LOKALER FROBENIUS UND QUADRATISCHE REZIPROZITÄT

KEVIN ZHANG

1. Hilbertsche Verzweigungstheorie

Sei $\mathcal{o}$ wieder ein beliebiger Dedekindring mit Quotientenkörper K. Wir betrachten hier den Fall einer endlichen galoisschen Körpererweiterung $L|K$ mit Galoisgruppe $G = G(L|K)$ vom Grad n. Wir nennen den ganzen Abschluss von $\mathcal{o}$ in L wieder $\mathcal{O}$.

Lemma 1. *Sei $\sigma \in G$, dann ist $\mathcal{O}$ σ-invariant. Ist zusätzlich $\mathfrak{p}$ ein Primideal in $\mathcal{o}$ und $\mathfrak{P}$ ein Primideal von $\mathcal{O}$ über $\mathfrak{p}$, so ist $\sigma\mathfrak{P}$ wieder ein Primideal von $\mathcal{O}$ über $\mathfrak{p}$.*

Beweis. Sei $a \in \mathcal{O}$. Dann existiert ein normiertes $P \in \mathcal{o}[X]$, sodass $P(a) = 0$. Da die Koeffizienten von P in K liegen, ist $P(\sigma a) = \sigma P(a) = 0$, folglich $\sigma a \in \mathcal{O}$. Ist $\mathfrak{P}$ ein Primideal von $\mathcal{O}$ über $\mathfrak{p}$, ist hiermit $\sigma\mathfrak{P}$ wieder ein Primideal von $\mathcal{O}$. Zudem ist $\sigma\mathfrak{P} \cap \mathcal{o} = \sigma(\mathfrak{P} \cap \mathcal{o}) = \sigma\mathfrak{p} = \mathfrak{p}$, folglich ist $\sigma\mathfrak{P}$ ebenfalls ein Primideal über $\mathfrak{p}$. □

Bemerkung 2. G operiert folglich auf der Menge der Primideale über $\mathfrak{p}$. Die $\sigma\mathfrak{P}$ werden auch die zu $\mathfrak{P}$ konjugierten Primideale genannt.

Satz 3. *G operiert transitiv auf der Menge der Primideale über $\mathfrak{p}$.*

Beweis. Angenommen es gibt zwei Primideale $\mathfrak{P}$ und $\mathfrak{P}'$ über $\mathfrak{p}$, sodass für alle $\sigma \in G$ gilt, dass $\sigma\mathfrak{P} \neq \mathfrak{P}'$. Wir erinnern uns, dass $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, wobei das Produkt die Primideale über $\mathfrak{p}$ durchläuft. Mit dem chinesischen Restsatz ist $\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}$, was die Exitenz eines $x \in \mathcal{O}$ impliziert, sodass $x \equiv 0 \bmod \mathfrak{P}'$ und $x \equiv 1 \bmod \sigma\mathfrak{P}$ für alle $\sigma \in G$.
Sei $N = \prod_{\sigma \in G} \sigma x$, so ist für $\sigma \in G$ beliebig $\sigma N = N$, folglich $N \in K$ und somit $N \in \mathcal{o}$. Nach Konstruktion ist somit $N \in \mathfrak{P}' \cap \mathcal{o} = \mathfrak{p}$. Es ist aber ebenfalls $\sigma x \notin \mathfrak{P}$ für alle $\sigma \in G$, folglich $N \notin \mathfrak{p}$, was ein Widerspruch ergibt. Somit folgt $\sigma\mathfrak{P} = \mathfrak{P}'$ für ein $\sigma \in G$. □

Definition 4. *Für ein Primideal $\mathfrak{P}$ von O sei die Zerlegungsgruppe von $\mathfrak{P}$ über K definiert als die Untergruppe $G_{\mathfrak{P}} := \{\sigma \in G | \sigma\mathfrak{P} = \mathfrak{P}\}$ und der Zerlegungskörper von $\mathfrak{P}$ über K als den Fixkörper $Z_{\mathfrak{P}} := \{x \in L | \forall \sigma \in G_{\mathfrak{P}} : \sigma x = x\}$.*

Bemerkung 5. Es existiert insbesondere eine wohldefinierte Bijektion zwischen den Nebenklassen $G/G_{\mathfrak{P}}$ und der Menge der konjugierten Primideale von $\mathfrak{P}$, gegeben durch $\sigma G_{\mathfrak{P}} \mapsto \sigma\mathfrak{P}$. Insbesondere ist die Anzahl der konjungierten Primidealen gegeben durch $[G : G_{\mathfrak{P}}]$. Insbesondere ist $\mathfrak{p}$ voll zerlegt genau dann, wenn $G_{\mathfrak{P}} = 1$ und unzerlegt, genau dann, wenn $G_{\mathfrak{P}} = G$.

