הרצאה 6

משפט יהיו $n,d\in\mathbb{N}$. אזי יש רק מספר סופי של שדות מספרים K ממעלה $n=[K:\mathbb{Q}]$ ועם דיסקרימיננטה $d_K=d$.

הערה כאשר $n=2$, הוכחנו בתרגיל כי d_K קובע את K. אבל עבור n גדול זה לא בהכרח נכון.

מסקנה לכל N יש רק מספר סופי של שדות מספרים עם $|d_K|\le N$.

הוכחה של המסקנה לכל שדה מספרים, $0\ne d_K\in\mathbb{Z}$.

לכן $1\le|d_K|$. לפי חסם מינקובסקי, בכל מחלקה של Cl_K יש אידיאל I עם $n=[K:\mathbb{Q}]$, $s\le\frac{n}{2}$

$$1\le N(I)<\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}\le\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{n/2}\sqrt{|d_K|}$$

$$\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}\le\sqrt{|d_K|}$$

$$\underbrace{\frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^n}\le|d_K|$$

שואף ל-∞ כאשר $n\to\infty$.

לכן, עבור d_K קבוע יש רק מספר סופי של מעלות n שמקיימות את החסם, ולפי המשפט לכל n יש רק מספר סופי של שדות K ממעלה n ו- $d_K=d$.

הוכחה בלי הגבלת הכלליות, ניתן לספר רק שדות מספ' K כך ש- $\sqrt{-1}\in K$. אזי, לכל מגדל $K<L<M$ הוכחנו בתרגיל הבית

$$D_{M/K}=D_{M/L}\cdot D_{L/K}$$

$$d_{L/K}=N_{L/K}(D_{L/K})$$

לכן:

$$d_{M/K}=N_{M/K}(D_{M/K})=N_{L/K}N_{M/L}(D_{M/L}\cdot D_{L/K})=$$

$$N_{L/K}\left(d_{M/L}\cdot D_{L/K}^{[M:L]}\right) = N_{L/K}(d_{M/L})\cdot d_{L/K}^{[M:L]}$$

$$\begin{array}{c} K(\sqrt{-1}) \\ 2\,| \\ K \\ | \\ \mathbb{Q} \end{array}$$

לכן, אם $\sqrt{-1}\notin K$, נתבונן במגדל

לכן, $d_{K(\sqrt{-1})} = N_{K/\mathbb{Q}}(\dots)\cdot d_K^2$

בפרט, $d_K \mid d_{K(\sqrt{-1})}$. אם נניח שיש מספר סופי של אפשרויות ל- $K(\sqrt{-1})$ ממעלה $2n$ ודיסק' d, לכל $K(\sqrt{-1})$ כנ"ל יש מספר סופי של אפשרויות לגבי שדה K. נשים לב $\{1,\sqrt{-1}\}\subseteq\mathcal{O}_{K(\sqrt{-1})}$ הינו K-בסיס של $K(\sqrt{-1})$. עבור הבסיס הנ"ל $\det\left(Tr_{K(\sqrt{-1})/K}(\alpha_i\alpha_j)\right) = \det\begin{pmatrix}2 & 0\\ 0 & -2\end{pmatrix} = -4$

לכן, $-4\in d_{K(\sqrt{-1})/K}$. לכן $(-4)^n = N_{K/\mathbb{Q}}(-4)\in N_{K/\mathbb{Q}}(d_{K(\sqrt{-1})/K})$

לכן, $d_{K(\sqrt{-1})} \mid d_K^2\cdot 4^n$. / לכן היוצר של $N_{K/\mathbb{Q}}(d_{K(\sqrt{-1})/K})$ מחלק את 4^n.

אז נניח כי $\sqrt{-1}\in K$. לכן אין ל- K שום שיכונים ממשיים. אז $[K:\mathbb{Q}]=n=2s$, ויהיו $\tau_1,\dots,\tau_s:K\hookrightarrow\mathbb{C}$ נציגים של הזוגות של שיכונים מרוכבים.

$$\iota: K\hookrightarrow\mathbb{R}^{2s}=\mathbb{R}^n$$

$$\iota(\alpha) = (\mathrm{Re}\,\tau_1(\alpha),\ \mathrm{Im}\,\tau_1(\alpha),\dots,\ \mathrm{Im}\,\tau_s(\alpha))$$

הוכחנו לפני הרבה זמן כי $\iota(\mathcal{O}_K)$ סריג ב- $\mathbb{R}^n$ מנפח $\mathrm{vol}(\iota(\mathcal{O}_K)) = \sqrt{|d_K|} = \sqrt{|d|}$ ($d=d_K$ אם)

נתבונן בתחום

$$X = \left\{(x_1,\dots,x_{2s})\in\mathbb{R}^{2s} : \begin{array}{l}|x_1|<1\\ |x_2|<C\sqrt{|d|}\end{array}\quad \sqrt{x_{2i-1}^2+x_{2i}^2}<1 \text{ לכל } 2\le i\le s\right\}$$

לכן נבחר C מספיק גדול כך ש- $\mathrm{vol}(X)>\underbrace{2^n\sqrt{|d|}}$

הבחירה של C תלויה רק ב-d,n.

