

טענה

יהי $p(x) \in \mathbb{F}[x]$ מדרגה $n \geq 1$. הראו ש $\mathbb{F}[x]/\langle p(x) \rangle$ הוא מ"ו ממימד n מעל \mathbb{F} .

פתרון

$$B = \{\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}\}$$

$$(\bar{x} = x \pmod{p(x)})$$

נוכיח שאברי B בת"ל:

$$\alpha_0 \cdot \bar{1} + \alpha_1 \cdot \bar{x} + \dots + \alpha_{n-1} \cdot \bar{x}^{n-1} = 0$$

כאשר לא כל $\alpha_i = 0$.

נגדיר $f = \alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1}$. אזי $f \equiv 0 \pmod{p(x)} \iff p \mid f$.
 p מדרגה n , f מדרגה קטנה מ- n - סתירה!
צ"ל ש B פורש את $V = \mathbb{F}[x]/\langle p(x) \rangle$.

$$\bar{f} \in V \quad f(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_k x^k \in \mathbb{F}[x]$$

נחלק את f ב p עם שארית:

$$f(x) = p(x)q(x) + r(x) \quad \deg r(x) < \deg p(x) = n$$

$$\implies \bar{f} = \bar{r} = \beta_0 \cdot \bar{1} + \beta_1 \cdot \bar{x} + \dots + \beta_k \cdot \bar{x}^k \quad k < n$$

■

מספרים ניתנים לבנייה

החוקים

1. ניתן להעביר ישר $L(P, Q)$ בין כל שתי נקודות ניתנות לבנייה P, Q .
 2. ניתן לבנות מעגל מעגל $C(P, Q)$ שמרכזו P ועובר דרך Q .
- הערה: $L(P, Q) = L(Q, P)$ אבל $C(P, Q) \neq C(Q, P)$.

משפטי עזר

1. בהנתן נקודה וישר ניתן להעביר ישר מקביל העובר דרך הנקודה.
2. בהנתן נקודה וישר ניתן לבנות ישר אנכי העובר דרך הנקודה.
3. בהנתן זווית ניתן לבנות חצי זווית.
4. ניתן לבנות מעגל $C(P, |QR|)$ שמרכזו P ורדיוסו $|QR|$ - אורך של קטע אחר.
5. בהינתן קטעים באורכים ניתנים לבניה $1, x, y$ ניתן לבנות קטעים באורכים $\sqrt{x}, x + y, xy, x^{-1}$.
6. אם $a \in \mathbb{C}$ שניתן לבניה מעל \mathbb{Q} אזי $[\mathbb{Q}[a] : \mathbb{Q}]$ הוא חזקה של 2.

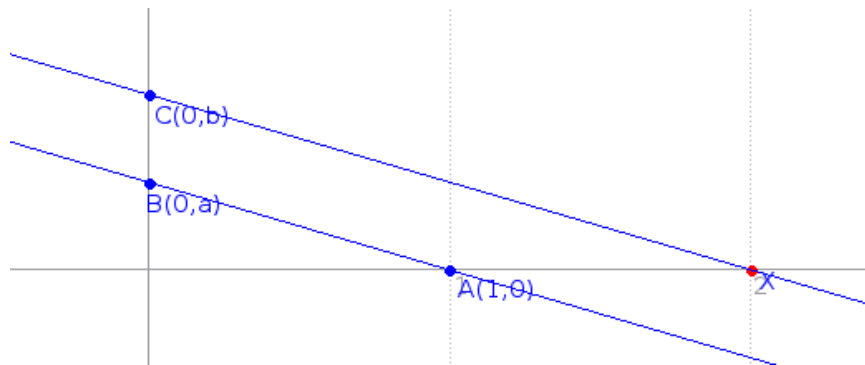
תרגיל

בהנתן שני מספרים $a, b \in \mathbb{R}$ ניתנים לבניה, הראו שניתן לבנות מהם את $\frac{b}{a}$.

