Bachelorarbeit

Über das Umkehrproblem der Galoistheorie

von

Julia Jöchler

Betreuer:

Univ.-Prof. Dr. Tim Netzer

SS2017

Fakultät für Mathematik, Informatik und Physik
an der Universität Innsbruck

Studiengang: Technische Mathematik

Leopold-Franzens-Universität Innsbruck

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt durch meine eigenhändige Unterschrift, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder inhaltlich den angegebenen Quellen entnommen wurden, sind als solche kenntlich gemacht.
Ich erkläre mich mit der Archivierung der vorliegenden Bachelorarbeit einverstanden.

Datum	Unterschrift

ABSTRACT: Beim inversen Galoisproblem handelt es sich um eine bis heute ungelöste Fragestellung der Algebra, genauer der Galoistheorie.
Ist jede endliche Gruppe als Galoisgruppe einer Körpererweiterung über $\mathbb{Q}$ realisierbar?
Diese Arbeit behandelt drei Teilresultate des Umkehrproblems:

- Treten alle **endlichen** Gruppen als Galoisgruppe einer Körpererweiterung über einem beliebigen Körper auf?

- Treten alle **zyklischen** Gruppen als Galoisgruppe einer Körpererweiterung über den rationalen Zahlen auf?

- Sind alle **endlichen abelschen** Gruppen als Galoisgruppe einer Körpererweiterung über $\mathbb{Q}$ realisierbar?

Ziel dieser Arbeit ist es, dem Leser anhand der Beweise dieser drei Aussagen einen kleinen Einblick in diese äußerst umfangreiche Thematik zu ermöglichen.

Inhaltsverzeichnis

1 Einleitung

Die Anfänge der Galoistheorie liegen im frühen 19.Jh. und wurde von ihrem Namensgeber, dem Mathematiker Evariste Galois, maßgeblich geprägt. Eine der Hauptfragen der Galoistheorie ist, unter welchen Bedingungen eine Gleichung in einer Unbekannten auflösbar ist. Man möchte also Eigenschaften von Polynomen über deren Lösbarkeit in einem bestimmten Körper charakterisieren. Diese Frage konnte Galois im Jahr 1832 beantworten, viel interessanter als die Lösung an sich war allerdings seine Vorgehensweise, mit welcher er fast schon revolutionär an dieses Problem heranging. Galois stellte Zusammenhänge zwischen unterschiedlichen Typen mathematischer Objekte her. Jeder Gleichung ordnete er ein Objekt zu, welches wir heute als Galoisgruppe kennen. Die Eigenschaften eben dieser Galoisgruppe geben Aufschluss darüber, ob die Gleichung auflösbar ist oder nicht. Eine der wichtigsten Anwendungen der Galoistheorie ist die Lösbarkeit von Polynomen durch Wurzelziehen. Das erste wichtige Resultat von Galois war zu beweisen, dass Polynome bzw. Gleichungen vom Grad 5 oder höher nicht durch alleinige Verwendung elementarer Rechenoperationen und Wurzelziehen lösbar sind.
Im modernen Ansatz der heutigen Zeit vermittelt die Galoistheorie einen Zusammenhang zwischen algebraischen Körpererweiterungen und der Gruppentheorie. Essentiell dafür ist der *Hauptsatz der Galoistheorie*. Dieser arbeitet mit gewissen Bijektionen zwischen den Zwischenkörpern einer Körpererweiterung und den Untergruppen der dazugehörigen Galoisgruppe (später dazu mehr). Dies ermöglicht spezielle Fragen und Problemstellungen von Körpern auf Gruppen zu übertragen (oder umgekehrt), diese mit Hilfe der dortigen Theorie zu lösen und anschließend wieder auf das Ursprüngliche zurückzuführen.
Eigentliches Thema dieser Arbeit ist allerdings das inverse Galoisproblem. Dieses Problem, welches bis heute jedoch ungelöst ist, fragt danach, ob alle endlichen Gruppen als Galoisgruppe einer Körpererweiterung über dem Körper der rationalen Zahlen realisierbar sind. Nicht diese Frage, aber drei kleinere Teilresultate dieser Fragestellung gilt es nun zu beweisen:

- Treten alle **endlichen** Gruppen als Galoisgruppe einer Körpererweiterung über einem beliebigen Körper auf?
- Treten alle **zyklischen** Gruppen als Galoisgruppe einer Körpererweiterung über den rationalen Zahlen auf?
- Sind alle **endlichen abelschen** Gruppen als Galoisgruppe einer Körpererweiterung über $\mathbb{Q}$ realisierbar?

Zuerst aber folgt noch eine kleine Auflistung grundlegender Theorie aus der Algebra.

2 Grundlegendes

2.1 Wichtige Definitionen

Um dem Leser das Verständnis der folgenden Arbeit zu erleichtern, gibt es hier eine Wiederholung einiger wichtiger Begriffe und Definitionen der Algebra und Galoistheorie. Die Theorie für diese Arbeit stammt, sofern nicht anders angegeben, aus dem Vorlesungsskript Algebra von Univ.-Prof. Dr. Tim Netzer [4].

Definition 1 (Charakteristik)**.**
Sei K ein Körper und

$$\begin{aligned} \iota :&\mathbb{Z} \to K \\ &z \mapsto \underbrace{1 + \cdots + 1}_{\text{z mal}}. \end{aligned}$$

Die Zahl p mit $\ker(\iota) = (p)$ heißt die **Charakteristik** des Körpers K. Sie wird auch mit $\operatorname{char}(K)$ bezeichnet.

Definition 2 (Körpererweiterung)**.**
Eine **Körpererweiterung** ist eine Inklusion $k \subseteq K$, wobei k ein Teilring von K und selbst ein Körper ist. Dabei heißt k Teilkörper von K und K Oberkörper von k. Statt $k \subseteq K$ schreibt man manchmal auch K/k. Dies ist nicht mit einer Restklassenkonstruktion zu verwechseln.

Definition 3 (Grad)**.**
Für eine Körpererweiterung $k \subseteq K$ nennen wir die k-Vektorraumdimension

$$\dim_k(K) =: [K : k]$$

den **Grad** der Körpererweiterung.

Definition 4 (irreduzibel)**.**
Für $a, b \in R$ (R Integritätsbereich) definieren wir:
$0 \neq a$ heißt **irreduzibel**, falls $a \notin R^\times$ und aus $a = bc$ stets $b \in R^\times$ oder $c \in R^\times$ folgt.

Definition 5 (algebraisch)**.**
(i) Ein Element $a \in K$ heißt **algebraisch über** k, falls es ein $0 \neq p \in k[x]$ gibt mit

$$p(a) = 0.$$

(ii) Ist a nicht algebraisch über k, so heißt a **transzendent über** k.
(iii) Die Körpererweiterung $k \subseteq K$ heißt **algebraisch**, falls jedes Element $a \in K$ algebraisch über k ist.

Definition 6 (SEPARABEL)**.**
(i) Ein irreduzibles Polynom $p \in k[x]$ heißt **separabel**, falls p in $\overline{k}$ (oder seinem Zerfällungskörper) $\deg(p)$ viele verschiedene Nullstellen besitzt.
(ii) Für eine Körpererweiterung $k \subseteq K$ heißt $a \in K$ **separabel über** k, falls a algebraisch über k ist und $\mathrm{Min}(a, k)$ separabel ist.
(iii) Eine algebraische Körpererweiterung $k \subseteq K$ heißt **separabel**, falls jedes $a \in K$ separabel über k ist.

