תורת השדות

הבעיות של ימי קדם

המתמטיקה של היוונים הייתה מאוד גיאומטרית. בשבילם לפתור בעיה זה אומר לצייר את הפתרון אם מחוגה וסרגל.

- להכפיל את הקוביה - לבנות במחוגה וסרגל את $\sqrt[3]{2}$.
- לשלש את הזווית - היוונים ידעו איך לחצות זווית עם מחוגה [1]. הם לא ידעו איך לשלש אותה - איך לבנות במחוגה וסרגל את $\frac{\alpha}{3}$ $\Leftarrow$ $\cos\left(20^\circ\right)$
- לרבע את המעגל - לבנות במחוגה וסרגל את $\sqrt{\pi}$.
- לבנות משובע משוכלל(עד משושה ידעו לבנות) - לבנות במחוגה וסרגל את $\frac{2\pi}{7}$ $\Leftarrow$ $\cos\left(\frac{2\pi}{7}\right)$
- (להוכיח את אקסיומת המקבילים [2])

הרעיון הכללי

בנייה במחוגה וסרגל = נתון המישור עם שתי נקודות מיוחדות: 0,1.

- סרגל = דרך כל שתי נקודות אפשר להעביר קו ישר.
  - הסרגל בא בלי סימונים - אי אפשר למדוד מרחק.
  - רק צד אחד של הסרגל הוא חלק - אי אפשר להשתמש בו בשביל לצייר מקבילים.
- מחוגה = אפשר להעביר מעגל שמרכזו נקודה נתונה ועובר דרך נקודה נתונה אחרת.
- אפשר לסמן את החיתוך של כל שני קווים

[1] לצייר מעגל שמרכזו בנקודת זוית ולסמן את המפגשים שלו עם הקרנות. ליצור מעגל ברדיוס שווה על כל מרכז כזה. הקו העובר בין הקטבים הוא חוצה הזווית

[2] שאם יש ישר ונקודה מחוץ לישר אז אפשר להעביר ישר מקביל אחד ויחיד דרכה

איך מתרגמים את זה לאלגברה?

נשים לב שכל הנקודות האלה הן על מישור. נגדיר:

$\mathbb{C}$	המישור
$\mathbb{R}$	הישר העובר דרך 0,1
F	אוסף הנקודות שאפשר לקבל בבנייה סופית במחוגה וסרגל מהנקודות 0,1

עובדות על F:

- $F \cap \mathbb{R} = F_0$ הוא שדה (ביחס לפעולות הרגילות)
- F שדה(ביחס לפעולות הרגילות)
- F סגור להוצאת שורש
- F הוא תת השדה הקטן ביותר של $\mathbb{C}$ שסגור להוצאת שורש <u>שני</u>
  - זה אומר ש$\dim(F) = \infty$, כי $\dim\left(\mathbb{Q}\left[\sqrt{2},\sqrt{3},\sqrt{5},\ldots\right]\right) = \infty$

מסקנה

לכל איבר $\alpha \in F$ יש שרשרת של שדות

$$\mathbb{Q} = \mathbb{F}_{\not{0}} \subset F_1 \subset F_2 \subset F_3 \subset \cdots \subset F_n \left(\subset F \subset \mathbb{C}\right)$$

כך ש $[F_{i+1} : F_i] = 2$ [3] ו $\alpha = F_n$

בקרוב נוכיח שאם $L_0 \subset L_1 \subset L_2$ אז $[L_2 : L_0] = [L_2 : L_1]\cdot[L_1 : L_0] \Leftarrow [L_1 : L_0] \mid [L_2 : L_0]$

$\Leftarrow$ המימד מעל $\mathbb{Q}$ של כל תת שדה של F_n הוא חזקת 2.

$\Leftarrow$ כל מספר ניתן לבנייה יוצר שדה ממימד חזקת 2.