Satz 6. *Für die Zerlegung $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ mit Trägheitsgraden $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}]$ gilt $f_1 = \ldots = f_r =: f$ und $e_1 = \ldots = e_r =: e$. Für ein entsprechendes Repräsentantensystem von $G/G_{\mathfrak{P}}$ erhalten wir somit die Zerlegung $\mathfrak{p}\mathcal{O} = \left(\prod_\sigma \sigma\mathfrak{P}\right)^e$.*

Beweis. Setze $\mathfrak{P} = \mathfrak{P}_1$. Aus Satz 3 folgt, dass $\sigma_i \in G$ existieren, sodass $\mathfrak{P}_i = \sigma_i\mathfrak{P}$. Für alle i induziert σ_i einen Isomorphismus zwischen $\mathcal{O}/\mathfrak{P}$ und $\mathcal{O}/\sigma_i\mathfrak{P}$, gegeben durch $x\mathfrak{P} \mapsto \sigma_i x (\sigma_i\mathfrak{P})$, folglich ist $f_i = [\mathcal{O}/\sigma_i\mathfrak{P} : \mathcal{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}] = f_1 =: f$.
Da $\mathcal{O}$ G-invariant ist, folgt für alle i $\sigma_i(\mathfrak{p}\mathcal{O}) \subseteq \mathfrak{p}\mathcal{O}$. Da σ_i invertierbar ist, folgt $\sigma_i(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$, folglich $\mathfrak{P}^\nu | \mathfrak{p}\mathcal{O} \Leftrightarrow \sigma_i(\mathfrak{P}^\nu) | \sigma_i(\mathfrak{p}\mathcal{O}) \Leftrightarrow (\sigma_i\mathfrak{P})^\nu | \mathfrak{p}\mathcal{O}$ und damit $e_i = e_1 =: e$. □

Satz 7. *Man betrachte die Körpererweiterung $Z_{\mathfrak{P}}|K$, sei $\mathcal{O}_Z$ der ganze Abschluss von $\mathcal{o}$ in $Z_{\mathfrak{P}}$. Sei $\mathfrak{P}_Z := \mathfrak{P} \cap \mathcal{O}_Z$ das Primideal von $Z_{\mathfrak{P}}$ unter $\mathfrak{P}$. So ist:*

(i) *$\mathfrak{P}_Z$ ist unzerlegt in L.*
(ii) *$\mathfrak{P}$ hat über $Z_{\mathfrak{P}}$ den Verzweigungsgrad e und Trägheitsgrad f.*
(iii) *$\mathfrak{P}_Z$ hat über K den Verzweigungsgrad 1 und Trägheitsgrad 1.*