לפי משפט מינקובסקי יש $0\neq\alpha\in\mathcal{O}_K$ כך ש- $\iota(\alpha)\in X$.

<u>תת-טענה</u> $K=\mathbb{Q}(\alpha)$.

<u>תת-הוכחה</u> כיוון ש- $1\le N_{K/\mathbb{Q}}(\alpha)=\prod_{i=1}^{s}|\tau_i(\alpha)|^2$

אבל $\iota(\alpha)\in X \Leftarrow$ $|\tau_i(\alpha)|<1$ לכל $i\geq 2$, לכן בהכרח
$|\mathrm{Re}\,\tau_1(\alpha)|<1$

וכן $|\mathrm{Im}\,\tau_1(\alpha)|>1$ ובפרט $\mathrm{Im}\,\tau_1(\alpha)\neq 0$ ולכן $\tau_1(\alpha)\neq\overline{\tau_1(\alpha)}$

בנוסף, $\tau(\alpha)\neq\tau_1(\alpha)$ לכל שיכון $\tau:K\hookrightarrow\mathbb{C}$
$\tau\neq\tau_1$.

טענה, אם $\tau=\overline{\tau_1}$ הוכחנו. אחרת

$\tau=\overline{\tau_i}$, $\tau=\tau_i$ עבור $i\geq 2$, לכן $|\tau(\alpha)|<1$
$\neq$
$|\tau_1(\alpha)|>1$.

סוף סוף, נניח בשלילה כי $\mathbb{Q}(\alpha)\subsetneq K$.

אז לכל שיכון של $\mathbb{Q}(\alpha)$ לתוך $\mathbb{C}$ (ובפרט ל- $\tau_1|_{\mathbb{Q}(\alpha)}$) יהיו $[K:\mathbb{Q}(\alpha)]>1$

הרחבות ששולחות את $\alpha\in\mathbb{Q}(\alpha)$ לאותו מקום. אבל

זה לא המצב, לכן בהכרח $[K:\mathbb{Q}(\alpha)]=1$.

אז כיוון ש- X חסומה, גם ניתן לחסום את

המקדמים של הפולינום המינימלי של α:

$$\prod_{i=1}^{s}(X-\tau_i(\alpha))(X-\overline{\tau_i(\alpha)})=$$

$$\prod_{i=1}^{s}\left(X^2-2\,\mathrm{Re}\,\tau_i(\alpha)+|\tau_i(\alpha)|^2\right)$$

לכן מספר סופי של פולי מינימליים אפשריים של α
(שכן החסם תלוי רק ב- n,d) לכן מספר סופי של α
לכן מספר סופי של $K=\mathbb{Q}(\alpha)$.

חוזרים לסטינג הכללי: A תחום דדקינד

$$K=\mathrm{Frac}\,A$$

L/K סופית ספרבילית

B הסגור השלם של A ב-L.

נניח בנוסף כי L/K נורמלית, כלומר היא גלואה.
תהי $G=\mathrm{Gal}(L/K)$ חבורת גלואה. נראה שהתמונה שקיבלנו קודם נהיית פשוטה יותר.

<u>הערה</u> יהי $0\neq\mathfrak{p}\trianglelefteq A$ אידיאל ראשוני. ויהי $P\trianglelefteq B$ אידיאל ראשוני שמחלק את $\mathfrak{p}$ ($P\mid\mathfrak{p}B$, נרשום $P\mid\mathfrak{p}$). יהי $\sigma\in G$. אזי $\sigma(P)$ גם אידיאל ראשוני של B,
בנוסף $\sigma(P)\cap A = P\cap A=\mathfrak{p}$. לכן $\sigma(P)\mid\mathfrak{p}$. כלומר,
G פועלת על הקבוצה של אידיאלים הראשוניים של B שמחלקים את $\mathfrak{p}$.

<u>טענה</u> הפעולה הנ"ל הינה טרנזיטיבית.

