Universität Konstanz
Fachbereich Mathematik und Statistik
Markus Schweighofer

§4 Das quadratische Reziprozitätsgesetz

[Johann Carl Friedrich Gauß *1777 †1855]

4.1 Kreisteilungskörper

Proposition 4.1.1. (a) *Sind $a, n \in \mathbb{Z}$, so*

$$\overline{a}^{(n)} \in (\mathbb{Z}/(n))^\times \iff (a,n) = (1).$$

(b) *Ist $n \in \mathbb{N}$, so*

$$(\mathbb{Z}/(n))^\times = \{\overline{a}^{(n)} \mid a \in \{0,\dots,n-1\}, (a,n) = (1)\}.$$

Beweis. (a) Seien $a, n \in \mathbb{Z}$. Ist $\overline{a} \in (\mathbb{Z}/(n))^\times$, so gibt es $s \in \mathbb{Z}$ mit $\overline{sa}^{(n)} = 1$ und daher auch $t \in \mathbb{Z}$ mit $sa + tn = 1$. Ist umgekehrt $(a,n) = 1$, so gibt es $s, t \in \mathbb{Z}$ mit $sa + tn = 1$ und daher $\overline{s}^{(n)}\overline{a}^{(n)} = 1$. □

Definition 4.1.2. Die Abbildung

$$\varphi\colon \mathbb{N} \to \mathbb{N},\ n \mapsto \#(\mathbb{Z}/(n))^\times$$

heißt *Eulersche φ-Funktion.* [Leonard Euler *1707 †1783]

Proposition 4.1.3. (a) $\forall m, n \in \mathbb{N} : ((m,n) = (1) \implies \varphi(mn) = \varphi(m)\varphi(n))$

(b) $\forall p \in \mathbb{P} : \forall k \in \mathbb{N} : \varphi(p^k) = (p-1)p^{k-1}$

(c) $\forall n \in \mathbb{N} : \varphi(n) = n \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} (1 - \frac{1}{p})$

Beweis. (a) Sind $m, n \in \mathbb{N}$ mit $(m,n) = (1)$, so gilt nach dem Chinesischen Restsatz $\mathbb{Z}/(mn) \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n)$ und daher $(\mathbb{Z}/(mn))^\times \cong (\mathbb{Z}/(m))^\times \times (\mathbb{Z}/(n))^\times$.

(b) Sind $p \in \mathbb{P}$ und $k \in \mathbb{N}$, so

$$\begin{aligned}\varphi(p^k) &\overset{4.1.1(b)}{=} \#\{a \in \{0,\dots,p^k-1\} \mid p \nmid a\} \\ &= \#(\{0,\dots,p^k-1\} \setminus \{0,p,\dots,p^k-p\}) = p^k - p^{k-1} = (p-1)p^{k-1}.\end{aligned}$$

(c) Sei $n \in \mathbb{N}$. Schreibe $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ mit $m \in \mathbb{N}_0$, $p_1, \dots, p_m \in \mathbb{P}$ paarweise verschieden und $\alpha_1, \dots, \alpha_m \in \mathbb{N}$. Dann

$$\begin{aligned}\varphi(n) &\overset{(a)}{=} \varphi(p_1^{\alpha_1}) \cdots \varphi(p_m^{\alpha_m}) \overset{(b)}{=} p_1^{\alpha_1 - 1} \cdots p_m^{\alpha_m - 1}(p_1 - 1) \cdots (p_m - 1) \\ &= \underbrace{p_1^{\alpha_1} \cdots p_m^{\alpha_m}}_{=n} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right).\end{aligned}$$

□

Bemerkung 4.1.4. Sei G eine multiplikativ geschriebene endliche zyklische Gruppe der Ordnung n. Sei $a \in G$ mit $G = \langle a \rangle$. Dann ist

$$\mathbb{Z}/\langle n \rangle \to G,\ \overline{k} \mapsto a^k\ (k \in \mathbb{Z})$$

wohldefiniert und ein Gruppenisomorphismus. Für alle $k \in \mathbb{Z}$ gilt

$$(k, n) = (1) \iff \overline{k} \in (\mathbb{Z}/(n))^\times \iff G = \langle a^k \rangle.$$

Definition 4.1.5. Sei K ein Körper und $\zeta \in K$. Man nennt ζ

- eine *Einheitswurzel* in K, wenn $\exists n \in \mathbb{N} : \zeta^n = 1$,
- eine *n-te Einheitswurzel* in K ($n \in \mathbb{N}$), wenn $\zeta^n = 1$ und
- eine *primitive n-te Einheitswurzel* in K ($n \in \mathbb{N}$), wenn $\zeta \in K^\times$ die Ordnung n hat.

Bemerkung 4.1.6. Sei K ein Körper.

(a) Die Einheitswurzeln in K bilden eine Untergruppe von $K^\times$.

(b) Ist $n \in \mathbb{N}$, so bilden die n-ten Einheitswurzeln in K eine zyklische Untergruppe von $K^\times$, deren Ordnung n teilt ($X^n - 1$ hat nur endlich viele Nullstellen, aber endliche Untergruppen von $K^\times$ sind zyklisch und nach Lagrange teilt die Ordnung eines Erzeugers n).

