ניתן להכליל את $N_{L/K}$ גם למקרה המקומי:

$$N_{L/K} : I(\mathcal{O}_L) \longrightarrow I(\mathcal{O}_K)$$

(אידיאלים שברים)

$$N_{L/K} : Cl(\mathcal{O}_L) \longrightarrow Cl(\mathcal{O}_K)$$

כי נורמה של עקרון = עקרון.

הרצאה 10

18/12/12

שדות מספרים

מעניינים כאלה ש- $\mathbb{Q} \subseteq K$, $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$. K שדה מספרים $\Leftrightarrow$ $K/\mathbb{Q}$ הרחבה סופית. (ניתן לשים K כ- $\mathbb{Q}$-ו.ו)

כלומר -

$\mathcal{O}_K$ הוא $\mathbb{Z}$-מ.ש.ח. דרגה $[K:\mathbb{Q}]$ (הוכחנו בתרגול)

נזכיר את ג'נרלים שלמדנו ב- $\mathcal{O}_K$: ג'נרל $N_{K/\mathbb{Q}}(I)$ של $I \subseteq \mathcal{O}_K$ הוא $|\mathcal{O}_K/I|$. נסמן $N(I) := |\mathcal{O}_K/I|$ - **הנורמה האידיאלית** של I. כלומר, $N(I) = (I\mathcal{O}_K)^{\mathbb{Q}}_{norm}$, וכן, $N(I\mathcal{O}_K) = N(I)$.

ו, בפרט, $N(I\mathcal{O}_K)$ קובעים **מספר** (Counting norm) שכן $|\mathcal{O}_K/I| = N(I)$. **נזכיר:** כי ה CRT בי ו הניח $I = p^k$, p ראשוני ב- $\mathbb{Z}$. אז, $\mathcal{O}_K/I \cong \mathcal{O}_K/p^k$ כמ"מ $\mathbb{Z}/p^k$. יתר (מהעזרה) $(\mathcal{O}_K/I)^* \cong$.

כיוון ש- $p = \#\mathbb{Z}/p$, נקבל ש-

$$N(p^k) = N(p)^k = p^{fk} = \#\mathcal{O}_K/p^k = \#\mathcal{O}_K/I$$

סכום של שני ריבועים

משפט: (פרמה)

מספר טבעי n הוא סכום של שני ריבועים $\Leftrightarrow$ לכל $p \equiv 3 \pmod 4$, $v_p(n)$ זוגי.

מסקנה: (משפט פרמה)

$$\#\{x=n \mid \exists a,b\in\mathbb{Z}\ a^2+b^2=n\} = \text{מעריך של } p \text{ ב-} n \text{ בפירוק לראשוניים}$$

(ו) הוכחה

הוכחה: $n=\mathrm{Norm}_{\mathbb{Z}[i]/\mathbb{Z}}(z) \Leftrightarrow a^2+b^2=n$ עבור $z=a+bi\in\mathbb{Z}[i]$. נסמן $n=\prod_j p_j^{a_j}$ כפירוק לראשוניים ב-$\mathbb{Z}$. אז

$$\mathbb{Z}[i] = \prod_j \mathfrak{p}_j^{a_j}$$

$$N(z) = \prod_{j:f(\mathfrak{p}_j)=1} \mathfrak{p}_j^{a_j} \cdot \prod_{j:f(\mathfrak{p}_j)=2} \mathfrak{q}_j^{a_j/2}$$

$$\mathbb{Z}\cap\mathfrak{p}_j = p_j \qquad \mathbb{Z}\cap\mathfrak{q}_j = p_j$$

$$f(\mathfrak{p}_j)=1 \Leftrightarrow p_j\equiv 1 \pmod 4 \quad \text{או} \quad p_j=2 \qquad f(\mathfrak{p}_j)=2 \Leftrightarrow p_j\equiv 3 \pmod 4$$

לכן n מיוצג כסכום שני ריבועים $\Leftrightarrow$ כל ראשוני $3 \bmod 4$ מופיע בפירוק שלו בחזקה זוגית. (זה נובע מכך ש-$\mathbb{Z}[i]$ הוא PID ולכן $\mathfrak{p}$ ראשוני $\Leftrightarrow$ $\mathbb{Z}[i]/\mathfrak{p}$ שדה סופי, $\mathfrak{p}=(p)$ או $\mathfrak{p}=(z)$ כאשר $z\bar{z}=p$ ראשוני ב-$\mathbb{Z}$ ו-$p\equiv 3 \bmod 4$ אם ורק אם p ראשוני ב-$\mathbb{Z}[i]$.)