Definition 7 (NORMAL)**.**
Eine algebraische Körpererweiterung $k \subseteq K$ heißt **normal**, falls jedes irreduzible Polynom $p \in k[x]$, welches in K eine Nullstelle hat, in K bereits zerfällt.

Definition 8 (GALOIS-ERWEITERUNG)**.**
Eine Körpererweiterung heißt **Galois-Erweiterung**, falls sie endlich, normal und separabel ist.

Definition 9 (GALOISGRUPPE)**.**
Sei $k \subseteq K$ eine Körpererweiterung. Wir definieren ihre **Galoisgruppe** folgendermaßen:

$$\mathrm{Gal}(K, k) := \{\varphi : K \to K | \, \varphi \, k\text{-Isomorphismus.}\}.$$

Elemente von $\mathrm{Gal}(K, k)$ nennen wir auch k-**Automorphismen** von K.

Weitere Definitionen und eventuell benötigte Sätze werden im Laufe der Arbeit zu gegebener Zeit erläutert.

2.2 Einige Vorbereitungen

Dieser Abschnitt soll als Vorbereitung für die folgenden Kapitel dienen. Es werden einige Aussagen und Behauptungen aufgestellt und bewiesen.

Aussage 1. *Jede endliche Gruppe G mit $\#G = n$ ist isomorph zu einer Untergruppe H von S_n.*

Beweis. Für $g \in G$ ist die Abbildung

$$\begin{aligned} m_g : & G \to G \\ & h \mapsto gh \end{aligned}$$

bijektiv und es gilt

$$m_{fg} = m_f \circ m_g \ , m_g^{-1} = m_{g^{-1}}.$$

Weiters ist: $m_g = \mathrm{id} \Leftrightarrow g = e$ (neutrales Element).

Also ist die Abbildung

$$\begin{aligned} G & \to \mathcal{S}(G) \\ g & \mapsto m_g \end{aligned}$$

ein injektiver Gruppenhomomorphismus und damit ist G isomorph zu seinem Bild, einer Untergruppe von $\mathcal{S}(G) \cong S_n$. □

Aussage 2. $ggT(k,n) = 1 \Longleftrightarrow k \in (\mathbb{Z}/n\mathbb{Z})^\times, \quad k,n \in \mathbb{Z}$

Wir werden diese Aussage mit Hilfe des euklidischen Algorithmus nachweisen. Zu diesem Zweck wollen wir kurz wiederholen, was genau beim euklidischen Algorithmus passiert: Gegeben seien zwei Zahlen a und b, wobei wir $b = r_0$ setzen. Jetzt führen wir eine Division mit Rest durch, sodass wir folgende Darstellung erhalten:

$$a = q_1 \cdot r_0 + r_1, \qquad (|r_1| < |r_0|)$$

Nun wird in jedem nachfolgendem Schritt mit dem Divisor und dem Rest des vorherigen Schrittes erneut eine Division mit Rest durchgeführt und das solange, bis eine Division mit Rest 0 aufgeht.

$$\begin{aligned} r_0 &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\vdots \\ r_{n-1} &= q_{n+1} \cdot r_n + 0 \end{aligned}$$

Der Divisor des letzten Schritts r_n ist nun der größte gemeinsame Teiler von a und b. Merkt man sich die Divisoren jedes Schrittes, so kann man mit dem erweiterten euklidischen Algorithmus durch Rückwärtslesen der Gleichungen zwei ganze Zahlen s und t finden, mit deren Hilfe man eine Darstellung des ggT erhält:

$$\mathrm{ggT}(a,b) = sa + tb$$

Mit diesem Wissen wollen wir jetzt die oben genannte Äquivalenz beweisen:

Beweis. "⇒": Sei $\mathrm{ggT}(k,n) = 1$

$$\begin{aligned}
&\Longrightarrow \exists s,t \in \mathbb{Z} : sk + tn = 1 \\
&\Longrightarrow sk = 1 \bmod n \\
&\Longrightarrow k \in (\mathbb{Z}/n\mathbb{Z})^\times
\end{aligned}$$

weil $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \exists b \in \mathbb{Z} : b \cdot a = a \cdot b = 1 \bmod n\}$.

"⇐": Sei $k \in (\mathbb{Z}/n\mathbb{Z})^\times$

$$\begin{aligned}
&\Longrightarrow \exists s \in \mathbb{Z} : sk = 1 \bmod n \\
&\Longrightarrow \exists t \in \mathbb{Z} : sk + tn = 1 \ (k \text{ ist teilerfremd zu } n) \\
&\Longrightarrow \mathrm{ggT}(k,n) = 1
\end{aligned}$$

□

3 Endliche Gruppen

Wir beginnen nun mit dem allgemeinen Fall einer beliebigen Galoiserweiterung $L \subseteq K$. Ziel ist es zu zeigen, dass in diesem Fall alle endlichen Gruppen als Galoisgruppe auftreten.

Zur Vorbereitung betrachten wir das Polynom

$$\begin{aligned} F(t) &= (t - x_1) \cdots (t - x_n) \\ &= t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n \end{aligned}$$

wobei X eine Variable über dem Ring $\mathbb{Q}[x_1, \ldots, x_n]$ ist und $x_1, \ldots, x_n$ algebraisch unabhängig über $\mathbb{Q}$ sind. Weiters ist jedes $s_i = s_i(x_1, \ldots, x_n)$ ein Polynom in den Variablen $x_1, \ldots, x_n$. Laut obiger Gleichung gilt zum Beispiel

$$s_1 = x_1 + \cdots + x_n \qquad \text{und} \qquad s_n = x_1 \cdots x_n.$$

Die Polynome $s_1, \ldots, s_n$ werden elementarsymmetrische Polynome genannt.

Um also zu zeigen, dass alle endlichen Gruppen als Galoisgruppe einer beliebigen Galoiserweiterung auftreten, betrachten wir die Körpererweiterung

$$\begin{array}{c} \mathbb{Q}(x_1, \ldots, x_n) \\ | \\ \mathbb{Q}(s_1, \ldots, s_n). \end{array}$$

Zuallererst müssen wir zeigen, dass es sich hierbei um eine Galoiserweiterung handelt, d.h. $\mathbb{Q}(s_1, \ldots, s_n) \subseteq \mathbb{Q}(x_1, \ldots, x_n)$ ist endlich, normal und separabel.
Die Endlichkeit ist offensichtlich gegeben, da die $x_i, i = 1, \ldots, n$, alle algebraisch sind. Wenn man endlich viele algebraische Elemente an einen Körper adjungiert, erhält man immer eine endliche Körpererweiterung.
Zunächst wollen wir uns also der Separabilität widmen und verwenden hierzu folgende Proposition:

Proposition 1. *Falls char$(k) = 0$ gilt, ist jedes irreduzible Polynom $p \in k[x]$ separabel. Insbesondere ist jede algebraische Körpererweiterung $k \subseteq K$ separabel.*