Beispiel 4.1.7. Sei $n \in \mathbb{N}$. Die n-ten Einheitswurzeln in $\mathbb{C}$ sind

$$e^{\frac{2k\pi i}{n}} \qquad (k \in \{0, \ldots, n-1\}).$$

Ist $k \in \mathbb{Z}$, so ist $e^{\frac{2k\pi i}{n}}$ gemäß Bemerkung 4.1.4 genau dann eine primitive n-te Einheitswurzel in $\mathbb{C}$, wenn $(k, n) = (1)$.

Proposition 4.1.8. *Sei K ein Körper, $p := \operatorname{char} K \in \{0\} \cup \mathbb{P}$ und $n \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:*

(a) *K besitzt eine primitive n-te Einheitswurzel.*

(b) *K besitzt n n-te Einheitswurzeln.*

(c) *$p \nmid n$ und $X^n - 1$ zerfällt in $K[X]$.*

Beweis. (a) $\Longrightarrow$ (b) ist trivial.

(b) $\Longrightarrow$ (a) ist klar mit 4.1.6(b).

Setzt man $f := X^n - 1$, so $f' = nX^{n-1}$ und daher

$$f \text{ separabel} \iff f' \neq 0 \iff n \neq 0 \text{ in } K \iff p \nmid n.$$

Hieraus (b) $\Longleftrightarrow$ (c). □

Definition 4.1.9. Sei $n \in \mathbb{N}$. Dann heißt

$$\Phi_n := \prod_{\substack{\zeta \text{ primitive} \\ n\text{-te Einheitswurzel} \\ \text{in } \mathbb{C}}} (X - \zeta) \overset{4.1.7}{=} \prod_{\substack{k=0 \\ (k,n)=(1)}}^{n-1} \left(X - e^{\frac{2k\pi i}{n}} \right) \in \mathbb{Q}[X]$$

[mit Galoistheorie angewandt auf den Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$ folgt leicht $\Phi_n \in \mathbb{Q}[X]$] das *n-te Kreisteilungspolynom* und sein Zerfällungskörper über $\mathbb{Q}$ der *n*-te *Kreisteilungskörper*.

Bemerkung 4.1.10. Sei $n \in \mathbb{N}$ und ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Dann ist $\mathbb{Q}(\zeta)$ der Zerfällungskörper von $X^n - 1$ und damit auch der n-te Kreisteilungskörper.

Satz 4.1.11. *Sei $n \in \mathbb{N}$. Der n-te Kreisteilungskörper ist galoissch über $\mathbb{Q}$ mit Galoisgruppe $G \cong (\mathbb{Z}/(n))^\times$. Sei ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Dann*

$$G \xrightarrow{\cong} (\mathbb{Z}/(n))^\times,\ \varphi \mapsto \overline{k} \text{ falls } k \in \mathbb{Z} \text{ mit } \varphi(\zeta) = \zeta^k.$$

Beweis. Als Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$ ist der n-te Kreisteilungskörper galoissch über $\mathbb{Q}$. Wendet man 4.1.4 auf die Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$ an, so sieht man, dass die Abbildung wohldefiniert ist. Sie ist auch ein Gruppenhomomorphismus, denn sind $\varphi, \psi \in G$ und $k, \ell \in \mathbb{Z}$ mit $\varphi(\zeta) = \zeta^k$ und $\psi(\zeta) = \zeta^\ell$, so $(\varphi\psi)(\zeta) = \varphi(\psi(\zeta)) = \varphi(\zeta^\ell) = (\varphi(\zeta))^\ell = (\zeta^k)^\ell = \zeta^{k\ell}$. Die Abbildung ist offensichtlich auch injektiv, womit $\#G \leq \varphi(n)$ folgt. Für die Surjektivität zeigen wir $\#G \geq \varphi(n)$. Mit Galoistheorie gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \#G$. Es ist daher $[\mathbb{Q}(\zeta) : \mathbb{Q}] \geq \varphi(n)$ zu zeigen. Setze $f := \operatorname{irr}_{\mathbb{Q}}(\zeta) \in \mathbb{Q}[X]$. Zu zeigen: $\deg f \geq \varphi(n)$. Es reicht zu zeigen, dass jede primitive n-te Einheitswurzel in $\mathbb{C}$ eine Nullstelle von f ist. Man überlegt sich, dass es wegen 4.1.4 reicht zu zeigen, dass für jede primitive n-te Einheitswurzel z in $\mathbb{C}$ und alle $p \in \mathbb{P}$ mit $p \nmid n$ gilt

$$f(z) = 0 \implies f(z^p) = 0.$$

Sei hierzu $z \in \mathbb{C}$ und $p \in \mathbb{P}$ mit $f(z) = 0$ und $f(z^p) \neq 0$. Zu zeigen ist $p \mid n$. Schreibe $X^n - 1 = fg$ mit $f, g \in \mathbb{Q}[X]$ normiert. Nach dem Lemma von Gauß gilt $f, g \in \mathbb{Z}[X]$. Wegen $f(z^p) \neq 0$ und $(fg)(z^p) = 0$ folgt $g(z^p) = 0$, das heißt z ist Nullstelle von $g(X^p)$ und es gibt $h \in \mathbb{Q}[X]$ mit $g(X^p) = fh$. Wieder mit dem Lemma von Gauß sieht man $h \in \mathbb{Z}[X]$. Reduziere nun die Koeffizienten modulo p (das heißt, wende den Ringhomomorphismus $\mathbb{Z}[X] \to \mathbb{F}_p[X],\ p \mapsto \overline{p}$ mit $\overline{X} = X$ an) und benutze den Frobeniushomomorphismus $\mathbb{F}_p[X] \to \mathbb{F}_p[X]$, um $X^n - 1 = \overline{f}\,\overline{g}$ und

$$\overline{g}^p = \overline{g}(X^p) = \overline{g(X^p)} = \overline{fh} = \overline{f} \cdot \overline{h}$$

zu erhalten. Wegen $\overline{f} \mid \overline{g}^p$ ist $X^n - 1$ nicht separabel über $\mathbb{F}_p$. Wegen $(X^n - 1)' = nX^{n-1} \in \mathbb{F}_p[X]$ gilt dann aber $n = 0$ in $\mathbb{F}_p[X]$, das heißt $p \mid n$ wie gewünscht. □

