Körper- und Galoistheorie

Prof. Dr. Holger Brenner
Universität Osnabrück
Fachbereich Mathematik/Informatik

Wintersemester 2018/2019

Inhaltsverzeichnis

Vorwort

Dieses Skript gibt die Vorlesung Körper- und Galoistheorie wieder, die ich im Wintersemester 2018/19 an der Universität Osnabrück im Studiengang Mathematik gehalten habe.

Beim Übungsgruppenleiter Jonathan Steinbuch bedanke ich mich für die Durchführung des Übungsbetriebs. Bei Frau Marianne Gausmann bedanke ich mich für die Erstellung der Pdf-Files und bei Toan und den Studierenden für einzelne Korrekturen.

Holger Brenner

1. Vorlesung - Die Formeln von Cardano

1.1. **Lösungen von polynomialen Gleichungen.**

Es sei eine polynomiale Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \ = \ 0$$

gegeben, wobei die Koeffizienten $a_0, a_1, \ldots, a_n$ reelle (oder komplexe) Zahlen seien und nach Elementen $x \in \mathbb{C}$ gesucht wird, die diese Gleichung erfüllen. Wie kann man solche Lösungen finden? Die Lösbarkeit hängt dabei natürlich wesentlich vom Grad der Gleichung ab, das ist der maximale Index n mit $a_n \neq 0$. Bei $n = 1$ liegt eine lineare Gleichung $a_1 x + a_0 = 0$ vor mit der eindeutigen Lösung $x = -\frac{a_0}{a_1}$. Dies kann man bilden, da nach Voraussetzung $a_1 \neq 0$ ist und da die Koeffizienten aus $\mathbb{C}$ sind, also aus einem Körper, wo man uneingeschränkt durch von 0 verschiedene Zahlen dividieren kann. Bei $n = 2$ liegt eine *quadratische Gleichung* vor, also

$$a_2 x^2 + a_1 x + a_0 \ = \ 0$$

mit $a_2 \neq 0$. Hier führt man zunächst eine *Normierung* durch, was man bei jedem Grad machen kann. Das bedeutet, dass man durch den Leitkoeffizienten a_n dividiert, um diesen zu 1 zu normieren. Dabei ändern sich die Lösungen der Gleichung offenbar nicht. Im quadratischen Fall gelangt man so zur äquivalenten Gleichung

$$x^2 + b_1 x + b_0 \ = \ 0.$$

Diese Gleichung führt man durch *quadratisches Ergänzen* auf eine reine Gleichung zurück. Man macht den Ansatz $y = x + \frac{b_1}{2}$ und schreibt dann die Gleichung als

$$\left(x + \frac{b_1}{2}\right)^2 + b_0 - \left(\frac{b_1}{2}\right)^2 \ = \ x^2 + b_1 x + b_0 \ = \ 0$$

bzw. als

$$y^2 + c_0 \ = \ 0$$

mit $c_0 = b_0 - \left(\frac{b_1}{2}\right)^2$. Dieser Koeffizient c_0 gehört wieder zum Körper. Wenn y_1 eine Lösung dieser Gleichung ist, so ist $x_1 = y_1 - \frac{b_1}{2}$ eine Lösung der quadratischen Ausgangsgleichung. Die neu gewonnene äquivalente Gleichung ist eine sogenannte *reine Gleichung*, d.h. eine Gleichung der Form

$$y^n \ = \ d.$$

Um eine solche reine Gleichung lösen zu können muss man „die“ n-te Wurzel aus d ziehen können. Die Schwierigkeit dieser Aufgabe und die Anzahl der Lösungen hängt von der Arithmetik des Körpers ab und ist nicht trivial. Dennoch ist es eine wesentliche Reduktion, wenn man, wie im quadratischen Fall, die Lösung einer polynomialen Gleichung auf die Lösung einer (oder mehrerer) reinen Gleichungen zurückführen kann.

1.2. **Kubische Gleichungen.**

Wir betrachten nun eine normierte kubische Gleichung

$$x^3 + a_2x^2 + a_1x + a_0 \;=\; 0,$$

wobei die Koeffizienten aus $\mathbb{C}$ seien. Mit einem Ergänzungstrick können wir den quadratischen Koeffizienten a_2 eliminieren. Wir machen den Ansatz $y = x + \frac{a_2}{3}$ und schreiben die Gleichung als

$$\left(x+\frac{a_2}{3}\right)^3+\left(a_1-3\left(\frac{a_2}{3}\right)^2\right)\left(x+\frac{a_2}{3}\right)-\left(a_1-3\left(\frac{a_2}{3}\right)^2\right)\frac{a_2}{3}-\left(\frac{a_2}{3}\right)^3+a_0 \;=\; 0$$

bzw. als $y^3 + py + q \;=\; 0$ mit den neuen Koeffizienten

$$p = a_1 - 3\left(\frac{a_2}{3}\right)^2 \text{ und } q = -\left(a_1 - 3\left(\frac{a_2}{3}\right)^2\right)\frac{a_2}{3} - \left(\frac{a_2}{3}\right)^3 + a_0\,.$$

Lösungen dieser vereinfachten Gleichung führen direkt zu Lösungen der Ausgangsgleichung.

Gerolamo Cardano (1501-1576)

Die vereinfachte Gleichung kann man über die folgende *Formel von Cardano* lösen. Wir brauchen dafür ein Lemma über dritte Einheitswurzeln von $\mathbb{C}$, das sind komplexe Zahlen η mit $\eta^3 \;=\; 1$, also die Lösungen der reinen kubischen Gleichung $x^3 \;=\; 1$.

Lemma 1.1. *Es gelten folgende Aussagen.*

(1) *Die dritten Einheitswurzeln in* $\mathbb{C}$ *sind* $1, \epsilon \;=\; -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}$ *und* $\eta \;=\; -\frac{1}{2} - \frac{\sqrt{3}}{2}\mathrm{i}$.
(2) *Es ist* $\epsilon^2 \;=\; \eta$ *und* $\eta^2 \;=\; \epsilon$.
(3) *Es ist* $1 + \epsilon + \epsilon^2 \;=\; 0$.
(4) *Es ist* $\epsilon + \epsilon^2 \;=\; -1$.

Beweis. Siehe Aufgabe 1.2. □

Satz 1.2. *Es sei*

$$x^3 + px + q = 0$$

mit $p, q \in \mathbb{C}$ eine kubische Gleichung. Wir setzen $D = -4p^3 - 27q^2$. Es seien

$$u = \sqrt[3]{\frac{1}{2}\left(-q + \frac{1}{9}\sqrt{-3D}\right)} \text{ und } v = \sqrt[3]{\frac{1}{2}\left(-q - \frac{1}{9}\sqrt{-3D}\right)},$$

wobei diese dritten Wurzeln so gewählt seien, dass $uv = -\frac{p}{3}$ ist. Dann sind (mit der dritten Einheitswurzel $\epsilon = -\frac{1}{2} + \frac{1}{2}\sqrt{3}\mathrm{i}$) die Elemente

$$u + v, \epsilon u + \epsilon^2 v \text{ und } \epsilon^2 u + \epsilon v$$

die Lösungen dieser kubischen Gleichung.

Beweis. Wir zeigen zuerst, dass die dritten Wurzeln u und v so gewählt werden können, dass ihr Produkt gleich $-\frac{1}{3}p$ ist. Für eine irgendwie gewählte Quadratwurzel $\sqrt{-3D}$ und irgendwie gewählte dritte Wurzeln u und v ist

$$\begin{aligned} uv &= \sqrt[3]{\frac{1}{4}\left(q^2 - \frac{1}{81}(-3D)\right)} \\ &= \sqrt[3]{\frac{1}{4}\left(q^2 + \frac{1}{27}\left(-4p^3 - 27q^2\right)\right)} \\ &= \sqrt[3]{\frac{1}{4} \cdot \frac{-4}{27}p^3} \\ &= \sqrt[3]{-\frac{1}{27}p^3} \\ &= \eta\left(-\frac{p}{3}\right), \end{aligned}$$

wobei η eine dritte Einheitswurzel ist. Ersetzt man nun v durch $\eta^2 v$, so ist das Produkt gleich $-\frac{p}{3}$.

Wir berechen nun

$$(x - u - v)(x - \epsilon u - \epsilon^2 v)(x - \epsilon^2 u - \epsilon v)$$

und müssen zeigen, dass dies gleich $x^3 + px + q$ ist. Die angegebenen Elemente sind offenbar die Nullstellen dieses faktorisierten Polynoms. Es ist

$$\begin{aligned} & (x - u - v)(x - \epsilon u - \epsilon^2 v)(x - \epsilon^2 u - \epsilon v) \\ = \; & x^3 - (u + v + \epsilon u + \epsilon^2 v + \epsilon^2 u + \epsilon v)x^2 \\ & +((u + v)(\epsilon u + \epsilon^2 v) + (u + v)(\epsilon^2 u + \epsilon v) + (\epsilon u + \epsilon^2 v)(\epsilon^2 u + \epsilon v))x \\ & -(u + v)(\epsilon u + \epsilon^2 v)(\epsilon^2 u + \epsilon v). \end{aligned}$$

Der quadratische Koeffizient ist (unter Verwendung von Lemma 1.1)

$$u\left(1 + \epsilon + \epsilon^2\right) + v\left(1 + \epsilon + \epsilon^2\right) = 0.$$

Der lineare Koeffizient ist

$$\begin{aligned} & (u+v)\left(\epsilon u+\epsilon^2 v\right)+(u+v)\left(\epsilon^2 u+\epsilon v\right)+\left(\epsilon u+\epsilon^2 v\right)\left(\epsilon^2 u+\epsilon v\right) \\ = \; & u^2\left(\epsilon+\epsilon^2+1\right)+v^2\left(\epsilon^2+\epsilon+1\right)+uv\left(\epsilon+\epsilon^2+\epsilon^2+\epsilon+\epsilon^2+\epsilon^4\right) \\ = \; & -\frac{p}{3}(-3) \\ = \; & p. \end{aligned}$$

Der konstante Koeffizient ist

$$\begin{aligned} & -(u+v)\left(\epsilon u+\epsilon^2 v\right)\left(\epsilon^2 u+\epsilon v\right) \\ = \; & -u^3-u^2 v\left(1+\epsilon+\epsilon^2\right)-uv^2\left(1+\epsilon+\epsilon^2\right)-v^3 \\ = \; & -u^3-v^3 \\ = \; & -\frac{1}{2}\left(-q+\frac{1}{9}\sqrt{-3D}\right)-\frac{1}{2}\left(-q-\frac{1}{9}\sqrt{-3D}\right) \\ = \; & q. \end{aligned}$$

□

Beispiel 1.3. Wir betrachten die kubische Gleichung

$$x^3+2x-1 \;=\; 0$$

und wenden darauf Satz 1.2 an. Es ist demnach $p=2$, $q=-1$ und $D=-59$ und somit $u=\sqrt[3]{\frac{1}{2}\left(1+\frac{1}{9}\sqrt{177}\right)}$ und $v=\sqrt[3]{\frac{1}{2}\left(1-\frac{1}{9}\sqrt{177}\right)}$. Dabei wählen wir jeweils die reellen dritten Wurzeln, was automatisch die reelle Bedingung $uv=-\frac{2}{3}$ sicherstellt. Somit ist $u+v$ eine reelle Lösung der Gleichung. Man sieht, dass diese Lösung aus Lösungen von rein-quadratischen und rein-kubischen Gleichungen mittels arithmetischer Ausdrücke zusammengesetzt ist, darüber hinaus aber keine einfache Gestalt besitzt. Den numerischen Wert dieser Lösung kann man beliebig genau durch beliebig genaue Berechnungen der Lösungen der reinen Gleichungen ausrechnen, doch könnte man genauso gut direkt (mit dem Halbierungsverfahren oder Ähnlichem) die Nullstelle numerisch berechnen.

Für den Fall eines Polynoms vom Grad 4 gibt es ebenfalls eine Lösungsformel in dem Sinne, dass man die Nullstellen als einen verschachtelten Ausdruck von reinen Wurzeln ausdrücken kann. Eine Hauptmotivation zur Entwicklung der Körper- und Galoistheorie war die Fragestellung, ob es für Polynome vom Grad ≥ 5 ebenfalls Formeln gibt, mit denen man die Nullstellen als arithmetische Ausdrücke in Lösungen zu reinen Gleichungen ausdrücken kann. Eines der Hauptergebnisse, das wir nach einigen Vorbereitungen beweisen werden, ist, dass es eine solche Formel nicht geben kann.

1.3. **Der Fundamentalsatz der Algebra.**

Sei ein Polynom $F \in K[X]$, wobei K einen Körper bezeichnet, bzw. die zugehörige Nullstellengleichung

$$F(x) \;=\; 0$$

gegeben. In K selbst muss F keine Nullstellen besitzen. Ist es überhaupt klar, dass F in irgend einem Körper Nullstellen besitzt? Oben gehörten alle Koeffizienten von F zum Körper $\mathbb{C}$ der komplexen Zahlen. Dies garantiert, dass es Lösungen zu der polynomialen Gleichung gibt. Diese Eigenschaft der komplexen Zahlen beruht auf dem Fundamentalsatz der Algebra, der in Analysis II bewiesen wurde und an den wir hier erinnern wollen.

Satz 1.4. *Jedes nichtkonstante Polynom $P \in \mathbb{C}[X]$ über den komplexen Zahlen besitzt eine Nullstelle.*

Beweis. Siehe den Beweis zu Satz 36.14 (Analysis (Osnabrück 2014-2016)). □

Bis jetzt kennen wir noch keinen anderen Körper mit dieser Eigenschaft, dennoch halten wir hier schonmal folgende Definition fest.

Definition 1.5. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nichtkonstante Polynom $F \in K[X]$ eine Nullstelle in K besitzt.

Mit diesem Begriff kann man den Fundamentalsatz der Algebra so ausdrücken, dass $\mathbb{C}$ algebraisch abgeschlossen ist.

Wenn man zu einem Polynom F eine Nullstelle α gefunden hat, so kann man nach Lemma 19.8 (Lineare Algebra (Osnabrück 2017-2018)) $F = (X-\alpha)\tilde{F}$ schreiben. Zu jedem normierten Polynom $F \in \mathbb{C}[X]$ vom Grad n gibt es daher eine Produktdarstellung

$$F = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$$

mit eindeutig komplexen Zahlen $\alpha_1, \ldots, \alpha_n$. Diese zu finden ist aber schwierig, selbst wenn die Koeffizienten von F harmlos sind (z.B. bei $F \in \mathbb{Q}[X]$), wie schon die Cardanosche Formel für den Grad 3 deutlich macht. Diese „Schwierigkeit“, bei höherem Grad Nullstellen explizit zu finden, ist ein wichtiges Thema dieser Vorlesung.

1.4. **Der algebraische Zugang.**

Es ist gut zu wissen, dass es zu einem Polynom $F \in \mathbb{C}[X]$ Nullstellen in $\mathbb{C}$ gibt und dass es daher eine Zerlegung des Polynoms in Linearfaktoren gibt. Allerdings muss man, neben der prinzipiellen Schwierigkeit, diese Nullstellen zu finden, bedenken, dass die komplexen Zahlen $\mathbb{C}$ auf den reellen Zahlen $\mathbb{R}$ beruhen, die selbst wiederum mit topologischen Mitteln (durch die Vervollständigung) aus den rationalen Zahlen $\mathbb{Q}$ konstruiert wurden. Hinter den komplexen Zahlen steckt also ein enormer technischer Apparat, während ein einzelnes Polynom eine völlig andere „Datenstruktur“ aufweist. Ein Polynom $F = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$ ist durch seine endlich vielen Koeffizienten $a_0, a_1, \ldots, a_n \in \mathbb{C}$ festgelegt, und seine Nullstellen sind n Zahlen $\alpha_1, \ldots, \alpha_n$ (die nicht verschieden sein müssen). Um Beziehungen zwischen den Koeffizienten und den Nullstellen ausdrücken zu können, braucht man

gar nicht die gesamten komplexen Zahlen. Es genügt, sich auf diejenigen arithmetischen Ausdrücke zu beschränken, die man ausgehend von den Koeffizienten und den Nullstellen konstruieren kann. Wenn z.B., wie das häufig der Fall sein wird, die Koeffizienten rationale Zahlen sind, so spielt sich alles innerhalb der polynomialen Ausdrücke über $\mathbb{Q}$ in den Nullstellen α_i ab, also Ausdrücken der Form

$$\sum_{\nu=(\nu_1,\ldots,\nu_n)} b_\nu \alpha_1^{\nu_1} \cdots \alpha_n^{\nu_n} .$$

Dabei sind die b_ν rationale Zahlen, und sämtliche Exponententupel $\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{N}^n$ sind erlaubt, wobei die Summe aber endlich ist.

Beispiel 1.6. Wir betrachten das Polynom $X^2 + 1$, dessen Koeffizienten zu $\mathbb{Q}$ gehören und das in $\mathbb{Q}$ (und auch in $\mathbb{R}$) keine Nullstelle besitzt. In den komplexen Zahlen besitzt es die beiden Nullstellen i und $-\mathrm{i}$, so dass in $\mathbb{C}[X]$ die Faktorzerlegung

$$X^2 + 1 = (X - \mathrm{i})(X + \mathrm{i})$$

vorliegt. Um dies hinschreiben zu können, braucht man aber nicht die gesamten komplexen Zahlen, sondern lediglich das Element i. Wir betrachten die Menge

$$\mathbb{Q}[\mathrm{i}] = \mathbb{Q}1 + \mathbb{Q}\mathrm{i} = \{a + b\mathrm{i} |\, a, b \in \mathbb{Q}\} ,$$

also einen zweidimensionalen $\mathbb{Q}$-Vektorraum mit den Basiselementen 1 und i, wobei zusätzlich noch eine Multiplikation durch die Bedingung $\mathrm{i}^2 = -1$ festgelegt wird. Dies ist die gleiche Konstruktion, mit der man aus $\mathbb{R}$ die komplexen Zahlen gewinnt, nur dass man hier von den rationalen Zahlen ausgeht. Es lässt sich leicht zeigen, dass das konstruierte Objekt $\mathbb{Q}[\mathrm{i}]$ ein Körper ist. Für ein von 0 verschiedenes Element $a + b\mathrm{i}$ ist

$$\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\mathrm{i}$$

das inverse Element, und dies gehört offenbar wieder zu $\mathbb{Q}[\mathrm{i}]$. Die Zerlegung $X^2 + 1 = (X - \mathrm{i})(X + \mathrm{i})$ gilt ebenfalls in $\mathbb{Q}[\mathrm{i}][X]$, und durch die Zuordnung $a+b\mathrm{i} \mapsto a-b\mathrm{i}$ gibt es auch eine Konjugation, die völlig analoge Eigenschaften hat wie die komplexe Konjugation in $\mathbb{C}$.

Beispiel 1.7. Wir betrachten das Polynom $X^2 - 3$, dessen Koeffizienten zu $\mathbb{Q}$ gehören. In den reellen Zahlen $\mathbb{R}$ besitzt dieses Polynom die Nullstelle[1] $\sqrt{3}$, die irrational ist. Über $\mathbb{R}$ hat man die Zerlegung $X^2-3 = (X-\sqrt{3})(X+\sqrt{3})$. Um dies auszudrücken, braucht man aber nicht die gesamten reellen Zahlen, sondern lediglich $\sqrt{3}$, das man einfach als ein Symbol auffassen kann mit der Eigenschaft, dass sein Quadrat gleich 3 sein soll. Eine „Verortung“ innerhalb der reellen Zahlen ist dazu nicht nötig. Präziser formuliert betrachtet man

$$L = \mathbb{Q}1 + \mathbb{Q}u = \{a + bu |\, a, b \in \mathbb{Q}\} ,$$

[1]Die Existenz der Nullstelle beruht auf dem Zwischenwertsatz, wobei sich die Existenz von $\sqrt{3}$ auch direkt aus der Vollständigkeit von $\mathbb{R}$ ergibt.

also einen zweidimensionalen $\mathbb{Q}$-Vektorraum mit den Basiselementen 1 und u, wobei eine Multiplikation durch die Bedingung $u^2 = 3$ (und distributive Fortsetzung) festgelegt wird. Das Element u ist hier lediglich ein Symbol, für das man häufig wegen der intendierten Eigenschaft auch $\sqrt{3}$ schreibt (man schreibt auch $L = \mathbb{Q}[\sqrt{3}]$). In L gilt die Zerlegung $X^2-3 = (X-u)(X+u)$, und wegen

$$(a+bu)\left(\frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}u\right) = \frac{a^2-3b^2}{a^2-3b^2} = 1$$

handelt es sich um einen Körper. Dazu muss man sich klar machen, dass bei $a+bu \neq 0$ mit rationalen Zahlen $a, b \in \mathbb{Q}$, die nicht beide 0 sind, auch $a^2-3b^2 \neq 0$ ist, was äquivalent zur Irrationalität von $\sqrt{3}$ ist. Es sind also wesentliche Eigenschaften des Polynoms X^2-3, die über $\mathbb{R}$ sichtbar werden, bereits über L sichtbar. Es gibt aber auch Unterschiede, beispielsweise sind bei dieser algebraischen Konstruktion von L die beiden Elemente u und $-u$ vollkommen gleichberechtigt, während innerhalb der reellen Zahlen die eine Quadratwurzel positiv und die andere negativ ist. Diese Gleichberechtigung zeigt sich auch darin, dass durch

$$L \longrightarrow L,\ a+bu \longmapsto a-bu,$$

eine „Konjugation“ definiert wird, die es innerhalb der reellen Zahlen nicht gibt.

1. Arbeitsblatt

1.1. **Aufwärmaufgaben.**

Aufgabe 1.1. Löse die quadratische Gleichung $4x^2+5x+2 = 0$ über $\mathbb{Z}/(7)$.

Aufgabe 1.2. Bestätige folgende Aussagen.

(1) Die dritten Einheitswurzeln in $\mathbb{C}$ sind 1, $\epsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}$ und $\eta = -\frac{1}{2} - \frac{\sqrt{3}}{2}\mathrm{i}$.
(2) Es ist $\epsilon^2 = \eta$ und $\eta^2 = \epsilon$.
(3) Es ist $1+\epsilon+\epsilon^2 = 0$.
(4) Es ist $\epsilon + \epsilon^2 = -1$.

Aufgabe 1.3. Eliminiere in der kubischen Gleichung

$$x^3 + 6x^2 - 5x - 2 = 0$$

den quadratischen Term.

Aufgabe 1.4.*
Eliminiere in der kubischen Gleichung

$$x^3 + 2x^2 - 2 = 0$$

den quadratischen Term.

Aufgabe 1.5. Finde die Nullstellen des Polynoms

$$X^3 - 3X^2 + 7X - 21$$

ohne die Formeln von Cardano.

Aufgabe 1.6.*
Zeige, dass

$$z = \sqrt[3]{-1+\sqrt{2}} + \sqrt[3]{-1-\sqrt{2}}$$

eine Nullstelle des Polynoms

$$X^3 + 3X + 2$$

ist.

Aufgabe 1.7. Finde die Lösungen der kubischen Gleichung

$$x^3 + px = 0$$

($p \in \mathbb{C}$) direkt und mit Hilfe der Formel von Cardano.

Aufgabe 1.8.*
Zeige, dass

$$-\frac{2}{3} + \frac{1}{3}\sqrt[3]{19+3\sqrt{33}} + \frac{1}{3}\sqrt[3]{19-3\sqrt{33}}$$

eine Nullstelle des Polynoms

$$X^3 + 2X^2 - 2$$

ist.

Aufgabe 1.9.*
Bestimme eine reelle Lösung der Gleichung

$$z^3 - \frac{4}{3}z - \frac{38}{27} = 0$$

mit der Cardanoschen Formel.

Aufgabe 1.10. Bestimme die Lösungen der Gleichung

$$x^3 - x + 5 = 0$$

mit der Cardanoschen Formel.

Aufgabe 1.11. Bestimme die komplexen Eigenwerte der Matrix

$$\begin{pmatrix} 3 & 2 & 0 \\ 1 & 4 & 2 \\ 0 & -1 & 5 \end{pmatrix}.$$

Aufgabe 1.12. Löse die biquadratische Gleichung $x^4 + 7x^2 - 11 = 0$ über $\mathbb{R}$.

Aufgabe 1.13.*

Es sei

$$P = \frac{1}{24}X^4 - \frac{1}{2}X^2 + 1.$$

(1) Bestimme die kleinste positive Nullstelle von P.
(2) Besteht ein Zusammenhang zwischen dieser Nullstelle und $\frac{\pi}{2}$?

Aufgabe 1.14. Es sei p eine Primzahl. Zeige unter Verwendung der eindeutigen Primfaktorzerlegung von natürlichen Zahlen, dass die reelle Zahl $\sqrt{p}$ irrational ist.

Aufgabe 1.15. Führe in $\mathbb{Q}[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = 3X^4 + 7X^2 - 2X + 5$ und $T = 2X^2 + 3X - 1$ durch.

Aufgabe 1.16. Es sei $x^3 + a_2x^2 + a_1x + a_0 = 0$ eine kubische Gleichung mit $a_i \in \mathbb{Q}$. Eliminiere den linearen Term. Ist dies stets über $\mathbb{Q}$ möglich?

1.2. **Aufgaben zum Abgeben.**

Aufgabe 1.17. (4 Punkte)

Es sei

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

eine polynomiale Gleichung mit $a_i \in \mathbb{C}$, $a_n \neq 0$. Zeige, dass es eine äquivalente polynomiale Gleichung der Form

$$x^n + b_{n-2} x^{n-2} + \cdots + b_1 x + b_0 = 0$$

gibt.

Aufgabe 1.18. (6 Punkte)

Bestimme die Lösungen der Gleichung

$$2x^3 - 4x^2 + 5x - 3 = 0$$

mit der Cardanoschen Formel.

Aufgabe 1.19. (5 Punkte)

Bestimme die Lösungen der polynomialen Gleichung

$$x^6 - 4x^2 + 7 = 0\,.$$

Aufgabe 1.20. (3 Punkte)

Sei K ein algebraisch abgeschlossener Körper. Zeige, dass K nicht endlich sein kann.

In der nächsten Aufgabe soll über dem Körper $L = \mathbb{Q}[\sqrt{3}]$ aus Beispiel 1.7 gerechnet werden.

Aufgabe 1.21. (4 Punkte)

Führe in $(\mathbb{Q}[\sqrt{3}])[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = 3X^3 - (2+\sqrt{3})X^2 + 5\sqrt{3}X + 1 + 2\sqrt{3}$ und $T = \sqrt{3}X^2 - X + 2 + 7\sqrt{3}$ durch.

2. Vorlesung - Die Gradformel

2.1. **Körpererweiterungen.**

In der letzten Vorlesung haben wir gesehen, dass es sinnvoll sein kann, das Studium der Nullstellen eines Polynoms $F \in \mathbb{Q}[X]$ nicht in $\mathbb{C}$, sondern in einem kleineren Körper, der $\mathbb{Q}$ umfasst, durchzuführen. Wir stellen dazu die nötige Terminologie zusammen.

Definition 2.1. Es sei K ein Körper. Ein Unterring $M \subseteq K$, der zugleich ein Körper ist, heißt *Unterkörper* von K.

Wenn ein Unterring $R \subseteq K$ in einem Körper vorliegt, so muss man nur noch schauen, ob R mit jedem von 0 verschiedenen Element x auch das Inverse x^{-1} (das in K existiert) enthält. Bei einem Unterring $R \subseteq S$, wobei R ein Körper ist, aber S nicht, spricht man nicht von einem Unterkörper. Die Situation, bei der ein Körper in einem anderen Körper liegt, wird als Körpererweiterung bezeichnet.

Definition 2.2. Sei L ein Körper und $K \subseteq L$ ein Unterkörper von L. Dann heißt L ein *Erweiterungskörper* (oder *Oberkörper*) von K und die Inklusion $K \subseteq L$ heißt eine *Körpererweiterung*.

Für eine Körpererweiterung gilt stets folgende wichtige Beobachtung.

Lemma 2.3. *Sei $K \subseteq L$ eine Körpererweiterung. Dann ist L in natürlicher Weise ein K-Vektorraum.*

Beweis. Die Skalarmultiplikation

$$K \times L \longrightarrow L,\ (\lambda, x) \longmapsto \lambda x,$$

wird einfach durch die Multiplikation in L gegeben. Die Vektorraumaxiome folgen dann direkt aus den Körperaxiomen. □

Definition 2.4. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlichdimensionaler Vektorraum über K ist.

Definition 2.5. Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.

Der Grad einer endlichen Körpererweiterung $K \subseteq L$ wird mit

$$\operatorname{grad}_K L$$

bezeichnet. Dass man hier von Grad spricht und nicht einfach von Dimension hat seinen Grund darin, dass dieser Grad mit dem Grad von gewissen Polynomen zusammenhängt, worauf wir ausführlich zu sprechen kommen werden. Da bei einer Körpererweiterung $K \subseteq L$ sofort eine K-Vektorraumstruktur auf L zur Verfügung steht, ist es naheliegend, für das Studium der Körpererweiterungen die lineare Algebra einzusetzen. Dies ist besonders bei endlichen

Körpererweiterungen ein schlagkräftiges Mittel. Durch diesen Apparat wird unter Anderem die additive Struktur auf L einfach beschreibbar, und man kann sich ganz auf die Multiplikation konzentrieren. Aber auch für diese ist die Vektorraumstruktur reich an Konsequenzen. Um ein typisches Beispiel für die lineare Argumentationsweise zu geben, betrachten wir eine endliche Körpererweiterung $K \subseteq L$ und ein beliebiges Element $x \in L$. Die Potenzen von x, also

$$x^0 = 1, x^1 = x, x^2, x^3, \ldots$$

bilden eine unendliche Familie (auch wenn es unter den Potenzen Wiederholungen geben kann). Da diese Potenzen alle zu L gehören und L ein endlichdimensionaler K-Vektorraum ist, kann diese unendliche Familie nicht linear unabhängig sein, sondern es muss eine Beziehung der Form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

geben, bei der nicht alle Koeffizienten $a_i \in K$ gleich 0 sind. Diese Beobachtung führt zu den Begriffen *algebraisches Element* und *Minimalpolynom*.

Die einzige Körpererweiterung vom Grad 1 ist die Identität $K \subseteq K$. Die Körpererweiterungen vom Grad zwei sind aber schon eine umfangreiche Beispielklasse und bekommen einen eigenen Namen. Zu ihnen gehören die beiden letzten Beispiele der ersten Vorlesung.

Definition 2.6. Eine endliche Körpererweiterung $K \subseteq L$ vom Grad zwei heißt eine *quadratische Körpererweiterung*.

Die folgende Aussage ist eine Version der quadratischen Ergänzung.

Lemma 2.7. *Es sei K ein Körper mit einer Charakteristik $\neq 2$[2] und es sei $K \subseteq L$ eine quadratische Körpererweiterung. Dann gibt es ein $x \in L$, $x \notin K$ und $x^2 \in K$.*

Beweis. Siehe Aufgabe 2.7. □

2.2. **Die Gradformel.**

Häufig studiert man Körpererweiterungen $K \subseteq M$ dadurch, dass man Zwischenkörper L, $K \subseteq L \subseteq M$, betrachtet, und die beiden einzelnen (häufig einfacheren) Körpererweiterungen $K \subseteq L$ und $L \subseteq M$ untersucht. Man spricht von einem *Körperturm* oder einer *Körperkette*. In dieser Situation gilt die folgende wichtige *Gradformel*.

Satz 2.8. *Seien $K \subseteq L$ und $L \subseteq M$ endliche Körpererweiterungen. Dann ist auch $K \subseteq M$ eine endliche Körpererweiterung und es gilt*

$$\operatorname{grad}_K M = \operatorname{grad}_K L \cdot \operatorname{grad}_L M.$$

[2]Diese Bedingung bedeutet, dass $0 \neq 2 = 1 + 1$ ist. Wir werden die Charakteristik eines Körpers bald einführen.

Beweis. Wir setzen $\operatorname{grad}_K L = n$ und $\operatorname{grad}_L M = m$. Es sei $x_1, \ldots, x_n \in L$ eine K-Basis von L und $y_1, \ldots, y_m \in M$ eine L-Basis von M. Wir behaupten, dass die Produkte

$$x_i y_j, 1 \leq i \leq n, 1 \leq j \leq m,$$

eine K-Basis von M bilden. Wir zeigen zuerst, dass diese Produkte den Vektorraum M über K erzeugen. Sei dazu $z \in M$. Wir schreiben

$$z = b_1 y_1 + \cdots + b_m y_m \text{ mit Koeffizienten } b_j \in L.$$

Wir können jedes b_j als $b_j = a_{1j} x_1 + \cdots + a_{nj} x_n$ mit Koeffizienten $a_{ij} \in K$ ausdrücken. Das ergibt

$$\begin{aligned} z &= b_1 y_1 + \cdots + b_m y_m \\ &= (a_{11} x_1 + \cdots + a_{n1} x_n) y_1 + \cdots + (a_{1m} x_1 + \cdots + a_{nm} x_n) y_m \\ &= \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} a_{ij} x_i y_j. \end{aligned}$$

Daher ist z eine K-Linearkombination der Produkte $x_i y_j$. Um zu zeigen, dass diese Produkte linear unabhängig sind, sei

$$0 = \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} c_{ij} x_i y_j$$

angenommen mit $c_{ij} \in K$. Wir schreiben dies als $0 = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} c_{ij} x_i \right) y_j$. Da die y_j linear unabhängig über L sind und die Koeffizienten der y_j zu L gehören, folgt, dass $\sum_{i=1}^{n} c_{ij} x_i = 0$ ist für jedes j. Da die x_i linear unabhängig über K sind und $c_{ij} \in K$ ist, folgt, dass $c_{ij} = 0$ für alle i, j ist. □

2.3. **Reine Gleichungen.**

Die Lösungsformel von Cardano für ein kubisches Polynom zeigt, dass man die Nullstellen eines solchen Polynoms durch arithmetisch verschachtelte reine (zweite und dritte) Wurzeln ausdrücken kann. Solche reinen Wurzeln sind Nullstellen von sogenannten reinen Polynomen, also von Polynomen der Form

$$X^n - a\,,$$

wobei $a \in K$ ist und die Nullstelle in einem geeigneten Erweiterungskörper L von K liegen soll. Verglichen mit beliebigen Polynomen gelten solche reinen Polynome als vergleichsweise einfach, insbesondere wenn man an ein reelles positives a und seine reelle positive Wurzel $\sqrt[n]{a}$ denkt (und bei geradem n noch die zweite reelle Lösung $-\sqrt[n]{a}$ berücksichtigt). Allerdings zerfällt das Polynom $X^n - a$ über $\mathbb{C}$ in n Linearfaktoren, so dass bei $n \geq 3$ im Reellen nicht alle komplexen Lösungen sichtbar sind. Ein extremes Beispiel ist dabei das Polynom

$$X^n - 1$$

bzw. die Gleichung $X^n = 1$. Dies führt zu den sogenannten Einheitswurzeln.

2.4. **Einheitswurzeln.**

Definition 2.9. Es sei K ein Körper und $n \in \mathbb{N}_+$. Dann heißen die Nullstellen des Polynoms

$$X^n - 1$$

in K die n-ten *Einheitswurzeln* in K.

Die 1 ist für jedes n eine n-te Einheitswurzel, und die -1 ist für jedes gerade n eine n-te Einheitswurzel. Es gibt maximal n n-te Einheitswurzel, da das Polynom $X^n - 1$ nach Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) maximal n Nullstellen besitzt. Die Einheitswurzeln bilden eine endliche Untergruppe (mit $x^n = 1$ und $y^n = 1$ ist auch $(xy)^n = 1$, usw.) der Einheitengruppe $K^\times = K \setminus \{0\}$ des Körpers.

Im Reellen gibt es nur die Einheitswurzeln 1 oder 1 und -1, je nachdem, ob n gerade oder ungerade ist. Die komplexen Einheitswurzeln lassen sich einfach beschreiben und besitzen eine einfache geometrische Interpretation.

Lemma 2.10. *Sei $n \in \mathbb{N}_+$. Die Nullstellen des Polynoms $X^n - 1$ über $\mathbb{C}$ sind*

$$e^{2\pi \mathrm{i} k/n} = \cos \frac{2\pi k}{n} + \mathrm{i} \sin \frac{2\pi k}{n}, k = 0, 1, \ldots, n-1.$$

In $\mathbb{C}[X]$ gilt die Faktorisierung

$$X^n - 1 = (X-1)(X - e^{2\pi \mathrm{i}/n}) \cdots (X - e^{2\pi \mathrm{i}(n-1)/n}).$$

Beweis. Der Beweis verwendet einige Grundtatsachen über die komplexe Exponentialfunktion. Es ist

$$\left(e^{2\pi \mathrm{i} k/n}\right)^n = e^{2\pi \mathrm{i} k} = \left(e^{2\pi \mathrm{i}}\right)^k = 1^k = 1.$$

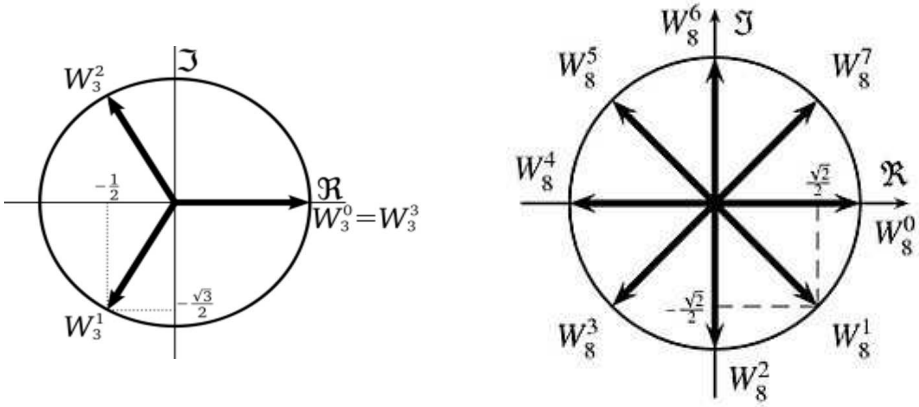
Die angegebenen komplexen Zahlen sind also wirklich Nullstellen des Polynoms $X^n - 1$. Diese Nullstellen sind alle untereinander verschieden, da aus

$$e^{2\pi \mathrm{i} k/n} = e^{2\pi \mathrm{i} \ell/n}$$

mit $0 \leq k \leq \ell \leq n-1$ sofort durch betrachten des Quotienten $e^{2\pi \mathrm{i}(\ell - k)/n} = 1$ folgt, und daraus

$$\ell - k = 0.$$

Es gibt also n explizit angegebene Nullstellen und daher müssen dies alle Nullstellen des Polynoms sein. Die explizite Beschreibung in Koordinaten folgt aus der eulerschen Formel. □



Korollar 2.11. *Es sei K ein Körper. Dann gilt in $K[X]$ die Beziehung*

$$X^n - 1 = (X-1) \cdot (X^{n-1} + X^{n-2} + \cdots + X + 1).$$

Für jede n-te Einheitswurzel $\zeta \neq 1$ gilt

$$\zeta^{n-1} + \zeta^{n-2} + \cdots + \zeta + 1 = 0$$

Beweis. Die erste Aussage ergibt sich durch Ausmultiplizieren der rechten Seite. Zum Beweis des Zusatzes sei eine n-te Einheitswurzel $\zeta \neq 1$ gegeben. Nach Definition ist $\zeta^n - 1 = 0$. Wegen $\zeta \neq 1$ muss also das rechte Polynom zu 0 werden, wenn man darin ζ einsetzt. □

Zu jedem $n \in \mathbb{N}$ gibt es einen kleinsten Unterkörper von $\mathbb{C}$, der alle n-ten Einheitswurzeln enthält, der sogenannte n-te *Kreisteilungskörper*. Wir werden bald sehen, dass der Kreisteilungskörper eine endliche Erweiterung von $\mathbb{Q}$ ist, und dass sein Grad maximal gleich $n-1$ ist. Genauere Gradberechnungen und weitere Strukturuntersuchungen dieser Körpererweiterungen werden im Laufe des Kurses noch folgen.