Beweis. Aus dem Hauptsatz der Galoistheorie folgt $G(L|Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$. Somit folgt auf Bemerkung 5, dass $\mathfrak{P}_Z$ unzerlegt ist.
Man erinnere sich, an die fundamentalste Gleichung $\sum_{i=1}^{r} e_i f_i = n$, im galoisschen Fall ergibt sich entsprechend $ref = n$. Da r die Anzahl der Primideale über $\mathfrak{p}$ ist, ist $r = [G : G_{\mathfrak{P}}]$. Da $Z_{\mathfrak{P}}$ der Fixkörper von $G_{\mathfrak{P}}$ ist, folgt hiermit $[L : Z_{\mathfrak{P}}] = |G_{\mathfrak{P}}| = ef$. Wir bezeichnen die Verzweigungsindezes und Trägheitsgrade von $\mathfrak{P}$ über $Z_{\mathfrak{P}}$ bzw. $\mathfrak{P}_z$ über K mit e' und f' bzw. e'' und f''. Es ist nach (i) $\mathfrak{P}_Z\mathcal{O} = \mathfrak{P}^{e'}$. Zudem erhalten wir in $Z_{\mathfrak{P}}|K$ die Zerlegung $\mathfrak{p}\mathcal{O}_Z = \mathfrak{P}_Z^{e''} * (\ldots)$ für weitere über $\mathfrak{p}$ liegenden Primideale. Da $\mathfrak{P}$ das eindeutige über $\mathfrak{P}_Z$ liegende Primideal ist, erhalten wir die Zerlegung $\mathfrak{p}\mathcal{O} = \mathfrak{P}^{e'e''} * (\ldots)$. Insbesondere folgt $e = e'e''$.
Mithilfe der Inklusionen $o/\mathfrak{p} \hookrightarrow \mathcal{O}_{\mathcal{Z}}/\mathcal{P}_{\mathcal{Z}} \hookrightarrow \mathcal{O}/\mathfrak{P}$ folgt genauso
$f = [\mathcal{O}/\mathfrak{P} : o/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{O}_{\mathcal{Z}}/\mathcal{P}_{\mathcal{Z}}]\,[\mathcal{O}_{\mathcal{Z}}/\mathcal{P}_{\mathcal{Z}} : o/\mathfrak{p}] = f'f''$.
Für die Zerlegung $\mathfrak{P}_Z\mathcal{O} = \mathfrak{P}^{e'}$ erhält man zudem aus der fundamentalsten Gleichung
$e'e''f'f'' = ef = [L : Z_{\mathfrak{P}}] = e'f'$. Da $e' \leqslant e$ und $f' \leqslant f''$, folgt also $e' = e$, $f' = f'$, $e'' = 1$ und $f'' = 1$. □

Satz 8. $(\mathcal{O}/\mathfrak{P})\,|\,(o/\mathfrak{p})$ *ist normal.*

Beweis. Man betrachte ein beliebiges Element $\theta\mathfrak{P} \in \mathcal{O}/\mathcal{P}$. Seien $f \in K[x]$ und $\bar{g} \in (o/\mathfrak{p})\,[X]$ die Minimalpolynome von θ und $\theta\mathfrak{P}$. Sei $\bar{f}$ das Bild unter dem Reduktionshomomorphismus $K[X] \to (o/\mathfrak{p})\,[X]$, so folgt $\bar{f}(\theta\mathfrak{P}) = 0$, was $\bar{g}|\bar{f}$ impliziert. Da $L|K$ normal ist, zerfällt f in $K[X]$ in Linearfaktoren, unter dem Reduktionshomomorphismus zerfällt $\bar{f}$ in $(o/\mathfrak{p})\,[X]$ somit auch in Linearfaktoren, und damit ebenfalls $\bar{g}$. Somit ist $(\mathcal{O}/\mathfrak{P})\,|\,(o/\mathfrak{p})$ normal. □

Satz 9. $\Phi : G_{\mathfrak{P}} \twoheadrightarrow \mathrm{Aut}_{(o/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})\,, \sigma \mapsto (a\mathfrak{P} \mapsto \sigma a\mathfrak{P})$ *definiert einen surjektiven Homomorphismus.*