Korollar 4.1.12. *Sei $n \in \mathbb{N}$. Der n-te Kreisteilungskörper ist ein Zahlkörper vom Grad $\varphi(n)$.*

Korollar 4.1.13. *Sei $n \in \mathbb{N}$. Dann ist Φ_n irreduzibel in $\mathbb{Q}[X]$ und es gilt $\Phi_n \in \mathbb{Z}[X]$.*

Beweis. Bezeichne ζ eine n-te primitive Einheitswurzel in $\mathbb{C}$. Nach 4.1.12 gilt

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = \deg(\Phi_n).$$

Also ist $\Phi_n = \mathrm{irr}_{\mathbb{Q}}(\zeta)$. Mit 2.1.14 folgt $\Phi_n \in \mathbb{Z}[X]$, da ζ ganz über $\mathbb{Z}$ ist. □

Bemerkung 4.1.14. Die für alle $n \in \mathbb{N}$ gültige Formel

$$X^n - 1 = \prod_{\substack{\zeta \in \mathbb{C} \\ \zeta^n = 1}} (X - \zeta) = \prod_{\substack{d \in \mathbb{N} \\ d|n}} \prod_{\substack{\zeta \text{ primitive} \\ d\text{-te Einheitswurzel}}} (X - \zeta) = \prod_{\substack{d \in \mathbb{N} \\ d|n}} \Phi_d$$

liefert ein rekursives Berechnungsverfahren für Φ_n. Zum Beispiel gilt

$$\Phi_{12} = \frac{X^{12} - 1}{\Phi_1 \Phi_2 \Phi_3 \Phi_4 \Phi_6} = \frac{X^{12} - 1}{(X^6 - 1)\Phi_4} = \frac{X^6 + 1}{\Phi_4} \quad \text{und}$$
$$\Phi_4 = \frac{X^4 - 1}{\Phi_1 \Phi_2} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1.$$

Also $\Phi_{12} = \frac{X^6+1}{X^2+1} = X^4 - X^2 + 1$.

Bemerkung 4.1.15. Aus 4.1.14 folgt leicht $\Phi_n(0) = 1$ für alle $n \in \mathbb{N}$ mit $n \geq 2$.

4.2 Zahlringe von Kreisteilungskörpern

Lemma 4.2.1. *Sei $p \in \mathbb{P}$, $m \in \mathbb{N}$, $n := p^m$, ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$ und $K := \mathbb{Q}(\zeta)$. Dann gilt:*

(a) $d_{K|\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\varphi(n)-1}) = (-1)^{\frac{\varphi(n)(\varphi(n)-1)}{2}} p^{p^{m-1}(m(p-1)-1)}$

(b) *Für alle weiteren primitiven n-te Einheitswurzeln ξ in $\mathbb{C}$ gilt $\frac{1-\xi}{1-\zeta} \in \mathcal{O}_K^\times$.*

(c) $p\mathcal{O}_K = (1 - \zeta)^{\varphi(n)} \mathcal{O}_K$

(d) $1 - \zeta$ *ist prim in* $\mathcal{O}_K$.

(e) $\mathcal{O}_K / (1 - \zeta)\mathcal{O}_k \cong \mathbb{F}_p$

Beweis. (a) Nach 2.4.22 gilt $d_{K|\mathbb{Q}}(1, \ldots, \zeta^{\varphi(n)-1}) = (-1)^{\frac{\varphi(n)(\varphi(n)-1)}{2}} N_{K|\mathbb{Q}}(\Phi_n'(\zeta))$. Nach 4.1.14 gilt $X^n - 1 = \Phi_n \cdot (X^{p^{m-1}} - 1)$. Ableiten liefert

$$nX^{n-1} = \Phi_n' \cdot (X^{p^{m-1}} - 1) + \Phi_n \cdot (p^{m-1} X^{p^{m-1}-1}).$$

Setzt man hier ζ ein, so erhält man $n\zeta^{n-1} = (\Phi_n'(\zeta))(\zeta^{p^{m-1}} - 1)$, also

$$(*) \qquad (\Phi_n'(\zeta))\zeta(z - 1) = n,$$

wobei $z := \zeta^{p^{m-1}}$ eine primitive p-te Einheitswurzel ist. Wegen

$$\operatorname{irr}_{\mathbb{Q}}(z) = \Phi_p \overset{4.1.14}{=} \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + 1 \quad \text{und}$$
$$\operatorname{irr}_{\mathbb{Q}}(z-1) = \Phi_p(X+1)$$

gilt nach 2.4.5 $N_{K|\mathbb{Q}}(z-1) = (-1)^{\varphi(n)} p^{[K:\mathbb{Q}(z-1)]}$. Weiter gilt $N_{K|\mathbb{Q}}(\zeta) \overset{2.4.5}{=} (-1)^{\varphi(n)} \Phi_n(0) \overset{4.1.15}{=} (-1)^{\varphi(n)}$. Wendet man die Norm auf beide Seiten von $(*)$ an, so folgt also

$$(**) \qquad N_{K|\mathbb{Q}}(\Phi_n'(\zeta)) p^{[K:\mathbb{Q}(z)]} = n^{[K:\mathbb{Q}]}.$$