Also können wir folgern:

$$\begin{aligned} \operatorname{char}(\mathbb{Q}) = 0 &\Rightarrow \operatorname{char}(\mathbb{Q}(s_1, \ldots, s_n)) = 0 \\ &\Rightarrow \mathbb{Q}(s_1, \ldots, s_n) \subseteq \mathbb{Q}(x_1, \ldots, x_n) \text{ ist separabel.} \end{aligned}$$

Es bleibt also die Normalität zu zeigen. Wir verwenden folgenden Satz:

Satz 1. *Für eine algebraische Körpererweiterung $k \subseteq K \subseteq \overline{k}$ sind äquivalent:*

1. *$k \subseteq K$ ist normal.*
2. *K ist Zerfällungskörper einer Menge von Polynomen p über k.*
3. *Jeder k-Homomorphismus $\varphi : K \to \overline{k}$ erfüllt $\varphi(K) \subseteq K$.*

Wir verwenden die Äquivalenz zwischen *1.* und *2.*, d.h. wir müssen zeigen, dass $\mathbb{Q}(x_1, \ldots, x_n)$ der Zerfällungskörper eines Polynoms über $\mathbb{Q}(s_1, \ldots, s_n)$ ist.

Definition 10. $k \subseteq K$ Körpererweiterung.

(i) $p \in k[t]$ zerfällt über K in Linearfaktoren, falls $b \in k$, $a_1, \ldots, a_d \in K$ existieren mit

$$p = b(t - a_1)(t - a_2) \cdots (t - a_d) \in K[t]$$

(ii) K heißt Zerfällungskörper (ZFK) von p über k, falls p über K zerfällt und mit den a_i wie in (i) gilt

$$K = k(a_1, \ldots, a_d)$$

Sei im Folgenden stets $K := \mathbb{Q}(x_1, \ldots, x_n)$ und $k := \mathbb{Q}(s_1, \ldots, s_n)$. Weiters sei

$$p = (t - x_1)(t - x_2) \cdots (t - x_n) \in K[t]$$

Wie wir nach der Vorbereitung wissen, gilt

$$p = t^n - s_1(x_1, \ldots, x_n)t^{n-1} + s_2(x_1, \ldots, x_n)t^{n-2} + \ldots + (-1)^n s_n(x_1, \ldots, x_n)$$

also, dass $p \in k[t]$.
Durch diese Wahl zerfällt p auf natürliche Weise in Linearfaktoren über K, denn wir wählen $b = 1$, $a_1 = x_1, \ldots, a_n = x_n$ und somit

$$p = b(t - a_1) \cdots (t - a_n) = (t - x_1) \cdots (t - x_n) \in K[t]$$

Zudem erkennt man leicht, dass

$$\begin{aligned} k(x_1, \ldots, x_n) &= (\mathbb{Q}(s_1, \ldots, s_n))(x_1, \ldots, x_n) \\ &= \mathbb{Q}(x_1, \ldots, x_n) \\ &= K \end{aligned}$$

Nach Definition 10 ist K der ZFK von p über k.
Es gilt also, dass $\mathbb{Q}(x_1, \ldots, x_n)$ der Zerfällungskörper von p über $\mathbb{Q}(s_1, \ldots, s_n)$ ist.
Also wissen wir, dass $\mathbb{Q}(s_1, \ldots, s_n) \subseteq \mathbb{Q}(x_1, \ldots, x_n)$ normal ist und somit auch, dass es sich bei $\mathbb{Q}(s_1, \ldots, s_n) \subseteq \mathbb{Q}(x_1, \ldots, x_n)$ um eine Galoiserweiterung handelt.

Nun, da wir wissen, dass es sich um eine Galoiserweiterung handelt, können wir den Hauptsatz der Galoistheorie anwenden.
Bevor wir dies tun, wollen wir zuerst noch zeigen, dass die Galoisgruppe von

$$\mathbb{Q}(s_1, \ldots, s_n) \subseteq \mathbb{Q}(x_1, \ldots, x_n)$$

zur Permutationsgruppe S_n isomorph ist. Ist dies nämlich der Fall, kann man daraus mit Hilfe des Haupsatzes bereits die gewünschte Aussage folgern, wie wir etwas später sehen werden.
Behauptung:

$$\mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n), \mathbb{Q}(s_1, \ldots, s_n)) \cong S_n$$

Beweis. Zunächst werden wir überprüfen, dass zumindest die Inklusion $\mathrm{Gal}(K, k) \subseteq S_n$ erfüllt ist.
Für alle $\varphi \in \mathrm{Gal}(K, k)$ gilt, dass Nullstellen nur auf Nullstellen abgebildet werden, da φ ein Isomorphismus und damit insbesondere ein Homomorphismus ist. Genauer bedeutet dies folgendes: Nehmen wir ein Element aus dem größeren Körper und ein Polynom des kleineren Körpers, welches dieses Element als Nullstelle hat. Dann muss jedes φ aus der Galoisgruppe dieses Element auf eine andere Nullstelle desselben Polynoms abbilden.
Denn:
Sei q ein Polynom mit Nullstelle a. Dann gilt

$$\begin{aligned} & q(a) = 0 \\ & \overset{\varphi \text{ Q-linear}}{\Rightarrow} q(\varphi(a)) \quad = \quad \varphi(q(a)) \quad \overset{\varphi \text{ Homomorphismus}}{=} \quad \varphi(0) \quad = \quad 0, \end{aligned}$$

also ist $\varphi(a)$ Nullstelle von q.

Das heißt also für alle $i = 1, \ldots, n$ gilt, dass $\varphi(x_i) = x_j$ für $j = 1, \ldots, n$.

Anders geschrieben:

$$\varphi(x_i) = x_{\sigma(i)}$$

für ein $\sigma \in S_n$.

$$\Longrightarrow Gal(\mathbb{Q}(x_1, \ldots, x_n), \mathbb{Q}(s_1, \ldots, s_n)) \subseteq S_n$$

Es bleibt noch die andere Inklusionsrichtung zu zeigen, also dass zu jeder Permutation ein Automorphismus aus der Galoisgruppe existiert, der genau das macht, was auch die Permutation mit den x_i machen würde. Genauer:

$$\forall \sigma \in S_n : \exists \varphi \in \mathrm{Gal}(K, k) : \forall i \in \{1, \ldots, n\} : \varphi(x_i) = x_{\sigma(i)}$$

Sei $\sigma \in S_n$ beliebig.
Wir definieren zunächst einen Ringhomomorphismus auf dem Polynomring

$$\begin{array}{rcl} \varphi_\sigma : \mathbb{Q}[x_1, \ldots, x_n] & \longrightarrow & \mathbb{Q}[x_1, \ldots, x_n] \\ x_i & \longmapsto & x_{\sigma(i)} \end{array}$$