Mit den Einheitswurzeln lassen sich wiederum die Lösungen zu beliebigen reinen Gleichungen charakterisieren, insbesondere, wenn eine bekannt ist, wie das bei $X^n = a$ mit $a \in \mathbb{R}_+$ der Fall ist.

Lemma 2.12. *Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Dann gelten folgende Aussagen.*

(1) *Wenn $b_1, b_2 \in K$ zwei Lösungen der Gleichung $X^n = a$ sind und $b_2 \neq 0$, so ist ihr Quotient b_1/b_2 eine n-te Einheitswurzel.*
(2) *Wenn $b \in K$ eine Lösung der Gleichung $X^n = a$ und ζ eine n-te Einheitswurzel ist, so ist auch ζb eine Lösung der Gleichung $X^n = a$.*

Beweis. Siehe Aufgabe 2.14. □

2. Arbeitsblatt

2.1. **Aufwärmaufgaben.**

Aufgabe 2.1.*

Sei $K \subseteq L$ eine Körpererweiterung. Zeige, dass L ein K-Vektorraum ist.

Aufgabe 2.2.*

Bestimme den Grad der Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$.

Aufgabe 2.3. Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad 1. Zeige, dass $L = K$ ist.

Aufgabe 2.4. Berechne im Körper $\mathbb{Q}[\sqrt{7}]$ das Produkt

$$(-2 + \sqrt{7}) \cdot (4 - \sqrt{7}) .$$

Aufgabe 2.5. Bestimme in $\mathbb{Q}[\sqrt{7}]$ das Inverse von $2 + 5\sqrt{7}$.

Aufgabe 2.6. Sei $K \subseteq L$ eine endliche Körpererweiterung und seien $v_1, \ldots, v_n \in L$ Elemente, die eine K-Basis von L bilden. Sei $x \in L$, $x \neq 0$. Zeige, dass auch $xv_1, \ldots, xv_n \in L$ eine K-Basis von L bilden.

Aufgabe 2.7.*

Es sei K ein Körper mit einer Charakteristik $\neq 2$ und es sei $K \subset L$ eine quadratische Körpererweiterung. Zeige, dass es dann ein $x \in L$, $x \notin K$, mit $x^2 \in K$ gibt.

Aufgabe 2.8. Es sei $X^3 + pX + q \in \mathbb{Q}[X]$ und es seien $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ die Nullstellen dieses Polynoms. Konstruiere unter Bezug auf die Formel von Cardano eine Kette

$$\mathbb{Q} \subseteq K \subseteq L \subseteq M$$

von endlichen Körpererweiterungen von „möglichst kleinem“ Grad, so dass M alle Nullstellen und alle „Hilfszahlen“, die in dieser Formel auftreten, enthält. Welche Grade können dabei auftreten?

Aufgabe 2.9. Es sei $\mathbb{C} \subseteq L$ eine endliche Körpererweiterung. Zeige $\mathbb{C} = L$.

Aufgabe 2.10. Zeige, dass die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$ nicht endlich ist.

Aufgabe 2.11. Zeige, dass die Menge der rationalen Funktionen über $\mathbb{R}$ einen Körper bildet.

(Dieser Körper wird mit $\mathbb{R}(X)$ bezeichnet.)

Aufgabe 2.12. Es sei K ein Körper, $n \in \mathbb{N}$ und sei M die Menge der n-ten Einheitswurzeln in K. Zeige, dass M eine Untergruppe der Einheitengruppe $K^\times$ ist.

Aufgabe 2.13.*

Bestimme die Lösungen der Gleichung

$$x^3 - 3x + 1 = 0$$

mit der Cardanoschen Formel und drücke diese Lösungen mit Hilfe der neunten primitiven komplexen Einheitswurzel aus.

Aufgabe 2.14. Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Beweise die folgenden Aussagen.

(1) Wenn $b_1, b_2 \in K$ zwei Lösungen der Gleichung $X^n = a$ sind und $b_2 \neq 0$, so ist ihr Quotient b_1/b_2 eine n-te Einheitswurzel.
(2) Wenn $b \in K$ eine Lösung der Gleichung $X^n = a$ und ζ eine n-te Einheitswurzel ist, so ist auch ζb eine Lösung der Gleichung $X^n = a$.

2.2. **Aufgaben zum Abgeben.**

Aufgabe 2.15. (3 Punkte)

Es sei $K \subseteq \mathbb{R}$ ein Unterkörper. Zeige, dass dann auch $K[\mathrm{i}]$ ein Unterkörper von $\mathbb{C}$ ist.

Aufgabe 2.16. (2 Punkte)

Bestimme in $\mathbb{Q}[\sqrt{11}]$ das Inverse von $3 + 5\sqrt{11}$.

Aufgabe 2.17. (2 Punkte)

Sei $K \subseteq L$ eine endliche Körpererweiterung und sei $x_1, \ldots, x_n \in L$ eine K-Basis von L. Zeige, dass die Multiplikation auf L durch die Produkte

$$x_i x_j, 1 \leq i \leq j \leq n,$$

eindeutig festgelegt ist.

Aufgabe 2.18. (3 Punkte)

Es seien $\mathbb{Q} \subseteq K \subset \mathbb{C}$ und $\mathbb{Q} \subseteq L \subset \mathbb{C}$ zwei endliche Körpererweiterungen von $\mathbb{Q}$ vom Grad d bzw. e. Es seien d und e teilerfremd. Zeige, dass dann

$$K \cap L = \mathbb{Q}$$

ist.

Aufgabe 2.19. (3 Punkte)

Zeige, dass man $\sqrt{3}$ nicht als $\mathbb{Q}$-Linearkombination von 1 und $\sqrt{2}$ schreiben kann.

Aufgabe 2.20. (3 Punkte)

Berechne die Quadratwurzeln, die vierten Wurzeln und die achten Wurzeln von i.

Aufgabe 2.21. (3 Punkte)

Zeige, dass die Körpererweiterung $\mathbb{R} \subseteq \mathbb{R}(X)$, wobei $\mathbb{R}(X)$ den Körper der rationalen Funktionen bezeichnet, nicht endlich ist.

3. Vorlesung - Hauptidealbereiche

setcountersection3

Es sei $K \subseteq L$ eine endliche Körpererweiterung und $x \in L$ ein Element. Dann sind die Potenzen x^i, $i \in \mathbb{N}$, linear abhängig, und das bedeutet, dass es Koeffizienten $a_i \in K$ mit $a_n \neq 0$ mit $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$ gibt. Mit diesen Koeffizienten können wir das (von 0 verschiedene) Polynom

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in K[X]$$

bilden. Wenn man in dieses Polynom x einsetzt, d.h. überall die Variable X durch x ersetzt, so ergibt sich 0. Das Ergebnis dieses Einsetzens bezeichnet man mit $P(x)$, es ist also $P(x) = 0$. Man sagt, dass P das Element x *annulliert*. Wir betrachten die Menge

$$I = \{P \in K[X] | \, P(x) = 0\} \subseteq K[X],$$

also die Menge aller Polynome, die bei Einsetzung von x zu 0 werden.[3] Es ergeben sich dabei folgende Fragen.

(1) Welche Struktur besitzt I?

[3]In der letzten Vorlesung haben wir gesehen, dass eine Einheitswurzel ζ nach Definition von $X^n - 1$ annulliert wird, bei $\zeta \neq 1$ aber auch von $X^{n-1} + \cdots + X^1 + 1$. Gibt es noch weitere annullierende Polynome? Gibt es noch weitere annullierende Polynome von kleinerem Grad?

(2) Gibt es unter den Elementen $P \in I$ besonders einfache Polynome, mit denen man I einfach beschreiben kann?
(3) Kann man mit Hilfe von I Eigenschaften von $x \in L$ beschreiben?

Zu all diesen Fragen gibt es überzeugende Antworten. Zur ersten Frage können wir folgende Beobachtung machen: Das Nullpolynom gehört zu I. Wenn zwei Polynome P_1, P_2 zu I gehören, so gehört auch ihre Summe zu I, es ist ja $(P_1 + P_2)(x) = P_1(x) + P_2(x) = 0 + 0 = 0$. Für $P \in I$ und ein beliebiges Polynom $F \in K[X]$ ist auch $FP \in I$, wegen $(FP)(x) = F(x) \cdot P(x) = F(x) \cdot 0 = 0$.

3.1. **Ideale.**

Die soeben formulierten Eigenschaften der Menge von annullierenden Polynomen führt zur folgenden Definition.

Definition 3.1. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Ein Ideal ist eine Untergruppe der additiven Gruppe von R, die zusätzlich die zweite oben angeführte Eigenschaft erfüllt. Die einfachsten Ideale sind das *Nullideal* 0 und das *Einheitsideal* R.

Für den Ring der ganzen Zahlen $\mathbb{Z}$ sind Untergruppen und Ideale identische Begriffe. Dies folgt einerseits aus der Gestalt $H = \mathbb{Z}d$ für jede Untergruppe von $\mathbb{Z}$ (die ihrerseits aus der Division mit Rest folgt), aber ebenso direkt aus der Tatsache, dass für $k \in H$ und beliebiges $r \in \mathbb{N}$ gilt $rk = k + k + \cdots + k$ (r Summanden) und entsprechend für negatives r. Die Skalarmultiplikation mit einem beliebigen Ringelement lässt sich also bei $\mathbb{Z}$ auf die Addition zurückführen.

Definition 3.2. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

$$\mathfrak{a} = (a) = Ra = \{ra : r \in R\}$$

heißt *Hauptideal*.

Definition 3.3. Zu einer Familie von Elementen $a_j \in R$, $j \in J$, in einem kommutativen Ring R bezeichnet $(a_j : j \in J)$ das von den a_j *erzeugte Ideal*. Es besteht aus allen (endlichen) *Linearkombinationen*

$$\sum_{j \in J_0} r_j a_j \,,$$

wobei $J_0 \subseteq J$ eine endliche Teilmenge und $r_j \in R$ ist.

Es handelt sich dabei um das kleinste Ideal in R, das alle a_j, $j \in J$, enthält. Dass ein solches Ideal existiert ist auch deshalb klar, weil der Durchschnitt

von einer beliebigen Familie von Idealen wieder ein Ideal ist. Ein Hauptideal ist demnach ein Ideal, das von einem Element erzeugt wird.

3.2. **Einige ringtheoretische Konzepte.**

In einem Körper folgt aus $xy = 0$, dass ein Faktor 0 sein muss. Diese Eigenschaft gilt nicht für beliebige Ringe. Ein Element $f \in R$ in einem kommutativen Ring heißt *Nichtnullteiler*, wenn aus $fg = 0$ stets $g = 0$ folgt. Man nennt einen Ring *nullteilerfrei*, wenn 0 der einzige Nullteiler ist.

Definition 3.4. Ein kommutativer, nullteilerfreier, von 0 verschiedener Ring heißt *Integritätsbereich*.

Der Ring $\mathbb{Z}$ der ganzen Zahlen und die Polynomringe $K[X]$ über einem Körper K sind Integritätsbereiche. Das sind für uns die wichtigsten Beispiele.

Definition 3.5. Ein Element u in einem kommutativen Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit $uv = 1$ gibt.

Ein kommutativer Ring ist ganau dann ein Körper, wenn in ihm jedes von 0 verschiedene Element eine Einheit ist (der Nullring ist kein Körper, da in ihm sogar die 0 eine Einheit ist).

Definition 3.6. Sei R ein kommutativer Ring, und a, b Elemente in R. Man sagt, dass a das Element b *teilt* (oder dass b von a geteilt wird, oder dass b ein *Vielfaches* von a ist), wenn es ein $c \in R$ derart gibt, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Eine Einheit kann man als einen Teiler der 1 auffassen. Idealtheoretisch kann man die Eigenschaft, dass a das Element b teilt, als Zugehörigkeit $b \in Ra$ auffassen.

Definition 3.7. Sei R ein kommutativer Ring. Man sagt, dass zwei Elemente $a, b \in R$ *teilerfremd* sind, wenn jedes Element $c \in R$, das sowohl a als auch b teilt, eine Einheit ist.

Definition 3.8. Eine Nichteinheit p in einem kommutativen Ring heißt *irreduzibel* (oder *unzerlegbar*), wenn eine Faktorisierung $p = ab$ nur dann möglich ist, wenn einer der Faktoren eine Einheit ist.

Diese Begriffsbildung orientiert sich offenbar an den Primzahlen. Dagegen taucht das Wort „prim“ in der folgenden Definition auf.

Definition 3.9. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring R heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt p einen der Faktoren.

Eine Einheit ist also nach Definition nie ein Primelement. Dies ist eine Verallgemeinerung des Standpunktes, dass 1 keine Primzahl ist. Dabei ist die

1 nicht deshalb keine Primzahl, weil sie „zu schlecht“ ist, sondern weil sie „zu gut“ ist. Für die ganzen Zahlen und für viele weitere Ringe fallen die beiden Begriffe prim und irreduzibel zusammen. Im Allgemeinen ist irreduzibel einfacher nachzuweisen, und prim ist der stärkere Begriff, jedenfalls für Integritätsbereiche.

Lemma 3.10. *In einem Integritätsbereich ist ein Primelement stets irreduzibel.*

Beweis. Angenommen, wir haben eine Zerlegung $p = ab$. Wegen der Primeigenschaft teilt p einen Faktor, sagen wir $a = ps$. Dann ist $p = psb$ bzw. $p(1 - sb) = 0$. Da p kein Nullteiler ist, folgt $1 = sb$, so dass also b eine Einheit ist. □

3.3. **Irreduzible Polynome.**

Beispiel 3.11. Ein nichtkonstantes Polynom $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$, wobei K einen Körper bezeichne, ist genau dann irreduzibel, wenn es keine Produktdarstellung $P = QR$ gibt, die die Gradbedingung

$$0 < \operatorname{grad}(Q) < \operatorname{grad}(P)$$

erfüllt.

Die irreduziblen Polynome sind gerade die irreduziblen Elemente im Polynomring $K[X]$ im Sinne der obigen allgemeinen ringtheoretischen Definition. Nach der weiter unten zu beweisenden Aussage könnte man auch von Primelementen bzw. Primpolynomen sprechen. Eine weitere wichtige Charakterisierung ist die Restklassencharakterisierung, die wir in Korollar 7.7 kennenlernen werden.

Beispiel 3.12. Die Irreduzibilität eines Polynoms hängt wesentlich vom Grundkörper ab. Zum Beispiel ist das reelle Polynom $X^2 + 1 \in \mathbb{R}[X]$ irreduzibel, dagegen zerfällt es als Polynom in $\mathbb{C}[X]$ als

$$X^2 + 1 = (X + \mathrm{i})(X - \mathrm{i}).$$

Ebenso ist das Polynom $X^2 - 5 \in \mathbb{Q}[X]$ irreduzibel, aber über $\mathbb{R}$ hat es die Zerlegung

$$X^2 - 5 = \left(X - \sqrt{5}\right)\left(X + \sqrt{5}\right).$$

Übrigens kann die Zerlegung über einem größeren Körper manchmal dazu benutzt werden um zu zeigen, dass ein Polynom über dem gegebenen Körper irreduzibel ist.

Die Existenz der Faktorzerlegung in der folgenden Aussage folgt unmittelbar aus der Definition von irreduzibel, für die Eindeutigkeit muss man aber wissen, dass in einem Polynomring die irreduziblen Polynome auch Primpolynome sind (siehe unten).

Satz 3.13. *Es sei K ein Körper und sei $F \in K[X]$ ein von 0 verschiedenes Polynom. Dann gibt es eine (bis auf die Reihenfolge der Faktoren) eindeutige Produktdarstellung*

$$F = aF_1 \cdots F_r$$

mit $a \in K^\times$ und irreduziblen normierten Polynomen F_i, $i = 1, \ldots, r$.

Beweis. Siehe Aufgabe 3.18. □

3.4. **Hauptidealbereiche.**

Definition 3.14. Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealbereich*.

Satz 3.15. *Ein Polynomring über einem Körper ist ein Hauptidealbereich.*

Beweis. Sei I ein von 0 verschiedenes Ideal in $K[X]$. Betrachte die nicht-leere Menge

$$\{\operatorname{grad}(P) |\, P \in I,\, P \neq 0\}\ .$$

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \operatorname{grad}(F)$. Wir behaupten, dass $I = (F)$ ist. Die Inklusion $\supseteq$ ist klar. Zum Beweis von $\subseteq$ sei $P \in I$ gegeben. Aufgrund von Satz 19.4 (Lineare Algebra (Osnabrück 2017-2018)) gilt

$$P = FQ + R \text{ mit } \operatorname{grad}(R) < \operatorname{grad}(F) \text{ oder } R = 0\,.$$

Wegen $R \in I$ und der Minimalität von $\operatorname{grad}(F)$ kann der erste Fall nicht eintreten. Also ist $R = 0$ und P ist ein Vielfaches von F. □

In der eingangs besprochenen Situation eines Elements $x \in L$ einer Körpererweiterung $K \subseteq L$ und des zugehörigen Annullationsideals

$$I = \{P \in K[X] |\, P(x) = 0\}$$

bedeutet dieser Satz, dass es ein Polynom geben muss, das dieses Ideal erzeugt. Dieses Polynom besitzt unter sämtlichen annullierenden Polynomen $\neq 0$ minimalen Grad, und man kann es als normiert ansetzen, wodurch es eindeutig festgelegt wird. Man spricht vom *Minimalpolynom* zu x.

Mit einem ähnlichen Argument wie im Beweis der letzten Aussage verwendet kann man zeigen, dass $\mathbb{Z}$ ebenfalls ein Hauptidealbereich ist. Die folgenden Aussagen gelten also auch für $\mathbb{Z}$.

Die beiden folgenden Aussagen nennt man *Lemma von Bezout* bzw. *Lemma von Euklid*.

Lemma 3.16. *Sei R ein Hauptidealbereich und seien $a, b \in R$ zwei teilerfremde Elemente. Dann kann man die 1 als Linearkombination von a und b darstellen, d.h. es gibt Elemente $r, s \in R$ mit $ra + sb = 1$.*

Beweis. Wir betrachten das von a und b erzeugte Ideal $I = (a, b)$. Da R ein Hauptidealbereich ist, gibt es ein $c \in R$ mit $(a, b) = (c)$. Daher ist c ein Teiler von a und von b. Die Teilerfremdheit impliziert, dass c eine Einheit ist. Wegen $c \in (a, b)$ gibt es eine Darstellung $c = ua + vb$. Multiplikation mit c^{-1} ergibt die Darstellung der 1. □

Lemma 3.17. *Sei R ein Hauptidealbereich und $a, b, c \in R$. Es seien a und b teilerfremd und a teile das Produkt bc. Dann teilt a den Faktor c.*

Beweis. Da a und b teilerfremd sind, gibt es nach dem Lemma von Bezout Elemente $r, s \in R$ mit $ra + sb = 1$. Die Voraussetzung, dass a das Produkt bc teilt, schreiben wir als $bc = da$. Damit gilt

$$c = c1 = c(ra + sb) = cra + csb = acr + ads = a(cr + ds),$$

was zeigt, dass c ein Vielfaches von a ist. □

Korollar 3.18. *Sei R ein Hauptidealbereich. Dann ist ein Element genau dann prim, wenn es irreduzibel ist.*

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 3.10 stets irreduzibel. Sei also umgekehrt p irreduzibel, und nehmen wir an, dass p das Produkt ab teilt, sagen wir $pc = ab$. Nehmen wir an, dass a kein Vielfaches von p ist. Dann sind aber a und p teilerfremd, da eine echte Inklusionskette $(p) \subset (p, a) = (d) \subset R$ der Irreduzibilität von p widerspricht. Damit teilt p nach dem Lemma von Euklid den anderen Faktor b. □

3. Arbeitsblatt

3.1. **Aufwärmaufgaben.**

Aufgabe 3.1. Sei $K \subseteq L$ eine Körpererweiterung und es sei $a \in L$. Zeige, dass die Einsetzungsabbildung, also die Zuordnung

$$\psi\colon K[X] \longrightarrow L,\ P \longmapsto P(a),$$

folgende Eigenschaften erfüllt (dabei seien $P, Q \in K[X]$).

(1) $(P + Q)(a) = P(a) + Q(a)$,
(2) $(P \cdot Q)(a) = P(a) \cdot Q(a)$,
(3) $1(a) = 1$.

Aufgabe 3.2. Es sei K ein Körper, $\varphi\colon V \to V$ ein Endomorphismus auf einem endlichdimensionalen K-Vektorraum und

$$K[X] \longrightarrow \mathrm{End}\,(V)\,,\ P \longmapsto P(\varphi),$$

der zugehörige Einsetzungshomomorphismus. Vergleiche diese Situation mit dem durch ein Element $a \in L$ zu einer Körpererweiterung $K \subseteq L$ gegebenen Einsetzungshomomorphismus $P \mapsto P(a)$.

Aufgabe 3.3. Zeige, dass ein Unterring eines Körpers ein Integritätsbereich ist.

Aufgabe 3.4. Es sei R ein kommutativer Ring und seien f, g Nichtnullteiler in R. Zeige, dass das Produkt fg ebenfalls ein Nichtnullteiler ist.

Aufgabe 3.5.*

Es sei R ein kommutativer Ring. Zu jedem $f \in R$ sei

$$\mu_f \colon R \longrightarrow R,\, g \longmapsto fg,$$

die Multiplikation mit f. Zeige, dass μ_f genau dann bijektiv ist, wenn es surjektiv ist.

Man zeige durch ein Beispiel, dass in dieser Situation aus der Injektivität nicht die Bijektivität folgt.

Aufgabe 3.6.*

Es sei R ein kommutativer Ring und $f \in R$. Charakterisiere mit Hilfe der Multiplikationsabbildung

$$\mu_f \colon R \longrightarrow R,\, g \longmapsto fg,$$

wann f ein Nichtnullteiler und wann f eine Einheit ist.

Aufgabe 3.7. Bestimme die Einheiten von $\mathbb{Z}$ und von $K[X]$, wobei K ein Körper sei.

Aufgabe 3.8. Zeige, dass $\mathbb{Z} \subseteq \mathbb{Q}$ eine Untergruppe, aber kein Ideal ist.

Aufgabe 3.9.*

Zeige, dass ein kommutativer Ring genau dann ein Körper ist, wenn er genau zwei Ideale enthält.

Aufgabe 3.10. Sei R ein kommutativer Ring und sei f_j, $j \in J$, eine Familie von Elementen in R. Es sei angenommen, dass die f_j zusammen das Einheitsideal erzeugen. Zeige, dass es eine endliche Teilfamilie f_j, $j \in J_0 \subseteq J$ gibt, die ebenfalls das Einheitsideal erzeugt.

Aufgabe 3.11. Sei R ein kommutativer Ring und sei

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$

eine aufsteigende Kette von Idealen. Zeige, dass die Vereinigung $\bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ ebenfalls ein Ideal ist. Zeige durch ein einfaches Beispiel, dass die Vereinigung von Idealen im Allgemeinen kein Ideal sein muss.

Aufgabe 3.12. Sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Zeige, dass p genau dann irreduzibel ist, wenn es genau zwei Hauptideale oberhalb von (p) gibt, nämlich (p) selbst und $(1) = R$.

Aufgabe 3.13. Beweise die Formel

$$X^u + 1 \,=\, (X+1)\left(X^{u-1} - X^{u-2} + X^{u-3} - \cdots + X^2 - X + 1\right)$$

für u ungerade.

Aufgabe 3.14. Zeige, dass ein reelles Polynom von ungeradem Grad nicht irreduzibel ist.

Aufgabe 3.15. Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad 3. Zeige, dass F entweder eine oder drei reelle Nullstellen besitzt.

Aufgabe 3.16.*

Zeige, dass das Polynom

$$X^3 - 3X + 1$$

über $\mathbb{Q}$ irreduzibel ist.

Aufgabe 3.17.*

Zeige, dass das Polynom

$$X^3 - 3X - 1$$

über $\mathbb{Q}$ irreduzibel ist.

Aufgabe 3.18. Es sei K ein Körper und sei $F \in K[X]$ ein von 0 verschiedenes Polynom. Zeige, dass es eine (bis auf die Reihenfolge der Faktoren) eindeutige Produktdarstellung

$$F = aF_1 \cdots F_r$$

mit $a \in K^\times$ und irreduziblen normierten Polynomen F_i, $i = 1, \dots, r$, gibt.

Aufgabe 3.19. Zeige, dass $\mathbb{Z}[X]$ und der Polynomring in zwei Variablen $K[X,Y]$ über einem Körper K keine Hauptidealbereiche sind.

Aufgabe 3.20.*

Es sei R ein kommutativer Ring und sei $p \in R$ ein Primelement. Zeige, dass p auch im Polynomring $R[X]$ prim ist.

3.2. **Aufgaben zum Abgeben.**

Aufgabe 3.21. (2 Punkte)

Sei K ein algebraisch abgeschlossener Körper. Bestimme in $K[X]$ die irreduziblen Polynome.

Aufgabe 3.22. (5 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass es unendlich viele normierte irreduzible Polynome in $K[X]$ gibt.

Aufgabe 3.23. (4 Punkte)

Es sei $P \in \mathbb{R}[X]$ ein nichtkonstantes Polynom mit reellen Koeffizienten. Zeige, dass man P als ein Produkt von reellen Polynomen vom Grad 1 oder 2 schreiben kann.

In der folgenden Aufgabe wird der *Quotientenkörper* zu einem Integritätsbereich definiert.

Aufgabe 3.24. (6 Punkte)

Es sei R ein Integritätsbereich. Zeige, dass man auf folgende Weise einen Körper K konstruieren kann, der R enthält.

Wir betrachten auf

$$M = R \times (R \setminus \{0\})$$

die durch

$$(a,b) \sim (c,d), \text{ falls } ad = bc\,,$$

definierte Relation.

a) Zeige, dass dies eine Äquivalenzrelation ist.

b) Definiere auf der Quotientenmenge $Q(R)$ Verknüpfungen derart, dass $Q(R)$ zu einem Körper wird und dass

$$\varphi\colon\ R \longrightarrow Q(R),\ r \longmapsto [(r,1)],$$

mit Addition und Multiplikation verträglich ist und $\varphi(1) = 1$ gilt.

4. Vorlesung - Gruppenhomomorphismen

In dieser und der nächsten Vorlesung werden wir uns mit Gruppentheorie, insbesondere mit Restklassenbildung, beschäftigen. Zum einen ist die Restklassenbildung für uns wichtig, um zu einem Ideal $I \subseteq K[X]$ den Restklassenring $K[X]/I$ zu konstruieren. Diese Konstuktion ist entscheidend, um die dritte zu Beginn der letzten Vorlesung gestellte Frage beantworten zu können. Zum andern treten Gruppen als Galoisgruppen von Körpererweiterungen auf, und die Korrespondenz zwischen Untergruppen der Galoisgruppe und Zwischenkörpern ist der Hauptgegenstand der Galoistheorie. Um unser hauptsächliches Interesse, die Körper- und Galoistheorie, nicht zu lange aus dem Blick zu verlieren, werden wir uns hier bei den ohnehin einfachen Beweisen kurz halten. Ähnliche Argumente sind aus der linearen Algebra bekannt.

4.1. **Gruppenhomomorphismen.**

Definition 4.1. Seien $(G, \circ, e_G)$ und $(H, \circ, e_H)$ Gruppen. Eine Abbildung

$$\psi\colon\ G \longrightarrow H$$

heißt *Gruppenhomomorphismus*, wenn die Gleichheit

$$\psi(g \circ g') \ = \ \psi(g) \circ \psi(g')$$

für alle $g, g' \in G$ gilt.

Die Menge der Gruppenhomomorphismen von G nach H wird mit

$$\operatorname{Hom}(G, H)$$

bezeichnet. Aus der linearen Algebra sind vermutlich die linearen Abbildungen zwischen Vektorräumen bekannt, welche insbesondere Gruppenhomomorphismen sind, darüber hinaus aber auch noch mit der skalaren Multiplikation verträglich sind. Die folgenden beiden Lemmata folgen direkt aus der Definition.

Lemma 4.2. *Es seien G und H Gruppen und $\varphi\colon\ G \to H$ sei ein Gruppenhomomorphismus. Dann ist $\varphi(e_G) = e_H$ und $(\varphi(g))^{-1} = \varphi(g^{-1})$ für jedes $g \in G$.*

Beweis. Siehe Aufgabe 4.1. □

Lemma 4.3. *Es seien F, G, H Gruppen. Dann gelten folgende Eigenschaften.*

(1) *Die Identität*
$$\mathrm{Id}\colon\ G \longrightarrow G$$
ist ein Gruppenhomomorphismus.

(2) *Sind $\varphi : F \to G$ und $\psi : G \to H$ Gruppenhomomorphismen, so ist auch die Hintereinanderschaltung $\psi \circ \varphi\colon\ F \to H$ ein Gruppenhomomorphismus.*

(3) *Ist $F \subseteq G$ eine Untergruppe, so ist die Inklusion $F \hookrightarrow G$ ein Gruppenhomomorphismus.*
(4) *Sei $\{e\}$ die triviale Gruppe. Dann ist die Abbildung $\{e\} \to G$, die e auf e_G schickt, ein Gruppenhomomorphismus. Ebenso ist die (konstante) Abbildung $G \to \{e\}$ ein Gruppenhomomorphismus.*

Beweis. Das ist trivial. □

Lemma 4.4. *Sei G eine Gruppe. Dann entsprechen sich eindeutig Gruppenelemente $g \in G$ und Gruppenhomomorphismen φ von $\mathbb{Z}$ nach G über die Korrespondenz*

$$g \longmapsto (n \mapsto g^n) \text{ und } \varphi \longmapsto \varphi(1)\,.$$

Beweis. Siehe Aufgabe 4.2. □

Man kann den Inhalt dieses Lemmas auch kurz durch $\mathrm{Hom}\,(\mathbb{Z}, G) \cong G$ ausdrücken. Die Gruppenhomomorphismen von einer Gruppe G nach $\mathbb{Z}$ sind schwieriger zu charakterisieren. Die Gruppenhomomorphismen von $\mathbb{Z}$ nach $\mathbb{Z}$ sind die Multiplikationen mit einer festen ganzen Zahl a, also

$$\mathbb{Z} \longrightarrow \mathbb{Z},\, x \longmapsto ax.$$

4.2. **Gruppenisomorphismen.**

Definition 4.5. Seien G und H Gruppen. Einen bijektiven Gruppenhomomorphismus

$$\varphi\colon\, G \longrightarrow H$$

nennt man einen *Isomorphismus* (oder eine *Isomorphie*). Die beiden Gruppen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt.

Lemma 4.6. *Seien G und H Gruppen und sei*

$$\varphi\colon\, G \longrightarrow H$$

ein Gruppenisomorphismus. Dann ist auch die Umkehrabbildung

$$\varphi^{-1}\colon\, H \longrightarrow G,\, h \longmapsto \varphi^{-1}(h),$$

ein Gruppenisomorphismus.

Beweis. Siehe Aufgabe 4.3. □

Isomorphe Gruppen sind bezüglich ihrer gruppentheoretischen Eigenschaften als gleich anzusehen. Isomorphismen einer Gruppe auf sich selbst nennt man auch *Automorphismen*. Wichtige Beispiele für Automorphismen sind die sogenannten inneren Automorphismen, siehe die nächste Vorlesung.

4.3. **Der Kern eines Gruppenhomomorphismus.**

Definition 4.7. Seien G und H Gruppen und sei

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann nennt man das Urbild des neutralen Elementes den *Kern* von φ, geschrieben

$$\operatorname{kern}\varphi\ =\ \varphi^{-1}(e_H)\ =\ \{g \in G |\, \varphi(g) = e_H\}\,.$$

Lemma 4.8. *Seien G und H Gruppen und sei*

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann ist der Kern von φ eine Untergruppe von G.

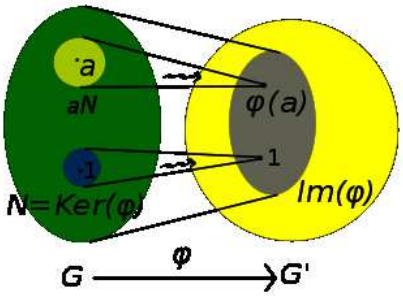
Beweis. Wegen $\varphi(e_G) = e_H$ ist $e_G \in \ker\varphi$. Seien $g, g' \in \ker\varphi$. Dann ist

$$\varphi(gg') = \varphi(g)\varphi(g') = e_H e_H = e_H$$

und daher ist auch $gg' \in \ker\varphi$. Der Kern ist also ein Untermonoid. Sei nun $g \in \ker\varphi$ und betrachte das inverse Element g^{-1}. Nach Lemma 4.2 ist

$$\varphi\left(g^{-1}\right) = (\varphi(g))^{-1} = e_H^{-1} = e_H,$$

also auch $g^{-1} \in \ker\varphi$. □



Lemma 4.9. *Seien G und H Gruppen. Ein Gruppenhomomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn der Kern von φ trivial ist.*

Beweis. Wenn φ injektiv ist, so darf auf jedes Element $h \in H$ höchstens ein Element aus G gehen. Da e_G auf e_H geschickt wird, darf kein weiteres Element auf e_H gehen, d.h. $\ker\varphi = \{e_G\}$. Sei umgekehrt dies der Fall und sei angenommen, dass $g, \tilde{g} \in G$ beide auf $h \in H$ geschickt werden. Dann ist

$$\varphi\left(g\tilde{g}^{-1}\right) = \varphi(g)\varphi(\tilde{g})^{-1} = hh^{-1} = e_H$$

und damit ist $g\tilde{g}^{-1} \in \ker\varphi$, also $g\tilde{g}^{-1} = e_G$ nach Voraussetzung und damit $g = \tilde{g}$. □

4.4. **Nebenklassen.**

Definition 4.10. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wir setzen $x \sim_H y$ (und sagen, dass x und y äquivalent sind) wenn $x^{-1}y \in H$.

Dies ist in der Tat eine Äquivalenzrelation: Aus $x^{-1}x = e_G \in H$ folgt, dass diese Relation reflexiv ist. Aus $x^{-1}y \in H$ folgt sofort $y^{-1}x = (x^{-1}y)^{-1} \in H$ und aus $x^{-1}y \in H$ und $y^{-1}z \in H$ folgt $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$.

Definition 4.11. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann heißt zu jedem $x \in G$ die Teilmenge

$$xH = \{xh |\, h \in H\}$$

die *Linksnebenklasse von* x in G bezüglich H. Jede Teilmenge von dieser Form heißt *Linksnebenklasse*. Entsprechend heißt eine Menge der Form

$$Hy = \{hy |\, h \in H\}$$

Rechtsnebenklasse (zu y).

Die Äquivalenzklassen zu der oben definierten Äquivalenzrelation sind wegen

$$\begin{aligned}
[x] &= \{y \in G |\, x \sim y\} \\
&= \left\{y \in G |\, x^{-1}y \in H\right\} \\
&= \left\{y \in G |\, \text{es gibt } h \in H \text{ mit } x^{-1}y = h\right\} \\
&= \{y \in G |\, \text{es gibt } h \in H \text{ mit } y = xh\} \\
&= xH
\end{aligned}$$

genau die Linksnebenklassen. Die Linksnebenklassen bilden somit eine disjunkte Zerlegung (eine *Partition*) von G. Dies gilt ebenso für die Rechtsnebenklassen. Im kommutativen Fall muss man nicht zwischen Links- und Rechtsnebenklassen unterscheiden.

Lemma 4.12. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Es seien $x, y \in G$ zwei Elemente. Dann sind folgende Aussagen äquivalent.*

(1) $x \in yH$.
(2) $y \in xH$.
(3) $y^{-1}x \in H$.
(4) $x^{-1}y \in H$.
(5) $xH \cap yH \neq \emptyset$.
(6) $x \sim_H y$.
(7) $xH = yH$.

Beweis. Die Äquivalenz von (1) und (3) (und die von (2) und (4)) folgt aus Multiplikation mit y^{-1} bzw. mit y. Die Äquivalenz von (3) und (4) folgt durch Übergang zum Inversen. Aus (1) folgt (5) wegen $1 \in H$. Wenn (5) erfüllt ist, so bedeutet das $xh_1 = yh_2$ mit gewissen $h_1, h_2 \in H$. Damit ist $x = yh_2h_1^{-1}$ und (1) ist erfüllt. (4) und (6) sind nach Definition 4.10 äquivalent. Da die

Linksnebenklassen die Äquivalenzklassen sind, ergibt sich die Äquivalenz von (5) und (7). □

4.5. **Gruppenordnung und Elementordnung.**

Definition 4.13. Zu einer endlichen Gruppe G bezeichnet man die Anzahl ihrer Elemente als *Gruppenordnung* oder als die *Ordnung der Gruppe*, geschrieben

$$\operatorname{ord}(G) = \#(G).$$

Definition 4.14. Sei G eine Gruppe und $g \in G$ ein Element. Dann nennt man die kleinste positive Zahl n mit $g^n = e_G$ die *Ordnung* von g. Man schreibt hierfür $\operatorname{ord}(g)$. Wenn alle positiven Potenzen von g vom neutralen Element verschieden sind, so setzt man $\operatorname{ord}(g) = \infty$.