Mit $\varphi(n) = [K:\mathbb{Q}] = [K:\mathbb{Q}(z)][\mathbb{Q}(z):\mathbb{Q}] = [K:\mathbb{Q}(z)]\varphi(p)$ und

$$\varphi(n) = \varphi(p^m) \overset{4.1.3(b)}{=} (p-1)p^{m-1} \overset{4.1.3(b)}{=} \varphi(p)p^{m-1}$$

folgt $[K:\mathbb{Q}(z)] = p^{m-1}$. Aus $(**)$ folgt daher

$$N_{K|\mathbb{Q}}(\Phi_n'(\zeta)) = p^{m\varphi(n) - p^{m-1}} = p^{m(p-1)p^{m-1} - p^{m-1}} = p^{p^{m-1}(m(p-1)-1)}.$$

(b) Sei ξ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Nach Bemerkung 4.1.4 kann man dann $\xi = \zeta^k$ für ein $k \in \{0, \ldots, n-1\}$ mit $(k,n) = (1)$ schreiben. Dann

$$\frac{1-\xi}{1-\zeta} = \frac{1-\zeta^k}{1-\zeta} = \zeta^{k-1} + \ldots + 1 \in \mathscr{O}_K.$$

Analog folgt $\frac{1-\zeta}{1-\xi} \in \mathscr{O}_K$.

(c) Es gilt

$$\Phi_n \overset{4.1.14}{=} \frac{X^n - 1}{X^{p^{m-1}} - 1} = X^{p^{m-1}(p-1)} + \ldots + X^{p^{m-1}} + 1$$

und daher

$$p = \Phi_n(1) = \prod_{\substack{k=0 \\ (k,n)=(1)}}^{n-1} (1 - \zeta^k),$$

woraus mit (b) das Gewünschte folgt.

(d) folgt aus 2.7.6, denn wäre $1-\zeta$ nicht prim in $\mathscr{O}_K$, so würde eine Primidealzerlegung von $(1-\zeta)\mathscr{O}_K$ in $\mathscr{O}_K$ wegen (c) zeigen, dass $e_{p\mathbb{Z}}(\mathscr{O}_K) > \varphi(n) = [K:\mathbb{Q}]$.

(e) folgt aus (c) und (d) wieder mit 2.7.6. □

Satz 4.2.2. *Sei $p \in \mathbb{P}$, $m \in \mathbb{N}$, $n := p^m$, K der n-te Kreisteilungskörper und ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Dann*

$$\mathscr{O}_K = \mathbb{Z}[\zeta] = \mathbb{Z} \oplus \mathbb{Z}\zeta \oplus \ldots \oplus \mathbb{Z}\zeta^{\varphi(n)-1}$$

und

$$d(\mathscr{O}_K) = (-1)^{\frac{\varphi(n)(\varphi(n)-1)}{2}} p^{p^{m-1}(m(p-1)-1)}.$$

Beweis. Da das n-te Kreisteilungspolynom Φ_n ein normiertes Polynom vom Grad $\varphi(n)$ mit ganzzahligen Koeffizienten ist [→4.1.9, 4.1.12, 4.1.13], folgt aus $\Phi_n(\zeta) = 0$, dass $\mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta + \ldots + \mathbb{Z}\zeta^{\varphi(n)-1}$. Natürlich bilden $1, \ldots, \zeta^{\varphi(n)-1}$ wegen $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\zeta)$, woraus insbesondere folgt, dass $1, \ldots, \zeta^{\varphi(n)-1}$ linear unabhängig im $\mathbb{Z}$-Modul $\mathbb{Z}[\zeta]$ sind. Daraus folgt, dass $1, \ldots, \zeta^{\varphi(n)-1}$ eine Basis des $\mathbb{Z}$-Moduls $\mathbb{Z}[\zeta]$ ist, weswegen $\mathbb{Z}[\zeta]$ ein Gitter in K ist und die behauptete Gleichheit $\mathbb{Z}[\zeta] = \mathbb{Z} \oplus \mathbb{Z}\zeta \oplus \ldots \oplus \mathbb{Z}\zeta^{\varphi(n)-1}$ gilt. Die Diskriminante $d(\mathbb{Z}[\zeta])$ [→ 3.1.5] des multiplikativen Gitters $\mathbb{Z}[\zeta]$ ist nach 4.2.1(a) bis auf das Vorzeichen eine Potenz von p und daher ist nach 3.1.7 auch $[\mathscr{O}_K : \mathbb{Z}[\zeta]]$ eine Potenz von p. Es gibt also $k \in \mathbb{N}_0$ mit $p^k\mathscr{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathscr{O}_K$. Setzt man

$$\mathfrak{q} := (1-\zeta)\mathscr{O}_K \overset{4.2.1(d)}{\in} M_{\mathscr{O}_K},$$