Dabei garantiert die Definition des Polynomrings, dass so ein Ringhomomorphismus existiert.
Offensichtlich handelt es sich sogar um einen Isomorphismus, denn wählt man die inverse Permutation $\sigma^{-1} \in S_n$, erhält man gerade die Umkehrabbildung.
Nun kann man einen Isomorphismus von Ringen immer zu einem Isomorphismus der Quotientenkörper fortsetzen. Bei $\mathbb{Q}(x_1, \ldots, x_n)$ handelt es sich ja um Brüche von Polynomen. Wenn man einen Isomorphismus auf Polynomebene gegeben hat, wendet man ihn einfach sowohl im Nenner als auch im Zähler an. Es handelt sich also um eine offensichtliche Beobachtung, dass man auf diese Art und Weise auch einen Isomorphismus auf dem Quotientenkörper erhält.
Wir haben bis jetzt gezeigt: zu einer Permutation $\sigma \in S_n$ gibt es einen Isomorphismus

$$\begin{array}{rcl} \varphi_\sigma : \mathbb{Q}(x_1, \ldots, x_n) & \longrightarrow & \mathbb{Q}(x_1, \ldots, x_n) \\ x_i & \longmapsto & x_{\sigma(i)} \end{array}$$

welcher per Konstruktion die Variablen genau so permutiert, wie die Permutation es vorgibt.
Es bleibt noch zu zeigen, dass

$$\varphi_\sigma \in \mathrm{Gal}(K, k).$$

Die Galoisgruppe besteht aus denjenigen Isomorphismen, welche den kleinen Körper festhalten. Was wir also zeigen müssen ist, dass φ_σ den Körper $\mathbb{Q}(s_1, \ldots, s_n)$ festhält. Dies lässt sich leicht überprüfen, da es sich gerade um die elementarsymmetrischen Polynome handelt, welche per Definition genau solche Polynome sind, die gleich bleiben, wenn man die Variablen permutiert:

$$z.z. \qquad \varphi_\sigma|_{\mathbb{Q}(s_1,\ldots,s_n)} = \mathrm{id}$$

$\forall i = 1, \ldots, n$:

$$\begin{aligned}\varphi_\sigma(s_i(x_1, \ldots, x_n)) &= s_i(\varphi_\sigma(x_1), \ldots, \varphi_\sigma(x_n)) \\ &= s_i(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \\ &= s_i(x_1, \ldots, x_n),\end{aligned}$$

also $S_n \subseteq \mathrm{Gal}(K, k)$. Damit haben wir die Behauptung

$$Gal(\mathbb{Q}(x_1, \ldots, x_n), \mathbb{Q}(s_1, \ldots, s_n)) \cong S_n$$

bewiesen. □

Jetzt kommt der Hauptsatz der Galoistheorie zur Anwendung:

Satz 2 (Hauptsatz der Galoistheorie)**.** *Es sei $k \subseteq K$ eine Galoiserweiterung. Dann sind die Zuordnungen $Fix(\cdot)$ und $Gal(K, \cdot)$ zueinander inverse inklusionsumkehrende Bijektionen zwischen Untergruppen von $G = Gal(K, k)$ und Zwischenkörpern von k und K.*

$$\begin{array}{ccc}\{L; k \subseteq L \subseteq K\} & \longleftrightarrow & \{H; H < Gal(K, k)\} \\ L & \longmapsto & Gal(K, L) \\ Fix(H) & \longleftarrow & H\end{array}$$

Weiter gilt für $H < G$:

(i) $\#H = [K : Fix(H)]$ und $|G : H| = [Fix(H) : k]$

(ii) $H \lhd G \Leftrightarrow Fix(H)$ normal über k.
In diesem Fall ist $k \subseteq Fix(H)$ wieder eine Galoiserweiterung und es gilt

$$Gal(Fix(H), k) \cong G/H.$$

Da es sich bei der Galoisgruppe von $\mathbb{Q}(s_1, \ldots, s_n) \subseteq \mathbb{Q}(x_1, \ldots, x_n)$ um S_n handelt, sind somit laut Aussage 1 alle endlichen Gruppen als Untergruppen vertreten. Nun gibt es nach dem Hauptsatz der Galoistheorie für jede (endliche) Untergruppe H einen dazugehörigen Zwischenkörper L mit $\mathbb{Q}(s_1, \ldots, s_n) \subseteq L \subseteq \mathbb{Q}(x_1, \ldots, x_n)$ für den gilt, dass $\mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n), L) = H$, womit die Behauptung gezeigt ist.

Wir wollen die wichtigsten Beweisschritte nochmals wiederholen:

- Betrachte die Körpererweiterung $\mathbb{Q}(s_1, \ldots, s_n) \subseteq \mathbb{Q}(x_1, \ldots, x_n)$ und zeige, dass es sich um eine Galoiserweiterung handelt.

- Zeige, dass die Galoisgruppe dieser Erweiterung der Permutationsgruppe S_n entspricht.

- Für alle endlichen Gruppen G mit $\#G = n$ gilt

$$G \cong H < S_n.$$

- Anwenden des Hauptsatzes:

$$\begin{array}{ccc} \{L; k \subseteq L \subseteq K\} & \longleftrightarrow & \{H; H < S_n\} \\ L & \longmapsto & \mathrm{Gal}(K, L) \\ \mathrm{Fix}(H) & \longleftarrow & H \\ & & \uparrow \\ & & \text{Nach Aussage 1} \\ & & \text{treten hier alle} \\ & & \text{endlichen Gruppen auf.} \end{array}$$

- Also treten alle endlichen Gruppen G als Galoisgruppe einer Galoiserweiterung auf: $\forall$ G mit $\#G < \infty$ $\exists$ L,K mit $L \subseteq K$ Galoiserweiterung:

$$\mathrm{Gal}(K, L) = G.$$

4 Zyklische Gruppen

In diesem Abschnitt stellen wir uns die Frage: Was für Galoisgruppen entstehen, wenn man als Grundkörper $\mathbb{Q}$ festhält?
Wir werden uns zunächst dem Teilresultat widmen, dass jede zyklische Gruppe als Galoisgruppe auftritt.

Für den Beweis benötigen wir folgenden Satz

Satz 3 (Satz von Dirichlet)**.** *Seien a und n natürliche Zahlen und teilerfremd. Dann gibt es unendlich viele Primzahlen $p \equiv a \bmod n$.*
Anders ausgedrückt: Jede arithmetische Progression

$$\{a + kn : k \in \mathbb{N}\}, \qquad ggt(a, n) = 1$$

enthält unendlich viele Primzahlen.

Beweis. Siehe [5, S. 248]. □

Mit Hilfe dieses Satzes können wir nun eine Primzahl p wählen, für die gilt, dass $p \equiv 1 \bmod n$ für ein $n \in \mathbb{N}$. Das heißt also, wir können p schreiben als

$$p = rn + 1 \quad , r \in \mathbb{N}.$$

Sei nun ξ die p-te primitive Einheitswurzel $\xi = e^{\frac{2\pi i}{p}}$. Wir betrachten die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\xi)$. Wie man leicht sieht, ist der Grad dieser Körpererweiterung $p - 1$.

Satz 4. *Sei $k \subseteq K$ eine Körpererweiterung und $a \in K$ algebraisch über k. Dann gilt*

$$[k(a) : k] = deg(Min(a, k)),$$

wobei $Min(a, k)$ das Minimalpolynom von a über k bezeichnet.

