19.12.13 חמישי ט"ז טבת התשע"ד

אלגברה מופשטת 3 - הרצאה מס' 10

שורשי יחידה

$\rho \in \mathbb{C}, \quad \rho^n = 1$ (פרימיטיבי)

מהו הפולינום המינימלי של ρ מעל $\mathbb{Q}$.

$$(*) \quad x^n - 1 = \prod_{d|n} \Phi_d(x) \quad \text{(מגדיר את } \Phi_n\text{)}$$

$$\Updownarrow$$

$$\Phi_d(n) = \prod_{(i,d)=1} \left(x - \rho^{ni/d}\right)$$ מאפס כל שורש יחידה פרימיטיבי מסדר d.

$$= \rho_n^{\frac{n}{d}\cdot i} = (\underbrace{\rho_n^{n/d}}_{\rho_d})^i$$

$(*) \Leftarrow \quad \Phi_n(x) \in \mathbb{Z}[x]$ מהלמה של גאוס,

באינדוקציה, מכיוון ש- $\Phi_d(x) \in \mathbb{Z}[x]$ לכל $d<n$ (מתוקנים) וגם $x^n - 1 \in \mathbb{Z}[x]$

$+ \quad \Phi_n(x) \in \mathbb{Q}[x] \Leftarrow \Phi_n(x) \in \mathbb{Z}[x]$.

n	$\Phi_n(x)$
1	$x-1$
2	$x+1$
3	x^2+x+1
4	x^2+1
5	$x^4+x^3+x^2+x+1$
6	x^2-x+1
p	$x^{p-1}+\dots+1$
8	x^4+1
9	
10	
12	x^4-x^2+1

$\Phi_n(x)=\prod(x-\rho')$
לכל ρ' כך ש- $o(\rho')=n$ ($\mathbb{C}^*$)

משפט: לכל n, $\Phi_n(x)$ אי-פריק מעל $\mathbb{Q}$ ($\Leftrightarrow$ מעל $\mathbb{Z}$).

הוכחה: (כמובן) מעל $\mathbb{Z}$.

נניח ש- $\Phi_n(x)=g\cdot h$, g אי-פריק.

מכיוון שגם ל-g וגם ל-h יש שורשים,

קיימים ראשוני p ושורש ρ של g כך ש- ρ^p שורש של h.

$h(x^p)$ מאפס את ρ ולכן $g|h(x^p)$ מעל $\mathbb{Q}$ ולכן מעל $\mathbb{Z}$.

מודולו p, $g(x)|h(x^p)=h(x)^p$ מעל $\mathbb{Z}/p\mathbb{Z}$.

כמו כן, $g|\Phi_n(x)|x^n-1$ מודולו p, אבל $(x^n-1)'=nx^{n-1}\neq 0$

ואז ל- x^n-1 מודולו p.

לכן x^n-1 ספרבילי מעל $\mathbb{Z}/p\mathbb{Z}$ ולכן גם g ספרבילי מעל $\mathbb{Z}/p\mathbb{Z}$.

לכן מ- $g|h^p$ נובע $g|h$ מודולו p.

אבל אז $g^2|gh=\Phi_n(x)|x^n-1$ וזו סתירה לספרביליות.

מסקנה: $[\mathbb{Q}[\rho_n]:\mathbb{Q}]=\deg\Phi_n(x)=\varphi(n)$.

- מזה נובע ש- $\mathbb{Q}[\rho_n]$ שדה של $\Phi_n(x)$ וגם של x^n-1

ולכן זו הרחבת גלואה של $\mathbb{Q}$.

$U_n\cong Aut(\mathbb{Z}_n)$
$U_n=\{1\le k\le n \mid (k,n)=1\}$

משפט: $Gal(\mathbb{Q}[\rho_n]/\mathbb{Q})\cong U_n$

נגדיר העתק מ- U_n ל- $Gal(\mathbb{Q}[\rho_n]/\mathbb{Q})$ כך

$k\mapsto(\rho\mapsto\rho^k)$.

לכל k זר ל- n, ρ^k שורש של $\Phi_n(x)$ שהוא אי-פריק ולכן

$$\mathbb{Q}[\rho]\cong\mathbb{Q}[x]/\langle\Phi_n(x)\rangle\cong\mathbb{Q}[\rho^k]=\mathbb{Q}[\rho]$$

$$\mathbb{Q}[\rho]\xrightarrow[\text{איזו}]{\varphi_k}\mathbb{Q}[\rho]$$

נסתכל לשורשים <u>שכולם</u> יודעים:

$$\rho_3=\frac{-1+\sqrt{-3}}{2}=\cos\left(\frac{2\pi}{3}\right)+i\sin\left(\frac{2\pi}{3}\right)$$

$$\rho_5=\cos\left(\frac{2\pi}{5}\right)+i\sin\left(\frac{2\pi}{5}\right)$$

נחשוב על ρ_5 מעל $\mathbb{Q}$:

19.12.13

המשך ט"ז סגור משפט

שדה הפיצול: $\mathbb{Q}[\rho,\rho^2,\rho^3,\rho^4]=\mathbb{Q}[\rho]$

חבורת גלואה: $\{1,2,3,4\}=U_5=\langle 2\rangle\cong\mathbb{Z}_4$ עם כפל מודולו 5

[הערה: $U_p=(\mathbb{Z}/p\mathbb{Z})^*$ ציקלית כי היא חבורה כפלית סופית בשדה]