so gilt nach 4.2.1(e) $\mathscr{O}_K/\mathfrak{q} \cong \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, also $\mathscr{O}_K = \mathbb{Z} + \mathfrak{q}$ und daher erst recht $\mathscr{O}_K = \mathbb{Z}[\zeta] + \mathfrak{q}$. Durch Multiplizieren mit $(1-\zeta)^\ell$ ergibt sich $\mathfrak{q}^\ell = (1-\zeta)^\ell\mathbb{Z}[\zeta] + \mathfrak{q}^{\ell+1}$ für alle $\ell \in \mathbb{N}_0$ und durch Induktion $\mathscr{O}_K = \mathbb{Z}[\zeta] + \mathfrak{q}^\ell$ für alle $\ell \in \mathbb{N}_0$. Speziell für $\ell := k\varphi(n)$ folgt laut 4.2.1(c)

$$\mathscr{O}_K = \mathbb{Z}[\zeta] + ((1-\zeta)^{\varphi(n)})^k\mathscr{O}_K = \mathbb{Z}[\zeta] + p^k\mathscr{O}_K = \mathbb{Z}[\zeta].$$

Schließlich gilt $d(\mathscr{O}_K) = d(\mathbb{Z}[\zeta]) \overset{4.2.1(a)}{=} (-1)^{\frac{\varphi(n)(\varphi(n)-1)}{2}} p^{p^{m-1}(m(p-1)-1)}$. □

Korollar 4.2.3. *Sei p eine ungerade Primzahl und K der p-te Kreisteilungskörper. Dann gibt es genau einen Zwischenkörper E von $K|\mathbb{Q}$ mit $[E : \mathbb{Q}] = 2$ und zwar gilt*

$$E = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right).$$

Beweis. Nach 4.1.3(b) gilt $\varphi(p) = p-1$. Daher gilt nach Satz 4.2.2

$$d(\mathscr{O}_K) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$$

und dies muss wegen Proposition 2.4.21 ein Quadrat in K sein, weil $K|\mathbb{Q}$ normal ist. Da $p-1$ gerade und $p-2$ ungerade ist, gilt $(-1)^{\frac{(p-1)(p-2)}{2}} = ((-1)^{\frac{p-1}{2}})^{p-2} = (-1)^{\frac{p-1}{2}}$. Da $p-3$ gerade ist, ist weiter p^{p-3} ein Quadrat in K. Insgesamt ist daher $(-1)^{\frac{p-1}{2}}p$ ein Quadrat in K und somit

$$E := \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$$

ein Unterkörper von K. Wegen $(-1)^{\frac{p-1}{2}}p \in \not\square$ gilt $[E : \mathbb{Q}] = 2$ [→ 3.2.4]. Dass E der einzige Zwischenkörper von $K|\mathbb{Q}$ vom Grad 2 über $\mathbb{Q}$ ist, folgt leicht aus Galoistheorie, denn die Galoisgruppe von $K|\mathbb{Q}$ besitzt genau eine Untergruppe vom Index 2. In der Tat: Diese Galoisgruppe ist nach 4.1.11 isomorph zu $\mathbb{F}_p^\times$ und daher zyklisch (endliche Untergruppen von multiplikativen Gruppen von Körpern sind zyklisch). Aber endliche zyklische Gruppen besitzen zu jedem Teiler ihrer Gruppenordnung genau eine Untergruppe vom entsprechenden Index, wie man sich sofort überlegt. □

4.3 Das Legendre-Symbol [Adrien-Marie Legendre *1752 †1833]

Definition 4.3.1. Seien $a, n \in \mathbb{Z}$. Wir nennen a einen *quadratischen Rest modulo n*, wenn es ein $k \in \mathbb{Z}$ gibt mit $a \equiv_{(n)} k^2$. Andernfalls nennen wir a einen *quadratischen Nichtrest modulo n*.

Definition 4.3.2. Sei $a \in \mathbb{Z}$ und $p \in \mathbb{P}$ eine ungerade Primzahl. Dann ist das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ durch

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist und } p \nmid a, \\ 0 & \text{falls } p \mid a, \\ -1 & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist} \end{cases}$$

definiert.

Satz 4.3.3. *Sei $p \in \mathbb{P}$ eine ungerade Primzahl. Dann gilt:*

(a) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *für alle $a, b \in \mathbb{Z}$ mit $a \equiv_{(p)} b$.*

(b) $\left(\frac{a}{p}\right) \equiv_{(p)} a^{\frac{p-1}{2}}$ *für alle $a \in \mathbb{Z}$ („Legendres Charakterisierung").*

(c) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ *für alle $a, b \in \mathbb{Z}$ („Multiplikativität").*

(d) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv_{(4)} 1 \\ -1 & \text{falls } p \equiv_{(4)} 3 \end{cases}$
(„erster Ergänzungssatz zum quadratischen Reziprozitätsgesetz")

(e) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv_{(8)} 1 \text{ oder } p \equiv_{(8)} 7 \\ -1 & \text{falls } p \equiv_{(8)} 3 \text{ oder } p \equiv_{(8)} 5 \end{cases}$
(„zweiter Ergänzungssatz zum quadratischen Reziprozitätsgesetz")

Beweis. (a) ist trivial.