Für $\xi = e^{\frac{2\pi i}{p}}$ gilt, dass das Minimalpolynom über $\mathbb{Q}$ gerade das p-te Kreisteilungspolynom ist, also

$$\mathrm{Min}(\xi, \mathbb{Q}) = \Phi_p = 1 + x + \cdots + x^{p-1}.$$

Offensichtlich ist ξ eine Nullstelle von $x^p - 1$ und dieses Polynom faktorisiert

$$x^p - 1 = (x - 1) \cdot \Phi_p.$$

Da aber ξ keine Nullstelle von $x - 1$ ist, muss also gelten dass $\Phi_p(\xi) = 0$. Da das Kreisteilungspolynom zudem irreduzibel und normiert ist, handelt es sich um das Minimalpolynom von ξ über $\mathbb{Q}$. Also gilt nach Satz 4 dass der Grad der Körpererweiterung

$p-1$ ist, weil $\deg(\mathrm{Min}(\xi, \mathbb{Q})) = \deg(1 + x + \cdots + x^{p-1}) = p-1$.
Nun wollen wir die Galoisgruppe dieser Körpererweiterung berechnen:
Wie wir oben bereits gesehen haben, ist das Minimalpolynom von $\xi = e^{\frac{2\pi i}{p}}$ das p-te Kreisteilungspolynom, welches in $K := \mathbb{Q}(e^{\frac{2\pi i}{p}})$ die $p-1$ verschiedenen Nullstellen $\xi, \xi^2, \ldots, \xi^{p-1}$ besitzt. Laut nachfolgender Proposition, gilt nun, dass es genau $p-1$ viele $\mathbb{Q}$-Homomorphismen von K gibt.

Proposition 2. *Seien $k \subseteq K$ und $k' \subseteq K'$ Körpererweiterungen sowie $\varphi : k \to k'$ ein Homomorphismus. Sei $a \in K$ algebraisch über k und $p = Min(a, k) \in k[x]$. Dann ist die Anzahl der Homomorphismen $\psi : k(a) \to K'$ mit $\psi_{|k} = \varphi$ gleich der Anzahl der verschiedenen Nullstellen von $p^{(\varphi)}$ in K.*

Dabei sind die $\mathbb{Q}$-Homomorphismen $\varphi_1, \ldots, \varphi_{p-1}$ bestimmt durch

$$\varphi_i(\xi) = \xi^i.$$

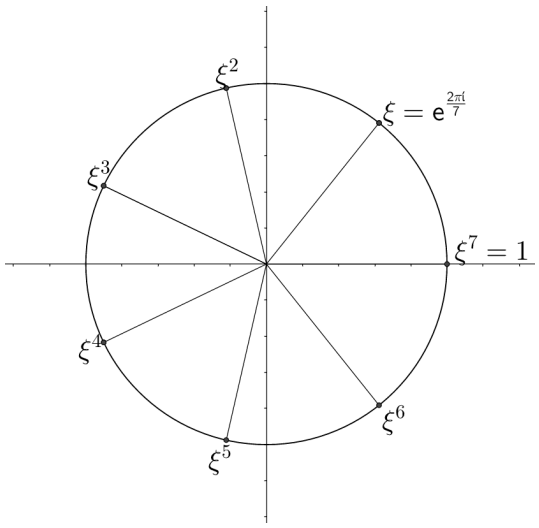

Abb.1 Beispiel: Die 7-te primitive Einheitswurzel und ihre Potenzen.

Außerdem kann man leicht zeigen, dass es sich zudem sogar um Automorphismen handelt, allerdings nur, da es sich bei p um eine Primzahl handelt.
Also haben wir die gesuchten Elemente der Galoisgruppe gefunden und sie lautet

$$\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{p}}), \mathbb{Q}) = \{\varphi_1, \ldots, \varphi_{p-1}\} \cong ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot).$$

Diese zwei Gruppen sind isomorph, da sie beide gleich viele Elemente besitzen, welche auch die gleichen Eigenschaften erfüllen. Die Einheitengruppe enthält alle multiplikativ

invertierbaren Elemente, in unserem Fall also gerade alle Zahlen, die teilerfremd zu p sind (Siehe Aussage 2). Da nun p genau eine Primzahl ist, ist die Anzahl der Elemente also gerade $p-1$. Man kann also einen Isomorphismus zwischen den beiden Gruppen folgendermaßen definieren:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{p}}),\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ \varphi_i & \longmapsto & i \end{array}$$

Genauso wie für $1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ gilt, dass $1 \cdot k = k \cdot 1 = k$ (1 = neutrales Element), gilt für φ_1 dass $\varphi_1 \circ \varphi_k = \varphi_1 \circ \varphi_k = \varphi_k$ und es gilt $k \cdot l = kl \bmod p-1$ sowie $\varphi_k \circ \varphi_l = \varphi_{kl \bmod p-1}$ für $k, l \in \{1, \ldots, p-1\}$.
Im Weiteren benötigen wir folgenden Satz:

Satz 5. *(zit. [7, S. 55])*
Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.

Daraus können wir nun folgern, dass die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch ist, da insbesondere gilt, dass die Einheitengruppe eines endlichen Körpers zyklisch ist. Wir wissen bereits, dass $(\mathbb{Z}/p\mathbb{Z})^\times$ $p-1$ Elemente besitzt, dadurch können wir nun folgern, dass es auch einen Isomorphismus zwischen $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ und $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ gibt. Wie dieser genau aussieht, lässt sich nicht ohne Weiteres allgemein formulieren, allerdings ist dies in unserem Fall von keiner größeren Bedeutung.
Wir wissen nun also, dass die zwei Gruppen $\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{p}}),\mathbb{Q})$ und $\mathbb{Z}/(p-1)\mathbb{Z}$ isomorph sind und da gilt, dass $p = rn + 1 \Leftrightarrow p - 1 = rn$, gilt also auch

$$\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{p}}),\mathbb{Q}) \cong \mathbb{Z}/rn\mathbb{Z}.$$

Offensichtlich gilt, dass $\mathbb{Z}/r\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}/rn\mathbb{Z}$ ist. Dies sieht man daran, dass es einen injektiven Gruppenhomomorphismus gibt mit

$$\begin{array}{rcr} \mathbb{Z}/r\mathbb{Z} & \hookrightarrow & \mathbb{Z}/rn\mathbb{Z} \\ 0 & \longmapsto & 0 \\ 1 & \longmapsto & n \\ 2 & \longmapsto & 2n \\ & \vdots & \end{array}$$

also $\mathbb{Z}/r\mathbb{Z} < \mathbb{Z}/rn\mathbb{Z}$.