$\square$

הוכחה: יהי p ראשוני. נסמן $\mathbb{Z}[i]/(p)=\mathbb{Z}[x]/(x^2+1,p)=\mathbb{Z}[x]/(x-a)(x+a)$ כאשר $a^2\equiv -1 \pmod p$. אם $p=2$ אז $a=1$ ו-$(x-1)(x+1)=(x-1)^2$ ולכן $(x-1)$ אינו ראשוני. אם $p\equiv 1 \pmod 4$ אז $a\neq -a$ ו-$(x-a)$ אינו ראשוני. אם $p\equiv 3 \pmod 4$ אז -1 אינו שארית ריבועית מודולו p ולכן $(x+a)$ ראשוני.

שאלה: מהי חבורת האוטומורפיזמים $\mathrm{Aut}(\mathbb{Z}[\sqrt{-5}])$?

טענה: יהי θ שורש של x^2+5 ב-$\mathbb{C}$. אז $\mathbb{Q}(\theta)=\mathbb{Q}(\sqrt{-5})$ ו-$[\mathbb{Q}(\theta):\mathbb{Q}]=2$.

הוכחה: $\mathbb{Z}[\sqrt{-5}]=\mathbb{Z}[\theta]$ הוא תחום שלמות שאינו שדה, ולכן $\mathbb{Z}[\sqrt{-5}]^\times=\{\pm 1\}$. כל אוטומורפיזם σ של $\mathbb{Z}[\sqrt{-5}]$ נקבע על ידי $\sigma(\theta)$, שהוא שורש של x^2+5. לכן $\mathrm{Aut}(\mathbb{Z}[\sqrt{-5}])\cong\mathbb{Z}/2\mathbb{Z}$.

שאלה: מהי $\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}$?

טענה: יהי $\mathbb{Q}(\sqrt{-5})$ שדה מספרים. אז $\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}=\mathbb{Z}[\sqrt{-5}]$.

הוכחה: יהי $\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}$ חוג השלמים של $\mathbb{Q}(\sqrt{-5})$. אז $\mathbb{Z}[\sqrt{-5}]\subseteq\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}$. יהי $\alpha\in\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}$. אז $\alpha=a+b\sqrt{-5}$ עבור $a,b\in\mathbb{Q}$. נסמן $\alpha=\frac{x}{y}$ כאשר $x,y\in\mathbb{Z}[\sqrt{-5}]$ ו-$\gcd(x,y)=1$. אז α שורש של $y^2x^2-x^2=0$. נסמן $y=c+d\sqrt{-5}$. אז $y^2=c^2-5d^2+2cd\sqrt{-5}$. נסמן $N(y)=c^2+5d^2$. אז $N(y)\mid x^2$. נסמן $x=e+f\sqrt{-5}$. אז $N(x)=e^2+5f^2$. נסמן $N(y)=p_1^{a_1}\cdots p_k^{a_k}$. אז $p_i\mid x^2$ לכל i. נסמן $p_i=\mathfrak{p}_i\mathfrak{p}_i'$. אז $\mathfrak{p}_i\mid x$ או $\mathfrak{p}_i'\mid x$. נסמן $x=\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_k^{b_k}\mathfrak{q}_1^{c_1}\cdots\mathfrak{q}_m^{c_m}$. אז $N(x)=p_1^{2b_1}\cdots p_k^{2b_k}q_1^{2c_1}\cdots q_m^{2c_m}$. נסמן $N(y)=p_1^{a_1}\cdots p_k^{a_k}$. אז $2b_i\geq a_i$ לכל i. נסמן $b_i=\lceil\frac{a_i}{2}\rceil$. אז $\mathfrak{p}_i^{b_i}\mid x$. נסמן $x=\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_k^{b_k}z$. אז $z\in\mathbb{Z}[\sqrt{-5}]$. נסמן $\alpha=\frac{x}{y}=\frac{\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_k^{b_k}z}{y}$. אז $\alpha\in\mathbb{Z}[\sqrt{-5}]$. לכן $\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}=\mathbb{Z}[\sqrt{-5}]$.

