KREISTEILUNGSKÖRPER

QUIRIN REDING

In diesem Abschnitt befassen wir uns mit dem n-ten Kreisteilungskörper $\mathbb{Q}(\zeta)$. Dabei bezeichnet ζ eine primitive n-te Einheitswurzel, das heisst $\zeta^n = 1$ und $\zeta^k \neq 1$ für alle $1 \leqslant k < n$. Die Körpererweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ ist galoissch von Grad $\varphi(n)$, wobei wir mit φ die Eulersche Phi-Funktion bezeichnen.

1. Ganze Zahlen

Die ganzen Zahlen in $\mathbb{Q}(\zeta)$ sind $\mathbb{Z}[\zeta]$. Um das zu zeigen, beweisen wir den folgende Satz.

Satz 1. *$1, \zeta, \ldots, \zeta^{d-1}$ mit $d = \varphi(n)$ ist eine Ganzheitsbasis für den Ring $\mathcal{O}$ der ganzen Zahlen von $\mathbb{Q}(\zeta)$, d.h.*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{d-1} = \mathbb{Z}[\zeta]$$

Für den Beweis benötigen wir das folgende Lemma.

Lemma 2. *Sei $n = q^\nu$ eine Primzahlpotenz und $\lambda = 1 - \zeta$. Dann ist das Hauptideal $(\lambda) \subseteq \mathcal{O}$ ein Primideal vom Grad 1 und für $d = \varphi(n)$ ist*

$$q\mathcal{O} = (\lambda)^d.$$

Ferner hat die Basis $1, \zeta, \ldots, \zeta^{d-1}$ von $\mathbb{Q}(\zeta)|\mathbb{Q}$ die Diskriminante

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \pm q^s,$$

mit $s = q^{\nu-1}(\nu q - \nu - 1)$.

Beweis. Das Minimalpolynom von ζ ist das n-te Kreisteilungspolynom

$$\phi_n(X) = \prod_{\substack{1 \leqslant k \leqslant n \\ (k,n)=1}} (X - \zeta^k) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^k) = (X^{q^\nu} - 1)/(X^{q^{\nu-1}} - 1)$$

$$= X^{q^{\nu-1}(q-1)} + \cdots + X^{q^{\nu-1}} + 1.$$

Also ist ζ ganz in $\mathbb{Q}(\zeta)$ und so auch

$$\varepsilon_k \coloneqq 1 + \zeta + \cdots + \zeta^{k-1} = \frac{1 - \zeta^k}{1 - \zeta}.$$

Mit $X = 1$ erhalten wir aus den obigen Gleichungen

$$q = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (1 - \zeta^k) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \varepsilon_k (1 - \zeta). \tag{1.1}$$

Da $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ invertierbar ist, gibt es ein $k' \in \mathbb{Z}$, so dass $k'k \equiv 1 \bmod n$. Somit ist

$$\frac{1 - \zeta}{1 - \zeta^k} = \frac{1 - (\zeta^k)^{k'}}{1 - \zeta^k} = 1 + \zeta^k + \cdots + (\zeta^k)^{k'-1} \in \mathcal{O}.$$

Das heisst ε_k ist eine Einheit in $\mathcal{O}$, also auch $\varepsilon \coloneqq \prod_k \varepsilon_k$. Es folgt, dass $q = \varepsilon(1 - \zeta)^d$ und somit auch $q\mathcal{O} = (\lambda)^d$. Wegen der fundamentalen Gleichung $\sum_i e_i f_i = d$ der Primidealzerlegung muss (λ) ein Primideal vom Grad 1 sein.

Für die Bestimmung der Diskriminanten verwenden wir, dass

$$\pm d(1, \zeta, \ldots, \zeta^{d-1}) = \prod_{i \neq j} (\zeta_i - \zeta_j) = \prod_{i=1}^{d} \phi_n'(\zeta_i),$$

wobei $\zeta_1, \ldots, \zeta_d$ die Konjugierten von ζ unter der Wirkung der Galois-Gruppe bezeichnen.

