Kreisteilungskörper und die Erzeugung ihrer Teilkörper

Bachelorarbeit

Anne Wald

27. Juli 2009

Erklärung

Hiermit versichere ich, die Arbeit eigenständig und nur unter Verwendung der angegebenen Hilfsmittel durchgeführt zu haben.

Saarbrücken, der 27. Juli 2009

Anne Wald

Inhaltsverzeichnis

Vorwort

Die vorliegende Arbeit mit dem Titel „Kreisteilungskörper und die Erzeugung ihrer Teilkörper“ zur Erlangung des Bachelorabschlusses in Mathematik ist in der Zeit vom 26. Mai 2009 bis zum 31. Juli 2009 am Lehrstuhl von Prof. Ernst-Ulrich Gekeler entstanden.
In dieser Zeit habe ich mich mit Kreisteilungskörpern, genauer gesagt mit deren Unterkörpern, beschäftigt und einige Eigenschaften dieser Unterkörper zusammen gestellt.
Ein Kreisteilungskörper $K_n = \mathbb{Q}(\zeta_n)$, kurz Kreiskörper, ist eine Erweiterung des Körpers der rationalen Zahlen $\mathbb{Q}$, der durch Adjunktion einer n-ten Einheitswurzel entsteht. Diese Erweiterung ist galoissch mit abelscher Galoisgruppe. Die Zahl n ist eine natürliche Zahl und wird *Führer* genannt.
In verschiedenen Situationen kann es hilfreich rein, den Erzeuger eines Körpers K zu kennen, der zwischen K_n und $\mathbb{Q}$ liegt. Alle algebraischen Zahlkörper L, zu denen auch die Kreisteilungskörper und ihre Teilkörper K gehören, werden von einem bestimmten Element des jeweiligen Körpers erzeugt. Dieser Erzeuger soll nun für die Teilkörper eines beliebigen Kreiskörpers gefunden werden.

$$\begin{array}{c} K_n = \mathbb{Q}(\zeta_n) \\ | \\ K = \mathbb{Q}(?) \\ | \\ \mathbb{Q} \end{array}$$

Es ist bekannt, dass bei Kreisteilungserweiterungen die Koeffizienten des Minimalpolynoms der Einheitswurzel ζ_n in dem betrachteten Unterkörper K von K_n ein Erzeugendensystem des Körpers K bilden. Daher kommen diese Koeffizienten auch jeder für sich alleine als Erzeuger in Betracht.
Ein Minimalpolynom eines Elementes α aus K_n in K ist ein normiertes Polynom mit minimalem Grad und Koeffizienten aus K, das α als Nullstelle hat. Einer dieser Koeffizienten ist die Spur von α in K, genannt λ_K. Ich betrachte ausschließlich $\alpha = \zeta_n$.
In meiner Arbeit habe ich untersucht, ob die Spur als Erzeuger von K infrage kommt und welche Bedingungen gegeben sein müssen, damit sie K erzeugt. Die verschiedenen Ergebnisse sind in Kapitel 3 zu finden und werden nach Beschaffenheit von n geordnet.
Im nächsten Schritt stellt man sich die Frage, wann λ_K nicht nur den Körper K, sondern auch den Ganzheitsring von K erzeugt. Der Ganzheitsring besteht aus allen Elementen von K, die ganz über $\mathbb{Q}$ sind. Die Ergebnisse sind in Kapitel 4 aufgeschrieben.
Auch das Minimalpolynom von λ_K in $\mathbb{Q}$ und insbesondere seine Koeffizienten werden betrachtet. Hier konnten einige Aussagen getroffen werden für den Fall, dass n eine Primzahl ist, wie man in Kapitel 5 nachlesen kann.

Beginnen werde ich jedoch mit den für das Verständnis benötigten Aussagen. Anschliessend möchte ich eine Beschreibung der Situation geben, die für die ganze Arbeit gültig ist.

Die Arbeit richtet sich an Leser, die bereits einige Vorkenntnisse auf dem Gebiet der Algebra und Zahlentheorie besitzen. Grundlegend sind einige Begriffe der Körpertheorie, der Galoistheorie sowie der algebraischen Zahlentheorie. Die wichtigsten Begriffe und Aussagen werden im Kapitel 1 zusammengestellt.

Die Berechnungen, die zu den in dieser Arbeit getroffenen Aussagen und Vermutungen führten, wurden mithilfe der Software *MAGMA Computational Algebra System* durchgeführt.

Saarbrücken, im Juli 2009 Anne Wald

1 Grundlagen

In diesem Kapitel sollen die Grundlagen behandelt werden, die zum Verständnis dieser Arbeit notwendig sind. Dazu gehören beispielsweise einige Aussagen der Körper- und der Galoistheorie sowie der algebraischen Zahlentheorie. Ein Leser, dem diese Dinge wohlbekannt sind, kann dieses Kapitel problemlos überspringen.
An verschiedenen Stellen dieser Arbeit wird auf die Aussagen dieses Kapitel verwiesen.

Die folgende Notation ist für die gesamte Arbeit gültig:

- $\mathbb{N} := \{1, 2, 3, ...\}$ ist die Menge der natürlichen Zahlen,
- $\mathbb{P}$ ist die Menge aller Primzahlen,
- p ist immer eine Primzahl.

1.1 Körpererweiterungen

1.1 Definition. *Sind K und L Körper mit $K \subset L$, so nennt man K einen Unterkörper von L beziehungsweise L einen Erweiterungskörper von K. Diese Körpererweiterung bezeichnet man mit $L|K$.*
L kann als K-Vektorraum aufgefasst werden. Man definiert den Grad der Körpererweiterung $[L : K]$ als Dimension des K-Vektorraums L.
Die Erweiterung $L|K$ heißt endlich, falls $[L : K]$ endlich ist.

Im ganzen Kapitel sei K der Grundkörper und L eine Erweiterung von K. Zwischenkörper einer solchen Erweiterung werden mit M bezeichnet.

1.2 Definition. *Ein Element $\alpha \in L$ heißt algebraisch über K, falls es Elemente $a_0, ..., a_n$, $n \in \mathbb{N}$, aus K gibt mit*

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0,$$

d.h. es gibt mindestens ein Polynom $g(X) = \sum_{1 \leq i \leq n} \alpha_i X^i \in K[X]$ mit $g(\alpha) = 0$.
Das Polynom $f_\alpha \in K[X]$, das die Eigenschaft $f_\alpha(\alpha) = 0$ erfüllt, minimalen Grad hat und normiert ist, heißt Minimalpolynom von α.
Eine Erweiterung $L|K$ heißt algebraisch, falls alle Elemente aus L algebraisch über K sind.

1.3 Proposition. *Ist $L|K$ endlich, so auch algebraisch (siehe [Lan84], Seite 161, Proposition 1).*

1.4 Bemerkung. Die Umkehrung von Proposition 1.3 gilt nicht.

1.5 Proposition. *Der Körpergrad ist multiplikativ. Es gilt*

$$[L : K] = [L : M] \cdot [M : K].$$

Ist $\{x_i\}_{i\in I}$ *eine Basis von* $M|K$ *und* $\{y_j\}_{j\in J}$ *eine Basis von* $L|M$*, so ist* $\{x_i y_j\}_{(i,j)\in I\times J}$ *eine Basis von* $L|K$ *([Lan84], Seite 162, Proposition 2).*

1.6 Definition. *Sei* $\alpha \in L$*. Dann bezeichnet man mit* $K(\alpha)$ *den kleinsten Körper, der* K *und* α *enthält. Es gilt ([Lan84], Seite 163, Proposition 3)*

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \ : \ f, g \in K[X],\ g(\alpha) \neq 0 \right\}$$

1.7 Proposition. *Seien* M_1, M_2 *Erweiterungen von* K *mit* $K \subset M_1, M_2 \subset L$*. Dann ist*

$$M_1 \cdot M_2 = \{ \sum_{1\leq i\leq n} m_{1,i} \cdot m_{2,i} \mid m_{1,i} \in M_1,\ m_{2,i} \in M_2\ \forall\ 1 \leq i \leq n\}.$$

$M_1 \cdot M_2$ *ist der kleinste Teilkörper von* L*, der* M_1 *und* M_2 *enthält und wird als Kompositum von* M_1 *und* M_2 *bezeichnet (siehe [Lan84], Seite 163).*

1.8 Bemerkung. Sei $L|K$ eine endliche Körpererweiterung. Dann gilt für $\alpha_1, ..., \alpha_n$ aus L

$$K(\alpha_1, ..., \alpha_n) = K(\alpha_1) \cdot ... \cdot K(\alpha_n).$$

1.2 Einige Auszüge aus der Galoistheorie

An dieser Stelle sollen einige Erläuterungen zur Galoistheorie gemacht werden. Dabei wird jedoch darauf verzichtet zu erklären, was man genau unter dem Begriff „galoissch“ versteht. Wie wir später sehen werden, ist die Eigenschaft „galoissch“ bei dem hier betrachteten Typ von Körpererweiterung immer gegeben. Leser dieser Arbeit, die trotzdem nicht auf eine Einführung in die Galoistheorie verzichten wollen, können diese beispielsweise in ([Lan84], Kapitel VII und VIII) nachlesen.

1.9 Definition. *Unter einem Körperautomorphismus versteht man eine bijektive Abbildung $\sigma : L \to L$ von einem Körper auf sich selbst mit den folgenden Eigenschaften: Für alle $\alpha, \beta \in L$ gilt*

$$\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta),$$
$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta).$$

Die Körperautomorphismen bilden eine Gruppe bezüglich Hintereinanderausführung. Dabei bilden die Automorphismen, die einen Körper $K \subset L$ festlassen, eine Untergruppe (siehe [Lan84], Kapitel VIII, §1, Seite 192-193).

1.10 Definition. *Die in Definition 1.9 eingeführte Untergruppe heißt Galoisgruppe der Körpererweiterung $L|K$. Sie wird bezeichnet mit $Gal(L|K)$.*

Wie bereits erwähnt, ist eine Körpererweiterung unter bestimmten Voraussetzungen galoissch. Ist dies für eine Körpererweiterung der Fall, so gilt der Hauptsatz der Galoistheorie:

1.11 Satz. *(Hauptsatz der Galoistheorie, siehe ([Lan84], Seite 192))*
Sei L eine endliche galoissche Erweiterung von K mit Galoisgruppe $G := Gal(L|K)$. Dann gibt es eine Bijektion zwischen der Menge der Teilkörper M mit $K \subset M \subset L$ und der Menge der Untergruppen H von G:

$$\begin{array}{ccc} \{\text{Teilkörper } M,\ K \subset M \subset L\} & \longleftrightarrow & \{\text{Untergruppen } H \subset G\} \\ M & \longrightarrow & Fix(M) \\ L^H & \longleftarrow & H \end{array}$$

mit

$$Fix(M) := \{\sigma \in G \mid \sigma(\alpha) = \alpha \ \forall\ \alpha \in M\},$$
$$L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall\ \sigma \in H\}.$$

L^H wird dabei als Fixkörper von L unter H und $Fix(M)$ als Fixgruppe von M bezeichnet.
Die Körpererweiterung $L|M$ ist ebenfalls galoissch und hat die Galoisgruppe H.
Des weiteren ist $M|K$ genau dann galoissch, wenn H normal in G ist, also wenn für alle $g \in G$ gilt: $gHg^{-1} = H$. Ist dies der Fall, so induziert die Abbildung $\sigma \mapsto \sigma|_M$ einen Isomorphismus von G/H nach $Gal(M|K)$.
Desweiteren gilt $\#(G) = [L : K]$.

1.3 Grundlegende Aussagen

Da in dieser Arbeit ausschließlich Kreisteilungserweiterungen betrachtet werden, also Körpererweiterungen, die von einer Einheitswurzel, die immer mit ζ_n bezeichnet wird, erzeugt werden, folgen nun einige Eigenschaften von Einheitswurzeln sowie von Kreisteilungserweiterungen.

1.12 Definition. *Allgemeines über Einheitswurzeln*
Sei $n \in \mathbb{N}$. Eine Zahl $\zeta_n \in \mathbb{C}$ heißt n-te Einheitswurzel, wenn gilt

$$\zeta_n{}^n = 1.$$

Gilt zusätzlich

$$\zeta_n{}^m \neq 1 \quad \forall m \in \mathbb{N} \text{ mit } 0 < m < n,$$

so bezeichnet man ζ_n als primitive Einheitswurzel.
Zu den Nullstellen des Polynoms $X^n - 1$ gehören unter anderem die primitiven n-ten Einheitswurzeln.

1.13 Satz. *Die Körpererweiterung $K_n|\mathbb{Q}$ mit $K_n := \mathbb{Q}(\zeta_n)$ ist galoissch nach ([Was97], Satz 2.5). Die zugehörige Galoisgruppe $G_n := Gal(K_n|\mathbb{Q})$ ist abelsch, also ist jede Untergruppe H von G_n normal in G_n.*
Ist $K_n|M|\mathbb{Q}$ eine Teilerweiterung, so ist daher nicht nur $K_n|M$ galoissch, sondern auch $M|\mathbb{Q}$.
Für die Galoisgruppe $G_n = Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ gilt nach ([Was97], Theorem 2.5)

$$G_n \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Die natürliche Zahl n wird *Führer* genannt.
Damit der Körper $\mathbb{Q}(\zeta_n)$ eindeutig durch eine primitive n-te Einheitswurzel erzeugt wird und nicht durch eine m-te Einheitswurzel ($m \neq n$), fordern wir noch, dass immer gilt

$$n \not\equiv 2 \bmod 4.$$

Es gilt genau dann $n \equiv 2 \bmod 4$, wenn man $n = 2m$ mit einer ungeraden natürlichen Zahl m schreiben kann.
Sei nun $n \equiv 2 \bmod 4$. Dann gilt

$$1 = \zeta_n^n = \zeta_n^{2m} = (\zeta_n^m)^2,$$

also ist ζ_n^m eine primitive zweite Einheitswurzel, also $\zeta_n^m = -1$. Es gilt jedoch

$$L := \mathbb{Q}(\zeta_n) = \mathbb{Q}(-\zeta_m) = \mathbb{Q}(\zeta_m),$$

also kann L in diesem Fall sowohl von einer n-ten als auch von einer m-ten Einheitswurzel erzeugt werden. Daher wird im folgenden der Fall $n \equiv 2 \bmod 4$ ausgeschlossen.

Ab jetzt gilt immer $n \not\equiv 2 \bmod 4$!

