09.01.14 ה' שבט תשע"ד בס"ד

אלגברה מופשטת 3 - הרצאה מספר 13

q ראשוני, חזקה של ראשוני.

$i_n(q)$ = מספר הפולינומים המתוקנים האי-פריקים ממעלה n מעל $\mathbb{F}_q$.

נתבונן בשדה $\mathbb{F}_{q^n}$.

לכל איבר שלו יש פול' מינימלי מעל $\mathbb{F}_q$, והמעלה שלו מחלקת את n.

$$\underbrace{\mathbb{F}_q \le \mathbb{F}_q[\alpha] \le \mathbb{F}_{q^n}}_{n}$$

מצד שני, אם g אי-פריק ו- $\deg g \mid n$, $\mathbb{F}_q[x]/\langle g\rangle \le \mathbb{F}_{q^n}$.

תרגיל: נתבונן ב- $x^3-2\in\mathbb{F}_{13}[x]$; אי-פריק.

יש לו שורש α ב- $\mathbb{F}_{13^3}$. פרק את הפולינום.

פתוח לגמרי: $x^3-2=(x-\alpha)(x-\_)(x-\_)$

השורשים הנוספים יהיו $\alpha^{13},\alpha^{13^2}$ שכן אוטומורפיזם פרובניוס

הוא אוטומורפיזם ומעביר שורש מסוים אל חזקה אחרת של השורש

$$x^3-2=\underset{(x-\alpha)}{(x-\alpha)}\,\underset{(x-3\alpha)}{(x-\alpha^{13})}\,\underset{(x-9\alpha)}{(x-\alpha^{169})}$$

נתבונן בפולינום $x^{q^n}-x$ מעל $\mathbb{F}_q$

$\mathbb{F}_{q^n}$ || שדה הפיצול

$$\prod_{\alpha\in\mathbb{F}_{q^n}}(x-\alpha)$$

מצד שני, $x^{q^n}-x \overset{(*)}{=} \prod_{\substack{g\in\mathbb{F}_q[x]\\ \deg g\mid n}} g$ (**)

נתבונן כעת במעלות של הפול' ב- (*):

$$q^n=\sum_{d\mid n}\underbrace{i_d(q)\cdot d}_{\substack{\text{זו המעלה של}\\ \text{החלק ב- (**)}\\ \prod g\\ \deg g=d}}$$

נוסחת ההיפוך של מביוס:

$$\mu(m)=\begin{cases}0, & p^2\mid m\\ (-1)^s, & m=p_1\dots p_s\end{cases}$$

המשך

$$F(n)=\sum_{d|n} f(d)$$
$$\Updownarrow$$
$$f(n)=\sum_{d|n} F(d)\cdot\mu\left(\tfrac{n}{d}\right)$$

$$\downarrow$$

$$i_n(q)=\frac{1}{n}\sum_{d|n}\mu\left(\tfrac{n}{d}\right)\cdot q^d \quad (>0)$$

(לדוגמא: $i_8(q)=\frac{1}{8}\left[q^8-q^4\right]$)

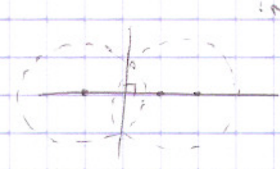
בניות במחוגה וסרגל:

הגדרה: אוסף המספרים הניתנים לבניה הוא הקבוצה A המינימלית באופן הבא:

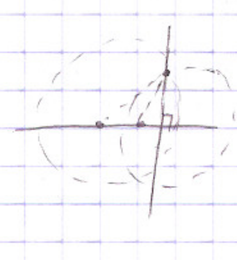
- נתונות שתי נקודות
- "סרגל": אם $a,b \in A$ נתונות אז הישר דרכן נתון.
- "מחוגה": אם $a,b \in A$ נתונות, אז נתון גם המעגל שמרכזו ב-a ורדיוסו $|a-b|$
- החיתוך של ישרים/ישר ומעגל/שני מעגלים נתונות גם [illegible] החיתוך.

בניות יסודיות:

(א) העלאת אנך באמצע:

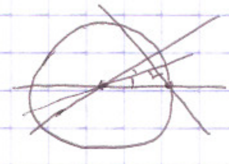


(ב) הורדת אנך:



(ג) העברת מקביל

(ד) חציית זווית:

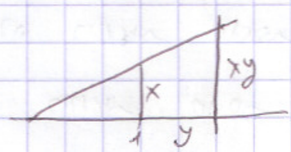


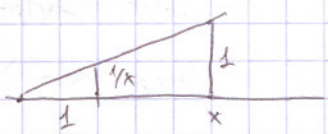
נסמן את שני הנקודות הראשונות ב- 0,1, ואת הישר דרכן ב- $\mathbb{R}$.

