Lokalen Frobenius und quadratische Reziprozität

1. Hilbertsche Verzweigungstheorie

Sei o ein bel. Dedekindring mit Quotkörper K.
Wir betr. eine galoische Körpererweiterung $L|K$ mit Galoisgruppe $G = G(L|K)$ vom Grad n. Wir nennen den ganzen Abschluss von o in L $\mathcal{O}$.

Lem. Sei $\sigma \in G$, dann ist $\mathcal{O}$ σ-invariant.

Ist p ein Primideal in o und P ein Primideal in $\mathcal{O}$ über p, so ist σP ein Primideal in O über p.

<u>Bew.</u> Sei $a \in O$. Dann $\exists f \in o[X]$, sodass $f(a)=0$. Da $o \subseteq K$, ist $f(\underline{\sigma a}) = \sigma(f(a)) = 0$. Somit folgt $\sigma a \in O$.

Ist P ein Primideal v. O ü. p, so ist σP wieder ein Ideal in groß O.

Da $\sigma P \cap o = \sigma(P \cap o) = \sigma p = p$

$\Rightarrow \sigma P$ ist ein Ideal über p.

<u>Bem.</u> G operiert auf der Menge der Primideale ü. p. Die σP die P konjugierten Primideale.

<u>Satz.</u> G operiert transitiv auf dieser Menge.

<u>Bew.</u> Angenommen es existiere Primideale P und P' über p, s.d. $\forall \sigma \in G: \sigma P \neq P'$.

Wir betrachten $p\mathcal{O} = \prod_{i=1}^{r} P_i^{e_i}$, das Produkt durchläuft alle Primideale über p.

Nach dem chinesischen Restsatz ist $\mathcal{O}/p\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/P_i^{e_i}$,

Dies impliziert die Existenz eines $x \in \mathcal{O}$, sodass $x \equiv 0 \mod P'$ und $\forall \sigma \in G: x \equiv 1 \mod \sigma P$.

Sei $N = \prod$

Sei $N = \overline{\prod_{\sigma \in G} \sigma x}$. Damit ist

$\forall \sigma \in G : \sigma N = N$, folglich

$N \in K$, liegt $N \in \mathcal{O}$.

Da $N \in P'$, folglich ist $N \in P' \cap \mathcal{O} = p$.

Da $\forall \sigma : \sigma x \notin P . \Rightarrow N \notin P$

Da $p \subseteq P \Rightarrow \lightning$

$\Rightarrow$ folglich existieren solche P, P' nicht.

Def Für ein Primideal P von

$\mathcal{O}$ ü p.

$G_P := \{\sigma \in G \mid \sigma P = P\} . < G$,

nennen wir die Zerlegungsgruppe.

Der Zerlegungskörper, ist der

dazugehörige $\boxed{\text{Fixkörper}}$ von G_P

in L, Z_P.

Bem. Da die Operation transitiv ist, existiert eine Bijektion von

$G/G_P \to \{$konj. Primideale v. $P\}$,

$\sigma G_P \mapsto \sigma P$. Daraus folgt.

$\#$ konj. Primid $= [G:G_P]$.

Insb. ist p voll zerlegt gdw.

$G_P = 1$ und unzerlegt, falls

$G_P = G$.

Satz Sei $pO = \prod_{i=1}^{r} P_i^{e_i}$ mit

Trägheitsgraden $f_i = [O/P_i : o/p]$.

Dann gilt

$e_1 = \dots = e_r =: e$ und

$f_1 = \dots = f_r =: f$.

