# פתרון תרגיל בית 2 בשדות ותורת גלואה
# 88-311 סמסטר א' תשע"ט

**שאלה 1.** למי שרוצה להתנסות בעוד משחק של בניות בסרגל ומחוגה מוזמן לנסות את המשחק Euclidea. זה מספיק ממכר שכדאי לוודא שנשאר זמן לשאר תרגיל הבית.

**שאלה 2.** הוכיחו כי ניתן לבנות מצולע משוכלל עם $n$ צלעות אם ורק אם המספר $\cos\frac{2\pi}{n}$ בר־בנייה. רמז עבה: מצולע משוכלל החסום במעגל היחידה.

פתרון. נניח שניתן לבנות כזה מצולע משוכלל שמרכזו ב-$(0,0)$, ובלי הגבלת הכלליות אחד מקודקודיו הוא $(1,0)$, כי אנחנו יודעים להזיז קטעים ולהגדיל (או להקטין) אותם ביחס בר־בנייה. נביט על הקודקוד ה"ראשון" מעל ציר $x$ (אם זזים נגד כיוון השעון). נוריד ממנו אנך לציר $x$. הוא פוגש אותו בדיוק בנקודה $\left(\cos\frac{2\pi}{n},0\right)$. בכיוון השני, נצייר אנך לציר $x$ העובר דרך $(\cos\frac{2\pi}{n},0)$. נצייר מעגל ברדיוס $1$ שמרכזו בראשית הצירים, הם נפגשים בקודקוד של המצולע, שאר הקודקודים נבנים בדרך דומה.

**שאלה 3.** תהי $K/F$ הרחבת שדות. נתבונן בחוג הפולינומים $K[x]$ ובשדה הפונקציות הרציונליות $F(x)$, ונחשוב על שניהם כתת־קבוצות של $K(x)$. הוכיחו $F(x)\cap K[x]=F[x]$.

פתרון. הוכחת ההכלה $(\supseteq)$ קלה כי כל פולינום מעל $F$ הוא פולינום מעל $K$ וגם פונקציה רציונלית מעל $F$.

להכלה $(\subseteq)$ נשים לב שלפונקציה רציונלית מעל $F$ (ששייכת ל-$K(x)$) שהיא גם פולינום מעל $K$ יש מכנה $1$ ומונה שהוא פולינום מעל $F$, כלומר פולינום מעל $F$ שנמצא ב-$K(x)$.

**שאלה 4.** תהי $K/F$ הרחבת שדות. יהי $f(x)\in F[x]$ פולינום מדרגה $n\geq 1$. הוכיחו או הפריכו את הטענות הבאות:

א. אם $a$ איבר אלגברי מעל $K$ אז הוא אלגברי מעל $F$.

ב. אם $a$ איבר אלגברי מעל $F$ אז הוא אלגברי מעל $K$.

ג. אם $a$ איבר אלגברי מעל $F$ אז גם $\alpha\cdot a$ הוא אלגברי לכל $\alpha\in F$.

פתרון.

א. הפרכה: $\pi$ הוא אלגברי מעל $K=\mathbb{R}$ כי הוא מאפס את הפולינום $x-\pi$, אבל הוא לא אלגברי מעל $\mathbb{Q}$. דוגמה אחרת, שאולי היא יותר פשוטה, זה ש-$x$ אלגברי מעל $\mathbb{C}(x)$, אבל לא מעל $\mathbb{C}$.

ב. הוכחה: $a$ אלגברי מעל $F$ ולכן יש פולינום $p(x)\in F[x]$ כך ש-$p(a)=0$. אבל $F\subseteq K$ ולכן $p(x)\in K[x]$. כלומר שיש פולינום מעל $K$ שמתאפס ב-$a$ ולכן $a$ אלגברי מעל $K$.

ג. הוכחה: $a$ אלגברי ולכן יש $p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$ כך ש-$p(a)=0$. אז

$$0=p(a)=\frac{1}{\alpha^n}(\alpha a)^n+a_{n-1}\frac{1}{\alpha^{n-1}}(\alpha a)^{n-1}+\cdots+a_1\frac{1}{\alpha}(\alpha a)+a_0$$

שהרי $a^i = \alpha^{-i} \cdot (\alpha a)^i$. נשים לב ש-$a_i \frac{1}{\alpha^j} \in F$ לכל $i, j$. לכן

$$q(x) = \frac{1}{\alpha^n} x^n + \frac{a_{n-1}}{\alpha^{n-1}} x^{n-1} + \cdots + \frac{a_1}{\alpha} x + a_0$$

הוא פולינום מעל $F$ שמתאפס ב-$\alpha a$.