Nach [3, Satz 2.6] ist ferner

$$\prod_{i=1}^{d} \phi_n'(\zeta_i) = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\phi_n'(\zeta)).$$

Aus der Identität $(X^{q^{\nu-1}} - 1)\phi_n(X) = (X^{q^\nu} - 1)$ für das n-te Kreisteilungspolynom ϕ_n erhalten wir durch differenzieren nach X und Auswertung bei $X = \zeta$, dass

$$\begin{aligned} q^{\nu-1}X^{q^{\nu-1}-1}\phi_n(X) + (X^{q^{\nu-1}} - 1)\phi_n'(X) &= q^\nu X^{q^\nu - 1} \\ 0 + (\zeta^{q^{\nu-1}} - 1)\phi_n'(\zeta) &= q^\nu \zeta^{q^\nu-1} = q^\nu \zeta^{-1}. \end{aligned}$$

Mit der primitiven q-ten Einheitswurzel $\xi := \zeta^{q^{\nu-1}}$ haben wir also

$$(\xi - 1)\phi_n'(\zeta) = q^\nu \zeta^{-1}.$$

Da q prim ist folgt nach [3, Satz 2.6], dass

$$N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi - 1) = \prod_{1 \leqslant k < q} (\xi^k - 1) = \pm\phi_q(1) = \pm q.$$

Es ist also

$$N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\xi - 1) = N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi - 1)^{q^{\nu-1}} = \pm q^{q^{\nu-1}}.$$

Wir folgern mit der Kenntnis, dass ζ^{-1} Norm ± 1 und $q^\nu = n$ Norm $n^{\varphi(n)}$ hat,

$$\pm d(1, \zeta, \ldots, \zeta^{d-1}) = \pm (q^\nu)^{q^{\nu-1}(q-1)} q^{-q^{\nu-1}} = \pm q^s$$

mit $s = q^{\nu-1}(\nu q - \nu - 1)$. □

Nun können wir Satz 1 beweisen.

Beweis von Satz 1. Wir nehmen zuerst an $n = q^\nu$ sei eine Primzahlpotenz. Wie in einem Lemma im Abschnitt über Dedeking Ringe gesehen gilt für die Diskriminante $d(1, \zeta, \ldots, \zeta^{d-1}) = \pm q^s$

$$q^s\mathcal{O} \subseteq \mathbb{Z} + \zeta\mathbb{Z} + \cdots + \zeta^{d-1}\mathbb{Z} = \mathbb{Z}[\zeta] \subseteq \mathcal{O}, \tag{1.2}$$

wobei wir verwendet haben, dass das Minimalpolynom ϕ_n von ζ Grad d hat und $\zeta \in \mathcal{O}$.

Da λ wegen Lemma 2 ein Primideal von Grad 1 mit $q\mathcal{O} = (\lambda)^d$ ist, gilt $\mathcal{O}/\lambda\mathcal{O} \cong \mathbb{Z}/q\mathbb{Z}$. Somit ist $\mathcal{O} = \mathbb{Z}/q\mathbb{Z} + \lambda\mathcal{O}$ und wegen $\mathbb{Z}/q\mathbb{Z} \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}$, ist auch $\mathcal{O} = \mathbb{Z}[\zeta] + \lambda\mathcal{O}$. Mulitplikation mit λ und einsetzen in die ursprüngliche Gleichung liefert $\mathcal{O} = \mathbb{Z}[\zeta] + \lambda\mathbb{Z}[\zeta] + \lambda^2\mathcal{O} = \mathbb{Z}[\zeta] + \lambda^2\mathcal{O}$. Induktiv erhalten wir also $\forall t \geqslant 1$:

$$\mathcal{O} = \mathbb{Z}[\zeta] + \lambda^t\mathcal{O}.$$

Also erhalten wir unter Verwendung von 1.2 und $(\lambda)^d = q\mathcal{O}$ aus Lemma 2

$$\mathcal{O} = \mathbb{Z}[\zeta] + \lambda^{ds}\mathcal{O} = \mathbb{Z}[\zeta] + (q\mathcal{O})^s\mathcal{O} = \mathbb{Z}[\zeta] + q^s\mathcal{O} = \mathbb{Z}[\zeta].$$

Im allgemeinen Fall sei $n = q_1^{\nu_1} \cdots q_r^{\nu_r}$ die Primfaktorzerlegung von n in $\mathbb{Z}$. Dann haben wir die Zerlegung