Für zwei Einheitswurzeln ζ_n und ζ_m mit $\mathrm{ggT}(n,m) = 1$ gilt

$$\zeta_{nm} = \zeta_n \cdot \zeta_m \tag{1}$$

(siehe beispielsweise [Lan84], Seite 204 und 205, Korollar mit Beweis).
Als Element der komplexen Zahlen $\mathbb{C}$ kann man eine n-te Einheitswurzel auch durch

$$\zeta_n = e^{j\frac{2\pi i}{n}}, \qquad 0 \leq j < n,$$

beschreiben.
ζ_n ist genau dann primitiv, wenn $\mathrm{ggT}(j,n) = 1$ gilt, also wenn j und n teilerfremd sind. Es gibt also $\varphi(n)$ verschiedene primitive Einheitswurzeln. Dabei ist φ die Eulersche Phi-Funktion:

1.14 Definition. *Die Abbildung*

$$\begin{array}{rccl} \varphi: & \mathbb{N} & \longrightarrow & \mathbb{N}, \\ & n & \longmapsto & \varphi(n) \quad = \quad \#\{a \in \{1,...,n\} \mid ggT(n,a) = 1\} \end{array}$$

heißt Eulersche Phi-Funktion. Sie ist schwach multiplikativ, d.h. für zwei teilerfremde natürliche Zahlen n und m gilt $\varphi(nm) = \varphi(n)\varphi(m)$.
Im Spezialfall $n = p^r$, $r \in \mathbb{N}$, $p \in \mathbb{P}$, gilt nach [SP07], Definition und Korollar 4.20,

$$\varphi(p^r) = (p-1)p^{r-1}. \tag{2}$$

So gilt beispielsweise $\#(G_n) = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ (siehe auch [Was97], Theorem 2.5).

1.15 Bemerkung. Betrachten wir nun noch einmal Satz 1.13. Es gilt $G_n \cong (\mathbb{Z}/n\mathbb{Z})^*$. Der kanonische Isomorphismus, der $(\mathbb{Z}/n\mathbb{Z})^*$ auf G_n abbildet, sieht folgendermaßen aus:

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \longleftrightarrow & G_n \\ i & \longmapsto & \sigma_i \end{array}$$

mit

$$\begin{array}{rccc} \sigma_i: & \mathbb{Q}(\zeta_n) & \longrightarrow & \mathbb{Q}(\zeta_n), \\ & \sum_{k=0}^{\varphi(n)-1} a_k \zeta_n{}^k & \longmapsto & \sum_{k=0}^{\varphi(n)-1} a_k \zeta_n{}^{ki}. \end{array}$$

Diese beiden Darstellungen von G_n werden in meiner Arbeit nicht weiter unterschieden. Ohne gesonderte Erwähnung wird in den meisten Fällen einfach $G_n = (\mathbb{Z}/n\mathbb{Z})^*$ geschrieben. Dies gilt auch für die Untergruppen H von G_n.

1.16 Definition. *Die Spur eines Elementes $\alpha \in K_n$ in einem Teilkörper $K \subset K_n$ ist definiert als Summe aller Bilder von α unter den Elementen der Galoisgruppe $H = Gal(K_n|K)$, also*

$$Tr_K^{K_n}(\alpha) := \sum_{\sigma \in H} \sigma(\alpha).$$

Sie ist also eine Abbildung $Tr : K_n \to K = K_n^H$.
Für $\alpha := \zeta_n$ nennen wir die Spur von ζ_n in K

$$\lambda_K := Tr_K^{K_n}(\zeta_n) = \sum_{\sigma \in H} \sigma(\zeta_n) = \sum_{i \in H} {\zeta_n}^i.$$

1.17 Bemerkung. Ist α bereits in K enthalten, so wird α von allen Elementen aus H festgelassen und es folgt

$$\begin{aligned} \mathrm{Tr}_K^{K_n}(\alpha) &= \sum_{\sigma \in H} \sigma(\alpha) \\ &= \sum_{\sigma \in H} \alpha \\ &= \#(H) \cdot \alpha \\ &= [K_n : K] \cdot \alpha. \end{aligned}$$

1.18 Satz. *Für die Spur einer n-ten Einheitswurzel ζ_n mit quadratfreiem $n \in \mathbb{N}$ in $\mathbb{Q}$ gilt*

$$Tr_{\mathbb{Q}}^{K_n}(\zeta_n) = (-1)^k.$$

Dabei ist $k \in \mathbb{N}$ die Anzahl der Primfaktoren von n.

Beweis. Betrachte zunächst $n = p \in \mathbb{P} - \{2\}$.
Sei

$$f_p(X) = \sum_{i=0}^{p-1} \alpha_i X^i$$

das Minimalpolynom. Dann gilt

$$\alpha_{p-2} = -\mathrm{Tr}_{\mathbb{Q}}^{K_n}(\zeta_p)$$

und mit

$$f_p(X) = X^{p-1} + X^{p-2} + ... + X + 1$$

folgt aus $\alpha_{p-2} = 1$

$$\mathrm{Tr}_{\mathbb{Q}}^{K_n}(\zeta_p) = -1.$$

Seien nun $n = pq$, p, q verschiedene ungerade Primzahlen. Nach Gleichung (1) gilt $\zeta_{pq} = \zeta_p \cdot \zeta_q$. Betrachte nun den folgenden Körperturm:

$$\begin{array}{c} \mathbb{Q}(\zeta_{pq}) \\ | \\ \mathbb{Q}(\zeta_p) \\ | \\ \mathbb{Q} \end{array}$$

Da man die Spur als Abbildung auffassen kann, bilden wir nun die folgende Hintereinanderausführung:

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}}^{K_{pq}} &= \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\mathrm{Tr}_{\mathbb{Q}(\zeta_p)}^{K_{pq}}(\zeta_p \cdot \zeta_q)) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\zeta_p \mathrm{Tr}_{\mathbb{Q}(\zeta_p)}^{K_{pq}}(\zeta_q)) \\ &= \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(-\zeta_p) \\ &= -(-1) = (-1)^2 = 1 \end{aligned}$$

Induktiv erhält man die Behauptung. □

1.19 Definition. *Seien $A \subset B$ Ringe. Ein Element x aus B heißt ganz über A, wenn eine der folgenden Bedingungen erfüllt ist:*

1. *x ist Nullstelle eines normierten Polynoms $g(X) \in A[X]$.*
2. *Der von x erzeugte Ring $A[x]$ ist als A-Modul endlich erzeugt.*

Die beiden Bedingungen sind nach [Lan70], Seite 4, äquivalent.

1.20 Definition. *Betrachte die folgende Situation:*

$$\{x \in \mathbb{Q}(\zeta_n) \mid x \text{ ist ganz in } \mathbb{Z}\} = \begin{array}{ccc} B & \hookrightarrow & L \\ | & & | \\ \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

Dann heißt B der Ganzheitsring von L. Er wird mit $\mathcal{O}_L$ bezeichnet.

1.21 Korollar. *In der Situation aus Definition 1.19 gilt: Die Spur von $x \in L$ in K ist ganz über K (siehe [Lan70], Seite 6, Korollar zu Proposition 5).*

1.22 Bemerkung. Betrachten wir wieder die Erweiterung $K_n|\mathbb{Q}$. Die Einheitswurzel ζ_n ist ganz über $\mathbb{Q}$, da ζ_n Nullstelle eines normierten Polynoms mit Koeffizienten in $\mathbb{Z}$ ist.
Nach Korollar 1.21 ist λ_K ebenfalls ganz über $\mathbb{Q}$.

2 Situation

Im Folgenden möchte ich mit einer Einführung in die gegebene Situation beginnen. Vorgegeben sei ein ganz spezieller Typ von Erweiterungen des Körpers $\mathbb{Q}$ der rationalen Zahlen, nämlich der Erweiterungskörper $\mathbb{Q}(\zeta_n)$, wobei ζ_n eine primitive n-te Einheitswurzel ist. Sei also $n \in \mathbb{N}$ und wähle $n \neq 2 \bmod 4$ wie in Kapitel 1 beschrieben. Man betrachte also die Erweiterung

$$\begin{array}{c} \mathbb{Q}(\zeta_n) =: K_n \\ | \\ \mathbb{Q} \end{array}$$

und schreibe statt $\mathbb{Q}(\zeta_n)$ auch K_n.
Man kann zusammenfassend folgende Aussagen über diese Körpererweiterung treffen:

- $\mathbb{Q}(\zeta_n) = \{\sum_{i=0}^{\varphi(n)-1} a_i \zeta_n^i | a_i \in \mathbb{Q}\}$.
  Dabei ist φ die Eulersche Phi-Funktion wie in Definition 1.14 beschrieben.
- $K_n|\mathbb{Q}$ ist galoissch nach ([Was97], Satz 2.5).
- Der Grad dieser Körpererweiterung $[K_n : \mathbb{Q}]$ ist gleich $\varphi(n)$.
  Im Fall $n = p$ ergibt sich $[K_n|\mathbb{Q}] = \varphi(p) = p - 1$.
- Für die zu $K_n|\mathbb{Q}$ gehörige Galoisgruppe $\mathrm{Gal}(K_n|\mathbb{Q})$ gilt (siehe auch Satz 1.13)

  $$\mathrm{Gal}(K_n|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

  und

  $$\#(\mathrm{Gal}(K_n|\mathbb{Q})) = \varphi(n).$$

- Für das Minimalpolynom $f_n(X)$ der Einheitswurzel ζ_n gilt (nach [Lan84], Seite 205 -207)

  $$\begin{aligned} f_n(X) &= \prod_{\sigma \in (Gal)(K_n|\mathbb{Q})} (X - \sigma(\zeta_n)) && (3) \\ &= \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta_n^i) && (4) \\ &= \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})} && (5) \end{aligned}$$

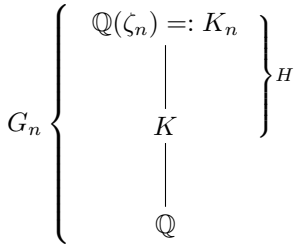
  mit $\deg(f_n) = \varphi(n)$. Die Funktion μ, die in Gleichung (5) auftritt, ist die Möbiusfunktion. Sie ist folgendermaßen definiert:

  $$\begin{array}{rccl} \mu: & \mathbb{N} & \longrightarrow & \{0, \pm 1\}, \\ & n & \longmapsto & \mu(n) \end{array} \quad = \begin{cases} (-1)^k & \text{falls } n = p_1 \cdot \ldots \cdot p_k \\ 0 & \text{sonst} \end{cases}$$

mit paarweise verschiedenen Primzahlen $p_1, ..., p_k$.
Betrachtet man wiederum den Fall $n = p$, so erhält man

$$f_p(X) = \frac{X^p - 1}{X - 1} \tag{6}$$
$$= X^{p-1} + X^{p-2} + ... + X + 1. \tag{7}$$

In dieser Arbeit soll das Hauptaugenmerk auf die Zwischenkörper dieser Erweiterung gelegt werden, also auf Körper K mit



Nach dem Hauptsatz der Galoistheorie (Satz 1.11) gibt es eine Bijektion zwischen den Untergruppen $H \subset G_n = \mathrm{Gal}(K_n|\mathbb{Q})$ und den Zwischenkörpern K, wobei $H := \mathrm{Gal}(K_n|K)$ die Galoisgruppe von $K_n|K$ ist.
Nach [Lan84], Seite 185, Theorem 14, wird jeder algebraische Zahlkörper aus einer endlichen algebraischen Erweiterung von einem Element erzeugt. Das Ziel ist es nun, einen Erzeuger für diese Zwischenkörper K zu finden, die als Zwischenkörper algebraischer Zahlkörper ebenfalls algebraische Zahlkörper sind.
Ein Kandidat für die Erzeugung von K könnte die Spur der Einheitswurzel ζ_n in K sein, da sie einer der Koeffizienten des Minimalpolynoms von ζ_n in K ist und K von diesen Koeffizienten erzeugt wird. Zunächst macht man also folgende Definition:

2.1 Definition. *Für einen Zwischenkörper K mit $K_n|K|\mathbb{Q}$ definiert man*

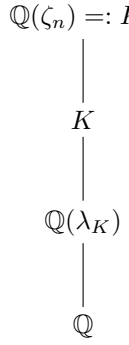
$$\lambda_K := Tr_K^{K_n}(\zeta_n) \tag{8}$$
$$= \sum_{\sigma \in H} \sigma(\zeta_n), \tag{9}$$

die Spur von ζ_n in K mit $H = Gal(K_n|K)$.

2.2 Bemerkung.
1. Der Name der Spur λ_K aus Definition 2.1 könnte ebenso gut λ_H sein, da dem Zwischenkörper K die Untergruppe H zugeordnet wird und umgekehrt. Diese Zuordnung ist nach dem Hauptsatz der Galoistheorie eindeutig.

2. Nach Definition liegt λ_K in K. Es kann jedoch vorkommen, dass λ_K bereits in einem echten Zwischenkörper $\mathbb{Q}(\lambda_K)$ von K und $\mathbb{Q}$ liegt. Ist dies der Fall, so

kann λ_K natürlich kein Erzeuger mehr von K sein. Insgesamt erhält man also folgenden Körperturm:



Dass die Spur λ_K keinesfalls immer den Körper K erzeugen kann, sieht man leicht am folgenden Beispiel.

2.3 Beispiel. Wähle nun $n = 9$. Um die Spur bestimmen zu können, betrachtet man zuerst die Galoisgruppe G_9 der Körpererweiterung $\mathbb{Q}(\zeta_9)|\mathbb{Q}$. Es gilt

$$G_9 \cong (\mathbb{Z}/9\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}.$$

Die Ordnung der Elemente $\overline{2}$ und $\overline{5}$ ist 6, die der Elemente $\overline{4}$ und $\overline{7}$ ist 3, die Ordnung von $\overline{8}$ ist 2 und die Ordnung von $\overline{1}$ ist trivialerweise 1.
Definieren wir nun also

$$H := \langle\overline{4}\rangle = \{\overline{1}, \overline{4}, \overline{7}\} \subset G_9,$$

und betrachten den zugehörigen Fixkörper

$$K := K_9^H,$$

der ein Teilkörper der Erweiterung $K_9|\mathbb{Q}$ ist, für den $\mathbb{Q} \subsetneq K \subsetneq K_9 = \mathbb{Q}(\zeta_9)$ gilt. Berechnet man die Spur λ_K, so stellt man fest, dass diese verschwindet:

$$\begin{aligned}\lambda_K = \mathrm{Tr}_K^{K_9}(\zeta_9) &= \sum_{i\in H} \zeta_9^i \\ &= \zeta_9 + \zeta_9^4 + \zeta_9^7 \\ &= \zeta_9(1 + \zeta_9^3 + \zeta_9^6) \\ &= \zeta_9(1 + \zeta_3 + \zeta_3^2) \\ &= 0\end{aligned}$$

Hier wurde ausgenutzt, dass das Minimalpolynom der dritten Einheitswurzel ζ_3 die Form

$$f_3(X) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$$

hat und ζ_3 eine Nullstelle dieses Polynoms ist, was den letzten Schritt der obigen Rechnung erklärt. In diesem Fall erhält man also für $\mathbb{Q}(\lambda_K) = \mathbb{Q}(0)$ den Grundkörper $\mathbb{Q}$.

Dieses Beispiel zeigt also, dass eine Aufgabe darin besteht, herauszufinden, in welchen Fällen λ_K den Körper K erzeugt und wie dies mit dem Parameter n zusammenhängt.