Lemma 4.15. *Sei G eine endliche Gruppe. Dann besitzt jedes Element $g \in G$ eine endliche Ordnung. Die Potenzen*

$$g^0 = e_G,\ g^1 = g,\ g^2, \ldots, g^{\operatorname{ord}(g)-1}$$

sind alle verschieden.

Beweis. Siehe Aufgabe 4.8. □

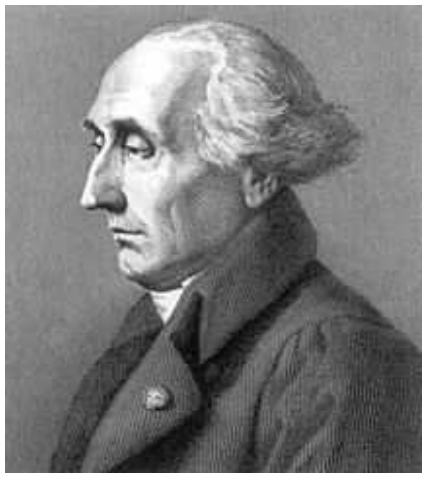
4.6. **Der Satz von Lagrange.**

Satz 4.16. *Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe von G. Dann ist ihre Kardinalität $\#(H)$ ein Teiler von $\#(G)$.*

Beweis. Betrachte die Linksnebenklassen $gH := \{gh |\, h \in H\}$ für sämtliche $g \in G$. Es ist

$$H \longrightarrow gH,\ h \longmapsto gh,$$

eine Bijektion zwischen H und gH, so dass alle Nebenklassen gleich groß sind (und zwar $\#(H)$ Elemente haben). Die Nebenklassen bilden (als Äquivalenzklassen) zusammen eine Zerlegung von G, so dass $\#(G)$ ein Vielfaches von $\#(H)$ sein muss. □



Joseph-Louis Lagrange (1736 Turin - 1813 Paris)

Korollar 4.17. *Sei G eine endliche Gruppe und sei $g \in G$ ein Element. Dann teilt die Ordnung von g die Gruppenordnung.*

Beweis. Sei H die von g erzeugte Untergruppe. Nach Lemma 4.15 ist

$$\operatorname{ord}(g) = \operatorname{ord}(H).$$

Daher teilt diese Zahl nach Satz 4.16 die Gruppenordnung von G. □

Definition 4.18. Zu einer Untergruppe $H \subseteq G$ heißt die Anzahl der (Links- oder Rechts-)Nebenklassen der *Index* von H in G, geschrieben

$$\operatorname{ind}_G H\,.$$

In der vorstehenden Definition ist Anzahl im Allgemeinen als die *Mächtigkeit* einer Menge zu verstehen. Der Index wird aber hauptsächlich dann verwendet, wenn er endlich ist, wenn es also nur endlich viele Nebenklassen gibt. Das ist bei endlichem G automatisch der Fall, kann aber auch bei unendlichem G der Fall sein, wie schon die Beispiele $\mathbb{Z}n \subseteq \mathbb{Z}$, $n \geq 1$, zeigen. Wenn G eine endliche Gruppe ist und $H \subseteq G$ eine Untergruppe, so gilt aufgrund des Satzes von Lagrange die einfache *Indexformel*

$$\#(G) = \#(H) \cdot \operatorname{ind}_G H.$$

4. Arbeitsblatt

4.1. **Aufwärmaufgaben.**

Aufgabe 4.1. Es seien G und H Gruppen und $\varphi\colon G \to H$ sei ein Gruppenhomomorphismus. Zeige, dass $\varphi(e_G) = e_H$ und $(\varphi(g))^{-1} = \varphi(g^{-1})$ für jedes $g \in G$ ist.

Aufgabe 4.2.*

Sei G eine Gruppe. Zeige, dass sich Gruppenelemente $g \in G$ und Gruppenhomomorphismen φ von $\mathbb{Z}$ nach G über die Korrespondenz

$$g \longmapsto (n \mapsto g^n) \text{ und } \varphi \longmapsto \varphi(1)$$

entsprechen.

Aufgabe 4.3. Seien G und H Gruppen und sei

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenisomorphismus. Zeige, dass auch die Umkehrabbildung

$$\varphi^{-1}\colon\ H \longrightarrow G,\ h \longmapsto \varphi^{-1}(h),$$

ein Gruppenisomorphismus ist.

Aufgabe 4.4. Seien G und H Gruppen und sei $\varphi\colon\ G \to H$ ein Gruppenhomomorphismus. Zeige, dass das Bild von φ eine Untergruppe von H ist.

Aufgabe 4.5. Sei G eine (multiplikativ geschriebene) kommutative Gruppe und sei $n \in \mathbb{N}$. Zeige, dass das Potenzieren

$$G \longrightarrow G,\ x \longmapsto x^n,$$

ein Gruppenhomomorphismus ist.

Aufgabe 4.6. Betrachte die Gruppe der komplexen Zahlen ohne null, $\mathbb{C}^\times = (\mathbb{C} \setminus \{0\}, \cdot, 1)$. Bestimme für jedes $n \in \mathbb{N}$ den Kern des Potenzierens

$$\mathbb{C}^\times \longrightarrow \mathbb{C}^\times,\ z \longmapsto z^n.$$

Sind diese Gruppenhomomorphismen surjektiv?

Aufgabe 4.7. Es sei $\varphi\colon\ G \to H$ ein surjektiver Gruppenhomomorphismus. Zeige, dass durch $U \mapsto \varphi(U)$ und $V \mapsto \varphi^{-1}(V)$ eine Bijektion zwischen den Untergruppen von H und denjenigen Untergruppen von G, die $\operatorname{kern}\varphi$ umfassen, gegeben ist.

Aufgabe 4.8. Sei G eine endliche Gruppe. Zeige, dass jedes Element $g \in G$ eine endliche Ordnung besitzt, und dass die Potenzen

$$g^0 = e_G,\ g^1 = g,\ g^2, \ldots, g^{\operatorname{ord}(g)-1}$$

alle verschieden sind.

Wichtige Beispiele für im Allgemeinen nicht kommutative Gruppen werden durch die allgemeine lineare Gruppe $\mathrm{GL}_K(V)$ gegeben, also die Menge der invertierbaren linearen Abbildungen auf einem K-Vektorraum V mit der Hintereinanderschaltung als Verknüpfung.

Aufgabe 4.9. Es sei K ein Körper und $n \in \mathbb{N}_+$. Zeige, dass die Determinante

$$\mathrm{GL}_n(K) \longrightarrow (K \setminus \{0\}, \cdot, 1),\ M \longmapsto \det M,$$

ein surjektiver Gruppenhomomorphismus ist.

Aufgabe 4.10. Man gebe für jedes $n \in \mathbb{N}$ eine invertierbare Matrix $M \in \mathrm{GL}_2(\mathbb{R})$ an, derart, dass die Ordnung von M gleich n ist.

Aufgabe 4.11.*

Man gebe eine Matrix $M \in \mathrm{GL}_2(\mathbb{Q})$ der Ordnung 4 an.

Aufgabe 4.12. Es sei $\varphi\colon V \to V$ eine lineare Abbildung auf einem endlichdimensionalen K-Vektorraum V. Zeige, dass φ genau dann endliche Ordnung besitzt, wenn das Minimalpolynom von φ ein Teiler von $X^n - 1$ für ein $n \in \mathbb{N}_+$ ist.

Aufgabe 4.13. Es sei K ein Körper mit positiver Charakteristik $p > 0$. Zeige, dass die Matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

die endliche Ordnung p besitzt.

Aufgabe 4.14. Es sei K ein endlicher Körper und M eine invertierbare $n \times n$-Matrix über K. Zeige, dass M endliche Ordnung besitzt.

Aufgabe 4.15. Bestimme die Nebenklassen zu den folgenden Untergruppen von kommutativen Gruppen.

(1) $(\mathbb{Z}, 0, +) \subseteq (\mathbb{R}, 0, +)$.
(2) $(\mathbb{Q}, 0, +) \subseteq (\mathbb{R}, 0, +)$.
(3) $(\mathbb{R}, 0, +) \subseteq (\mathbb{C}, 0, +)$.
(4) $(\mathbb{Z}n, 0, +) \subseteq (\mathbb{Z}, 0, +)$ $(n \in \mathbb{N})$.
(5) $(\{z \in \mathbb{C} |\ |z| = 1\}, 1, \cdot) \subseteq (\mathbb{C} \setminus \{0\}, 1, \cdot)$.
(6) $(\{z \in \mathbb{C} |\ z^n = 1\}, 1, \cdot) \subseteq (\{z \in \mathbb{C} |\ |z| = 1\}, 1, \cdot)$ $(n \in \mathbb{N})$.

Wann bestehen die Nebenklassen aus endlich vielen Elementen, wann ist der Index endlich?

Aufgabe 4.16.*

Stifte einen surjektiven Gruppenhomomorphismus von der Gruppe der komplexen Zahlen ohne null $(\mathbb{C} \setminus \{0\}, \cdot, 1)$ in die multiplikative Gruppe der positiven reellen Zahlen $(\mathbb{R}_+, \cdot, 1)$.

Was ist der Kern dieser Abbildung?

Aufgabe 4.17.*

Stifte einen Gruppenisomorphismus zwischen der additiven Gruppe der reellen Zahlen $(\mathbb{R}, 0, +)$ und der multiplikativen Gruppe der positiven reellen Zahlen $(\mathbb{R}_+, 1, \cdot)$.

Aufgabe 4.18. Zeige, dass die beiden kommutativen Gruppen $(\mathbb{Q}, 0, +)$ und $(\mathbb{Q}_+, 1, \cdot)$ nicht isomorph sind.

Aufgabe 4.19. Zeige, dass die Abbildung

$$S_n \longrightarrow \mathrm{GL}_n(\mathbb{R})\,,\ \pi \longmapsto M_\pi,$$

die einer Permutation π auf $\{1, \ldots, n\}$ ihre Permutationsmatrix M_π zuordnet, ein injektiver Gruppenhomomorphismus ist.

Aufgabe 4.20. Sei $M = \{1, \ldots, n\}$ und sei π eine Permutation auf M. Die zugehörige *Permutationsmatrix* M_π ist dadurch gegeben, dass

$$a_{\pi(i),i} = 1$$

ist und alle anderen Einträge 0 sind. Zeige, dass

$$\det M_\pi = \mathrm{sgn}(\pi)$$

ist.

4.2. **Aufgaben zum Abgeben.**

Aufgabe 4.21. (2 Punkte)

Betrachte die Matrix

$$\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}.$$

Zeige, dass diese Matrix einen Gruppenhomomorphismus von $\mathbb{Q}^2$ nach $\mathbb{Q}^2$ und ebenso von $\mathbb{Z}^2$ nach $\mathbb{Z}^2$ definiert. Untersuche diese beiden Gruppenhomomorphismen in Hinblick auf Injektivität und Surjektivität.

Aufgabe 4.22. (3 Punkte)

Bestimme die Gruppenhomomorphismen von $(\mathbb{Q}, +, 0)$ nach $(\mathbb{Z}, +, 0)$.

Aufgabe 4.23. (3 Punkte)

Sei $n \in \mathbb{N}_+$. Zeige, dass die Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$ und die Gruppe $\mathbb{Z}/(n)$ isomorph sind.

Aufgabe 4.24. (4 Punkte)

Man gebe für jedes $n \in \mathbb{N}$ eine invertierbare Matrix $M \in \mathrm{GL}_k(\mathbb{Q})$ an (dabei sei k geeignet gewählt), derart, dass die Ordnung von M gleich n ist.

Aufgabe 4.25. (3 Punkte)

Sei G eine Gruppe, in der jedes Element die Ordnung zwei hat, d.h. für jedes Gruppenelement g gilt $g^2 = e$. Zeige, dass die Gruppe G dann abelsch ist.

Aufgabe 4.26. (5 Punkte)

Man gebe eine Matrix $M \in \mathrm{GL}_2(\mathbb{Q})$ der Ordnung 3 an.

5. Vorlesung - Restklassengruppen

In dieser Vorlesung diskutieren wir Normalteiler, das sind Untergruppen, für die Links- und Rechtsnebenklassen übereinstimmen. Für Normalteiler kann man Restklassengruppen konstruieren.

5.1. **Innere Automorphismen.**

Definition 5.1. Sei G eine Gruppe und $g \in G$ fixiert. Die durch g definierte Abbildung

$$\kappa_g \colon G \longrightarrow G,\, x \longmapsto gxg^{-1},$$

heißt *innerer Automorphismus*.

Eine solche Abbildung nennt man auch *Konjugation* (mit g). Wenn G eine kommutative Gruppe ist, so ist wegen $gxg^{-1} = xgg^{-1} = x$ die Identität der einzige innere Automorphismus. Der Begriff ist also nur bei nicht kommutativen Gruppen von Interesse. Ein wichtiges Beispiel für eine Konjugation tritt auf, wenn lineare Abbildungen durch Matrizen bezüglich verschiedener Basen beschrieben werden sollen, siehe Lemma 11.11 (Lineare Algebra (Osnabrück 2017-2018)). Man spricht auch von ähnlichen Matrizen (wobei der Ähnlichkeitsbegriff auch für nicht invertierbare Matrizen definiert ist).

Lemma 5.2. *Ein innerer Automorphismus ist in der Tat ein Automorphismus. Die Zuordnung*

$$G \longrightarrow \operatorname{Aut} G,\, g \longmapsto \kappa_g,$$

ist ein Gruppenhomomorphismus.

Beweis. Es ist

$$\kappa_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \kappa_g(x)\kappa_g(y),$$

so dass ein Gruppenhomomorphismus vorliegt. Wegen

$$\kappa_g(\kappa_h(x)) = \kappa_g(hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = \kappa_{gh}$$

ist einerseits

$$\kappa_{g^{-1}} \circ \kappa_g = \kappa_{g^{-1}g} = \mathrm{id}_G,$$

so dass κ_g bijektiv, also ein Automorphismus, ist. Andererseits ist deshalb die Gesamtabbildung κ ein Gruppenhomomorphismus. □

5.2. **Normalteiler.**

Definition 5.3. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Man nennt H einen *Normalteiler*, wenn

$$xH = Hx$$

für alle $x \in G$ ist, wenn also die Linksnebenklasse zu x mit der Rechtsnebenklasse zu x übereinstimmt.

Bei einem Normalteiler braucht man nicht zwischen Links- und Rechtsnebenklassen zu unterscheiden und spricht einfach von *Nebenklassen*. Statt xH oder Hx schreiben wir meistens $[x]$. Die Gleichheit $xH = Hx$ bedeutet *nicht*, dass $xh = hx$ für alle $h \in H$ ist, sondern lediglich, dass es zu jedem $h \in H$ ein $\tilde{h} \in H$ mit $xh = \tilde{h}x$. gibt.

Lemma 5.4. *Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann sind folgende Aussagen äquivalent.*

(1) *H ist ein Normalteiler*
(2) *Es ist $xhx^{-1} \in H$ für alle $x \in G$ und $h \in H$.*
(3) *H ist invariant unter jedem inneren Automorphismus von G.*

Beweis. (1) bedeutet bei gegebenem $h \in H$, dass man $xh = \tilde{h}x$ mit einem $\tilde{h} \in H$ schreiben kann. Durch Multiplikation mit x^{-1} von rechts ergibt sich $xhx^{-1} = \tilde{h} \in H$, also (2). Dieses Argument rückwärts ergibt die Implikation (2) $\Rightarrow$ (1). Ferner ist (2) eine explizite Umformulierung von (3). □

Beispiel 5.5. Wir betrachten die Permutationsgruppe $G = S_3$ zu einer dreielementigen Menge, d.h. S_3 besteht aus den bijektiven Abbildungen der Menge $\{1, 2, 3\}$ in sich. Die triviale Gruppe $\{\mathrm{id}\}$ und die ganze Gruppe sind Normalteiler. Die Teilmenge $H = \{\mathrm{id}, \varphi\}$, wobei φ die Elemente 1 und 2 vertauscht und 3 unverändert lässt, ist eine Untergruppe. Sie ist aber kein Normalteiler. Um dies zu zeigen, sei ψ die Bijektion, die 1 fest lässt und 2 und 3 vertauscht. Dieses ψ ist zu sich selbst invers. Die Konjugation $\psi\varphi\psi^{-1} = \psi\varphi\psi$ ist dann die Abbildung, die 1 auf 3, 2 auf 2 und 3 auf 1 schickt, und diese Bijektion gehört nicht zu H.

Lemma 5.6. *Seien G und H Gruppen und sei*

$$\varphi\colon G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann ist der Kern $\ker\varphi$ *ein Normalteiler in G.*

Beweis. Wir verwenden Lemma 5.4. Sei also $x \in G$ beliebig und $h \in \ker\varphi$. Dann ist

$$\varphi\left(xhx^{-1}\right) = \varphi(x)\varphi(h)\varphi\left(x^{-1}\right) = \varphi(x)e_H\varphi\left(x^{-1}\right) = \varphi(x)\varphi(x)^{-1} = e_H,$$

also gehört xhx^{-1} ebenfalls zum Kern. □

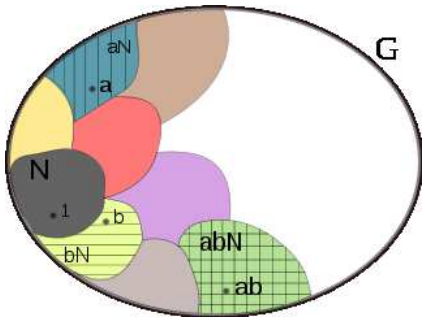
5.3. **Restklassenbildung.**

Wir zeigen nun umgekehrt, dass jeder Normalteiler sich als Kern eines geeigneten, surjektiven Gruppenhomomorphismus realisieren lässt.

Satz 5.7. *Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Es sei G/H die Menge der Nebenklassen (die Quotientenmenge) und*

$$q\colon G \longrightarrow G/H,\ g \longmapsto [g],$$

die kanonische Projektion. Dann gibt es eine eindeutig bestimmte Gruppenstruktur auf G/H derart, dass q ein Gruppenhomomorphismus ist.



Die Multiplikation der Nebenklassen zu einem Normalteiler $N \subseteq G$.

Beweis. Da die kanonische Projektion zu einem Gruppenhomomorphismus werden soll, muss die Verknüpfung durch

$$[x][y] = [xy]$$

gegeben sein. Wir müssen also zeigen, dass durch diese Vorschrift eine wohldefinierte Verknüpfung auf G/H definiert ist, die unabhängig von der Wahl der Repräsentanten ist. D.h. wir haben für $[x] = [x']$ und $[y] = [y']$ zu zeigen, dass $[xy] = [x'y']$ ist. Nach Voraussetzung können wir $x' = xh$ und $hy' = \tilde{h}y = yh'$ mit $h, \tilde{h}, h' \in H$ schreiben. Damit ist

$$x'y' = (xh)y' = x(hy') = x(yh') = xyh'.$$

Somit ist $[xy] = [x'y']$. Aus der Wohldefiniertheit der Verknüpfung auf G/H folgen die Gruppeneigenschaften, die Homomorphieeigenschaft der Projektion und die Eindeutigkeit. □

Definition 5.8. Sei G eine Gruppe und $H \subseteq G$ ein Normalteiler. Die Quotientenmenge

$$G/H$$

mit der aufgrund von Satz 5.7 eindeutig bestimmten Gruppenstruktur heißt *Restklassengruppe von G modulo H*. Die Elemente $[g] \in G/H$ heißen *Restklassen*. Für eine Restklasse $[g]$ heißt jedes Element $g' \in G$ mit $[g'] = [g]$ ein *Repräsentant* von $[g]$.

Beispiel 5.9. Die Untergruppen der ganzen Zahlen sind nach Satz 44.3 (Lineare Algebra (Osnabrück 2017-2018)) von der Form (diese Aussage ist analog zu der in Vorlesung 3 bewiesenen Aussage, dass $K[X]$ ein Hauptidealbereich ist) $\mathbb{Z}n$ mit $n \geq 0$. Die Restklassengruppen werden mit

$$\mathbb{Z}/(n)$$

bezeichnet (sprich „$\mathbb{Z}$ modulo n“). Bei $n = 0$ ist das einfach $\mathbb{Z}$ selbst, bei $n = 1$ ist das die triviale Gruppe. Im Allgemeinen ist die durch die Untergruppe $\mathbb{Z}n$ definierte Äquivalenzrelation auf $\mathbb{Z}$ dadurch gegeben, dass zwei ganze Zahlen a und b genau dann äquivalent sind, wenn ihre Differenz $a - b$ zu $\mathbb{Z}n$

gehört, also ein Vielfaches von n ist. Daher ist (bei $n \geq 1$) jede ganze Zahl zu genau einer der n Zahlen

$$0, 1, 2, \ldots, n-1$$

äquivalent (oder, wie man auch sagt, *kongruent modulo* n), nämlich zum Rest, der sich bei Division durch n ergibt. Diese Reste bilden also ein Repräsentantensystem für die Restklassengruppe, und diese besitzt n Elemente. Die Tatsache, dass die Restklassenabbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n),\ a \longmapsto [a] = a \mod n,$$

ein Homomorphismus ist, kann man auch so ausdrücken, dass der Rest einer Summe von zwei ganzen Zahlen nur von den beiden Resten, nicht aber von den Zahlen selbst, abhängt.[4] Als Bild der zyklischen Gruppe[5] $\mathbb{Z}$ ist auch $\mathbb{Z}/(n)$ zyklisch, und zwar ist 1 (aber auch -1) stets ein Erzeuger.

5.4. **Die Homomorphiesätze für Gruppen.**

Satz 5.10. *Seien G, Q und H Gruppen, es sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus und $\psi\colon G \to Q$ ein surjektiver Gruppenhomomorphismus. Es sei vorausgesetzt, dass*

$$\operatorname{kern}\psi \subseteq \operatorname{kern}\varphi$$

ist. Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi}\colon Q \longrightarrow H$$

derart, dass $\varphi = \tilde{\varphi} \circ \psi$ ist. Mit anderen Worten: das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle\psi}\downarrow & \nearrow{\scriptstyle\tilde{\varphi}} & \\ Q & & \end{array}$$

ist kommutativ.

Beweis. Wir zeigen zuerst die Eindeutigkeit. Für jedes Element $u \in Q$ gibt es mindestens ein $g \in G$ mit $\psi(g) = u$. Wegen der Kommutativität des Diagramms muss

$$\tilde{\varphi}(u) = \varphi(g)$$

gelten. Das bedeutet, dass es maximal ein $\tilde{\varphi}$ geben kann. Wir haben zu zeigen, dass durch diese Bedingung eine wohldefinierte Abbildung gegeben ist. Seien also $g, g' \in G$ zwei Urbilder von u. Dann ist

$$\psi\left(g'g^{-1}\right) = uu^{-1} = e_Q$$

[4]Dies gilt auch für das Produkt von zwei Zahlen, was bedeutet, dass diese Abbildung ein Ringhomomorphismus ist.

[5]Eine Gruppe G heißt *zyklisch*, wenn sie von einem Element erzeugt wird.

und somit ist $g'g^{-1} \in \operatorname{kern}\psi \subseteq \operatorname{kern}\varphi$. Daher ist $\varphi(g) = \varphi(g')$. Die Abbildung ist also wohldefiniert. Seien $u, v \in Q$ und seien $g, h \in G$ Urbilder davon. Dann ist gh ein Urbild von uv und daher ist

$$\tilde{\varphi}(uv) = \varphi(gh) = \varphi(g)\varphi(h) = \tilde{\varphi}(u)\tilde{\varphi}(v).$$

D.h. $\tilde{\varphi}$ ist ein Gruppenhomomorphismus. □

Die im vorstehenden Satz konstruierte Abbildung heißt *induzierte Abbildung* oder *induzierter Homomorphismus* und entsprechend heißt der Satz auch *Satz vom induzierten Homomorphismus*.

Korollar 5.11. *Seien G und H Gruppen und sei*

$$\varphi\colon\ G \longrightarrow H$$

ein surjektiver Gruppenhomomorphismus. Dann gibt es eine kanonische Isomorphie

$$\tilde{\varphi}\colon\ G/\operatorname{kern}\varphi \longrightarrow H.$$

Beweis. Wir wenden Satz 5.10 auf $Q = G/\operatorname{kern}\varphi$ und die kanonische Projektion $q\colon\ G \to G/\operatorname{kern}\varphi$ an. Dies induziert einen Gruppenhomomorphismus

$$\tilde{\varphi}\colon\ G/\operatorname{kern}\varphi \longrightarrow H$$

mit $\varphi = \tilde{\varphi} \circ q$, der surjektiv ist. Sei $[x] \in G/\operatorname{kern}\varphi$ und $[x] \in \operatorname{kern}\tilde{\varphi}$. Dann ist

$$\tilde{\varphi}([x]) = \varphi(x) = e_H,$$

also $x \in \operatorname{kern}\varphi$. Damit ist $[x] = e_Q$, d.h. der Kern von $\tilde{\varphi}$ ist trivial und nach Lemma 4.9 ist $\tilde{\varphi}$ auch injektiv. □

Satz 5.12. *Seien G und H Gruppen und sei*

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann gibt es eine kanonische Faktorisierung

$$G \xrightarrow{q} G/\operatorname{kern}\varphi \xrightarrow{\theta} \operatorname{bild}\varphi \overset{\iota}{\hookrightarrow} H\,,$$

wobei q die kanonische Projektion, θ ein Gruppenisomorphismus und ι die kanonische Inklusion der Bildgruppe ist.

Beweis. Dies folgt aus Korollar 5.11, angewandt auf die Bildgruppe $U = \operatorname{bild}\varphi \subseteq H$. □

Diese Aussage wird häufig kurz und prägnant so formuliert:

Bild = Urbild modulo Kern.

Satz 5.13. *Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler mit der Restklassengruppe $Q = G/N$. Es sei $H \subseteq G$ ein weiterer Normalteiler in G, der N umfasst. Dann ist das Bild $\overline{H}$ von H in Q ein Normalteiler und es gilt die kanonische Isomorphie*

$$G/H \cong Q/\overline{H}.$$

Beweis. Für die erste Aussage siehe Aufgabe 5.25. Damit ist die Restklassengruppe $Q/\overline{H}$ wohldefiniert. Wir betrachten die Komposition

$$p \circ q : G \longrightarrow Q \longrightarrow Q/\overline{H}\,.$$

Wegen

$$\begin{array}{rcl} \operatorname{kern}(p \circ q) & = & \{x \in G |\, (p \circ q)(x) = e\} \\ & = & \{x \in G |\, q(x) \in \operatorname{kern} p\} \\ & = & \left\{x \in G |\, q(x) \in \overline{H}\right\} \\ & = & H \end{array}$$

ist $\operatorname{kern}(p \circ q) = H$. Daher ergibt Korollar 5.11 die kanonische Isomorphie

$$G/H \longrightarrow Q/\overline{H}.$$

□

Kurz gesagt ist also

$$G/H = (G/N)/(H/N).$$

5. Arbeitsblatt

5.1. **Aufwärmaufgaben.**

Aufgabe 5.1. Es sei $\mathrm{GL}_n(K)$ die Menge der invertierbaren $n \times n$-Matrizen über einem Körper K. Zeige, dass für zueinander konjugierte Matrizen M und N aus $\mathrm{GL}_n(K)$ die folgenden Eigenschaften bzw. Invarianten übereinstimmen: Die Determinante, die Eigenwerte, die Dimension der Eigenräume zu einem Eigenwert, die Diagonalisierbarkeit, die Trigonalisierbarkeit.

Aufgabe 5.2. Sei G eine Gruppe. Betrachte die Relation R auf G, wobei xRy bedeutet, dass es einen inneren Automorphismus κ_g mit $x = \kappa_g(y)$ gibt. Zeige, dass diese Relation eine Äquivalenzrelation ist.

Die Äquivalenzklassen zu dieser Äquivalenzrelation bekommen einen eigenen Namen:

Zu einer Gruppe G nennt man die Äquivalenzklassen zur Äquivalenzrelation, bei der zwei Elemente als äquivalent (oder *konjugiert*) gelten, wenn sie durch einen inneren Automorphismus ineinander überführt werden können, die *Konjugationsklassen*.

Aufgabe 5.3.
(1) Bestimme die Konjugationsklassen auf der Drehgruppe $\mathrm{SO}_2(\mathbb{R})$.
(2) Bestimme die Konjugationsklassen der Elemente $\varphi \in \mathrm{SO}_2(\mathbb{R})$ innerhalb von $\mathrm{O}_2(\mathbb{R})$.

(3) Bestimme die Konjugationsklassen der Elemente $\varphi \in \mathrm{SO}_2(\mathbb{R})$ innerhalb von $\mathrm{SL}_2(\mathbb{R})$.
(4) Bestimme die Konjugationsklassen der Elemente $\varphi \in \mathrm{SO}_2(\mathbb{R})$ innerhalb von $\mathrm{GL}_2(\mathbb{R})$.

Aufgabe 5.4. Sei $n \in \mathbb{N}_+$ und sei $K \subseteq \mathbb{C}$ ein Unterkörper. Wir betrachten den Gruppenhomomorphismus

$$S_n \longrightarrow \mathrm{GL}_n(K)\,,\ \pi \longmapsto M_\pi,$$

der jeder Permutation π die zugehörige Permutationsmatrix zuordnet. Zeige, dass zwei Permutationen π, ρ genau dann konjugiert in S_n sind, wenn ihre zugehörigen Permutationsmatrizen M_π, M_ρ ähnlich sind.

Aufgabe 5.5.*

Seien G und H Gruppen und sei

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Zeige, dass das Urbild $\varphi^{-1}(N)$ eines Normalteilers $N \subseteq H$ ein Normalteiler in G ist.

Aufgabe 5.6. Zeige, dass der Durchschnitt von Normalteilern N_i, $i \in I$, in einer Gruppe G ein Normalteiler ist.

Aufgabe 5.7. Seien G und H Gruppen und sei

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenhomomorphismus. Ist das Bild von φ ein Normalteiler in H?

Zu $n \in \mathbb{N}$ heißt die Untergruppe

$$A_n := \{\sigma \in S_n |\ \mathrm{sgn}(\sigma) = 1\}$$

der geraden Permutationen die *alternierende Gruppe*.

Aufgabe 5.8. Bestimme, ob die alternierende Gruppe A_n ein Normalteiler in der Permutationsgruppe S_n ist.

Aufgabe 5.9. Es sei K ein Körper, $n \in \mathbb{N}_+$, $\mathrm{GL}_n(K)$ die allgemeine lineare Gruppe der invertierbaren Matrizen und

$$\mathrm{SL}_n(K) \subseteq \mathrm{GL}_n(K)$$

die Untergruppe der Matrizen mit Determinante 1. Zeige, dass die Linksnebenklasse (und auch die Rechtsnebenklasse) zu $M \in \mathrm{GL}_n(K)$ gleich der Menge aller Matrizen ist, deren Determinante mit $\det M$ übereinstimmt.

Zeige auf möglichst viele Weisen, dass $\mathrm{SL}_n(K)$ ein Normalteiler in $\mathrm{GL}_n(K)$ ist.

Aufgabe 5.10. Man gebe ein Beispiel von drei Untergruppen $F \subseteq G \subseteq H$ an derart, dass F ein Normalteiler in G und G ein Normalteiler in H, aber F kein Normalteiler in H ist.

In der folgenden Aufgabe wird das *Zentrum* einer Gruppe verwendet.

Sei G eine Gruppe. Das *Zentrum* $Z = Z(G)$ von G ist die Teilmenge

$$Z = \{g \in G | \, gx = xg \text{ für alle } x \in G\}.$$

Aufgabe 5.11.*

Sei G eine Gruppe und sei $H \subseteq Z$ eine Untergruppe des Zentrums von G. Zeige, dass H ein Normalteiler in G ist.

Aufgabe 5.12. Sei G eine Gruppe. Zeige, dass das Zentrum $Z \subseteq G$ ein Normalteiler in G ist. Man bringe das Zentrum in Zusammenhang mit dem Gruppenhomomorphismus

$$\kappa \colon G \longrightarrow \mathrm{Aut}\,(G),\ g \longmapsto \kappa_g.$$

Was ist das Bild von diesem Homomorphismus, und was besagen die Homomorphiesätze in dieser Situation?

Aufgabe 5.13. Sei G eine Gruppe und sei M eine Menge mit einer Verknüpfung. Es sei

$$\varphi \colon G \longrightarrow M$$

eine surjektive Abbildung mit $\varphi(gh) = \varphi(g)\varphi(h)$ für alle $g, h \in G$. Zeige, dass M eine Gruppe und φ ein Gruppenhomomorphismus ist.

Aufgabe 5.14. Es seien G und H Gruppen mit der Produktgruppe $G \times H$. Zeige, dass die Gruppe $G \times \{e_H\}$ ein Normalteiler in $G \times H$ ist, und dass die Restklassengruppe $(G \times H)/G \times \{e_H\}$ kanonisch isomorph zu H ist.

Aufgabe 5.15. Es seien G_1 und G_2 Gruppen und seien $N_1 \subseteq G_1$ und $N_2 \subseteq G_2$ Normalteiler. Zeige, dass $N_1 \times N_2$ ein Normalteiler in $G_1 \times G_2$ ist und dass eine Isomorphie

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$$

vorliegt.

Aufgabe 5.16. Zeige, dass für jede reelle Zahl $a \neq 0$ die Restklassengruppen $\mathbb{R}/\mathbb{Z}a$ untereinander isomorph sind.

Aufgabe 5.17. Bestimme die Restklassengruppe zu $\{1, -1\} \subset \mathbb{R}^\times$.

Aufgabe 5.18.*

Zeige, dass es in der Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ zu jedem $n \in \mathbb{N}_+$ Elemente gibt, deren Ordnung gleich n ist.

Aufgabe 5.19. Zeige, dass es keine Untergruppe $F \subseteq (\mathbb{Q}, 0, +)$ derart gibt, dass

$$F \longrightarrow \mathbb{Q}/\mathbb{Z}$$

ein Isomorphismus ist.

Aufgabe 5.20. Sei G eine Gruppe und $g \in G$ ein Element mit dem (nach Lemma 4.4) zugehörigen Gruppenhomomorphismus

$$\varphi\colon\ \mathbb{Z} \longrightarrow G,\ n \longmapsto g^n.$$

Beschreibe die kanonische Faktorisierung von φ gemäß Satz 5.12.

Aufgabe 5.21. Zeige mit Hilfe der Homomorphiesätze, dass zyklische Gruppen mit der gleichen Ordnung isomorph sind.

5.2. **Aufgaben zum Abgeben.**

Aufgabe 5.22. (2 Punkte)

Es sei S_3 die Gruppe der bijektiven Abbildungen der Menge $\{1,2,3\}$ in sich selbst. Bestimme die Konjugationsklassen dieser Gruppe.

Aufgabe 5.23. (5 Punkte)

Es sei p eine Primzahl und $\mathbb{Z}/(p)$ die zyklische Gruppe mit p Elementen. Finde eine Gruppe G derart, dass $\mathbb{Z}/(p) \subseteq G$ eine Untergruppe ist und dass in G je zwei von 0 verschiedene Elemente aus $\mathbb{Z}/(p)$ zueinander konjugiert sind.

Aufgabe 5.24. (3 Punkte)

Bestimme die Konjugationsklassen der (eigentlichen) Würfelgruppe.

Aufgabe 5.25. (2 Punkte)

Seien G und H Gruppen und sei

$$\varphi\colon\ G \longrightarrow H$$

ein surjektiver Gruppenhomomorphismus. Zeige, dass das Bild $\varphi(N)$ eines Normalteilers $N \subseteq G$ ein Normalteiler in H ist.

Aufgabe 5.26. (2 Punkte)

Zeige, dass jede Untergruppe vom Index zwei in einer Gruppe G ein Normalteiler in G ist.

6. Vorlesung - Algebren

6.1. **Ringhomomorphismen.**

Wir besprechen nun die strukturerhaltenden Abbildungen zwischen Ringen (und Körpern).

Definition 6.1. Seien R und S Ringe. Eine Abbildung

$$\varphi\colon\ R \longrightarrow S$$

heißt *Ringhomomorphismus*, wenn folgende Eigenschaften gelten:

(1) $\varphi(a+b) = \varphi(a)+\varphi(b)$.
(2) $\varphi(1) = 1$.
(3) $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.

Ein Ringhomomorphismus ist also zugleich ein Gruppenhomomorphismus für die additive Struktur und ein Monoidhomomorphismus für die multiplikative Struktur. Einen bijektiven Ringhomomorphismus nennt man einen *Ringisomorphismus*, und zwei Ringe heißen *isomorph*, wenn es einen Ringisomorphismus zwischen ihnen gibt. Zu einem Unterring $S \subseteq R$ ist die natürliche Inklusion ein Ringhomomorphismus. Die konstante Abbildung $R \to 0$ in den Nullring ist stets ein Ringhomomorphismus, dagegen ist die umgekehrte Abbildung, also $0 \to R$, nur bei $R = 0$ ein Ringhomomorphismus.

6.2. **Die Charakteristik eines Ringes.**

Satz 6.2. *Sei R ein Ring. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\mathbb{Z} \longrightarrow R.$$

Beweis. Ein Ringhomomorphismus muss die 1 auf die 1_R abbilden. Deshalb gibt es nach Lemma 4.4 genau einen Gruppenhomomorphismus

$$\mathbb{Z} \longrightarrow (R, +, 0),\ n \longmapsto n1_R.$$

Wir müssen zeigen, dass diese Abbildung auch die Multiplikation respektiert, d.h. dass $(mn)1_R = (m1_R) * (n1_R)$. ist, wobei $*$ hier die Multiplikation in R bezeichnet. Dies folgt aber aus dem allgemeinen Distributivgesetz. □

Den in dieser Aussage konstruierten und eindeutig bestimmten Ringhomomorphismus nennt man auch den *kanonischen Ringhomomorphismus* (oder den *charakteristischen Ringhomomorphismus*) von $\mathbb{Z}$ nach R.