Für Repräsentantensystem von

G/G_P ist $pO = \left(\prod_{\sigma} \sigma P\right)^e$

Beweis. Sei $P = P_1$. Dann kann man $\forall i$ ein $\sigma_i \in G$ wählen, sodass $P_i = \sigma P$. Dann induziert σ_i ein Isomorphismus $\mathcal{O}/P \xrightarrow{\sim} \mathcal{O}/\sigma_i P$.

$$\begin{tikzcd}
\mathcal{O} \arrow[r, "\overset{\sigma_i}{\sim}"] \arrow[d, two heads] \arrow[dr] & \mathcal{O} \arrow[d] \\
\mathcal{O}/P_i \arrow[r, "\sim", "\boxed{\tilde{\sigma}}"'] & \mathcal{O}/\sigma P_i
\end{tikzcd}$$

Somit folgt $f_i = [\mathcal{O}/\sigma_i P : o/p]$
$= [\mathcal{O}/P : o/p] = f_1 =: f$.

Da $\mathcal{O}$ G-invariant.

$\sigma_i(p\mathcal{O}) \subseteq p\mathcal{O}$. Da σ_i invertierbar ist, $\sigma_i(p\mathcal{O}) = p\mathcal{O}$. Für beliebige

$\boxed{U}$

$$P^U \mid pO \Leftrightarrow \sigma_i(P^U) \mid \sigma_i(pO)$$

$$\Leftrightarrow \underline{\sigma_i}(P^U) \mid pO$$

$$\Leftrightarrow (\sigma_i P)^U \mid pO.$$

$$\Rightarrow e_i = e_1 =: e.$$

<u>Satz</u>. Wir betrachte $Z_p | K$.

Sei O_Z der ganze Abschluss von O in Z_p. Sei $P_Z := P \cap O_Z$.

(i) <u>P_Z ist unzerlegt in L</u>

(ii) <u>P hat über Z_p</u> den Verzw.grad e und Trägheitsgrad f.

(iii) <u>P_Z hat über K</u> den Vgrad 1 und Träggrad 1.

$$\begin{array}{cccc} G & K & O & P \\ | & | & | & | \\ G_Z & Z_p & O_Z & P_Z \end{array}$$

$\rightarrow$ nicht unbedingt Galoisch.

$$
\begin{array}{cccc}
G_Z & Z_p & O_Z & P_Z \\
| & | & | & | \\
\boxed{1} & L & O & P
\end{array}
$$

<u>Bew.</u> Aus der Galoistheorie ist $G(L|Z_p) = G_p$. Also ist P_Z unzerlegt.

<u>Erinn.</u>: Fundamentale Gleichg.:

$$\sum_{i=1} e_i f_i = n.$$

Im Galoischen Fall $ref = n$.

$r = [G : G_p]$, genauso $n = |G|$

$\rightsquigarrow$ $|G_p| = ef$.

Für

$$
\begin{array}{ccc}
P & & P_Z \\
 & & \\
Z_p & & K
\end{array}
$$

Sehen die Verzwgr. bzw. Trägheitsgr.

ges d.

e' e''

f' f''

Nach (1) erhalten wir

$P_Z O = P^{e'}$.

In $Z_p|K$ erhalten wir

$p O_Z = P_Z^{e''} \cdot (\ldots)$.

Für $L|K$ erhalten wir

$p O = P^{e' \cdot e''} \cdot (\ldots)$

$\Rightarrow e = e' \cdot e''$.

Es gibt Inklusionen:

$o/p \hookrightarrow O_Z/P_Z \hookrightarrow O/P$.

Dann ist $O/P \,|\, O_Z/P_Z \,|\, o/p$ ein Körperturm.

$f = [O/P \,|\, o/p] = [\ldots][\ldots] = f' f''$.

Dann ist nach der Fundam. Gl.

$e'e''f'f'' = ef = [L:\mathbb{Z}_p] = e'f'$

$\leadsto e''f'' = 1 \Rightarrow e'' = 1, f'' = 1$

$\Rightarrow e' = e, f' = f.$

<u>Satz.</u> $(\mathcal{O}/\mathfrak{P}) \mid (o/\mathfrak{p})$ ist normal

<u>Satz:</u> $\boxed{\Phi}: G_\mathfrak{P} \to \underline{\mathrm{Aut}_{(o/\mathfrak{p})}(\mathcal{O}/\mathfrak{P})}$,

$\sigma \longmapsto (a\mathfrak{P} \mapsto \sigma a \mathfrak{P})$, ist ein

wohldef. und surjektiv.