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1) \cdots \mathbb{Q}(\zeta_r),$$

mit den primitiven $q_i^{\nu_i}$-ten Einheitswurzeln $\zeta_i := \zeta^{n/q_i^{\nu_i}}$. Sei $d_i := \varphi(q_i^{\nu_i})$, dann ist nach vorheriger Betrachtung jeweils $1, \zeta_i, \ldots, \zeta_i^{d_i-1}$ eine Ganzheitsbasis von $\mathbb{Q}(\zeta_i)|\mathbb{Q}$ mit Diskriminante $q_i^{s_i}$. Da diese Diskriminanten zueinander paarweise teilerfremd sind und $\mathbb{Q}(\zeta_1)\cdots\mathbb{Q}(\zeta_{i-1}) \cap \mathbb{Q}(\zeta_i) = \mathbb{Q}$ für alle $1 < i \leqslant r$ gilt, ist nach [3, Satz 2.11] die Menge $\{\zeta_1^{j_1} \cdots \zeta_r^{j_r} : 0 \leqslant j_i \leqslant d_i - 1\}$ eine Ganzheitsbasis von $\mathbb{Q}(\zeta)|\mathbb{Q}$. Da diese Basiselemente alle Potenzen von ζ sind, gibt es für jedes $\alpha \in \mathcal{O}$ ein Polynom $f \in \mathbb{Z}[X]$, so dass $f(\zeta) = \alpha$. Mithilfe von $\zeta^d = 1$ können wir f vom Grad $\leqslant d - 1$ wählen und erhalten somit eine Darstellung der Form $\alpha = a_0 + a_1\zeta + \cdots + a_{d-1}\zeta^{d-1}$, womit $1, \zeta, \ldots, \zeta^{d-1}$ auch eine Ganzheitsbasis ist. □

2. Primidealzerlegung

Im Kreisteilungskörper $\mathbb{Q}(\zeta)$ können wir die Zerlegung in Primideale explizit angeben.

Satz 3. *Sei $n = \prod_p p^{\nu_p}$ die Primzerlegung von n und ζ eine primitive n-te Einheitswurzel. Ferner sei $f_p \in \mathbb{Z}$ für jede Primzahl p die kleinste postive ganze Zahl mit $p^{f_p} \equiv 1 \mod n/p^{\nu_p}$.*

Dann zerlegt sich p über $\mathbb{Q}(\zeta)$ in

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{\nu_p})},$$

wobei die $\mathfrak{p}_i$ verschiedene Primideale vom Grad f_p sind.

Beweis. Der Führer von $\mathbb{Z}[\zeta]$ ist 1, da $\mathbb{Z}[\zeta]$ der Ring der ganzen Zahlen von $\mathbb{Q}(\zeta)$ ist. Also können wir für p prim Satz 8.3 aus [3] anwenden. Folglich zerfällt p in $\mathbb{Q}(\zeta)$ auf gleiche Weise in Primideale wie das Minimalpolynom $\phi_n(X)$ von ζ in irreduzible Faktoren mod p. Es genügt also zu zeigen, dass

$$\phi_n(X) \equiv \big(p_1(X) \cdots p_r(X)\big)^{\varphi(p^{\nu_p})} \mod p$$

mit verschiedenen irreduziblen Polynomen $p_1(X), \ldots, p_r(X)$ über $\mathbb{Z}/p\mathbb{Z}$ vom Grad f_p.

Wir schreiben $m \coloneqq n/p^{\nu_p}$ und definieren ξ_i und η_j als die primitiven m-ten bzw. p^{ν_p}-ten Einheitswurzeln. Entsprechend sind die Produkte $\xi_i\eta_j$ genau die primitiven n-ten Einheitswurzeln. Also ist

$$\phi_n(X) = \prod_{i,j}(X - \xi_i\eta_j),$$

wobei die Indizes i und j über die entsprechenden Einheitengruppen $(\mathbb{Z}/m\mathbb{Z})^\times$ bzw. $(\mathbb{Z}/p^{\nu_p}\mathbb{Z})^\times$ laufen. Nun ist für jedes Primideal $\mathfrak{p} \supseteq (p)$ jedoch $\eta_j \equiv 1 \mod \mathfrak{p}$, da $X^{p^{\nu_p}} - 1 \equiv (X-1)^{p^{\nu_p}} \mod p$. Folglich haben wir

$$\phi_n(X) \equiv \prod_i (X - \xi_i)^{\varphi(p^{\nu_p})} = \phi_m(X)^{\varphi(p^{\nu_p})} \mod \mathfrak{p}.$$