Definition 6.3. Die *Charakteristik* eines kommutativen Ringes R ist die kleinste positive natürliche Zahl n mit der Eigenschaft $n \cdot 1_R = 0$. Die Charakteristik ist 0, falls keine solche Zahl existiert.

Die Charakteristik beschreibt genau den Kern des obigen kanonischen (charakteristischen) Ringhomomorphismus.

6.3. **Der Einsetzungshomomorphismus.**

Satz 6.4. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Es sei A ein weiterer kommutativer Ring und es sei $\varphi\colon R \to A$ ein Ringhomomorphismus und $a \in A$ ein Element. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\psi\colon R[X] \longrightarrow A$$

mit $\psi(X) = a$ und mit $\psi \circ i = \varphi$, wobei $i\colon R \to R[X]$ die kanonische Einbettung ist. Dabei geht das Polynom $P = \sum_{j=0}^{n} c_j X^j$ auf $\sum_{j=0}^{n} \varphi(c_j) a^j$.

Beweis. Bei einem Ringhomomorphismus

$$\psi\colon\ R[X] \longrightarrow A$$

mit $\psi \circ i = \varphi$. müssen die Konstanten $c \in R$ auf $\varphi(c)$ und X auf a gehen. Daher muss X^j auf a^j gehen. Da Summen respektiert werden, kann es nur einen Ringhomorphismus geben, der die im Zusatz angegebene Gestalt haben muss. Es ist also zu zeigen, dass durch diese Vorschrift wirklich ein Ringhomomorphismus definiert ist. Dies folgt aber direkt aus dem Distributivgesetz. □

Den in diesem Satz konstruierten Ringhomomorphismus nennt man den *Einsetzungshomomorphismus*. Es wird ja für die Variable X das Element a eingesetzt.

6.4. **Algebren.**

Ein wichtiges Konzept für das Studium von Körpern und Ringen ist, diese als eine Erweiterung von einfacheren Ringen aufzufassen (Grundring, Grundkörper) und dann mit Hilfe des schon verstandenen einfacheren Objektes das erweiterte Objekt zu untersuchen. Man spricht vom relativen Standpunkt. Diese Idee wird durch den Begriff Algebra präzisiert.

Definition 6.5. Seien R und A kommutative Ringe und sei $R \to A$ ein fixierter Ringhomomorphismus. Dann nennt man A eine *R-Algebra*.

Häufig ist der Ringhomomorphismus, der zum Begriff der Algebra gehört, vom Kontext her klar und wird nicht explizit aufgeführt. Z.B. ist der Polynomring $R[X]$ eine R-Algebra, indem man die Elemente aus R als konstante Polynome auffasst. Jeder Ring A ist auf eine eindeutige Weise eine $\mathbb{Z}$-Algebra über den kanonischen Ringhomomorphismus $\mathbb{Z} \to A$, $n \mapsto n_A$. Bei einer Körpererweiterung $K \subseteq L$ ist L eine K-Algebra. Der Begriff der Algebra ist auch für nicht-kommutative Ringe A (bei kommutativem Grundring R) sinnvoll, wobei dann in aller Regel die Voraussetzung gemacht wird, dass die Elemente aus R mit allen Elementen aus A vertauschen.

Wir werden den Begriff der Algebra vor allem in dem Fall verwenden, wo der Grundring R ein Körper K ist. Eine K-Algebra A kann man stets in natürlicher Weise als Vektorraum über dem Körper K auffassen. Die Skalarmultiplikation wird dabei einfach über den Strukturhomomorphismus erklärt. Eine typische Situation ist dabei, dass $\mathbb{Q}$ der Grundkörper ist und ein Zwischenring L, $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$, gegeben ist. Dann ist L über die Inklusion direkt eine $\mathbb{Q}$-Algebra.

Wenn man zwei Algebren über einem gemeinsamen Grundring hat, so sind vor allem diejenigen Ringhomomorphismen interessant, die den Grundring mitberücksichtigen. Dies führt zu folgendem Begriff.

Definition 6.6. Seien A und B kommutative R-Algebren über einem kommutativen Grundring R. Dann nennt man einen Ringhomomorphismus

$$\varphi\colon\ A \longrightarrow B$$

einen R- *Algebrahomomorphismus* , wenn er zusätzlich mit den beiden fixierten Ringhomomorphismen $R \to A$ und $R \to B$ verträglich ist.

Zum Beispiel ist jeder Ringhomomorphismus ein $\mathbb{Z}$-Algebrahomomorphismus, da es zu jedem Ring A überhaupt nur den kanonischen Ringhomomorphismus $\mathbb{Z} \to A$ gibt.

Mit dieser Terminologie kann man den Einsetzungshomomorphismus jetzt so verstehen, dass der Polynomring $R[X]$ mit seiner natürlichen Algebrastruktur und eine weitere R-Algebra A mit einem fixierten Element $a \in A$ vorliegt und dass dann durch $X \mapsto a$ ein R-Algebrahomomorphismus $R[X] \to A$ definiert wird.

6.5. **Ideale unter einem Ringhomomorphismus.**

Der Zusammenhang zwischen Ringhomomorphismen und Idealen wird durch folgenden Satz hergestellt.

Satz 6.7. *Seien R und S kommutative Ringe und sei*

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus. Dann ist der Kern

$$\operatorname{kern}\varphi\ =\ \{f \in R |\ \varphi(f) = 0\}$$

ein Ideal in R.

Beweis. Sei

$$I\ :=\ \varphi^{-1}(0).$$

Wegen $\varphi(0) = 0.$ ist $0 \in I$. Seien $a, b \in I$. Das bedeutet $\varphi(a) = 0$ und $\varphi(b) = 0$. Dann ist

$$\varphi(a+b)\ =\ \varphi(a) + \varphi(b)\ =\ 0 + 0\ =\ 0$$

und daher $a + b \in I$.

Sei nun $a \in I$ und $r \in R$ beliebig. Dann ist

$$\varphi(ra)\ =\ \varphi(r)\varphi(a)\ =\ \varphi(r) \cdot 0\ =\ 0,$$

also ist $ra \in I$. □

Da ein Ringhomomorphismus insbesondere ein Gruppenhomomorphismus der zugrunde liegenden additiven Gruppe ist, gilt wieder das Kernkriterium für die Injektivität. Eine Anwendung davon ist das folgende Korollar.

Korollar 6.8. *Es sei K ein Körper und S ein vom Nullring verschiedener Ring. Es sei*

$$\varphi\colon K \longrightarrow S$$

ein Ringhomomorphismus. Dann ist φ injektiv.

Beweis. Es genügt nach Lemma 4.9 zu zeigen, dass der Kern der Abbildung gleich 0 ist. Nach Satz 6.7 ist der Kern ein Ideal. Da die 1 auf $1 \neq 0$ geht, ist der Kern nicht ganz K. Da es nach Lemma 20.9 (Lineare Algebra (Osnabrück 2017-2018)) in einem Körper überhaupt nur zwei Ideale gibt, muss der Kern das Nullideal sein. □

6.6. **Algebraische Elemente und Minimalpolynom.**

Definition 6.9. Sei K ein Körper und A eine kommutative K-Algebra. Es sei $f \in A$ ein Element. Dann heißt f *algebraisch* über K, wenn es ein von 0 verschiedenes Polynom $P \in K[X]$ mit $P(f) = 0$ gibt.

Wenn ein Polynom $P \neq 0$ das algebraische Element $f \in A$ annulliert (also $P(f) = 0$ ist), so kann man durch den Leitkoeffizienten dividieren und erhält dann auch ein normiertes annullierendes Polynom.

Definition 6.10. Sei K ein Körper und A eine K-Algebra. Es sei $f \in A$ ein über K algebraisches Element. Dann heißt das normierte Polynom $P \in K[X]$ mit $P(f) = 0$, welches von minimalem Grad mit dieser Eigenschaft ist, das *Minimalpolynom* von f.

Wenn f nicht algebraisch ist, so wird das Nullpolynom als Minimalpolynom betrachtet.

Beispiel 6.11. Bei einer Körpererweiterung $K \subseteq L$ sind die Elemente $a \in K$ trivialerweise algebraisch, und zwar ist jeweils $X - a \in K[X]$ das Minimalpolynom. Weitere Beispiele liefern über $K = \mathbb{Q}$ die komplexen Zahlen $\sqrt{2}, \mathrm{i}, 3^{1/5}$, etc. Annullierende Polynome aus $\mathbb{Q}[X]$ sind dafür $X^2 - 2$, $X^2 + 1$, $X^5 - 3$ (es handelt sich dabei übrigens um die Minimalpolynome, was in den ersten beiden Fällen einfach und im dritten Fall etwas schwieriger zu zeigen ist). Man beachte, dass beispielsweise $X - \sqrt{2}$ zwar ein annullierendes Polynom für $\sqrt{2}$ ist, dessen Koeffizienten aber nicht zu $\mathbb{Q}$ gehören.

Lemma 6.12. *Sei K ein Körper, A eine K-Algebra und $f \in A$ ein Element. Es sei P das Minimalpolynom von f über K. Dann ist der Kern des kanonischen K-Algebrahomomorphismus*

$$K[X] \longrightarrow A,\ X \longmapsto f,$$

das von P erzeugte Hauptideal.

Beweis. Wir betrachten den kanonischen Einsetzungshomorphismus

$$K[X] \longrightarrow A,\ X \longmapsto f.$$

Dessen Kern ist nach Satz 6.7 und nach Satz 3.15 ein Hauptideal, sagen wir $\mathfrak{a} = (F)$, wobei wir F als normiert annehmen dürfen (im nicht-algebraischen Fall liegt das Nullideal vor und die Aussage ist trivialerweise richtig). Das Minimalpolynom P gehört zu $\mathfrak{a}$. Andererseits ist der Grad von F größer oder gleich dem Grad von P, da ja dessen Grad minimal gewählt ist. Daher muss der Grad gleich sein und somit ist $P = F$, da beide normiert sind. □

Definition 6.13. Eine Körpererweiterung $K \subseteq L$, heißt *algebraisch*, wenn jedes Element $f \in L$ algebraisch über K ist.

6.7. **Erzeugendensysteme.**

Definition 6.14. Sei A eine R-Algebra und sei $f_i \in A$, $i \in I$, eine Familie von Elementen aus A. Dann heißt die kleinste R-Unteralgebra von A, die alle f_i enthält, die von diesen Elementen *erzeugte R-Algebra*. Sie wird mit $R[f_i,\, i \in I]$ bezeichnet.

Man kann diese R-Algebra auch als den kleinsten Unterring von A charakterisieren, der sowohl R als auch die f_i enthält. Wir werden hauptsächlich von erzeugten K-Algebren in einer Körpererweiterung $K \subseteq L$ sprechen, wobei nur ein einziger Erzeuger vorgegeben ist. Man schreibt dafür dann einfach $K[f]$, und diese K-Algebra besteht aus allen K-Linearkombinationen von Potenzen von f. Dies ist das Bild unter dem durch $X \mapsto f$ gegebenen Einsetzungshomomorphismus.

Gelegentlich werden wir auch den kleinsten Unterkörper von L betrachten, der sowohl K als auch eine Elementfamilie f_i, $i \in I$, enthält. Dieser wird mit $K(f_i, i \in I)$ bezeichnet, und man sagt, dass die f_i ein *Körper-Erzeugendensystem* von diesem Körper bilden. Es ist $K[f_i, i \in I] \subseteq K(f_i, i \in I)$ und insbesondere $K[f] \subseteq K(f)$.

Definition 6.15. Es sei K ein Körper. Der *Primkörper* von K ist der kleinste Unterkörper von K.

Definition 6.16. Eine Körpererweiterung $K \subseteq L$, heißt *einfach*, wenn es ein Element $x \in L$ mit

$$L = K(x)$$

gibt.

Definition 6.17. Eine Körpererweiterung $K \subseteq L$ heißt eine *einfache Radikalerweiterung*, wenn es ein $b \in L$ gibt mit $L = K(b)$ und ein $n \in \mathbb{N}$ mit $b^n \in K$.

Definition 6.18. Eine Körpererweiterung $K \subseteq L$ heißt eine *Radikalerweiterung*, wenn es Zwischenkörper

$$K \subseteq L_1 \subseteq \ldots \subseteq L_{n-1} \subseteq L_n = L$$

derart gibt, dass $L_i \subseteq L_{i+1}$ für jedes i eine einfache Radikalerweiterung ist.

Bemerkung 6.19. Bei einer Radikalerweiterung entstehen die einzelnen einfachen Radikalerweiterungen durch die Hinzunahme von reinen Wurzelausdrücken. Dies gilt aber im Allgemeinen nicht für die Gesamterweiterung. Beispielsweise kann man eine Situation der Form

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{7}] \subseteq (\mathbb{Q}[\sqrt[3]{7}]) \left[\sqrt[5]{2+9\sqrt[3]{7}-4\sqrt[3]{7}^2}\right]$$

haben (alles spiele sich innerhalb von $\mathbb{C}$ ab). In den Einzelschritten kommt eine reine Wurzel aus dem Vorgängerkörper hinzu, insgesamt entstehen dabei aber beliebig verschachtelte Wurzelausdrücke. Radikalerweiterungen sind dafür da, solche verschachtelten Wurzelausdrücke systematisch zu erfassen.

Wenn eine komplexe Zahl $z \in \mathbb{C}$ als Nullstelle eines normierten Polynoms mit Koeffizienten aus $\mathbb{Q}$ auftritt, so ist es eine wichtige Frage, ob man sie innerhalb einer Radikalerweiterung beschreiben kann. Die Formel von Cardano besagt insbesondere, dass man die Nullstellen einer kubischen Gleichung $x^3+px+q=0$ innerhalb einer Radikalerweiterung realisieren kann, und zwar braucht man dazu die dritten Einheitswurzeln, die Quadratwurzel $\sqrt{3\,(4p^3+27q^2)}$ und noch dritte Wurzeln von zuvor erzeugten Ausdrücken. Siehe auch Aufgabe 2.8.

6. Arbeitsblatt

6.1. **Aufwärmaufgaben.**

Aufgabe 6.1. Zeige, dass die Umkehrabbildung eines Ringisomorphismus wieder ein Ringhomomorphismus ist.

Aufgabe 6.2. Zeige, dass das Bild unter einem Ringhomomorphismus ein Unterring ist.

Aufgabe 6.3. Zeige, dass das Bild eines Ideals unter einem Ringhomomorphismus nicht unbedingt wieder ein Ideal ist.

Aufgabe 6.4. Es sei R ein Integritätsbereich der Charakteristik $n \in \mathbb{N}$. Zeige, dass die Ordnung von jedem Element $x \in R$, $x \neq 0$, ebenfalls n ist.

Aufgabe 6.5. Es sei R ein kommutativer Ring der Charakteristik $n \in \mathbb{N}$. Zeige, dass die Ordnung von jedem Element $x \in R$, $x \neq 0$, ein Teiler von n ist.

Aufgabe 6.6. Sei R ein kommutativer Ring und sei $\varphi\colon \mathbb{Z} \to R$ der kanonische Homomorphismus. Zeige, dass die Charakteristik von R der eindeutig bestimmte nichtnegative Erzeuger des Kernideals $\ker \varphi \subseteq \mathbb{Z}$ ist.

Aufgabe 6.7. Sei R ein kommutativer Ring. Zeige, dass der kanonische Homomorphismus $\varphi\colon \mathbb{Z} \to R$ eine eindeutige Faktorisierung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n) \longrightarrow R$$

besitzt, wobei n die Charakteristik von R ist.

Aufgabe 6.8. Bestimme sämtliche Primkörper.

Aufgabe 6.9. Sei R ein kommutativer Ring mit endlich vielen Elementen. Zeige, dass R genau dann ein Integritätsbereich ist, wenn R ein Körper ist.

Aufgabe 6.10. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Berechne das Bild des Polynoms X^3+4X-3 unter dem durch $X \mapsto X^2+X-1$ definierten Einsetzungshomomorphismus $K[X] \to K[X]$.

Aufgabe 6.11. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $a \in K$ ein fixiertes Element. Bestimme den Kern des Einsetzungshomomorphismus

$$K[X] \longrightarrow K,\ X \longmapsto a.$$

Aufgabe 6.12. Es sei $A \subseteq \mathbb{Q}$ die Menge derjenigen rationalen Zahlen, die eine abbrechende Dezimalentwicklung besitzen. Zeige, dass A ein Unterring von $\mathbb{Q}$ ist und bestimme die Einheiten von A.

Aufgabe 6.13. Es sei $C = \mathrm{C}^0(\mathbb{R}, \mathbb{R})$ der Ring der stetigen Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Entscheide, ob die folgenden Teilmengen von C einen Unterring bilden.

(1) Die Menge der stetigen 2π-periodischen Funktionen.
(2) Die Menge der stetigen geraden Funktionen.
(3) Die Menge der stetigen ungeraden Funktionen.

Aufgabe 6.14. Es sei $\mathbb{K} = \mathbb{R}$ oder $\mathbb{C}$ und es sei $D_{\mathbb{K}} = \mathrm{C}^1(\mathbb{K}, \mathbb{K})$ der Ring der stetig-differenzierbaren Funktionen von $\mathbb{K}$ nach $\mathbb{K}$. Zeige, dass der Einsetzungshomomorphismus

$$\Psi\colon\ \mathbb{K}[X] \longrightarrow D_{\mathbb{K}},\ X \longmapsto \mathrm{Id}_{\mathbb{K}},$$

injektiv ist. Bestimme die Polynome $F \in \mathbb{K}[X]$, für die $\Psi(F)$ eine Einheit in $D_{\mathbb{K}}$ ist.

Aufgabe 6.15.*

Sei R ein Integritätsbereich und $R[X]$ der Polynomring über R. Zeige, dass die Einheiten von $R[X]$ genau die Einheiten von R sind.

6.2. **Aufgaben zum Abgeben.**

Aufgabe 6.16. (3 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Berechne das Bild des Polynoms $X^4 - 2X^2 + 5X - 2$ unter dem durch $X \mapsto 2X^3 + X - 1$ definierten Einsetzungshomomorphismus $K[X] \to K[X]$.

Aufgabe 6.17. (5 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $P \in K[X]$ ein nicht-konstantes Polynom. Zeige, dass der durch $X \mapsto P$ definierte Einsetzungshomomorphismus von $K[X]$ nach $K[X]$ injektiv ist und dass der durch P erzeugte Unterring $K[P] \subseteq K[X]$ isomorph zum Polynomring in einer Variablen ist.

Zeige, dass bei $\mathrm{grad}\,(P) \geq 2$ ein echter Unterring $K[P] \subset K[X]$ vorliegt.

Aufgabe 6.18. (4 Punkte)

Es sei K ein Körper. Betrachte den Matrizenring $\mathrm{Mat}_3(K)$ und darin die Matrix

$$M = \begin{pmatrix} 3 & 4 & 5 \\ 2 & 4 & 6 \\ 1 & 4 & 7 \end{pmatrix}.$$

Definiere einen Ringhomomorphismus

$$K[X] \longrightarrow \mathrm{Mat}_3(K),$$

der X auf M schickt. Bestimme den Kern dieser Abbildung.

Aufgabe 6.19. (2 Punkte)

Es sei K ein Körper der Charakteristik 0 und $K \subseteq L$ eine quadratische Körpererweiterung. Zeige, dass dies eine einfache Radikalerweiterung ist.

7. Vorlesung - Restklassenringe

7.1. **Restklassenringe.**

Nach Satz 6.7 ist der Kern eines Ringhomomorphismus ein Ideal. Man kann umgekehrt zu jedem Ideal $I \subseteq R$ in einem (kommutativen) Ring einen Ring R/I konstruieren, und zwar zusammen mit einem surjektiven Ringhomomorphismus

$$R \longrightarrow R/I,$$

dessen Kern gerade das vorgegebene Ideal I ist. Ideale und Kerne von Ringhomomorphismen sind also im Wesentlichen äquivalente Objekte, so wie das bei Gruppen für Kerne von Gruppenhomomorphismen und Normalteilern gilt. In der Tat gelten die entsprechenden Homomorphiesätze hier wieder, und können weitgehend auf die Gruppensituation zurückgeführt werden. Wir werden uns bei den Beweisen also kurz fassen können.

Definition 7.1. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Zu $a \in R$ heißt die Teilmenge

$$a + I = \{a + f | \, f \in I\}$$

die *Nebenklasse von* a zum Ideal I. Jede Teilmenge von dieser Form heißt *Nebenklasse* zu I.

Diese Nebenklassen sind gerade die Nebenklassen zur Untergruppe $I \subseteq R$, die wegen der Kommutativität ein Normalteiler ist. Zwei Elemente $a, b \in R$ definieren genau dann die gleiche Nebenklasse, also $a + I = b + I$, wenn ihre Differenz $a - b$ zum Ideal gehört. Man sagt dann auch, dass a und b dieselbe Nebenklasse *repräsentieren*.

Definition 7.2. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Dann ist der *Restklassenring* R/I (sprich „R modulo I“) ein kommutativer Ring, der durch folgende Daten festgelegt ist.

(1) Als Menge ist R/I die Menge der Nebenklassen zu I.
(2) Durch
$$(a + I) + (b + I) := (a + b + I)$$
wird eine Addition von Nebenklassen definiert.
(3) Durch
$$(a + I) \cdot (b + I) := (a \cdot b + I)$$
wird eine Multiplikation von Nebenklassen definiert.
(4) $\bar{0} = 0 + I = I$ definiert das neutrale Element für die Addition (die Nullklasse).
(5) $\bar{1} = 1 + I$ definiert das neutrale Element für die Multiplikation (die Einsklasse).

Man muss dabei zeigen, dass diese Abbildungen (also Addition und Multiplikation) wohldefiniert sind, d.h. unabhängig vom Repräsentanten, und dass die Ringaxiome erfüllt sind. Da I insbesondere eine Untergruppe der kommutativen Gruppe $(R,+,0)$ ist, liegt ein Normalteiler vor, so dass R/I eine Gruppe ist und die Restklassenabbildung

$$R \longrightarrow R/I,\, a \longmapsto a+I =: \bar{a},$$

ein Gruppenhomomorphismus ist. Das einzig Neue gegenüber der Gruppensituation ist also die Anwesenheit einer Multiplikation. Die Wohldefiniertheit der Multiplikation ergibt sich so: Seien zwei Restklassen gegeben mit unterschiedlichen Repräsentanten, also $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$. Dann ist $a - a' \in I$ und $b - b' \in I$ bzw. $a' = a + x$ und $b' = b + y$ mit $x, y \in I$. Daraus ergibt sich

$$a'b' = (a+x)(b+y) = ab + ay + xb + xy.$$

Die drei hinteren Summanden gehören zum Ideal, so dass die Differenz $a'b' - ab \in I$ ist.

Aus der Wohldefiniertheit folgen die anderen Eigenschaften und insbesondere, dass ein Ringhomomorphismus in den Restklassenring vorliegt. Diesen nennt man wieder die *Restklassenabbildung* oder den *Restklassenhomomorphismus*. Das Bild von $a \in R$ in R/I wird häufig mit $[a]$, $\bar{a}$ oder einfach mit a selbst bezeichnet und heißt die *Restklasse* von a. Bei dieser Abbildung gehen genau die Elemente aus dem Ideal auf 0, d.h. der Kern dieser Restklassenabbildung ist das vorgegebene Ideal.

Das einfachste Beispiel für diesen Prozess ist die Abbildung, die einer ganzen Zahl a den Rest bei Division durch eine fixierte Zahl d zuordnet. Jeder Rest wird dann repräsentiert durch eine der Zahlen $0, 1, 2, \ldots, d-1$. Im Allgemeinen gibt es nicht immer ein solch übersichtliches Repräsentantensystem.

7.2. **Die Homomorphiesätze für Ringe.**

Für Ringe, ihre Ideale und Ringhomomorphismen gelten die analogen Homomorphiesätze wie für Gruppen, ihre Normalteiler und Gruppenhomomorphismen, siehe die fünfte Vorlesung. Wir beschränken uns auf kommutative Ringe.

Satz 7.3. *Seien R, S und T kommutative Ringe, es sei $\varphi\colon R \to S$ ein Ringhomomorphismus und $\psi\colon R \to T$ ein surjektiver Ringhomomorphismus. Es sei vorausgesetzt, dass*

$$\operatorname{kern}\psi \subseteq \operatorname{kern}\varphi$$

ist. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi}\colon T \longrightarrow S$$

derart, dass $\varphi = \tilde{\varphi} \circ \psi$ ist. Mit anderen Worten: das Diagramm

$$\begin{array}{ccc} R & \longrightarrow & T \\ & \searrow & \downarrow \\ & & S \end{array}$$

ist kommutativ.

Beweis. Aufgrund von Satz 5.10 gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi}\colon\ T \longrightarrow S,$$

der die Eigenschaften erfüllt. Es ist also lediglich noch zu zeigen, dass $\tilde{\varphi}$ auch die Multiplikation respektiert. Seien dazu $t, t' \in T$, und diese seien repräsentiert durch r bzw. r' aus R. Dann wird tt' durch rr' repräsentiert und daher ist

$$\tilde{\varphi}(tt') = \varphi(rr') = \varphi(r)\varphi(r') = \tilde{\varphi}(t)\tilde{\varphi}(t').$$

□

Die im vorstehenden Satz konstruierte Abbildung heißt wieder *induzierte Abbildung* oder *induzierter Homomorphismus* und entsprechend heißt der Satz auch *Satz vom induzierten Homomorphismus.*

Korollar 7.4. *Es seien R und S kommutative Ringe und es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein surjektiver Ringhomomorphismus. Dann gibt es eine kanonische Isomorphie von Ringen

$$\tilde{\varphi}\colon\ R/\operatorname{kern}\varphi \longrightarrow S.$$

Beweis. Aufgrund von Korollar 5.11 liegt ein natürlicher Gruppenisomorphismus vor, der wegen Satz 7.3 auch die Multiplikation respektiert, also ein Ringhomomorphismus ist. □

Satz 7.5. *Es seien R und S kommutative Ringe und es sei*

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus. Dann gibt es eine kanonische Faktorisierung

$$R \xrightarrow{q} R/\operatorname{kern}\varphi \xrightarrow{\theta} \operatorname{bild}\varphi \xhookrightarrow{\iota} S\,,$$

wobei q die kanonische Projektion, θ ein Ringisomorphismus und ι die kanonische Inklusion des Bildes ist.

Beweis. Dies beruht auf Satz 5.12 und Satz 7.3. □

Es gilt also wieder:

Bild = Urbild modulo Kern.

7.3. **Restklassenringe von Hauptidealbereichen.**

Da wir nun die Restklassenbildung für kommutative Ringe zur Verfügung haben, kehren wir zu Hauptidealbereichen, insbesondere zu Polynomringen über einem Körper zurück.

Satz 7.6. *Sei R ein Hauptidealbereich und $p \neq 0$ ein Element. Dann sind folgende Bedingungen äquivalent.*

(1) *p ist ein Primelement.*
(2) *$R/(p)$ ist ein Integritätsbereich.*
(3) *$R/(p)$ ist ein Körper.*

Beweis. Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt in jedem kommutativen Ring (auch für $p = 0$), siehe Aufgabe 7.1, und (3) impliziert natürlich (2). Sei also (1) erfüllt und sei $a \in R/(p)$ von 0 verschieden. Wir bezeichnen einen Repräsentanten davon in R ebenfalls mit a. Es ist dann $a \notin (p)$ und es ergibt sich eine echte Idealinklusion $(p) \subset (a, p)$. Ferner können wir $(a, p) = (b)$ schreiben, da wir in einem Hauptidealring sind. Es folgt $p = cb$. Da c keine Einheit ist und p prim (also nach Lemma 3.10 auch irreduzibel) ist, muss b eine Einheit sein. Es ist also $(a, p) = (1)$, und das bedeutet modulo p, also in $R/(p)$, dass a eine Einheit ist. Also ist $R/(p)$ ein Körper. □

Korollar 7.7. *Es sei K ein Körper und $P \in K[X]$, $P \neq 0$, ein Polynom. Dann ist P genau dann irreduzibel, wenn der Restklassenring $K[X]/(P)$ ein Körper ist.*

Beweis. Dies folgt direkt aus Satz 3.15 und Satz 7.6. □

Jedes irreduzible Polynom $F \in K[X]$ definiert also eine (endliche) Körpererweiterung $K \subseteq K[X]/(F)$, und dies wird unsere Hauptkonstruktionsweise für endliche Körpererweiterungen sein.

Für die ganzen Zahlen hat man das entsprechende Resultat.

Korollar 7.8. *Es sei $n \geq 1$ eine natürliche Zahl und $\mathbb{Z}/(n)$ der zugehörige Restklassenring. Dann sind folgende Aussagen äquivalent.*

(1) *$\mathbb{Z}/(n)$ ist ein Körper.*
(2) *$\mathbb{Z}/(n)$ ist ein Integritätsbereich.*
(3) *n ist eine Primzahl.*

Beweis. Dies folgt direkt aus Satz 7.6. □

7.4. **Rechnen in $K[X]/(P)$.**

Körper werden häufig ausgehend von einem schon bekannten Körper als Restklassenkörper des Polynomrings konstruiert. Die Arithmetik in einem solchen Erweiterungskörper wird in der folgenden Aussage beschrieben.

Proposition 7.9. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $P = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom vom Grad n und $R = K[X]/(P)$ der zugehörige Restklassenring. Dann gelten folgende Rechenregeln (wir bezeichnen die Restklasse von X in R mit x).*

1. *Man kann stets P als normiert annehmen (also $a_n = 1$; das werden wir im Folgenden tun).*
2. *In R ist $x^n = -\sum_{i=0}^{n-1} a_i x^i$.*
3. *Höhere Potenzen x^k, $k \geq n$, kann man mit den Potenzen x^i, $i \leq n-1$, ausdrücken, indem man mittels Vielfachen von (2) sukzessive den Grad um eins reduziert.*
4. *Die Potenzen $x^0 = 1$, $x^1, \ldots, x^{n-1}$ bilden eine K-Basis von R.*
5. *R ist ein K-Vektorraum der Dimension n.*
6. *In R werden zwei Elemente $P = \sum_{i=0}^{n-1} b_i x^i$ und $Q = \sum_{i=0}^{n-1} c_i x^i$ komponentenweise addiert, und multipliziert, indem sie als Polynome multipliziert werden und dann die Restklasse berechnet wird.*

Beweis. (1) Es ist $(P) = \left(\frac{P}{a_n}\right)$, da es bei einem Hauptideal nicht auf eine Einheit ankommt.

(2) Dies folgt direkt durch Umstellung der definierenden Gleichung $P = 0$.

(3) Dies folgt durch Multiplikation der Gleichung in (2) mit Potenzen von x.

(4) Dass die Potenzen x^i, $i = 0, \ldots, n-1$, ein Erzeugendensystem bildet, folgt aus Teil (2) und (3). Zum Beweis der linearen Unabhängigkeit sei angenommen, es gebe eine lineare Abhängigkeit, sagen wir $\sum_{i=0}^{n-1} c_i x^i = 0$. D.h., dass das Polynom $Q = \sum_{i=0}^{n-1} c_i X^i$ unter der Restklassenabbildung auf 0 geht, also zum Kern gehört. Dann muss es aber ein Vielfaches von P sein, was aber aus Gradgründen erzwingt, dass Q das Nullpolynom sein muss. Also sind alle $c_i = 0$.

(5) Dies folgt direkt aus (4).

(6) Dies ist klar.

□

Beispiel 7.10. Wir betrachten den Restklassenring

$$L = \mathbb{Q}[X]/(X^3 + 2X^2 - 5)$$

und bezeichnen die Restklasse von X mit x. Aufgrund von Proposition 7.9 besitzt jedes Element f aus L eine eindeutige Darstellung $f = ax^2 + bx + c$ mit $a, b, c \in \mathbb{Q}$, so dass also ein dreidimensionaler $\mathbb{Q}$-Vektorraum vorliegt. Da $X^3 + 2X^2 - 5$ in L zu 0 gemacht wird, gilt

$$x^3 = -2x^2 + 5.$$

Daraus ergeben sich die Gleichungen

$$x^4 = -2x^3 + 5x = -2(-2x^2 + 5) + 5x = 4x^2 + 5x - 10,$$

$$x^5 = -2x^4 + 5x^2 = -2(4x^2 + 5x - 10) + 5x^2 = -3x^2 - 10x + 20,$$

etc. Man kann hierbei auf verschiedene Arten zu dem eindeutig bestimmten kanonischen Repräsentanten reduzieren.

Berechnen wir nun das Produkt

$$(3x^2 - 2x + 4)(2x^2 + x - 1)\,.$$

Dabei wird distributiv ausmultipliziert und anschließend werden die Potenzen reduziert. Es ist

$$\begin{aligned} & (3x^2 - 2x + 4)(2x^2 + x - 1) \\ = \; & 6x^4 + 3x^3 - 3x^2 - 4x^3 - 2x^2 + 2x + 8x^2 + 4x - 4 \\ = \; & 6x^4 - x^3 + 3x^2 + 6x - 4 \\ = \; & 6(4x^2 + 5x - 10) + 2x^2 - 5 + 3x^2 + 6x - 4 \\ = \; & 29x^2 + 36x - 69. \end{aligned}$$

7.5. **Restklassendarstellung von Unteralgebren.**

Satz 7.11. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Es sei P das Minimalpolynom von f. Dann gibt es eine kanonische K-Algebraisomorphie*

$$K[X]/(P) \longrightarrow K[f],\, X \longmapsto f.$$

Beweis. Die Einsetzung $X \mapsto f$ ergibt nach Satz 6.4 den kanonischen K-Algebrahomomorphismus

$$K[X] \longrightarrow L,\, X \longmapsto f.$$

Das Bild davon ist genau $K[f]$, so dass ein surjektiver K-Algebrahomomorphismus

$$K[X] \longrightarrow K[f]$$

vorliegt. Daher gibt es nach Korollar 7.4 eine Isomorphie zwischen $K[f]$ und dem Restklassenring von $K[X]$ modulo dem Kern der Abbildung. Der Kern ist aber nach Lemma 6.12 das vom Minimalpolynom erzeugte Hauptideal. □

Lemma 7.12. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann gelten folgende Aussagen.*

(1) *Das Minimalpolynom P von f über K ist irreduzibel.*
(2) *Wenn $Q \in K[X]$ ein normiertes, irreduzibles Polynom mit $Q(f) = 0$ ist, so handelt es sich um das Minimalpolynom.*

Beweis. (1) Es sei $P = P_1P_2$ eine Faktorzerlegung des Minimalpolynoms. Dann gilt in L die Beziehung

$$0 = P(f) = P_1(f)P_2(f).$$

Da L ein Körper ist, muss ein Faktor 0 sein, sagen wir $P_1(f) = 0$. Da aber P unter allen Polynomen $\neq 0$, die f annullieren, den minimalen Grad besitzt, müssen P und P_1 den gleichen Grad besitzen und folglich muss P_2 konstant ($\neq 0$), also eine Einheit sein.

(2) Wegen $Q(f) = 0$ ist Q aufgrund von Lemma 6.12 ein Vielfaches des Minimalpolynoms P, sagen wir $Q = GP$. Da Q nach Voraussetzung irreduzibel ist, und da P zumindest den Grad 1 besitzt, muss G konstant sein. Da schließlich sowohl P als auch Q normiert sind, ist $P = Q$.

□

7. Arbeitsblatt

7.1. **Aufwärmaufgaben.**

Aufgabe 7.1. Sei R ein kommutativer Ring und $p \in R$, $p \neq 0$. Zeige, dass p genau dann ein Primelement ist, wenn der Restklassenring $R/(p)$ ein Integritätsbereich ist.

Aufgabe 7.2. Sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring $S = R/\mathfrak{a}$. Zeige, dass ein Element $f \in R$ genau dann eine Einheit in S ist, wenn in R das Ideal $\mathfrak{a}$ zusammen mit f das Einheitsideal erzeugt.

Aufgabe 7.3. Sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring $S = R/\mathfrak{a}$. Zeige, dass die Ideale von S eindeutig denjenigen Idealen von R entsprechen, die $\mathfrak{a}$ umfassen.

Aufgabe 7.4. Sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring $S = R/\mathfrak{a}$. Zu einem Ideal $I \subseteq R$ welches $\mathfrak{a}$ enthält, sei $I' = IR/\mathfrak{a}$ das zugehörige Ideal in S. Zeige, dass es eine kanonische Ringisomorphie

$$R/I \cong S/I'$$

gibt.

Aufgabe 7.5. Wende Satz 7.5 auf den kanonischen Ringhomomorphismus $\mathbb{Z} \to R$ zu einem kommutativen Ring R an.

Aufgabe 7.6. Es sei K ein Körper, A eine K-Algebra mit einem Element $f \in A$. Wende Satz 7.5 auf den zugehörigen Einsetzungshomomorphismus $K[X] \to A$, $X \mapsto f$, an.

Aufgabe 7.7. Zeige, dass die komplexen Zahlen $\mathbb{C}$ die Restklassendarstellung

$$\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$$

besitzen.

Aufgabe 7.8. Sei X ein topologischer Raum und $R = \mathrm{C}^0(X, \mathbb{R})$ der Ring der stetigen Funktionen auf X. Es sei $T \subseteq X$ eine Teilmenge. Zeige, dass die Teilmenge

$$I = \{f \in R | \, f|_T = 0\}$$

ein Ideal in R ist. Definiere einen Ringhomomorphismus

$$R/I \longrightarrow \mathrm{C}^0(T, \mathbb{R}).$$

Ist dieser immer injektiv? Surjektiv?

Aufgabe 7.9. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(7)$.

Aufgabe 7.10.*

Berechne 3^{1457} in $\mathbb{Z}/(13)$.

Aufgabe 7.11. Sei p eine Primzahl. Beweise durch Induktion den kleinen Fermat, also die Aussage, dass $a^p - a$ ein Vielfaches von p für jede ganze Zahl a ist.

Aufgabe 7.12. Bestimme im Polynomring $\mathbb{F}_5[X]$ alle irreduziblen Polynome vom Grad 3.

Aufgabe 7.13. Bestimme die fünf kleinsten Primzahlen p mit der Eigenschaft, dass das Polynom $X^6 - 1$ über $\mathbb{Z}/(p)$ in Linearfaktoren zerfällt.