שאלה: מהי חבורת האוטומורפיזמים $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})})$?

טענה: יהי $\mathbb{Q}(\sqrt{-5})$ שדה מספרים. אז $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})})\cong\mathbb{Z}/2\mathbb{Z}$.

הוכחה: $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})})=\mathrm{Aut}(\mathbb{Z}[\sqrt{-5}])\cong\mathbb{Z}/2\mathbb{Z}$.

שאלה: מהי חבורת האוטומורפיזמים $\mathrm{Aut}(\mathbb{Z}[\sqrt{-d}])$ עבור $d>0$?

טענה: יהי $d>0$ שלם חופשי מריבועים. אז $\mathrm{Aut}(\mathbb{Z}[\sqrt{-d}])\cong\mathbb{Z}/2\mathbb{Z}$ אם $d\neq 1,3$, ו-$\mathrm{Aut}(\mathbb{Z}[\sqrt{-d}])\cong\mathbb{Z}/4\mathbb{Z}$ אם $d=1$, ו-$\mathrm{Aut}(\mathbb{Z}[\sqrt{-d}])\cong\mathbb{Z}/6\mathbb{Z}$ אם $d=3$.

הוכחה: יהי θ שורש של x^2+d. אז $\mathbb{Q}(\theta)=\mathbb{Q}(\sqrt{-d})$ ו-$[\mathbb{Q}(\theta):\mathbb{Q}]=2$. $\mathbb{Z}[\sqrt{-d}]=\mathbb{Z}[\theta]$ הוא תחום שלמות שאינו שדה, ולכן $\mathbb{Z}[\sqrt{-d}]^\times=\{\pm 1\}$ אם $d\neq 1,3$, $\mathbb{Z}[\sqrt{-d}]^\times=\{\pm 1,\pm i\}$ אם $d=1$, ו-$\mathbb{Z}[\sqrt{-d}]^\times=\{\pm 1,\pm\omega,\pm\omega^2\}$ אם $d=3$ כאשר $\omega=\frac{-1+\sqrt{-3}}{2}$. כל אוטומורפיזם σ של $\mathbb{Z}[\sqrt{-d}]$ נקבע על ידי $\sigma(\theta)$, שהוא שורש של x^2+d. לכן $\mathrm{Aut}(\mathbb{Z}[\sqrt{-d}])\cong\mathbb{Z}/2\mathbb{Z}$ אם $d\neq 1,3$, $\mathrm{Aut}(\mathbb{Z}[\sqrt{-d}])\cong\mathbb{Z}/4\mathbb{Z}$ אם $d=1$, ו-$\mathrm{Aut}(\mathbb{Z}[\sqrt{-d}])\cong\mathbb{Z}/6\mathbb{Z}$ אם $d=3$.

שאלה: מהי חבורת האוטומורפיזמים $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})})$?

טענה: יהי $d>0$ שלם חופשי מריבועים. אז $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})})\cong\mathbb{Z}/2\mathbb{Z}$ אם $d\neq 1,3$, $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})})\cong\mathbb{Z}/4\mathbb{Z}$ אם $d=1$, ו-$\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})})\cong\mathbb{Z}/6\mathbb{Z}$ אם $d=3$.

הוכחה: $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})})=\mathrm{Aut}(\mathbb{Z}[\sqrt{-d}])$.

שאלה: מהי חבורת האוטומורפיזמים $\mathrm{Aut}(\mathbb{Z}[\sqrt{d}])$ עבור $d>0$?

טענה: יהי $d>0$ שלם חופשי מריבועים. אז $\mathrm{Aut}(\mathbb{Z}[\sqrt{d}])\cong\mathbb{Z}/2\mathbb{Z}$.

הוכחה: יהי θ שורש של x^2-d. אז $\mathbb{Q}(\theta)=\mathbb{Q}(\sqrt{d})$ ו-$[\mathbb{Q}(\theta):\mathbb{Q}]=2$. $\mathbb{Z}[\sqrt{d}]=\mathbb{Z}[\theta]$ הוא תחום שלמות שאינו שדה, ולכן $\mathbb{Z}[\sqrt{d}]^\times=\{\pm 1\}$. כל אוטומורפיזם σ של $\mathbb{Z}[\sqrt{d}]$ נקבע על ידי $\sigma(\theta)$, שהוא שורש של x^2-d. לכן $\mathrm{Aut}(\mathbb{Z}[\sqrt{d}])\cong\mathbb{Z}/2\mathbb{Z}$.