<u>הוכחה</u> נניח שלא. אז נבחר אידיאלים ראשוניים $P,Q\trianglelefteq B$ במסלולים שונים של הפעולה. לפי משפט השאריות הסיני, קיים $\alpha\in B$ כך ש-

$$B/\mathfrak{p}B=\prod B/P_i^{e_i}$$

$$\alpha\equiv 0 \mod Q$$

$$\alpha\equiv 1 \mod \sigma(P)$$ לכל $\sigma\in G$.

נזכיר כי- $N_{L/K}(\alpha)=\prod_{\sigma\in G}\sigma(\alpha)\in A$

לכל $\sigma\in G$, $\alpha\notin\sigma^{-1}(P)$ $\Leftarrow$ $\sigma(\alpha)\notin P$ $\Leftarrow$ $N_{L/K}(\alpha)\notin P$

כי P ראשוני.

מצד שני $\alpha\in Q$, לכן $N_{L/K}(\alpha)=\alpha\cdot\prod(\ldots \text{האחרים})\in Q$

לכן $N_{L/K}(\alpha)\in Q\cap A=\mathfrak{p}$ לכן $N_{L/K}(\alpha)\in\mathfrak{p}B\subseteq P$

סתירה.

מסקנה יהי $\mathfrak{p}B=P_1^{e_1}\cdots P_r^{e_r}$ ויהי $f_i=[B/P_i : A/\mathfrak{p}]$

אם L/K גלואה, אזי $e_1=\dots=e_r$
$f_1=\dots=f_r$.

הוכחה בהינתן P_i, P_j יהי $\sigma\in G$ כך ש- $\sigma(P_i)=P_j$,

קיים לפי הטענה הקודמת. גם כן $\sigma(B)=B$, כי

σ שולחת שורשים של פולינום מינימלי מתוקן ב-$A[x]$ לשורשים

של אותו פולינום. לכן מקבלים איזומורפיזם

$B/P_i\xrightarrow{\sigma}B/\sigma(P_i)=B/P_j$ הינו העתקה של

מרחבים וקטוריים מעל $A/\mathfrak{p}$

לכן בפרט נקבל: $f_i=f_j$.

$\sigma(\mathfrak{p})=\mathfrak{p}$, לכן

$$\mathfrak{p}B=P_1^{e_1}\cdots\underbrace{P_i^{e_i}}_{P_j^{e_j}}\cdots P_r^{e_r}=\sigma(\mathfrak{p}B)=\underbrace{\sigma(P_1)^{e_1}\cdots\sigma(P_r)^{e_r}}_{P_j^{e_i}}$$

ויחידות הפירוק $\Leftarrow$ $e_i=e_j$.

מסקנה יהי $e=e_1=\dots=e_r$ אזי הנוסחה היסודית מקבלת צורה
$f=f_1=\dots=f_r$ פשוטה: $n=[L:K]=\sum_{i=1}^{r}e_if_i=efr$

הגדרה: יהי $P|\mathfrak{p}$. תת-החבורה הפירוק של $P/\mathfrak{p}$ (decomposition subgroup) הינה:

$$G_P=\{\sigma\in G \mid \sigma(P)=P\} = stab_G(P) \le G .$$

הערות 1) יהי $Q|\mathfrak{p}$ אידיאל אחר, $Q=\sigma(P)$. אזי $G_Q=\sigma G_P \sigma^{-1}$. לכן $\mathfrak{p}$ קובע את G_P עד כדי צמידות.

2) לפי משפט מסלול-מייצב, $[G:G_P]=r$

3) בפרט, $G=G_P \Leftarrow P$ הינו הראשוני היחיד של B שמחלק את $\mathfrak{p} \Leftarrow \mathfrak{p}B=P^e$ ⇐ $\mathfrak{p}$ לא מתפצל ב-B (non-split)

4) $G_P=\{e\} \Leftarrow r=[G:G_P]=\underset{=[L:K]}{n} \Leftarrow e=f=1 \Leftarrow$

$\mathfrak{p}B=P_1P_2\cdots P_n$ כאשר P_i ראשוניים שונים $B/P_i\cong A/\mathfrak{p}$

($\mathfrak{p}$ מתפצל לגמרי ב-B) splits completely

טענה: נניח מגדל

$$\begin{array}{ccc} M\supset C & & P \\ | \quad \cup & & \\ L\supset B & & Q \\ | \quad \cup & & \\ K\supset A & & \mathfrak{p} \end{array}$$

