תרגול 12 - תורת גלואה

בניות בסרגל ומחוגה

נתון המישור $\mathbb{R}^2$, נתונים ציר ה-x והנקודות $(0,0)$ ו-$(1,0)$.

- מותר להעביר ישר בין שתי נקודות.
- מותר להעביר מעגל בין שתי נקודות.
- כל נקודת חיתוך היא נקודה חדשה שלנו.

הגדרה:

מספר $a\in\mathbb{R}$ הוא בר-בנייה (constructible) אם אפשר להגיע לנקודה $(a,0)$. מספר $a+ib\in\mathbb{C}$ הוא בר-בנייה אם a,b בני-בנייה.

תרגיל:

אם a,b בני-בנייה אז $a+b$, $a-b$, $a\cdot b$, $\frac{a}{b}$ ו-$\sqrt{a}$ בני-בנייה.

הוכחה:

בהרצאה.

הגדרה:

הרחבת שדות K/F נקראת הרחבה ריבועית חוזרת (מוגדרת ריבועית, 2-רדיקלית) אם יש שדות ביניים

$$F=F_0\subseteq F_1\subseteq\dots\subseteq F_k=K$$

כך ש-$[F_{i+1}:F_i]=2$.

משפט:

מספר $a\in\mathbb{C}$ הוא בר-בנייה אם ורק אם קיימת הרחבה ריבועית חוזרת K/F כך ש- $a\in K$.

מסקנה:

מעלת הפולינום המינימלי של a, $[\mathbb{Q}(a):\mathbb{Q}]$, היא חזקת 2.

הערה:

הרחבת גלואה $K/\mathbb{Q}$ היא ריבועית חוזרת $\iff$ $Gal(K/F)$ היא חבורת-2.

דוגמה:

מצולע משוכלל עם n צלעות ניתן לבנייה $\iff$ ζ_n בר-בנייה $\iff$ $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})\cong U_n$ חבורת-2 $\iff$ $\varphi(n)$ חזקת 2.

בפרט, אם p ראשוני מהצורה $p=2^n+1$, אז ζ_p בר-בנייה.
[במקרה הזה p חייב להיות מהצורה $p=2^{2^n}+1$]

תרגיל: (ממבחן)

א. הסבירו מדוע אי-אפשר לבנות מצולע משוכלל עם 21 צלעות.

ב. נניח שנתון משושה משוכלל. הראו שניתן לבנות בעזרתו את המצולע מסעיף א'.

פתרון:

א. לפי הטיעון הנ"ל אפשר לבנות מצולע משוכלל עם 21 צלעות $\iff$ $\varphi(21)$ חזקת 2. אבל $\varphi(21)=\varphi(3\cdot 7)=2\cdot 6=12$ אינו חזקת 2.

ב. לפי המשפט, יש לנו את ρ_7. בנוסף ρ_3 בר-בנייה כי $\varphi(3)=2$.

לכן $\rho_{21}=\rho_3\cdot\rho_7$ בר-בנייה.

דרך אחרת:

$$\mathbb{Q}\subseteq\mathbb{Q}(\rho_7)\underset{2}{\subseteq}\mathbb{Q}(\rho_{21})$$

תרגיל:

האם ניתן באמצעות סרגל ומחוגה לחלק זווית לשבע?

פתרון:

לא, כי אחרת היינו יכולים לבנות את הזווית $\frac{2\pi}{7}$ $\Leftarrow$ את ρ_7, אבל ρ_7 אינו בר-בנייה.

תרגיל: (ממבחן)

הוכיחו שניתן לבנות באמצעות סרגל ומחוגה את הזווית 24°.

הוכחה:

$24^\circ=\frac{2\pi}{15}$. ρ_{15} הוא בר-בנייה, כי $\varphi(15)=\varphi(3\cdot5)=2\cdot4=8$. לכן

גם ρ_{15}^{-1} בר-בנייה, ולכן גם $\cos\frac{2\pi}{15}=\frac{1}{2}(\rho_{15}+\rho_{15}^{-1})$ בר-בנייה.

זה מראה שניתן לבנות את הזווית 24°.