הסתכלות אלגברית על בעיות ימי קדם:

- הכפלת הקוביה: $\sqrt[3]{2}$ הוא שורש של $x^3 - 2$ ולכן $[\mathbb{Q}\left[\sqrt[3]{2}\right] : \mathbb{Q}] = 3$ (כי $x^3 - 2$ אי פריק ו$\deg\left(x^3-2\right) = 3$) - ולכן אי אפשר לבנות אותו.
- שילוש הזווית: אם נצליח לבנות את $\frac{\alpha}{3}$ נוכל למצוא את $\beta = \cos\left(20^\circ\right)$. זהו שורש של $8x^3 - 6x - 1$ - פולינום אי־פריק ושוב אי אפשר לבנות אותו.
- בניית משובע: שוב, זה מאפשר למצוא את $\eta = 2\cos\left(\frac{2\pi}{7}\right)$ שהוא שורש של $\eta^3 - \eta^2 - 2\eta + 1 = 0$.

[3] $[A : B]$ מסמן את המימד של A מעל B

- ריבוע המעגל: π הוא בכלל לא מספר אלגברי, והוא יוצר שדה ממימד אינסופי.

משוואות פולינומיות

(2) משוואות ריבועיות - $ax^2+bx+c=0$

הבבלים ידעו את הנוסחא: $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. הפתרון מתקבל מהוצאת <u>שורש שני</u>.

(3) פתרון משוואות ממעלה שלישית

מי שגילה את השיטה הוא דל־פרו בשנת 1515.

נתון $y^3+ay^2+by+c=0$.

אם נציב $y=x-\frac{a}{3}$ נקבל משוואה שבה המקדם של x^2 הוא אפס.

נתבונן במשוואה $x^3-ax+b=0$. נכתוב $x=\alpha+\beta$:

$$\alpha^3+\beta^3+3\alpha\beta x-ax+b=0$$

נחליט ש$\alpha\beta=\frac{a}{3}$:

$$\alpha^3+\beta^3+\cancel{3\alpha\beta x}-\cancel{ax}+b=0$$

$$\alpha^3+\beta^3=-b$$

אבל לפי ההחלטה $\alpha\beta=\frac{a}{3}$ מתקיים $\alpha^3\beta^3=\left(\frac{a}{3}\right)^3$, ואז α^3,β^3 הם השורשים של הפולינום

$$\left(z-\alpha^3\right)\left(z-\beta^3\right)=z^2+bz+\frac{a^3}{27}$$

ויוצא ש

$$\alpha,\beta=\sqrt[3]{\frac{-b\pm\sqrt{b^3-\frac{4a^3}{27}}}{2}}$$

הבחירה בין $+$ ל$-$ היא בעצם מה שמבדיל בין α לβ, לכן נבחר תמיד $+$ עבור α: $\alpha=\sqrt[3]{\frac{-b+\sqrt{b^3-\frac{4a^3}{27}}}{2}}$. נקבל 3 אפשרויות ל$\alpha$, ולכל אחד מהם יש β יחד $\beta=\frac{a/3}{\alpha}$. כך ניתן למצוא את שלושת הxים באמצעות $x=\alpha+\beta$, ולפי זה את שלושת הyים.

כלומר הפתרון מתקבל מהוצאת **שורש שני** ואח"כ **שורש שלישי**.

משמעות היסטורית

- זהו ההישג המשמעותי הראשון של מתמטיקאים באירופה מאז פיבונ'צי.
- בשביל להגיע אפילו לפתרון פשוט כמו $(x-1)(x-2)(x-3)$ צריך לעבור דרך מספרים מרוכבים. זה הוביל להכרה במספרים המרוכבים בתור מספרים "לגיטימיים".

(4)פתרון משוואת ממעלה רביעית

הפתרון התגלה ע"י טרטליה, 1545.

אחרי החלפה פשוטה $x \mapsto x - \alpha$ אפשר להגיע למשוואה

$$x^4 - ax^2 + bx - c = 0$$

מנסים להציג את זה בתור

$$\left(x^2 + Ax + B\right)\left(x^2 - A'x + D\right) = 0$$

$$||$$

$$x^4 + (A - A')\,x^3 + (B + D - AA')\,x^2 + (AD - A'B)\,x + BD$$

השוואת מקדמים נותנת

$$\left\{\begin{array}{c} A' = A \\ B + D - AA' = -a \\ AD - A'B = b \\ BD = -C \end{array}\right. \Rightarrow \left\{\begin{array}{c} B + D - A^2 = -a \\ A\,(D - B) = b \\ BD = -C \end{array}\right.$$

$$B + D = A^2 - a$$

$$D - B = \frac{b}{A}$$

$$D = \frac{1}{2}\left(A^2 - a + \frac{b}{A}\right) \qquad B = \frac{1}{2}\left(A^2 - a - \frac{b}{A}\right)$$