Betrachten wir nun noch den Ganzheitsring $\mathcal{O}_{K_n}$ eines Kreiskörpers $K_n = \mathbb{Q}(\zeta_n)$, also den Ring, der aus den Elementen von K_n besteht, die ganz über $\mathbb{Q}$ sind. Nach [Was97], Theorem 2.6, gilt

$$\mathcal{O}_{K_n} = \mathbb{Z}[\zeta_n] = \langle \zeta_n, {\zeta_n}^2, ..., {\zeta_n}^{n-1} \rangle.$$

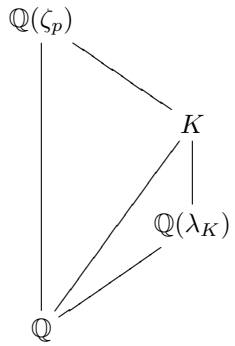
Interessant ist nun, ob man eine ähnliche Aussage auch für die Zwischenkörper K von $K_n|\mathbb{Q}$ treffen kann. Dies wird in Kapitel 4 behandelt.

3 Die Unterkörper von $\mathbb{Q}(\zeta_n)$ und deren Erzeugung

Wie bereits in Kapitel 2 angesprochen, stellt sich die Frage nach der Erzeugung der Zwischenkörper K, die zwischen den Körpern $\mathbb{Q}$ und $\mathbb{Q}(\zeta_n) = K_n$ liegen. In diesem Kapitel wird nun untersucht, ob die Spur der n-ten Einheitswurzel ζ_n, genannt λ_K, den Zwischenkörper K erzeugen kann und wenn ja, für welche $n \in \mathbb{N}$ dies der Fall ist. Mithilfe des Computeralgebra-Programmes MAGMA lassen sich die Zwischenkörper der Erweiterung $K_n|\mathbb{Q}$ bestimmen. Anschließend kann man λ_K berechnen und prüfen, ob die Körper K und $\mathbb{Q}(\lambda_K)$ gleich sind, beispielsweise indem man den Index von $\mathbb{Q}(\lambda_K)$ in K berechnen lässt. Bei der Zusammenstellung der Ergebnisse unterscheidet man sinnvollerweise die folgenden Fälle für den Führer n:

- $n \in \mathbb{P}$
- n ist quadratfrei
- $n = p^r, \quad p \in \mathbb{P}, r \geq 2$, also ist n eine Primpotenz
- n ist weder quadratfrei noch eine Primpotenz

Betrachten wir nun also zuerst den einfachsten Fall, nämlich $n = p \in \mathbb{P}$.



3.1 Satz. *In der Situation dieser Arbeit sei $n = p \in \mathbb{P} - \{2\}$ eine Primzahl. Dann werden alle Zwischenkörper K der Körpererweiterung $K_p|K|\mathbb{Q}$ von λ_K, der Spur von ζ_p in K, erzeugt.*

Beweis. Mit $n = p$ folgt

$$\mathrm{Gal}(K_p|\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, ..., \overline{p-1}\}.$$

Nach dem Hauptsatz der Galoistheorie (siehe Satz 1.11) ist jeder Unterkörper K von K_p eindeutig durch seine Galoisgruppe bestimmt. Zu zeigen ist also, dass $\mathbb{Q}(\lambda_K)$ der Fixkörper zu $H = \mathrm{Gal}(K_p|K)$ ist, also, dass

$$H = \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}(\lambda_K)) \tag{10}$$

gilt. Ebenso wie die Inklusion $\mathbb{Q}(\lambda_K) \subset K$ (siehe auch Kapitel 2) ist auch die Inklusion

$$H \subset \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}(\lambda_K)) = \{\sigma \in G_p | \sigma(\lambda_K) = \lambda_K\} \tag{11}$$

klar.
Es bleibt noch zu zeigen, dass $\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}(\lambda_K)) \subset H$ ist. Dazu zeigt man:

$$\text{Ist} \quad \tau \in G_p - H, \quad \text{so gilt} \quad \tau \notin \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}(\lambda_K)).$$

Dabei ist die letzte Aussage äquivalent zu $\tau(\lambda_K) \neq \lambda_K$.
Sei also $\tau \in G_p - H$.
Wie in Bemerkung 1.15 beschrieben, stellt man nun die Elemente der Gruppen G_p und H als Elemente von $(\mathbb{Z}/p\mathbb{Z})^*$ dar. Zu jeder Abbildung $\tau \in G_p$ gehört ein $\overline{t} \in (\mathbb{Z}/p\mathbb{Z})^*$, sodass

$$\begin{aligned} \tau: \qquad K_p &\longrightarrow K_p \\ \zeta_p &\longmapsto \zeta_p^{\overline{t}} \end{aligned}$$

gilt. Also schreibt man

$$\tau(\lambda_K) = \tau(\sum_{\overline{s} \in H} \zeta_p^{\overline{s}}) = \sum_{\overline{s} \in H} \zeta_p^{\overline{st}},$$

mit $\overline{st} \notin H$, da $\overline{t}$ ein Element von $G_p - H$ ist.
Annahme: Die Spur λ_K wird von einem Element $\tau \in G_p - H$ festgelassen, also auf sich selbst abgebildet. Dann folgt

$$\sum_{\overline{s} \in H} \zeta_p^{\overline{st}} - \sum_{\overline{s} \in H} \zeta_p^{\overline{s}} = 0. \tag{12}$$

Man betrachte das Polynom

$$P(X) = \sum_{\overline{s} \in H} X^{st} - \sum_{\overline{s} \in H} X^{s},$$

wobei die Exponenten $s,\ st$ die eindeutig bestimmten Repräsentanten aus $\mathbb{Z}/p\mathbb{Z}$ mit $1 \leq s,\ st \leq p-1$ sind. Dieses Polynom ist nicht das Nullpolynom, da mit $\overline{t}$ auch $\overline{st}$ kein Element von H ist und sich somit die Summanden nicht gegenseitig auslöschen können. Außerdem hat es nach (12) die Nullstelle ζ_p und es gilt $\deg(P) \leq p-1$. Da s und st Repräsentanten von Elementen aus $(\mathbb{Z}/p\mathbb{Z})^*$ sind, sind alle Exponenten ungleich 0. Man betrachtet

$$P(X) = X \cdot \underbrace{(\sum_{\overline{s} \in H} X^{st-1} - \sum_{\overline{s} \in H} X^{s-1})}_{\tilde{P}(X)}$$

und erhält das Polynom $\tilde{P}$ mit $\deg \tilde{P} \leq p-2$ und Nullstelle ζ_p, was jedoch ein Widerspruch zu der Tatsache ist, dass das Minimalpolynom

$$f_p(X) = \frac{X^p - 1}{X - 1}$$

von ζ_p den Grad $\deg f = p - 1 > p - 2$ hat.
Also muss gelten

$$\sum_{\overline{s} \in H} \zeta_p^{\overline{st}} - \sum_{\overline{s} \in H} \zeta_p^{\overline{s}} \neq 0 \quad \forall \tau \in G_p - H,$$

was die zweite Inklusion zeigt.
Damit ist auch die Aussage (11) gezeigt. □

3.2 Satz. *Sei n eine Primpotenz, n lasse sich also schreiben als $n = p^r$ für ein $r \geq 2$ und $p \in \mathbb{P} - \{2\}$. Dann gilt*

$$K = \mathbb{Q}(\lambda_K) \quad \Leftrightarrow \quad \frac{n}{p} + 1 \notin H \quad \Leftrightarrow \quad p \nmid \#H. \tag{13}$$

Aus $\frac{n}{p} + 1 \in H$ folgt $\lambda_K = 0$ und damit $\mathbb{Q}(\lambda_K) = \mathbb{Q}$.

Beweis. Die zweite Äquivalenz ist trivial, da $\frac{n}{p} + 1$ die Gruppe der Elemente der Ordnung p in G_{p^r} erzeugt.
Der Beweis zur ersten Äquivalenz funktioniert ähnlich wie der Beweis zu Satz 3.1. Betrachten wir also zunächst das Minimalpolynom f_{p^r} der primitiven Einheitswurzel ζ_{p^r}. Nach Gleichung (5) folgt für f_{p^r}:

$$f_{p^r}(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} \tag{14}$$

$$= (X^{p^{r-1}})^{p-1} + (X^{p^{r-1}})^{p-2} + ... + X^{p^{r-1}} + 1 \tag{15}$$

Man betrachte nun den Fall, dass p kein Teiler der Ordnung von H ist.
Analog zum Beweis von 3.1 zeigt man wieder, dass gilt:

$$\forall \tau \in G_{p^r} - H : \quad \tau(\lambda_K) \neq \lambda_K \tag{16}$$

Annahme: Es gibt ein $\tau \in G_{p^r} - H$, sodass

$$\sum_{\overline{s} \in H} \zeta_{p^r}^{\overline{st}} - \sum_{\overline{s} \in H} \zeta_{p^r}^{\overline{s}} = 0. \tag{17}$$

ζ_{p^r} ist also Nullstelle des Polynoms

$$P(X) = \sum_{\overline{s} \in H} X^{st} - \sum_{\overline{s} \in H} X^s = X \cdot \underbrace{(\sum_{\overline{s} \in H} X^{st-1} - \sum_{\overline{s} \in H} X^{s-1})}_{=: \tilde{P}(X)}$$

mit eindeutig bestimmten Exponenten $1 \leq st, s \leq p^r - 1$. Damit ist ζ_{p^r} auch Nullstelle von $\tilde{P}(X)$ mit $\deg(\tilde{P}) \leq p^r - 2$. Also muss das Minimalpolynom f_{p^r} ein Teiler von $\tilde{P}$ sein. Es muss also ein Polynom $h \in \mathbb{Q}[X]$ geben mit

$$f_{p^r}(X)h(X) = \tilde{P}(X). \tag{18}$$

Nach dem Lemma von Gauß (siehe beispielsweise [SP07], Satz 11.2) liegt h sogar in $\mathbb{Z}[X]$.
Betrachtet man den Grad der Polynome f_{p^r}, h und $\tilde{P}$, so erhält man

$$\begin{aligned}
\deg(f_{p^r}) &= \varphi(p^r) = (p-1)p^{r-1}, \\
\deg(\tilde{P}) &\leq p^r - 2, \\
\deg(h) &= \deg(\tilde{P}) - \deg(f_{p^r}) \\
&\leq p^r - 2 - (p-1)p^{r-1} \\
&= p^r - 2 - p^r + p^{r-1} \\
&= p^{r-1} - 2 \\
&< p^{r-1}.
\end{aligned}$$

Bei dem Minimalpolynom f_{p^r} stellt man fest, dass zwischen zwei Koeffizienten, die ungleich Null sind, immer $p^{r-1} - 1$ Koeffizienten verschwinden. Da $\deg(h) \leq p^{r-1} - 2$ ist, kann man leicht die Anzahl der Koeffizienten von $f_{p^r} \cdot h$ bestimmen, die nicht Null sind. Sei x die Anzahl der Koeffizienten von h, die nicht Null sind. Dann hat $f_{p^r} \cdot h$ insgesamt $p \cdot x$ Koeffizienten ungleich Null. Für $\tilde{P}$ erhält man $2 \cdot \#H$ solche Koeffizienten.
Mit Gleichung (18) folgt

$$p \cdot x = 2 \cdot \#H. \tag{19}$$

Da p ein Teiler der linken Seite der Gleichung (19) ist, muss p auch die rechte Seite teilen. Da $p \neq 2$ vorausgesetzt ist, muss $p|\#H$ gelten, was ein Widerspruch zur Voraussetzung $p \nmid \#(H)$ ist. Damit kann (19) nicht erfüllt sein und die Annahme (17) war falsch.
Also gilt

$$K = K_n^H = \mathbb{Q}(\lambda_K).$$

Jetzt muss noch der Fall $p|\#H$ behandelt werden. Sei also $\#H$ durch p teilbar. Dann gilt

$$i\frac{n}{p} + 1 \in H \qquad \text{für} \quad i = 0, ..., p-1,$$

da dies die $p - 1$ Elemente der Ordnung p in G_{p^r} sind.

Die Berechnung der Spur liefert

$$\begin{aligned}
\lambda_K &= \sum_{\overline{s}\in H/\langle\overline{\frac{n}{p}+1}\rangle} \sum_{i=0}^{p-1} \zeta_n^{\overline{s(i\frac{n}{p}+1)}} \\
&= \sum_{\overline{s}\in H/\langle\overline{\frac{n}{p}+1}\rangle} \zeta_n^{\overline{s}} \sum_{i=0}^{p-1} \zeta_n^{\overline{is\frac{n}{p}}} \\
&= \sum_{\overline{s}\in H/\langle\overline{\frac{n}{p}+1}\rangle} \zeta_n^{\overline{s}} \sum_{i=0}^{p-1} (\zeta_n^{\overline{s\frac{n}{p}}})^i \\
&= \sum_{\overline{s}\in H/\langle\overline{\frac{n}{p}+1}\rangle} \zeta_n^{\overline{s}} \cdot 0 \\
&= 0.
\end{aligned}$$

Insgesamt folgt, dass K genau dann von λ_K erzeugt wird, wenn p die Ordnung von H nicht teilt. Die Spur λ_K erzeugt also entweder den Körper K oder sie ist Null. □

Bisher wurde der Fall, dass n eine 2-Potenz ist, nicht behandelt. Der Beweis zum vorangegangenen Satz zeigt, dass man $p = 2$ gesondert betrachten muss. Man erhält jedoch ähnliche Aussagen:

3.3 Satz. *Ist $n = 2^r$, $r \geq 2$, so gilt für $H \subset G_n$ eine der folgenden Aussagen:*

1. $H = \{1\}$, *d.h.* $K = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\lambda_K)$
2. $H = \{\pm 1\}$
3. $H = \{\frac{n}{2} - 1, 1\}$
4. $\frac{n}{2} + 1 \in H$

In den Fällen 2 und 3 erzeugt λ_K den Körper K, im Fall 4 ist $\lambda_K = 0$.

Bevor Satz 3.3 gezeigt wird, benötigen wir noch zwei Hilfssätze:

3.4 Hilfssatz. *Es gilt*

$$3^{2^s} \equiv 1 + 2^{s+2} \bmod 2^{s+3} \tag{20}$$

für $s \in \mathbb{N}$.

Beweis. Beweis durch vollständige Induktion:
Induktionsanfang: $s = 1$

$$9 = 3^{2^1} = 1 + 2^{1+2} = 9 \bmod 16$$

Induktionsvoraussetzung: Sei (3.4) gezeigt für ein $s \in \mathbb{N}$.
Induktionsschritt: $s \to s + 1$
Nach Induktionsvoraussetzung gilt

$$3^{2^s} = 1 + 2^{s+2} + k \cdot 2^{s+3}$$

für ein $k \in \mathbb{Z}$. Dann gilt

$$\begin{aligned} 3^{2^{s+1}} &= 3^{2 \cdot 2^s} = (3^{2^s})^2 \\ &\overset{\text{IV}}{=} (1 + 2^{s+2} + k \cdot 2^{s+3})^2 \\ &= 1 + 2^{2s+4} + k^2 \cdot 2^{2s+6} + 2 \cdot 2^{s+2} + 2 \cdot k \cdot 2^{s+3} + 2 \cdot 2^{s+2} \cdot k \cdot 2^{s+3} \\ &\equiv 1 + 2^{s+3} \bmod 2^{s+4}, \end{aligned}$$

was Hilfssatz 3.4 zeigt. □

3.5 Hilfssatz. *Für $r \geq 3$ gilt*

$$(\mathbb{Z}/2^r\mathbb{Z})^* = \langle 3 \rangle \times \{\pm 1\} \tag{21}$$
$$\cong (\mathbb{Z}/2^{r-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}). \tag{22}$$

Im Fall $r = 2$ gilt trivialerweise $(\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\} = \langle 3 \rangle$.

