  $F$ , במקרים הבאים:

א.  $F = \mathbb{Q}$  (נק' 13)

ב.  $F = \mathbb{Q}(\sqrt{-3})$  (נק' 12)

פתרון.

א. השורשים של  $f$  הם  $\sqrt[3]{10}, \sqrt[3]{10}\zeta_3, \sqrt[3]{10}\zeta_3^2$ , כאשר  $\zeta_3$  שורש יחידה פרימיטיבי מסדר 3. לכן שדה הפיצול של  $f$  מעל  $\mathbb{Q}$  הוא  $E = \mathbb{Q}(\sqrt[3]{10}, \zeta_3)$ . לפי מגדל השדות  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{10}) \subseteq E$  ניתן לראות כי

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{10})] \cdot [\mathbb{Q}(\sqrt[3]{10}) : \mathbb{Q}] = 2 \cdot 3 = 6$$

לכן  $\text{Gal}(E/\mathbb{Q})$  איזומורפית לתת-חבורה של  $S_3$  מסדר 6, ומכאן שהיא איזומורפית ל- $S_3$ .

ב. נשים לב כי  $\zeta_3 = \frac{1}{2} + \frac{\sqrt{-3}}{2}$ , ולכן  $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) = F$ . לכן שדה הפיצול של  $f$  מעל  $F$  הוא  $E = F(\sqrt[3]{10})$ . כיוון ש- $[F : \mathbb{Q}] = 2$ , מכפלות המימד נקבל ש- $[E : F] = 3$ . זה מראה ש- $\text{Gal}(E/F)$  היא חבורה מסדר 3, ומכאן שהיא חייבת להיות איזומורפית ל- $\mathbb{Z}/3\mathbb{Z}$ .

#### שאלה 4.

א. (13 נק') קבעו והוכיחו אילו מן הזוויות הבאות ניתנות לבנייה במחוגה וסרגל:  $1^\circ, 3^\circ, 5^\circ$ .

ב. (12 נק') יהי  $F$  שדה ממאפיין שונה מ-2. הוכיחו שאם  $\zeta_{2m+1} \in F$ , אז קיים גם  $\zeta_{2(2m+1)} \in F$ .  
(כאן מסמן שורש יחידה פרימיטיבי מסדר  $n$ .)

פתרון.

א. נזכור כי זווית  $\frac{2\pi}{n}$  ניתנת לבנייה אם ורק אם  $\cos \frac{2\pi}{n}, \sin \frac{2\pi}{n}$  ניתנים לבנייה, אם ורק אם  $\rho_n$  ניתן לבנייה. כמו כן, ניתן לבנייה אם ורק אם  $\text{Gal}(\mathbb{Q}(\rho_n)/\mathbb{Q})$  היא חבורת-2, אם ורק אם  $\varphi(n)$  הוא חזקת 2. נבדוק את שלושת המקרים בשאלה:

•  $1^\circ = \frac{2\pi}{360}$ : במקרה זה  $n = 360 = 2^3 \cdot 3^2 \cdot 5$ , כלומר

$$\varphi(360) = 360 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96$$

שאינו חזקת 2, לכן לא ניתן לבנות את  $1^\circ$ .

•  $3^\circ = \frac{2\pi}{120}$ : במקרה זה  $n = 120 = 2^3 \cdot 3 \cdot 5$ , כלומר

$$\varphi(120) = 120 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 120 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 32$$

חזקת 2, לכן ניתן לבנות את  $3^\circ$ .

•  $5^\circ = \frac{2\pi}{72}$ : במקרה זה  $n = 72 = 2^3 \cdot 3^2$ , כלומר

$$\varphi(72) = 72 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 72 \cdot \frac{1}{2} \cdot \frac{2}{3} = 24$$

שאינו חזקת 2, לכן לא ניתן לבנות את  $5^\circ$ .

ב. יהי  $\zeta_{2m+1}$  שורש יחידה פרימיטיבי מסדר  $2m+1$ . נתבונן ב- $a = -\zeta_{2m+1}$  או

$$a^n = 1 \iff (-\zeta_{2m+1})^n = 1 \iff \zeta_{2m+1}^n = (-1)^n$$

נשים לב כי  $\zeta_{2m+1}^{2(2m+1)} = 1 = (-1)^{2(2m+1)}$ , לכן  $a^{2(2m+1)} = 1$ . עוד נשים לב כי אם  $\zeta_{2m+1}^n = -1$ , אז  $\zeta_{2m+1}^{2n} = 1$ . לכן  $2n \mid (2m+1)$ , ומכאן  $(2m+1) \mid n$ . אך זו סתירה, כי אם  $n = k(2m+1)$ , אז  $\zeta_{2m+1}^n = (\zeta_{2m+1}^{2m+1})^k = 1$  והשדה איננו ממאפיין 2. לכן  $a^n = 1$  אם ורק אם  $n$  זוגי ו- $\zeta_{2m+1}^n = 1$ , אבל אז בהכרח  $n \geq 2(2m+1)$ . בסך הכל,  $o(a) = 2(2m+1)$ , כנדרש.