**שאלה 5.** תהי $K/F$ הרחבה סופית (כלומר $[K:F] < \infty$). הוכיחו כי כל איבר של $K$ הוא אלגברי מעל $F$. רמז: חשבו על הקבוצה $\left\{1, a, a^2, a^3, \ldots\right\}$.
רשות: להרחבה כמו בשאלה קוראים הרחבה אלגברית. האם כל הרחבה אלגברית היא סופית?

פתרון. יהי $a \in K$. מכיוון שדרגת ההרחבה סופית, הקבוצה $\left\{1, a, a^2, \ldots\right\}$ חייבת להיות תלויה לינארית מעל $F$. כלומר יש צירוף לינארי לא טריוויאלי של החזקות שמתאפס:

$$b_n a^n + b_{n-1} a^{n-1} + \cdots + b_0 = 0$$

ולכן $b_n x^n + \cdots + b_0 \in F[x]$ הוא פולינום שמתאפס ב-$a$. כלומר $a$ אלגברי מעל $F$, כדרוש.
לא כל הרחבה אלגברית היא סופית. למשל המספרים בני־הבנייה הם הרחבה אלגברית של $\mathbb{Q}$ שאינה סופית.

**שאלה 6.** הוכיחו כי $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

פתרון. ברור כי $\sqrt{2} + \sqrt{3} \in \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ ולכן $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \supseteq \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$. מצד שני

$$\left(\sqrt{2} + \sqrt{3}\right)^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 = 2\sqrt{6} + 5$$

ולכן $\sqrt{6} \in \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$. בנוסף $\sqrt{6}\left(\sqrt{2} + \sqrt{3}\right) = 2\sqrt{3} + 3\sqrt{2}$ ולכן

$$2\sqrt{3} + 3\sqrt{2} - 2\left(\sqrt{2} + \sqrt{3}\right) = \sqrt{2} \in \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$$

ובוודאי

$$\sqrt{3} = \sqrt{2} + \sqrt{3} - \sqrt{2} \in \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$$

ולכן $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \subseteq \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$, כנדרש. הזכרו שאם $\alpha$ אלגברי מעל $F$, אז $F[\alpha] = F(\alpha)$, ולכן הסתפקנו "רק" בהוכחת $\mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right] = \mathbb{Q}\left[\sqrt{2} + \sqrt{3}\right]$.

**שאלה 7.** יהי $F$ שדה, ותהי $G \leq F^*$ תת־חבורה סופית של החבורה הכפלית של השדה. הוכיחו כי $G$ ציקלית. הדרכה: העזרו בתורת המבנה של חבורות אבליות סופיות ובחישוב $\exp(G)$.

פתרון. לפי משפט המבנה של חבורות אבליות סופיות, ניתן להציג את $G$ כמכפלה

$$G \cong \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right) \times \left(\mathbb{Z}/p_2^{k_2}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p_t^{k_t}\mathbb{Z}\right)$$

כאשר $p_1, \ldots, p_t$ ראשוניים כלשהם (אולי שווים) ו-$k_1, \ldots, k_t \in \mathbb{N}$. נסמן

$$m = \operatorname{lcm}(p_1^{k_1}, p_2^{k_2}, \ldots, p_t^{k_t})$$

וכידוע לנו מתורת החבורות $\exp(G) = m$ ולכן $m \leq |G|$. כלומר $x^m = e_G$ לכל $x \in G$. אבל לפולינום $x^m - 1$ ישנם לכל היותר $m$ פתרונות בשדה $F$. כלומר $|G| \leq m$, וקיבלנו $|G| = m$. לכן בהכרח $p_i \neq p_j$ לכל $i \neq j$, שכן אחרת

$$m = \operatorname{lcm}(p_1^{k_1}, p_2^{k_2}, \ldots, p_t^{k_t}) < p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_t^{k_t} = |G|$$

קיבלנו ש-$G$ היא מכפלה ישרה של חבורות ציקליות מסדרים זרים בזוגות, ולפי משפט השאריות הסיני נסיק שהיא ציקלית.

בהצלחה!