למשל האוטו' $\sigma:\rho\to\rho^2$ יוצר את החבורה

$$\begin{array}{ccc} K & & \\ | & H & \\ K^H & & G \\ | & G/H & \\ F=K^G & & \end{array}$$

$$\begin{array}{ccc} \mathbb{Q}[\rho] & & 1 \\ | \;\sigma^2 & \mathbb{Q}[\sqrt{5}] & | \\ \mathbb{Q}[\rho+\rho^{-1}]=\mathbb{Q}[\rho]^{\sigma^2} & & \langle\sigma^2\rangle=H \\ | & & | \\ \mathbb{Q} & \langle\sigma\rangle & \langle\sigma\rangle \end{array}$$

$$\alpha=2\cos\left(\tfrac{2\pi}{5}\right)$$

$$\sigma:\underset{\alpha}{\rho+\rho^{-1}}\longmapsto\rho^2+\rho^{-2}\overset{\circledast}{=}-1-\alpha$$

$$\circledast\quad I_5(\lambda)=\rho^4+\rho^3+\rho^2+\rho+1=0$$

$$\rho^2+\rho+1+\rho^{-1}+\rho^{-2}=0$$

$$\alpha^2=\rho^2+\rho^{-2}+2$$

$$\alpha^2+\alpha=\rho^2+\rho^{-2}+\rho+\rho^{-1}+2=1$$

$$\alpha^2+\alpha-1=0$$

$$\underset{2\cos\left(\frac{2\pi}{5}\right)}{\alpha}=\frac{-1\pm\sqrt{5}}{2}$$

ρ_{17}: $\Phi_{17}(x)$

$$Gal(\mathbb{Q}[\rho_{17}]/\mathbb{Q})=U_{17}\cong\mathbb{Z}_{16}=\langle 3\rangle$$

$$\begin{array}{lll}] & 1 & \\ [\ldots] & \langle\sigma^8\rangle & \rho\longmapsto\rho^{-1} \\ [\ldots] & \langle\sigma^4\rangle & \rho\to\rho^{13} \\ [\ldots] & \langle\sigma^2\rangle & \rho\to\rho^{9} \\ & \langle\sigma\rangle & \rho\longmapsto\rho^{3} \end{array}$$

$$\sigma:\rho\longrightarrow\rho^3$$

$$\cos\left(\frac{2\pi}{17}\right)=\frac{1}{8}\left[\frac{\sqrt{17}-1}{2}+\sqrt{\frac{17-\sqrt{17}}{2}}+\sqrt{(3+\sqrt{17})(\ldots)(\ldots-\sqrt{17\ldots}}\ldots\right.$$

הרחבות ציקליות

טענה: נניח F שדה שמכיל כל ל-n, $\rho=\rho_n\in F$.

אם הפולינום $x^n-a\in F[x]$ אי-פריק אז שדה הפיצול

הוכחה: נסמן $\alpha=\sqrt[n]{a}$.

השורשים של הפולינום הם $\rho^k\alpha$, $k=0,\dots,n-1$

לכן שדה הפיצול הוא $F[\alpha,\rho\alpha,\dots,\rho^{n-1}\alpha]=F[\alpha,\rho]=F[\alpha]$

[הערה: אפשר לנסח את הטענה הכללית אנלוגית:

ננית F שדה ממאפיין זר ל-n,

אם הפולינום $x^n-a\in F[x]$ אי-פריק אז שה"פ הוא $F[\sqrt[n]{a},\rho]$

וחבורת גלואה שלו מעל $F[\rho]$ היא $\mathbb{Z}/n\mathbb{Z}$.]

תשובה: ($\rho\in F$) חבורת גלואה של $F[\alpha]/F$:

מסדר n לפי המשפט ולכן k:

$\sigma_k:\alpha\longmapsto\rho^k\alpha$ מגדיר אוטו'

$\sigma_k\cdot\sigma_{k'}=\sigma_{k+k'}$

לכן $Gal(K/F)\cong\mathbb{Z}/n\mathbb{Z}$.

...חבה מהצורה $K=F[\sqrt[n]{a}]/F$ נקראת הרחבה שורשית.

...חבה ציקלית = הרחבת גלואה שחבורת גלואה שלה היא ציקלית.

המשפט: אם $\rho\in F$, כל הרחבה שורשית מסדר n היא ציקלית.

...פט: יהי F שדה עם $\rho_n\in F$.

אז כל הרחבה ציקלית ממימד n היא שורשית.

תזכורת: יהי K/F הרחבת גלואה עם חבורה $G=Gal(K/F)$

הנורמה $N_{K/F}:K\longrightarrow F$ מוגדרת לפי

$$N_{K/F}(\alpha)=\prod_{\sigma\in G}\sigma(\alpha)$$

בפרט, אם $G=\langle\sigma\rangle\cong\mathbb{Z}/n\mathbb{Z}$, $N(\alpha)=\prod_{i=0}^{n-1}\sigma^i(\alpha)$

הערה: יהי K/F הרחבה ציקלית עם $Gal(K/F)=\langle\sigma\rangle$

אז לכל $y\in K^*$,

$$N\left(\frac{\sigma(y)}{y}\right)=\prod_{0}^{n-1}\sigma^i\left(\frac{\sigma(y)}{y}\right)=\frac{\prod_{1}^{n}\sigma^i(y)}{\prod_{0}^{n-1}\sigma^i(y)}=\frac{\sigma^n(y)}{y}=1$$

משפט 90 של הילברט: יהי K/F הרחבה ציקלית.

1.12.13

[illegible]

$y \in K^*$ [illegible] ש- $x = \frac{\sigma(y)}{y}$.