(b) Es reicht zu zeigen, dass die Untergruppe $(\mathbb{F}_p^\times)^2 := \{a^2 \mid a \in \mathbb{F}_p^\times\}$ von $\mathbb{F}_p^\times$ gleich $A := \{a \in \mathbb{F}_p^\times \mid a^{\frac{p-1}{2}} = 1\}$ ist, wobei die Inklusion $(\mathbb{F}_p^\times)^2 \subseteq A$ klar ist. Offenbar ist der Gruppenhomomorphismus $\mathbb{F}_p^\times \to (\mathbb{F}_p^\times)^2$, $x \mapsto x^2$ surjektiv mit genau zweielementigem Kern $\{-1, 1\}$. Also $\#(\mathbb{F}_p^\times)^2 = \frac{p-1}{2}$. Wegen 4.1.6(b) gilt andererseits $\#A \leq \frac{p-1}{2}$. Es folgt $A = (\mathbb{F}_p^\times)^2$ wie gewünscht.

(c) und (d) folgen leicht aus (b) mit Hilfe der trivialen Tatsache, dass zwei Elemente von $\{-1, 0, 1\} \subseteq \mathbb{Z}$ gleich sind, wenn sie modulo (p) kongruent sind.

(e) beweisen wir wieder mit (b) durch Rechnen im Ring $A := \mathbb{Z}[\overset{\circ}{i}]/(p)$, in den $\mathbb{F}_p$ kanonisch eingebettet ist. Wegen $p = 0$ in A gilt für alle $a, b \in A$

$$(*) \qquad (a+b)^p = a^p + b^p.$$

Bezeichne $i \in A$ die Kongruenzklasse von $\overset{\circ}{i} = \sqrt{-1}$ modulo (p). Man sieht leicht

$$(**) \qquad a + ib = 0 \iff (a = 0 \,\&\, b = 0)$$

für alle $a, b \in \mathbb{F}_p$. Nun rechnen wir

$$1 + i^p = 1^p + i^p \overset{(*)}{=} (1+i)^p = (1+i)((1+i)^2)^{\frac{p-1}{2}} = (1+i)(2i)^{\frac{p-1}{2}} = (1+i)i^{\frac{p-1}{2}}2^{\frac{p-1}{2}}.$$

Im Folgenden benutzen wir, dass wegen $i^4 = 1$ gilt $i^{\frac{k}{2}} = i^{\frac{\ell}{2}}$ für alle geraden $k, \ell \in \mathbb{Z}$ mit $k \equiv_{(8)} \ell$.

Fall 1: $p \equiv_{(8)} 1$
Dann $1 + i = (1+i)i^{\frac{1-1}{2}}2^{\frac{p-1}{2}} = (1+i)2^{\frac{p-1}{2}}$ und daher $2^{\frac{p-1}{2}} = 1$ in $\mathbb{F}_p$.

Fall 2: $p \equiv_{(8)} 3$
Dann $1 - i = 1 + i^3 = (1+i)i^{\frac{3-1}{2}}2^{\frac{p-1}{2}} = (i-1)2^{\frac{p-1}{2}}$ und daher $2^{\frac{p-1}{2}} = -1$ in $\mathbb{F}_p$.

Fall 3: $p \equiv_{(8)} 5$
Dann $1 + i = 1 + i^5 = (1+i)i^{\frac{5-1}{2}}2^{\frac{p-1}{2}} = (-1-i)2^{\frac{p-1}{2}}$ und daher $2^{\frac{p-1}{2}} = -1$ in $\mathbb{F}_p$.

Fall 4: $p \equiv_{(8)} 7$
Dann $1 - i = 1 + i^7 = (1+i)i^{\frac{7-1}{2}}2^{\frac{p-1}{2}} = (1-i)2^{\frac{p-1}{2}}$ und daher $2^{\frac{p-1}{2}} = 1$ in $\mathbb{F}_p$. □

Lemma 4.3.4. *Sei p eine ungerade Primzahl und K der p-te Kreisteilungskörper. Sei weiter q eine Primzahl ungleich p. Dann gilt:*

(a) *Der Verzweigungsindex $e_{q\mathbb{Z}}(\mathcal{O}_K)$ des Primideals $q\mathbb{Z}$ von $\mathbb{Z}$ in $\mathcal{O}_K$ [→ 2.7.6] ist 1.*

(b) *Der Trägheitsindex $f_{q\mathbb{Z}}(\mathcal{O}_K)$ des Primideals $q\mathbb{Z}$ von $\mathbb{Z}$ in $\mathcal{O}_K$ [→ 2.7.6] ist gleich der Ordnung von $\bar{q}$ in $\mathbb{F}_p^\times$.*

Beweis. Wähle eine primitive p-te Einheitswurzel ζ in $\mathbb{C}$ [→ 4.1.7].

(a) Es ist ζ natürlich ganz über $\mathbb{Z}$ und gemäß 4.1.13 ist $\Phi_p \in \mathbb{Z}[X]$ das Minimalpolynom von ζ über $\mathbb{Q}$. Nach Satz 3.2.2 ist zu zeigen, dass $\overline{\Phi_p}$ in $\mathbb{F}_q[X]$ ein Produkt von paarweisen verschiedenen normierten irreduziblen Polynomen ist. Dazu reicht es zu zeigen, dass $\overline{\Phi_p}$ separabel ist. Da Φ_p in $\mathbb{Z}[X]$ und damit $\overline{\Phi_p}$ in $\mathbb{F}_q[X]$ ein Teiler von $X^p - 1$ ist [→ 4.1.14], reicht es dann zu zeigen, dass $X^p - 1 \in \mathbb{F}_q[X]$ separabel ist. Wegen $q \nmid p$, folgt dies aber aus Proposition 4.1.8.