<u>Bem.</u> $[\mathcal{O}_Z/\mathfrak{P}_Z \mid o/\mathfrak{p}] = 1$, d.h.

$\boxed{o/\mathfrak{p} \hookrightarrow \mathcal{O}_Z/\mathfrak{P}_Z}$ ist ein

Isomorphismus.

O.B.d.A. $\mathfrak{p} = \mathfrak{P}_Z$, $K = Z_\mathfrak{P}$.

$\Rightarrow o = \mathcal{O}_Z$, $G = G_\mathfrak{P}$.

Sei $\sigma\mathcal{O} = \mathcal{O}$ und $\sigma\mathfrak{P} = \mathfrak{P}$, folglich

Φ ist wohldefiniert.

Sei $\hat{k}$ der eindeutige Zwkörper von $(O/P)|(o/p)$, sd.
$k|(o/p)$ separabel und
$(O/P)|k$ rein inseparabel.

$\hat{k} = \{a \in O/P \mid a \text{ ist separ. ü } o/p\}$.

Dann $\hat{k}|(o/p)$ ist galoisch mit Galoisgruppe $\hat{G}$.

Da $(O/P)|\hat{k}$ rein inseparabel.
$\boxed{\mathrm{Aut}_{\hat{k}}(O/P) = \{id_{O/P}\},}$ insb.

$$\mathrm{Aut}_{(o/p)}(O/P) \longrightarrow \hat{G},$$
$$G \longmapsto G|_{\hat{k}} \text{ ein Isomorphis.}$$

Aus dem Satz des primitiven Elem. existiert $\hat{a} \in \hat{k}$, sd.
$\hat{k} = (o/p)(\hat{a})$. Dann $\exists a \in \mathcal{L}$,

$aP = \hat{a}$.

$f \in \mathbb{Z}[x]$ ist das Minpol von a,

$\bar{g} \in (O/p)[x]$ ist das Minpol von $\hat{a}$.

Wir wählen $\tilde{\sigma} \in \tilde{G}$ bel.

Wir schreiben $\bar{f}$ als das Bild von f in $(O/p)[x]$.

$f(a) = 0 \Rightarrow \bar{f}(\hat{a}) = 0$

$\Rightarrow \bar{g} \mid \bar{f}$.

$$\bar{g}(\tilde{\sigma}\hat{a}) = 0$$
$$\parallel$$
$$\bar{f}(\tilde{\sigma}\hat{a})$$

Da f in Linearfaktor zerfällt.

Insb. besitzt f eine Nullstelle

$f(a') = 0$, sodass $a'P = \tilde{\sigma}\hat{a}$.

Dann existiert ein $\sigma \in G$, s.d.

$\sigma a = a'$.

Das Bild eines Automorphismus

eind charakter. ist, durch d.
Bild d. prim Elem., weil

$\Phi(\sigma)(\tilde{a}) = \sigma a P = a' P = \tilde{\sigma} \tilde{a}$

$\Rightarrow \Phi(\sigma) = \tilde{\sigma}$.

$\Rightarrow \Phi$ surjektiv.

<u>Def.</u> Wir nennen kern von Φ
die Trägheitsgruppe I_p.
Der " körper T_p
ist entspr. der Fixkörper.

<u>Bem.</u> $I_p \lhd G_p \subset G$

$\leadsto$ körperErw. $L | T_p | Z_p | K$.

<u>Kor.</u> Die Erw. $T_p | Z_p$ ist wieder
galoisch, $G(T_p | Z_p) \cong \mathrm{Aut}_{(\mathcal{O}/p)}(\mathcal{O}/P)$,
$G(L | T_p) = I_p$.