Beweis. Da $\sigma\mathcal{O} = \mathcal{O}$ und $\sigma\mathfrak{P} = \mathfrak{P}$ ist Φ ein wohldefinierter Homomorphismus.
Aus Satz 7 wissen wir $[\mathcal{O}_{\mathcal{Z}}/\mathcal{P}_{\mathcal{Z}} : o/\mathfrak{p}] = 1$, die Inklusion $o/\mathfrak{p} \hookrightarrow \mathcal{O}_{\mathcal{Z}}/\mathcal{P}_{\mathcal{Z}}$ ist folglich ein Isomorphismus, demnach genügt es O.B.d.A. den Fall $\mathfrak{p} = \mathcal{P}_{\mathcal{Z}}$ und $K = Z_{\mathfrak{P}}$ zu betrachten. Daraus ergibt sich entsprechend $o = \mathcal{O}_{\mathcal{Z}}$ und $G = G_{\mathfrak{P}}$. Sei nun $\tilde{K}$ der eindeutige Zwischenkörper von $(\mathcal{O}/\mathfrak{P})\,|\,(o/\mathfrak{p})$, sodass $\tilde{K}|\,(o/\mathfrak{p})$ seperabel und $(\mathcal{O}/\mathfrak{P})\,|\tilde{K}$ rein inseperabel ist, das heißt
$\tilde{K} = \{a \in \mathcal{O}/\mathfrak{P} | a \text{ ist seperabel über } o/\mathfrak{p}\}$. Dann ist $\tilde{K}|\,(o/\mathfrak{p})$ eine endliche galoissche Körpererweiterung mit Galoisgruppe $\tilde{G}$. Da $(\mathcal{O}/\mathfrak{P})\,|\tilde{K}$ rein inseperabel ist, ist $\mathrm{Aut}_{\tilde{K}}\,(\mathcal{O}/\mathfrak{P}) = \{\mathrm{id}_{\mathcal{O}/\mathfrak{P}}\}$, folglich ist die Einschränkung auf $\tilde{K}$ ein Isomorphismus zwischen $\mathrm{Aut}_{(o/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})$ und $\tilde{G}$, wir können folglich $\mathrm{Aut}_{(o/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})$ durch $\tilde{G}$ identifizieren.
Nach dem Satz des primitiven Elements kann man ein $\tilde{a}$ wählen, sodass $\tilde{K} = (o/\mathfrak{p})\,(\tilde{a})$. Sei $a \in L$, sodass $a\mathfrak{P} = \tilde{a}$. Seien nun $f \in K[x]$ und $\bar{g} \in (o/\mathfrak{p})\,[X]$ die Minimalpolynome von a und $\tilde{a}$ und $\bar{f}$ das Bild von f in $o/\mathfrak{p}$. Sei $\tilde{\sigma} \in \tilde{G}$ beliebig, dann ist $\bar{g}(\tilde{\sigma}\tilde{a}) = \bar{f}(\tilde{\sigma}\tilde{a}) = 0$. Da f in Linearfaktoren zerfällt, existiert $a' \in L$, sodass $a'\mathfrak{P} = \tilde{\sigma}\tilde{a}$ und $f(a') = 0$. Insbesondere existiert also $\sigma \in G$, sodass $\sigma a = a'$. Da durch das Bild des primitiven Elementes ein Automorphismus eindeutig definiert ist, ist mit $\Phi(\sigma)(\tilde{a}) = \sigma a\mathfrak{P} = a'\mathfrak{P} = \tilde{\sigma}\tilde{a}$ folglich $\Phi(\sigma) = \tilde{\sigma}$, also ist Φ surjektiv. □

Definition 10. *Wir nennen den Kern von Φ auch die Trägheitsgruppe von $\mathfrak{P}$ über K und bezeichnen ihn mit $I_{\mathfrak{P}}$. Der Trägheitskörper $T_{\mathfrak{P}}$ ist dann entsprechend definiert als der Fixkörper von $I_{\mathfrak{P}}$ in L.*

Korollar 11. *Die Erweiterung $T_{\mathfrak{P}}|Z_{\mathfrak{P}}$ ist wieder galoissch, und es ist $G(T_{\mathfrak{P}}|Z_{\mathfrak{P}}) \cong \mathrm{Aut}_{(o/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})$ und $G(L|T_{\mathfrak{P}}) = I_{\mathfrak{P}}$.*

Beweis. Als Kern eines Homomorphismus ist $I_{\mathfrak{P}}$ ein Normalteiler von $G_{\mathfrak{P}}$, insbesondere folgt aus dem Hauptsatz der Galoistheorie, dass $T_{\mathfrak{P}}|Z_{\mathfrak{P}}$ normal ist. $G(T_{\mathfrak{P}}|Z_{\mathfrak{P}}) \cong \mathrm{Aut}_{(o/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})$ folgt dann entsprechend aus dem Isomorphiesatz, $G(L|T_{\mathfrak{P}}) = I_{\mathfrak{P}}$ folgt aus der Definition von $T_{\mathfrak{P}}$. □