(b) Um $m := f_{q\mathbb{Z}}(\mathcal{O}_K)$ zu bestimmen, wählen wir ein Primideal $\mathfrak{q}$ von $\mathcal{O}_K$ mit $(q) \subseteq \mathfrak{q}$ [→ 2.7.5(b)]. Dann gilt $m = [(\mathcal{O}_K/\mathfrak{q}) : \mathbb{F}_q]$ nach 2.7.6 und 2.7.5(a). Da m endlich ist oder auch wegen 3.2.1, ist $\mathcal{O}_K/\mathfrak{q}$ ein endlicher Körper. Es gilt also $\mathcal{O}_K/\mathfrak{q} = \mathbb{F}_{q^m}$. Wegen Satz 4.2.2 gilt andererseits $\mathcal{O}_K/\mathfrak{q} = \mathbb{F}_q[\overline{\zeta}]$. Also $\mathbb{F}_{q^m} = \mathbb{F}_q[\overline{\zeta}]$.

Hilfsbehauptung: $\overline{\zeta}$ ist ein Element von $(\mathcal{O}_K/\mathfrak{q})^\times$ der Ordnung p

Begründung: Wegen $\zeta^p = 1$ in $\mathcal{O}_K$ gilt $\overline{\zeta}^p = 1$ in $\mathcal{O}_K/\mathfrak{q}$. Daher teilt die Ordnung von $\overline{\zeta}$ in $(\mathcal{O}_K/\mathfrak{q})^\times$ die Primzahl p, ist also gleich 1 oder p. Wäre die Ordnung 1, dann

$\overline{\zeta} = 1$ in $\mathscr{O}_K/\mathfrak{q}$, das heißt $1 - \zeta \in \mathfrak{q}$ und daher erst recht $(1-\zeta)^{p-1} \in \mathfrak{q}$ und somit nach Lemma 4.2.1(c) auch $p \in \mathfrak{q}$, was wegen $q \in \mathfrak{q}$ und $p \neq q$ nicht möglich ist.

Der Frobenius-Automorphismus

$$\varphi\colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m},\ x \mapsto x^q$$

hat bekanntlich die Ordnung m in der Automorphismengruppe der Körpererweiterung $\mathbb{F}_{q^m}|\mathbb{F}_q$. Daher ist zu zeigen, dass für alle $k \in \mathbb{Z}$ gilt

$$\overline{q}^k = 1 \text{ in } \mathbb{F}_p^\times \iff \varphi^k = \mathrm{id}_{\mathbb{F}_{q^m}}.$$

Wegen $\mathbb{F}_{q^m} = \mathbb{F}_q[\overline{\zeta}]$ kann man das umschreiben zu

$$\overline{q}^k = 1 \text{ in } \mathbb{F}_p^\times \iff \overline{\zeta}^{q^k} = \overline{\zeta},$$

was sofort aus der Hilfsbehauptung folgt. □

Lemma 4.3.5. *Sei $p \in \mathbb{P}$ ungerade und K der p-te Kreisteilungskörper. Sei weiter q eine Primzahl ungleich p und E der eindeutig bestimmte Zwischenkörper von $K|\mathbb{Q}$ mit $[E:\mathbb{Q}] = 2$ [→ 4.2.3].*

(a) *Ist q in E zerlegt [→ 2.1.17, 3.2.4], so ist $\#Q$ gerade für $Q := \{\mathfrak{q} \in M_{\mathscr{O}_K} \mid \mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}\}$.*

(b) *Ist q in E träge [→ 2.1.17, 3.2.4], so ist $f_{q\mathbb{Z}}(\mathscr{O}_K)$ gerade.*

Beweis. (a) Wähle $\mathfrak{p}_1, \mathfrak{p}_2 \in M_{\mathscr{O}_E}$ mit $\mathfrak{p}_1 \neq \mathfrak{p}_2$ und $q\mathscr{O}_E = \mathfrak{p}_1\mathfrak{p}_2$. Setze

$$Q_i := \{\mathfrak{q} \in M_{\mathscr{O}_K} \mid \mathfrak{q} \cap \mathscr{O}_E = \mathfrak{p}_i\} \overset{2.7.5(a)}{=} \{\mathfrak{q} \in M_{\mathscr{O}_K} \mid \mathfrak{p}_i \subseteq \mathfrak{q}\}$$

für $i \in \{1,2\}$. Man zeigt dann leicht $Q = Q_1 \dot\cup Q_2$, so dass es reicht, $\#Q_1 = \#Q_2$ zu zeigen. Nach 2.7.5(b) ist dann weder Q_1 noch Q_2 leer. Wähle dementsprechend $\mathfrak{q}_1 \in Q_1$ und $\mathfrak{q}_2 \in Q_2$. Wegen $\mathfrak{q}_1, \mathfrak{q}_2 \in Q$, gibt es nach 2.7.6 einen Automorphismus φ der Körpererweiterung $K|\mathbb{Q}$ mit $\varphi(\mathfrak{q}_1) = \mathfrak{q}_2$. Wegen $\varphi(\mathscr{O}_E) = \mathscr{O}_E$ gilt dann $\varphi(\mathfrak{p}_1) = \mathfrak{p}_2$ und $\varphi(\mathfrak{q}) \in Q_2$ für alle $\mathfrak{q} \in Q_1$ sowie $\varphi^{-1}(\mathfrak{q}) \in Q_1$ für alle $\mathfrak{q} \in Q_2$.