Da die Kreisteilungspolynome $\phi_n(X)$ und $\phi_m(X)$ Koeffizienten in $\mathbb{Z}$ haben, folgt auch, dass

$$\phi_n(X) \equiv \phi_m(X)^{\varphi(p^{\nu_p})} \mod p.$$

Ferner ist $\mathbb{Z}[\zeta]/\mathfrak{p}$ eine endliche Körpererweiterung von $\mathbb{F}_p$, also von der Form $\mathbb{F}_{p^f}$ für ein $f \geqslant 1$. Nun haben wegen $(m,p) = 1$ die Polynome $X^m - 1$ und mX^{m-1} keine gemeinsamen Nullstellen mod $\mathfrak{p}$. Deshalb haben sowohl $X^m - 1$ als auch $\phi_m(X)$ keine mehrfachen Nullstellen mod $\mathfrak{p}$. Folglich ist das Bild $\bar{\zeta}_m$ der primitiven m-ten Einheitswurzel ζ_m unter der Abbildung $\mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/\mathfrak{p}$ wiederum eine primitive m-te Einheitswurzel. Deshalb teilt die Ordung m vom $\bar{\zeta}_m$ die Kardinalität der Einheitengruppe $\mathbb{F}_{p^f}^\times = \mathbb{F}_{p^f} - \{0\}$. Das heisst $p^f \equiv 1 \mod m$. Also ist $f \geqslant f_p$.

Da nun aber auch die Bilder $\bar{\zeta}_m^i \in \mathbb{Z}[\zeta]/\mathfrak{p}$ primitive m-te Einheitswurzeln sind für alle $1 \leqslant i < m$ mit $(i,m) = 1$, zerfällt das Bild $\bar{\phi}_m(X)$ des Kreisteilungspolynoms $\phi_m(X)$ in $\mathbb{Z}[\zeta]/\mathfrak{p} = \mathbb{F}_{p^{f_p}}$ in Linearfaktoren. Seien nun $P_i(X)$ die irreduziblen Faktoren von $\phi_m(X)$ mod p. Dann hat jedes $P_i(X)$ mindestens Grad f mit $p^f \equiv 1 \mod m$ und maximal Grad f_p, da $\bar{\phi}_m(X)$ in $\mathbb{F}_{p^{f_p}}$ in Linearfaktoren zerfällt. Somit ist $f = f_p$. □

3. Grosser Fermatscher Satz für reguläre Primzahlen

Als Anwendung der Kreisteilungskörper betrachten wir den grossen Fermatschen Satz:

Satz 4. *Die Gleichung $x^n + y^n = z^n$ hat für jede natürliche Zahl $n > 2$ keine positiven ganzzahligen Lösungen $(x,y,z) \in \mathbb{Z}^3_{>0}$.*

Und zwar betrachten wir den Fall, dass $n = p \geqslant 5$ eine Primzahl ist. Wir argumentieren per Widerspruch, sei also (x,y,z) eine positive ganzzahlige Lösung. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass x, y, z paarweise teilerfremd sind. Wir nehmen zudem an dass p keine der Zahlen x, y, z teilt. (Der andere Fall, nämlich dass p genau eine der Zahlen x, y, z teilt, ist etwas aufwendiger.)

Wir faktorisieren nun die Summe $x^p + y^p$ in $\mathbb{Q}(\zeta)$ mit ζ einer primitiven p-ten Einheitswurzel. Es gilt

$$t^p - 1 = \prod_{0 \leqslant k < p} (t - \zeta^k)$$

und somit

$$\begin{aligned}(-x/y)^p - 1 &= \prod_{0\leqslant k<p} (-x/y - \zeta^k)\\ x^p + y^p &= \prod_{0\leqslant k<p} (x + y\zeta^k).\end{aligned}$$

