

## אלגברה ב2

© ארזים

29 במרץ 2017

### 1 הרחבת שדות

בשיעור שעבר, ראינו שאם  $K$  שדה,  $f \in K[x]$  אי פריק, אז יש הרחבה  $L/K$  שמקיימת  $f(\alpha) = 0$ ,  $L = K(\alpha)$ , כאשר  $\text{irr}(\alpha, K) = f(x)$  (כלומר  $f(\alpha) = 0$ ).

תזכורת יש לנו את

$$\varphi : K[x] \rightarrow K[x]/I$$

העתקת המנה הטבעית מודולו  $I = (f)$ . אז נוכל לסמן  $L = K[x]/I$ ,  $\alpha = \varphi(x)$  ומתקיים כי  $L$  שדה (ראינו בשיעור שעבר). אפשר לזהות את  $K$  עם תמונתו בתוך  $K[x]$  והטלתה לתוך  $L$ . לכן  $K \subseteq L$ . כעת, ברור כי  $K = f(\alpha)$ , ולכן

$$f(\alpha) = f(\varphi(x)) = \varphi(f(x)) = 0$$

**מסקנה 1.1** סגור אלגברית אם ורק אם לכל  $f \in K[x]$  שאינו קבוע יש שורש בתוך  $K$ .

**הוכחה:** נניח כי  $K$  סגור אלגברית. נניח בשלילה שיש  $f \in F[x]$  לא קבוע וללא שורש. ניקח  $f$  כזה ממעלה מינימלית. אזי הוא וודאי אי פריק (אחרת גם לגורמים שלו לא היה שורש). לכן  $K[x]/(f)$  הרחבה אלגברית של  $K$ , וכיוון שהוא סגור אלגברית, נקבל  $[K[x]/(f) : K] = 1 = \deg f$ . לכן  $f(x) = ax - b$  עם  $a \neq 0$ . לכן  $f(\frac{b}{a}) = 0$ , בסתירה. בכיוון השני, נניח כי  $L/K$  הרחבה אלגברית, ונניח בשלילה כי  $L \neq K$ . נקח  $\alpha \in L \setminus K$  ויהי  $f = \text{irr}(\alpha, K)$ . לפי ההנחה, יש בתוך  $K$  שורש של  $f$ , שנסמנו  $\beta$ , ואז

$$f(x) = (x - \beta) \tilde{f}$$

כעת,  $f$  אי פריק, ולכן נקבל כי

$$f(x) = x - \beta$$

■ לכן  $\alpha = \beta \in K$ , בסתירה.

נרצה כעת להוכיח כי לכל שדה יש סגור אלגברי, אבל לשם כך נצטרך כלי מתורת הקבוצות:

**משפט 1.2** (הלמה של צורן) אם  $\mathcal{F} \neq \emptyset$  קבוצה סדורה חלקית, כך שלכל שרשרת (כלומר תת קבוצה שבה כל שני איברים הם ברי השוואה) יש חסם עליון, אזי יש בתוך  $\mathcal{F}$  איבר מקסימלי.

**הערה 1.3** משפט זה שקול לאקסיומת הבחירה.

בעזרת הלמה של צורן, נוכיח את המשפט האלגברי הכללי הבא:

**הגדרה 1.4** יהי  $R$  חוג. אידאל  $M \subsetneq R$  ייקרא מקסימלי אם לכל אידאל  $J \neq R$  המקיים  $M \subseteq J$ , מתקיים  $J = M$ .

**משפט 1.5** יהי  $R$  חוג, ויהי  $I \triangleleft R$  אידאל שאינו כל החוג. אזי קיים אידאל מקסימלי  $M$  המקיים  $I \subseteq M$ .

**הוכחה:** נגדיר את  $\mathcal{F}$  להיות קבוצת כל האידאלים של  $R$  שאינם  $R$ , שמכילים את  $I$ .  $\mathcal{F}$  לא ריקה, כי  $I \in \mathcal{F}$ . נסדר אותה לפי הכלה:

$$J_1 \leq J_2 \iff J_1 \subseteq J_2$$

תהי  $\{J_i\} \subseteq \mathcal{F}$  שרשרת, כאשר לכל  $i \neq j$  מתקיים  $J_i \subseteq J_j$  או  $J_j \subseteq J_i$ . נגדיר