Beispiel 1. Für $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$ gilt

$$\begin{array}{rcr} & & \overbrace{\quad}^{\mathbb{Z}/2\cdot 3\mathbb{Z}} \\ \mathbb{Z}/2\mathbb{Z} & \hookrightarrow & \mathbb{Z}/6\mathbb{Z} \\ 0 & \longmapsto & 0 \\ 1 & \longmapsto & 3 \end{array}$$

$\Rightarrow \mathbb{Z}/2\mathbb{Z} < \mathbb{Z}/6\mathbb{Z}$. $\Diamond$

Jetzt überprüfen wir noch, dass es sich bei $\mathbb{Q} \subseteq \mathbb{Q}(e^{\frac{2\pi i}{p}})$ um eine Galoiserweiterung handelt.
Wir zeigen also, dass die Körpererweiterung separabel und normal ist.
Wie bereits im ersten Abschnitt können wir für die Separabilität verwenden, dass $\mathrm{char}(\mathbb{Q}) = 0$ ist. Damit folgt aus Proposition 1, dass es sich um eine separable Körpererweiterung handelt.
Für die Normalität verwenden wir wiederum Satz 1. Wie wir bereits gesehen haben, ist das p-te Kreisteilungspolynom Φ_p das Minimalpolynom von $e^{\frac{2\pi i}{p}}$ über $\mathbb{Q}$. Wenn wir nun den Zerfällungskörper von Φ_p über $\mathbb{Q}$ betrachten, sehen wir, dass es sich dabei gerade um $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ handelt. Also ist $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ der Zerfällungskörper einer Menge von Polynomen über $\mathbb{Q}$ und damit die Körpererweiterung normal. (Dies gilt nicht nur für Primzahlen p, sondern für beliebiges $n \in \mathbb{N}$ mit $\xi = e^{\frac{2\pi i}{n}}$.)
Wir können jetzt also den Hauptsatz anwenden:

$$\begin{array}{ccc} & & \overbrace{\quad}^{\cong \mathbb{Z}/rn\mathbb{Z}} \\ \{L \,|\, \mathbb{Q} \subseteq L \subseteq \mathbb{Q}(\xi)\} & \longleftrightarrow & \{H | H < \mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})\} \\ & & \underbrace{\quad}_{\ni\, \mathbb{Z}/r\mathbb{Z},\, \text{weil } \mathbb{Z}/r\mathbb{Z} < \mathbb{Z}/rn\mathbb{Z}} \\ \mathrm{Fix}(\mathbb{Z}/r\mathbb{Z}) & \longleftarrow & \mathbb{Z}/r\mathbb{Z} \end{array}$$

Mit diesem Wissen können wir nun den Punkt (ii) des Haupsatzes verwenden. Zur Wiederholung:
Für $H < G$ gilt:

(ii) $H \lhd G \Leftrightarrow \mathrm{Fix}(H)$ normal über k.
In diesem Fall ist $k \subseteq \mathrm{Fix}\ (H)$ wieder eine Galoiserweiterung und es gilt

$$\mathrm{Gal}(\mathrm{Fix}(H), k) \cong G/H.$$

Wir wollen zeigen, dass Folgendes gilt:

$$\mathbb{Z}/r\mathbb{Z} \lhd \mathbb{Z}/rn\mathbb{Z}$$

Wir betrachten die Mengen
$H := \mathbb{Z}/r\mathbb{Z} = \{0, 1, 2, \ldots, r-1\}$ und
$G := \mathbb{Z}/rn\mathbb{Z} = \{0, 1, \ldots, r-1, r, \ldots, 2r-1, \ldots, rn-1\}$.
Da die Verknüpfung + kommutativ ist, gilt

$$\begin{aligned}\forall g \in G : g + H &= \{g, g+1, g+2, \ldots, g+(r-1)\} \\ &= \{g, 1+g, 2+g, \ldots, (r-1)+g\} = H + g\end{aligned}$$

$$\Longrightarrow \mathbb{Z}/r\mathbb{Z} \lhd \mathbb{Z}/rn\mathbb{Z}.$$

Aus dem Hauptsatz folgt nun:

$$\Longrightarrow \mathbb{Q} \subseteq \mathrm{Fix}(\mathbb{Z}/r\mathbb{Z}) \text{ ist Galoiserweiterung}$$

und es gilt

$$\mathrm{Gal}(\mathrm{Fix}(\mathbb{Z}/r\mathbb{Z}), \mathbb{Q}) \cong (\mathbb{Z}/rn\mathbb{Z})\big/(\mathbb{Z}/r\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}.$$

Da n zu Anfang beliebig gewählt war, gibt es zu jeder natürlichen Zahl eine Galoiserweiterung L über $\mathbb{Q}$, sodass gilt

$$\mathrm{Gal}(L, \mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}$$

womit die Behauptung gezeigt ist.

Zusammenfassung der wichtigsten Beweisschritte:

- Wähle eine Primzahl $p = 1 \bmod n\,(= rn+1)$ für beliebiges $n \in \mathbb{N}$ um die Körpererweiterung
$$\mathbb{Q} \subseteq \mathbb{Q}(e^{\frac{2\pi i}{p}})$$
zu betrachten.

- Berechne die Galoisgruppe dieser Körpererweiterung und zeige, dass diese isomorph zu $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/rn\mathbb{Z}$ ist.

- Überprüfe, dass es sich um eine Galoiserweiterung handelt, um den Hauptsatz anwenden zu können.

- Aus der Tatsache, dass $\mathbb{Z}/r\mathbb{Z} \lhd \mathbb{Z}/rn\mathbb{Z}$, folgt, dass $\mathbb{Q} \subseteq \mathrm{Fix}(\mathbb{Z}/r\mathbb{Z})$ eine Galoiser-

weiterung ist, deren Galoisgruppe laut Hauptsatz gerade

$$\mathrm{Gal}(\mathrm{Fix}(\mathbb{Z}/r\mathbb{Z}), \mathbb{Q}) \cong (\mathbb{Z}/rn\mathbb{Z})\big/(\mathbb{Z}/r\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$$

womit die Behauptung gezeigt ist.

5 Endliche abelsche Gruppen

Jetz kommen wir zum eigentlichen Ziel dieser Arbeit, nämlich folgendes Teilresultat des inversen Galoisproblems zu beweisen:

Alle endlichen abelschen Gruppen treten als Galoisgruppe einer Körpererweiterung über $\mathbb{Q}$ auf.

Wir beschäftigen uns jetzt also mit endlichen abelschen Gruppen. Wie eine solche Gruppe aussieht, sagt uns der Struktursatz für endliche abelsche Gruppen:

Satz 6 (Strukturssatz für endliche abelsche Gruppen)**.** *(zit. [6, S. 137])*
Jede endliche abelsche Gruppe G ist isomorph zu einem Produkt

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_t\mathbb{Z},\ m_1|m_2|\ldots|m_t,\ m_1 > 1.$$

Die Anzahl t und die auftauchenden Ordnungen m_i mit ihren Vielfachheiten sind durch diese Teilbarkeitsbedingungen eindeutig bestimmt.