Die Gleichung $x^p + y^p = z^p$ führt also zur folgenden Hauptidealgleichung in $\mathbb{Z}[\zeta]$

$$(x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}) = (z)^p. \tag{3.1}$$

Wir zeigen nun mithilfe der Primidealzerlegung in $\mathbb{Z}[\zeta]$, dass das Hauptideal $(x+y\zeta)$ keine gemeinsamen Primidealfaktoren mit den den anderen Hauptidealen auf der linken Seite von Gleichung 3.1 hat. Angenommen dies sei nicht der Fall. Dann gibt es ein Primideal π mit $\pi \supseteq (x + y\zeta)$ und $\pi \supseteq (x + y\zeta^k)$ für ein $k \not\equiv 1 \bmod p$. Folglich

$$\begin{aligned}\pi &\supseteq (x + y\zeta^k) - (x + y\zeta)\\ \pi &\supseteq \big(y\zeta(\zeta^{k-1} - 1\big) = \big(y(\zeta^{k-1} - 1)\big),\end{aligned}$$

wobei wir im letzten Schritt verwendet haben, dass ζ eine Einheit in $\mathbb{Z}[\zeta]$ ist. Analog zu Gleichung 1.1 erhalten wir die Hauptidealgleichung $(p) = (1-\zeta)\cdots(1-\zeta^{p-1})$. Somit folgt, dass $\pi \supseteq (yp)$. Zudem folgt direkt aus Gleichung 3.1, dass $\pi \supseteq (z)^p$ und da π prim ist, muss folglich auch $\pi \supseteq (z)$ gelten. Da aber p, y und z paarweise teilerfremd sind, ist $\pi \supseteq (z) + (yp) = \mathbb{Z}[\zeta]$ im Widerspruch zur Annahme, dass π prim ist. Dies zeigt die Behauptung.

Somit ist der Verzweigungsindex jedes Primidealfaktors von $(x+y\zeta)$ durch p teilbar. Folglich ist $(x + y\zeta) = I^p$ die p-te Potenz eines Ideals I. Wir nehmen nun im folgenden an p sei eine reguläre Primzahl um zu zeigen, dass I ein Hauptideal ist.

Definition 5. *Eine Primzahl $p \in \mathbb{Z}$ heisst* regulär *falls p die Kardinalität der Klassengruppe von $\mathbb{Q}(\zeta)$ nicht teilt. (ζ ist eine primitive p-te Einheitswurzel)*

Wenn also p regulär ist, so gibt es keine Elemente der Ordnung p in der Klassengruppe von $\mathbb{Q}(\zeta)$. Sei C die Klasse in der das Ideal I liegt. Dann ist wegen $I^p \in C^p$ die Klasse C^p das triviale Element der Klassengruppe, da $I^p = (x + y\zeta)$ ein Hauptideal ist. Somit ist die Ordnung von C ein Teiler von p und folglich 1. Somit ist C bereits trivial in der Klassengruppe, d.h. I ist ein Hauptideal.

Wir können also schreiben $x + y\zeta = u\alpha^p$ für ein $\alpha \in \mathbb{Z}[\zeta]$. Unter Verwendung von $(\beta+\gamma)^p \equiv \beta^p + \gamma^p \bmod p$ für alle $\beta, \gamma \in \mathbb{Z}[\zeta]$ ist

$$\alpha^p = \Big(\sum_{i=0}^{p-1} a_i\zeta^i\Big)^p \equiv \sum_{i=0}^{p-1} a_i^p\zeta^{ip} \in \mathbb{Z}.$$

Nun verwenden wir, dass für jede Einheit $u \in \mathbb{Z}[\zeta]$ der Quotient $u/\bar{u}$ eine p-te Einheitswurzel ist. Es ist folglich

$$x + y\zeta = u\alpha^p \equiv (u/\bar{u})\overline{u\alpha^p} = \zeta^k(x + y\zeta^{-1}).$$

Wir behaupten, dass $k \equiv 1 \bmod p$. Denn andernfalls folgt aus

$$\begin{aligned}p &\mid \zeta^k(x + y\zeta^{-1}) - (x + y\zeta)\\ p &\mid x(\zeta^k - 1) + y(\zeta^{k-1} - \zeta)\\ p &\mid -x - y\zeta + x\zeta^k + y\zeta^{k-1},\end{aligned}$$

dass p auch x oder y teilt, (da $1, \zeta, \ldots, \zeta^{p-2}$ eine Ganzheitsbasis ist) im Widerspruch zur ursprünglichen Annahme.

Für $k \equiv 1$ erhalten wir nun $x + y\zeta \equiv x\zeta + y$, also $x \equiv y \bmod p$. Wegen p ungerade gilt aber auch $x^p + (-z)^p = (-y)^p$ und folglich $x \equiv -z \bmod p$. Zusammen erhalten wir

$$\begin{aligned}2x^p &\equiv x^p + y^p = z^p \equiv -x^p\\ &\Rightarrow p \mid 3x^p\\ &\Rightarrow p \mid x,\end{aligned}$$

im Widerspruch zur ursprünglichen Annahme. Somit haben wir gezeigt, dass es keine positiv ganzzahligen Lösungen zur Gleichung $x^p + y^p = z^p$ gibt für $p \geqslant 5$ eine reguläre Primzahl mit $p \nmid xyz$.