Beweis. Allgemein kann man für $n = 2^r, r \geq 2$

$$(\mathbb{Z}/2^r\mathbb{Z})^* \cong (\mathbb{Z}/2^{s_1}\mathbb{Z}) \times ... \times (\mathbb{Z}/2^{s_l}\mathbb{Z})$$

ansetzen, wobei

$$s_1 \geq s_2 \geq ... \geq s_l$$

gewählt wird, damit die Zerlegung eindeutig ist und es muss gelten

$$\sum_{i=1}^{l} s_i = r - 1, \tag{23}$$

da die Gruppengröße $\varphi(n) = 2^{r-1}$ ist.
Behauptung: Für die Ordnung der Elemente 3, -1, $\frac{n}{2}+1$ und $\frac{n}{2}-1$ aus $(\mathbb{Z}/2^r\mathbb{Z})^*$ gilt

$$\operatorname{ord}(3) = 2^{r-2} \tag{24}$$
$$\operatorname{ord}(-1) = 2 \tag{25}$$
$$\operatorname{ord}(\frac{n}{2}+1) = 2 \tag{26}$$
$$\operatorname{ord}(\frac{n}{2}-1) = 2. \tag{27}$$

(25) ist klar, (26) und (27) folgen aus

$$(\frac{n}{2} \pm 1)^2 = 2^{2r-2} \pm n + 1 = 2^{r-2}n \pm n + 1 \equiv 1 \bmod n.$$

Aus Hilfssatz 3.4 folgt mit $s = r-3$

$$3^{2^{r-3}} \equiv 1 + \frac{n}{2} \bmod n = 1 + 2^{r-1} \bmod 2^r$$

und mit (26) folgt dann (24) durch Quadrieren dieser Gleichung auf beiden Seiten.
Also existiert in $(\mathbb{Z}/2^r\mathbb{Z})^*$ ein Element der Ordnung 2^{r-2}, nämlich die 3. Damit gilt $s_1 \geq r-2$. Da es drei Elemente der Ordnung 2 gibt, muss $(\mathbb{Z}/n\mathbb{Z})$ in mindestens zwei Faktoren zerfallen. Also gilt $s_1, s_2 \geq 1$.
Damit und mit (23) sind die s_i eindeutig bestimmt und es folgt insgesamt

$$(\mathbb{Z}/2^r\mathbb{Z})^* \cong (\mathbb{Z}/2^{r-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Da 3 eine Untergruppe der Ordnung 2^{r-2} erzeugt und in $\langle 3\rangle$ nur ein Element der Ordnung 2 existiert, nämlich $\frac{n}{2}+1$ (siehe Hilfssatz 3.4), folgt, dass der zweite Faktor von -1 erzeugt werden kann. Also gilt auch

$$(\mathbb{Z}/2^r\mathbb{Z})^* = \langle 3\rangle \times \{\pm 1\}$$

□

Beweis. (zu Satz 3.3)
Sei $n = 2^r, \quad r \geq 2$. Dann gilt nach Satz 3.5

$$(\mathbb{Z}/2^r\mathbb{Z})^* \cong \langle 3\rangle \times \{\pm 1\}.$$

Zunächst muss gezeigt werden, dass die Fallunterscheidung in Satz 3.3 richtig ist. Sei H also so gewählt, dass keine der Beschreibungen (1) bis (3) zutrifft. Nun ist zu zeigen, dass dann $\frac{n}{2}+1$ in H enthalten ist. Gibt es in einem solchen H nur Elemente der Ordnung 2, so ist $\frac{n}{2}+1$ trivialerweise ein Element von H (denn dann ist $H = \{\frac{n}{2}+1, 1\}$ oder $H = \{\frac{n}{2}+1, \frac{n}{2}-1, -1, 1\}$). Ansonsten enthält H ein Element $a \times b \in \langle 3\rangle \times \{\pm 1\}$ der Ordnung 4. Dann ist auch $(a \times b)^2 \in H$. Mit $b^2 = 1$ folgt, dass $(a \times b)^2 \in \langle 3\rangle$ gilt. Dies ist ein Element der Ordnung 2 und muss daher gleich $\frac{n}{2}+1$ sein. Damit ist die Gültigkeit der Fallunterscheidung gezeigt.
Betrachten wir nun wieder die in 3.3 angegebenen vier Fälle.

1. $H = \{1\}$. Hier ist nichts zu zeigen.

2. $H = \{\pm 1\}$
   Für die Spur λ_K gilt dann

$$\lambda_K = \mathrm{Tr}_K^{K_n}(\zeta_n) = \zeta_n + \overline{\zeta_n} = 2\mathrm{Re}(\zeta_n).$$

   Wähle $\tau \in G - H$ mit $\tau : \zeta_n \mapsto \zeta_n^b$. Dann ist

$$\tau(\lambda_K) = \zeta_n^b + \zeta_n^{-b} = 2\mathrm{Re}(\zeta_n^b) \neq 2\mathrm{Re}(\zeta_n)$$

   Also lässt ein $\tau \in G - H$ die Spur λ_K nie fest und es gilt $\mathbb{Q}(\lambda_K) = K$. Der Körper K ist in diesem Fall eine Teilmenge der reellen Zahlen $\mathbb{R}$.

3. $H = \{1, \frac{n}{2} - 1\}$
   Berechnet man λ_K, so erhält man nun einen rein imaginären Wert:

$$\lambda_K = \zeta_n + \zeta_n^{\frac{n}{2}-1} = 2i \cdot \mathrm{Im}(\zeta_n).$$

   Führt man obige Rechnung nochmals für $\tau \in G - H$ durch, so erhält man wieder

$$\tau(\lambda_K) = \zeta_n^b + \zeta_n^{(\frac{n}{2}-1)b} = 2i \cdot \mathrm{Im}(\zeta_n^b) \neq \lambda_K$$

   und es folgt

$$K = \mathbb{Q}(\lambda_K).$$

4. $\frac{n}{2} + 1 \in H$
   Nun erhält man für λ_K:

$$\begin{aligned}
\lambda_K = \mathrm{Tr}_K^{K_n}(\zeta_n) &= \sum_{a \in H} \zeta_n^a \\
&= \sum_{b \in H/\langle \frac{n}{2}+1 \rangle} (\zeta_n^b + \zeta_n^{b(\frac{n}{2}+1)}) \\
&= \sum_{b \in H/\langle \frac{n}{2}+1 \rangle} (\zeta_n^b + \zeta_n^b \cdot \zeta_n^{b\frac{n}{2}}) \\
&= \sum_{b \in H/\langle \frac{n}{2}+1 \rangle} (\zeta_n^b + \zeta_n^b \cdot (-1)) \qquad \text{da} \quad \mathrm{ggT}(b, n) = 1 \\
&= 0
\end{aligned}$$

   Also erzeugt λ_K den Körper K in diesem Fall nicht, da $\mathbb{Q}(\lambda_K) = \mathbb{Q}(0) = \mathbb{Q}$ ist.

□

3.6 Bemerkung. Anschaulich kann man die Ergebnisse aus den Sätzen 3.2 und 3.3, also für $n = p^r, r \in \mathbb{N}$, so interpretieren, dass die Spur λ_K dann Null wird, wenn man den Körper K_n „zu groß“ gewählt hat, also wenn man einen kleineren Kreiskörper K_m wählen kann, der den Unterkörper K besitzt. Damit dann die Spur nicht verschwindet, muss K_m minimal mit der Eigenschaft $K \subset K_m$ gewählt werden.

3.7 Beispiel. Betrachten wir nun die Körpererweiterung $\mathbb{Q}(\zeta_8)|\mathbb{Q}$. Die zugehörige Galoisgruppe $G_8 = \mathrm{Gal}(K_8|\mathbb{Q})$ ist

$$G_8 \xrightarrow{\cong} (\mathbb{Z}/8\mathbb{Z})^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

Alle Elemente der Galoisgruppe außer der $\overline{1}$ haben Ordnung 2. Es gibt also nur die Untergruppen

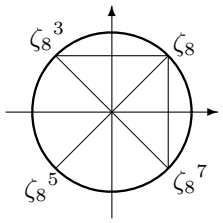
$$\begin{aligned} H_1 &\cong \{\overline{1}\}, \\ H_2 &\cong \{\overline{1}, \overline{3}\}, \\ H_3 &\cong \{\overline{1}, \overline{5}\}, \\ H_4 &\cong \{\overline{1}, \overline{7}\}, \\ H_5 &\cong G_8 \end{aligned}$$

Beginnen wir mit den trivialen Untergruppen von G_8, nämlich H_1 und H_5.
Der Fixkörper $K_8^{H_1}$ von H_1 ist wieder $K_8 = \mathbb{Q}(\zeta_8)$. Für die Spur gilt $\lambda_K = {\zeta_8}^1 = \zeta_8$ und sie erzeugt offensichtlich K_8.
Im Fall $H = H_5 = G_8$ gilt $K_8^H = \mathbb{Q}$ und die Spur λ_K von ζ_8 in $\mathbb{Q}$ liegt offensichtlich in $\mathbb{Q}$. Also gilt auch hier $K_8^H = \mathbb{Q}(\lambda_K)$.

Befassen wir uns nun mit den interessanten Fällen:
Sei zunächst $H = H_2 \cong \{\overline{1}, \overline{3}\}$. Dann gilt für λ_K

$$\lambda_K = \sum_{\sigma \in H_2} \sigma(\zeta_8) = \sum_{i \in \{\overline{1}, \overline{3}\}} \zeta_8^i = \zeta_8 + {\zeta_8}^3 \neq 0.$$

Betrachte dazu folgende Veranschaulichung:



Wie man sieht, ist $\zeta_8 + {\zeta_8}^3$ eine rein imaginäre Zahl und es gilt

$$\lambda_K = \zeta_8 + {\zeta_8}^3 = 2i\mathrm{Im}(\zeta_8),$$

λ_K ist also kein Element von $\mathbb{Q}$. Es ist klar, dass

$$\mathbb{Q}(\lambda_K) \subset K_8^H \tag{28}$$

gilt. Wird λ_K nur von den Elementen aus G_8 festgehalten, die in $H = H_2$ liegen, so gilt in Gleichung (28) die Gleichheit. Das dies der Fall ist, folgt wie im Beweis zu Satz 3.3.
Eine analoge Rechnung ergibt sich für $H = H_4 = \{\overline{1}, \overline{7}\}$. Hier gilt für die Spur

$$\lambda_K = \zeta_8 + {\zeta_8}^7 = 2\mathrm{Re}(\zeta_8).$$

Auch in diesem Fall erzeugt sie den Zwischenkörper $K = K_8^H$.
Anders sieht es im Fall $H = H_3 = \{\overline{1}, \overline{5}\}$ aus. Hier erhält man

$$\lambda_K = \zeta_8 + {\zeta_8}^5 = \zeta_8 + \zeta_8^{1+4} = \zeta_8 + \zeta_8 \cdot {\zeta_8}^4 = \zeta_8 + \zeta_8 \cdot (-1) = 0.$$

D.h. in diesem Fall kann $K = K_8^{H_3}$ nicht von λ_K erzeugt werden.
Wie man sieht, ist H_5 die einzige echte Untergruppe von G_8, die das Element $\sigma : \zeta_8 \mapsto \zeta_8^5$ enthält. Mit $5 = \frac{n}{2} + 1$ lässt sich das Ergebnis auch mithilfe von Satz 3.3 erklären.

3.8 Satz. *Sei $n \in \mathbb{N}$ quadratfrei. Dann werden alle Zwischenkörper K zwischen $\mathbb{Q}$ und $\mathbb{Q}(\zeta_n)$ von der Spur λ_K erzeugt.*

Beweis. Schreibe

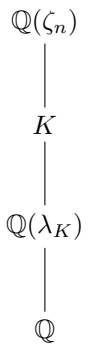
$$n = p_1 \cdot p_2 \cdot ... \cdot p_k, \qquad p_1, ..., p_k \in \mathbb{P}$$

mit paarweise verschiedenen $p_i, \quad 1 \leq i \leq k$.
Aus Satz 1.18 ist bereits bekannt, dass die Spur von ζ_n in $\mathbb{Q}$ bei quadratfreiem $n = p_1 \cdot p_2 \cdot ... \cdot p_k$ nur die Werte 1 oder -1 annimmt:

$$\mathrm{Tr}_{\mathbb{Q}}^{K_n}(\zeta_n) = (-1)^k.$$

Nun betrachtet man erneut die Spur von ζ_n in $\mathbb{Q}$. Man nutzt nun aus, dass die Spur

eine Abbildung von einem Körper in einen Unterkörper ist.