אזי $e(P/\mathfrak{p})=e(P/Q)e(Q/\mathfrak{p})$

$f(P/\mathfrak{p})=f(P/Q)f(Q/\mathfrak{p})$

אכן:

$$f(P/\mathfrak{p})=\dim_{A/\mathfrak{p}} C/P = \left(\dim_{A/\mathfrak{p}} B/Q\right)\left(\dim_{B/Q} C/P\right) = f(P/Q)f(Q/\mathfrak{p})$$

$$\mathfrak{p}B = Q^{e(Q/\mathfrak{p})}\cdots$$

$$QC = P^{e(P/Q)}\cdots$$

$$\mathfrak{p}C = (\mathfrak{p}B)C = (QC)^{e(Q/\mathfrak{p})}\cdots = P^{e(P/Q)e(Q/\mathfrak{p})}\cdots$$

<u>טענה</u> יהיו A,B,K,L כנ"ל, $G=Gal(L/K)$, $P|\mathfrak{p}$,
G_p חבורת פירוק. יהי Z שדה השבת של G_p.

$$Z=\{x\in L:\ \sigma(x)=x\quad \forall\sigma\in G_p\}.$$

L/Z גלואה ממעלה $|G_p|$, Z/K הרחבה ממעלה r.
יהי C הסגור השלם של A ב- Z.
יהי $Q=P\cap C$.

$$\begin{array}{cc} B & P \\ | & \\ C & Q \\ | & \\ A & \mathfrak{p} \end{array}$$

<u>טענה</u> 1) P הינו האידיאל הראשוני היחיד של B שמעליו Q.

2) $e(Q/\mathfrak{p})=f(Q/\mathfrak{p})=1$.

<u>הוכחה</u> 1)

$$Gal(L/Z)=G_p$$

כי $\sigma(P)=P$ לכל $\sigma\in G_p$

$$(Gal(L/Z))_P=(G_p)_P=G_p$$

לכן Q לא מתפצל ב- B.

2)

נוסחה ל-L/K

$$|G_p|=[L:Z]=\frac{n}{r}=e(P/\mathfrak{p})\cdot f(P/\mathfrak{p})$$

$$=e(P/Q)\cdot f(P/Q)$$

נוסחה יסודית עבור L/Z
$r=1$ מן הסעיף הראשון

מן הטענה הקודמת,

$$e(P/Q)\mid e(P/\mathfrak{p})$$
$$f(P/Q)\mid f(P/Q)$$

$$\Longleftarrow\quad e(P/\mathfrak{p})=e(P/Q),\quad f(P/\mathfrak{p})=f(P/Q)$$

ולכן $e(Q/\mathfrak{p})=f(Q/\mathfrak{p})=1$

$$\begin{array}{c} L \\ | \\ Z \\ | \\ K \end{array}$$

כיון כל Q לא מתפצל

כיון $\mathfrak{p}$ מתפצל לגמרי

$\mathfrak{p}C=Q_1\cdots Q_{[Z:K]}$

<u>המסקנה.</u>

טענה נסמן שדות שאריות: $k = A/\mathfrak{q}$

$l = B/\mathfrak{p}$

טענה נניח כי l/k הרחבה ספרבילית. אזי

1) ההרחבה l/k הינה גלואה. (מתקיים כל הזמן כי L/K גלואה).

2) ההעתקה הטבעית $G_p \longrightarrow Gal(l/k)$ הינה על.

$$\sigma \rightsquigarrow B/p \xrightarrow{\sigma} B/\sigma(p) = B/p$$

הוכחה 1) l/k סופית וספרבילית, לכן פרימיטיבית. יהי $\bar{\theta}$ יוצר: $l = k(\bar{\theta})$ ויהי $\theta \in B$ הרמה של $\bar{\theta}$.

יהי $\bar{g}(x) \in k[x]$ פול' מינימלי של $\bar{\theta}$

$f(x) \in A[x]$ פול' מינ' של θ.

$f(\theta) = 0$

אזי $\bar{f}(\bar{\theta}) = 0$ (ב-$k[x]$) $\Rightarrow$ $\bar{g} | \bar{f}$ אבל L/K נורמלית,

לכן $f(x)$ מתפרק למכפלה של גורמים לינאריים (ב-$B[x]$).

לכן (רדוקציה מודולו p) $\bar{f}$ מתפרק לגורמים לינאריים ב- $l[x]$, לכן $\bar{g}$ גם מתפרק כך, לכן l מכיל את כל השורשים של $\bar{g}$ $\Rightarrow$ l/k נורמלית.