Aufgabe 7.14.*

Betrachte den Körper $K = \mathbb{F}_4 = \mathbb{Z}/(2)[U]/(U^2+U+1)$. Führe im Polynomring $K[X]$ die Polynomdivision

$$X^4 + uX^3 + (u+1)X + 1 \text{ durch } uX^2 + X + u + 1$$

aus, wobei u die Restklasse von U in K bezeichnet.

Aufgabe 7.15. a) Bestimme die Primfaktorzerlegung des Polynoms $F = X^3 + X + 2$ in $\mathbb{Z}/(5)[X]$.

b) Zeige, dass durch

$$K = \mathbb{Z}/(5)[T]/(T^2 - 2)$$

ein Körper mit 25 Elementen gegeben ist.

c) Bestimmen die Primfaktorzerlegung von $F = X^3 + X + 2$ über $K = \mathbb{Z}/(5)[T]/(T^2 - 2)$.

Aufgabe 7.16.*

Sei p eine Primzahl und sei $f(x)$ ein Polynom mit Koeffizienten in $\mathbb{Z}/(p)$ vom Grad $d \geq p$. Zeige, dass es ein Polynom $g(x)$ mit einem Grad $< p$ derart gibt, dass für alle Elemente $a \in \mathbb{Z}/(p)$ die Gleichheit

$$f(a) = g(a)$$

gilt.

Aufgabe 7.17.*

Es sei R ein kommutativer Ring und $R[X]$ der Polynomring über R. Es sei $\mathfrak{a} \subseteq R[X]$ ein Ideal mit Erzeugern

$$\mathfrak{a} = (F_0, F_1, \ldots, F_n),$$

wobei $F_0 = X - r$ mit $r \in R$ sei. Für $i \geq 1$ seien G_i die Elemente aus R, die entstehen, wenn man in F_i die Variable X durch r ersetzt. Zeige, dass eine Ringisomorphie der Restklassenringe

$$R[X]/\mathfrak{a} \cong R/(G_1, \ldots, G_n)$$

vorliegt.

Aufgabe 7.18.*

Bestimme in $\mathbb{Q}[X]/(X^3 + 4X^2 - 7)$ das Inverse von $\frac{1}{3}x + 5$ (x bezeichnet die Restklasse von X).

Aufgabe 7.19.*

Bestimme in $\mathbb{Q}[X]/(X^3 - 7)$ das Inverse von $3x + 4$ (x bezeichnet die Restklasse von X).

Aufgabe 7.20. Bestimme das Inverse von

$$1 + \sqrt{2} + 3\sqrt{10}$$

im Körper $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$.

Aufgabe 7.21. Sei p eine Primzahl.

a) Zeige, dass das Polynom $X^4 - p$ irreduzibel über $\mathbb{Q}$ ist.

b) Schließe daraus, dass

$$\mathbb{Q}[\sqrt[4]{p}] \subseteq \mathbb{R}$$

über $\mathbb{Q}$ den Grad vier besitzt.

c) Finde einen echten Zwischenkörper

$$\mathbb{Q} \subseteq K \subseteq \mathbb{Q}[\sqrt[4]{p}].$$

Aufgabe 7.22. Zeige, dass die Abbildung

$$\mathbb{Q}[\mathrm{i}]^\times \longrightarrow (\mathbb{Q}_+, 1, \cdot),\ z = x + \mathrm{i}y \longmapsto |z|^2 = x^2 + y^2,$$

ein Gruppenhomomorphismus ist.

Aufgabe 7.23. Zeige, dass die Menge

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] |\ |z| = 1\}$$

mit der Multiplikation in $\mathbb{Q}[\mathrm{i}]$ eine kommutative Gruppe ist.

Aufgabe 7.24. Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] |\ |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[\mathrm{i}]^\times$ ererbten Gruppenstruktur. Berechne die ersten vier Potenzen von $\frac{3}{5} + \frac{4}{5}\mathrm{i} \in S^1_{\mathbb{Q}}$.

7.2. **Aufgaben zum Abgeben.**

Aufgabe 7.25. (3 Punkte)

Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(11)$.

Aufgabe 7.26. (5 Punkte)

Bestimme im Polynomring $\mathbb{Z}/(3)[X]$ alle irreduziblen Polynome vom Grad 4.

Aufgabe 7.27. (4 Punkte)

Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] |\ |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[\mathrm{i}]^\times$ ererbten Gruppenstruktur. Zeige, dass die Gruppen $S^1_{\mathbb{Q}}$ und $\mathbb{Q}/\mathbb{Z}$ nicht isomorph sind.

Aufgabe 7.28. (5 Punkte)
Zeige, dass der Gruppenhomomorphismus

$$\mathbb{Q}[\mathrm{i}]^\times \longrightarrow (\mathbb{Q}_+, 1, \cdot),\ x + \mathrm{i}y \longmapsto x^2 + y^2,$$

nicht surjektiv ist.

Aufgabe 7.29. (5 (1+1+2+1) Punkte)
Betrachte den Körper $\mathbb{Z}/(13) = \{0, 1, 2, ..., 12\}$ mit 13 Elementen.

(1) Zeige, dass 5 kein Quadrat in $\mathbb{Z}/(13)$ ist und folgere, dass

$$\mathbb{Z}/(13)[X]/(X^2 - 5) =: \mathbb{Z}/(13)[\sqrt{5}]$$

ein Körper ist.
(2) Betrachte die quadratische Körpererweiterung

$$\mathbb{Z}/(13) \subset \mathbb{Z}/(13)[\sqrt{5}]$$

und berechne

$$(2 + 3\sqrt{5})(1 + 11\sqrt{5})(10 + 7\sqrt{5})$$

(3) Finde das Inverse zu $7 + 3\sqrt{5}$ in $\mathbb{Z}/(13)[\sqrt{5}]$.
(4) Zeige, dass -5 kein Quadrat in $\mathbb{Z}/(13)$ ist, dafür aber in $\mathbb{Z}/(13)[\sqrt{5}]$.

Aufgabe 7.30. (4 Punkte)
Bestimme das Inverse von

$$2 + 3\sqrt{5} + \sqrt{7} + 3\sqrt{35}$$

im Körper $\mathbb{Q}[\sqrt{5}, \sqrt{7}]$.

Aufgabe 7.31. (4 Punkte)
Bestimme das Minimalpolynom von

$$\sqrt{3} + \sqrt{5}$$

über $\mathbb{Q}$.

8. Vorlesung - Norm und Spur

8.1. **Norm und Spur bei einer Körpererweiterung.**

Ein Element $f \in L$ einer Körpererweiterung (oder allgemeiner einer K-Algebra A) $K \subseteq L$ definiert durch Multiplikation eine K-lineare Abbildung

$$\mu_f \colon L \longrightarrow L,\, y \longmapsto fy.$$

Dies erlaubt es, Begriffe und Methoden der linearen Algebra anzuwenden. Zu einer K-Basis von L wird die Multiplikationsabbildung durch eine $(n \times n)$-Matrix beschrieben, wobei n den Grad der Körpererweiterung bezeichnet. Für $f \in K$ liegt bezüglich einer beliebigen Basis die Streckungsmatrix

$$\begin{pmatrix} f & 0 & 0 & \dots & 0 \\ 0 & f & 0 & \dots & 0 \\ 0 & 0 & f & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & f \end{pmatrix}$$

vor, für beliebige Elemente $f \in L$ werden die Matrizen ziemlich kompliziert, was man teilweise durch Wahl einer geeigneten Basis korrigieren kann. Insbesondere sind Konzepte relevant, die nicht von der Wahl einer Basis abhängen.

Beispiel 8.1. Es sei $F = X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0 \in K[X]$ ein irreduzibles Polynom über einem Körper K und

$$K \subseteq K[X]/\left(X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0\right) =: L$$

die zugehörige endliche Körpererweiterung. Nach Proposition 7.9 bilden die Potenzen x^i, $0 \leq i \leq n-1$, (wobei x die Restklasse von X bezeichnet) eine K-Basis von L. Zu einem $g \in L$ wird die Multiplikationsabbildung

$$\mu_g \colon L \longrightarrow L,\, y \longmapsto gy,$$

bezüglich der gegebenen Basis durch die $(n \times n)$-Matrix beschrieben, deren Spalten aus den Koordinanten zu den Produkten $g \cdot x^i$, $0 \leq i \leq n-1$, bezüglich der Basis besteht. Wegen $x^0 = 1$ stehen in der ersten Spalte einfach die Koordinaten von g selbst. Zu x ist diese Matrix gleich

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

beschrieben. Zu einem beliebigen Element

$$g = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$$

wird die Matrix schnell kompliziert, wir führen nur die ersten beiden Spalten an

$$\begin{pmatrix} b_0 & -a_0b_{n-1} & \dots & * & * \\ b_1 & b_0 - a_1b_{n-1} & \dots & * & * \\ b_2 & b_1 - a_2b_{n-1} & \dots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n-1} & b_{n-2} - a_{n-1}b_{n-1} & \dots & * & * \end{pmatrix}.$$

In der folgenden Aussage wird zu einem K-Vektorraum mit $\mathrm{End}_K(V)$ der (nichtkommutative) Ring bezeichnet, der aus allen K-linearen Abbildungen besteht und wobei die Multiplikations durch die Hintereinanderschaltung von Abbildungen gegeben ist.

Lemma 8.2. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist die Abbildung*

$$L \longrightarrow \mathrm{End}_K(L),\ f \longmapsto \mu_f,$$

ein injektiver Ringhomomorphismus.

Beweis. Siehe Aufgabe 8.6. □

Über diese Konstruktion bzw. Zuordnung werden Norm und Spur von f erklärt.

Bemerkung 8.3. Zu einer linearen Abbildung

$$\varphi\colon V \longrightarrow V$$

eines endlichdimensionalen K-Vektorraumes V in sich wird die Determinante $\det(\varphi)$ und die Spur $S(\varphi)$ wie folgt berechnet. Man wählt eine K-Basis $v_1, \dots, v_n \in V$ und repräsentiert die lineare Abbildung bezüglich dieser Basis durch eine quadratische $n \times n$-Matrix

$$\begin{pmatrix} \lambda_{1,1} & \cdots & \lambda_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & \lambda_{n,n} \end{pmatrix}$$

mit $\lambda_{ij} \in K$ und rechnet dann die Determinante aus. Es folgt aus dem Determinantenmultiplikationssatz, dass dies unabhängig von der Wahl der Basis ist. Die Spur ist durch

$$S(\varphi) = \lambda_{1,1} + \lambda_{2,2} + \cdots + \lambda_{n,n}$$

gegeben, und dies ist nach Aufgabe 8.17 ebenfalls unabhängig von der Wahl der Basis.

Definition 8.4. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Determinante der K-linearen Abbildung

$$\mu_f\colon L \longrightarrow L,\ y \longmapsto fy,$$

die *Norm* von f. Sie wird mit $N(f)$ bezeichnet.

Definition 8.5. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Spur der K-linearen Abbildung

$$\varphi_f \colon L \longrightarrow L,\, y \longmapsto fy,$$

die *Spur* von f. Sie wird mit $S(f)$ bezeichnet.

Beispiel 8.6. Es sei $K \subseteq L = K[X]/(X^n - a)$ eine Körpererweiterung, die durch die Hinzunahme einer n-ten Wurzel aus einem Element $a \in K$ entstehe. Es sei x die Restklasse von X. Dann wird μ_x bezüglich der K-Basis $1, x, x^2, \ldots, x^{n-1}$ von L durch die Matrix

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & a \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

beschrieben. Somit ist die Norm von x gleich $\pm a$ (das Vorzeichen hängt davon ab, ob n gerade oder ungerade ist) und die Spur ist 0.

Lemma 8.7. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann hat die Norm*

$$N \colon L \longrightarrow K,\, f \longmapsto N(f),$$

folgende Eigenschaften:

(1) *Es ist $N(fg) = N(f)N(g)$.*
(2) *Für $f \in K$ ist $N(f) = f^n$, wobei n den Grad der Körpererweiterung bezeichne.*
(3) *Es ist $N(f) = 0$ genau dann, wenn $f = 0$ ist.*

Beweis. (1) Dies folgt aus dem Determinantenmultiplikationssatz und Lemma 8.2.
(2) Zu einer beliebigen Basis von L wird die Multiplikation mit einen Element $f \in K$ durch die Diagonalmatrix beschrieben, bei der jeder Diagonaleintrag f ist. Die Determinante ist daher f^n nach Lemma 16.4 (Lineare Algebra (Osnabrück 2017-2018)).
(3) Die eine Richtung ist klar, sei also $f \neq 0$. Dann ist f eine Einheit in L und daher ist die Multiplikation mit f eine bijektive K-lineare Abbildung $L \to L$, und deren Determinante ist $\neq 0$ nach Satz 16.11 (Lineare Algebra (Osnabrück 2017-2018)).

□

Lemma 8.8. *Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann hat die Spur*

$$S \colon L \longrightarrow K,\, f \longmapsto S(f),$$

folgende Eigenschaften:

(1) *Die Spur ist K-linear, also $S(f+g) = S(f)+S(g)$ und $S(\lambda f) = \lambda S(f)$ für $\lambda \in K$.*
(2) *Für $f \in K$ ist $S(f) = nf$.*

Beweis. Dies folgt aus den Definitionen. □

Norm und Spur sind Elemente aus K.

Lemma 8.9. *Es sei $K \subseteq L$ eine endliche Körpererweiterung und $f \in L$ mit der zugehörigen K-linearen Abbildung*

$$\mu_f \colon L \longrightarrow L,\, x \longmapsto fx.$$

Dann stimmt das Minimalpolynom von f mit dem Minimalpolynom von μ_f überein.

Beweis. Dies folgt aus dem kommutativen Diagramm

$$\begin{array}{ccc} K[X] & \stackrel{X \mapsto f}{\longrightarrow} & L \\ & X \mapsto \mu_f \searrow & \downarrow \mu \\ & & \operatorname{End}(L) \end{array}$$

von Ringhomomorphismen, in dem horizontal die Einsetzungshomomorphismen stehen, und Lemma 8.2. □

Im Minimalpolynom zu $f \in L$ finden sich Norm und Spur in folgender Weise wieder.

Satz 8.10. *Sei $K \subseteq L = K[f]$ eine einfache endliche Körpererweiterung vom Grad n. Dann hat das Minimalpolynom P von f die Gestalt*

$$P = X^n - S(f)X^{n-1} + \cdots + (-1)^n N(f).$$

Beweis. Das Minimalpolynom und das charakteristische Polynom der durch f definierten K-linearen Multiplikationsabbildung

$$\mu_f \colon L \longrightarrow L,\, y \longmapsto fy,$$

haben beide den Grad n. Nach dem Satz von Cayley-Hamilton annulliert das charakteristische Polynom die lineare Abbildung und ist somit ein Vielfaches des Minimalpolynoms, so dass sie übereinstimmen. Sei bezüglich einer Basis $v_1, \ldots, v_n$ von L diese lineare Abbildung μ_f durch die Matrix $(\lambda_{ij})_{ij}$ gegeben. Dann ist das charakteristische Polynom gleich

$$\chi_{\mu_f} = \det \begin{pmatrix} X-\lambda_{1,1} & \cdots & -\lambda_{1,n} \\ \vdots & \ddots & \vdots \\ -\lambda_{n,1} & \cdots & X-\lambda_{n,n} \end{pmatrix} = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

Zum Koeffizienten a_{n-1} leisten (in der Leibniz-Formel zur Berechnung der Determinante) nur diejenigen Permutationen einen Beitrag, bei denen $(n-1)$-mal die Variable X vorkommt, und das ist nur bei der identischen Permutation (also der Diagonalen) der Fall. Multipliziert man die Diagonale distributiv

aus, so ergibt sich $X^n - \sum_{i=1}^n \lambda_{i,i} X^{n-1} + \ldots$, so dass also $a_{n-1} = -S(f)$ gilt. Setzt man in der obigen Gleichung $X = 0$, so ergibt sich, dass a_0 die Determinante der negierten Matrix ist, woraus $a_0 = (-1)^n N(f)$ folgt. □

Weitere Beschreibungen des Minimalpolynoms und der Norm und der Spur finden sich in Korollar 13.9 und Korollar 13.10.

8.2. **Diskriminante.**

Die Lösbarkeit einer quadratischen Gleichung $x^2 + px + q = 0$ über einem Körper K hängt im Wesentlichen davon ab, ob die „Diskriminante“ $p^2 - 4q$ eine Quadratwurzel in K besitzt. Für die Lösungen einer kubischen Gleichung $x^3 + px + q = 0$ spielt nach Satz 1.2 der Ausdruck $-4p^3 - 27q^2$ (bzw. das -3-fache davon) eine wichtige Rolle. Beide Terme fallen unter das allgemeine Konzept einer Diskriminante, das wir kurz vorstellen.

Definition 8.11. Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ Elemente in L. Dann wird die *Diskriminante* von $b_1, \ldots, b_n$ durch

$$\triangle(b_1, \ldots, b_n) = \det\left(S(b_i b_j)_{i,j}\right)$$

definiert.

Die Produkte $b_i b_j$, $1 \leq i, j \leq n$, sind dabei Elemente in L, von denen man jeweils die Spur nimmt, die in K liegt. Man erhält also eine quadratische $n \times n$-Matrix über K. Deren Determinante ist nach Definition die Diskriminante. Im folgenden werden wir vor allem an der Diskriminante von speziellen Basen interessiert sein.

Beispiel 8.12. Wir betrachten eine quadratische Gleichung $X^2 + pX + q = 0$ und (unter der Voraussetzung, dass das Polynom irreduzibel ist) die zugehörige quadratische Körpererweiterung $K \subseteq L = K[X]/\left(X^2 + pX + q\right)$. Wir bestimmen die Diskriminante dieser Erweiterung zur Basis $1, x$. Wir müssen also die Spuren der Elemente $1, x, x^2 = -px - q$ bestimmen. Die Matrizen dieser Elemente sind

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix} \text{ und } \begin{pmatrix} -q & pq \\ -p & p^2 - q \end{pmatrix}$$

und ihre Spuren sind 2, $-p$ und $p^2 - 2q$. Somit ist die Diskriminante gleich

$$\triangle(1, x) = \det \begin{pmatrix} 2 & -p \\ -p & p^2 - 2q \end{pmatrix} = 2\left(p^2 - 2q\right) - p^2 = p^2 - 4q.$$

Beispiel 8.13. Wir betrachten die kubische Gleichung

$$x^3 + px + q = 0$$

und (unter der Voraussetzung, dass das Polynom irreduzibel ist) die zugehörige kubische Körpererweiterung $K \subseteq L = K[X]/\left(X^3 + pX + q\right)$. Wir bestimmen die Diskriminante dieser Erweiterung zur Basis $1, x, x^2$. Die Matrix

zu x ist $\begin{pmatrix} 0 & 0 & -q \\ 1 & 0 & -p \\ 0 & 1 & 0 \end{pmatrix}$, die Matrix zu x^2 ist $\begin{pmatrix} 0 & -q & 0 \\ 0 & -p & -q \\ 1 & 0 & -p \end{pmatrix}$, die Matrix zu $x^3 = -px - q$ ist $\begin{pmatrix} -q & 0 & pq \\ -p & -q & p^2 \\ 0 & -p & -q \end{pmatrix}$, die Matrix zu $x^4 = -px^2 - qx$ ist $\begin{pmatrix} 0 & pq & q^2 \\ -q & p^2 & 2pq \\ -p & -q & p^2 \end{pmatrix}$. Die Diskriminante ist daher die Determinante der Matrix

$$\begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix},$$

also gleich

$$3\left(-4p^3 - 9q^2\right) - 2p(-4p^2) = -4p^3 - 27q^2.$$

Dies ist die Zahl D aus Satz 1.2.

Bei einem Basiswechsel verhält sich die Diskriminante wie folgt.

Lemma 8.14. *Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ zwei K-Basen von L. Der Basiswechsel werde durch $c = Tb$ mit der Übergangsmatrix $T = (t_{ij})_{ij}$ beschrieben. Dann gilt für die Diskriminanten die Beziehung*

$$\triangle(c_1, \ldots, c_n) = (\det(T))^2 \triangle(b_1, \ldots, b_n).$$

Beweis. Ausgeschrieben haben wir die Beziehungen $c_i = \sum_{j=1}^n t_{ij} b_j$. Damit gilt

$$c_i c_k = \left(\sum_{j=1}^n t_{ij} b_j\right)\left(\sum_{m=1}^n t_{km} b_m\right) = \sum_{j,m} t_{ij} t_{km} b_j b_m.$$

Wir schreiben $c_{ik} := S(c_i c_k)$ und $b_{jm} := S(b_j b_m)$. Wegen der K-Linearität der Spur gilt

$$c_{ik} = S(c_i c_k) = S\left(\sum_{j,m} t_{ij} t_{km} b_j b_m\right) = \sum_{j,m} t_{ij} t_{km} S(b_j b_m) = \sum_{j,m} t_{ij} t_{km} b_{jm}.$$

Wir schreiben diese Gleichung mit den Matrizen $C = (c_{ik})$, $B = (b_{jm})$ und $T = (t_{ij})$ als

$$C = T^{\text{transp}} B T$$

und die Behauptung folgt dann aus dem Determinantenmultiplikationssatz und Satz 17.5 (Lineare Algebra (Osnabrück 2017-2018)). □

Satz 8.15. *Sei K ein Körper der Charakteristik 0 und sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und sei $b_1, \ldots, b_n$ eine K-Basis von L. Dann ist*

$$\triangle(b_1, \ldots, b_n) \neq 0.$$

Beweis. Siehe Aufgabe 8.22. □

8. Arbeitsblatt

8.1. **Aufwärmaufgaben.**

Aufgabe 8.1. Sei $K \subseteq L$ eine Körpererweiterung und $f \in L$. Zeige, dass die Abbildung

$$\mu_f \colon L \longrightarrow L,\, x \longmapsto fx,$$

K-linear ist.

Aufgabe 8.2. Wir betrachten die endliche Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$. Beschreibe die Matrix der Multiplikationsabbildung zu $7 + 5\mathrm{i}$ bezüglich der reellen Basis $1, \mathrm{i}$ von $\mathbb{C}$.

Aufgabe 8.3. Wir betrachten die quadratische Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}] = L$. Erstelle die Matrix der Multiplikationsabbildung zu $-4 + 9\sqrt{3}$ bezüglich der $\mathbb{Q}$-Basis $1, \sqrt{3}$ von L.

Aufgabe 8.4. Erstelle die Multiplikationsmatrix zum Element $7x^2 - 4x + 5$ in der kubischen Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 6X^2 + 5X - 8\right).$$

Aufgabe 8.5.*

Es seien p, q verschiedene Primzahlen und

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p}, \sqrt{q}] =: L$$

die zugehörige Körpererweiterung. Erstelle die Multiplikationsmatrix zu einem Element $a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \in L$ bezüglich der Basis $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$.

Aufgabe 8.6. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass die Abbildung

$$L \longrightarrow \mathrm{End}_K(L),\, f \longmapsto \mu_f,$$

ein injektiver Ringhomomorphismus ist.

Aufgabe 8.7. Es sei $K \subseteq M \subseteq L$ eine Körpererweiterung. Es sei $f \in M$ und B die beschreibende Matrix der Multiplikationsabbildung $\mu_f \colon M \to M$ bezüglich einer K-Basis von M. Zeige, dass bezüglich einer geeigneten K-Basis von L die Multiplikationsabbildung $\mu_f \colon L \to L$ durch eine Blockmatrix der Form

$$\begin{pmatrix} B & 0 & \ldots & 0 \\ 0 & B & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & B \end{pmatrix}$$

beschrieben wird.

Aufgabe 8.8. Bringe für die Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$ die Konzepte Norm und Spur mit dem Betrag und dem Realteil einer komplexen Zahl in Verbindung.

Aufgabe 8.9. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass die Norm einen Gruppenhomomorphismus

$$N \colon L^\times \longrightarrow K^\times,\ f \longmapsto N(f),$$

definiert.

Aufgabe 8.10. Berechne für das Element $2 + 4x + 5x^2$ in der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

die Norm und die Spur.

Aufgabe 8.11. Es sei $K \subseteq M \subseteq L$ eine Kette von quadratischen Körpererweiterungen. Zeige, dass für die Normen die Beziehung

$$N_K^L = N_K^M \circ N_M^L$$

gilt.

Aufgabe 8.12.*

Bestimme für sämtliche Elemente der Körpererweiterung

$$\mathbb{Z}/(2) \subseteq \mathbb{Z}/(2)[X]/\left(X^2 + X + 1\right)$$

die Multiplikationsmatrizen bezüglich der Basis $1, x$ sowie ihre Norm und ihre Spur.

Aufgabe 8.13. Sei $K \subseteq L$ eine endliche Körpererweiterung und sei $f \in L$ gegeben mit der zugehörigen Multiplikationsabbildung μ_f. Zeige, dass das charakteristische Polynom χ_{μ_f} ein Vielfaches des Minimalpolynoms zu f ist.

Aufgabe 8.14.*

Es sei $K \subseteq L$ eine endliche Körpererweiterung und $f \in L$. Zeige, dass es für die Eigenwerttheorie der K-linearen Multiplikationsabbildung

$$\mu_f \colon L \longrightarrow L$$

grundsätzlich nur zwei Möglichkeiten gibt.

Aufgabe 8.15. Sei K ein Körper und sei $P = X^n - c \in K[X]$ ein irreduzibles Polynom. Es sei

$$f = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0$$

ein Element in der einfachen endlichen Körpererweiterung

$$K \subseteq L = K[X]/(P)$$

vom Grad n. Zeige, dass die Spur von f gleich na_0 ist.

Aufgabe 8.16. Sei p eine Primzahl und sei

$$L = \mathbb{Q}[X]/\left(X^3 - p\right)$$

der durch das irreduzible Polynom $X^3 - p$ definierte Erweiterungskörper von $\mathbb{Q}$. Es sei

$$f = 2 + 3x - 4x^2 \, .$$

(1) Finde die Matrix bezüglich der $\mathbb{Q}$-Basis $1, x, x^2$ von L der durch die Multiplikation mit f definierten $\mathbb{Q}$-linearen Abbildung.
(2) Berechne die Norm und die Spur von f.
(3) Bestimme das Minimalpolynom von f.
(4) Finde das Inverse von f.
(5) Berechne die Diskriminante der Basis $1, f, f^2$.

Wir erinnern an einige Eigenschaften der Spur.

Aufgabe 8.17. Zeige, dass die Definition . der Spur einer linearen Abbildung unabhängig von der gewählten Matrix ist.

Aufgabe 8.18. Es sei K ein Körper und es sei A eine $m \times n$-Matrix und B eine $n \times m$-Matrix über K. Zeige

$$\operatorname{Spur}(A \circ B) = \operatorname{Spur}(B \circ A) \, .$$

Aufgabe 8.19. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K mit der Eigenschaft, dass das charakteristische Polynom in Linearfaktoren zerfällt, also

$$\chi_M = (X-\lambda_1)^{\mu_1} \cdot (X-\lambda_2)^{\mu_2} \cdots (X-\lambda_k)^{\mu_k}.$$

Zeige, dass

$$\operatorname{Spur}(M) = \sum_{i=1}^{k} \mu_i \lambda_i$$

ist.

Aufgabe 8.20. Es sei

$$M \in \operatorname{Mat}_n(K)$$

eine Matrix mit n (paarweise) verschiedenen Eigenwerten. Zeige, dass die Spur von M die Summe der Eigenwerte ist.

Aufgabe 8.21. Berechne die Diskriminante zur Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{i}]$$

zur Basis 1 und i und zur Basis $2-5\mathrm{i}$ und $4+7\mathrm{i}$.

Aufgabe 8.22.*

Sei K ein Körper der Charakteristik 0 und sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und sei $b_1, \ldots, b_n$ eine K-Basis von L. Zeige, dass dann

$$\triangle(b_1, \ldots, b_n) \neq 0.$$

8.2. **Aufgaben zum Abgeben.**

Aufgabe 8.23. (2 Punkte)

Erstelle die Multiplikationsmatrix zum Element $7x^2+3x-8$ in der kubischen Körpererweiterung

$$\mathbb{Q} = \mathbb{Q}[X]/\left(X^3+9X^2-2X+5\right).$$

Aufgabe 8.24. (3 Punkte)

Bestimme für sämtliche Elemente der Körpererweiterung

$$\mathbb{Z}/(3) \subseteq \mathbb{Z}/(3)[X]/\left(X^2-2\right)$$

die Multiplikationsmatrizen bezüglich der Basis $1, x$ sowie ihre Norm und ihre Spur.

Aufgabe 8.25. (6 Punkte)

Sei K ein Körper und sei p eine Primzahl. Es sei $a \in K$ ein Element, das in K keine p-te Wurzel besitzt. Zeige, dass das Polynom $X^p - a$ irreduzibel ist.

(Tipp: Betrachte die Norm zu einer geeigneten Körpererweiterung.)

Aufgabe 8.26. (4 Punkte)

Es sei $K \subseteq L$ eine Körpererweiterung, $f \in L$ und $M = K[f]$. Zeige, dass das charakteristische Polynom der Multiplikationsabbildung

$$\mu_f \colon L \longrightarrow L$$

eine Potenz des Minimalpolynoms von f ist.

Aufgabe 8.27. (3 Punkte)

Bestimme die Diskriminante zur Basis $1, x, x^2$ der kubischen Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 5X^2 + 6X - 3\right) =: L.$$

9. Vorlesung - Einheitengruppe

9.1. Endliche Untergruppen der Einheitengruppe eines Körpers.

Zu einer Primzahl p ist $\mathbb{Z}/(p)$ ein Körper mit p Elementen und somit besitzt die Einheitengruppe $\mathbb{Z}/(p)^\times$ genau $p-1$ Elemente. Nach dem Satz von Lagrange folgt daraus direkt $x^{p-1} = 1 \mod p$ für $x \neq 0 \mod p$. Daraus ergibt sich der sogenannte *Kleine Fermat*.

Satz 9.1. *Für eine Primzahl p und eine beliebige ganze Zahl a gilt*

$$a^p \equiv a \mod p\,.$$

Anders ausgedrückt: $a^p - a$ ist durch p teilbar.

Beweis. Ist a nicht durch p teilbar, so definiert a ein Element $\bar{a}$ in der Einheitengruppe $(\mathbb{Z}/(p))^\times$; diese Gruppe hat die Ordnung $p-1$, und nach dem Satz von Lagrange gilt $\bar{a}^{p-1} = 1$. Durch Multiplikation mit a ergibt sich die Behauptung. Für Vielfache von p gilt die Aussage ebenso, da dann beidseitig 0 steht. □

Wir wollen darüber hinaus zeigen, dass die Einheitengruppe von $\mathbb{Z}/(p)$, p Primzahl, zyklisch ist, also von einem Element erzeugt wird. Dafür brauchen wir einige gruppentheoretische Vorbereitungen.

Lemma 9.2. *Sei G eine kommutative Gruppe und $x, y \in G$ Elemente der endlichen Ordnungen $n = \operatorname{ord}(x)$ und $m = \operatorname{ord}(y)$, wobei n und m teilerfremd seien. Dann hat xy die Ordnung nm.*

Beweis. Sei $(xy)^k = 1$. Wir haben zu zeigen, dass k ein Vielfaches von nm ist. Es ist

$$1 = \left(x^k y^k\right)^n = x^{kn} y^{kn} = y^{kn},$$

da ja n die Ordnung von x ist. Aus dieser Gleichung erhält man, dass kn ein Vielfaches der Ordnung von y, also von m sein muss. Da n und m teilerfremd sind, folgt aus Lemma 3.17, dass k ein Vielfaches von m ist. Ebenso ergibt sich, dass k ein Vielfaches von n ist, so dass k, wieder aufgrund der Teilerfremdheit, ein Vielfaches von nm sein muss. □

Definition 9.3. Der *Exponent* $\exp(G)$ einer endlichen Gruppe G ist die kleinste positive Zahl n mit der Eigenschaft, dass $x^n = 1$ für alle $x \in G$ ist.

Lemma 9.4. *Sei G eine endliche kommutative Gruppe und sei $\exp(G) = \operatorname{ord}(G)$, wobei $\exp(G)$ den Exponenten der Gruppe bezeichnet. Dann ist G zyklisch.*

Beweis. Sei

$$n = \operatorname{ord}(G) = p_1^{r_1} \cdots p_k^{r_k}$$

die Primfaktorzerlegung der Gruppenordnung. Der Exponent der Gruppe ist

$$\exp(G) = \operatorname{kgV}(\operatorname{ord}(x) : x \in G).$$

Sei p_i ein Primteiler von n. Wegen

$$\exp(G) = \operatorname{ord}(G)$$

gibt es ein Element $x \in G$, dessen Ordnung ein Vielfaches von $p_i^{r_i}$ ist. Dann gibt es auch (in der von x erzeugten zyklischen Untergruppe) ein Element x_i der Ordnung $p_i^{r_i}$. Dann hat das Produkt $x_1 \cdots x_k \in G$ nach Lemma 9.2 die Ordnung n. □

Satz 9.5. *Sei $U \subseteq K^\times$ eine endliche Untergruppe der multiplikativen Gruppe eines Körpers K. Dann ist U zyklisch.*

Beweis. Sei $n = \operatorname{ord}(U)$ und $e = \exp(U)$ der Exponent dieser Gruppe. Dies bedeutet, dass alle Elemente $x \in U$ eine Nullstelle des Polynoms $X^e - 1$ sind. Nach Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) ist die Anzahl der Nullstellen aber maximal gleich dem Grad, so dass $n = e$ folgt. Nach Lemma 9.4 ist dann U zyklisch. □

Satz 9.6. *Es sei K ein endlicher Körper. Dann ist die Einheitengruppe $K^\times$ eine zyklische Gruppe.*

Beweis. Dies folgt direkt aus Satz 9.5. □

Satz 9.7. *Sei p eine Primzahl. Dann ist die Einheitengruppe $(\mathbb{Z}/(p))^\times$ zyklisch mit der Ordnung $p-1$. Es gibt also Elemente g mit der Eigenschaft, dass die Potenzen g^i, $i = 0, 1, \ldots, p-2$, alle Einheiten durchlaufen.*

Beweis. Dies folgt unmittelbar aus Satz 9.5, da $\mathbb{Z}/(p)$ ein endlicher Körper ist. □

Die endlichen Untergruppen von $\mathbb{R}^\times$ sind lediglich $\{1\}$ und $\{1,-1\}$. Dies gilt für jeden angeordneten Körper, da etwa aus $x > 1$ sofort folgt, dass die x^n eine unendliche Familie bilden. Bei $K = \mathbb{C}$ sind die endlichen Untergruppen von $\mathbb{C}^\times$ Untergruppen des komplexen Einheitskreises. Es handelt sich um die von einer primitiven komplexen Einheitswurzel erzeugten Gruppen.

Definition 9.8. Eine Einheit $u \in (\mathbb{Z}/(n))^\times$ heißt *primitiv* (oder eine *primitive Einheit*), wenn sie die Einheitengruppe erzeugt.

Beispiel 9.9. Wir betrachten die Einheitengruppe des Restklassenkörpers $\mathbb{Z}/(23)$. Nach Satz 9.7 ist sie zyklisch und es gibt daher Erzeuger der Einheitengruppe, also primitive Elemente. Wie kann man diese finden? Man ist hierbei prinzipiell auf Probieren angewiesen, man kann dies allerdings deutlich vereinfachen. Man weiß, dass die Einheitengruppe 22 Elemente besitzt, als Ordnung von Elementen dieser Gruppe kommen also nur $1, 2, 11$ und 22 in Frage. Es gibt genau ein Element mit der Ordnung 1, nämlich 1, und ein Element mit der Ordnung 2, nämlich $-1 = 22$. Alle anderen Elemente haben also die Ordnung 11 oder 22, und genau die letzteren sind primitiv. Der erste Kandidat ist 2. Wir müssen also

$$2^{11} \mod 23$$

ausrechnen. Es ist $2^5 = 32 = 9$ und daher ist

$$2^{11} = 9 \cdot 9 \cdot 2 = 12 \cdot 2 = 24 = 1.$$

Die Ordnung ist also 11, und die 2 ist nicht primitiv. Betrachten wir die 3. Es ist $3^3 = 27 = 4$ und daher ist

$$3^{11} = 4 \cdot 4 \cdot 4 \cdot 9 = 18 \cdot 9 = 162 = 1,$$

also wieder nicht primitiv. Der nächste Kandidat 4 muss nicht gecheckt werden, denn wegen $4 = 2^2$ ist sofort $4^{11} = 2^{22} = 1$ (diese Beobachtung gilt für alle Quadratzahlen, und zwar auch für diejenigen Zahlen, die nur modulo 23 ein Quadrat sind). Betrachten wir also 5. Es ist $5^2 = 2$. Damit ist

$$5^{11} = 2^5 \cdot 5 = 9 \cdot 5 = 45 = -1 \neq 1.$$

Daher hat 5 die Ordnung 22 und ist ein primitives Element.

Man kann diesen Sachverhalt auch so ausdrücken, dass die Abbildung

$$\mathbb{Z}/(22) \longrightarrow (\mathbb{Z}/(23))^\times, \, k \longmapsto 5^k,$$

einen Gruppenisomorphismus definiert. Dieser übersetzt die Addition in die Multiplikation, daher spricht man von einer *diskreten Exponentialfunktion* und nennt die Umkehrabbildung auch einen *diskreten Logarithmus*. Solche Abbildungen spielen eine wichtige Rolle in der *Kryptologie*. Wenn man wie in diesem Beispiel einen solchen Isomorphismus gefunden hat, so kann man viele Eigenschaften der Einheitengruppe in der „einfacheren“ Gruppe entscheiden.

Z.B. sind in $\mathbb{Z}/(22)$ alle ungeraden Elemente außer 11 ein Gruppenerzeuger, daher sind in der Einheitengruppe alle Elemente der Form

$$5^u, u \text{ ungerade}, u \neq 11,$$

primitiv.

9.2. **Primitive Einheitswurzeln.**

Die Menge der n-ten Einheitswurzeln in einem Körper K bilden eine endliche Untergruppe von $K^\times$, die wegen Satz 9.5 zyklisch ist.

Definition 9.10. Eine n-te Einheitswurzel heißt *primitiv*, wenn sie die Ordnung n besitzt.