Es gilt

$$\begin{aligned}
(-1)^k &= \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_n)}(\zeta_n) \\
&= \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}(\mathrm{Tr}_{\mathbb{Q}(\lambda_K)}^{K} \underbrace{(\mathrm{Tr}_{K}^{\mathbb{Q}(\zeta_n)}(\zeta_n))}_{\lambda_K}) \\
&= \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}(\mathrm{Tr}_{\mathbb{Q}(\lambda_K)}^{K}(\lambda_K)) \\
&= \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}([K:\mathbb{Q}(\lambda_K)] \cdot \lambda_K) \qquad \text{da} \quad \lambda_K \in \mathbb{Q}(\lambda_K) \\
&= \underbrace{[K:\mathbb{Q}(\lambda_K)]}_{\in\mathbb{N}} \cdot \underbrace{\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}(\lambda_K)}_{\in\mathbb{Z}\ (*)}
\end{aligned}$$

Behauptung $(*)$**:** $\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}(\lambda_K)$ ist ein Element von $\mathbb{Z}$.
Da ζ_n im Ganzheitsring $\mathcal{O}_{K_n}$ von K_n liegt, liegen auch λ_K sowie die Spur von λ_K in $\mathbb{Q}$ in $\mathcal{O}_{K_n}$. Mit $\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}(\lambda_K) \in \mathbb{Q}$ (nach Definition) und $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}} = \mathbb{Q} \cap \mathcal{O}_{K_n}$ folgt dann obige Behauptung.
Insgesamt folgt mit

$$(-1)^k = \underbrace{[K:\mathbb{Q}(\lambda_K)]}_{\in\mathbb{N}} \cdot \underbrace{\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}(\lambda_K)}_{\in\mathbb{Z}},$$

dass $[K:\mathbb{Q}(\lambda_K)] = 1$ und $\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}(\lambda_K) = (-1)^k$.
Somit ist $K = \mathbb{Q}(\lambda_K)$. □

3.9 Korollar. *Sei $n = p_1 \cdot \ldots \cdot p_k$ quadratfrei. Aus dem Beweis zu Satz 3.8 ergibt sich*

$$Tr_{\mathbb{Q}}^{\mathbb{Q}(\lambda_K)}(\lambda_K) = Tr_{\mathbb{Q}}^{K}(\lambda_K) = (-1)^k.$$

Nun fehlt noch der allgemeine Fall. Sei ab jetzt $n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_k^{r_k}$, $p_1, ..., p_k \in \mathbb{P}$ und $r_i \in \mathbb{N}\ \forall i = 1, ..., k$. Zunächst definiert man:

3.10 Definition. *Sei $n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_k^{r_k}$, $p_1, ..., p_k \in \mathbb{P}$. Dann gilt nach dem Chinesischen Restsatz (siehe [SP07], Satz 4.13)*

$$G = (\mathbb{Z}/_{n\mathbb{Z}})^* \overset{\cong}{\to} (\mathbb{Z}/_{p_1^{r_1}\mathbb{Z}})^* \times ... \times (\mathbb{Z}/_{p_k^{r_k}\mathbb{Z}})^*.$$

*Eine Untergruppe $H \subset G$ liegt **diagonal** in G, wenn gilt: Unter obigem Isomorphismus entspricht H einer Gruppe*

$$H_1 \times ... \times H_k \quad mit \quad H_i \subset (\mathbb{Z}/_{p_i^{r_i}\mathbb{Z}})^*,\ i = 1, ..., k. \tag{29}$$

3.11 Satz. *Sei n wie oben gefordert und sei H eine Untergruppe von G, die diagonal in G liegt. Dann gilt*

$$K = \mathbb{Q}(\lambda_K) \quad \Leftrightarrow \quad \forall i = 1, ..., k:\ p_i^{r_i - 1} + 1 \notin H_i. \tag{30}$$

Ist keines der $p_i = 2$, so gilt auch

$$K = \mathbb{Q}(\lambda_K) \quad \Leftrightarrow \quad \forall\ i = 1, ..., k:\ p_i \nmid \#H_i.$$

Um diesen Satz zu zeigen, benötigt man noch folgendes Lemma:

3.12 Lemma. *(Schwache Multiplikativität der Spur)*
Sei H diagonal in G.

$$\begin{array}{ccccccccc} G & \overset{\cong}{\to} & (\mathbb{Z}/_{p_1^{r_1}\mathbb{Z}})^* & \times & ... & \times & (\mathbb{Z}/_{p_k^{r_k}\mathbb{Z}})^* \\ \cup & & \cup & & & & \cup \\ H & \overset{\cong}{\to} & H_1 & \times & ... & \times & H_k \end{array}$$

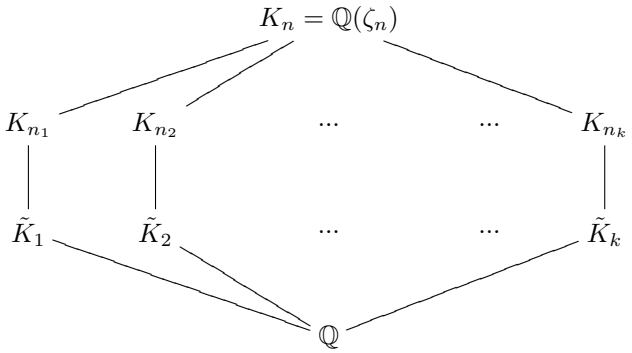
Setze

$$\begin{aligned} n_i &:= p_i^{r_i}, \\ \tilde{K}_i &:= K_{n_i}^{H_i}, \\ \lambda_i &:= Tr_{\tilde{K}_i}^{K_{n_i}}(\zeta_{n_i}). \end{aligned}$$

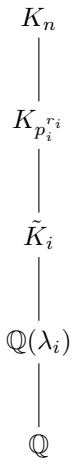
Dann gilt

$$\lambda_K = \lambda_1 \cdot \lambda_2 \cdot ... \cdot \lambda_k. \tag{31}$$

Anschaulich betrachtet man die obige Situation also folgendermaßen:



Man kann also die Ergebnisse für den Fall, dass n eine Primpotenz ist, nutzen. Der Körper K_n besitzt die $K_{p_i^{r_i}}$ als Unterkörper. Zu jedem dieser $K_{p_i^{r_i}}$ gibt es eine Untergruppe $H_i \subset (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$, zu der man den Fixkörper $(K_{p_i^{r_i}})^{H_i} =: \tilde{K}_i$ definiert. Man befindet sich also wieder in der gleichen Situation wie in Satz 3.2.



Gilt also $\lambda_K = \prod_{i=1}^{k} \lambda_i$, so folgt:
Ist eines der $\lambda_i = 0$, was äquivalent ist zu der Aussage $p_i | \# H_i$, so ist auch $\lambda_K = 0$.

Beweis. zu Lemma 3.12
Sei

$$\begin{array}{ccccccc} G & = & (\mathbb{Z}/mn\mathbb{Z})^* & \overset{\cong}{\to} & (\mathbb{Z}/m\mathbb{Z})^* & \times & (\mathbb{Z}/n\mathbb{Z})^* \\ \cup & & & & \cup & & \cup \\ H & & & \overset{\cong}{\to} & H_1 & \times & H_2 \\ & & & & \in & & \in \\ & & & & \sigma_1 & & \sigma_2 \end{array}$$

mit $\mathrm{ggT}(m,n) = 1$. Dann gilt

$$\begin{aligned} \lambda_K &= \sum_{\overline{s}\in H} \zeta_{mn}^{\overline{s}} \\ &= \sum_{\overline{s}\in H} (\zeta_m \cdot \zeta_n)^{\overline{s}} \\ &= \sum_{\overline{s}_1\times\overline{s}_2 \in H_1\times H_2} (\zeta_m \cdot \zeta_n)^{\overline{s}_1\times\overline{s}_2} \\ &= \sum_{\overline{s}_1\in H_1} \zeta_m^{\overline{s}_1} \sum_{\overline{s}_2\in H_2} \zeta_n^{\overline{s}_2} \\ &= \underbrace{\mathrm{Tr}_{K_m^{H_1}}^{K_m}(\zeta_m)}_{=:\lambda_1} \cdot \underbrace{\mathrm{Tr}_{K_n^{H_2}}^{K_n}(\zeta_n)}_{=:\lambda_2} \\ &= \lambda_1 \cdot \lambda_2 \end{aligned}$$

Da man n in ein Produkt von Primpotenzen zerlegen kann, erhält man

$$n = \underbrace{p_1^{r_1}}_{=:n_1} \cdot ... \cdot \underbrace{p_k^{r_k}}_{=:n_k}$$

mit $\mathrm{ggT}(n_i, n_j) = 1$ für alle $i, j \in 1, ..., k$ und $i \neq j$. Mit Hilfe von obiger Rechnung erhält man nun

$$\lambda_K = \prod_{i=1}^{k} \mathrm{Tr}_{\tilde{K}_i}^{K_{n_i}}(\zeta_{n_i}) = \prod_{i=1}^{k} \lambda_i, \tag{32}$$

wobei $\tilde{K}_i := K_{n_i}^{H_i}$ gilt. Damit ist also die schwache Multiplikativität der Spur gezeigt. □

Um Satz 3.11 zu zeigen, fehlt nur noch die Aussage

$$\forall i = 1, ..., k : p_i \nmid \#H_i \Rightarrow K = \mathbb{Q}(\lambda_K).$$

Die andere Richtung folgt, wie bereits erwähnt, aus der schwachen Multiplikativität der Spur. Nimmt man an, dass es ein i gibt, sodass p_i ein Teiler von H_i ist, so folgt $\mathbb{Q}(\lambda_K) = \mathbb{Q}$. In diesem Fall kann λ_K den Körper K also nicht erzeugen.
Obige Aussage soll nun im Folgenden bewiesen werden.

Beweis. (zu 3.11)
Sei also die Bedingung

$$\forall i = 1, ..., k : p_i \nmid \#H_i$$

erfüllt. Dann ist λ_K ungleich Null nach 3.12. Es ist zu zeigen, dass λ_K den Körper K erzeugt. Dazu zeigt man

$$\sigma(\lambda_K) = \lambda_K \quad \Leftrightarrow \quad \sigma \in H = H_1 \times ... \times H_k.$$

Ist $\sigma \in H$, so gilt natürlich auch $\sigma(\lambda_K) = \lambda_K$, da $\lambda_K \in K$ ist und K der Fixkörper von K_n unter H ist.
Um die andere Richtung zu zeigen, zeigt man die stärkere Aussage

$$\sigma(\lambda_K) = q \cdot \lambda_K,\ q \in \mathbb{Q}^* \quad \Leftrightarrow \sigma \in H. \tag{33}$$

Dabei ist die Richtung „$\Leftarrow$“ auch wieder klar (mit $q = 1$). Wir zeigen nun Gleichung 33 durch Induktion nach der Anzahl k der Primteiler von n.
Induktionsanfang: $n = 1$
Dann gilt $n = p^r$, $r \geq 1$.
Zeige nun also

$$\sigma(\lambda_K) = q \cdot \lambda_K,\ q \in \mathbb{Q}^* \quad \Rightarrow \quad \sigma \in H. \tag{34}$$

Annahme: Es gibt ein $\tau \notin H$ mit $\tau(\zeta_n) = \zeta_n^t$ und $\tau(\lambda_K) = q \cdot \lambda_K$.
Dann gilt

$$\begin{aligned} 0 &= \tau(\lambda_K) - q \cdot \lambda_K \\ &= \tau(\sum_{\overline{s} \in H} \zeta_{p^r}^{\overline{s}}) - q \cdot \sum_{\overline{s} \in H} \zeta_{p^r}^{\overline{s}} \\ &= \sum_{\overline{s} \in H} \zeta_{p^r}^{\overline{st}} - q \cdot \sum_{\overline{s} \in H} \zeta_{p^r}^{\overline{s}} \end{aligned}$$

Betrachte das Polynom

$$\sum_{\overline{s} \in H} X^{st} - q \cdot \sum_{\overline{s} \in H} X^s = X \cdot \underbrace{(\sum_{\overline{s} \in H} X^{st-1} - q \cdot \sum_{\overline{s} \in H} X^{s-1})}_{=: g(X)}$$

mit Exponenten $1 \leq st, s \leq p^r - 1$ wie im Beweis zu Satz 3.2.
$g(X)$ hat die Nullstelle ζ_{p^r} und Grad $\deg(g) \leq p^r - 2$. Das Polynom kann nicht das Nullpolynom sein, da die Exponenten der ersten Summe und die der zweiten Summe unterschiedlich sind, denn es gilt

$$\overline{s} \in H,\ \overline{t} \notin H \quad \Rightarrow \quad \overline{st} \notin H.$$

Dann ist das Minimalpolynom $f_{p^r}(X)$ mit $\deg(f_{p^r}) = (p-1)p^{r-1}$ ein Teiler von g.
Wie im Beweis zu 3.2 folgt an dieser Stelle der Widerspruch. Also war die Annahme falsch und es muss gelten

$$\sigma(\lambda_K) = q \cdot \lambda_K,\ q \in \mathbb{Q} \quad \Leftrightarrow \quad \sigma \in H.$$

Damit ist der Induktionsanfang bewiesen.
Induktionsschritt: Sei für ein beliebiges $k \in \mathbb{N}$ (und damit $n = p_1^{r_1} \cdot ... \cdot p_k^{r_k}$, $r_i \geq 1$ für $i = 1, ..., k$) die Aussage

$$\sigma(\lambda_K) = q \cdot \lambda_K,\ q \in \mathbb{Q} \quad \Leftrightarrow \sigma \in H = H_1 \times ... \times H_k\ \subset G_n \tag{35}$$

gezeigt.
Induktionsschritt: Definiere zunächst, um später die Induktionsvoraussetzung benutzen zu können:

$$H \cong \underbrace{H_1 \times ... \times H_i}_{H_\mathrm{I}} \times \underbrace{H_{i+1} \times ... \times H_{k+1}}_{H_\mathrm{II}}$$

Desweiteren sei σ_1 ein Element von H_I und σ_2 ein Element von H_II.
Mit den vorigen Bezeichnungen sei

$$\lambda_\mathrm{I} := \lambda_1 \cdot \lambda_2 \cdot ... \cdot \lambda_i$$

und

$$\lambda_\mathrm{II} := \lambda_{i+1} \cdot ... \cdot \lambda_{k+1}.$$

Außerdem definiert man

$$\begin{aligned} m_1 &:= p_1^{r_1} \cdot ... \cdot p_i^{r_i}, \\ m_2 &:= p_{i+1}^{r_{i+1}} \cdot ... \cdot p_{k+1}^{r_{k+1}}. \end{aligned}$$

Dann gilt

$$\begin{aligned} \lambda_\mathrm{I} \cdot \lambda_\mathrm{II} \cdot q &= q \cdot \lambda_K \\ &= (\sigma_1 \times \sigma_2)(\lambda_K) \\ &= (\sigma_1 \times \sigma_2)(\lambda_\mathrm{I} \cdot \lambda_\mathrm{II}) \\ &= \sigma_1(\lambda_\mathrm{I}) \cdot \sigma_2(\lambda_\mathrm{II}). \end{aligned}$$

Nach Voraussetzung sind die $\lambda_1, ..., \lambda_{k+1}$ ungleich Null, also kann man schreiben

$$\underbrace{\frac{\sigma_1(\lambda_\mathrm{I})}{\lambda_\mathrm{I}}}_{\in K_{m_1} = \mathbb{Q}(\zeta_{m_1})} = q \quad \cdot \underbrace{\frac{\lambda_\mathrm{II}}{\sigma_2(\lambda_\mathrm{II})}}_{\in K_{m_2} = \mathbb{Q}(\zeta_{m_2})} \qquad \in (K_{m_1} \cap K_{m_2}) = \mathbb{Q},$$

Die Quotienten $\frac{\sigma_j(\lambda_J)}{\lambda_J}$, wobei $j = J = 1, 2$ ist, sind also Elemente von $\mathbb{Q}$.
Damit erhält man

$$\lambda_\mathrm{I} = \frac{\sigma_1(\lambda_\mathrm{I})\sigma_2(\lambda_\mathrm{II})}{q\lambda_\mathrm{II}} = \underbrace{\frac{1}{q} \cdot \frac{\sigma_2(\lambda_\mathrm{II})}{\lambda_\mathrm{II}}}_{\in \mathbb{Q}} \cdot \sigma_1(\lambda_\mathrm{I}) \quad \overset{\text{Ind.Vor.}}{\Longleftrightarrow} \sigma_1 \in H_\mathrm{I},$$

woraus folgt

$$\sigma_2(\lambda_\mathrm{II}) = q \cdot \lambda_\mathrm{II} \overset{\text{Ind.Vor.}}{\Longleftrightarrow} \sigma_2 \in H_\mathrm{II}$$

Insgesamt erhält man also

$$\begin{aligned}(\sigma_1 \times \sigma_2)(\lambda_K) &\Longleftrightarrow q \cdot \sigma_1 \in H_{\mathrm{I}} \text{ und } \sigma_2 \in H_{\mathrm{II}} \\ &\Longleftrightarrow \sigma_1 \times \sigma_2 \in H\end{aligned}$$

Da aus $\sigma \in H$ auch $\sigma(\lambda_K) = \lambda_K$ folgt, muss gelten

$$\sigma(\lambda_K) = \lambda_K \quad \Leftrightarrow \quad \sigma \in H$$

und damit gilt auch

$$\mathbb{Q}(\lambda_K) = K \quad \Leftrightarrow \quad p_i \nmid \#H_i \quad \forall i \in \{1, ..., k\}.$$

Damit ist Satz 3.11 bewiesen. □

Nun wurden einige Untergruppen der Galoisgruppe G_n nicht behandelt, nämlich solche Untergruppen H, die nicht diagonal in G_n liegen. Um dies zu untersuchen, muss man sich detaillierter mit den Untergruppen von $(\mathbb{Z}/n\mathbb{Z})^*$ auseinandersetzen.
Schaut man sich die bisherigen Ergebnisse an, so stellt man fest, dass nirgends der Fall aufgetreten ist, dass $\mathbb{Q}(\lambda_K)$ ein echter Zwischenkörper der Erweiterung $K|\mathbb{Q}$ ist. Auch die Berechnungen am Computer lieferten keine Untergruppe H von G_n, für die dieser Fall eintritt. Es liegt also folgende Vermutung nahe:

3.13 Vermutung. *Die Spur λ_K ist entweder Null oder sie erzeugt den Körper K.*

Diese Vermutung habe ich mithilfe eines MAGMA-Programmes für die Führer $n = 1, ..., 1300$ überprüft und konnte keine Abweichung feststellen. Für die Fälle, dass n eine quadratfreie Zahl oder eine Primpotenz ist und für diagonale Untergruppen H wurde diese Vermutung in diesem Kapitel bereits bewiesen. Um sie vollständig zu beweisen, ist sicher eine gute Kenntnis der Struktur der Untergruppen von G_n vonnöten.