2) יהי $\bar{\sigma} \in Gal(l/k)$. לפי הטענה הקודמת, ($G_p = Gal(L/Z)$, $l/k = l/(C/Q)$) ($Q = P \cap C$, $C/Q \simeq A/\mathfrak{q} = k$)

לכן נחליף את L/K ב- L/Z.

יהי $\bar\theta$ כנ"ל. אזי $\bar\sigma(\bar\theta)$ הינו שורש של $\bar g$.

לפי הטענה של השבוע הקודם ניתן להרים אותה לשורש η של f כי f מתפרק מעל B לגורמים לינאריים.

אבל L/K נורמלי, לכן קיים $\sigma\in Gal(L/K)$ כך ש- $\sigma(\theta)=\eta$. ה-σ ב- $G_P = Gal(L/K)$ הינו מקור של $\bar\sigma$.

<u>הגדרה</u> תת-חבורת ההתמדה של $P/\mathfrak{p}$ הינה

$$I_P = \ker\left(G_P \twoheadrightarrow Gal(\ell/k)\right)$$

$$|I_P| = \frac{|G_P|}{f} = e \quad \Leftarrow \quad |Gal(\ell/k)| = f(P/\mathfrak{p})$$

לכן $\mathfrak{p}$ לא מסתעף ב- B $\iff$ $I_P\simeq\{e\}$ לכל $P|\mathfrak{p}$.

שדות <u>ציקלוטומיים</u> $\zeta_n = e^{2\pi i/n}$, $e^{2\pi i c/n}$ $(c,n)=1$

יהי n טבעי, יהי ζ_n שורש n-י פרימיטיבי של 1.

$$L_n = \mathbb{Q}(\zeta_n)$$

<u>הערה</u> כל הצמודים של ζ_n הם ζ_n^c עבור $c\in(\mathbb{Z}/n\mathbb{Z})^*$,

לכן $L_n/\mathbb{Q}$ הרחבת גלואה ממעלה $\underbrace{\varphi(n)}_{\text{פונקצית } \varphi \text{ של אוילר}}$

<u>טענה</u> יהי $n=p^a$ כאשר p ראשוני.

אזי 1) האידיאל $P=(1-\zeta_n)\mathcal{O}_{L_n}$ הינו ראשוני.

2) $p\mathcal{O}_{L_n} = P^{\varphi(n)}$.

הוכחה: הפולינום המינימלי של ζ_n הינו

$$\Phi_n = \prod_{c\in(\mathbb{Z}/n\mathbb{Z})^\times} (x-\zeta_n^c) = \frac{x^{p^a}-1}{x^{p^{a-1}}-1} = 1 + x^{p^{a-1}} + x^{2p^{a-1}} + \dots + x^{(p-1)p^{a-1}}.$$

כל שורש n-מ של 1 שאינו פרימיטיבי הינו שורש p^{a-1}!
כי $m|p^a,\ m\neq p^a \Rightarrow m|p^{a-1}$

נציב $x=1$

$$\Phi_n(1) = \prod_{c\in(\mathbb{Z}/n\mathbb{Z})^\times} (1-\zeta_n^c) = 1+1+\dots+1 = p$$

מסקנה:
$$N_{L_n/\mathbb{Q}}(1-\zeta_n) = \prod_{\sigma\in Gal(L_n/\mathbb{Q})} \sigma(1-\zeta_n) = p \qquad (*)$$

לכן $N((1-\zeta_n)\mathcal{O}_{L_n}) = p \Rightarrow (1-\zeta_n)\mathcal{O}_{L_n} = P$ אידיאל ראשוני.

נשאר להוכיח כי $(1-\zeta_n^c) = (1-\zeta_n)$ $(**)$ ואז

$(*)$ גורר
$$p\mathcal{O}_L = \prod (1-\zeta_n^c)\mathcal{O}_L = P^{\varphi(n)}.$$

נוכיח $(**)$:
$$(1-\zeta_n^c) = (1-\zeta_n)(1+\zeta_n+\zeta_n^2+\dots+\zeta_n^{c-1})$$

לכן $(1-\zeta_n^c) \subseteq (1-\zeta_n)$.

אך $(c,n)=1$, לכן קיים d כך ש- $cd\equiv 1 \mod n$.

אזי
$$1-\zeta_n = 1-\zeta_n^{cd} = (1-\zeta_n^c)(1+\zeta_n^c+\zeta_n^{2c}+\dots+\zeta_n^{(d-1)c})$$

לכן גם $(1-\zeta_n) \subseteq (1-\zeta_n^c)$.