דרך אחרת: הדרך לבאר,

$$\cos 24^\circ=\frac{1}{8}(1+\sqrt{5})+\frac{1}{4}\sqrt{\frac{3}{2}(5-\sqrt{5})}$$

$$\mathbb{Q}\underset{2}{\subseteq}\mathbb{Q}(\sqrt{5})\underset{2}{\subseteq}\mathbb{Q}(\cos 24^\circ)$$

תרגיל:

נניח שנתון $a\in\mathbb{R}$ כך שהפולינום המינימלי שלו הוא ממעלה שהיא חזקת 2.
האם a בר-בנייה?

פתרון:

לא!

ניקח את a להיות השורש של הפולינום $f(x)=x^4-4x+2$.
אי-פריק לפי איזנשטיין עם $p=2$. אם E שדה הפיצול של f
מעל $\mathbb{Q}$, אפשר לבדוק ש- $Gal(E/\mathbb{Q})\cong S_4$, וזו אינה חבורת-2.

תרגיל:

תהי E/F הרחבת גלואה (סופית). הוכיחו שקיים שדה ביניים $F\subseteq K\subseteq E$
כך שמתקיים:

א. K/F הרחבת גלואה.

ב. $Gal(K/F)$ אבלית.

ג. K מקסימלית ביחס ל-א׳+ב׳. כלומר: אם $F\subseteq K'\subseteq E$ שדה
ביניים כך ש- K'/F גלואה ו- $Gal(K'/F)$ אבלית, אז $K'\subseteq K$.

הוכחה:

נסמן $G=Gal(E/F)$. תהי G' תת-חבורת הקומוטטורים של G,
ונסמן $K=E^{G'}$.
ידוע $G'\trianglelefteq G$ ו- G/G' הוא המנה האבלית המקסימלית של G.
$\Downarrow$
K/F גלואה, $Gal(K/F)\cong G/G'$ אבלית.

נניח את המקסימליות. נניח ש- $F\subseteq K'\subseteq E$ מקיימת את א' + ב'.

$H=Gal(E/K')$. K'/F גלואה, ולכן

$$Gal(K'/F)\cong Gal(E/F)/Gal(E/K') = G/H$$ ← אבלי.

לכן $H\supseteq G'$ $\Leftarrow$ $K'=E^H\subseteq E^{G'}=K$.

$\square$

<u>פתירות ע"י רדיקלים</u>

<u>משפט:</u>

פולינום $f\in\mathbb{Q}[x]$ פתיר ע"י רדיקלים אם ורק אם $Gal(\mathbb{Q}_f/\mathbb{Q})$ פתירה.

<u>תרגיל:</u>

האם הפולינום $f(x)=5x^5-100x+10$ פתיר ע"י רדיקלים?

<u>פתרון:</u>

f אי-פריק לפי אייזנשטיין עם $p=2$.

$$f'(x)=25x^4-100=0$$
$$x^4=4$$
$$x=\pm\sqrt{2}$$

$f(\sqrt{2})>0$, $\quad f(-\sqrt{2})<0$

ולכן יש לו בדיוק 3 שורשים ממשיים ו-2 מרוכבים. לפי משפט,

$$Gal(\mathbb{Q}_f/\mathbb{Q})\cong S_5$$

לא פתירה, לכן f אינו פתיר ע"י רדיקלים.

<u>תרגיל:</u>

האם הפולינום $f(x)=x^6-3x^3+6$ פתיר ע"י רדיקלים?

<u>הוכחה:</u>

השורשים של f מתקבלים ע"י פתרון משוואה ריבועית עם $y=x^3$:

$$y^2-3y+6=0$$

$$y_{1,2}=\frac{3\pm\sqrt{-15}}{2}$$

ולכן $f(x)$ מתפרק מעל הרחבה רדיקלית של $\mathbb{Q}$ לפי

$$f(x)=\left(x^3-\frac{3+\sqrt{-15}}{2}\right)\left(x^3-\frac{3-\sqrt{-15}}{2}\right)=f_1(x)f_2(x)$$

$\deg f_i=3$. ניזכר שמעל $\mathbb{Q}$ כל פולינום ממעלה 3 הוא פתיר ע"י רדיקלים (כי חבורת גלואה שלו משוכנת ב-S_3 שהיא פתירה),

אם K_1,K_2 שדות הפיצול של f_1,f_2 מעל ההרחבה F של $\mathbb{Q}$, אז $K_1/F, K_2/F$ פתירות $\Leftarrow$ K_1K_2/F פתירה, ו-K_1K_2 שדה הפיצול של f מעל $\mathbb{Q}$. לכן $f(x)$ פתיר ע"י רדיקלים.