Satz. Falls $(\mathcal{O}/P)\,|\,(o/p)$ galoisch, dann ist $|I_P| = e$, $[G_P : I_P] = f$.
Sei P_T das unter P liegende Primideal von T_P.
Dann hat P über P_T den Verzwgrd e und Trägheitsg 1.

P_T über P_Z hat Verzw. 1 und Trägheitsg f.

2. Lokaler Frobenius.

$o = \mathbb{Z}$, $k = \mathbb{Q}$. Dazu sei endl. Galoiserweiterung $L|\mathbb{Q}$.
Sei P unverzweigtes Primideal in $\mathbb{Z}_L$ über (p).

Satz: Es existiert genau ein $\sigma \in G(L|\mathbb{Q})$ s.d. $\forall a \in \mathbb{Z}_L : \sigma(a) \equiv a^p \mod P$.
Dieser Automorphismus wird der

Dieser Automorphismus wird der lokale Frobenius zum Primideal P über (p).

Bew. Man sieht, dass $(\mathbb{Z}_L/P) \mid (\mathbb{Z}/(p))$ ist endliche Körpererw. Charakteristik p.

$G((\mathbb{Z}_L/P) \mid (\mathbb{Z}/(p))) = \langle F \rangle$,

$F: \mathbb{Z}_L/P \to \mathbb{Z}_L/P,\ x \mapsto x^p$.

Da die Erw galois ist, und P unverzweigt ist. $e = |I_P| = 1$, hat Φ trivialen Kern.

Somit ist Φ ein Isomorphismus.

Es gibt genau ein $\sigma := \Phi^{-1}(F) \in G_P$, sodass $\sigma a \equiv a^p \bmod P$.

Weil jeder Automorph., der die gewünschte Eigsch. erfüllt P invariant

Sein muss, müsste er in G_P.

$\Rightarrow$ Eindeutigkeit in ganz G.

Bem. Falls $G(L|\mathbb{Q})$ abelsch ist, so ist lokale Frobenius unabh. von der Wahl von P.
Dann schreiben wir auch $\left(\frac{L|\mathbb{Q}}{p}\right)$.

Bem. Seien P und P' Primid. ü. (p).
Seien σ und σ' ihre lokale Frobeniusabb.
Wir wählen $\tau \in G(L|\mathbb{Q})$, sd. $\tau P = P'$. Sei $a \in \mathbb{Z}_L$ bel.

$$\begin{aligned}
(\tau \circ \sigma \circ \tau^{-1})(aP') &= \tau(\sigma(\tau^{-1}(aP'))) \\
&= \tau(\sigma(\tau^{-1}(a)P)) \\
&= \tau((\tau^{-1}(a))^p P) \\
&= \tau(\tau^{-1}(a^p)P) \\
&= a^p P'
\end{aligned}$$

$\rightsquigarrow$ Eind. d. lok. Frob.

$\Rightarrow \tau \circ \sigma \circ \tau^{-1} = \sigma'$

Im Fall dass $G(L|\mathbb{Q})$ abelsch ist, folgt $\sigma = \sigma'$.

Bem. Sei P in L über (p) unverzweigt. Dann ist der lokale Frob der triv. Autom. gdw. (p) total zerlegt in L liegt.

Bew. $\Phi : G_p \to \langle F \rangle$

$\sigma = \Phi^{-1}(F)$ ist das neutr. Elem. gdw. F das neutr. Elem.

$\Rightarrow \mathrm{Gal}((\mathbb{Z}_L/P) \mid \mathbb{Z}/(p)) = 1$

$\Rightarrow f = 1. \rightsquigarrow$ total zerlegt ist.

Bem. Für ein quadratfreies a und eine ungerade zu a teilerfremde Primzahl p ist $\left(\frac{a}{p}\right) = 1$ gdw. (p) total zerlegt in $\mathbb{Q}(\sqrt{a})$ ist.

Bew. $\left(\frac{a}{p}\right)$ ist 1 gdw. $\alpha \in \mathbb{Z}$ exist. s.d.