שאלה: מהי חבורת האוטומורפיזמים $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{d})})$?

טענה: יהי $d>0$ שלם חופשי מריבועים. אז $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{d})})\cong\mathbb{Z}/2\mathbb{Z}$.

הוכחה: $\mathrm{Aut}(\mathbb{Z}_{\mathbb{Q}(\sqrt{d})})=\mathrm{Aut}(\mathbb{Z}[\sqrt{d}])$.

$$\frac{2p\,91}{2q-2a} \in \mathbb{Z}$$

f פתיר $\Leftrightarrow$ $\frac{p^2}{a} \in \mathbb{Z}$

המינימלי (מצא) $x^2 - \frac{p^2}{a}x + \frac{2p\,91}{2q-2a}$

$$f_2 = \frac{1}{2p}\begin{pmatrix} a & 1 \\ pq & a \end{pmatrix}$$

שכיח מינימלי של כפל f: $(0,1,0,0,\dots)$

$$f = \frac{1}{2p}(0q+a)\,,\quad a,q \in \mathbb{Z}$$

לכן, $\mathbb{Z}[\frac{1}{2p}][\Theta] \supseteq \mathbb{Z}[\Theta]$. מאחר ש- $p \neq 2$ שדה מספרים ריבועי. נסמן $\sqrt{p} = \Theta$. אז $p = \Theta^2$. ריבועי

כלומר הסיומת מהצורה $[\mathbb{Q}:\mathbb{Q}] = 2$ ולפיכך $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\Theta)$

הערה כיצד

מאחר ש- $\mathbb{Z}[\Theta]$ היא חוג. עבור S_3 נבחר 2 ו- Θ. לכן נבחר

$$\mathbb{Z}\ni \frac{b}{c} = \frac{1}{4} + \frac{1}{2}$$

ולכן המינימלי שלה הוא -

$$\frac{2\Theta+\Theta}{2} \rightsquigarrow \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \Rightarrow$$

$$\Theta \rightsquigarrow \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \Theta^2 \rightsquigarrow \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

נבחן מינימלי כזה $\mathbb{Z}_2, \mathbb{Z}_3, 1$.

ל- $\frac{2\Theta+\Theta}{2}$ אחת בסיס $\mathbb{Z}$ המינימלי הוא:

$\frac{2\Theta+\Theta}{2}$ שהם. (תשלב)

מכאן שאין. רק הקבוצה של- $\frac{2\Theta+\Theta}{2}$, $\frac{2}{2}$, $\frac{2\Theta+1}{2}$ ו $\frac{2\Theta+\Theta+1}{2}$ הם בסיס $\mathbb{Z}$: כי קבוצת $\mathbb{Z}$ שאין $\mathbb{Z}_3, \mathbb{Z}_3$ כי הסדר, $\neq 0$

תזכורת: $(\mathbb{Z}_2^2)\mathbb{Q} = 7$, המינימלי $g - [\mathbb{Z}_2^2]\mathbb{Z} = 7$. כלומר $\mathbb{Z}_3^2 - x^2$. נקבל:

$\Leftarrow$ $A \in \mathbb{Z}$, $Ap^2 = a$. לכן,

$$\frac{a^2 - db^2}{4p^2} = \frac{A^2p^2 - db^2}{4p^2} \in \mathbb{Z}$$

לכן $4p^2 \mid a^2 - db^2$. מאידך, כפכם $4p^2 \mid db^2$ ולכן $4p^2 \mid A^2p^2 d$.
ולכפכם $2 \mid A$. ע"ג p הסר כלומר, כי $2 \mid b$.
יהי $q \mid p^2$. לכן B/q שלם (מפני ש $B^2 = B/q$ נשלם).
יהי $Bp^2 = q$. ואז, $\frac{\theta B + A}{2} = \gamma$. הפולינום המינימלי
של γ (מכיוון ש $\theta \neq \beta$ ואינו שם הפולינום המינימלי)

$$x^2 - Ax + \frac{A^2 - dB^2p^2}{4}$$

וזה שלם –

$$\gamma = \frac{\alpha + \beta\theta}{2} + \beta(\theta)$$

$\mathbb{Z}[\theta]$ כאשר α, β כלשהם – γ שלם אם ורק אם
לכן יש לנו שתי אפשרויות: $\alpha = 0, \beta = 1$ כלומר θ
" " " $\alpha = 1, \beta = 0$ " $\frac{\theta+1}{2}$

לכן –

① $\mathbb{Z}[\theta] = \mathcal{O}_Q$

② $\frac{\theta+1}{2}$ שלם. ואז, $\mathbb{Z}[\frac{\theta+1}{2}] = \mathcal{O}_Q$.