$$J = \bigcup_i J_i$$

ברור כי לכל  $i$ , מתקיים  $J_i \leq J$  - לא ברור כי  $J \in \mathcal{F}$ . נראה זאת.  $1 \notin J_i$  ולכן גם  $1 \notin J$ . כלומר  $J \neq R$ . ברור כי  $I \subseteq J$ , כי לכל  $i$  מתקיים  $I \subseteq J_i$ . כעת, נותר להוכיח כי  $J$  אידאל. יהיו  $x, y \in J$ . אזי קיימים  $i_1, i_2$  עבורם  $x \in J_{i_1}, y \in J_{i_2}$ . ובלי הגבלת הכלליות,  $J_{i_2} \subseteq J_{i_1}$ . כעת,  $x, y \in J_{i_1}$ , כלומר  $x + y \in J_{i_1} \subseteq J$ . לכן  $J$  סגור לחיבור. באופן דומה, אם  $r \in R, x \in J$ , אז קיים  $i$  עבורו  $x \in J_i$ , ואז  $rx \in J_i \subseteq J$  ולכן  $J$  אידאל.

אם כן, מצאנו לשרשרת שלנו חסם עליון. מהלמה של צורן, נקבל כי בקבוצה  $\mathcal{F}$  יש איבר מקסימלי, שנשמנו  $M$ . אזי זהו אידאל שמכיל את  $I$ , ואינו  $R$ . נראה שזהו אידאל מקסימלי בחוג  $R$ .

יהי  $M' \neq R$  אידאל של  $R$  המכיל את  $M$ . מתקיים  $M \subseteq M' \subseteq R$ , ולכן  $M' \in \mathcal{F}$ . ממקסימליות  $M$  מתקבל  $M' \subseteq M$ , ולכן  $M' = M$ . לכן  $M$  מקסימלי. ■

נראה טענה נוספת מאלגברה:

**טענה 1.6** יהי  $R$  חוג, ויהי  $M \subseteq R$  אידאל מקסימלי. אזי  $R/M$  הוא שדה.

**הוכחה:** צריך להוכיח שכל  $\bar{x} \in R/M$ ,  $\bar{x} \neq 0$  הוא הפיך. נבחר  $x \in R$  המקיים  $x + M = \bar{x}$ . כעת,  $x \notin M$ , כי  $\bar{x} \neq 0$ , ולכן

$$M \subsetneq \langle x, M \rangle = R$$

כי  $M$  מקסימלי. לכן קיימים  $a \in R, b \in M$  המקיימים

$$1 = ax + b$$

כעת, אם ניקח תמונה מודולו  $M$ , נקבל

$$1 = \bar{a} \cdot \bar{x} + 0$$

ולכן  $\bar{x}$  הפיך.

■ זהו למעשה מקרה כללי של הטענה שחוג פולינומים מעל שדה מודולו אידאל שנוצר על ידי פולינום אי פריק הוא שדה - אידאל שנוצר על ידי פולינום אי פריק הוא מקסימלי.

**משפט 1.7** יהי  $K$  שדה. אזי קיים סגור אלגברי של  $K$ .

**הוכחה:** נבנה באינדוקציה מגדל של הרחבות של שדות

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots$$

עם התכונה שלכל פולינום אי פריק  $f \in K_i[x]$  יש שורש בתוך  $K_{i+1}$ .  
הבסיס ברור -  $K_0 = K$ . כעת, נניח שכבר בנינו את  $K_i$ . נסמן

$$F = \{f \in K_i[x] \mid f \text{ is irreducible}\}$$

נגדיר

$$R = K_i[x_f \mid f \in F]$$

זהו חוג פולינומים עם כמות משתנים שווה לעוצמה

$$|F| = |K| + \aleph_0$$

נגדיר אידאל:

$$I = \langle f(x_f) \mid f \in F \rangle$$

אזי קל לראות כי  $1 \notin I$ : אחרת

$$1 = a_1(\underline{x}) f_1(x_{f_1}) + \dots + a_n(\underline{x}) f_n(x_{f_n})$$

ואז  $0 = \deg 1 \geq \deg f_1 > 0$ . בסתירה.

לכן יש אידאל מקסימלי  $M$  כלשהו שמכיל את  $I$ . כעת, נסמן

$$K_{i+1} = R/M$$

$$\varphi : R \rightarrow R/M$$

כאשר  $\varphi$  ההטלה הטבעית. נזהה את  $K$  עם תמונתו על ידי

$$K_i \xrightarrow{\varphi} R/M = K_{i+1}$$

כעת,  $K_{i+1}$  שדה כי  $M$  מקסימלי, ולכל פולינום אי פריק  $f \in K_i[x]$ , האיבר  $\alpha_f := \varphi(x_f) \in K_{i+1}$  הוא שורש של  $f$ , כי  $f(x_f) \in I \subseteq M$  ולכן

$$f(\alpha_f) = \varphi(f(x_f)) = 0$$

ולכן סיימנו את הבנייה.  
נראה כעת כי

$$\Omega = \left\{ x \in \bigcup_{i=1}^{\infty} K_i \mid [K(x) : K] < \infty \right\}$$