Man beachte, dass ein Erzeuger der Gruppe der Einheitswurzeln nur dann primitiv heißt, wenn es n verschiedene Einheitswurzeln gibt. Wenn ζ eine primitive n-te Einheitswurzel ist, so sind genau die ζ^i mit $i < n$ und i teilerfremd zu n die primitiven Einheitswurzeln.[6]

9.3. **Endliche Körper.**

Definition 9.11. Ein Körper heißt *endlich*, wenn er nur endlich viele Elemente besitzt.

Über die Anzahl der Elemente in einem endlichen Körper gilt folgende wichtige Bedingung.

Lemma 9.12. *Sei K ein endlicher Körper. Dann besitzt K genau p^n Elemente, wobei p eine Primzahl ist und $n \geq 1$.*

Beweis. Der endliche Körper kann nicht die Charakteristik 0 besitzen, und als Charakteristik eines Körpers kommt ansonsten nach Satz Anhang 5.2 nur eine Primzahl in Frage. Diese sei mit p bezeichnet. Das bedeutet, dass K den Körper $\mathbb{Z}/(p)$ enthält. Damit ist aber K ein Vektorraum über $\mathbb{Z}/(p)$, und zwar, da K endlich ist, von endlicher Dimension. Sei n die Dimension, $n \geq 1$. Dann hat man eine $\mathbb{Z}/(p)$-Vektorraumisomorphie

$$K \cong (\mathbb{Z}/(p))^n$$

und somit besitzt K gerade p^n Elemente. □

Die vorstehende Aussage gilt allgemeiner für endliche Ringe, die einen Körper enthalten. Es sei schon jetzt erwähnt, dass es zu jeder Potenz p^n bis auf Isomorphie genau einen Körper mit p^n Elementen gibt. Dies werden wir in der übernächsten Vorlesung beweisen. Für einige Beispiele siehe auch die Aufgaben.

[6] Insbesondere gibt es, wenn es überhaupt primitive Einheitswurzeln gibt, genau $\varphi(n)$ primitive Einheitswurzeln, wobei $\varphi(n)$ die eulersche φ-Funktion bezeichnet. Siehe Vorlesung 19.

Beispiel 9.13. Wir konstruieren einen Körper mit $23^2 = 529$ Elementen und knüpfen dabei an Beispiel 9.9 an. Da die $5 \in \mathbb{Z}/(23)$ primitiv ist, folgt, dass das Polynom $X^2 - 5 \in \mathbb{Z}/(23)[X]$ irreduzibel ist. Andernfalls müsste es eine Nullstelle haben und dann wäre $5 = a^2$ ein Quadrat mit $a \in \mathbb{Z}/(23)$. Doch dann wäre $5^{11} = a^{22} = 1$, was nicht der Fall ist.

Es folgt nach Satz 7.6, dass

$$K = \mathbb{Z}/(23)[X]/(X^2 - 5)$$

ein Körper ist. Dieser hat 23^2 Elemente, da man jede Restklasse auf genau eine Weise als $ax + b$ mit $a, b \in \mathbb{Z}/(23)$ schreiben kann (x bezeichne die Restklasse von X). Dieser Körper enthält $\mathbb{Z}/(23)$, und die Ordnungen dieser Elemente ändern sich nicht (und sie sind insbesondere nicht primitiv im größeren Körper).

Wir möchten eine primitive Einheit in diesem Körper finden und orientieren uns an Lemma 9.2. Die Ordnung von $K^\times$ ist $528 = 16 \cdot 3 \cdot 11$. Wir müssen für jede dieser Primzahlpotenzen ein Element mit dieser Ordnung finden. Die 2 hat die Ordnung 11. Das Element $11 - x$ hat die Ordnung 3, es ist nämlich

$$(11-x)^3 = 121 \cdot 11 - 3 \cdot 121x + 33x^2 - x^3 = 66 - 3 \cdot 6x + 50 - 5x = 116 - 23x = 1.$$

Um ein Element der Ordnung 16 zu finden, ziehen wir sukzessive Quadratwurzeln aus -1. Es ist

$$(3x)^2 = 9x^2 = 45 = -1.$$

Eine Quadratwurzel aus $3x$ ist $14 + 19x$, wegen

$$(14 + 19x)^2 = 196 + 361 \cdot 5 + 2 \cdot 14 \cdot 19x = 12 + 16 \cdot 5 + 5 \cdot 19x = 3x.$$

Um eine Quadratwurzel für $14+19x$ zu finden, setzen wir $(a+bx)^2 = 14+19x$ an, was zum Gleichungssystem $a^2+5b^2 = 14$ und $2ab = 19$ über $\mathbb{Z}/(23)$ führt. Es ist dann $a = 21 \cdot b^{-1}$, was zu $4b^{-2} + 5b^2 = 14$ bzw. zur *biquadratischen Gleichung*

$$5b^4 + 9b^2 + 4 = 0$$

führt. Normieren ergibt $b^4 + 11b^2 + 10 = 0$. *Quadratisches Ergänzen* führt zu

$$(b^2 + 17)^2 = 17^2 - 10 = 49.$$

Daher ist $b^2 = 13$ und somit $b = 6$ und $a = 15$, also ist $15 + 6x$ ein Element der Ordnung 16. Damit ist insgesamt

$$2(11 - x)(15 + 6x) = 2(165 - 30 + 51x) = 2(20 + 5x) = 17 + 10x$$

eine primitive Einheit nach Lemma 9.2.

Satz 9.14. *Sei K ein endlicher Körper. Dann ist das Produkt aller von 0 verschiedener Elemente aus K gleich -1.*

Beweis. Die Gleichung $x^2 = 1$ hat in einem Körper nur die Lösungen 1 und -1, die allerdings gleich sein können. Das bedeutet, dass für $x \neq 1, -1$ immer $x \neq x^{-1}$ ist. Damit kann man das Produkt aller Einheiten als

$$1(-1)x_1x_1^{-1}\cdots x_kx_k^{-1}$$

schreiben. Ist $-1 \neq 1$, so ist das Produkt -1. Ist hingegen $-1 = 1$, so fehlt in dem Produkt der zweite Faktor und das Produkt ist $1 = -1$. □

Die folgende Aussage heißt *Satz von Wilson.*

Korollar 9.15. *Sei p eine Primzahl. Dann ist $(p-1)! = -1 \bmod p$.*

Beweis. Dies folgt unmittelbar aus Satz 9.14, da ja die Fakultät durch alle Zahlen zwischen 1 und $p-1$ läuft, also durch alle Einheiten im Restklassenkörper $\mathbb{Z}/(p)$. □

9. Arbeitsblatt

9.1. **Aufwärmaufgaben.**

Aufgabe 9.1. Finde primitive Einheiten in den Restklassenkörpern $\mathbb{Z}/(2)$, $\mathbb{Z}/(3)$, $\mathbb{Z}/(5)$, $\mathbb{Z}/(7)$ und $\mathbb{Z}/(11)$.

Aufgabe 9.2.*

Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(13)$.

Aufgabe 9.3.*

Wie viele Quadrate und wie viele primitive Elemente besitzt $\mathbb{Z}/(31)$?

Wie viele Elemente besitzt $\mathbb{Z}/(31)$, die weder primitiv noch ein Quadrat sind?

Sei x ein primitives Element von $\mathbb{Z}/(31)$. Liste explizit alle Elemente x^i auf, die weder primitiv noch ein Quadrat sind.

Aufgabe 9.4. Sei $K = \mathbb{Z}/(59)$ der Körper mit 59 Elementen.

a) Bestimme die Anzahl der primitiven Elemente in K.

b) Berechne in K die Zweierpotenzen 2^4, 2^8 und 2^{16}.

c) Berechne 2^{29} in K.

d) Man gebe für jede mögliche (multiplikative) Ordnung in $K^\times$ ein Element an, das diese Ordnung besitzt.

Aufgabe 9.5. Sei p eine ungerade Primzahl und $\mathbb{Z}/(p)$ der zugehörige Restklassenkörper. Zeige, dass das Produkt von zwei primitiven Einheiten niemals primitiv ist.

Aufgabe 9.6. Bestimme die Einheiten von $\mathbb{Z}/(8)$.

Aufgabe 9.7. Konstruiere einen Körper $\mathbb{F}_9$ mit 9 Elementen.

Aufgabe 9.8.*

Sei p eine Primzahl und $x \in (\mathbb{Z}/(p))^\times$ eine Einheit. Es sei a die Ordnung von x in der additiven Gruppe $(\mathbb{Z}/(p), +, 0)$ und es sei b die Ordnung von x in der multiplikativen Gruppe $((\mathbb{Z}/(p))^\times, \cdot, 1)$. Zeige, dass a und b teilerfremd sind.

Aufgabe 9.9.*

Bestimme in der Einheitengruppe $\mathbb{Z}/(17)^\times$ zu jeder möglichen Ordnung k ein Element $x \in \mathbb{Z}/(17)^\times$, das die Ordnung k besitzt. Man gebe auch eine Untergruppe

$$H \subseteq \mathbb{Z}/(17)^\times$$

an, die aus vier Elementen besteht.

Aufgabe 9.10.*

Beschreibe den Körper mit neun Elementen $\mathbb{F}_9$ als einen Restklassenkörper von $\mathbb{Z}/(3)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_9$ an.

Aufgabe 9.11. Bestimme in $\mathbb{F}_9$ für jedes Element die multiplikative Ordnung. Man gebe insbesondere die primitiven Einheiten an.

Aufgabe 9.12. Wie viele primitive Elemente besitzt der Körper mit 529 Elementen?

Aufgabe 9.13.*

Es sei $\mathbb{Z}/(p) \subseteq \mathbb{F}_q$ eine Erweiterung endlicher Körper mit $q = p^e$ und es sei u eine primitive Einheitswurzel von $\mathbb{F}_q$. Was ist die erste Potenz u^n, $n \geq 1$, die zu $\mathbb{Z}/(p)$ gehört? Ist dieses u^n ein primitives Element von $(\mathbb{Z}/(p))^\times$?

Aufgabe 9.14. Es sei p eine Primzahl und F ein Körper mit p^2 Elementen. Welche Ringhomomorphismen zwischen $\mathbb{Z}/(p^2)$ und F gibt es? Man betrachte beide Richtungen.

Aufgabe 9.15. a) Sei K ein Körper. Zeige, dass die Einheitengruppe von K nicht zyklisch unendlich ist.

b) Sei R ein kommutativer Ring, dessen Charakteristik nicht zwei ist. Zeige, dass die Einheitengruppe von R nicht zyklisch unendlich ist.

c) Beschreibe einen kommutativen Ring, dessen Einheitengruppe zyklisch unendlich ist.

Aufgabe 9.16. Bestimme den Rest von 44! modulo 47.

Aufgabe 9.17. Bestimme die Zerlegung von $X^{p-1} - 1$ in irreduzible Polynome im Polynomring $\mathbb{Z}/(p)[X]$. Beweise aus dieser Zerlegung den Satz von Wilson.

Aufgabe 9.18.*

Sei p eine Primzahl. Man gebe einen Körper der Charakteristik p an, der unendlich viele Elemente besitzt.

Aufgabe 9.19.*

Zeige, dass die Matrizen

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

eine kommutative Gruppe bilden, in der jedes Element zu sich selbst invers ist.

Zeige insbesondere, dass die Gruppe in der vorstehenden Aufgabe nicht zyklisch ist.

9.2. **Aufgaben zum Abgeben.**

Aufgabe 9.20. (3 Punkte)

Finde primitive Einheiten in den Restklassenkörpern $\mathbb{Z}/(13)$, $\mathbb{Z}/(17)$ und $\mathbb{Z}/(19)$.

Aufgabe 9.21. (5 Punkte)

Konstruiere zu einer Primzahl p einen Körper mit p^2 Elementen.

Aufgabe 9.22. (4 Punkte)

Konstruiere endliche Körper mit $4, 8, 9, 16, 25, 27, 32$ und 49 Elementen.

Aufgabe 9.23. (4 Punkte)

Es sei $\mathbb{F}_9 = \mathbb{Z}/(3)[Z]/(Z^2+1)$ der Körper mit 9 Elementen (z bezeichne die Restklasse von Z). Führe in $\mathbb{F}_9[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = X^4 + (1+2z)X^3 + zX^2 + 2X + 2 + z$ und $T = (z+1)X^2 + zX + 2$ durch.

Aufgabe 9.24. (4 Punkte)

Finde einen Erzeuger der Einheitengruppe eines Körpers mit 25 Elementen. Wie viele solche Erzeuger gibt es?

10. Vorlesung - Algebraischer Abschluss

10.1. Erzeugte Algebra und erzeugter Körper.

Satz 10.1. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann ist die von f erzeugte K-Algebra $K[f] \subseteq L$ ein Körper.*

Beweis. Nach Satz 7.11 liegt eine K-Algebraisomorphie $K[X]/(P) \cong K[f]$ vor, wobei P das Minimalpolynom zu f ist. Nach Lemma 7.12 (2) ist P irreduzibel, so dass wegen Korollar 7.7 der Restklassenring $K[f]$ ein Körper ist. □

Korollar 10.2. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann stimmen die von f über K erzeugte Unteralgebra und der von f über K erzeugte Unterkörper überein. Es gilt also $K[f] = K(f)$.*

Beweis. Die Inklusion $K[f] \subseteq K(f)$ gilt immer, und nach Voraussetzung ist der Unterring $K[f]$ aufgrund von Satz 10.1 schon ein Körper. □

Bemerkung 10.3. Sei K ein Körper, $P \in K[X]$ ein irreduzibles Polynom und $K \subseteq L = K[X]/(P)$ die zugehörige Körpererweiterung. Dann kann man zu $z = F(x)$, $z \neq 0$, (mit $F \in K[X]$, $x = \overline{X}$) auf folgende Art das Inverse z^{-1} bestimmen. Es sind P und F teilerfremde Polynome in $K[X]$ und daher gibt es nach Satz 3.15 und Lemma 3.16 eine Darstellung der 1, die man mit Hilfe des euklidischen Algorithmus finden kann. Wenn $RF+SP = 1$ ist, so ist die Restklasse von R, also $\overline{R} = R(x)$, das Inverse zu $\overline{F} = z$.

10.2. **Charakterisierung von algebraischen Elementen.**

Satz 10.4. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein Element. Dann sind folgende Aussagen äquivalent.*

(1) *f ist algebraisch über K.*
(2) *Es gibt ein normiertes Polynom $P \in K[X]$ mit $P(f) = 0$.*
(3) *Es besteht eine lineare Abhängigkeit zwischen den Potenzen*

$$f^0 = 1, f^1 = f, f^2, f^3, \ldots .$$

(4) *Die von f über K erzeugte K-Algebra $K[f]$ hat endliche K-Dimension.*
(5) *f liegt in einer endlichdimensionalen K-Algebra $M \subseteq L$.*

Beweis. (1) $\Rightarrow$ (2). Das ist trivial, da man ein von 0 verschiedenes Polynom stets normieren kann, indem man durch den Leitkoeffizienten dividiert. (2) $\Rightarrow$ (3). Nach (2) gibt es ein Polynom $P \in K[X]$, $P \neq 0$, mit $P(f) = 0$. Sei $P = \sum_{i=0}^{n} c_i X^i$. Dann ist

$$P(f) = \sum_{i=0}^{n} c_i f^i = 0$$

eine lineare Abhängigkeit zwischen den Potenzen. (3) $\Rightarrow$ (1). Umgekehrt bedeutet die lineare Abhängigkeit, dass es Elemente c_i gibt, die nicht alle 0 sind mit $\sum_{i=0}^{n} c_i f^i = 0$. Dies ist aber die Einsetzung $P(f)$ für das Polynom $P = \sum_{i=0}^{n} c_i X^i$, und dieses ist nicht das Nullpolynom. (2) $\Rightarrow$ (4). Sei

$$P = \sum_{i=0}^{n} c_i X^i$$

ein normiertes Polynom mit $P(f) = 0$, also mit

$$c_n = 1.$$

Dann kann man umstellen

$$f^n = -\sum_{i=0}^{n-1} c_i f^i$$

D.h. f^n kann man durch kleinere Potenzen ausdrücken. Durch Multiplikation dieser Gleichung mit weiteren Potenzen von f ergibt sich, dass man auch die höheren Potenzen durch die Potenzen f^i, $i \leq n-1$, ausdrücken kann. (4) $\Rightarrow$ (5). Das ist trivial. (5) $\Rightarrow$ (3). Wenn f in einer endlichdimensionalen Algebra $M \subseteq L$ liegt, so liegen darin auch alle Potenzen von f. Da es in einem endlichdimensionalen Vektorraum keine unendliche Folge von linear unabhängigen Elementen geben kann, müssen diese Potenzen linear abhängig sein. $\square$

Mit dieser Charakterisierung können wir noch einen zweiten Beweis von Satz 10.1 geben, der unabhängig von der Restklassenbildung ist und der zugleich zeigt, wie man aus dem Minimalpolynom eines algebraischen Elementes das inverse Element beschreiben kann.

Nach Satz 10.4 ist $M = K[f]$ eine endlichdimensionale K-Algebra. Wir müssen zeigen, dass M ein Körper ist. Sei dazu $g \in M$ ein von 0 verschiedenes Element. Damit ist auch $K[g] \subseteq M = K[f]$, so dass $K[g]$ wieder eine endlichdimensionale Algebra ist. Daher ist, wiederum nach Satz 10.4, das Element g algebraisch über K und es gibt ein Polynom $P \in K[X]$, $P \neq 0$, mit $P(g) = 0$. Wir ziehen aus diesem Polynom die höchste Potenz von X heraus und schreiben $P = QX^k$, wobei der konstante Term von Q von 0 verschieden sei. Die Ersetzung von X durch g ergibt

$$0 = P(g) = Q(g)g^k.$$

Da $g \neq 0$ ist und sich alles im Körper L abspielt, folgt $Q(g) = 0$. Wir können durch den konstanten Term von Q dividieren und erhalten die Gleichung

$$1 + c_1 g + \cdots + c_d g^d = 0.$$

Umstellen ergibt

$$g\left(-c_1 g^0 - \cdots - c_d g^{d-1}\right) = 1.$$

Das heißt, dass das Inverse zu g sich als Polynom in g schreiben lässt und daher zu $K[g]$ und erst recht zu $K[f]$ gehört.

10.3. **Algebraischer Abschluss.**

Definition 10.5. Sei $K \subseteq L$ eine Körpererweiterung. Dann nennt man die Menge

$$M = \{x \in L | \, x \text{ ist algebraisch über } K\}$$

den *algebraischen Abschluss* von K in L.

Satz 10.6. *Sei $K \subseteq L$ eine Körpererweiterung und sei M der algebraische Abschluss von K in L. Dann ist M ein Unterkörper von L.*

Beweis. Wir müssen zeigen, dass M bezüglich der Addition, der Multiplikation, des Negativen und des Inversen abgeschlossen ist. Seien $x, y \in M$. Wir betrachten die von x und y erzeugte K-Unteralgebra $U = K[x, y]$, die aus allen K-Linearkombinationen der $x^i y^j$, $i, j \in \mathbb{N}$, besteht. Da sowohl x als auch y algebraisch sind, kann man nach Satz 10.4 gewisse Potenzen x^n und y^m durch kleinere Potenzen ersetzen. Daher kann man alle Linearkombinationen mit den Monomen $x^i y^j$, $i < n$, $j < m$, ausdrücken. D.h. alle Operationen spielen sich in dieser endlichdimensionalen Unteralgebra ab. Daher sind Summe, Produkt und das Negative nach Satz 10.4 wieder algebraisch. Für das Inverse sei $z \neq 0$ algebraisch. Dann ist $K[z]$ nach Satz 10.1 ein Körper von endlicher Dimension. Daher ist $z^{-1} \in K[z]$ selbst algebraisch. □

10.4. **Algebraische Zahlen.**

Die über den rationalen Zahlen $\mathbb{Q}$ algebraischen komplexen Zahlen erhalten einen speziellen Namen.

Definition 10.7. Eine komplexe Zahl z heißt *algebraisch* oder *algebraische Zahl*, wenn sie algebraisch über den rationalen Zahlen $\mathbb{Q}$ ist. Andernfalls heißt sie *transzendent*.

Die Menge der algebraischen Zahlen wird mit $\mathbb{A}$ bezeichnet.

Ferdinand von Lindemann (1852-1939)

Bemerkung 10.8. Eine komplexe Zahl $z \in \mathbb{C}$ ist genau dann algebraisch, wenn es ein von 0 verschiedenes Polynom P mit rationalen Koeffizienten und mit $P(z) = 0$ gibt. Durch Multiplikation mit einem Hauptnenner kann man für eine algebraische Zahl auch ein annullierendes Polynom mit ganzzahligen Koeffizienten finden (das allerdings nicht mehr normiert ist). Eine rationale Zahl q ist trivialerweise algebraisch, da sie Nullstelle des linearen rationalen Polynoms $X - q$ ist. Weiterhin sind die reellen Zahlen $\sqrt{q}$ und $q^{1/n}$ für $q \in \mathbb{Q}$ algebraisch. Dagegen sind die Zahlen e und π nicht algebraisch. Diese Aussagen sind keineswegs selbstverständlich, die Transzendenz von π wurde beispielsweise von Ferdinand von Lindemann 1882 gezeigt.

10.5. **Algebraautomorphismen.**

Wir beginnen nun mit der eigentlichen Galoistheorie. Die folgenden Definitionen werden wir vor allem für eine Körpererweiterung $K \subseteq L$ anwenden.

Definition 10.9. Es sei K ein kommutativer Ring und A eine kommutative K-Algebra. Ein bijektiver K-Algebrahomomorphismus

$$\varphi\colon\ A \longrightarrow A$$

heißt K- *Algebraautomorphismus* .

Lemma 10.10. *Es sei K ein kommutativer Ring und A eine kommutative K-Algebra. Dann gelten folgende Aussagen.*

(1) *Die Identität ist ein K-Algebraautomorphismus.*
(2) *Die Verknüpfung $\varphi \circ \psi$ von zwei K-Algebraautomorphismen φ und ψ ist wieder ein Automorphismus.*
(3) *Die Umkehrabbildung φ^{-1} zu einem K-Algebraautomorphismus φ ist wieder ein Automorphismus.*
(4) *Die Menge der K-Algebraautomorphismen bilden mit der Hintereinanderschaltung als Verknüpfung eine Gruppe.*

Beweis. Siehe Aufgabe 10.6. □

Definition 10.11. Es sei K ein kommutativer Ring und A eine kommutative K-Algebra. Die Menge der K-Algebra-Automorphismen

$$\varphi \colon A \longrightarrow A$$

mit der Hintereinanderschaltung als Verknüpfung heißt *Automorphismengruppe* der Algebra. Sie wird mit $\mathrm{Aut}_K(A)$ bezeichnet.

Beispiel 10.12. Es sei K ein Körper und $K[X_1, \ldots, X_n]$ der Polynomring über K in n Variablen. Es sei

$$\alpha \colon K^n \longrightarrow K^n$$

ein linearer Automorphismus, der durch eine invertierbare Matrix

$$\alpha = (a_{ij})_{1 \leq i,j \leq n}$$

gegeben ist. Wir definieren dazu direkt einen K-Algebraautomorphismus, nämlich den durch

$$X_i \longmapsto a_{i1}X_1 + \cdots + a_{in}X_n$$

definierten Einsetzungshomomorphismus (in mehreren Variablen), den wir mit φ_α bezeichnen. Dabei handelt es sich in der Tat um einen Algebraautomorphismus: Der inverse lineare Automorphismus α^{-1} definiert in der gleichen Weise einen Algebrahomomorphismus $\varphi_{\alpha^{-1}}$, und es gilt $\varphi_{\alpha^{-1}} \circ \varphi_\alpha = \mathrm{Id}$, da diese Hintereinanderschaltung jede Variable auf sich selbst abbildet.

Bei einem Polynomring in einer Variablen über einem Körper K ist jeder K-Automorphismus ein linearer Automorphismus, also durch die Zuordnung $X \mapsto aX$ mit $a \neq 0$ gegeben. Dies ist in mehreren Variablen nicht der Fall, in der Tat ist schon die Automorphismengruppe von $K[X, Y]$ nicht vollständig verstanden. Ein wichtiges offenes Problem ist hierbei das Jacobiproblem.

10.6. **Die Galoisgruppe einer Körpererweiterung.**

Definition 10.13. Sei $K \subseteq L$ eine Körpererweiterung. Dann nennt man die Automorphismengruppe

$$\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L)$$

die *Galoisgruppe* der Körpererweiterung.

Lemma 10.14. *Sei $K \subseteq L$ eine Körpererweiterung und es sei $x_i \in L$, $i \in I$, ein Erzeugendensystem (als Körper) von L über K. Es sei $\varphi \in \mathrm{Gal}\,(L|K)$ mit $\varphi(x_i) = x_i$ für alle $i \in I$. Dann ist $\varphi = \mathrm{Id}$.*

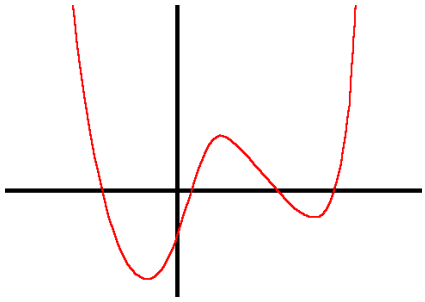
Beweis. Wir zeigen, dass die Teilmenge

$$M = \{x \in L | \, \varphi(x) = x\}$$

gleich L ist. Da φ ein K-Algebrahomomorphismus ist, ist $K \subseteq M$ und nach Voraussetzung ist $x_i \in M$. Mit $x, y \in M$ ist wegen $\varphi(x+y) = \varphi(x)+\varphi(y) = x+y$ (und entsprechend für die Multiplikation) auch $x+y, xy \in M$. Ferner ist mit $x \in M$, $x \neq 0$, wegen

$$\varphi\left(x^{-1}\right) = (\varphi(x))^{-1} = x^{-1}$$

auch $x^{-1} \in M$. Also ist M ein Unterkörper, der K und das Körpererzeugendensystem x_i umfasst und daher ist $M = L$. □



Unter einem K-Körperautomorphismus φ muss ein Element $x \in L$, dass Nullstelle eines Polynoms F aus $K[X]$ ist, auf eine Nullstelle dieses Polynoms abgebildet werden. Das schränkt die Möglichkeiten wesentlich ein.

Es ist eine grundlegende Frage, welche Eigenschaften eines Elementes $x \in L$ unter einem K-Algebraautomorphismus erhalten bleiben und welche nicht.

Lemma 10.15. *Sei $K \subseteq L$ eine Körpererweiterung, $x \in L$, $F \in K[X]$ ein Polynom mit $F(x) = 0$ und sei $\varphi \in \mathrm{Gal}\,(L|K)$. Dann ist auch $F(\varphi(x)) = 0$.*

Beweis. Sei $F = a_0 + a_1X + \cdots + a_nX^n$ mit $a_i \in K$. Dann ist

$$F(\varphi(x)) = a_0 + a_1\varphi(x) + \cdots + a_n(\varphi(x))^n = \varphi(F(x)) = \varphi(0) = 0.$$

□

Satz 10.16. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist die Galoisgruppe $\mathrm{Gal}\,(L|K)$ endlich.*

Beweis. Die Körpererweiterung besitzt ein endliches K-Algebraerzeugendensystem, also $L = K[x_1, \ldots, x_n]$. Nach Lemma 10.14 ist ein K-Algebraautomorphismus

$$\varphi\colon L \longrightarrow L$$

durch $\varphi(x_i)$, $i = 1, \ldots, n$, eindeutig festgelegt. Da jedes x_i nach Satz 10.4 algebraisch ist, gibt es Polynome

$$F_i \neq 0$$

mit $F_i(x_i) = 0$. Nach Lemma 10.15 ist auch $F_i(\varphi(x_i)) = 0$. Die Polynome F_i besitzen aber nach Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) jeweils nur endlich viele Nullstellen, so dass nur endlich viele Werte für $\varphi(x_i)$ in Frage kommen. □

10. Arbeitsblatt

10.1. **Aufwärmaufgaben.**

Aufgabe 10.1. Es sei $R = \mathbb{Z}[\frac{2}{3}]$ der von $\mathbb{Z}$ und $2/3$ erzeugte Unterring von $\mathbb{Q}$. Zeige, dass R alle rationalen Zahlen enthält, die sich mit einer Potenz von 3 im Nenner schreiben lassen.

Aufgabe 10.2. Zeige, dass die Menge der algebraischen Zahlen $\mathbb{A}$ keine endliche Körpererweiterung von $\mathbb{Q}$ ist.

Aufgabe 10.3. Zeige, dass es nur abzählbar viele algebraische Zahlen gibt.

Aufgabe 10.4.*

Es seien $K \subseteq L$ und $L \subseteq M$ algebraische Körpererweiterungen. Zeige, dass dann auch $K \subseteq M$ eine algebraische Körpererweiterung ist.

Aufgabe 10.5. Es sei K ein Körper. Zeige, dass es außer K keine endliche K-Unteralgebra $A \subseteq K[X]$ gibt.

Aufgabe 10.6. Es sei K ein kommutativer Ring und A eine kommutative K-Algebra. Beweise die folgenden Aussagen.

(1) Die Identität ist ein K-Algebraautomorphismus.
(2) Die Verknüpfung $\varphi \circ \psi$ von zwei K-Algebraautomorphismen φ und ψ ist wieder ein Automorphismus.
(3) Die Umkehrabbildung φ^{-1} zu einem K-Algebraautomorphismus φ ist wieder ein Automorphismus.

(4) Die Menge der K-Algebraautomorphismen bilden mit der Hintereinanderschaltung als Verknüpfung eine Gruppe.

Aufgabe 10.7. Es sei K ein Körper der Charakteristik $\neq 2$ und sei $K \subseteq L$ eine quadratische Körpererweiterung. Zeige, dass es neben der Identität einen weiteren K-Algebraautomorphismus $L \to L$ gibt.

Aufgabe 10.8. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass ein Polynom $P \in K[X]$ genau dann irreduzibel ist, wenn das um $a \in K$ „verschobene" Polynom (das entsteht, wenn man in P die Variable X durch $X - a$ ersetzt) irreduzibel ist.

Aufgabe 10.9.*

Sei $x = \sqrt{2} + \sqrt{5} \in \mathbb{R}$ und betrachte die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(x) = L\,.$$

Zeige, dass diese Körpererweiterung algebraisch ist und bestimme den Grad der Körpererweiterung, das Minimalpolynom von x und das Inverse von x. (Man darf dabei verwenden, dass $\sqrt{2}, \sqrt{5}, \sqrt{10}$ irrationale Zahlen sind.)

Aufgabe 10.10.*

Es sei p eine Primzahl.

a) Bestimme den Grad der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{p}].$$

Man gebe auch eine $\mathbb{Q}$-Basis von $\mathbb{Q}[\sqrt[3]{p}]$ an.

b) Zeige, dass in $\mathbb{Q}[\sqrt[3]{p}]$ alle Elemente der Form m^3p und n^3p^2 mit $m, n \in \mathbb{Q}$ eine dritte Wurzel besitzen.

c) Die rationale Zahl $x \in \mathbb{Q}$ besitze in $\mathbb{Q}[\sqrt[3]{p}]$ eine dritte Wurzel. Zeige, dass x die Form

$$x = k^3 \text{ oder } x = m^3p \text{ oder } x = n^3p^2$$

mit $k, m, n \in \mathbb{Q}$ besitzt.

d) Es sei nun q eine weitere, von p verschiedene Primzahl. Bestimme den Grad der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{p}, \sqrt[3]{q}].$$

Aufgabe 10.11.*

Es sei K ein Körper und seien $K \subseteq L_1$ und $K \subseteq L_2$ endliche Körpererweiterungen. Zeige, dass es eine endliche Körpererweiterung $K \subseteq M$ gibt, die sowohl L_1 als auch L_2 als Zwischenkörper enthält.

Aufgabe 10.12. Sei $K \subseteq L$ eine Körpererweiterung und es sei $x_i \in L$, $i \in I$, ein Körper-Erzeugendensystem (als Körper) von L über K. Es seien $\varphi, \psi \in \mathrm{Gal}\,(L|K)$ mit $\varphi(x_i) = \psi(x_i)$ für alle $i \in I$. Zeige, dass $\varphi = \psi$ ist.

Aufgabe 10.13.*

Es sei $z = a + b\mathrm{i} \in \mathbb{C}$, $a, b \in \mathbb{R}$, eine algebraische Zahl. Zeige, dass auch die konjugiert-komplexe Zahl $\overline{z} = a - b\mathrm{i}$ sowie der Real- und der Imaginärteil von z algebraisch sind. Man bestimme den Grad der Körpererweiterung

$$\mathbb{A} \cap \mathbb{R} \subseteq \mathbb{A}\,.$$

Aufgabe 10.14.*

Es sei $\epsilon = \frac{-1+\sqrt{3}\mathrm{i}}{2}$ die dritte komplexe Einheitswurzel. Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\epsilon\sqrt[3]{7}] = L \subseteq \mathbb{C}.$$

(1) Bestimme das Minimalpolynom von $\epsilon\sqrt[3]{7}$.
(2) Zeige, dass der Grad der Körpererweiterung $\mathbb{Q} \subseteq L$ gleich 3 ist.
(3) Zeige, dass die komplexe Konjugation nicht L in L überführt.

10.2. **Aufgaben zum Abgeben.**

Aufgabe 10.15. (3 Punkte)

Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein Element. Zeige: f ist genau dann algebraisch über K, wenn $K[f] = K(f)$ ist.

Aufgabe 10.16. (3 Punkte)

Bestimme das Inverse von $2x^2+3x-1$ im Körper $\mathbb{Q}[X]/(X^3-5)$ (x bezeichnet die Restklasse von X).

Aufgabe 10.17. (4 Punkte)

Sei $K \subseteq L$ eine Körpererweiterung, wobei L algebraisch abgeschlossen sei. Zeige, dass auch der algebraische Abschluss $\overline{K}$ von K in L algebraisch abgeschlossen ist.[7]

[7]Die Bezeichnungen wären natürlich schlecht gewählt, wenn dies nicht gelten würde.

Aufgabe 10.18. (3 Punkte)

Es sei K ein Körper und sei $K[X,Y]$ der Polynomring über K in zwei Variablen. Sei $P \in K[X]$ ein Polynom in der einen Variablen X. Zeige, dass durch die Einsetzung $X \mapsto X$ und $Y \mapsto Y + P(X)$ ein K-Algebraautomorphismus von $K[X,Y]$ in sich definiert wird, der im Allgemeinen nicht linear ist.

Aufgabe 10.19. (5 Punkte)

Sei K ein Körper und sei $L = K(X)$ der rationale Funktionenkörper über K. Zeige, dass es zu jedem $n \in \mathbb{N}_+$ einen Ringhomomorphismus $\varphi\colon L \to L$ derart gibt, dass $L \cong \varphi(L) \subseteq L$ eine endliche Körpererweiterung vom Grad n ist.

11. Vorlesung - Zerfällungskörper

11.1. **Zerfällungskörper.**

Wir wollen zu einem Polynom $F \in K[X]$ einen Körper konstruieren, über dem F in Linearfaktoren zerfällt. Dies beruht auf einer recht einfachen Konstruktion. Zu jedem Körper kann man sogar einen Körper $K \subseteq \overline{K}$ konstruieren, der algebraisch abgeschlossen ist, was wir aber nicht ausführen werden. Eine erste Anwendung ist die Konstruktion und die Charakterisierung von endlichen Körpern.

Lemma 11.1. *Sei K ein Körper und F ein Polynom aus $K[X]$. Dann gibt es einen Erweiterungskörper $K \subseteq L$ derart, dass F über L in Linearfaktoren zerfällt.*

Beweis. Sei $F = P_1 \cdots P_r$ die Zerlegung in Primpolynome in $K[X]$, und sei P_1 nicht linear. Dann ist

$$K \longrightarrow K[Y]/(P_1(Y)) =: K'$$

eine Körpererweiterung von K nach Satz 7.6. Wegen $P_1(Y) = 0$ in K' ist die Restklasse y von Y in K' eine Nullstelle von P_1. Daher gilt in $K'[X]$ die Faktorisierung $P_1 = (X - y)\tilde{P}$, wobei $\tilde{P}$ einen kleineren Grad als P_1 hat. Das Polynom F hat also über K' mindestens einen Linearfaktor mehr als über K. Induktive Anwendung von dieser Konstruktion liefert eine Kette von Erweiterungen $K \subset K' \subset K'' \subset \ldots$, die stationär wird, sobald F in Linearfaktoren zerfällt. □

Wenn F quadratisch ist, so ist man nach einer einzigen Körpererweiterung fertig, da aus der Existenz einer Nullstelle direkt folgt, dass das Polynom in Linearfaktoren zerfällt. Aber schon ab Grad 3 ist es eher eine Ausnahme, dass über $K[X]/(F)$ das Polynom bereits in Linearfaktoren zerfällt, und dann muss man wie im Lemma beschrieben induktiv weitermachen.

Beispiel 11.2. Das Polynom $X^3 - 3X + 1 \in \mathbb{Q}[X]$ ist irreduzibel nach Aufgabe 3.16 und definiert daher eine Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

vom Grad 3. Die Restklasse von X in L sei mit α bezeichnet. Es gilt also

$$\alpha^3 - 3\alpha + 1 = 0.$$

Nach Aufgabe 11.7 sind auch die Elemente aus L

$$\beta = \alpha^2 - 2$$

und

$$\gamma = -\alpha^2 - \alpha + 2$$

Nullstellen der definierenden Gleichung und daher zerfällt das Polynom bereits über L. Der Zerfällungskörper des Polynoms $X^3 - 3X + 1$ ist also L.

Definition 11.3. Es sei K ein Körper, $F \in K[X]$ ein Polynom und $K \subseteq L$ eine Körpererweiterung, über der F in Linearfaktoren zerfällt. Es seien $a_1, \ldots, a_n \in L$ die Nullstellen von F. Dann nennt man

$$K[a_1, \ldots, a_n] \subseteq L$$

einen *Zerfällungskörper* von F.[8]

Es handelt sich hierbei wirklich um einen Körper, wie wir gleich sehen werden. Häufig beschränkt man sich auf Polynome vom Grad ≥ 1, bei konstanten Polynomen sehen wir einfach K selbst als Zerfällungskörper an. Über dem Zerfällungskörper zerfällt das gegebene Polynom in Linearfaktoren, da er ja nach Definition alle Nullstellen enthält, mit denen alle beteiligten Linearfaktoren formuliert werden können.