Sein nun G eine beliebige endliche abelsche Gruppe. Nach vorherigem Satz gibt es also $n_i \in \mathbb{N}$ mit obigen Eigenschaften, sodass

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}.$$

Nun haben wir bereits im vorherigen Abschnitt gesehen, dass nach dem Satz von Dirichlet in jeder arithmetischen Folge $\{ak + b \,|\, k \in \mathbb{N}\}$, $\mathrm{ggT}(a, b) = 1$ unendlich viele Primzahlen auftauchen. Deshalb wählen wir nun Primzahlen $p_1, \ldots, p_r$ so, dass gilt:

$$\begin{aligned} p_1 &\equiv 1 \bmod n_1 \\ p_2 &\equiv 1 \bmod n_2 \\ &\vdots \\ p_r &\equiv 1 \bmod n_r \end{aligned}$$

Zudem können wir fordern, dass die Primzahlen alle verschieden sein sollen, da ja in jeder Folge unendlich viele Primzahlen vorkommen.
Sei nun $n = p_1 \cdot p_2 \cdots p_r$ und weiters $\xi = e^{\frac{2\pi i}{n}}$.
Wie vorher betrachten wir die Galoiserweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\xi)$ und wollen ihre Galoisgruppe bestimmen. Wir werden zeigen, dass gilt

$$\mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

Wie wir bereits wissen, gilt für alle φ aus der Galoisgruppe, dass Nullstellen eines Polynoms nur auf Nullstellen desselben Polynoms abgebildet werden. In diesem Fall können wir unter den Nullstellen eine Unterscheidung treffen und zwar in primitive und nicht primitive Einheitswurzeln. Dabei erzeugen primitive Einheitswurzeln alle anderen Einheitswurzeln, nicht primitive hingegen nicht, wie zum Beispiel die Eins ($1^k = 1, \forall k \in \{1, \dots, n\}$).
Dabei werden von den $\mathbb{Q}$-Automorphismen der Galoisgruppe primitive Einheitswurzeln stets auf primitive abgebildet und nicht primitive auf nicht primitive Einheitswurzeln.
Wir wollen uns nun überlegen, wann genau eine Einheitswurzel denn primitiv ist: *Eine Einheitswurzel ist genau dann primitiv, wenn ihre Potenz bezüglich* $e^{\frac{2\pi i}{n}}$ *teilerfremd zu* n *ist.*
Diese Aussage gilt es nun zu beweisen:
Sei $\xi = e^{\frac{2\pi i}{n}}$.

$$\text{z.z.:} \quad \xi^k \text{ primitiv} \quad \Longleftrightarrow \quad \text{ggT}(k, n) = 1.$$

Beweis. "$\Rightarrow$": Sei ξ^k eine primitive Einheitswurzel, d.h. ξ^k erzeugt alle anderen Einheitswurzeln.
Wähle $1 \leq l < n$ sodass gilt

$$\begin{aligned} &\xi^{k \cdot l} = \xi \\ \Longrightarrow &kl = 1 \bmod n \\ \Longrightarrow &kl = rn + 1 \\ \Longrightarrow &1 = lk - rn \\ \Longrightarrow &\text{ggT}(k, n) = 1 \end{aligned}$$

"$\Leftarrow$": Sei $1 \leq k < n$ mit $\text{ggT}(k, n) = 1$.
Man kann ein eindeutiges $l \in \{1, \dots, n-1\}$ finden, sodass gilt

$$k \cdot l = 1 \bmod n$$

Daraus folgt nun, dass $\xi^{k \cdot l} = \xi$.
Da ξ eine primitive Einheitswurzel ist, muss folglich auch ξ^k primitiv sein.
Denn sei η eine beliebige Einheitswurzel, dann gibt es $m \in \{1, \dots, n-1\}$ mit

$$\eta = \xi^m = \xi^{(kl)m} = \xi^{k(lm)}$$

$$\Longrightarrow \xi^k \text{ erzeugt alle Einheitswurzeln.}$$

□

Wir wissen jetzt also eine Einheitswurzel ist genau dann primitiv, wenn ihre Potenz bezüglich ξ teilerfremd zu n ist.
Was wir aber eigentlich folgern wollen, ist, dass die Galoisgruppe der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ entspricht. Das heißt wir müssen zeigen, dass die Potenzen der primitiven Einheitswurzeln -auf welche die Einheitswurzeln durch die $\mathbb{Q}$-Automorphismen der Galoisgruppe abgebildet werden- in der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ liegen.

Mit dem Beweis von Aussage 2 wissen wir bereits, dass die zwei Aussagen "ξ^k ist primitiv" und "$k \in (\mathbb{Z}/n\mathbb{Z})^\times$" zueinander äquivalent sind.
Wir betrachten jetzt nochmals die Galoisgruppe

$$\mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q}) = \{\varphi : \mathbb{Q}(\xi) \to \mathbb{Q}(\xi) \,|\, \varphi \text{ Automorphismus } \wedge\, \varphi|_{\mathbb{Q}} = id\}.$$

Sei φ aus dieser Galoisgruppe beliebig. Aufgrund der Homogenität müssen Nullstellen auf Nullstellen abgebildet werden, also muss $\varphi(\xi)$ die Gestalt ξ^k für ein $k \in \{1, \ldots, n\}$ haben. Da es sich zudem um einen Isomorphismus handelt, wissen wir, dass ξ^k ebenfalls primitiv sein muss. Das heißt, wenn man sich überlegt zu welcher Potenz ξ erhoben werden kann, sodass das Bild primitiv bleibt, sind das gerade jene Potenzen aus $(\mathbb{Z}/n\mathbb{Z})^\times$.
Noch einmal exakt formuliert:
Gegeben: $\varphi : \mathbb{Q}(\xi) \longrightarrow \mathbb{Q}(\xi)$ mit $\varphi(\xi) = \xi^k$, für ein $k = 1, \ldots, n$. Es gilt:

$\varphi \in \mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$ (also Isomorphismus) $\Leftrightarrow \xi^k$ primitiv $\Leftrightarrow \mathrm{ggT}(k, n) = 1 \Leftrightarrow k \in (\mathbb{Z}/n\mathbb{Z})^\times$

also $\mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

An dieser Stelle können wir nun den chinesischen Restsatz verwenden um die Situation auf den Fall der zyklischen Gruppen zurückzuführen. Anschließend können wir analog argumentieren um das gewünschte Resultat zu folgern.

Satz 7 (Chinesischer Restsatz)**.** *Sei R ein Ring und $I_1, \ldots, I_n \lhd R$ Ideale mit*

$$I_i + I_j = R \text{ für } i \neq j.$$

Dann induzieren die kanonischen Projektionen einen Isomorphismus

$$R/(I_1 \cap \ldots \cap I_n) \cong R/I_1 \times \ldots \times R/I_n.$$

Insbesondere gibt es für jede Wahl von $a_1, \ldots, a_n \in R$ ein Element $a \in R$ mit

$$a \equiv a_i \bmod I_i$$

für $i = 1, \ldots, n$.

