Vorlesung 4.12.23

Lemma:

a) $\frac{1-\zeta_n^a}{1-\zeta_n} \in \mathbb{Z}[\zeta_n]^\times$, falls $(a,n)=1$

Bew: $\frac{1-\zeta_n^a}{1-\zeta_n} = \sum_{i=0}^{a-1} \zeta_n^i \in \mathbb{Z}[\zeta_n]$

$\frac{1-\zeta_n}{1-\zeta_n^a} = \frac{1-\zeta_n^{ab}}{1-\zeta_n^a} = \sum_{i=0}^{b-1} \zeta_n^{ai}$,

wobei $ab \equiv 1 \pmod n$

b) $1-\zeta_{nm} \in \mathbb{Z}[\zeta_{nm}]^\times$, falls $n,m \in \mathbb{N}$, $n,m > 1$, $(n,m)=1$

Beweis:

$\frac{1-\zeta_n}{1-\zeta_{nm}} = 1 + \zeta_{nm} + \dots + \zeta_{nm}^{m-1}$

$\Rightarrow 1-\zeta_{nm}$ teilt $1-\zeta_n$

Sei $(X^n-1) = (X-1)\underbrace{(X^{n-1}+\dots+X+1)}_{=:g(X)}$

$\Rightarrow nX^{n-1} = g(X) + (X-1)g'(X)$

$\Rightarrow n\zeta_n^{n-1} = (\zeta_n - 1)g'(\zeta_n)$

$\Rightarrow \zeta_n - 1$ teilt n

Insgesamt: $1-\zeta_{nm}$ teilt n

Analog: $1-\zeta_{nm}$ teilt m

$\Rightarrow 1-\zeta_{nm} \in \mathbb{Z}[\zeta_{nm}]^\times$

Hilbertsche Verzweigungstheorie

L/K Galoiserweiterung von Zahlkörp.
Dann sind

$$\mathcal{O}_L,\ \mathcal{P}_L,\ I_L,\ \mathcal{O}_L^\times,\ \mathcal{A}_L$$

G-Mengen, wobei $G := \mathrm{Gal}(L/K)$.

Zum Beispiel: G wirkt auf I_L vermöge

$\mathfrak{a}$ gebrochenes Ideal, $\sigma \in G$ $\Rightarrow \sigma(\mathfrak{a}) \in I_L$

Oder: G wirkt auf $\mathcal{P}_L$ = Hauptideale.

$\Rightarrow$ G wirkt auf $\mathcal{A}_L = I_L/\mathcal{P}_L$ vermöge:

$$\sigma\left(\mathfrak{a}\mathcal{P}_L\right) := \sigma(\mathfrak{a})\,\mathcal{P}_L.$$

Ziel: Studiere die G-Wirkung auf I_L.

Beobachtung: $\sigma \in G$, $\mathfrak{P} \mid \mathfrak{p} \Rightarrow \sigma(\mathfrak{P}) \mid \mathfrak{p}$

Denn: $\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \sigma\left(\mathfrak{P} \cap \mathcal{O}_K\right) = \sigma(\mathfrak{p}) = \mathfrak{p}$.

Satz: G wirkt transitiv auf die Menge $\{\mathfrak{P} \mid \mathfrak{p}\}$ der Primideale über $\mathfrak{p}$.

Beweis: Seien $\mathfrak{P}', \mathfrak{P}$ Primideale über $\mathfrak{p}$.

Angenommen: $\sigma(\mathfrak{P}) \neq \mathfrak{P}, \forall \sigma \in G$.