4 Die Ganzheitsringe der Zwischenkörper

Nachdem die Erzeugung der Teilkörper K der Körpererweiterung $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ betrachtet wurde, interessiert man sich nun für die Ganzheitsringe dieser Teilkörper. Es soll untersucht werden, in welchen Fällen auch der Ganzheitsring von λ_K erzeugt wird. Berechnet man für verschiedene Führer $n \in \mathbb{N}$ mithilfe eines Magma-Programmes den Index des Ganzheitsringes über $\mathbb{Z}[\lambda_K]$, so stellt man zunächst fest, dass dieser Index meist größer als 1 ist. Es lassen sich also nur wenige Aussagen treffen.

4.1 Satz. *Sei $n \in \mathbb{P} - \{2\}$ eine Primzahl. Erfüllt $H \subset G_p$ eine der beiden folgenden Eigenschaften*

1. *$H = \{\pm 1\}$*
2. *$H = \{s \in G_p \mid s \text{ ist Quadrat in } G_p = (\mathbb{Z}/p\mathbb{Z})^*\}$,*

so gilt für den Ganzheitsring $\mathcal{O}_K$ von K

$$\mathcal{O}_K = \mathbb{Z}[\lambda_K] = \mathbb{Z}[Tr_K^{K_p}(\zeta_p)].$$

4.2 Bemerkung. Wie sehen Elemente aus $\mathcal{O}_K$ aus?

$$\begin{array}{ccc} K_n = \mathbb{Q}(\zeta_p) & & \mathcal{O}_{K_n} = \mathbb{Z}[\zeta_p] \\ | & & | \\ K & & \mathcal{O}_K = \mathcal{O}_{K_n} \cap K \\ | & & | \\ \mathbb{Q} & & \mathcal{O}_{\mathbb{Q}} = \mathbb{Z} \end{array}$$

Elemente x aus $\mathbb{Z}[\zeta_p]$ sehen folgendermaßen aus:

$$x = \alpha_1\zeta_p + \alpha_2\zeta_p^2 + ... + \alpha_{p-1}\zeta_p^{p-1}, \quad \alpha_i \in \mathbb{Z} \quad \forall \quad i = 1, ..., p-1 \tag{36}$$

Die Koeffizienten α_i sind eindeutig bestimmt.
Die Elemente von $\mathcal{O}_K = K \cap \mathbb{Z}[\zeta_p]$ sind diejenigen $x \in \mathbb{Z}[\zeta_p]$, die von $H = \mathrm{Gal}(K_p|K)$ festgelassen werden.

Beweis. (zu Satz 4.1)
Wie bereits bewiesen wurde, werden alle Zwischenkörper K der Erweiterung $K_p|\mathbb{Q}$ von der Spur λ_K erzeugt. Sei zunächst $H = \{\pm 1\}$. Dann gilt

$$\lambda_K = \mathrm{Tr}_K^{K_n}(\zeta_p) = \zeta_p + \zeta_p^{-1}.$$

Nun ist zu zeigen, dass gilt

$$\mathcal{O}_K = \mathbb{Z}[\lambda_K].$$

Es ist klar, dass gilt $\mathbb{Z}[\lambda_K] \subset \mathcal{O}_K$, denn mit ζ_p ist auch $\zeta_p + \zeta_p^{-1} = \lambda_K$ ein Element von $\mathcal{O}_{K_n}$. Also ist $\lambda_K \in K \cap \mathcal{O}_{K_n} = \mathcal{O}_K$.
Damit ein $x \in \mathcal{O}_{K_n}$ wie in Gleichung (36) auch in K und damit in $\mathcal{O}_K$ liegt, muss x von allen Elementen aus H festgelassen werden. Wenden wir nun also die beiden Abbildungen

$$\begin{array}{rccc} \sigma_1: & K_p & \to & K_p, \\ & \zeta_p & \mapsto & \zeta_p^1 \end{array}$$

$$\begin{array}{rccc} \sigma_2: & K_p & \to & K_p, \\ & \zeta_p & \mapsto & \zeta_p^{-1} \end{array}$$

auf x an und fordern, dass x festgelassen wird, so erhält man

$$\begin{aligned} \sigma_1(x) &= \alpha_1\zeta_p + \alpha_2\zeta_p^2 + ... + \alpha_{p-1}\zeta_p^{p-1} \\ \sigma_2(x) &= \alpha_1\zeta_p^{p-1} + \alpha_2\zeta_p^{p-2} + ... + \alpha_{p-1}\zeta_p \overset{!}{=} x. \end{aligned}$$

Durch Koeffizientenvergleich erhält man

$$\begin{aligned} \alpha_1 &= \alpha_{p-1} \\ \alpha_2 &= \alpha_{p-2} \\ &\vdots \\ \alpha_{\frac{p-1}{2}} &= \alpha_{\frac{p+1}{2}} \end{aligned}$$

Also hat $x \in \mathcal{O}_K$ die Gestalt

$$x = \alpha_1 \underbrace{(\zeta_p^{p-1} + \zeta_p)}_{=:\eta_1} + \alpha_2 \underbrace{(\zeta_p^{p-2} + \zeta_p^2)}_{=:\eta_2} + ... + \alpha_{\frac{p-1}{2}} \underbrace{(\zeta_p^{\frac{p+1}{2}} + \zeta_p^{\frac{p-1}{2}})}_{=:\eta_{\frac{p-1}{2}}}.$$

Die $\eta_i,\ i \in 1, ..., \frac{p-1}{2}$, erzeugen also den Ganzheitsring $\mathcal{O}_K$ von K.
Es bleibt zu zeigen, dass diese Erzeuger Elemente von $\mathbb{Z}[\lambda_K]$ sind.
Dies lässt sich durch Induktion nach i, also nach der Nummer des Erzeugers, beweisen:
Induktionsanfang: $i = 1$
Es ist klar, dass

$$\eta_1 = \zeta_p + \zeta_p^{p-1} = \zeta_p + \zeta_p^{-1} = \lambda_K$$

in $\mathbb{Z}[\lambda_K]$ liegt.
Induktionsvoraussetzung: Sei für ein beliebiges i mit $1 \leq i < \frac{p-1}{2}$ gezeigt:

$$\zeta_p^{p-i} + \zeta_p^i \in \mathbb{Z}[\lambda_K],$$

also $\zeta_p^{p-i} + \zeta_p^i$ lässt sich als Linearkombination der $\zeta_p^{p-k} + \zeta_p^k$ mit $1 \leq k < i$ schreiben. Betrachte dazu

$$\begin{aligned}(\zeta_p + \zeta_p^{p-1})^i &= \sum_{k=0}^{i} \binom{i}{k} \zeta_p^k (\zeta_p^{p-1})^{i-k} \\ &= \sum_{k=0}^{i} \binom{i}{k} \zeta_p^k \zeta_p^{(p-1)(i-k)}) \\ &= \sum_{k=0}^{i} \binom{i}{k} \zeta_p^k \zeta_p^{k-i} \\ &= \sum_{k=0}^{i} \binom{i}{k} \zeta_p^{2k-i}\end{aligned}$$

Letzere Summe ist eine Linearkombination der $\zeta_p^k + \zeta_p^{-k}$, $1 \leq k < i$.
Induktionsschritt: Zu zeigen ist nun, dass sich $\zeta_p^{-i-1} + \zeta_p^{i+1}$ als Linearkombination der $\zeta_p^{-k} + \zeta_p^k$ mit $1 \leq k \leq i$ schreiben lässt. Es gilt

$$\begin{aligned}(\zeta_p + \zeta_p^{-1})^{i+1} &= \sum_{k=0}^{i+1} \binom{i+1}{k} \zeta_p^k (\zeta_p^{-1})^{i+1-k} \\ &= \sum_{k=0}^{i+1} \binom{i+1}{k} \zeta_p^{2k-i-1} \\ &= \zeta_p^{-i-1} + \zeta_p^{i+1} + \sum_{k=1}^{i} \binom{i+1}{k} \zeta_p^{2k-i-1}\end{aligned}$$

Stellt man diese Gleichung um, so erhält man

$$\zeta_p^{-i-1} + \zeta_p^{i+1} = (\zeta_p + \zeta_p^{-1})^{i+1} - \sum_{k=1}^{i} \binom{i+1}{k} \zeta_p^{2k-i-1},$$

was eine Linearkombination der $\zeta_p^k + \zeta_p^{-k}$, $1 \leq k \leq i$, ist.
Also gilt

$$\zeta_p^{-i-1} + \zeta_p^{i+1} \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$$

und damit auch

$$\mathcal{O}_K = \mathcal{O}_{K_n} \cap K \subset \mathbb{Z}[\lambda_K].$$

Insgesamt gilt also $\mathcal{O}_K = \mathbb{Z}[\lambda_K]$.

Betrachten wir nun den Fall, dass H die Menge aller Quadrate in G_p ist. Dann gilt für den Erzeuger λ_K von K

$$\lambda_K = \mathrm{Tr}_K^{K_n}(\zeta_p) = \sum_{\substack{i \text{ Quadrat} \\ \text{in } G_p}} \zeta_p^i$$

und es ist zu zeigen, dass λ_K auch den Ganzheitsring erzeugt.
Wie im ersten Fall ist es auch hier klar, dass gilt $\mathbb{Z}[\lambda_K] \subset \mathcal{O}$.
Sei also nun $x \in \mathcal{O}_K = \mathcal{O}_{K_n} \cap K$. Damit ein $x \in \mathcal{O}_{K_n}$ in K liegt, muss es von allen Elementen aus H auf sich selbst abgebildet werden.
Es gilt

$$H = \{\sigma_i \in G_p \mid i \text{ ist Quadrat in } (\mathbb{Z}/p\mathbb{Z})^*\},$$

wobei die σ_i auf folgende Weise abbilden:

$$\begin{array}{rccc} \sigma_i : & K_p & \to & K_p \\ & \zeta_p & \mapsto & \zeta_p^i \end{array}$$

Außerdem ist die Anzahl der Elemente in H gerade $\frac{p-1}{2}$, da es in $(\mathbb{Z}/p\mathbb{Z})^*$ genauso viele Quadrate wie Nichtquadrate gibt.
Definieren wir nun die Abbildung

$$\begin{array}{rccc} \phi : & (\mathbb{Z}/p\mathbb{Z})^* & \to & (\mathbb{Z}/p\mathbb{Z})^*, \\ & \overline{b} & \mapsto & \overline{ab}, \end{array} \tag{37}$$

wobei $\overline{a}$ ein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^*$ ist, so bildet ϕ Quadrate auf Quadrate ab und Nichtquadrate auf Nichtquadrate.
Wendet man also ein $\sigma_i \in H$ auf ein $x \in \mathcal{O}_{K_n}$ an, so werden die ζ_p^i, für die i ein Quadrat in G_p ist, untereinander vertauscht und diejenigen ζ_p^i, für die i kein Quadrat ist, werden ebenfalls untereinander vertauscht. Das bedeutet für x, dass alle Koeffizienten, die vor einem ζ_p^i mit quadratischem Exponenten stehen, gleich sein müssen. Auch die übrigen Koeffizienten müssen gleich sein.
Also muss gelten

$$\begin{array}{ll} \alpha_1 = \alpha_i & \forall\ i = \text{Quadrat in } (\mathbb{Z}/p\mathbb{Z})^* \\ \alpha_j = \alpha_{ij} & \forall\ i = \text{Quadrat}, j = \text{Nichtquadrat in } (\mathbb{Z}/p\mathbb{Z})^* \end{array}$$

Also gilt, wenn j nicht quadratischer Rest modulo p ist,

$$x = \alpha_1 \cdot \Big(\sum_{\substack{i \text{ Quadrat} \\ \text{in } G_p}} \zeta_p^i \Big) + \alpha_j \cdot \Big(\sum_{\substack{i \text{ Nichtquadrat} \\ \text{in } G_p}} \zeta_p^i \Big) \tag{38}$$

$$= \alpha_1 \cdot \underbrace{\lambda_K}_{\in \mathbb{Z}[\lambda_K]} + \alpha_j \cdot \underbrace{(-1 - \lambda_K)}_{\in \mathbb{Z}[\lambda_K]} \tag{39}$$

wobei Gleichung (39) durch Einsetzen von ζ_p in das Minimalpolynom von ζ_p entsteht:

$$\begin{aligned} 0 &= \sum_{0 \le i \le p-1} \zeta_p^i \\ &= 1 + \sum_{i \text{ Quadrat}} \zeta_p^i + \sum_{i \text{ Nichtquadrat}} \zeta_p^i \end{aligned}$$

Aus Gleichung (39) folgt also, dass $\mathcal{O}_K \subset \mathbb{Z}[\lambda_K]$ gilt und insgesamt $\mathcal{O}_K = \mathbb{Z}[\lambda_K]$ gilt. □

4.3 Zusammenfassung. Im Großen und Ganzen kann man sagen, dass λ_K den Ganzheitsring $\mathcal{O}_K$ von K nicht erzeugt. Für den Fall, dass der Führer $n = p$ eine Primzahl ist, so werden die Ganzheitsringe der Teilkörper K, die zu den Untergruppen $H = \{\pm 1\}$ oder $H = \{x \in G_p \mid x \text{ ist Quadrat in } G_p\}$ gehören, von λ_K erzeugt.