הוא סגור אלגברית, ולכן סגור אלגברי של  $K$ . נקח  $f \in \Omega[x]$  לא קבוע, ונרצה להראות שיש לו שורש. נניח שלא, ונקח  $f$  מדרגה מינימלית שכזה. אזי ברור שהוא אי פריק כמו שראינו כבר (אחרת גם לגורמים אין שורש). אבל, מקדמי  $f$  הם מתוך  $\bigcup K_i$ , ולכן כל מקדם של  $f$  שייך לאיזשהו  $K_i$  - כלומר קיים  $i$  גדול מספיק שמקיים  $f \in K_i[x]$ . לכן, מהתכונה של המגדל, יש שורש של  $f$  בתוך  $K_{i+1}$ , שנשמנו  $\alpha$ . נותר להוכיח כי  $\alpha$  אלגברי מעל  $K$ . נסמן  $a_1, \dots, a_n$  את מקדמי  $f$ , שכולם אלגבריים מעל  $K$  (כי הם מתוך  $\Omega$ ). לכן,

$$K \subseteq K(a_1) \subseteq K(a_1, a_2) \subseteq \dots \subseteq K(a_1, \dots, a_n)$$

מגדל של הרחבות סופיות, ולכן ממשפט המכפלה מתקיים

$$[K(a_1, \dots, a_n) : K] < \infty$$

כמובן  $\alpha$  אלגברי מעל  $K(a_1, \dots, a_n)$ , ולכן גם

$$[K(a_1, \dots, a_n)(\alpha) : K(a_1, \dots, a_n)] < \infty$$

ואז שוב ממשפט המכפלה מתקיים

$$[K(a_1, \dots, a_n, \alpha) : K] < \infty$$

ובפרט  $\alpha$  אלגברי מעל  $K$ . ■

**הערה 1.8** למעשה,  $\Omega = K_1$ ,  
אם  $x, y$  אלגבריים אזי

$$K \subseteq K(x) \subseteq K(x, y)$$

ולכן  $K(x, y)$  אלגברי מעל  $K$ , ובפרט סכום או מכפלה של איברים אלגבריים נותנים איבר אלגברי.

**תרגיל** מה הפולינום המינימלי של  $\sqrt{2} + \sqrt{3}$ .

### 1.1 בניות עם סרגל ומחוגה

נרצה לשאול מה ניתן לבנות בעזרת סרגל ומחוגה. סרגל מאפשר להעביר קו ישר בין שתי נקודות, ומחוגה מאפשרת לבנות מעגל עם מרכז מסויים ורדיוס מסויים. אפשר בקלות למצוא איך לחלק קטע לשתיים, בדיוק באמצע, ואיך להעביר אנך. אנחנו עובדים במישור, ונחשוב עליו בתור  $\mathbb{C}$ . היוונים ידעו לצייר את הרציונאליים, את  $\sqrt{2}$ , ועוד הרבה (לצייר מחומש למשל, או לחצות זווית).

הם לא ידעו, בין היתר, להכפיל את הקוביה (לצייר קוביה גדולה פי 2, שקול לצייר את  $\sqrt[3]{2}$ ), לחלק זווית לשלוש, או אילו פולינומים משוכללים אפשר לצייר, למשל לא ידעו לצייר "משובעשר" משוכלל (17 צלעות). הם גם לא ידעו לרבע את המעגל - לצייר מרובע ששטחו  $\pi$ .

ננסה לתת שפה פורמלית לעניין.

**הגדרה 1.9** בהנתן שתי נקודות  $p, q \in \mathbb{C}$ , נאמר כי המעגל שמרכזו  $p$  ורדיוסו  $|p - q|$  הוא המעגל המוגדר על ידי  $p, q$ , והישר ביניהן הוא הישר שמוגדר על ידיהן. אם  $p = q$  שניהם מוגדרים להיות הסינגלטון  $\{p\} = \{q\}$ .

**הגדרה 1.10** תהי  $X \subseteq \mathbb{C}$  קבוצה.  $C(X)$  היא קבוצת כל הנקודות שהן חיתוך של שני ישרים, שני מעגלים או ישר ומעגל שמוגדרים על ידי שתי נקודות מתוך  $X$ . נסמן

$$C^n(X) = \underbrace{C(C(\dots C(X)))}_n$$

ונאמר כי  $p$  ניתנת לבנייה מתוך  $X$  אם קיים  $n$  עבורו  $p \in C^n(x)$ . אם לא מזכירים את  $X = \{0, 1\}$ .