Finde nach CR $x \in \mathcal{O}_L$ mit

$$x \equiv 0 \pmod{\mathfrak{P}'}$$
$$x \equiv 1 \pmod{\sigma(\mathfrak{P})}, \forall \sigma \in G.$$

$$\Rightarrow N_{L|K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$$

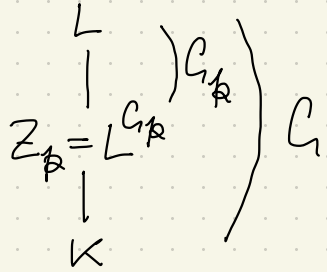
Andererseits:

$$x \notin \sigma(\mathfrak{P}), \forall \sigma \in G \Rightarrow \sigma(x) \notin \mathfrak{P}, \forall \sigma$$
$$\Rightarrow N_{L|K}(x) = \prod_{\sigma \in G} \sigma(x) \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \quad \lightning$$

Definition: Sei $\mathfrak{P}|\mathfrak{p}$ in $L|K$. Dann heißt

$$G_{\mathfrak{P}} := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

Zerlegungsgruppe von $\mathfrak{P}$. Der Fixkörper $Z_{\mathfrak{P}} \subseteq L$ heißt Zerlegungskp. von $\mathfrak{P}$.



Lemma:

a) $\#\{\mathfrak{P} \mid \mathfrak{p}\} = [G : G_{\mathfrak{P}}] = [Z_{\mathfrak{P}} : K]$

b) $G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L$

$\iff \mathfrak{p}$ ist voll zerlegt.

c) $G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K$

$\iff \mathfrak{p}$ ist unzerlegt

d) Sei $\sigma \in G$. Dann gilt:

$$G_{\sigma(\mathfrak{P})} = \sigma G_{\mathfrak{P}} \sigma^{-1}$$

Beweis: b) und c) folgen aus a).

a) folgt aus: Sei X eine G-Menge. Dann gilt:

$$X = \bigcup_{x \in X/\sim} G/G_x \cdot x \quad \text{wobei}$$

$x \sim y :\iff \exists\, \tau \in G : \tau(y) = x.$

$G_x = \mathrm{Stab}_G(x)$.

Nutze zusätzlich Transitivität.

Zu d) $\tau \in G_{\sigma(\mathfrak{P})} \Leftrightarrow \tau(\sigma(\mathfrak{P})) = \sigma(\mathfrak{P})$

$\Leftrightarrow (\sigma^{-1}\tau\sigma)(\mathfrak{P}) = \mathfrak{P} \Leftrightarrow \sigma^{-1}\tau\sigma \in G_{\mathfrak{P}}$

$\Leftrightarrow \tau \in \sigma G_{\mathfrak{P}} \sigma^{-1}$ ▨

Erinnerung: Im Allgemeinen

$$\begin{array}{ccccc} L & \supseteq & \mathcal{O}_L & \supseteq & \mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \\ n \,\big| & & \big| & & \\ K & \supseteq & \mathcal{O}_K & \supseteq & \mathfrak{p} \end{array} \qquad \sum_{i=1}^{r} e_i f_i = n$$

$$f_i := \left[\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}\right].$$

Satz: Falls L/K galoissch ist, so gilt:

$$f_1 = \ldots = f_r =: f$$

$$e_1 = \ldots = e_r =: e$$

Also auch: • $efr = n$.

• $\mathfrak{p}\mathcal{O}_L = \left(\prod_{\sigma \in G/G_{\mathfrak{P}}} \sigma(\mathfrak{P})\right)^e$

Beweis: Sei $\sigma(\mathfrak{P}) = \mathfrak{P}'$ für $\mathfrak{P}, \mathfrak{P}'$ über $\mathfrak{p}$.

Dann induziert $\sigma: \mathcal{O}_L \xrightarrow{\cong} \mathcal{O}_L$ einen

Isomorphismus

$$\mathcal{O}_L/\mathfrak{p} \xrightarrow{\cong} \mathcal{O}_L/\mathfrak{p}'$$

$$\alpha + \mathfrak{p} \longmapsto \sigma(\alpha) + \mathfrak{p}'$$

von $\mathcal{O}_K/\mathfrak{p}$ - VR $\Rightarrow f = f'$

Wegen $\sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{p})\,\sigma(\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$

folgt weiter

$$\mathfrak{p}^r \mid \mathfrak{p}\mathcal{O}_L \iff (\mathfrak{p}')^r \mid \mathfrak{p}\mathcal{O}_L$$

$$\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{p}^r \qquad\qquad \mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{p}'^r$$