$x^2 - a \equiv (x-\alpha)(x+\alpha) \mod (p)$.

$p \nmid 2\alpha$. $\leadsto$ $x^2 - a$ in unterschiedl. Linfaktor zerf.

Mit d. Zerlegungsgesetz folgt (p) total zerlegt.

Satz: Für zwei versch. ungerade Primzahlen p und q ist.

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Bew. $q^* := (-1)^{\frac{q-1}{2}} q$.

$$\left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

Es genügt zu zeigen, dass

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right).$$

Wir betrachten Kreiskörper

$\mathbb{Q}(\xi_q) \mid \mathbb{Q}(\sqrt{q^*}) \mid \mathbb{Q}$.

Da $G(\mathbb{Q}(\xi_q) \mid \mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ abelsch, ist loLc trolsend.

$\boxed{q} = \prod_{p'} p'^{\nu_p} = q$

$\rightsquigarrow (p) = (\underline{p_1 \cdots p_r})^{\boxed{e(p^{\nu_p})}}$

wobei $\nu_p = 0$

$\Rightarrow$ Verzweigungsgrad $= 1$

$\Rightarrow (p)$ ist unverzw. in $\mathbb{Q}(\xi_q)$,

(p) ist unverzweigt in $\mathbb{Q}(\sqrt{q^*})$

Sei $\mathfrak{P}$ ein Primideal ü. (p) in $\mathbb{Q}(\xi_q)$

$\mathfrak{p}' = \mathfrak{P} \cap \mathbb{Q}(\sqrt{q^*})$ $\boxed{\text{Da } \mathbb{Q}(\sqrt{q^*}) \mid \mathbb{Q} \text{ normal}}$

$\underline{\boxed{\left(\frac{\mathbb{Q}(\xi_q)/\mathbb{Q}}{\mathfrak{P}}\right)\Big|_{\mathbb{Q}\sqrt{q^*}} (a)}} - a^p \in \underline{\mathfrak{P}} \cap \boxed{\mathbb{Q}(\sqrt{q^*})}$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad \overset{\shortparallel}{\mathfrak{p}'}$

$\Rightarrow \left(\frac{\mathbb{Q}(\xi_q)/\mathbb{Q}}{}\right) \qquad\qquad / \left(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}\right)$

$$\Rightarrow \left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)\Big|_{\mathbb{Q}(\sqrt{q^*})} = \left(\frac{\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}}{p}\right).$$

Aus dem Galoistheorie $\exists$ Isom.

$$G(\mathbb{Q}(\zeta_q)|\mathbb{Q}) \Big/ G(\mathbb{Q}(\zeta_q)|\mathbb{Q}(\sqrt{q^*})) \xrightarrow{\sim} G(\mathbb{Q}(\sqrt{q^*})|\mathbb{Q}).$$

$\Rightarrow \exists$ surj Hom.

$$\underset{\cong (\mathbb{Z}/q\mathbb{Z})^\times}{G(\mathbb{Q}(\zeta_q)|\mathbb{Q})} \twoheadrightarrow \underset{\cong \{\pm 1\}}{G(\mathbb{Q}(\sqrt{q^*})|\mathbb{Q})},$$

geg. $\sigma \mapsto \sigma|_{\mathbb{Q}(\sqrt{q^*})}$.

Da diese Gruppe zykl. sind.

ist dieser Hom eind.

$$a \mapsto \left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \mod q.$$

ist dieser eind. Hom.

Falls σ def. $\zeta_q \mapsto \zeta_q^p$,

so ist $\sigma|_{\mathbb{Q}(\sqrt{q^*})}$ der Frob.

Unter diesen Identifik.

[illegible]

folgt $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)\Big|_{\mathbb{Q}(\sqrt{q^*})} = \left(\frac{\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}}{p}\right) = \left(\frac{p}{q}\right)$

Andererseits folgt $\quad = \left(\frac{q^*}{p}\right)$