**למה 1.11** יהיו  $z, w \in \mathbb{C}$ .

1. אם  $x, y \in \mathbb{R}, z = x + iy$ , אזי  $z$  ניתן לבנייה אם ורק אם  $x, y$  ניתנים לבנייה.

2. אם  $z, w$  ניתנים לבנייה אזי גם  $z + w, zw, \frac{z}{w}$  ניתנים לבנייה.

3. אם  $z$  ניתן לבנייה, גם  $\sqrt{z}$  ניתן לבנייה.

**הוכחה:** ניתנה בצירוף. ניתן להעביר אנכים, ולכן לקבל חלק ממשי ומדומה ולהיפך.  $z + w$  ניתן לבנייה בבירור, עבור  $zw, \frac{z}{w}$  משתמשים במשפט תאלס. את  $\sqrt{z}$  בונים על ידי משפט פיתגורס אם  $z$  ממשי וגדול מאפס. ■

- למה 1.12** יהי  $F \subseteq \mathbb{C}$  ויהיו  $L \neq L'$  ישרים,  $C \neq C'$  מעגלים המוגדרים מנקודות של  $F$ .
1.  $L \cap L' = \emptyset$  או שהחיתוך הוא בדיוק נקודה אחת מתוך  $F$ .
  2.  $L \cap C = \emptyset$ , או שמכיל לכל היותר שתי נקודות, שתיהן מתוך  $F[\sqrt{z}]$  עבור  $z \in F$  כלשהו.
  3.  $C \cap C' = \emptyset$  או שמכיל לכל היותר שתי נקודות, שתיהן מתוך  $F[\sqrt{z}]$  עבור  $z \in F$  כלשהו.

**הוכחה:**

1.

$$ax + b = cx + d$$

אם יש פתרון אז הוא

$$x = \frac{d - b}{a - c}$$

2.

$$\begin{aligned} (x - x_0)^2 + (y - y_0)^2 &= r^2 \\ ax + by + c &= 0 \end{aligned}$$

והפתרונות מקיימים משוואה ריבועית.

3. כמו 2.

■

**מסקנה 1.13** אם  $\alpha \in \mathbb{C}$  ניתן לבנייה, אזי  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ , ואפילו יש מגדל של שדות  $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$ , כאשר  $\alpha \in K_m$ , ולכל  $i$  קיים  $\sqrt{z_i} \in K_{i+1}$  המקיים  $K_{i+1} = K_i(\sqrt{z_i})$ .

**הוכחה:** לפי הגדרה,  $\alpha$  ניתן לבנייה על ידי חיתוך של ישרים ומעגלים המוגדרים מעל  $\mathbb{Q}$  ומעל השדות המתקבלים באמצע. לפי הלמה הקודמת, בכל שלב נקבל הרחבה ריבועית, ולכן

$$\alpha \in K_m$$

כמו שרצינו, ובפרט

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{[K_m : \mathbb{Q}]}{[K_m : \mathbb{Q}(\alpha)]} = \frac{[K_m : K_{m-1}] \dots [K_1 : K_0]}{[K_m : \mathbb{Q}(\alpha)]} = 2^n$$

■

**מסקנה 1.14** אי אפשר לחלק זווית לשלוש על ידי סרגל ומחוגה.

**הוכחה:** נראה כי  $\sin 10$  אינו ניתן לבנייה, וזה מספיק, כי אפשר לבנות זווית של 30 מעלות, ואז אם נצליח לחלק אותה לשלוש נקבל את  $\sin 10$ . מתקיים

$$4 \sin 3x = 4 \sin x - \sin^3 x$$
$$\alpha^3 - 4\alpha + 2 = 0$$

זה פולינום אי פריק (איזנשטיין). לכן המעלה של ההרחבה היא 3, ולכן לא ניתן לבנות את  $\alpha$ . ■

באופן דומה  $x^3 - 2$  אי פריק ולא ניתן לבנות את  $\sqrt[3]{2}$ .  $\pi$  הוא טרנסנדנטי ולכן לא ניתן לבנייה. בעתיד נראה שאפשר לבנות מצולע משוכלל בעל 17 צלעות.

**משפט 1.15** גם הכיוון ההפוך נכון. אם יש מגדל של הרחבות

$$\mathbb{Q} = K_0 \subseteq \dots \subseteq K_m$$

כאשר  $[K_{i+1} : K_i] = 2$ ,  $\alpha \in K_m$ , אזי  $\alpha$  ניתן לבנייה.

**הערה 1.16** התנאי  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$  הוא לא מספיק טוב.

נראה את הדברים הללו בעתיד, בעזרת תורת גלואה.