$\Updownarrow$

$x^2 - x + \frac{1-p^2}{4} \in \mathbb{Z}[x]$

$\Updownarrow$

$p \equiv 1 \pmod 4$

סיכום:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\theta], & d \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{\theta+1}{2}], & d \equiv 1 \pmod 4 \end{cases}$$

לכן מספק כולנו שם שאלות ו תשובות!

$[M:\mathbb{Q}] =$ מימד – שדה מספרי שדה מספרי

דוגמאות ו שאלות

תהי L/K הרחבה סופית מדרגה n, ויהי $\sigma \in \mathrm{Aut}(L)$ כך ש- $\sigma|_K = \mathrm{id}_K$. נסמן $H = \langle \sigma \rangle$. אזי $[L:L^H] = [K:K]$.

הוכחה: ① ברור כי $L^H \supseteq K$.

② נראה כי $L^H = K$. נניח בשלילה כי $L^H \supsetneq K$, אז קיים $\alpha \in L^H \setminus K$.

③ α אלגברי מעל K $\Rightarrow$ $K(\alpha)/K$ הרחבה נורמלית (מדוע?)

α - $K(\alpha)$ מעל K.

$*-(\zeta_3 = e^{2\pi i/3})\ \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q} = M$, $\mathbb{Q} = L \cap M$. יהי -

$[L:\mathbb{Q}] = 3$, $[M:\mathbb{Q}] = 2$

$\mathrm{Gal}(M/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3$

(לא הוכחנו)

מסקנה - L/K מורחבת גלואה $\Leftrightarrow$ $|\mathrm{Aut}_K(L)| = [L:K]$

הוכחה

$$\mathrm{Hom}_K(M, \mathbb{C}) \xrightarrow{\text{res}} \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$$

כל $\mathbb{Q}$-הומומורפיזם $L \to \mathbb{C}$ מוגדר על ידי $\sqrt[3]{2} \mapsto$ אחד משלושת השורשים של x^3-2

σ ו- id הם כל ההומומורפיזמים $L \to L$ $\Leftrightarrow$ $L/\mathbb{Q}$ נורמלית.

משפט שקיים - $\mathrm{Tr}_{M/K}(x) = \mathrm{Tr}_{L/K}(x)^{M/L}$

משפט: $M = N \supseteq K$ שדות. N סופית. $[N:K] = n$ ו- M מוכלת

ב- $\mathbb{C}$. אזי, $|\mathrm{Hom}_K(N, \mathbb{C})| \leq n$

הוכחה: באינדוקציה על n. עבור $n=1$ הטענה ברורה. נניח שהטענה נכונה עבור $n-1$ ונוכיח עבור n. יהי $\sigma_0 \in \mathrm{Hom}_K(N, \mathbb{C})$ כלשהו. נבחר $\alpha \in N \setminus K$. α אלגברי מעל K, יהי $f(x) \in K[x]$ הפולינום המינימלי של α מעל K. $\deg f = d > 1$. f פריק מעל $\mathbb{C}$, $f = (x-\alpha_1)\cdots(x-\alpha_d)$, $\alpha = \alpha_1$. $\sigma_0(\alpha) = \alpha_i$ עבור i כלשהו. σ_0 מוגדר על ידי $\alpha \mapsto \alpha_i$ ועל K הוא id

ζ_m שורש יחידה מסדר m אם $\zeta_m^m = 1$ ו- $\zeta_m^k \neq 1$ לכל $0 < k < m$.

משפט: יהי ζ_m שורש יחידה מסדר m. אז $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$.

הוכחה: נסמן $\zeta = \zeta_m$. נתבונן ב- $\mathbb{Q}(\zeta)$.

ζ הוא שורש של $x^m - 1$, ולכן הוא שורש של כל פולינום מתוקן $f(x) \in \mathbb{Q}[x]$ שהוא הפולינום המינימלי של ζ מעל $\mathbb{Q}$.