4. Eine weitere Anwendung

Zu guter Letzt beweisen wir noch folgende Aussage über quadratische Zahlkörper.

Satz 6. *Für jede ungerade Primzahl p mit $p^\star = (-1)^{\frac{p-1}{2}} p$ ist $\mathbb{Q}(\sqrt{p^\star}) \subseteq \mathbb{Q}(\zeta)$. Wobei ζ eine primitive p-te Einheitswurzel bezeichnet.*

Beweis. Nach dem Eulerschen Kriterium ist $p^\star = \left(\frac{-1}{p}\right)p$. Sei ferner

$$\tau \coloneqq \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a.$$

Wir zeigen nun, dass $p^\star = \tau^2$. Wir berechnen wie folgt, wobei die Summierungsindizes a, b, c jeweils über die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ laufen.

$$\begin{aligned}
\left(\frac{-1}{p}\right)\tau^2 &= \left(\frac{-1}{p}\right)\left(\sum_a \left(\frac{a}{p}\right)\zeta^a\right)\left(\sum_b \left(\frac{b}{p}\right)\zeta^b\right) \\
&= \sum_{a,b}\left(\frac{a}{p}\right)\left(\frac{-b}{p}\right)\zeta^{a+b} = \sum_{a,b'}\left(\frac{a}{p}\right)\left(\frac{b'}{p}\right)\zeta^{a-b'}
\end{aligned}$$

Wobei wir im letzten Schritt $b' \coloneqq -b$ substituiert haben. Weiter gilt $\left(\frac{b}{q}\right) = \left(\frac{b^{-1}}{q}\right)$ nach dem Eulerschen Kriterium. Somit ist

$$\begin{aligned}
\left(\frac{-1}{p}\right)\tau^2 &= \sum_{a,b}\left(\frac{a}{p}\right)\left(\frac{b^{-1}}{p}\right)\zeta^{a-b} = \sum_{a,b}\left(\frac{ab^{-1}}{p}\right)\zeta^{a-b} \\
&= \sum_{b,c}\left(\frac{c}{p}\right)\zeta^{bc-b}, \text{ mit } c \coloneqq ab^{-1} \\
&= \sum_{c}\left(\frac{c}{p}\right)\sum_b \zeta^{b(c-1)} \\
&= \sum_{c\neq 1}\left(\frac{c}{p}\right)\sum_b \xi^b + \left(\frac{1}{p}\right)\sum_b 1, \text{ mit } \xi \coloneqq \zeta^{c-1} \\
&= \sum_{c\neq 1}\left(\frac{c}{p}\right)(-1) + p - 1.
\end{aligned}$$

Ferner ist $\sum_c \left(\frac{c}{p}\right) = 0$, da für $\left(\frac{x}{p}\right) = -1$

$$-\sum_c \left(\frac{c}{p}\right) = \left(\frac{x}{p}\right)\sum_c\left(\frac{c}{p}\right) = \sum_c \left(\frac{xc}{p}\right) = \sum_{c'}\left(\frac{c'}{p}\right),$$

mit der Substitution $c' \coloneqq xc$ in der Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$.

Somit haben wir

$$\left(\frac{-1}{p}\right)\tau^2 = -\left(\frac{1}{p}\right)(-1) + p - 1 = p.$$

Es folgt, dass

$$\tau^2 = \left(\frac{-1}{p}\right)\left(\frac{-1}{p}\right)\tau^2 = \left(\frac{-1}{p}\right)p = p^\star.$$

□

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969

[2] S. Müller–Stach and J. Piontkowski, *Elementare und algebraische Zahlentheorie*. Second edition. Vieweg + Teubner, Wiesbaden, 2011

[3] J. Neukirch, *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992

[4] A. Schmidt, *Einführung in die algebraische Zahlentheorie*. Springer, Berlin, 2007

[5] U. Zannier, *Lecture notes on Diophantine analysis*. Edizioni della Normale, Pisa, 2009

Email address: `quirin.reding@math.ethz.ch`