(b) Sei q in E träge. Dann $[\mathscr{O}_E/q\mathscr{O}_E : \mathbb{Z}/q\mathbb{Z}] = 2$ und daher ist $f_{q\mathbb{Z}}(\mathscr{O}_K) = [\mathscr{O}_K/\mathfrak{r}\mathscr{O}_E : \mathscr{O}_E/q\mathscr{O}_E][\mathscr{O}_E/q\mathscr{O}_E : \mathbb{Z}/q\mathbb{Z}]$ gerade, wobei $\mathfrak{r} \in M_{\mathscr{O}_K}$ mit $\mathfrak{r} \cap E = q\mathscr{O}_E$ beliebig gewählt ist. □

Lemma 4.3.6. *Seien $p, q \in \mathbb{P}$ ungerade mit $p \neq q$ und setze $p^* := (-1)^{\frac{p-1}{2}} p$.*

(a) $(\frac{p^*}{q}) = 1 \implies (\frac{q}{p}) = 1$

(b) $\left((\frac{p^*}{q}) = -1 \,\&\, p \equiv_{(4)} 3\right) \implies (\frac{q}{p}) = -1$

Beweis. Bezeichne K den p-ten Kreisteilungskörper und $E := \mathbb{Q}(\sqrt{p^*})$ den eindeutig bestimmten Zwischenkörper von $K|\mathbb{Q}$ mit $[E : \mathbb{Q}] = 2$ [$\to$ 4.2.3]. Weiter setzen wir $Q := \{\mathfrak{q} \in M_{\mathcal{O}_K} \mid \mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}\}$ und benutzen die Gleichung

$$(*) \qquad f_{q\mathbb{Z}}(\mathcal{O}_K)\#Q = p - 1,$$

die aus Lemma 4.3.4 und aus $[K : \mathbb{Q}] = \varphi(p) = p - 1$ folgt.

(a) Gelte $(\frac{p^*}{q}) = 1$. Gemäß Fall 1.1.2 in 3.2.4 ist dann q zerlegt in E. Dann ist $\#Q$ gerade nach Lemma 4.3.5(a). Daher ist $f_{q\mathbb{Z}}(\mathcal{O}_K)$ wegen $(*)$ ein Teiler von $\frac{p-1}{2}$ und nach Lemma 4.3.4(b) daher $q^{\frac{p-1}{2}} \equiv_{(p)} 1$. Aus Legendres Charakterisierung 4.3.3(b) folgt daher $(\frac{q}{p}) = 1$.

(b) Gelte $(\frac{p^*}{q}) = -1$ und $p \equiv_{(4)} 3$. Gemäß Fall 1.2 in 3.2.4 ist dann q träge in E. Dann ist $f_{q\mathbb{Z}}(\mathcal{O}_K)$ gerade nach Lemma 4.3.5(b). Nach Lemma 4.3.4(b) ist damit die Ordnung von $\bar{q}$ in $\mathbb{F}_p^\times$ gerade. Wegen $p \equiv_{(4)} 3$ ist $\frac{p-1}{2}$ ungerade und daher $\bar{q}^{\frac{p-1}{2}} \neq 1$ in $\mathbb{F}_p^\times$. Aus Legendres Charakterisierung 4.3.3(b) folgt dann $(\frac{q}{p}) = -1$. □

Satz 4.3.7 (Quadratisches Reziprozitätsgesetz)**.** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{falls } p \equiv_{(4)} q \equiv_{(4)} 3, \\ 1 & \text{sonst.} \end{cases}$$

Beweis. Setze $p^* := (-1)^{\frac{p-1}{2}} p$ und $q^* := (-1)^{\frac{q-1}{2}} q$. Ist $p \equiv_{(4)} q \equiv_{(4)} 1$, so gilt $p = p^*$ sowie $q = q^*$ und die Behauptung des Satzes folgt durch zweimalige Anwendung von Lemma 4.3.6(a). Da die Aussage des Satzes symmetrisch in p und q ist, können wir also im folgenden Œ

$$p \equiv_{(4)} 3$$

voraussetzen. Aus Lemma 4.3.6 folgt daher $(\frac{p^*}{q}) = (\frac{q}{p})$. Es folgt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \overset{4.3.3(c)}{=} \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p^*}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right).$$

Wegen $p \equiv_{(4)} 3$ ist $\frac{p-1}{2}$ ungerade und daher

$$\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = \left(\frac{-1}{q}\right) \overset{4.3.3(d)}{=} \begin{cases} 1 & \text{falls } q \equiv_{(4)} 1 \\ -1 & \text{falls } q \equiv_{(4)} 3 \end{cases}$$

wie behauptet. □

Beispiel 4.3.8. 221 ein quadratischer Nichtrest modulo der Primzahl 383 [$\to$ 4.3.1]. Um dies zu zeigen, berechnen wir zunächst die Primfaktorzerlegung $221 = 13 \cdot 17$ von 221

und benutzen dann das quadratische Reziprozitätsgesetz flankiert von 4.3.3(a)(c)(d)(e):

$$\left(\frac{221}{383}\right) = \left(\frac{13}{383}\right)\left(\frac{17}{383}\right) = \left(\frac{383}{13}\right)\left(\frac{383}{17}\right) = \left(\frac{6}{13}\right)\left(\frac{9}{17}\right)$$
$$= \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -\left(\frac{3}{13}\right) = -\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$