נסמן $f(x) = \Phi_m(x)$ (הפולינום המחזורי ה- m-י). נוכיח ש- $\Phi_m(x) \in \mathbb{Z}[x]$ ואי-פריק מעל $\mathbb{Q}$.

נוכיח באינדוקציה על m. עבור $m = 1$: $\Phi_1(x) = x - 1$.

נניח שהטענה נכונה לכל $k < m$. מתקיים:

$$x^m - 1 = \prod_{d \mid m} \Phi_d(x)$$

לכן:

$$\Phi_m(x) = \frac{x^m - 1}{\prod_{d \mid m,\, d < m} \Phi_d(x)}$$

מכיוון שהמכנה הוא מתוקן ושייך ל- $\mathbb{Z}[x]$ (לפי הנחת האינדוקציה), ומכיוון שחילוק פולינומים מתוקנים נותן פולינום מתוקן, נובע ש- $\Phi_m(x) \in \mathbb{Z}[x]$.

טענה: $\Phi_m(x)$ אי-פריק מעל $\mathbb{Q}$.

הוכחה: נניח בשלילה ש- $\Phi_m(x) = g(x)h(x)$ עם $g, h \in \mathbb{Z}[x]$ מתוקנים ולא קבועים. נסמן $g(\zeta) = 0$.

יהי p ראשוני כך ש- $p \nmid m$. נוכיח ש- $g(\zeta^p) = 0$.

נניח בשלילה ש- $h(\zeta^p) = 0$. אז ζ הוא שורש של $h(x^p)$, ולכן $g(x) \mid h(x^p)$ ב- $\mathbb{Q}[x]$.

נסמן $h(x^p) = g(x)k(x)$. נעבור למודולו p: $\bar{h}(x^p) = \bar{g}(x)\bar{k}(x)$.

מכיוון ש- $\mathbb{F}_p$ שדה מאפיין p, מתקיים $\bar{h}(x^p) = \bar{h}(x)^p$ (חזקת פרובניוס).

לכן $\bar{g}(x) \mid \bar{h}(x)^p$, ומכאן ש- $\bar{g}$ ו- $\bar{h}$ חולקים גורם משותף.

אבל $\bar{g}(x) \mid x^m - 1$ ב- $\mathbb{F}_p[x]$, ולכן $x^m - 1$ יש שורש כפול, כלומר $\gcd(x^m - 1, mx^{m-1}) \neq 1$. זה קורה רק כאשר $p \mid m$, בסתירה להנחה.

לכן $g(\zeta^p) = 0$ לכל $p \nmid m$.

באינדוקציה על k, $g(\zeta^k) = 0$ לכל $\gcd(k, m) = 1$.

כל שורש של Φ_m הוא מהצורה ζ^k עבור $\gcd(k, m) = 1$, ולכן $g = \Phi_m$, בסתירה לכך ש- g לא קבוע.

לכן $\Phi_m(x)$ אי-פריק מעל $\mathbb{Q}$.

מסקנה: $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \deg \Phi_m = \varphi(m)$.

דוגמה: $\Phi_1(x) = x - 1$

$\Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1$

$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$ עבור p ראשוני

$\Phi_4(x) = \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1$

$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1$

תכונות:

1. $\deg \Phi_m = \varphi(m)$
2. $\Phi_m(x) = \prod_{\gcd(k,m)=1} (x - \zeta_m^k)$
3. $\Phi_m(x) \in \mathbb{Z}[x]$ מתוקן ואי-פריק מעל $\mathbb{Q}$
4. $x^m - 1 = \prod_{d \mid m} \Phi_d(x)$
5. $\mathbb{Z}[\zeta_m] = \mathcal{O}_{\mathbb{Q}(\zeta_m)}$
6. יהי p ראשוני, $p \nmid m$. אז $\Phi_m(x)$ מתפרק מעל $\mathbb{F}_p$ למכפלת גורמים ממעלה $\operatorname{ord}_m(p)$, כאשר $\operatorname{ord}_m(p)$ הוא הסדר הכפלי של p מודולו m.
7. $\Phi_m(1) = \begin{cases} p & m = p^k \\ 1 & \text{אחרת} \end{cases}$

הוכחה: נסמן $\zeta = \zeta_m$. נתבונן ב- $\mathbb{Q}(\zeta)$.