Berechnet man mit MAGMA den Index von $\mathbb{Z}[\lambda_K]$ im Ganzheitsring $\mathcal{O}_K$ von K, so erhält man teilweise recht große Werte. Die folgende Tabelle verdeutlicht dies für $p = 53$.

$\#(H) = [K_{53} : K]$	$[\mathcal{O}_K : \mathbb{Z}[\lambda_K]]$
26	1
13	13
4	10007415161
2	1

Tabelle 1: Indizes von $\mathbb{Z}[\lambda_K]$ in $\mathcal{O}_K$ für $\mathbb{Q} \subset K \subset K_{53}$

Dabei ist die Untergruppe H mit $[\mathcal{O}_K : \mathbb{Z}[\lambda_K]] = 1$ im Fall $[K_{53} : K] = 2$ die Gruppe $\{\pm 1\}$ und im Fall $[K_{53} : K] = 26$ die Gruppe der Quadrate in $(\mathbb{Z}/p\mathbb{Z})^*$.

5 Eigenschaften des Minimalpolynoms von λ_K im Fall $\lambda_K \neq 0$ und $O_K = \mathbb{Z}[\lambda_K]$

In den vorangegangenen Kapiteln haben wir uns mit der Erzeugung der Teilkörper K sowie mit den Ganzheitsringen dieser Körper beschäftigt. Die Spur λ_K scheint entweder den Körper K zu erzeugen oder sie ist ist Null. Tritt der erste Fall ein, so kann man nun das Minimalpolynom von λ_K betrachten und einige Eigenschaften bestimmen. So ist es beispielsweise interessant, wie die Koeffizienten des Minimalpolynoms aussehen. Wir beschäftigen uns hier nur mit primen Führern n:

5.1 Bemerkung. Im ganzen Kapitel sei $n = p \in \mathbb{P}$ eine ungerade Primzahl. Also werden nach Satz 3.1 alle Teilkörper K von $K_p = \mathbb{Q}(\zeta_p)$ von $\lambda_K = \mathrm{Tr}_K^{K_n}(\zeta_n)$ erzeugt, λ_K ist also ungleich Null.

5.2 Bemerkung. Sei

$$f(X) = \sum_{i=0}^{k} \alpha_i X^i \tag{40}$$

das Minimalpolynom von λ_K. Für den Grad des Minimalpolynoms f gilt

$$k = \deg(f) = [K : \mathbb{Q}] = \frac{[K_p : \mathbb{Q}]}{[K_p : K]} = \frac{\#G}{\#H}.$$

Außerdem gilt für den Koeffizienten α_{k-1}

$$\alpha_{k-1} = -\mathrm{Tr}_{\mathbb{Q}}^{K}(\lambda_K).$$

5.1 Erster Fall: $H = \{\pm 1\}$

5.3 Satz. *Sei $H = \{\pm 1\}$. Dann gilt für die Koeffizienten des Minimalpolynoms der Spur λ_K:*

1. $\alpha_{k-1} = 1$,
2. $\alpha_{k-2} = -\frac{p-3}{2}$,
3. $\alpha_{k-3} = -\frac{p-3}{2} + 1 = -\frac{p-5}{2}$.

Beweis. Für das Minimalpolynom f von λ_K gilt:

$$\begin{aligned} f(X) &= \prod_{\sigma_i \in G/H} (X - \sigma_i(\lambda_K)) \\ &= \prod_{i \in \{1,\dots,\frac{p-1}{2}\}} (X - (\zeta_p^i + \zeta_p^{-i})) \\ &= X^{\frac{p-1}{2}} + (\underbrace{\sum_{i \in \{1,\dots,\frac{p-1}{2}\}} (\zeta_p^i + \zeta_p^{-i})}_{=\mathrm{Tr}_{\mathbb{Q}}^K(\lambda_K)}) X^{\frac{p-3}{2}} \\ &\quad + (\underbrace{\sum_{1 \le i < j \le \frac{p-1}{2}} (\zeta_p^i + \zeta_p^{-i})(\zeta_p^j + \zeta_p^{-j})}_{=\alpha_{k-2}}) X^{\frac{p-5}{2}} \\ &\quad + \quad ... \end{aligned}$$

1.) ist trivial: Nach Bemerkung 5.2 gilt

$$\alpha_{k-1} = -\mathrm{Tr}_{\mathbb{Q}}^K(\lambda_K)$$

und mit Korollar 3.9 folgt für $k = 1$ die Behauptung.
Um 2.) zu beweisen, betrachtet man zuerst das Minimalpolynom $g(X)$ von ζ_p,

$$g(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + ... + X + 1 \tag{41}$$

mit $g(\zeta_p) = 0$. Durch Einsetzen von ζ_p in (41) erhält man

$$\underbrace{\zeta_p^{p-1} + ... + \zeta_p}_{p-1 \text{ Summanden}} = -1. \tag{42}$$

Um α_{k-2} zu berechnen, benutzt man nun die Siebformel:

$$\begin{aligned}
&\sum_{1\le i<j\le \frac{p-1}{2}} (\zeta_p^i+\zeta_p^{-i})(\zeta_p^j+\zeta_p^{-j}) \\
&= \frac{1}{2}\Big(\sum_{1\le i,j\le \frac{p-1}{2}} (\zeta_p^i+\zeta_p^{-i})(\zeta_p^j+\zeta_p^{-j})\Big) - \sum_{1\le i\le \frac{p-1}{2}} (\zeta_p^i+\zeta_p^{-i})^2\Big) \\
&= \frac{1}{2}\Big(\sum_{1\le i\le \frac{p-1}{2}}\sum_{1\le j\le \frac{p-1}{2}} (\zeta_p^i+\zeta_p^{-i})(\zeta_p^j+\zeta_p^{-j}) - \sum_{1\le i\le \frac{p-1}{2}} (\zeta_p^{2i}+2+\zeta_p^{-2i})\Big) \\
&= \frac{1}{2}\Big(\underbrace{\sum_{1\le i\le \frac{p-1}{2}} (\zeta_p^i+\zeta_p^{-i})}_{=-1 \text{ nach (42)}}\underbrace{\sum_{1\le j\le \frac{p-1}{2}} (\zeta_p^j+\zeta_p^{-j})}_{=-1 \text{ nach (42)}} - \underbrace{\sum_{1\le i\le \frac{p-1}{2}} (\zeta_p^{2i}+\zeta_p^{-2i})}_{=-1 \text{ nach (42)}} - \sum_{1\le i\le \frac{p-1}{2}} 2\Big) \\
&= \frac{1}{2}((-1)\cdot(-1)-(-1)-(\frac{p-1}{2})\cdot 2) \\
&= -\frac{p-3}{2}
\end{aligned}$$

3.) erhält man auf dieselbe Art und Weise, die Rechnung ist jedoch viel aufwendiger und wird daher hier weggelassen. □

Im Allgemeinen kann man ähnliche Aussagen sicher zu allen Koeffizienten des Minimalpolynoms von λ_K treffen. Die Berechnung wird jedoch immer aufwendiger, je kleiner die Nummer des Koeffizienten wird. Der Beweis zu Satz 5.3, Aussage (3), war insofern leicht, da man sich keine Gedanken machen musste, wie oft der Summand $\zeta_p^{zp}=1,\ z\in\mathbb{Z}$, auftritt, da hier der höchste Exponent einer Potenz von ζ_p die Zahl $p-1$ war. Da außerdem alle Koeffizienten von f in $\mathbb{Q}$ und sogar in $\mathbb{Z}$ liegen, denn λ_K ist eine ganze Zahl in K, müssen sich die Potenzen von ζ_p, die in der Summe vorkommen, so aufaddieren, dass eine ganze Zahl herauskommt. Dazu nutzt man die Identität (42): Die Summe von $p-1$ verschiedenen Summanden ergibt -1. Die Anzahl der auftretenden Summanden, die alle eine Potenz von ζ_p mit Exponenten zwischen 1 und $p-1$ sind, ist ein Vielfaches von $p-1$.
Um α_{k-i} zu berechnen, muss man die Summe

$$\alpha_{k-i} \quad = (-1)^i \sum_{1\le j_1<\ldots<j_i\le \frac{p-1}{2}} \prod_{1\le l\le i} (\zeta_p^{j_l}+\zeta_p^{-j_l}) \tag{43}$$

berechnen. Wie man leicht sieht, treten ab $i\ge 3$ bereits Summanden auf, die gleich 1 sind. Ist beispielsweise $n=p=11$, so erhält man, wenn man obige Summe für

$(j_1, j_2, j_3) = (1, 2, 3)$ auswertet:

$$\begin{aligned}\prod_{1\le l\le 3}(\zeta_p^{j_l}+\zeta_p^{-j_l}) &= (\zeta_p+\zeta_p^{-1})(\zeta_p^2+\zeta_p^{-2})(\zeta_p^3+\zeta_p^{-3})\\ &= \zeta_{11}^6+\underbrace{\zeta_{11}^0}_{=1}+\zeta_{11}^2+\zeta_{11}^{-4}+\zeta_{11}^4+\zeta_{11}^{-2}+\underbrace{\zeta_{11}^0}_{=1}+\zeta_{11}^{-6}\\ &= \zeta_{11}^6+1+\zeta_{11}^2+\zeta_{11}^{-4}+\zeta_{11}^4+\zeta_{11}^{-2}+1+\zeta_{11}^{-6}\end{aligned}$$

Die Anzahl der vorkommenden Einsen ist nicht leicht zu bestimmen. Klar ist jedoch, dass die gesamte Summe eine ganze Zahl ergeben muss. Berücksichtigt man dies, so kann man die Koeffizienten modulo p bestimmen:

5.4 Satz. *Die Koeffizienten des Minimalpolynoms f von λ_K für $H = \{\pm 1\}$ nehmen modulo p die Werte*

$$\alpha_{k-i} \equiv (-1)^i \cdot 2^i \binom{\frac{p-1}{2}}{i} \mod p$$

an.

Beweis. Die Aussage aus 5.4 erhält man durch Abzählen der Summanden. Zuerst überlegt man sich, wieviele Summanden es in Gleichung (43) insgesamt gibt, wenn man die Summe ausschreibt ohne die Summanden zusammenzufassen.
Die Anzahl der i-Tupel aus $\{1, ..., \frac{p-1}{2}\}$ ist $\binom{\frac{p-1}{2}}{i}$.
Für jedes Tupel erhält man 2^i Summanden, da jeder Faktor aus zwei Summanden besteht und es i Faktoren gibt. Insgesamt erhält man also für die Gesamtzahl der Summanden die Zahl

$$2^i \binom{\frac{p-1}{2}}{i}.$$

Diese $2^i\binom{\frac{p-1}{2}}{i}$ Summen werden indiziert durch die Menge

$$\mathcal{S} := \{S \subset (\mathbb{Z}/p\mathbb{Z})^* \mid \#(S) = i,\ S \cap (-S) = \emptyset\}$$

Für $s \in \mathcal{S}$ sei

$$m(S) := \sum_{x\in S} x.$$

Der zu einer Menge S gehörende Summand ist

$$\zeta_p^{\sum_{x\in S} x} = \zeta_p^{m(S)}.$$

Betrachte nun die Abbildung

$$\begin{array}{ccc} \mathcal{S} & \longrightarrow & \mathbb{Z}/p\mathbb{Z}, \\ S & \longmapsto & m(S). \end{array}$$

Die Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ operiert auf $\mathcal{S}$ durch Multiplikation $S \mapsto yS$ und es gilt $m(yS) = ym(s)$, was man durch Einsetzen schnell überprüft.
Also ist $\#(S \in \mathcal{S} \mid m(S) = y)$ für $y \neq 0$ unabhängig von $y \in \mathbb{Z}/p\mathbb{Z}$. Dementsprechend zerfällt $\{S \in \mathcal{S} \mid m(S) \neq 0\}$ in lauter Bahnen $\mathcal{L}$ der Länge $p-1 = \#(\mathbb{Z}/p\mathbb{Z})^*$, in denen jeweils alle Elemente von $(\mathbb{Z}/p\mathbb{Z})^*$ als $m(s)$ auftreten. Nach Gleichung (42) gilt

$$\sum_{S \in \mathcal{L}} \zeta_p^{m(S)} = -1.$$

Also gilt insgesamt

$$(-1)^i \alpha_{k-i} = \sum_{S \in \mathcal{S}} \zeta_p^{m(S)} = \underbrace{\sum_{\substack{S \text{ mit} \\ m(S)=0}}}_{=a} + (-1) \cdot \underbrace{\#(\text{Bahnen } \mathcal{L} \text{ aus } S \text{ mit } m(S) \neq 0)}_{=b} \tag{44}$$

Also ist a die Anzahl der Summanden, die $1 = \zeta_p^{zp},\ z \in \mathbb{Z}$ sind und sei b die Zahl, die angibt, wie oft die Summe $\sum_{j=1}^{p-1} \zeta_p^j = -1$ vorkommt. Dann gibt es also

$$a \cdot 1 + b \cdot (p-1) = 2^i \binom{\frac{p-1}{2}}{i} \tag{45}$$

Summanden.
Nun sieht man, dass die linke Seite von (44) und die rechte Seite von (45) kongruent sind modulo p. Es gilt also

$$(-1)^i \alpha_{k-i} \equiv 2^i \binom{\frac{p-1}{2}}{i} \bmod p.$$

Multipliziert man diese Gleichung noch auf beiden Seiten mit $(-1)^i$, so erhält man die Behauptung.

□

5.5 Bemerkung. Dies kann man noch umformen zu

$$\alpha_{k-i} \equiv \frac{(2i)!}{(i!)^2 \cdot 2^i} \bmod p.$$

5.6 Korollar. *Im Fall $H = \{\pm 1\}$ gilt für die Koeffizienten α_{k-i} des Minimalpolynoms f von λ_K*

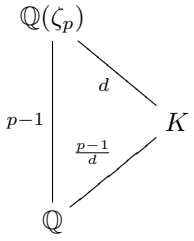
$$\alpha_{k-i} \neq 0 \quad \forall\ 0 \leq i \leq k.$$

Beweis. Aus dem Bemerkung 5.5 folgt $\alpha_{k-i} \neq 0 \bmod p$:

$$p \mid \frac{(2i)!}{(i!)^2 \cdot 2^i} \quad \Leftrightarrow \quad p \mid (2i)!,$$

damit die Primzahl p jedoch ein Teiler von $(2i)!$ sein kann, muss $2i > p$ gelten. Aus $i \leq \frac{p-1}{2}$ folgt allerdings $2i \leq p-1$. Also kann p die Zahl $(2i)!$ nicht teilen und damit kann α_{k-i} nicht Null modulo p sein.
Daraus folgt $\alpha_{k-i} \neq 0$, denn sonst wäre auch $\alpha_{k-i} \equiv 0 \bmod p$. □

5.7 Bemerkung. Ähnliche Aussagen wie in Satz 5.4 kann man auch für das Minimalpolynom von λ_K für den Fall $[K_p : K] = d$ mit $d|n$ treffen:



Dann bestehen die Koeffizienten α_{k-i} aus jeweils $d^i\binom{\frac{p-1}{d}}{i}$ Summanden und man kann die gleiche Rechnung durchführen wie im Fall $d = 2$.