Also: $e = e'$ ∎

<u>Satz:</u> Sei $\mathfrak{p}_Z = \mathfrak{p} \cap Z_{\mathfrak{p}}$. Dann gilt:

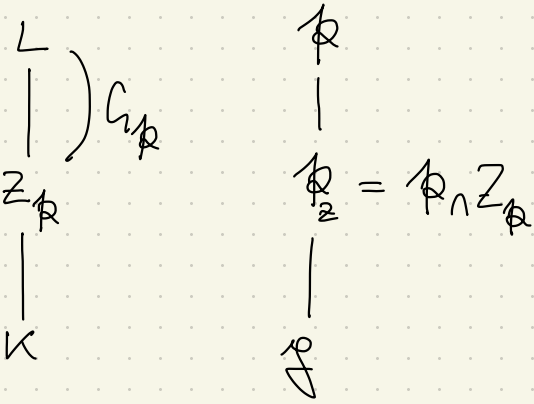
(i) $\mathfrak{p}_Z$ ist unverzweigt in $L/Z_{\mathfrak{p}}$.

(ii) $\mathfrak{p}$ hat über $Z_{\mathfrak{p}}$ den Verzweigungsindex $e = e(\mathfrak{p}|\mathfrak{p})$ und den Restklassenkp.grad $f = f(\mathfrak{p}|\mathfrak{p})$. D.h. $\mathfrak{p}_Z\mathcal{O}_L = \mathfrak{p}^e$

(iii) Verzweigungsindex und Restklassengrad von $\mathfrak{P}_2 / \mathfrak{p}$ sind gleich 1, d.h.

$$e(\mathfrak{P}_2 | \mathfrak{p}) = 1 = f(\mathfrak{P}_2 | \mathfrak{p}).$$

(iv) Falls $G_{\mathfrak{P}} \trianglelefteq G$, so ist $\mathfrak{p}$ voll zerlegt in $Z_{\mathfrak{P}}$.



<u>Beweis:</u> $\left.\begin{aligned} ef \cdot r &= |G| = [L:K] \\ r &= [G : G_{\mathfrak{P}}] = [Z_{\mathfrak{P}} : K] \end{aligned}\right\} \Rightarrow$

$$\Rightarrow [L : Z_{\mathfrak{P}}] = ef \quad (*)$$

<u>Zu (i):</u> $L | Z_{\mathfrak{P}}$ ist Galoissch mit Gruppe $G_{\mathfrak{P}}$. $G_{\mathfrak{P}}$ wirkt transitiv auf $\{ \mathfrak{Q} \text{ in } L/Z_{\mathfrak{P}} \mid \mathfrak{Q} | \mathfrak{P}_2 \} = \{ \tau(\mathfrak{P}) \mid \tau \in G_{\mathfrak{P}} \} = \{ \mathfrak{P} \}$.

Aus (*) folgt:

$$ef = e(\mathfrak{P}|\mathfrak{P}_2)\, f(\mathfrak{P}|\mathfrak{P}_2)$$

Man zeigt leicht:

$$e = e(\mathfrak{P}|\mathfrak{p}) \overset{!}{=} e(\mathfrak{P}|\mathfrak{P}_2)\, e(\mathfrak{P}_2|\mathfrak{p})$$

$$f = f(\mathfrak{P}|\mathfrak{p}) \overset{!}{=} f(\mathfrak{P}|\mathfrak{P}_2)\, f(\mathfrak{P}_2|\mathfrak{p}).$$

Hieraus folgt (ii) und (iii).

Zu (iv): Folgt aus $Z_{\mathfrak{P}}/K$ galoissch. ∎

ZIEL: Studiere $L/Z_{\mathfrak{P}}$ bzw. inkopradiere e gruppentheoretisch.