<u>טענה:</u> $A\cap\mathbb{R}$ שדה, הסגור להוצאת שורש ממספר חיובי.

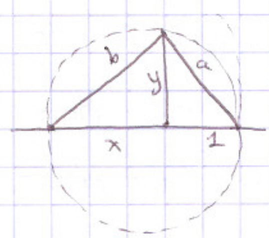
כיוון ראשון:

- לבנות קטע שאורכו סכום האורכים של קטעים נתונים.
- לבנות קטע שאורכו מכפלת אורכים.





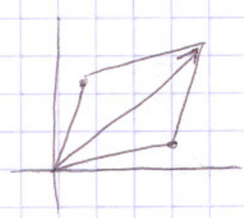
- הוצאת שורש:



$$x^2+y^2=b^2$$
$$1+y^2=a^2$$
$$x^2+2x+1=(x+1)^2=a^2+b^2$$
$$\overline{\qquad\qquad}$$
$$x=y^2$$

<u>טענה:</u> $A^{\subseteq\mathbb{C}}$ שדה, הסגור להוצאת שורש.

- חיבור וקטורים



- כפל מספרים מרוכבים: כפל האורכים
חיבור זווית

- $\frac{1}{|z|}=\frac{|\bar{z}|}{|z\bar{z}|}$

- חצוי שורש מהאורך + חצוי זווית } $\Leftarrow$ ($\sqrt{z}\in A \Leftarrow z\in A$)

סימון: A הוא תת-השדה הקטן ביותר של $\mathbb{C}$ שסגור להוצאת שורש.

הגדרה: E הוא הרחבה ריבועית חוזרת אם יש שרשרת הרחבות ריבועיות

$$\mathbb{Q} \subset F_1 \subset F_2 \subset \dots \subset F_n = \mathbb{Q}[\alpha]$$

משפט: התנאים הבאים שקולים:

(1) $\alpha \in A$

(2) α שייך להרחבה ריבועית חוזרת, E.

(3) α שייך להרחבה ריבועית חוזרת שהיא הרחבת גלואה של $\mathbb{Q}$

(4) $\mathbb{Q}[\alpha]$ הרחבה ריבועית חוזרת

(5) חבורת גלואה של ((שדה הפיצול של) הפולינום המינימלי של α) היא חבורת-2. ($Gal(E/\mathbb{Q}) = 2^{?}$)

הוכחה: (1) $\Rightarrow$ (2): כל איבר של A נבנה משורשים.

(2) $\Rightarrow$ (3): נניח ש-E הרחבה ריבועית חוזרת

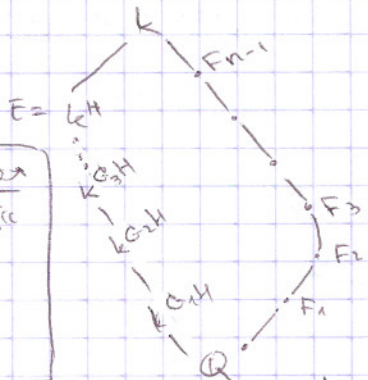
(כלומר $E = \mathbb{Q}[t]$) ויהי K שדה הפיצול של הפולינום

המינימלי של t. כלומר $K = \mathbb{Q}[t_1, \dots, t_n]$

כאשר $t_1 = t$ ו-t_i הם הצמודים של t.

K היא הרחבה ריבועית חוזרת כי הרכבה של שרשראות.

(3) $\Rightarrow$ (4): נניח K הרחבה ריבועית חוזרת שהיא גם גלואה, $E \subseteq K$.



נסמן $E = K^H$, את החבורה

נסמן ב- $F_i = K^{G_i}$

$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n = 1$

$G_0H \supset G_1H \supset \dots \supset H$

תזכורת: $G_{i+1} \triangleleft G_i$ ⇐

$HG_{i+1} \triangleleft HG_i$

(4) $\Rightarrow$ (1): ישר מהגדרת A.

(3) $\Rightarrow$ (5): $|Gal(K/\mathbb{Q})| = [K:\mathbb{Q}] = 2^n$

(כי הוא מכפלה של שרשרת של הרחבות ריבועיות)

(5) $\Rightarrow$ (2): נתון ש- $|G| = |Gal(\ )| = 2^n$

יש שרשרת תת $G \supset G_1 \supset G_2 \supset \dots \supset G_n = 1$

עם $[G_i : G_{i+1}] = 2$ לפי משפט על שרשרת

תמה ההוכחה את השדות.

09.01.14 תרג' ה' שאלה תשע'

א נניח לשלילה $\Leftarrow \not\Rightarrow$ $[\mathbb{Q}[\alpha]:\mathbb{Q}] = 2^n$