Lässt man sich das Minimalpolynom von λ_K im Fall $H = \{\pm 1\}$ ausgeben, zum Beispiel mithilfe eines MAGMA-Programmes, so kann man folgende Regelmäßigkeiten bei den Koeffizienten α_0 und α_1 feststellen:

5.8 Vermutung. *Für die Koeffizienten α_0 und α_1 gilt*

$$\alpha_0 = \begin{cases} +1 & \textit{falls } p \equiv 1, 3 \bmod 8 \\ -1 & \textit{falls } p \equiv 5, 7 \bmod 8 \end{cases}$$

$$\alpha_1 = \begin{cases} -\frac{p-1}{4} & \textit{falls } p \equiv 1 \bmod 8 \\ \frac{p+1}{4} & \textit{falls } p \equiv 3 \bmod 8 \\ \frac{p-1}{4} & \textit{falls } p \equiv 5 \bmod 8 \\ -\frac{p+1}{4} & \textit{falls } p \equiv 1 \bmod 8 \end{cases}$$

In der folgenden Tabelle sind die Minimalpolynome von λ_K im Fall $H = \{\pm 1\}$ für einige Primzahlen p aufgelistet:

$p \in \mathbb{P}$	Minimalpolynom von λ_K
5	$X^2 + X - 1$
7	$X^3 + X^2 - 2X - 1$
11	$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$
13	$X^6 + X^5 - 5X^4 - 4X^3 + 6X^2 + 3X - 1$
17	$X^8 + X^7 - 7X^6 - 6X^5 + 15X^4 + 10X^3 - 10X^2 - 4X + 1$
19	$X^9 + X^8 - 8X^7 - 7X^6 + 21X^5 + 15X^4 - 20X^3 - 10X^2 + 5X + 1$

Tabelle 2: Minimalpolynome für $H = \{\pm 1\}$

5.2 Zweiter Fall: $H = \{$Quadrate in $G_p\}$

Betrachten wir nun das Minimalpolynom f von λ_K für den Fall, dass H die Menge aller Quadrate in G_p ist.
Sei also ab jetzt $H = \{s \in G_p \mid s \text{ ist Quadrat in } G_p = (\mathbb{Z}/p\mathbb{Z})^*\}$. Für den Grad von f gilt in diesem Fall

$$\deg(f) = \frac{\#G}{\#H} = \frac{p-1}{\frac{p-1}{2}} = 2,$$

also hat f die Form

$$f(X) = X^2 + \alpha X + \beta. \tag{46}$$

Über die Koeffizienten α und β kann man nun die folgenden Aussagen treffen:

5.9 Satz. *Mit Bezeichnungen wie in (46) gilt für die Koeffizienten des Minimalpolynoms f von λ_K:*

$$\alpha = 1$$
$$\beta = \begin{cases} -\frac{p-1}{4} & p \equiv 1 \bmod 4 \\ \frac{p+1}{4} & p \equiv 3 \bmod 4 \end{cases}$$

5.10 Bemerkung. Betrachtet man die obige Fallunterscheidung für β, so sieht man, dass man die gleichen Fälle beim Spezialfall des quadratischen Reziprozitätsgesetzes hat. Es gilt für $p \neq 2$ (siehe auch [SP07], Satz 8.21)

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 1 \bmod 4 \end{cases}. \tag{47}$$

Sei nun n ein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^*$. Dann gilt

$$\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right) \cdot \underbrace{\left(\frac{n}{p}\right)}_{1} = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 3 \bmod 4 \end{cases}. \tag{48}$$

Das heißt also, dass $-n$ ebenfalls ein Quadrat modulo p ist, wenn $p \equiv 1 \bmod 4$ ist, beziehungsweise, dass $-n$ keines ist, wenn $p \equiv 3 \bmod 4$ gilt.
Dies wird im folgenden Beweis benötigt.

Beweis. zu Satz 5.9
Das Minimalpolynom f von λ_K hat die Form

$$f(X) = (X - \lambda_K)(X - \sigma(\lambda_K)) = X^2 - (\lambda_K + \sigma(\lambda_K))X + \lambda_K \cdot \sigma(\lambda_K), \tag{49}$$

wobei die Abbildung σ die komplexe Konjugation ist:

$$\begin{array}{rccll} \sigma: & K & \to & K, & \\ & \zeta_p & \mapsto & \zeta_p^a, & a \text{ ein beliebiges Nichtquadrat in } (\mathbb{Z}/p\mathbb{Z})^* \end{array}$$

Es gilt

$$\lambda_K = \sum i \in H \zeta_p^i.$$

Betrachten wir nun zuerst den Fall, dass $p \equiv 3 \bmod 4$ ist.
Dann ist nach dem quadratischen Reziprozitätsgesetz (...) die Zahl -1 kein Quadrat modulo p. Definiere also

$$\begin{array}{rccc} \sigma: & K & \to & K, \\ & \zeta_p & \mapsto & \zeta_p^{-1}. \end{array}$$

Aus $i \in H$, also daraus, dass i ein Quadrat modulo p ist, folgt nun, dass $-i$ kein Quadrat modulo p ist, siehe auch Bemerkung 5.10. Daher gilt $-i \in G_p - H$.
Damit folgt für den Koeffizienten β

$$\begin{aligned} \beta &= \lambda_K \cdot \sigma(\lambda_K) \\ &= (\sum_{i \in H} \zeta_p^i) \cdot (\sum_{i \in H} \zeta_p^{-i}) \\ &= (\sum_{\substack{i \,\square \text{ in} \\ (\mathbb{Z}/p\mathbb{Z})^*}} \zeta_p^i) \cdot (\sum_{\substack{j \,\not\square \text{in} \\ (\mathbb{Z}/p\mathbb{Z})^*}} \zeta_p^j). \end{aligned}$$

β hat also insgesamt $\left(\frac{p-1}{2}\right)^2$ Summanden, von denen $\frac{p-1}{2}$ bereits $1 = \zeta_p^i \cdot \zeta_p^{-i}$ sind. Zieht man von der Gesamtzahl der Summanden die Summanden ab, die gleich 1 sind, so bleiben $\left(\frac{p-1}{2}\right)^2 - \frac{p-1}{2}$ übrig. Da diese restlichen Summanden eine ganze Zahl ergeben

müssen, addieren sich jeweils $p-1$ passende Summanden wie in (42) zu -1 auf. Also gilt für β

$$\begin{aligned}\beta &= \left(\frac{p-1}{2}\right)\cdot 1 + \left(\frac{\left(\frac{p-1}{2}\right)^2 - \frac{p-1}{2}}{p-1}\right)\cdot(-1)\\ &= \frac{p-1}{2} - \left(\frac{p-1}{4} - \frac{1}{2}\right)\\ &= \frac{p+1}{4}.\end{aligned}$$

Nun fehlt noch der Fall $p \equiv 1 \bmod 4$.
Nach Bemerkung 5.10, Gleichung (48), ist -1 nun ein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^*$. Man erhält

$$\beta = \Big(\sum_{\substack{i \ \square \text{ in} \\ (\mathbb{Z}/p\mathbb{Z})^*}} \zeta_p^i\Big)\cdot\Big(\sum_{\substack{j \ \not\square \text{ in} \\ (\mathbb{Z}/p\mathbb{Z})^*}} \zeta_p^j\Big).$$

Wieder besitzt β insgesamt $\left(\frac{p-1}{2}\right)^2$ Summanden. Von diesen Summanden ist diesmal jedoch keiner gleich 1:

$$\zeta_p^{i+j} = 1 \quad \Leftrightarrow \quad i+j \equiv 0 \bmod p \quad i \equiv -j \bmod p,$$

Nach Voraussetzung ist i ein Quadrat und j ein Nichtquadrat, also folgt mit Gleichung (48), dass $-j$ ebenfalls kein Quadrat modulo p ist. Also kann nicht gelten $i \equiv -j \bmod p$. Es können dementsprechend keine Summanden auftreten, die gleich 1 sind. β gibt also an, wie oft die Summe $\zeta_p + ... + \zeta_p^{p-1}$ auftritt. Teilt man also die Anzahl der Summanden durch $p-1$, so erhält man

$$\beta = \frac{(\frac{p-1}{2})^2}{p-1}\cdot(-1) = -\frac{p-1}{4}.$$

Die Aussage für den Koeffizienten α ist klar, wir wissen bereits

$$\alpha = -\mathrm{Tr}_{\mathbb{Q}}^K(\lambda_K) \overset{3.9}{=} -(-1) = 1.$$

Damit ist also Satz 5.9 bewiesen. □

Abschließend werden in der folgenden Tabelle auch für die Untergruppe der Quadrate aus G_p einige Beispiele für das Minimalpolynom von λ_K aufgeführt.

$p \in \mathbb{P}$	Minimalpolynom von λ_K
7	$X^2 + X + 2$
11	$X^2 + X + 3$
13	$X^2 + X - 3$
17	$X^2 + X - 4$
19	$X^2 + X + 5$
23	$X^2 + X + 6$
29	$X^2 + X - 7$
31	$X^2 + X + 8$

Tabelle 3: Minimalpolynome für $H = \{\text{Quadrate in } G_p\}$

6 Zusammenfassung und Ausblick

Abschließend sollen nun die Ergebnisse dieser Arbeit noch einmal zusammengefasst werden. Für den Führer n wurden in Kapitel 3 verschiedene Fälle betrachtet, bei denen es jeweils bestimmte Bedingungen gab, damit ein Zwischenkörper K der Erweiterung $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ von der Spur λ_K, also der Spur der Einheitswurzel ζ_n in K, erzeugt wird. Diese Bedingungen werden im Folgenden noch einmal kurz zusammengestellt.

Ist $n = p$ eine **Primzahl**, so werden alle Zwischenkörper K von $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ von der Spur der p-ten Einheitswurzel ζ_p in K erzeugt.
Ebenso verhält es sich, falls n **quadratfrei** ist. Auch in diesem Fall können alle Zwischenkörper K von λ_K erzeugt werden.
Sei n nun eine **Primpotenz**, also $n = p^r$ für ein $r \in \mathbb{N}$. Dann wird ein Zwischenkörper K genau dann von der Spur λ_K erzeugt, wenn die Zahl $\frac{n}{p} + 1 = p^{r-1} + 1$ nicht in $H = \mathrm{Gal}(K_n|K)$ liegt.

In diesen drei Spezialfällen ist die Situation also klar. Lässt sich n keinem dieser Fälle zuordnen, so wurde nur zu einem bestimmten Typ von Untergruppen H eine Aussage gemacht, nämlich zu Untergruppen, die diagonal in der Galoisgruppe G_n von $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ liegen. Ist $n = p_1^{r_1} \cdot ... \cdot p_k^{r_k}$ mit paarweise verschiedenen Primzahlen p_i, $i = 1, ..., k$, und $H = H_1 \times ... \times H_k$ diagonal in G_n mit $H_k \subset \mathbb{Z}/p_i^{r_i}\mathbb{Z}$, so wird der zu H gehörige Zwischenkörper K genau dann von λ_K erzeugt, wenn in keinem der H_i das Element $\frac{n}{p} + 1$ enthalten ist.
Für Untergruppen, die nicht diagonal in G_n liegen, wurden keine Aussagen getroffen. Will man dennoch weitere Aussagen hierzu treffen, wird man sich zuerst mit den verschiedenen Untergruppen der Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ beschäftigen müssen.
Ich vermute jedoch, dass insgesamt die Aussage „Die Spur λ_K ist entweder Null oder sie erzeugt den Körper K“ auch für die in dieser Arbeit nicht betrachteten Untergruppen H von G_n zutrifft.

In Kapitel 4 wurde für prime Führer $n = p \in \mathbb{P}$ gezeigt, dass die Ganzheitsringe der Zwischenkörper K von λ_K erzeugt werden, wenn die zu K gehörige Untergruppe H entweder nur 1 und -1 oder alle Quadrate aus G_p enthält.
Im Allgemeinen scheint λ_K den Ganzheitsring jedoch nicht zu erzeugen.

Zuletzt wurde noch das Minimalpolynom der Spur λ_K betrachtet. Dies macht natürlich nur Sinn, wenn $\lambda_K \neq 0$ ist. Ich habe mich in meinen Betrachtungen auf die Fälle beschränkt, in denen auch der Ganzheitsring von K von λ_K erzeugt wird, also für $n \in \mathbb{P}$ und $H = \{\pm 1\}$ oder $H = \{\text{Quadrate in } G_n\}$. Beispielsweise wurde gezeigt, dass alle Koeffizienten des Minimalpolynoms von λ_K in beiden betrachteten Fällen ungleich Null sind.

Diese Arbeit ließe sich beispielsweise durch Vervollständigung der Aussagen über die Erzeugung der Zwischenkörper K durch die Spur λ_K von ζ_n in K ergänzen. Eine weitere Richtung könnte die Suche nach anderen Kandidaten für Erzeuger sein. Die Norm der Einheitswurzel ζ_n in K wäre vielleicht ein solcher Kandidat, auch wenn bereits klar

ist, dass nur ein Kreisteilungskörper, der zwischen $\mathbb{Q}$ und $\mathbb{Q}(\zeta_n)$ liegt, infrage kommt (denn die Norm ist als Produkt von Einheitswurzeln wieder eine Einheitswurzel oder sogar 1). Andere Koeffizienten des Minimalpolynoms von ζ_n in K sind ebenfalls Kandidaten, da K bekanntermaßen von den Koeffizienten dieses Polynoms erzeugt wird.
Eine weitere interessante Frage wäre die Frage nach den Erzeugern der Ganzheitsringe der Zwischenkörper.
Da in Kapitel 5 nur zwei ganz spezielle Fälle betrachtet wurden, gibt es auch hier noch vieles zu erforschen. Beispielsweise könnte man eine Abschätzung für die Größe der Koeffizienten des Minimalpolynoms von λ_K angeben.

Dieses Gebiet bietet also noch viele weitere interessante Fragestellungen!

An dieser Stelle möchte ich mich abschließend noch bei all denen bedanken, die mich bei der Anfertigung dieser Arbeit unterstützt haben. Mein ganz besonderer Dank gilt Prof. Ernst-Ulrich Gekeler, der diese Arbeit betreut hat und immer ein offenes Ohr für Fragen hatte.
Außerdem bedanke ich mich herzlich bei Thorsten Paul, meinen Eltern Jutta und Ulrich Wald, meinem Bruder Philip Wald sowie Helga Wald, Sarah Detzler und Bernadette Hahn, Johannes Lengler und Olaf Leidinger.

Literatur

[Lan70] Serge Lang, *Algebraic number theory*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970. MR MR0282947 (44 #181)

[Lan84] Serge Lang, *Algebra*, second ed., Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1984. MR MR783636 (86j:00003)

[SP07] Rainer Schulze-Pillot, *Elementare Algebra und Zahlentheorie*, 1. ed., Springer-Verlag, Berlin, Heidelberg, 2007.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR MR1421575 (97h:11130)