Sei $\sigma \in G_{\mathfrak{P}}$. Dann induziert σ einen Atm.

$$\overline{\sigma} : \mathcal{O}_L/\mathfrak{P} \xrightarrow{\sim} \mathcal{O}_L/\mathfrak{P}$$

$$\alpha + \mathfrak{P} \longmapsto \sigma(\alpha) + \mathfrak{P}.$$

Setze: $\kappa(\mathfrak{P}) := \mathcal{O}_L/\mathfrak{P}$, $\kappa(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$.

Satz: $G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$, $\sigma \mapsto \overline{\sigma}$ ist surjektiver Gruppenhom.

Def.: Der Kern von $\sigma \mapsto \overline{\sigma}$ heißt (Bez: $I_{\mathfrak{P}}$) Trägheitsgruppe oder Verzweigungsgruppe von $\mathfrak{P}$.
Der Fixkörper $T_{\mathfrak{P}} := L^{I_{\mathfrak{P}}}$ heißt Trägheitskörper.

Es gilt: • $G_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$

• $|I_{\mathfrak{P}}| = e = e(\mathfrak{P}|\mathfrak{p})$

Beweis des Satzes:

$$\begin{array}{ccc} L & & \mathfrak{P} \\ | & & | \\ F = Z_{\mathfrak{P}} & & \mathfrak{q} = \mathfrak{P}_Z \\ | & & | \\ K & & \mathfrak{p} \end{array}$$

Wegen $\mathcal{O}_F/\mathfrak{q} = \mathcal{O}_K/\mathfrak{p}$ kann man o.E. $K = F$ voraussetzen.

Sei $\bar{\Theta}$ ein primitives Element für $k(\mathfrak{P})\,|\,k(\mathfrak{p})$, d.h.

$$k(\mathfrak{P}) = k(\mathfrak{p})(\bar{\Theta}), \text{ o.E. } \Theta \in \mathcal{O}_L.$$

Sei $f \in \mathcal{O}_K[x]$ das Mipo von Θ über K.
Sei $\bar{g}(x) \in k(\mathfrak{p})[x]$ das Mipo von $\bar{\Theta}$

Sei $f(x) = \prod_i (x - \Theta_i)^{g_i}$ mit Θ_i in K in verschiedene Θ_i, paarweise verschieden

$\bar{f}(\bar{\Theta}) = 0 \Longrightarrow \bar{g} \mid \bar{f}$ in $\kappa(\mathfrak{p})[x]$

$$\bar{f} = \prod_i (x - \bar{\Theta}_i)$$

Sei $\bar{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{P}) / \kappa(\mathfrak{p}))$.

$\bar{\sigma}(\bar{\Theta})$ ist Nst. von $\bar{g}$, also auch von $\bar{f}$.

Also gibt es eine Nst. Θ_{i_0} von f mit

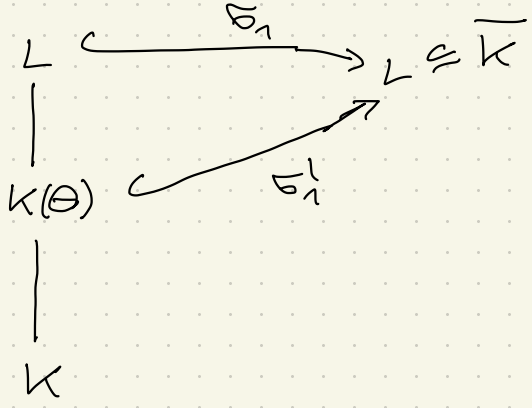
$$\Theta_{i_0} \equiv \bar{\sigma}(\bar{\Theta}) \pmod{\mathfrak{P}}$$

Sei $\sigma_1' \in G\left(K(\Theta)/K, \overline{K}/K\right)$ definiert durch

$$\Theta \longmapsto \Theta_{i_0}$$

Sei $\sigma_1 : L \to L$ eine Fortsetzung von σ_1'.

Dann gilt: $\overline{\sigma_1} = \bar{\sigma}$.



∎