In unserem Fall ist der Ring R der Ring der ganzen Zahlen $\mathbb{Z}$ und die Ideale sind

$p_i\mathbb{Z}, i = 1, \ldots, r$.
Zuerst müssen wir überprüfen, ob die Eigenschaft der Ideale $I_i + I_j = R$ für $i \neq j$ erfüllt ist.
Im Allgemeinen gilt, dass $n\mathbb{Z} + m\mathbb{Z} = \text{ ggT}(n, m)\mathbb{Z}$.
Da es sich bei den $p_i, i = 1, \ldots, r$, um Primzahlen handelt und sie also teilerfremd sind, erhalten wir

$$p_i\mathbb{Z} + p_j\mathbb{Z} = 1 \cdot \mathbb{Z} = \mathbb{Z}, \text{ für } i \neq j.$$

Da diese Eigenschaft erfüllt ist und somit die Voraussetzungen des chinesischen Restsatzes, gilt also

$$\mathbb{Z}/(p_1\mathbb{Z} \cap \ldots \cap p_r\mathbb{Z}) \cong \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r\mathbb{Z}.$$

Nun sind wir fast am Ziel. Betrachten wir den Schnitt $p_1\mathbb{Z} \cap \ldots \cap p_r\mathbb{Z}$.
Der Schnitt dieser Ideale beinhaltet all jene Elemente, die Vielfaches von allen $p_i (i = 1, \ldots, r)$ gleichzeitig sind. Anders formuliert, sind das also alle Vielfachen der kleinsten Zahl, die von allen p_i geteilt wird, also gerade die Vielfachen des kleinsten gemeinsamen Vielfachen von $p_1, \ldots, p_r$.
Da es sich bei allen p_i um Primzahlen handelt und sie somit teilerfremd sind, gilt

$$\text{kgV}(p_1, \ldots, p_r) = p_1 \cdot p_2 \cdots p_r.$$

Also folgt insgesamt:

$$\begin{aligned} \mathbb{Z}/(p_1\mathbb{Z} \cap \ldots \cap p_r\mathbb{Z}) &= \mathbb{Z}/p_1 \cdot p_2 \cdots p_r\mathbb{Z} \\ &\cong \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r\mathbb{Z} \end{aligned}$$

Mit diesem Wissen können wir nun die letzten Beweisschritte durchführen und das Endresultat folgern:

Wir waren stehengeblieben an dem Punkt, dass

$$\text{Gal}(\mathbb{Q}(\xi), \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

wobei $n = p_1 \cdot p_2 \cdots p_r$. Also

$$\text{Gal}(\mathbb{Q}(\xi), \mathbb{Q}) \cong (\mathbb{Z}/p_1 \cdot p_2 \cdots p_r\mathbb{Z})^\times.$$

Wie wir bereits vorher gesehen haben, folgt nun aus dem chinesischem Restsatz

$$(\mathbb{Z}/p_1 \cdot p_2 \cdots p_r\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r\mathbb{Z})^\times.$$

Es gilt, dass die Einheitengruppe eines kartesischen Produktes gerade das kartesische

Produkt der Einheitengruppen ist:

$$\begin{aligned}(\mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r\mathbb{Z})^\times &= (\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r\mathbb{Z})^\times \\ &\overset{p_i \text{ Primzahlen}}{=} \mathbb{Z}/(p_1-1)\mathbb{Z} \times \ldots \times \mathbb{Z}/(p_r-1)\mathbb{Z} \\ &\overset{p_i = s_i n_i + 1}{=} \mathbb{Z}/s_1n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/s_rn_r\mathbb{Z}.\end{aligned}$$

In den einzelnen Komponenten dieses Produktes befinden wir uns jetzt endlich im vorherigen Fall der zyklischen Gruppen. Durch analoge Vorgehensweise gibt es für jede zyklische Gruppe $\mathbb{Z}/s_in_i\mathbb{Z}$ einen Normalteiler $\mathbb{Z}/s_i\mathbb{Z}$, dessen Fixkörper $\mathrm{Fix}(\mathbb{Z}/s_i\mathbb{Z})$ eine Galoiserweiterung von $\mathbb{Q}$ ist.
Nach dem Haupsatz der Galoistheorie ist nun wiederum

$$\begin{aligned}\mathrm{Gal}(\mathrm{Fix}(\mathbb{Z}/s_i\mathbb{Z}), \mathbb{Q}) &\cong (\mathbb{Z}/s_in_i\mathbb{Z})/(\mathbb{Z}/s_i\mathbb{Z}) \\ &\cong \mathbb{Z}/n_i\mathbb{Z}\end{aligned}$$

Diese Vorgehensweise kann man analog für das Produkt durchführen, da stets gilt: der Normalteiler des Produktes, ist das Produkt der Normalteiler usw...
Das heißt am Ende erhalten wir:

$$\begin{aligned}&\mathrm{Gal}(\mathrm{Fix}(\mathbb{Z}/s_1\mathbb{Z} \times \ldots \times \mathbb{Z}/s_r\mathbb{Z}), \mathbb{Q}) && \cong \\ &(\mathbb{Z}/s_1n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/s_rn_r\mathbb{Z})/(\mathbb{Z}/s_1\mathbb{Z} \times \ldots \times \mathbb{Z}/s_r\mathbb{Z}) && \cong \\ &\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z} && \cong G\end{aligned}$$

$\Rightarrow$ Alle endlichen abelschen Gruppen treten als Galoiserweiterung einer Körpererweiterung über $\mathbb{Q}$ auf.

Auch hier wollen wir die wichtigsten Beweisschritte nochmals angeben:

- Betrachte eine beliebige endliche abelsche Gruppe G mit

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$$

- Wähle verschiedene Primzahlen

$$\begin{aligned}p_1 &\equiv 1 \bmod n_1 \\ &\vdots \\ p_r &\equiv 1 \bmod n_r\end{aligned}$$

- Betrachte die Galoiserweiterung $\mathbb{Q} \subseteq \mathbb{Q}(e^{\frac{2\pi i}{n}})$ mit $n = p_1 \cdot p_2 \cdots p_r$ und bestimme ihre Galoisgruppe und zeige, dass

$$\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}}), \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

- Schreibe $(\mathbb{Z}/n\mathbb{Z})^\times$ mit Hilfe des chinesischen Restsatzes als

$$\mathbb{Z}/s_1n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/s_rn_r\mathbb{Z}$$

- Nun wendet man die Vorgehensweise für die zyklischen Gruppen auf die einzelnen Faktoren an und erhält die gewünschte Aussage

$$\mathrm{Gal}(\mathrm{Fix}(\mathbb{Z}/s_1\mathbb{Z} \times \ldots \times \mathbb{Z}/s_r\mathbb{Z}), \mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}.$$

- Da alle n_i beliebig gewählt sind, ist also jede endliche abelsche Gruppe die Galoisgruppe einer Körpererweiterung über $\mathbb{Q}$.

Literatur

[1] Fischer G. (2011) *Lehrbuch der Algebra: Mit lebendigen Beispielen, ausführlichen Erläuterungen und zahlreichen Bildern* (2., überarbeitete Auflage), Wiesbaden : Vieweg+Teubner Verlag

[2] Grieser D. (2007) *Grundideen der Galoistheorie: Eine Kurzeinführung für Interessierte (fast) ohne Vorkenntnisse*, Oldenburg http://www.staff.uni-oldenburg.de/daniel.grieser/wwwpapers/Grundideen_Galois.pdf

[3] Lang S., Axler S., Gehring F.W., Ribet K.A. (2012) *Algebra (Graduate Texts in Mathematics)* (Revised Third Edition), New York: Springer

[4] Netzer T. (2017) *Algebra* (Vorlesungsskript), Innsbruck: Universität, Institut für Mathematik

[5] Rose H. (1994) *A Course in Number Theory* (Second Edition), Oxford

[6] Scharlau R. (2013) *Algebra und Zahlentheorie*, http://www.mathematik.tu-dortmund.de/%7Ealgebra/Algebra_ZT_2013/Skript/algebra-zt_kap2-3.pdf

[7] Stroth G. (2012) *Elementare Algebra und Zahlentheorie*, Basel: Birkhäuser