Satz 12. *Wir nehmen zudem an, dass $(\mathcal{O}/\mathfrak{P})\,|\,(o/\mathfrak{p})$ ebenfalls galoissch ist, so gilt $|I_{\mathfrak{P}}| = e$ und $[G_{\mathfrak{P}} : I_{\mathfrak{P}}] = f$.*
Betrachte man den Körperturm $K|Z_{\mathfrak{P}}|T_{\mathfrak{P}}|L$, und sei dann wieder mit $\mathfrak{P}_T$ das unter $\mathfrak{P}$ liegende Primideal von $T_{\mathfrak{P}}$ bezeichnet, so hat $\mathfrak{P}$ über $\mathfrak{P}_T$ den Verzweigungsindex e und Trägheitsgrad 1, $\mathfrak{P}_T$ hat über $\mathfrak{P}_Z$ den Verzweigungsindex 1 und Trägheitsgrad f.

Beweis. Falls $(\mathcal{O}/\mathfrak{P}) \mid (\mathcal{o}/\mathfrak{p})$ galoissch ist, ist die Körpererweiterung insbesondere seperabel, so ist insbesondere $[G_{\mathfrak{P}} : I_{\mathfrak{P}}] = |G(T_{\mathfrak{P}}|Z_{\mathfrak{P}})| = |G(\mathcal{O}/\mathfrak{P}|\mathcal{o}/\mathfrak{p})| = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}] = f$. Da $|G_{\mathfrak{P}}| = ef$, folgt $|I_{\mathfrak{P}}| = e$.
Sei $\mathcal{O}_T$ der ganzer Abschluss von $\mathcal{o}$ in $T_{\mathfrak{P}}$. Per Definition wird $I_{\mathfrak{P}}$ durch Φ auf das neutrale Element abgebildet, was insbesondere auch für den entsprechenden Homomorphismus
$I_{\mathfrak{P}} \to \mathrm{Aut}_{(\mathcal{O}_\mathcal{T}/\mathcal{P}_\mathcal{T})}(\mathcal{O}/\mathfrak{P})$ gilt. Nach Satz 9 ist dieser Homomorphismus surjektiv, folglich ist $[\mathcal{O}/\mathfrak{P} : \mathcal{O}_\mathcal{T}/\mathcal{P}_\mathcal{T}] = 1$. Da $I_{\mathfrak{P}}$ eine Untergruppe von $G_{\mathfrak{P}}$ ist, lässt $I_{\mathfrak{P}}$ ebenfalls $\mathfrak{P}$ invariant, somit ist $\mathfrak{P}_T$ unzerlegt in L, somit folgt aus der fundamentalsten Gleichung, dass der Verzweigungsindex e ist.
Da $f = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{O}_\mathcal{T}/\mathcal{P}_\mathcal{T}]\,[\mathcal{O}_\mathcal{T}/\mathcal{P}_\mathcal{T} : \mathcal{O}_\mathcal{Z}/\mathcal{P}_\mathcal{Z}]$, folgt dass $\mathfrak{P}_T$ über $\mathfrak{P}_Z$ Trägheitsgrad f hat. Entsprechend folgt wieder aus Unzerlegtheit, dass der Verzweigungsindex 1 ist. □

2. Der Lokale Frobenius

Beispiel 13. *Wir betrachten den Fall $\mathcal{o} = \mathbb{Z}$, folglich $K = \mathbb{Q}$ und zusätzlich eine endliche Galois Erweiterung $L|\mathbb{Q}$. Sei $\mathfrak{P}$ ein unverzweigtes Primideal in $\mathbb{Z}_L$ über ein Primideal (p). Dann existiert genau ein $\sigma \in G(L|\mathbb{Q})$, sodass für alle $a \in \mathbb{Z}_L$ gilt, dass $\sigma(a) \equiv a^p \bmod \mathfrak{P}$. Dieser Automorphismus wird auch der lokale Frobenius zum Primideal $\mathfrak{P}$ über (p) genannt.*

