

### מעריך תרגול 11 מופשטת 3

**תרגיל 11.1** מצאו את תתי השדות של  $\mathbb{Q}(\rho)$  כאשר  $\rho = e^{\frac{2\pi i}{7}}$  הוא שורש 7 פרימיטבי של 1.

**פתרון:** במילים אחרות, מחפשים את שדות הביניים  $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\rho)$ . צריך להשתמש בהתאמת גלואה. הפולינום המינימלי של  $\rho$  הוא כזכור

$$x^6 + x^5 + \dots + 1$$

ו  $\mathbb{Q}(\rho)$  הוא שדה הפיצול שלו. לכן חבורת גלואה היא מסדר 6. בנוסף, היא פועלת טרנזיטיבית על השורשים  $\rho, \rho^2, \dots, \rho^6$ . נסמן ב  $\varphi_k$  את האיבר בחבורת גלואה שמקיים

$$\varphi_k(\rho) = \rho^k$$

אפשר לראות ש  $\varphi_k \rightarrow k$  מהווה איזומורפיזם של חבורות  $G = \text{Gal}(\mathbb{Q}(\rho), \mathbb{Q}) \cong U_7 \cong \mathbb{Z}_6$  (דרך אגב, זה נכון לכל  $p$  ראשוני ונשתמש בזה עוד בהמשך הקורס). ל  $\mathbb{Z}_6$  יש בדיוק שתי תתי חבורות לא טריויאליות שאיזומורפיות ל  $\mathbb{Z}_2, \mathbb{Z}_3$  בנוסף,  $\varphi_3$  הוא יוצר של  $G$  (כי 3 יוצר של  $U_7$ ) ולכן  $\varphi_3^2, \varphi_3^3$  יוצרים את תתי החבורות של  $G$ . אם נסמן  $E = \mathbb{Q}(\rho)$  אז שני שדות הביניים שאנחנו מחפשים הם

$$E^{\varphi_3^2}, E^{\varphi_3^3}$$

אפשר לחשב ש

$$\varphi_3^2(\rho) = \rho^2$$

$$\varphi_3^2(\rho^2) = \rho^4$$

$$\varphi_3^2(\rho^4) = 1$$

מכאן אפשר להסיק ש

$$\rho + \rho^2 + \rho^4$$

מיוצב ע"י  $\varphi_3^2$ . לכן

$$\mathbb{Q}(\rho + \rho^2 + \rho^4) \subseteq E^{\varphi_3^2}$$

ומשיקולי מימד יש שוויון.

באופן דומה אפשר לעשות אותו חישוב עבור  $\varphi_3^3$  ולקבל

$$\varphi_3^3(\rho) = \rho^6$$

$$\varphi_3^3(\rho^6) = 1$$

ולכן משיקולים דומים

$$E^{\varphi_3^3} = \mathbb{Q}(\rho + \rho^6)$$

ואלה שני שדות הביניים שחיפשנו. דרך אגב, שתיהן הרחבות נורמליות של  $\mathbb{Q}$ .

**תזכורת 11.2** כמה עובדות על שדות סופיים. שדה סופי חייב כמובן להיות ממאפיין  $p > 0$ . כל שדה סופי ממאפיין  $p$  הוא מגודל  $p^k$  כלשהוא. לכל  $k$  יש בדיוק שדה אחד מגודל  $p^k$  שהוא שדה הפיצול של הפולינום  $x^{p^k} - x$ . כל הרחבה היא הרחבת גלואה. חבורת גלואה היא תמיד ציקלית. לפעמים נסמן ב  $F_{p^k}$  את השדה מסדר  $p^k$ . חבורת גלואה

$$\text{Gal}(F_{p^k}/F) \cong \mathbb{Z}_k$$

נוצרת על ידי אוטומורפיזם פרוביניוס  $x \rightarrow x^p$ .

**תרגיל 11.3** בנה במפורט שדה בן 8 איברים.

**פתרון:** זה צריך להיות שדה ממאפיין 2, שהוא שדה הפיצול של  $x^8 - x$ .

$$x^8 - x = x(x-1)(x^6 + x^5 + \dots + 1)$$

נשים לב שכאן  $x^6 + x^5 + \dots + x + 1$  הוא פולינום פריק

$$(x^3 + x^2 + 1)(x^3 + x + 1)$$

(עם קצת ניסוי וטעיה). נשים לב ששני הפולינומים אי פריקים מעל  $F_2$ . השדה שלנו הוא

$$F_2[x]/(x^3 + x + 1)$$

כלומר בניה מפורשת שלו היא

$$a + bx + cx^2$$

$$\text{כאשר } x^3 = -1 - x$$

**תרגיל 11.4** מצאו את מימד שדה הפיצול של  $x^3 - 2$  מעל  $F_3, F_5, F_7$ . בכל מקרה תאר את הפעולה של האוטומורפיזמים היוצרים את חבורת גלואה.

**פתרון:** נסמן ב  $\alpha$  שורש של הפולינום בשדה הפיצול. נזכור ש  $F(\alpha)/F$  נורמלית ולכן זה שדה הפיצול  $F(\alpha)$  צריך להכיל את כל שורשי הפולינום. נותר רק לקבוע מה הגודל של  $F(\alpha)$ .

אם  $F = F_3$  אז הפולינום מתפרק

$$x^3 - 2 = (x - 2)^3$$

ולכן שדה הפיצול הוא  $F_3$  עצמו וחבורת גלואה טריוויאלית.

אם  $F = F_5$  אז הפולינום מתפרק

$$x^3 - 2 = (x - 3)(x^2 + 3x - 1)$$

$$x^2 + 3x - 1$$

הוא פולינום אי פריק ולכן זאת הרחבה ממימד 2 כלומר שדה הפיצול הוא

$$F_{25}$$

חבורת גלואה היא  $\mathbb{Z}_2$ . את אברי השדה אפשר לתאר כ

$$a + bx$$

ולכן אוטומורפיזם פרוביניוס  $x \rightarrow x^5$  מתואר ע"י הפעולה  $x^2 = -3x - 1$

$$\begin{aligned}\varphi(a + bx) &= a + bx^5 = a + bx(-3x - 1)(-3x - 1) = \\ &= a + bx(4x^2 + x + 1) = a + bx(-x - 3) = a + b(3x - 2) = a - 2 + 3bx\end{aligned}$$

$F = F_7$ . הפולינום  $x^3 - 2$  הוא אי פריק כי אם יש לו שורש ב  $F_7$  אז אותו שורש צריך לקיים

$$x^6 = 4$$

אבל מתורת החבורות אנחנו יודעים ש  $x^6 = 1$  (משפט לגרנז'). ולכן שדה הפיצול הוא השדה

$$F_7[x]/\langle x^3 - 2 \rangle \cong F_{7^3}$$

חבורת גלואה שלו היא  $\mathbb{Z}_3$ . את השדה אפשר לרשום כ

$$a + bx + cx^2$$

ואוטומורפיזם פרוביניוס  $x \rightarrow x^7$  פועל ככה:

$$\varphi(a + bx + cx^2) = a + bx^7 + cx^{14}$$

עכשיו

$$x^7 = xx^3x^3 = 4x$$

$$x^{14} = 16x^2 = 2x^2$$

ולכן בסה"כ יוצא

$$1 + 4bx + 2cx^2$$