פתרון

$$A = (1, 0) \quad B = (0, a) \quad C = (0, b)$$

1. להעביר ישר דרך AB
2. להעביר ישר מקביל ל $L(A, B)$ דרך C ונקרא לו M
3. קיבלנו את X כחיתוך של M עם ציר x .



בגלל שהמשולשים $C0X$ ו $B0A$ הם דומים, נקבל

$$\frac{b}{a} = \frac{|C0|}{|B0|} = \frac{|0X|}{|0A|} = \frac{u}{1}$$

$$u = \frac{b}{a}$$

וקיבלנו ש $\frac{b}{a}$ ניתן לבניה.

■

משפט

(a, b) ניתן לבניה $\iff a, b$ ניתנים לבניה.

משפט

$\deg(f) = [F(a) : \mathbb{F}]$ כאשר f אי-פריק וגם $f(a) = 0$. אם f מתוקן אזי f נקרא פולינוס מינימלי.

$$x^n + a_{n-1}x^{n-1} + \dots$$

תרגיל

הראו שלא ניתן לחלק זזית ב7. (צריך להראות זזית ספציפית שלא ניתן לחלק ב7)

פתרון

נראה תחילה שהמספר $e^{i\frac{2\pi}{7}} = \cos \frac{2\pi}{7} + i \sin \frac{2\pi}{7} = \text{cis} \frac{2\pi}{7}$ לא ניתן לבנייה.

$$\left(\text{cis} \frac{2\pi}{7}\right)^7 = \text{cis} \frac{2\pi}{7} \cdot 7 = \text{cis} 2\pi = 1$$

רואים ש $\text{cis} \frac{2\pi}{7}$ הוא שורש של $x^7 - 1$.

$$\Phi_7 = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + \dots + 1$$

הוא פולינוס אי-פריק, וגם $\text{cis} \frac{2\pi}{7}$ הוא שורש שלו. לכן $[\mathbb{Q}(\text{cis} \frac{2\pi}{7}) : \mathbb{Q}] = 6$. לא חזקה של 2, ולכן $\text{cis} \frac{2\pi}{7}$ לא ניתן לבניה.

(תזכורת: $\mathbb{F}(a) \cong \mathbb{F}[x]/\langle f(x) \rangle$ כאשר $f(x)$ הפולינוס המינימלי)

זזית π ניתנת לבניה (זזית ישרה). נניח בשלילה שניתן לחלק ב7: $\frac{\pi}{7}$. אם ניתן לבנות את הזזית $\frac{\pi}{14}$ אזי ניתן לבנות את המספר $\text{cis} \frac{\pi}{14}$. ניתן לקחת חזקה רביעית ולקבל $(\text{cis} \frac{\pi}{14})^4 = \text{cis} \frac{2\pi}{7}$ ומספר זה לא ניתן לבנייה. סתירה.

תרגיל

\mathbb{F} שדה. הראו שאם $G \leq \mathbb{F}^*$ תת-חבורה סופית אזי היא ציקלית.

פתרון

G היא חבורה אבלית. $G = \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_r^{k_r}}$. לפי המשפט היסודי של חבורות אבליות סופיות

$$m = \exp G = \text{lcm}(p_1^{k_1}, \dots, p_r^{k_r})$$

$$m \leq |G| = n$$

$$g^m = 1 \quad g \in M$$

\Leftarrow כל האיברים בחבורה הם שורשים של $x^m - 1 = 0$.

מספר שורשים של פולינום בשדה \geq לדרגה של הפולינום.

לכן $|G| = m \Leftarrow |G| \leq m$.

לא ייתכן ש $p_i = p_j$ אחרת $m < n$ ולכן $\text{lcm}(p_1^{k_1}, \dots, p_r^{k_r}) = p_1^{k_1} \dots p_r^{k_r}$.
קיבלנו מכפלה של חבורות ציקליות מסדרים זרים וזה ציקלי.