Beweis. Man bemerke, dass $\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p)$ eine endliche Körpererweiterung der Charakteristik p ist. Insbesondere ist die Erweiterung zyklisch mit $G(\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p)) = \langle F\rangle$, wobei
$F : \mathbb{Z}_L/\mathfrak{P} \to \mathbb{Z}_L/\mathfrak{P}, x \mapsto x^p$ der Frobeniusendomorphismus ist.
Da insbesondere $\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p)$ galoissch ist, und da $\mathfrak{P}$ unverzweigt ist, folgt aus Satz 12, dass $I_{\mathfrak{P}} = 1$, somit ist der Homomorphismus $\Phi : G_{\mathfrak{P}} \to G(\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p))$ aus Satz 9 ein Isomorphismus. Folglich gibt es genau ein $\sigma := \Phi^{-1}(F) \in G_{\mathfrak{P}}$, sodass für alle $a \in \mathbb{Z}_L$ gilt, dass $\sigma a \equiv a^p \bmod \mathfrak{P}$.
Da jedes Element aus $G(L|\mathbb{Q})$, welches diese Eigenschaft hat insbesondere $\mathfrak{P}$ invariant lässt, liegt dieses ebenfalls in $G_{\mathfrak{P}}$, folglich ist dieses σ in ganz $G(L|\mathbb{Q})$ eindeutig. □

Bemerkung 14. Falls $G(L|\mathbb{Q})$ abelsch ist, so ist dieser Automorphismus unabhängig von der Wahl von $\mathfrak{P}$. Dann schreibe man für den lokalen Frobenius auch $\left(\frac{L/\mathbb{Q}}{p}\right)$.

Beweis. Seien $\mathfrak{P}$ und $\mathfrak{P}'$ zwei verschiedene Primideale über (p), und seien entsprechend σ und σ' ihre lokalen Frobeniusabbildungen. Nach Satz 3 können wir ein $\tau \in G(L|\mathbb{Q})$ wählen, sodass
$\tau\mathfrak{P} = \mathfrak{P}'$. Sei $a \in \mathbb{Z}_L$ beliebig, dann ist
$\left(\tau \circ \sigma \circ \tau^{-1}\right)(a\mathfrak{P}') = \tau\left(\sigma\left(\tau^{-1}(a)\,\mathfrak{P}\right)\right) = \tau\left(\left(\tau^{-1}(a)\right)^p\mathfrak{P}\right) = a^p\mathfrak{P}'$, aus der Eindeutigkeit folgt somit $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. Im Fall einer abelschen Erweiterung folgt schließlich $\sigma = \sigma'$. □

Lemma 15. *Sei das Primideal $\mathfrak{P}$ in L über (p) unverzweigt. Dann ist der lokale Frobenius der triviale Automorphismus genau dann, wenn (p) total zerlegt ist.*

Beweis. Aus der Konstruktion des lokalen Frobenius folgt, dass dieser nur dann trivial sein kann, falls F in $G(\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p)) = \langle F\rangle$ trivial ist, was gleichbedeutend ist mit $f = 1$, das heißt (p) ist total zerlegt, ist. □

Lemma 16. *Für quadratfreies a und einer ungeraden zur a teilerfremden Primzahl p ist $\left(\frac{a}{p}\right) = 1$ genau dann, wenn (p) total zerlegt in $\mathbb{Q}(\sqrt{a})$ ist.*

Beweis. Es ist $\left(\frac{a}{p}\right) = 1$ per Definition genau dann, wenn ein $\alpha \in \mathbb{Z}$ existiert, sodass für die Polynome gilt $x^2 - a \equiv (x-\alpha)(x+\alpha) \bmod (p)$. Jetzt ist $x^2 - a$ das Minimalpolynom von $\sqrt{a}$, und da q und a teilerfremd sind, zerfällt dieses also in unterschiedliche Linearfaktoren, nach dem Zerlegungsgesetz aus Vorlesung 4 folgt demnach, dass (p) totalzerlegt in $\mathbb{Q}(\sqrt{a})$ ist.
Ist hingegen $\left(\frac{a}{p}\right) = -1$, so ist $x^2 - a$ irreduzibel mod$p$, insbesondere erhielte man $f = 2$, (p) wäre dann nicht total zerlegt in $\mathbb{Q}(\sqrt{a})$. □

Beispiel 17. *Hiermit erhalten wir einen alternativen Beweis für das quadratische Reziprozitätsgesetz $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ für zwei verschiedene ungerade Primzahlen p und q.*