Lemma 11.4. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von F. Es sei $K \subseteq K' \subseteq L$ ein Zwischenkörper. Dann ist L auch ein Zerfällungskörper des Polynoms $F \in K'[X]$.*

Beweis. Das ist trivial. □

Lemma 11.5. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von F. Dann ist $K \subseteq L$ eine endliche Körpererweiterung.*

Beweis. Es sei $K \subseteq M$ eine Körpererweiterung, über der F in Linearformen zerfällt und $L = K[a_1, \ldots, a_n] \subseteq M$, wobei $a_i \in M$ die Nullstellen von F seien. Es liegt eine Kette von K-Algebren

$$K \subseteq K[a_1] \subseteq K[a_1, a_2] \subseteq \cdots \subseteq K[a_1, \ldots, a_n] = L \subseteq M$$

[8]Der Sprachgebrauch ist nicht ganz einheitlich. Manche Autoren nennen jeden Körper, über dem das gegebene Polynom in Linearfaktoren zerfällt, einen Zerfällungskörper, und bezeichnen den von den Nullstellen erzeugten Zerfällungskörper als minimalen Zerfällungskörper.

vor. Dabei ist sukzessive a_i algebraisch über $K[a_1, \ldots, a_{i-1}]$, da ja a_i eine Nullstelle von $F \in K[X]$ ist. Daher sind die Inklusionen nach Satz 10.1 endliche Körpererweiterungen und nach Satz 2.8 ist dann die Gesamtkörpererweiterung ebenfalls endlich. □

Satz 11.6. *Es sei K ein Körper und sei $F \in K[X]$ ein Polynom. Es seien $K \subseteq L_1$ und $K \subseteq L_2$ zwei Zerfällungskörper von F. Dann gibt es einen K-Algebraisomorphismus*

$$\varphi\colon\ L_1 \longrightarrow L_2.$$

Insbesondere gibt es bis auf Isomorphie nur einen Zerfällungskörper zu einem Polynom.

Beweis. Wir beweisen die Aussage durch Induktion über den Grad $\operatorname{grad}_K L_1$. Wenn der Grad eins ist, so ist $K = L_1$ und das Polynom F zerfällt bereits über K in Linearfaktoren. Dann gehören alle Nullstellen von F in einem beliebigen Erweiterungskörper $K \subseteq M$ zu K selbst. Also ist auch $L_2 = K$. Es sei nun $\operatorname{grad}_K L_1 \geq 2$ und die Aussage sei für kleinere Grade bewiesen. Dann zerfällt F über K nicht in Linearfaktoren. Daher gibt es einen irreduziblen Faktor P von F mit $\operatorname{grad}(P) \geq 2$ und $K' = K[X]/(P)$ ist nach Satz 7.6 und nach Proposition 7.9 eine Körpererweiterung von K vom Grad ≥ 2. Da P als Faktor von F ebenfalls über L_1 und über L_2 in Linearfaktoren zerfällt, gibt es K-Algebrahomomorphismen $K' \to L_1$ und $K' \to L_2$. Diese sind injektiv, so dass K' sowohl von L_1 als auch von L_2 ein Unterkörper ist. Nach Lemma 11.3 sind dann L_1 und L_2 Zerfällungskörper von $F \in K'[X]$. Nach Satz 2.8 ist

$$\operatorname{grad}_{K'} L_1 < \operatorname{grad}_K L_1,$$

so dass wir auf K', L_1, L_2 die Induktionsvoraussetzung anwenden können. Es gibt also einen K'-Algebraisomorphismus

$$\varphi\colon\ L_1 \longrightarrow L_2.$$

Dieser ist erst recht ein K-Algebraisomorphismus. □

11.2. **Konstruktion endlicher Körper.**

Definition 11.7. Sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte. Der *Frobeniushomomorphismus* ist der Ringhomomorphismus

$$R \longrightarrow R,\ f \longmapsto f^p.$$

Endliche Körper mit der Anzahl p^e konstruiert man, indem man ein in $(\mathbb{Z}/(p))[X]$ irreduzibles Polynom vom Grad n findet. Ob ein gegebenes Polynom irreduzibel ist, lässt sich dabei grundsätzlich in endlich vielen Schritten entscheiden, da es ja zu jedem Grad überhaupt nur endlich viele Polynome gibt, die als Teiler in Frage kommen können. Zur Konstruktion von einigen kleinen endlichen Körpern siehe Aufgabe 9.22 und Aufgabe 11.23. Generell

kann man einen Körper mit $q = p^e$ Elementen als Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{Z}/(p)$ erhalten.

Ferdinand Georg Frobenius (1849-1917)

Lemma 11.8. *Sei K ein Körper der Charakteristik p, sei $q = p^e$, $e \geq 1$. Es sei*

$$M = \{x \in K | \, x^q = x\}.$$

Dann ist M ein Unterkörper von K.

Beweis. Zunächst gilt für jedes Element $x \in \mathbb{Z}/(p) \subseteq K$, dass

$$x^{p^e} = (x^p)^{p^{e-1}} = x^{p^{e-1}} = \ldots = x$$

ist, wobei wir wiederholt den kleinen Fermat benutzt haben. Insbesondere ist also $0, 1, -1 \in M$. Es ist $z^q = F^e(z)$ und der Frobeniushomomorphismus

$$F\colon K \longrightarrow K,\, x \longmapsto x^p,$$

ist ein Ringhomomorphismus nach Aufgabe 11.10. Daher ist für $x, y \in M$ einerseits

$$(x+y)^q = F^e(x+y) = F^e(x) + F^e(y) = x^q + y^q = x + y$$

und andererseits

$$(xy)^q = x^q y^q = xy.$$

Ferner gilt für $x \in M$, $x \neq 0$, die Gleichheit

$$\left(x^{-1}\right)^q = (x^q)^{-1} = x^{-1},$$

so dass auch das Inverse zu M gehört und in der Tat ein Körper vorliegt. □

Im Beweis der nächsten Aussage werden wir die Technik des *formalen Ableitens* verwenden. Ableiten ist eigentlich eine analytische Technik, und bekanntlich ist die Ableitung eines Monoms X^m gleich mX^{m-1}, und die Ableitung eines Polynoms ergibt sich durch lineare Fortsetzung dieser Regel. Da der Exponent der Variablen zum Vorfaktor wird, und da man jede ganze Zahl in jedem Körper eindeutig interpretieren kann, ergeben solche Ableitungen auch rein algebraisch für jeden Grundkörper Sinn. Wir definieren daher.

Definition 11.9. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zu einem Polynom $F = \sum_{i=0}^{n} a_i X^i \in K[X]$ heißt das Polynom

$$F' = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 3a_3X^2 + 2a_2X + a_1$$

die *formale Ableitung* von F.

Man beachte, dass, insbesondere bei positiver Charakteristik, das algebraische Ableiten einige überraschende Eigenschaften haben kann. In positiver Charakteristik p ist beispielsweise

$$(X^p)' = pX^{p-1} = 0.$$

Für einige grundlegende Eigenschaften des Ableitens siehe die Aufgaben. Wichtig ist für uns, dass man mit der formalen Ableitung testen kann, ob die Nullstellen eines Polynoms einfach oder mehrfach sind (eine Nullstelle a heißt *mehrfach*, wenn das zugehörige lineare Polynom $X-a$ das Polynom mehrfach teilt, d.h. wenn es in der Primfaktorzerlegung mit einem Exponenten ≥ 2 vorkommt).

Lemma 11.10. *Sei K ein Körper der Charakteristik $p > 0$, sei $q = p^e$, $e \geq 1$. Das Polynom $X^q - X$ zerfalle über K in Linearfaktoren. Dann ist*

$$M = \{x \in K \mid x^q = x\}$$

ein Unterkörper von K mit q Elementen.

Beweis. Nach Lemma 11.8 ist M ein Unterkörper von K, und nach Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) besitzt er höchstens q Elemente. Es ist also zu zeigen, dass $F = X^q - X$ keine mehrfache Nullstellen hat. Dies folgt aber aus der formalen Ableitung $F' = -1$ und Aufgabe 11.28. □

Satz 11.11. *Sei p eine Primzahl und $e \in \mathbb{N}_+$. Dann gibt es bis auf Isomorphie genau einen Körper mit $q = p^e$ Elementen.*

Beweis. Zur Existenz. Wir wenden Lemma 11.1 auf den Grundkörper $\mathbb{Z}/(p)$ und das Polynom $X^q - X$ an und erhalten einen Körper L der Charakteristik p, über dem $X^q - X$ in Linearfaktoren zerfällt. Nach Lemma 11.10 gibt es dann einen Unterkörper M von L, der aus genau q Elementen besteht.

Zur Eindeutigkeit. Wir zeigen, dass ein Körper mit q Elementen der Zerfällungskörper des Polynoms $X^q - X$ sein muss, so dass er aufgrund dieser

Eigenschaft nach Satz 11.6 eindeutig bestimmt ist. Sei also L ein Körper mit q Elementen, der dann $\mathbb{Z}/(p)$ als Primkörper enthält. Da $L^\times$ genau $q-1$ Elemente besitzt, gilt nach Korollar 4.17 die Gleichung $x^{q-1} = 1$ für jedes $x \in L^\times$ und damit auch $x^q = x$ für jedes $x \in L$. Dieses Polynom vom Grad q hat also in L genau q verschiedene Nullstellen, so dass es also über L zerfällt. Zugleich ist der von allen Nullstellen erzeugte Unterkörper gleich L, so dass L der Zerfällungskörper ist. □

Notation 11.12. Sei p eine Primzahl und $e \in \mathbb{N}_+$. Der aufgrund von Satz 11.11 bis auf Isomorphie eindeutig bestimmte endliche Körper mit $q = p^e$ Elementen wird mit

$$\mathbb{F}_q$$

bezeichnet.

Für $q = p$ ist $\mathbb{F}_p = \mathbb{Z}/(p)$. Dagegen sind für $q = p^e$, $e \geq 2$, die Ringe $\mathbb{F}_q$ und $\mathbb{Z}/(q)$ verschieden, obwohl beide Ringe q Elemente besitzen. Dies liegt einfach daran, dass $\mathbb{F}_q$ ein Körper ist, $\mathbb{Z}/(q)$ aber nicht.

11. Arbeitsblatt

11.1. **Aufwärmaufgaben.**

Aufgabe 11.1. Zeige, dass der Körper der komplexen Zahlen $\mathbb{C}$ der Zerfällungskörper des Polynoms $X^2 + 1 \in \mathbb{R}[X]$ ist.

Aufgabe 11.2. Es sei $P = X^2 + aX + b \in K[X]$ ein quadratisches Polynom über einem Körper K. Welche Möglichkeiten gibt es für den Zerfällungskörper von P?

Aufgabe 11.3. Es sei K ein Körper und seien $F_1, \ldots, F_r \in K[X]$ Polynome. Zeige, dass es eine endliche Körpererweiterung $K \subseteq L$ derart gibt, dass diese Polynome in $L[X]$ in Linearfaktoren zerfallen.

Aufgabe 11.4. Es sei K ein Körper, $F \in K[X]$ ein Polynom vom Grad n und $K \subseteq L$ der Zerfällungskörper von F. Zeige, dass die Abschätzung

$$\operatorname{grad}_K L \leq n!$$

gilt.

Aufgabe 11.5.*

Es sei $X^n - a \in \mathbb{Q}[X]$ mit $n \geq 4$ gerade. Zeige, dass der Zerfällungskörper von $X^n - a$ maximal den Grad $\frac{n!}{2}$ besitzt.

Aufgabe 11.6. Es sei $q \in \mathbb{Q}$ eine rationale Zahl und es sei L der Zerfällungskörper von $X^3 - q$. Welchen Grad besitzt L (über $\mathbb{Q}$)? Man gebe für jeden möglichen Grad Beispiele an.

Aufgabe 11.7.*

Das Polynom $F = X^3 - 3X + 1 \in \mathbb{Q}[X]$ ist irreduzibel nach Aufgabe 3.16 und definiert daher eine Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

vom Grad 3. Die Restklasse von X in L sei mit α bezeichnet. Zeige, dass auch die Elemente aus L

$$\beta = \alpha^2 - 2$$

und

$$\gamma = -\alpha^2 - \alpha + 2$$

Nullstellen von F sind.

Aufgabe 11.8.*

Es sei $F \in \mathbb{Q}[X]$ und $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$ der Zerfällungskörper zu F. Zeige, dass die komplexe Konjugation den Körper L in sich überführt, also ein Element in der Galoisgruppe $\mathrm{Gal}\,(L|K)$ definiert.

Aufgabe 11.9. Sei $K \subseteq L$ eine Körpererweiterung von endlichen Körpern. Zeige, dass dies eine einfache Körpererweiterung ist.

Aufgabe 11.10. Sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte (dabei ist p eine Primzahl). Zeige, dass die Abbildung

$$R \longrightarrow R,\ f \longmapsto f^p,$$

ein Ringhomomorphismus ist, den man den *Frobeniushomomorphismus* nennt.

Aufgabe 11.11. Sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte. Zeige, dass die e-te Hintereinanderschaltung des Frobeniushomomorphismus

$$F\colon\ R \longrightarrow R,\ f \longmapsto f^p,$$

durch $f \mapsto f^q$ mit $q = p^e$ gegeben ist.

Aufgabe 11.12. Sei K ein endlicher Körper der Charakteristik p. Zeige, dass der Frobeniushomomorphismus ein Körperautomorphismus ist.

Aufgabe 11.13. Sei K ein Körper der positiven Charakteristik p. Sei $F\colon K \to K$ der Frobeniushomomorphismus. Zeige, dass genau die Elemente aus $\mathbb{Z}/(p)$ invariant unter F sind.

Aufgabe 11.14. Sei $\mathbb{F}_q$ der Körper mit $q = p^e$ Elementen. Bestimme die Ordnung des Frobeniushomomorphismus in der Automorphismengruppe von $\mathbb{F}_q$.

Aufgabe 11.15. Sei p eine Primzahl und $q = p^n$, $n \geq 2$. Zeige, dass $\mathbb{Z}/(p^n)$ kein Vektorraum über $\mathbb{Z}/(p)$ sein kann.

Aufgabe 11.16. Bestimme die formale Ableitung von

$$2X^7 + X^6 + 2X^5 + X^4 + X^3 + X^2 + 2 \in \mathbb{Z}/(3)[X]\,.$$

Aufgabe 11.17. Sei K ein Körper der positiven Charakteristik $p > 0$. Bestimme die Menge der Polynome $F \in K[T]$ mit formaler Ableitung $F' = 0$.

Aufgabe 11.18.*

Sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik ungleich 2. Zeige unter Verwendung der Isomorphiesätze, dass genau die Hälfte der Elemente aus $\mathbb{F}_q^\times$ ein Quadrat in $\mathbb{F}_q$ ist.

Aufgabe 11.19. Zeige, dass das Polynom $X^9 - X \in \mathbb{Z}/(3)[X]$ die Zerlegung

$$\begin{aligned} X^9 - X &= \left(X^3 - X\right)\left(X^8 + X^6 + X^4 + X^2 + 1\right) \\ &= X(X-1)(X+1)\left(X^2+1\right)\left(X^2+2X+1\right) \\ &\qquad \left(X^2+X+2\right)\left(X^2+2X+2\right) \end{aligned}$$

besitzt, wobei die Faktoren in der zweiten Zerlegung irreduzibel sind. Zeige, dass die Restklassenkörper

$$\begin{aligned} &\mathbb{Z}/(3)[X]/\left(X^2+1\right),\ \mathbb{Z}/(3)[X]/\left(X^2+2X+1\right), \\ &\qquad \mathbb{Z}/(3)[X]/\left(X^2+X+2\right),\ \mathbb{Z}/(3)[X]/\left(X^2+2X+2\right) \end{aligned}$$

untereinander isomorph sind.

Aufgabe 11.20.*

Beschreibe den Körper mit acht Elementen $\mathbb{F}_8$ als einen Restklassenkörper von $\mathbb{Z}/(2)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_8$ an.

Aufgabe 11.21.*

Es sei p eine ungerade Primzahl. Es sei $q = p^e$ und $c \in \mathbb{F}_q$ ein Nichtquadrat.

(1) Zeige
$$\mathbb{F}_{q^2} \cong \mathbb{F}_q[X]/\left(X^2 - c\right).$$
(2) Zeige, dass es eine Kette von rein-quadratischen Erweiterungen
$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^4} \subseteq \mathbb{F}_{p^8} \subseteq \mathbb{F}_{p^{16}} \subseteq \dots$$
gibt.
(3) Zeige, dass die Restklasse von X in $\mathbb{Z}/(3)[X]/\left(X^2 - 2\right)$ ein Quadrat ist.
(4) Es sei nun $p = 1 \mod 4$. Zeige, dass die Restklasse x von X in $\mathbb{F}_q[X]/\left(X^2 - c\right)$ ein Nichtquadrat ist.
(5) Es sei $p = 1 \mod 4$ und sei $a \in \mathbb{Z}/(p)$ ein Nichtquadrat. Zeige, dass $Y^{2^n} - a$ für alle $n \geq 1$ irreduzibel ist.

Aufgabe 11.22.*

Finde ein primitives Element in $\mathbb{Z}/(11)$ und in $\mathbb{Z}/(121)$. Man gebe ferner ein Element der Ordnung 10 und ein Element der Ordnung 11 in $\mathbb{Z}/(121)$ an. Gibt es Elemente der Ordnung 10 und der Ordnung 11 auch in $\mathbb{F}_{121}$?

11.2. **Aufgaben zum Abgeben.**

Aufgabe 11.23. (4 Punkte)

Konstruiere endliche Körper mit $64, 81, 121, 125$ und 128 Elementen.

Aufgabe 11.24. (4 Punkte)

Sei p eine Primzahl und $e, d \in \mathbb{N}_+$. Zeige: $\mathbb{F}_{p^d}$ ist ein Unterkörper von $\mathbb{F}_{p^e}$ genau dann, wenn e ein Vielfaches von d ist.

Aufgabe 11.25. (4 Punkte)

Sei q eine echte Primzahlpotenz und $\mathbb{F}_q$ der zugehörige endliche Körper. Zeige, dass in $\mathbb{F}_{q^2}$ jedes Element aus $\mathbb{F}_q$ ein Quadrat ist.

Aufgabe 11.26. (4 Punkte)

Finde einen Erzeuger der Einheitengruppe eines Körpers mit 27 Elementen. Wie viele solche Erzeuger gibt es?

Aufgabe 11.27. (3 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Beweise die folgenden Rechenregeln für das formale Ableiten $F \mapsto F'$:

(1) Die Ableitung eines konstanten Polynoms ist 0.
(2) Die Ableitung ist K-linear.
(3) Es gilt die *Produktregel*, also

$$(FG)' = FG' + F'G.$$

Es sei K ein Körper. Ein Element $a \in K$ heißt *mehrfache Nullstelle* eines Polynoms $P \in K[X]$, wenn in der Primfaktorzerlegung von P das lineare Polynom $X - a$ mit einem Exponenten ≥ 2 vorkommt.

Aufgabe 11.28. (4 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $F \in K[X]$ und $a \in K$. Zeige, dass a genau dann eine mehrfache Nullstelle von F ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

12. Vorlesung - Graduierte Körperweiterungen

12.1. **Graduierungen.**

Wir möchten Körpererweiterungen beschreiben, die eine besonders übersichtliche Struktur aufweisen und eng mit einfachen Radikalerweiterungen zusammenhängen. Insbesondere sind ihre Galoisgruppen und ihre Zwischenkörper häufig einfach beschreibbar.

Definition 12.1. Es sei K ein Körper und D eine kommutative Gruppe.[9] Eine K-Algebra A heißt *D-graduiert*, wenn es eine direkte Summenzerlegung

$$A = \bigoplus_{d \in D} A_d$$

mit K-Untervektorräumen A_d derart gibt, dass $K \subseteq A_0$ ist und für die Multiplikation auf A die Beziehung

$$A_d \cdot A_e \subseteq A_{d+e}$$

gilt.

Bemerkung 12.2. In einer D-graduierten K-Algebra besitzt jedes Element $a \in A$ eine eindeutige Darstellung

$$a = \sum_{d \in D} a_d \text{ mit } a_d \in A_d\,,$$

wobei nur endlich viele der a_d ungleich 0 sein können. Die a_d heißen dabei die *homogenen Komponenten* von a, die A_d heißen ebenfalls die *homogenen*

[9] Diese Gruppe wird fast immer additiv geschrieben.

Komponenten von A (oder d-te Stufe) und Elemente $a \in A_d$ heißen *homogen* vom *Grad* d. Die Gruppe D heißt die *graduierende Gruppe*. Der Fall $A_d = 0$ ist erlaubt.

Durch eine Graduierung wird die Multiplikation auf einer Algebra A übersichtlicher strukturiert. Man muss lediglich für homogene Elemente $a \in A_d$ und $b \in A_e$ die Produkte $ab \in A_{d+e}$ kennen, dadurch ist schon die gesamte Multiplikation distributiv festgelegt.

Beispiel 12.3. Es sei K ein Körper und $K[X_1, \ldots, X_n]$ der Polynomring in n Variablen über K. Dieser ist in naheliegender Weise $\mathbb{Z}$-graduiert. Man definiert für ein Monom $X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ den Grad durch $k_1 + k_2 + \cdots + k_n$ und setzt A_d als den Vektorraum aller Polynome an, die Linearkombinationen von Monomen vom Grad d sind. Bei der Multiplikation von zwei Monomen verhält sich der Grad offensichtlich additiv, so dass dadurch eine graduierte K-Algebra entsteht. Es ist $A_0 = K$ und $A_n = 0$ für negativen Grad n. Diese Graduierung heißt auch die *Standardgraduierung* auf dem Polynomring.

Beispiel 12.4. Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Dann besitzt die Restklassenalgebra $A = K[X]/(X^n - a)$ eine Graduierung mit der graduierenden Gruppe $D = \mathbb{Z}/(n)$, und zwar setzt man (wobei x die Restklasse von X sei)

$$A_d = \left\{ \lambda x^d | \, \lambda \in K \right\}.$$

Jedes Element $f \in A$ kann man durch ein Polynom repräsentieren, das maximal den Grad $n-1$ besitzt. Daher besitzt jedes f eine Summendarstellung mit Summanden aus den A_d. Diese Summenzerlegung ist direkt, da man mit der einzigen gegebenen Gleichung $X^n = a$ nicht weiter reduzieren kann. Die Multiplikationseigenschaft folgt aus $\lambda x^d \cdot \mu x^e = \lambda\mu x^{d+e}$, und dies ist gleich $\lambda\mu a x^{d+e-n}$, falls $d + e \geq n$ ist, und andernfalls gleich $\lambda\mu x^{d+e}$. So oder so ist es ein Element aus A_{d+e}.

12.2. **Graduierte Körpererweiterungen.**

Im vorstehenden Beispiel ist es eine nicht-triviale Frage, unter welchen Bedingungen die Algebra A wieder ein Körper ist. Falls ja, so liegt eine graduierte Körpererweiterung im Sinne der folgenden Definition vor.

Definition 12.5. Es sei K ein Körper und D eine endliche kommutative Gruppe. Unter einer *D-graduierten Körpererweiterung* versteht man eine Körpererweiterung $K \subseteq L$, bei der auf L eine D-Graduierung $L = \bigoplus_{d \in D} L_d$ mit $L_0 = K$ und $L_d \neq 0$ für alle $d \in D$ gegeben ist.

Beispiel 12.6. Die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ ist durch die Gruppe $D = \mathbb{Z}/(2)$ graduiert. Die 0-te homogene Komponente ist $\mathbb{R}$ und die 1-te Komponente ist $\mathbb{R}$i (das i gehört da dazu, während man unter dem Imaginärteil einer komplexen Zahl die reelle Zahl vor dem i versteht). Die übliche Schreibweise $z = a + b$i ist also die Zerlegung in die homogenen Komponenten.

Beispiel 12.7. Die $\mathbb{Q}$-Algebra $\mathbb{Q}[X]/(X^4+4)$ ist eine $\mathbb{Z}/(4)$-graduierte $\mathbb{Q}$-Algebra. Das Polynom X^4+4 besitzt keine Nullstelle in $\mathbb{Q}$, es ist aber nicht irreduzibel, wie die Zerlegung

$$X^4+4 = (X^2-2X+2)(X^2+2X+2)$$

zeigt. Es liegt also keine graduierte Körpererweiterung vor.

Beispiel 12.8. Wir betrachten den von $\sqrt{2}$ und $\sqrt{3}$ erzeugten Unterkörper $L = \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}[\sqrt{2},\sqrt{3}]$ von $\mathbb{C}$ (oder von $\mathbb{R}$). Die Elemente $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ bilden dabei unmittelbar ein $\mathbb{Q}$-Erzeugendensystem und sogar eine Basis, da man andernfalls $\sqrt{3}$ als rationale Linearkombination von 1 und $\sqrt{2}$ ausdrücken könnte. Damit liegt insgesamt eine Körpererweiterung vom Grad vier vor. Sei $D = \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Wir setzen

$$L_{(0,0)} = \mathbb{Q},\ L_{(1,0)} = \mathbb{Q}\cdot\sqrt{2},\ L_{(0,1)} = \mathbb{Q}\cdot\sqrt{3}\,, L_{(1,1)} = \mathbb{Q}\cdot\sqrt{6}\,,$$

und erhalten dadurch eine D-graduierte Körpererweiterung von $\mathbb{Q}$.

Beispiel 12.9. Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq L := \mathbb{Q}[\mathrm{i},\sqrt{2}]$$

in $\mathbb{C}$. Diese besitzt eine $D = \mathbb{Z}/(2)\times\mathbb{Z}/(2)$-Graduierung, bei der $1, \mathrm{i}, \sqrt{2}, \mathrm{i}\sqrt{2}$ eine homogene Basis bilden. Das (in dieser Graduierung nicht homogene) Element $\zeta_8 = \frac{1}{2}\left(\sqrt{2}+\sqrt{2}\mathrm{i}\right)$ ist eine 8-te primitive Einheitswurzel und wegen $\zeta^2 = \mathrm{i}$ ist $L = \mathbb{Q}(\zeta_8)$ der achte Kreisteilungskörper Das Minimalpolynom zu ζ_8 ist X^4+1, so dass man auch $L \cong \mathbb{Q}[X]/(X^4+1)$ schreiben kann. Dies zeigt, dass L auch eine $\mathbb{Z}/(4)$-graduierte Körpererweiterung von $\mathbb{Q}$ ist, bei der ζ_8 homogen ist.

Lemma 12.10. *Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Dann gelten folgende Eigenschaften*

(1) *Jede homogene Stufe L_d besitzt die K-Dimension 1.*
(2) *Es ist $\operatorname{grad}_K L = \#(D)$.*
(3) *Es sei $D = (d_1,\ldots,d_m)$ ein Erzeugendensystem von D und es sei $x_i \in L_{d_i}$, $x_i \neq 0$, fixiert. Dann ist $L = K[x_1,\ldots,x_m]$. Insbesondere wird L von homogenen Elementen erzeugt.*
(4) *Jedes homogene Element $x \in L_d$, $x \neq 0$, besitzt ein Minimalpolynom der Form $X^n - a$ mit $a \in K$.*
(5) *Die Körpererweiterung $K \subseteq L$ ist eine Radikalerweiterung.*

Beweis. (1). Nach Voraussetzung ist $L_d \neq 0$. Seien $a, b \in L_d$ von 0 verschieden und sei $c \in L_{-d}$ ebenfalls $\neq 0$. Dann sind ca und cb Elemente $\neq 0$ in $L_0 = K$ und daher besteht die Beziehung $ca = \lambda cb$ mit $\lambda \in K$, die sich durch Multiplikation mit c^{-1} (dieses Element gibt es, da wir in einem Körper sind) zurückübersetzt zu $a = \lambda b$. (2) folgt direkt aus (1). (3) ist klar wegen

(1). (4). Sei $n \in \mathbb{N}$ die Ordnung von $d \in D$. Für ein homogenes Element $x \in L_d$, $x \neq 0$, ist daher

$$a = x^n \in L_{nd} = L_0 = K.$$

Also ist $X^n - a \in K[X]$ ein annullierendes Polynom. Die Potenzen x^i, $0 \leq i \leq n-1$, liegen alle in verschiedenen homogenen Stufen. Daher sind sie linear unabhängig und es kann kein annullierendes Polynom von kleinerem Grad geben. (5) folgt aus (3) und (4). □

12.3. **Charaktergruppe und Automorphismengruppe bei einer graduierten Körpererweiterung.**

Wir wollen nun die Automorphismen auf einer graduierten Körpererweiterung kennenlernen. Die Graduierung erlaubt es, die Automorphismen übersichtlich zu beschreiben, was für eine beliebige Körpererweiterung keineswegs selbstverständlich ist. Die Automorphismen hängen eng mit den sogenannten Charakteren der graduierenden Gruppe zusammen, so dass wir zuerst über Charaktere sprechen.

Definition 12.11. Es sei G ein Monoid und K ein Körper. Dann heißt ein Monoidhomomorphismus

$$\chi\colon G \longrightarrow (K^\times, 1, \cdot)$$

ein *Charakter* von G in K.

Die Menge der Charaktere von G nach K bezeichnen wir mit $\operatorname{Char}(G, K)$. Mit dem *trivialen Charakter* (also der konstanten Abbildung nach 1) und der Verknüpfung

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$$

ist $\operatorname{Char}(G, K)$ selbst ein Monoid, und zwar ein Untermonoid des Abbildungsmonoid von G nach $K^\times$. Da es zu jedem Charakter den inversen Charakter χ^{-1} gibt, der durch

$$\chi^{-1}(g) = (\chi(g))^{-1}$$

definiert ist, bildet $\operatorname{Char}(G, K)$ sogar eine kommutative Gruppe(siehe unten).

Definition 12.12. Es sei G ein Gruppe und K ein Körper. Dann nennt man die Menge der Charaktere

$$G^\vee := \operatorname{Char}(G, K) = \left\{\chi : G \to K^\times \,|\, \chi \text{ Charakter}\right\}$$

die *Charaktergruppe* von G (in K).

Beispiel 12.13. Zur Gruppe $G = \mathbb{Z}/(n)$ und zum Körper $\mathbb{C}$ besteht die Charaktergruppe aus allen Gruppenhomomorphismen $\varphi\colon \mathbb{Z}/(n) \to \mathbb{C}^\times$. Da ein solcher durch das Bild des Erzeugers 1 festgelegt ist, und dieser auf eine n-te Einheitswurzel geht, besteht eine natürliche Isomorphie zwischen der

Charaktergruppe $(\mathbb{Z}/(n))^\vee$ und der Gruppe μ_n der n-ten komplexen Einheitswurzeln. Diese Gruppe ist selbst isomorph zu $\mathbb{Z}/(n)$, aber nicht in kanonischer Weise.

Lemma 12.14. *Sei G eine Gruppe, K ein Körper und $G^\vee = \operatorname{Char}(G,K)$ die Charaktergruppe zu G. Dann gelten folgende Aussagen.*

(1) *$G^\vee$ ist eine kommutative Gruppe.*
(2) *Bei einer direkten Gruppenzerlegung $G = G_1 \times G_2$ ist $(G_1 \times G_2)^\vee = G_1^\vee \times G_2^\vee$.*

Beweis. Siehe Aufgabe 12.12. □

Lemma 12.15. *Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Dann gibt es einen Gruppenhomomorphismus*

$$D^\vee = \operatorname{Char}(D,K) \longrightarrow \operatorname{Aut}_K(A),\ \chi \longmapsto (a_d \mapsto \chi(d)a_d),$$

der Charaktergruppe von D in die (homogene) K-Automorphismengruppe von A. Wenn alle $A_d \neq 0$ sind, so ist diese Zuordnung injektiv.

Beweis. Zu jedem Charakter

$$\chi\colon\ D \longrightarrow K^\times$$

ist die durch $\varphi_\chi\left(\sum_{d\in D} a_d\right) = \sum_{d\in D} \chi(d)\cdot a_d$ definierte Abbildung φ_χ mit der Addition verträglich. Die Verträglichkeit mit der Multiplikation folgt für homogene Elemente $a_d \in A_d$ und $a_e \in A_e$ aus

$$\varphi_\chi(a_d \cdot a_e) = \chi(d+e)a_d \cdot a_e = \chi(d)\cdot\chi(e)a_d \cdot a_e = \varphi_\chi(a_d)\cdot\varphi_\chi(a_e),$$

woraus sich aufgrund des Distributivgesetzes auch der allgemeine Fall ergibt. Für $a \in A_0$ (und insbesondere für $a \in K$) ist ferner $\varphi_\chi(a) = \chi(0)a = a$, so dass ein K-Algebrahomomorphismus vorliegt. Der triviale (konstante) Charakter geht bei dieser Zuordnung auf die Identität. Es seien nun zwei Charaktere $\chi_1, \chi_2 \in \operatorname{Char}(D,K)$ gegeben. Für ein homogenes Element $a_d \in A_d$ ist

$$\begin{aligned}
\varphi_{\chi_1\cdot\chi_2}(a_d) &= (\chi_1\cdot\chi_2)(d)\cdot a_d \\
&= \chi_1(d)\cdot\chi_2(d)\cdot a_d \\
&= \chi_1(d)\cdot\varphi_{\chi_2}(a_d) \\
&= \varphi_{\chi_1}(\varphi_{\chi_2}(a_d)) \\
&= (\varphi_{\chi_1}\circ\varphi_{\chi_2})(a_d),
\end{aligned}$$

so dass die Gesamtzuordnung mit den Verknüpfungen verträglich ist. Daher gilt auch

$$\varphi_\chi \circ \varphi_{\chi^{-1}} = \varphi_{\chi\circ\chi^{-1}} = \varphi_1 = \mathrm{Id}_A,$$

so dass jedes φ_χ ein K-Algebraautomorphismus und die Gesamtzuordnung ein Gruppenhomomorphismus ist. Die Injektivität ergibt sich unter Verwendung von Lemma 4.9 folgendermaßen. Bei $\chi \neq 1$ gibt es ein $d \in D$ mit

$\chi(d) \neq 1$. Nach Voraussetzung ist

$$A_d \neq 0,$$

sei also $a \in A_d$, $a \neq 0$. Damit ist $\varphi_\chi(a) = \chi(d)a \neq a$, da $\chi(d) - 1$ eine Einheit ist. Also ist $\varphi_\chi \neq \mathrm{Id}_A$. □

Beispiel 12.16. Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$ derart, dass $X^n - a$ irreduzibel ist. Dann ist $K \subseteq K[X]/(X^n - a)$ nach Korollar 7.7 und nach Beispiel 9.5 eine $\mathbb{Z}/(n)$-graduierte Körpererweiterung.

Eine notwendige Voraussetzung für die Irreduzibilität von $X^n - a$ ist, dass a in K keine n-te Wurzel besitzt, da sonst das Polynom sofort einen Linearfaktor besitzt. Bei $n = 2$ oder $n = 3$ ist diese Bedingung auch hinreichend. Bei $n = 2$ und wenn die Charakteristik von K nicht gleich 2 ist, so ist $1 \neq -1$ und der nichttriviale Charakter

$$\chi\colon\ D = \mathbb{Z}/(2) \longrightarrow K^\times$$

mit $\chi(0) = 1$ und $\chi(1) = -1$ definiert über Lemma 12.15 den nichttrivialen K-Körperautomorphismus mit $x \mapsto -x$ (wobei x die Restklasse von X sei), also die Konjugation in der quadratischen Körpererweiterung $K \subseteq K[X]/(X^2 - a)$.

12. Arbeitsblatt

12.1. **Aufwärmaufgaben.**

Aufgabe 12.1. Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Zeige, dass zu einem Untermonoid $M \subseteq D$ der K-Vektorraum

$$\oplus_{d \in M} A_d$$

ein Unterring von A ist.

Aufgabe 12.2. Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra, die ein Integritätsbereich sei. Zeige, dass die Menge

$$M = \{d \in D |\, A_d \neq 0\}$$

ein Untermonoid von D ist.

Aufgabe 12.3. Es sei K ein kommutativer Ring, D eine kommutative Gruppe und $A = \bigoplus_{d \in D} A_d$ eine D-graduierte K-Algebra. Es sei $f \in A$ eine homogene Einheit vom Grad d. Zeige, dass das inverse Element f^{-1} homogen vom Grad $-d$ ist.

Aufgabe 12.4. Wir betrachten die $\mathbb{Z}/(10)$-graduierte $\mathbb{Q}$-Algebra

$$L = \mathbb{Q}[X]/\left(X^{10}-5\right) = \mathbb{Q}\oplus 5^{\frac{1}{10}}\cdot\mathbb{Q}\oplus 5^{\frac{2}{10}}\cdot\mathbb{Q}\oplus 5^{\frac{3}{10}}\cdot\mathbb{Q}\oplus\cdots\oplus 5^{\frac{8}{10}}\cdot\mathbb{Q}\oplus 5^{\frac{9}{10}}\cdot\mathbb{Q}.$$

(1) Berechne das Inverse von

$$5^{\frac{1}{10}}.$$

(2) Berechne

$$\left(5^{\frac{7}{10}}\right)^4.$$

(3) Berechne

$$\left(\frac{2}{7}-\frac{4}{3}\cdot 5^{\frac{3}{10}}-5\cdot 5^{\frac{8}{10}}\right)\left(\frac{2}{3}+\frac{5}{4}\cdot 5^{\frac{5}{10}}+4\cdot 5^{\frac{7}{10}}-\frac{1}{2}\cdot 5^{\frac{9}{10}}\right).$$

(4) Bestimme graduierte Unterringe von L.

Aufgabe 12.5. Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Zeige, dass zu einem Untermonoid $M \subseteq D$ der K-Vektorraum

$$\oplus_{d\in M} A_d$$

ein Unterkörper von A ist.

Aufgabe 12.6. Es sei K ein Körper der Charakteristik $\neq 2$. Zeige, dass eine quadratische Körpererweiterung $K \subseteq L$ graduiert ist.

Aufgabe 12.7. Es sei $\epsilon = \frac{-1+\sqrt{3}\mathrm{i}}{2}$ die dritte komplexe Einheitswurzel. Zeige, dass die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\epsilon] = L \subseteq \mathbb{C}$$

graduiert ist.

Aufgabe 12.8. Zeige, dass eine $\mathbb{Z}/(n)$-graduierte Körpererweiterung einfach ist.

Aufgabe 12.9. Es sei $K \subseteq L$ eine D-graduierte Körpererweiterung, wobei D nicht zyklisch sei. Zeige, dass die Körpererweiterung nicht von einem homogenen Element erzeugt wird.