נציב במשוואה $BD = -C$:

$$A^4 - 2aA^2 + a^2 - \frac{b^2}{A^2} = -4c$$

$$A^6 - 2aA^4 + \left(a^2 + 4c\right) - b^2 = 0$$

זו אמנם נראית כמו משוואה ממעלה שישית, אבל בעצם אפשר לפתור אותה כמו משוואה ממעלה שלישית בA^2.

מוצאים את A^2 ($\sqrt{\ }$ ואח"כ $\sqrt[3]{\ }$); - 3 אפשרויות

מוצאים את A ($\sqrt{\ }$); - 2 אפשרויות

פותרים את $x^2 + Ax + B = 0$ ואת $x^2 - Ax + D = 0$ ($\sqrt{\ }$, כבר הוצאנו את ה$\sqrt{\Delta}$ הדרוש)

לכאורה מקבלים יותר מ4 אפשרויות - אבל חלק יובילו לאותו הדבר.

משוואות ממעלה יותר גבוהה

ניסו להפעיל את הרעיון הזה על משוואות ממעלה יותר גבוהה, אבל לא הצליחו. יש הבדל עקרוני בין מעלה רביעית למעלה חמישית.

תזכורת

סדרת הרכב של חבורה G:

$$1 = G_t \lhd \cdots \lhd G_2 \lhd G_1 \lhd G$$

כאשר G_i/G_{i-1}(=הגורמים) הן חבורות פשוטות.
ניתן להוכיח שסדרת הרכב היא פשוטה עד כדי סדר הגורמים.
מגדירים חבורה פתירה = כל המנות בסדרת הרכב הן אבליות.

דוגמאות

1. $S_2 \lhd 1$ - זאת סדרת ההרכב היחידה. המנה מסדר 2.
2. $(\cong D_3)\ \underbrace{S_3}_{\langle(1\,2),(1\,3)\rangle} \overset{2}{\lhd} \underbrace{A_3}_{\langle(1\,2\,3)\rangle} \overset{3}{\lhd} 1$. המנות מסדר 2 ו3.
3. $\underbrace{S_4}_{\langle(i\,j)\rangle} \overset{2}{\lhd} \underbrace{A_4}_{\langle(i\,j\,k)\rangle} \overset{3}{\lhd} \underbrace{K_4}_{\langle(i\,j)(k\,l)\rangle} \overset{2}{\lhd} \mathbb{Z}_2 \overset{2}{\lhd} 1$. הגורמים מסדר 2, 3, 2, 2.

יש קשר בין הוצאות השורש הדרושות לפתרון משוואה ממעלה n לבין הסדרים של המנות של סדרות הרכב של S_n!

משפט גלואה

<u>אפשר לפתור</u> את המשוואה $f = 0$ על ידי פעולות שדה והוצאת שורשים $\Leftrightarrow$ "חבורת גלואה של f"(מוכלת בS_n) פתירה.

הסבר כללי למשפט (דרך הדוגמה של פולינום ממעלה 4)

נתון פולינום f ומקדמים ב$\mathbb{Q}$. סדרת ההרכב רומזת על הרחבות של השדה $\mathbb{Q}$:

$$\begin{tikzcd}
F_4 \arrow[d, dash] & 1 \arrow[d, dash, "2"] \\
F_3 \arrow[d, dash] & \mathbb{Z}_2 \arrow[d, dash, "2"] \\
F_2 \arrow[d, dash] & K_2 \arrow[d, dash, "3"] \\
F_1 \arrow[d, dash, "2"'] & A_4 \arrow[d, dash, "2"] \\
\mathbb{Q} & S_4
\end{tikzcd}$$

כאשר בכל שלב מקבלים מקדמים בשדה אחר(מבצעים פעולה של הוצאת שורש שני על מקדמים ב$\mathbb{Q}$ ומקבלים מקדמים בF_1 וכו').