Beweis. Sei $q^\star := (-1)^{\frac{q-1}{2}}q$. Nach der 2. Vorlesung folgt aus der
Multiplikativität $\left(\frac{q^\star}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$. Es genügt folglich $\left(\frac{q^\star}{p}\right) = \left(\frac{p}{q}\right)$ zu zeigen.
Man betrachte hierfür den Körperturm $\mathbb{Q}(\zeta_q)|\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q}$ für eine $q$te primitive Einheitswurzel. Da

$G(\mathbb{Q}(\zeta_q)|\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$, ist die Erweiterung abelsch, zudem ist, da p und q verschiedene Primzahlen sind, p unverzweigt in $\mathbb{Q}(\zeta_q)$, folglich auch in $\mathbb{Q}(\sqrt{q^\star})$.
Seien $\mathfrak{P}$ und $\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Q}(\sqrt{q^\star})$ Primideale von $\mathbb{Q}(\zeta_q)$ bzw. $\mathbb{Q}(\sqrt{q^\star})$ über (p). Man bemerke, dass $\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q}$ normal ist. Da zudem für alle $a \in \mathbb{Z}_{\mathbb{Q}(\sqrt{q^\star})}$ gilt, dass
$\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)|_{\mathbb{Q}(\sqrt{q^\star})}(a) - a^p \in \mathfrak{P} \cap \mathbb{Q}(\sqrt{q^\star}) = \mathfrak{P}'$, ist $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)|_{\mathbb{Q}(\sqrt{q^\star})} = \left(\frac{\mathbb{Q}(\sqrt{q^\star})/\mathbb{Q}}{p}\right)$.
Da $\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q}$ normal ist, erhält man nach dem Hauptsatz der Galoistheorie durch die Einschränkung einen Isomorphismus $G(\mathbb{Q}(\zeta_q)|\mathbb{Q})/G(\mathbb{Q}(\zeta_q)|\mathbb{Q}(\sqrt{q^\star})) \to G(\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q})$, beziehungsweise somit einen surjektiven Homomorphismus $G(\mathbb{Q}(\zeta_q)|\mathbb{Q}) \twoheadrightarrow G(\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q}), \sigma \mapsto \sigma_{\mathbb{Q}(\sqrt{q^\star})}$. Da $G(\mathbb{Q}(\zeta_q)|\mathbb{Q})$ und $G(\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q})$ zyklisch sind, ist solch ein Homomorphismus eindeutig. Wir identifizieren $G(\mathbb{Q}(\zeta_q)|\mathbb{Q})$ durch $(\mathbb{Z}/q\mathbb{Z})^\times$ und $G(\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q})$ durch $\{1, -1\}$. Aus Vorlesung 2 folgt, dass dieser Homomorphismus dann eindeutigerweise durch $a \mapsto \left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \bmod q$ definiert ist.
Sei $\sigma \in G(\mathbb{Q}(\zeta_q)|\mathbb{Q})$ definiert durch $\zeta_q \mapsto \zeta_q^p$. Da $p \in \mathfrak{P}$, folgt für alle $a \in \mathbb{Z}_{\mathbb{Q}(\zeta_q)}$ somit $\sigma(a) \equiv a^p \bmod \mathfrak{P}$, folglich aus Eindeutigkeit $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right) = \sigma$. Unter der obigen Identifikation ist die Einschränkung auf $\mathbb{Q}(\sqrt{q^\star})$ gegeben als $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)|_{\mathbb{Q}(\sqrt{q^\star})} = \left(\frac{\mathbb{Q}(\sqrt{q^\star})/\mathbb{Q}}{p}\right) = \left(\frac{p}{q}\right)$.
Aus Lemma 15 und 16 folgt entsprechend $\left(\frac{\mathbb{Q}(\sqrt{q^\star})/\mathbb{Q}}{p}\right) = \left(\frac{q^\star}{p}\right)$, folglich haben wir $\left(\frac{q^\star}{p}\right) = \left(\frac{p}{q}\right)$ gezeigt. $\square$

References

[1] A. Schmidt, Einführung in die algebraisch Zahlentheorie. Springer, Berlin, 2007

Email address: `kezhang@ethz.ch`