**שאלה 5.** יהי  $F$  שדה, יהי  $f(x) = (x^2 - a)(x^2 - b) \in F[x]$  פולינום (כאשר  $a, b \in F$ ), ויהי  $K$  שדה הפיצול של  $f$  מעל  $F$ . קבעו מהן האפשרויות ל- $[K : F]$ , כאשר:

א.  $F = \mathbb{Q}$  ('נק' 7).

ב.  $F = \mathbb{F}_2$  ('נק' 6).

ג.  $F = \mathbb{F}_4$  ('נק' 6).

ד.  $F = \mathbb{F}_{11}$  ('נק' 6).

פתרון. באופן כללי, לכל שדה  $F$  נטען כי  $[K : F]$  יכול להיות רק 1, 2 או 4. אכן, נסמן על ידי  $L$  את שדה הפיצול של  $x^2 - a$  מעל  $F$ . אז  $[L : F] \leq 2! = 2$ , וכיוון ש- $K$  הוא שדה הפיצול של  $x^2 - b$  מעל  $L$ , גם  $[K : L] \leq 2! = 2$ . זה מראה ש- $[K : F] = [K : L][L : F]$  יכול להיות רק מהאופציות 1, 2 או 4. נעבור על ארבעת הסעיפים:

א. עבור  $F = \mathbb{Q}$ : אפשר לקבל את כל האופציות הנ"ל. אכן,

• אם נבחר  $a = b = 0$ , נקבל ש- $K = \mathbb{Q}$ , ולכן  $[K : \mathbb{Q}] = 1$ ;

• אם נבחר  $a = 0, b = 2$ , נקבל ש- $K = \mathbb{Q}(\sqrt{2})$ , ולכן  $[K : \mathbb{Q}] = 2$ ;

• אם נבחר  $a = 2, b = 3$ , נקבל ש- $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , ולכן  $[K : \mathbb{Q}] = 4$  (כפי שראינו בתרגול).

ב. עבור  $F = \mathbb{F}_2$ : בהכרח  $[K : F] = 1$ , כלומר  $K = F$ . אכן, לכל  $a \in \mathbb{F}_2$  מתקיים  $x^2 - a = (x - a)^2$ , כלומר מתקיים  $f(x) = (x - a)^2(x - b)^2$ . לכן  $f$  מתפצל מעל  $F$ , ומכאן ש- $K = F$ .

ג. עבור  $F = \mathbb{F}_4$ : גם פה בהכרח  $[K : F] = 1$ . אפשר לבדוק ישירות שלכל  $a \in \mathbb{F}_4$ , הפולינום  $x^2 - a$  מתפצל מעל  $\mathbb{F}_4$ . בדרך אחרת, חבורת גלואה  $\text{Gal}(\mathbb{F}_4/\mathbb{F}_2)$  נוצרת על ידי אוטומורפיזם פרובניוס, שבמקרה הזה הוא מהצורה  $\sigma(x) = x^2$ . בפרט הוא על, ולכן לכל  $a \in \mathbb{F}_4$ , לפולינום  $x^2 - a$  יש שורש ב- $\mathbb{F}_4$ , ובפרט הוא מתפצל בו (כי הוא ממעלה 2).

ד. עבור  $F = \mathbb{F}_{11}$ : האפשרויות היחידות הן  $[K : F] = 1, 2$ . אכן, ראינו שמעל  $\mathbb{F}_p$ , כל פולינום ממעלה  $d$  מתפצל ב- $\mathbb{F}_{p^d}$ ; לכן  $f$  מתפצל ב- $\mathbb{F}_{11^2}$ , כלומר  $[K : F] \leq 2$ . כמובן, ייתכן  $[K : F] = 1$  (למשל עם  $a = b = 0$ ). כדי להוכיח שגם ייתכן  $[K : F] = 2$ , צריך להראות שקיים  $a \in \mathbb{F}_{11}$  שעבורו לפולינום  $x^2 - a$  אין שורש ב- $\mathbb{F}_{11}$ . אפשר לחשב זאת ישירות על ידי מעבר על כל האופציות, או לזכור שהחבורה הכפלית של השדה היא ציקלית,  $\mathbb{F}_{11}^* \cong \mathbb{Z}/10\mathbb{Z}$ , והריבועים של חבורה זו הם תת-חבורה מאינדקס 2 בה (ובפרט, לא כל האיברים הם ריבועים בה).