ζ הוא שורש של $x^m - 1$, ולכן הוא שורש של כל פולינום מתוקן $f(x) \in \mathbb{Q}[x]$ שהוא הפולינום המינימלי של ζ מעל $\mathbb{Q}$.

נסמן $f(x) = \Phi_m(x)$ (הפולינום המחזורי ה- m-י). נוכיח ש- $\Phi_m(x) \in \mathbb{Z}[x]$ ואי-פריק מעל $\mathbb{Q}$.

נוכיח באינדוקציה על m. עבור $m = 1$: $\Phi_1(x) = x - 1$.

נניח שהטענה נכונה לכל $k < m$. מתקיים:

$$x^m - 1 = \prod_{d \mid m} \Phi_d(x)$$

לכן:

$$\Phi_m(x) = \frac{x^m - 1}{\prod_{d \mid m,\, d < m} \Phi_d(x)}$$

מכיוון שהמכנה הוא מתוקן ושייך ל- $\mathbb{Z}[x]$ (לפי הנחת האינדוקציה), ומכיוון שחילוק פולינומים מתוקנים נותן פולינום מתוקן, נובע ש- $\Phi_m(x) \in \mathbb{Z}[x]$.

טענה: $\Phi_m(x)$ אי-פריק מעל $\mathbb{Q}$.

הוכחה: נניח בשלילה ש- $\Phi_m(x) = g(x)h(x)$ עם $g, h \in \mathbb{Z}[x]$ מתוקנים ולא קבועים. נסמן $g(\zeta) = 0$.

יהי p ראשוני כך ש- $p \nmid m$. נוכיח ש- $g(\zeta^p) = 0$.

נניח בשלילה ש- $h(\zeta^p) = 0$. אז ζ הוא שורש של $h(x^p)$, ולכן $g(x) \mid h(x^p)$ ב- $\mathbb{Q}[x]$.

נסמן $h(x^p) = g(x)k(x)$. נעבור למודולו p: $\bar{h}(x^p) = \bar{g}(x)\bar{k}(x)$.

מכיוון ש- $\mathbb{F}_p$ שדה מאפיין p, מתקיים $\bar{h}(x^p) = \bar{h}(x)^p$ (חזקת פרובניוס).

לכן $\bar{g}(x) \mid \bar{h}(x)^p$, ומכאן ש- $\bar{g}$ ו- $\bar{h}$ חולקים גורם משותף.

אבל $\bar{g}(x) \mid x^m - 1$ ב- $\mathbb{F}_p[x]$, ולכן $x^m - 1$ יש שורש כפול, כלומר $\gcd(x^m - 1, mx^{m-1}) \neq 1$. זה קורה רק כאשר $p \mid m$, בסתירה להנחה.

לכן $g(\zeta^p) = 0$ לכל $p \nmid m$.

באינדוקציה על k, $g(\zeta^k) = 0$ לכל $\gcd(k, m) = 1$.

כל שורש של Φ_m הוא מהצורה ζ^k עבור $\gcd(k, m) = 1$, ולכן $g = \Phi_m$, בסתירה לכך ש- g לא קבוע.

לכן $\Phi_m(x)$ אי-פריק מעל $\mathbb{Q}$.

מסקנה: $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \deg \Phi_m = \varphi(m)$.

דוגמה: $\Phi_1(x) = x - 1$

$\Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1$

$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$ עבור p ראשוני

$\Phi_4(x) = \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1$

$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1$

תכונות:

1. $\deg \Phi_m = \varphi(m)$
2. $\Phi_m(x) = \prod_{\gcd(k,m)=1} (x - \zeta_m^k)$
3. $\Phi_m(x) \in \mathbb{Z}[x]$ מתוקן ואי-פריק מעל $\mathbb{Q}$
4. $x^m - 1 = \prod_{d \mid m} \Phi_d(x)$
5. $\mathbb{Z}[\zeta_m] = \mathcal{O}_{\mathbb{Q}(\zeta_m)}$
6. יהי p ראשוני, $p \nmid m$. אז $\Phi_m(x)$ מתפרק מעל $\mathbb{F}_p$ למכפלת גורמים ממעלה $\operatorname{ord}_m(p)$, כאשר $\operatorname{ord}_m(p)$ הוא הסדר הכפלי של p מודולו m.
7. $\Phi_m(1) = \begin{cases} p & m = p^k \\ 1 & \text{אחרת} \end{cases}$