Aufgabe 12.10.*

Es seien $p, q \in \mathbb{Z}$ verschiedene Primzahlen und

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p}, \sqrt{q}]$$

die zugehörige Körpererweiterung vom Grad 4. Bestimme, ob die folgenden Elemente die $\mathbb{Q}$-Algebra L erzeugen oder nicht.

(1) $\sqrt{p}$,
(2) $\sqrt{p} + \sqrt{q}$,
(3) $\sqrt{pq}$,
(4) $\sqrt{p} + \sqrt{pq}$.

Aufgabe 12.11. Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[4]{7}\mathrm{i}] = L.$$

(1) Bestimme das Minimalpolynom von $\sqrt[4]{7}\mathrm{i}$.
(2) Zeige, dass der Grad der Körpererweiterung $\mathbb{Q} \subseteq L$ gleich 4 ist.
(3) Finde einen echten Zwischenkörper

$$\mathbb{Q} \subset M \subset L.$$

(4) Zeige, dass L eine $\mathbb{Z}/(4)$-graduierte Körpererweiterung von $\mathbb{Q}$ ist.
(5) Zeige, dass $L[\mathrm{i}] = \mathbb{Q}[\sqrt[4]{7}, \mathrm{i}]$ eine $\mathbb{Z}/(4) \times \mathbb{Z}/(2)$- graduierte Körpererweiterung von $\mathbb{Q}$ ist. Durch welche Untergruppe von $\mathbb{Z}/(4) \times \mathbb{Z}/(2)$ wird L beschrieben?

Aufgabe 12.12. Sei D eine Gruppe, K ein Körper und $D^\vee = \mathrm{Char}\,(D, K)$ die Charaktergruppe zu D. Beweise die folgenden Aussagen.

(1) $D^\vee$ ist eine kommutative Gruppe.
(2) Bei einer direkten Gruppenzerlegung $D = D_1 \times D_2$ ist $(D_1 \times D_2)^\vee = D_1^\vee \times D_2^\vee$.

Aufgabe 12.13. Sei D eine endliche Gruppe, K ein Körper und $\chi \in D^\vee = \mathrm{Char}\,(D, K)$ ein Charakter. Zeige, dass $\chi(d)$ für jedes $d \in D$ eine Einheitswurzel in K ist.

Aufgabe 12.14.*

Es seien D_1 und D_2 kommutative Gruppen und seien $D_1^\vee$ und $D_2^\vee$ die zugehörigen Charaktergruppen zu einem Körper K.

(1) Zeige, dass zu einem Gruppenhomomorphismus

$$\varphi\colon\ D_1 \longrightarrow D_2$$

durch die Zuordnung $\chi \mapsto \chi \circ \varphi$ ein Gruppenhomomorphismus

$$\varphi^\vee\colon\ D_2^\vee \longrightarrow D_1^\vee$$

definiert wird.

(2) Es sei D_3 eine weitere kommutative Gruppe und sei

$$\psi\colon\ D_2 \longrightarrow D_3$$

ein Gruppenhomomorphismus. Zeige die Gleichheit

$$(\psi \circ \varphi)^\vee \ = \ \varphi^\vee \circ \psi^\vee.$$

Aufgabe 12.15. Es sei D eine kommutative Gruppe und K ein Körper.

a) Zeige, dass durch

$$D \longrightarrow (D^\vee)^\vee,\ d \longmapsto (\mathrm{ev}_d : \chi \mapsto \chi(d)),$$

ein natürlicher Gruppenhomomorphismus von D in das Doppeldual $(D^\vee)^\vee$ gegeben ist.

b) Es sei nun D endlich und es sei vorausgesetzt, dass K eine m-te primitive Einheitswurzel enthält, wobei m der Exponent von D sei. Zeige, dass dann die Abbildung aus a) ein Isomorphismus ist.

Die in der vorstehenden Aufgabe auftretende Abbildung ev_d heißt *Evaluierungsabbildung* (zu d).

Aufgabe 12.16. Es sei D eine endliche kommutative Gruppe und es sei K ein Körper. Wir betrachten die Zuordnung

$$E \longmapsto E^\perp = \{\chi \in D^\vee \mid \chi(d) = 1 \text{ für alle } d \in E\}\ ,$$

die einer Untergruppe von D eine Untergruppe von $D^\vee$ zuordnet. Zeige die folgenden Aussagen.

a) Die Zuordnung ist inklusionsumkehrend.

b) Unter der kanonischen Abbildung

$$D \longrightarrow (D^\vee)^\vee,\ d \longmapsto (\mathrm{ev}_d : \chi \mapsto \chi(d)),$$

ist $\mathrm{ev}_d(E) \subseteq (E^\perp)^\perp$.

c) Es sei vorausgesetzt, dass K eine m-te primitive Einheitswurzel enthält, wobei m der Exponent von D sei. Zeige, dass dann $\mathrm{ev}_d(E) = (E^\perp)^\perp$ gilt.

Aufgabe 12.17. Es sei D eine endliche kommutative Gruppe mit dem Exponenten m, und es sei K ein Körper, der eine primitive m-te Einheitswurzel besitzt. Zeige, dass die Zuordnungen

$$E \longmapsto E^{\perp} = \{\chi \in D^{\vee} | \, \chi(d) = 1 \text{ für alle } d \in E\}$$

und

$$H \longmapsto H^{\perp} = \{d \in D | \, \chi(d) = 1 \text{ für alle } \chi \in H\}$$

(zwischen den Untergruppen von D und den Untergruppen von $D^{\vee}$) zueinander invers sind.

Aufgabe 12.18. Es sei D eine endliche kommutative Gruppe mit dem Exponenten m, und es sei K ein Körper, der eine primitive m-te Einheitswurzel besitzt. Zeige, dass in der in Aufgabe 12.17 beschriebenen Korrespondenz zwischen den Untergruppen von D und von $D^{\vee}$ Durchschnitte von Untergruppen in die Summe von Untergruppen überführt werden. Es gilt also

$$(E_1 \cap E_2)^{\perp} \, = \, E_1^{\perp} + E_2^{\perp}.$$

Aufgabe 12.19. Sei K ein algebraisch abgeschlossener Körper und sei $F \in K[X,Y]$ ein homogenes Polynom. Zeige: F zerfällt in Linearfaktoren.

Aufgabe 12.20. Zeige, dass es im Polynomring in n Variablen genau $\binom{d+n-1}{n-1}$ Monome vom Grad d gibt.

Vor der nächsten Aufgabe erwähnen wir die folgende Definition.

Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte K-Algebra. Ein K-Automorphismus

$$\varphi \colon \, A \longrightarrow A$$

heißt *homogen*, wenn für jedes homogene Element $a \in A_d$ gilt $\varphi(a) \in A_d$.

Aufgabe 12.21. Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Zeige, dass der in Lemma 12.15 zu einem Charakter $\chi \in D^{\vee}$ eingeführte Automorphismus

$$\varphi_{\chi} \colon \, A \longrightarrow A$$

homogen ist.

Aufgabe 12.22. Wir betrachten die $\mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2)$-graduierte Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}, \sqrt{5}, \sqrt{7}]$$

und den durch $\chi(e_1) = -1$, $\chi(e_2) = 1$, $\chi(e_3) = -1$, gegebenen Charakter. Bestimme

$$\varphi_\chi \left(3 - 2\sqrt{3} - 2\sqrt{5} + 6\sqrt{7} + \sqrt{15} - 4\sqrt{21} + 3\sqrt{35} - 5\sqrt{105}\right) .$$

Aufgabe 12.23. Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq L := \mathbb{Q}[\mathrm{i}, \sqrt{2}] = \mathbb{Q}[\zeta_8]$$

mit $\zeta_8 = \frac{1}{2}\left(\sqrt{2} + \sqrt{2}\mathrm{i}\right)$ gemäß Beispiel 12.9. Zeige, dass die Galoisgruppe isomorph zu $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ ist.

Aufgabe 12.24.*

Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}, \mathrm{i}] = L\,.$$

a) Bestimme den Grad der Körpererweiterung $\mathbb{Q} \subseteq L$.

b) Beschreibe eine möglichst einfache $\mathbb{Q}$-Basis von L.

c) Zeige, dass eine graduierte Körpererweiterung vorliegt. Was ist die graduierende Gruppe?

d) Bestimme die $\mathbb{Q}$-Automorphismen von L.

e) Bestimme das Minimalpolynom von $\sqrt{3} + \mathrm{i}$.

Aufgabe 12.25. Es sei G die Menge der stetigen geraden Funktionen und U die Menge der stetigen ungeraden Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Zeige, dass

$$\mathrm{C}^0(\mathbb{R}, \mathbb{R}) = G \oplus U$$

eine $\mathbb{Z}/(2)$-graduierte $\mathbb{R}$-Algebra ist.

Aufgabe 12.26. Bestimme die Galoisgruppe des fünften Kreisteilungskörpers

$$\mathbb{Q} \subseteq \mathbb{Q}[\zeta_5]$$

mit $\zeta_5 = e^{2\pi\mathrm{i}/5}$.

Aufgabe 12.27.*

Zeige, dass der fünfte Kreisteilungskörper $\mathbb{Q} \subseteq \mathbb{Q}[\zeta_5]$ mit $\zeta_5 = e^{2\pi\mathrm{i}/5}$ nicht graduierbar ist.

12.2. **Aufgaben zum Abgeben.**

Aufgabe 12.28. (4 Punkte)

Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Es sei

$$\varphi\colon A \longrightarrow A$$

ein homogener Automorphismus. Zeige, dass es einen Charakter $\chi \in D^\vee$ mit $\varphi = \varphi_\chi$ gibt, wobei φ_χ der gemäß Lemma 12.15 zu χ gehörige Automorphismus ist.

Aufgabe 12.29. (4 Punkte)

Betrachte die Körpererweiterung

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}, \sqrt{7}] = L.$$

Zeige, dass einerseits $1, \sqrt{5}, \sqrt{7}, \sqrt{35}$ und andererseits $(\sqrt{5} + \sqrt{7})^i$, $i = 0, 1, 2, 3$, eine $\mathbb{Q}$-Basis von L bildet. Berechne die Übergangsmatrizen für diese Basen.

Aufgabe 12.30. (5 Punkte)

Es sei

$$f\colon \mathbb{C} \longrightarrow \mathbb{C}$$

eine stetige Funktion. Zeige, dass die beiden folgenden Aussagen äquivalent sind.

(1) Es gibt eine stetige Funtion
$$g\colon \mathbb{R}_{\geq 0} \longrightarrow \mathbb{C}$$
mit $f(z) = g(|z|)$ für alle $z \in \mathbb{C}$.
(2) Für alle n-ten Einheitswurzeln $\zeta \in \mathbb{C}$ (alle $n \in \mathbb{N}$) ist $f(\zeta z) = f(z)$ für alle $z \in \mathbb{C}$.

Aufgabe 12.31. (4 Punkte)

Es sei K ein Körper und sei D eine endliche kommutative Gruppe mit dem Exponenten m. Zeige, dass folgende Aussagen äquivalent sind.

(1) K besitzt eine m-te primitive Einheitswurzel.
(2) Zu jedem Primpotenzteiler p^r von m besitzt K eine p^r-te primitive Einheitswurzel.
(3) Zu jedem Teiler n von m besitzt K eine n-te primitive Einheitswurzel.
(4) Zu jeder Ordnung n eines Elementes $d \in D$ besitzt K eine n-te primitive Einheitswurzel.

Aufgabe 12.32. (4 (1+3) Punkte)

Es sei D eine endliche kommutative Gruppe und $E \subseteq D$ eine Untergruppe. Es sei K ein Körper.

a) Zeige, dass der Kern des natürlichen Gruppenhomomorphismus

$$\psi\colon\ D^\vee \longrightarrow E^\vee,\ \chi \longmapsto \chi|_E,$$

gleich $E^\perp$ ist.

b) Es sei vorausgesetzt, dass K eine m-te primitive Einheitswurzel besitzt, wobei m der Exponent von D sei. Zeige, dass ψ surjektiv ist.

13. Vorlesung - Der Satz vom primitiven Element

Wir interessieren uns für die Frage, wann eine endliche Körpererweiterung $K \subseteq L$ einfach ist, also in der Form $L = K(x)$ mit einem Element $x \in L$ geschrieben werden kann. Antwort gibt der *Satz vom primitiven Element* (d.h. erzeugenden Element), der besagt, dass dies unter der recht schwachen Voraussetzung der Separabilität der Fall ist.

13.1. **Separable Körpererweiterungen.**

Definition 13.1. Es sei K ein Körper. Ein Polynom $P \in K[X]$ heißt *separabel*, wenn es über keinem Erweiterungskörper $K \subseteq L$ mehrfache Nullstellen besitzt.

Lemma 13.2. *Es sei K ein Körper und sei $P \in K[X]$ ein Polynom. Dann sind die folgenden Aussagen äquivalent.*

(1) *P ist separabel.*
(2) *Es gibt eine Körpererweiterung $K \subseteq L$ derart, dass P über L in einfache Linearfaktoren zerfällt.*
(3) *P und die Ableitung P' sind teilerfremd.*
(4) *P und die Ableitung P' erzeugen das Einheitsideal.*

Beweis. (1) $\Rightarrow$ (2). Dies folgt aus Lemma 11.1. (2) $\Rightarrow$ (3). Nehmen wir an, dass P und P' einen gemeinsamen nichttrivialen Teiler in $K[X]$ besitzen. Dies ist dann auch in $L[X]$ der Fall. Dies bedeutet wiederum, dass ein Linearfaktor von P auch ein Teiler von P' ist. Daher besitzen P und P' eine gemeinsame Nullstelle und somit besitzt P eine mehrfache Nullstelle im Widerspruch zur Voraussetzung. (3) $\Rightarrow$ (4). Dies folgt aus Lemma 3.16. (4) $\Rightarrow$ (1). Sei $K \subseteq L$ eine Körpererweiterung, so dass $P \in L[X]$ in Linearfaktoren zerfällt. Nach Voraussetzung kann man 1 in $K[X]$ als Linearkombination von P und P' darstellen. Diese Eigenschaft überträgt sich direkt auf $L[X]$. Wenn P in L eine mehrfache Nullstelle hätte, so wäre diese Nullstelle auch eine Nullstelle der Ableitung. Das kann aber wegen der Darstellbarkeit der 1 nicht sein. $\square$

Definition 13.3. Eine endliche Körpererweiterung $K \subseteq L$ heißt *separabel*, wenn für jedes Element $x \in L$ das Minimalpolynom separabel ist.

Bemerkung 13.4. In Charakteristik 0 ist ein irreduzibles Polynom P stets separabel, da seine formale Ableitung P' nicht 0 ist und somit teilerfremd zu P ist. Da das Minimalpolynom zu einem Element nach Lemma 7.12 irreduzibel ist, ergibt sich, dass eine endliche Körpererweiterung in Charakteristik 0 separabel ist.

Lemma 13.5. *Es sei $K \subseteq L$ eine endliche separable Körpererweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann ist auch $M \subseteq L$ eine separable Körpererweiterung.*

Beweis. Siehe Aufgabe 13.5. □

Unser erstes wichtiges Ziel ist es, zu zeigen, dass eine endliche Körpererweiterung bereits dann separabel ist, wenn die Minimalpolynome zu einem Erzeugendensystem separabel sind.

Lemma 13.6. *Es sei $K \subseteq L = K[x] = K(x)$ eine endliche einfache Körpererweiterung vom Grad $d = \operatorname{grad}_K L$. Es sei $K \subseteq M$ eine Körpererweiterung, unter der das Minimalpolynom F von x in Linearfaktoren zerfällt. Dann ist F genau dann ein separables Polynom, wenn es d verschiedene K-Einbettungen von L in M gibt.*

Beweis. Es sei also $K \subseteq L = K[x] = K[X]/(F)$ vom Grad d mit dem Minimalpolynom F gegeben. Dieses Polynom F ist genau dann separabel, wenn es in M genau d Nullstellen besitzt. Diese Nullstellen stehen gemäß Satz 6.4 in Bijektion zu den K-Algebrahomomorphismen von $L = K[X]/(F)$ nach M. □

Lemma 13.7. *Es sei $K \subseteq L = K[x_1, \ldots, x_n]$ eine endliche Körpererweiterung vom Grad $d = \operatorname{grad}_K L$ mit der Eigenschaft, dass die Minimalpolynome $F_i \in K[X]$ zu den x_i separabel sind. Es sei $K \subseteq M$ eine Körpererweiterung, unter der die F_i in Linearfaktoren zerfallen. Dann gibt es d verschiedene K-Einbettungen von L in M.*

Beweis. Wir führen Induktion über n, bei $n = 0$ ist der Grad der Körpererweiterung gleich 1 und es gibt auch nur die K-Einbettung $K \subseteq M$. Sei die Aussage für n bewiesen. Wir betrachten die Körperkette

$$K \subseteq K' = K[x_1, \ldots, x_n] \subseteq K'[x_{n+1}] = L.$$

Wir wissen also, dass es $\operatorname{grad}_K K'$ verschiedene K-Einbettungen von K' nach M gibt. Aufgrund der Gradformel genügt es zu zeigen, dass es für $K' \subseteq K'[x_{n+1}] = L$ so viele K'-Einbettungen von L in M gibt, wie es der Körpergrad $\operatorname{grad}_{K'} L$ vorgibt. Es genügt also, den Fall $n = 1$ zu beweisen, und dieser folgt aus Lemma 13.6. □

Wir betonen die folgenden Korollare.

Korollar 13.8. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann gibt es genau n Einbettungen von L in die komplexen Zahlen $\mathbb{C}$.*

Beweis. Dies folgt unmittelbar aus Lemma 13.7 und Bemerkung 13.4. □

Korollar 13.9. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und $z \in L$ ein Element. Es seien*

$$\rho_1, \ldots, \rho_n \colon L \longrightarrow \mathbb{C}$$

die verschiedenen komplexen Einbettungen und es sei $M = \{z_1, \ldots, z_k\}$ die Menge der verschiedenen Werte $\rho_i(z)$. Dann gilt für das Minimalpolynom G von z die Gleichung

$$G = (X - z_1)(X - z_2) \cdots (X - z_k).$$

Beweis. Siehe Aufgabe 13.13. □

Korollar 13.10. *Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $\rho_i \colon L \to \mathbb{C}$ die n verschiedenen komplexen Einbettungen. Es sei $z \in L$ und $z_i = \rho_i(z)$, $i = 1, \ldots, n$. Dann ist*

$$N(z) = z_1 \cdots z_n \text{ und } S(z) = z_1 + \cdots + z_n \, .$$

Beweis. Siehe Aufgabe 13.14. □

Satz 13.11. *Es sei $K \subseteq L = K[x_1, \ldots, x_n]$ eine endliche Körpererweiterung. Es sei vorausgesetzt, dass die Minimalpolynome F_i der x_i separabel sind. Dann ist die Erweiterung $K \subseteq L$*

separabel.

Beweis. Wir führen Induktion über den Grad der Körpererweiterung, wobei der Grad 1 trivial ist. Es sei $x \in L$, $x \notin K$, mit Minimalpolynom $F \in K[X]$. Wir betrachten den zugehörigen Zwischenkörper

$$K \subseteq K[x] \cong K[X]/(F) \subseteq L,$$

wobei die Grade mit $d_1 = \operatorname{grad}_K K[x]$, $d_2 = \operatorname{grad}_{K[x]} L$ und mit $d = d_1 d_2 = \operatorname{grad}_K L$ bezeichnet seien. Es sei $K \subseteq M$ ein Körper, über dem F und die F_i in Linearfaktoren zerfallen. Wir betrachten die Abbildung

$$\Psi \colon \operatorname{Hom}_K(L, M) \longrightarrow \operatorname{Hom}_K(K[x], M),$$

wobei einfach der Definitionsbereich eingeschränkt wird. Nach Lemma 13.7 gibt es d verschiedene K-Algebrahomomorphismen von L nach M. Nach Induktionsvoraussetzung ist $K[x] \subseteq L$ eine separable Körpererweiterung vom Grad d_2 und daher gibt es nach Lemma 13.6 zu jedem fixierten K-Algebrahomomorphismus von $K[x]$ nach M genau d_2 K-Algebrahomomorphismen von L nach M, die diesen Homomorphismus fortsetzen. Die Anzahl der Elemente in den Fasern von Ψ ist also stets gleich d_2 und somit

besitzt das Bild $\mathrm{Hom}_K(K[x], M)$ genau d_1 Elemente. Also gibt es d_1 K-Algebrahomomorphismen von $K[x] \cong K[X]/(F)$ nach M und somit ist F, wiederum nach Lemma 13.6, ein separables Polynom. □

13.2. **Der Satz vom primitiven Element.**

Lemma 13.12. *Es sei $K \subseteq L = K(x)$ eine endliche einfache Körpererweiterung und $K \subseteq M \subseteq L$ ein Zwischenkörper. Es sei $G = \sum_{j=0}^{k} b_j X^j \in M[X]$ das Minimalpolynom von x über M. Dann ist $M = K(b_0, \ldots, b_k)$.*

Beweis. Wir gehen von der Inklusion $K' = K(b_0, \ldots, b_k) \subseteq M$ aus. Die Körpererweiterung $K' \subseteq L$ ist ebenfalls einfach mit dem Erzeuger x, und $G \in K'[X]$ ist irreduzibel, da es ja irreduzibel in $M[X]$ ist. Somit ist G nach Lemma 7.12 auch das Minimalpolynom von x über K'. Daher ist $L = M[X]/(G)$ und $L = K'[X]/(G)$ und insbesondere

$$\mathrm{grad}_M L = \mathrm{grad}(G) = \mathrm{grad}_{K'} L.$$

Nach der Gradformel, angewendet auf $K' \subseteq M \subseteq L$, folgt $K' = M$. □

Satz 13.13. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist $K \subseteq L$ genau dann eine einfache Körpererweiterung, wenn es nur endlich viele Zwischenkörper $K \subseteq M \subseteq L$ gibt.*

Beweis. Wenn K ein endlicher Körper ist, so ist auch L endlich und die Voraussetzung über die endlich vielen Zwischenkörper ist automatisch erfüllt. In diesem Fall ist aber auch nach Satz 9.6 die Körpererweiterung einfach. Wir können also annehmen, dass K unendlich ist. Sei zunächst vorausgesetzt, dass es in $K \subseteq L$ nur endlich viele Zwischenkörper gibt. Sei $\mathrm{grad}_K L = n$. Jeder von L verschiedene Zwischenkörper M_i, $i = 1, \ldots, k$, ist ein maximal $(n-1)$-dimensionaler K-Untervektorraum von L und daher gibt es eine von 0 verschiedene K-lineare Abbildung

$$\varphi_i \colon L \longrightarrow K$$

mit $\varphi_i(M_i) = 0$. Zu φ_i gehört ein lineares Polynom P_i (in n Variablen)[10] mit der entsprechenden Eigenschaft. Das Polynom $P = \prod_{i=1}^{k} P_i$ ist dann auf der Vereinigung aller Zwischenkörper $M_i \neq L$ gleich 0. Da K unendlich ist, gibt es aber nach Aufgabe 13.26 auch Elemente $a = (a_1, \ldots, a_n) \in L$ mit $P(a) \neq 0$. Der von einem solchen Element a über K erzeugte Körper muss gleich L sein, da er nach Konstruktion in keinem anderen Zwischenkörper liegt.

Sei nun

$$L = K(x) = K[x] = K[X]/(F)$$

[10] Man fixiert hierzu eine K-Basis von L, die zugehörige Dualbasis entspricht dann den n Variablen. Die folgende Tupelschreibweise bezieht sich ebenfalls auf die Basis.

eine einfache Körpererweiterung mit dem Minimalpolynom $F \in K[X]$. Für jeden Zwischenkörper M, $K \subseteq M \subseteq L$, ist $L = M(x)$ und das Minimalpolynom G von x über M ist in $M[X]$ und insbesondere in $L[X]$ ein Teiler von F. Nach Lemma 13.12 besteht die Beziehung $M = K(b_0, \ldots, b_k)$, wobei die b_j die Koeffizienten von G sind. Da F in $L[X]$ nur endlich viele (normierte) Teiler besitzt, gibt es nur endlich viele Zwischenkörper. □

Korollar 13.14. *Es sei $K \subseteq L$ eine endliche einfache Körpererweiterung und $K \subseteq M \subseteq L$ ein Zwischenkörper. Dann ist auch $K \subseteq M$ eine einfache Körpererweiterung.*

Beweis. Dies folgt unmittelbar aus Satz 13.13, da ja $K \subseteq M$ unter der Voraussetzung auch nur endlich viele Zwischenkörper besitzt. □

Der folgende Satz heißt *Satz vom primitiven Element.*

Satz 13.15. *Sei $K \subseteq L$ eine endliche separable Körpererweiterung. Dann wird L von einem Element erzeugt, d.h. es gibt ein $f \in L$ mit*

$$L = K(f) \cong K[X]/(P)$$

mit einem irreduziblen (Minimal-)Polynom $P \in K[X]$.

Beweis. Bei K endlich folgt die Aussage sofort aus Satz 9.6, wir können also K als unendlich annehmen. Es sei $K \subseteq L = K[x_1, \ldots, x_n]$. Es genügt zu zeigen, dass man sukzessive zwei Erzeuger davon durch einen Erzeuger ersetzen kann. Dabei ist $K \subseteq K[x_1, x_2]$ ebenfalls separabel. Sei also $L = K[x, y]$ gegeben und $n = \operatorname{grad}_K L$. Es sei $K \subseteq M$ eine Körpererweiterung, unter der die Minimalpolynome von x und von y in Linearfaktoren zerfallen. Es gibt gemäß Lemma 13.7 n K-Einbettungen

$$\sigma_1, \ldots, \sigma_n \colon L \longrightarrow M.$$

Wir betrachten das Polynom

$$P = \prod_{i \neq j} \left((\sigma_i(y) - \sigma_j(y))X + \sigma_i(x) - \sigma_j(x) \right),$$

das zu $M[X]$ gehört. Dies ist nicht das Nullpolynom, da keiner der Linearfaktoren gleich 0 ist. Daher besitzt P nur endlich viele Nullstellen und somit gibt es, da K unendlich ist, ein $c \in K$ mit $P(c) \neq 0$. Die Elemente $\sigma_i(x + cy) = \sigma_i(x) + c\sigma_i(y)$ sind alle verschieden. Aus $\sigma_i(x) + c\sigma_i(y) = \sigma_j(x) + c\sigma_j(y)$ für $i \neq j$ folgt nämlich $(\sigma_i(y) - \sigma_j(y))c + \sigma_i(x) - \sigma_j(x) = 0$, und c wäre doch eine Nullstelle von P. Es gibt also n verschiedene Einbettungen von $K(x + cy)$ nach M und insbesondere ist $\operatorname{grad}_K K(x + cy) \geq n$, also ist $K(x + cy) = L$. □

13. Arbeitsblatt

13.1. **Aufwärmaufgaben.**

Aufgabe 13.1. Sei $K \subseteq L$ eine endliche Körpererweiterung, deren Grad eine Primzahl sei. Zeige, dass dann eine einfache Körpererweiterung vorliegt.

Aufgabe 13.2. Es sei K ein Körper und $L = K(X)$ der Quotientenkörper des Polynomrings $K[X]$. Zeige, dass $K \subset L$ eine einfache, aber keine endliche Körpererweiterung ist.

Aufgabe 13.3. Es sei K ein Körper und $P \in K[X]$ ein separables Polynom. Zeige, dass ein Teiler $F \in K[X]$ von P ebenfalls separabel ist.

Aufgabe 13.4. Sei K ein Körper. Ist ein konstantes Polynom $P \in K[X]$ separabel?

Aufgabe 13.5.*

Es sei $K \subseteq L$ eine endliche separable Körpererweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Zeige, das auch $M \subseteq L$ eine separable Körpererweiterung ist.

Aufgabe 13.6. Es sei K ein Körper der Charakteristik p und sei $F \in K[X]$ ein irreduzibles Polynom, dessen Grad kein Vielfaches von p sei. Zeige, dass F separabel ist.

Aufgabe 13.7. Es sei K ein Körper der Charakteristik p und sei $X^p - a$, $a \in K$, ein irreduzibles Polynom. Zeige, dass die Körpererweiterung

$$K \subseteq K[x] = K[X]/(X^p - a)$$

nicht separabel ist.

Aufgabe 13.8. Es sei K ein Körper der Charakteristik p und sei $X^p - X - a$, $a \in K$, ein irreduzibles Polynom. Zeige, dass die Körpererweiterung

$$K \subseteq K[x] = K[X]/(X^p - X - a)$$

separabel ist.

Aufgabe 13.9. Es sei K ein Körper der Charakteristik p und sei $K \subseteq L$ eine Körpererweiterung, dessen Grad kein Vielfaches von p sei. Zeige, dass diese Körpererweiterung separabel ist.

Aufgabe 13.10. Es sei K ein Körper der Charakteristik p und sei $K \subseteq L$ eine D-graduierte Körpererweiterung. Zeige, dass diese Erweiterung genau dann separabel ist, wenn die Ordnung von D kein Vielfaches von p ist.

Aufgabe 13.11. Bestimme die Anzahl der $\mathbb{Q}$-Algebrahomomorphismen von $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$ nach $\mathbb{C}$.

Aufgabe 13.12. Es sei ζ eine primitive n-te komplexe Einheitswurzel. Bestimme die Anzahl der $\mathbb{Q}$-Algebrahomomorphismen von $\mathbb{Q}[\zeta]$ nach $\mathbb{C}$.

Aufgabe 13.13.*

Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und $z \in L$ ein Element. Es seien

$$\rho_1, \ldots, \rho_n \colon L \longrightarrow \mathbb{C}$$

die verschiedenen komplexen Einbettungen und es sei $M = \{z_1, \ldots, z_k\}$ die Menge der verschiedenen Werte $\rho_i(z)$. Zeige, dass dann für das Minimalpolynom G von z die Gleichung

$$G = (X - z_1)(X - z_2) \cdots (X - z_k)$$

gilt.

Aufgabe 13.14. Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $\rho_i \colon L \to \mathbb{C}$ die n verschiedenen komplexen Einbettungen. Es sei $z \in L$ und $z_i = \rho_i(z)$, $i = 1, \ldots, n$. Zeige, dass dann

$$N(z) = z_1 \cdots z_n \text{ und } S(z) = z_1 + \cdots + z_n$$

gilt.

Aufgabe 13.15. Diskutiere Lemma 13.12 für die Extremfälle $M = K$ und $M = L$.

Aufgabe 13.16. Diskutiere Lemma 13.12 für die Körpererweiterung

$$\mathbb{Z}/(5) \subseteq \mathbb{F}_{625} \cong \mathbb{Z}/(5)[X]/\left(X^4 - 2\right)$$

und den Zwischenkörper $\mathbb{F}_{25}$.

Aufgabe 13.17.*

Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq L := \mathbb{Q}[\mathrm{i}, \sqrt{2}] = \mathbb{Q}[\zeta_8]$$

mit $\zeta_8 = \frac{1}{2}\left(\sqrt{2} + \sqrt{2}\mathrm{i}\right)$. Bestimme die Minimalpolynome zu ζ_8 über den folgenden Zwischenkörpern M, $\mathbb{Q} \subseteq M \subseteq L$.

(1) $M = \mathbb{Q}$.
(2) $M = \mathbb{Q}[\mathrm{i}]$.
(3) $M = \mathbb{Q}[\sqrt{2}]$.
(4) $M = L$.

In den nächsten Aufgaben verwenden wir die folgende Definition.

Ein Körper K heißt *vollkommen*, wenn jedes irreduzible Polynom $P \in K[X]$ separabel ist.

Aufgabe 13.18. Es sei K ein vollkommener Körper und $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass $K \subseteq L$ eine separable Körpererweiterung ist.

Aufgabe 13.19. Zeige, dass jeder Körper der Charakteristik 0 vollkommen ist.

Aufgabe 13.20. Zeige, dass jeder algebraisch abgeschlossene Körper vollkommen ist.

Aufgabe 13.21. Zeige, dass ein endlicher Körper vollkommen ist.

Aufgabe 13.22.*

Es sei K ein Körper der Charakteristik p. Zeige, dass K genau dann vollkommen ist, wenn der Frobeniushomomorphismus auf K surjektiv ist.

Aufgabe 13.23. Zeige, dass der Körper $\mathbb{F}_p(X)$ der rationalen Funktionen nicht vollkommen ist.

Aufgabe 13.24. Man gebe ein Beispiel für eine endliche einfache Körpererweiterung $K \subseteq L$, die nicht separabel ist.

Aufgabe 13.25. Man gebe ein Beispiel für eine graduierte Körpererweiterung, die nicht einfach ist.

13.2. **Aufgaben zum Abgeben.**

Aufgabe 13.26. (6 Punkte)

Sei K ein unendlicher Körper und sei $F \in K[X_1, \ldots, X_n]$ ein von 0 verschiedenes Polynom. Zeige, dass dann die zugehörige Polynomfunktion

$$F\colon\ K^n \longrightarrow K,\ (a_1, \ldots, a_n) \longmapsto F(a_1, \ldots, a_n),$$

nicht die Nullfunktion ist.

Aufgabe 13.27. (3 Punkte)

Es sei K ein Körper und $L = K(X)$ der Quotientenkörper des Polynomrings $K[X]$. Zeige, dass es unendlich viele Zwischenkörper zwischen K und L gibt.

Aufgabe 13.28. (3 Punkte)

Es sei K ein Körper und $L = K(X)$ der Quotientenkörper des Polynomrings $K[X]$. Es sei M, $K \subseteq M \subseteq L$, $M \neq K$, ein Zwischenkörper. Zeige, dass $M \subseteq L$ eine endliche Körpererweiterung ist.

Aufgabe 13.29. (5 Punkte)

Es sei K ein Körper der positiven Charakteristik p. Wir betrachten die Körpererweiterung

$$K(X^p, Y^p) \subseteq K(X, Y)\,.$$

Zeige, dass dies keine einfache Körpererweiterung ist.

14. Vorlesung - Galoiserweiterungen

14.1. **Automorphismen und Nullstellen.**

Beispiel 14.1. Wir betrachten den Zerfällungskörper L zum Polynom $X^8 - 1$, also den achten Kreisteilungskörper. Er wird von einer primitiven achten Einheitswurzel ζ erzeugt und besitzt nach Beispiel 12.9 die Darstellungen

$$L\ =\ \mathbb{Q}[\zeta]/\left(\zeta^4 + 1\right)\ =\ \mathbb{Q}[\sqrt{2}, \mathrm{i}].$$

Die Nullstellen von $X^8 - 1$ sind die acht verschiedenen Einheitswurzeln, die die Potenzen von ζ sind. Die primitiven Einheitswurzeln besitzen allesamt das Minimalpolynom $X^4 + 1$. Die $\mathbb{Q}$-Automorphismen

$$\varphi\colon\ L \longrightarrow L$$

führen die achten Einheitswurzeln ineinander über, und zwar werden primitive Einheitswurzeln auf primitive Einheitswurzeln angebildet. Die komplexe Konjugation bildet ζ auf ζ^7 und ζ^3 auf ζ^5 und $\zeta^2 = \mathrm{i}$ auf $\zeta^6 = -\mathrm{i}$ ab. Der durch $\sqrt{2} \mapsto -\sqrt{2}$ und $\mathrm{i} \mapsto \mathrm{i}$ gegebene Automorphismus (vergleiche Lemma

12.15) $\zeta = \frac{1}{2}\left(\sqrt{2}+\sqrt{2}\mathrm{i}\right)$ bildet ζ auf ζ^5 und ζ^3 auf ζ^7 ab. In jedem Fall induziert jeder Automorphismus eine Permutation der achten Einheitswurzeln, also der Nullstellen des Polynoms X^8-1.

Lemma 14.2. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von F. Es seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von F in L. Dann gibt es einen natürlichen injektiven Gruppenhomomorphismus*

$$\mathrm{Gal}\,(L|K) \longrightarrow S(\{\alpha_1, \ldots, \alpha_n\})$$

der Galoisgruppe in die Permutationsgruppe der Nullstellen.

Beweis. Sei $\varphi \in \mathrm{Gal}\,(L|K)$. Nach Lemma 10.15 ist $\varphi(\alpha_i)$ wieder eine Nullstelle von F, daher muss $\varphi\,(\alpha_i) = \alpha_j$ für ein gewisses j sein. Dies definiert ein Abbildung der Nullstellenmenge in sich selbst. Da φ injektiv ist, ist auch diese induzierte Abbildung injektiv, also nach Lemma 10.5 (Analysis (Osnabrück 2014-2016)) bijektiv und somit eine Permutation. Die Gesamtzuordnung ist offenbar ein Gruppenhomomorphismus. Da die Nullstellen ein Erzeugendensystem des Zerfällungskörpers bilden, liegt nach Lemma 10.14 ein injektiver Homomorphismus vor. □

Beispiel 14.3. Nach Beispiel 11.2 ist

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3-3X+1\right) =: L$$

eine Körpererweiterung vom Grad 3 und dabei sind, wenn man die Restklasse von X in L mit α bezeichnet, neben α auch $\beta = \alpha^2-2$ und $\gamma = -\alpha^2-\alpha+2$ Nullstellen der definierenden Gleichung. Somit besitzen die Elemente α, β, γ das Minimalpolynom X^3-3X+1. Durch

$$\varphi\colon\ L = \mathbb{Q}[X]/\left(X^3-3X+1\right) \longrightarrow L = \mathbb{Q}[X]/\left(X^3-3X+1\right),\ X \longmapsto \beta,$$

wird ein nichtidentischer $\mathbb{Q}$-Algebraautomorphismus auf L festgelegt. Dieser sendet α auf β, β wegen

$$\begin{aligned}
\varphi(\beta) &= \varphi(\alpha^2-2)\\
&= \beta^2-2\\
&= (\alpha^2-2)^2-2\\
&= \alpha^4-4\alpha^2+4-2\\
&= \alpha\,(3\alpha-1)-4\alpha^2+2\\
&= -\alpha^2-\alpha+2\\
&= \gamma
\end{aligned}$$

auf γ und γ aufgrund einer ähnlichen Rechnung zurück auf α. Die einzigen Automorphismen $\mathrm{Id}, \varphi, \varphi^2$ entsprechen also den geraden Permutationen $\mathrm{Id}, \alpha \mapsto \beta \mapsto \gamma \mapsto \alpha, \alpha \mapsto \gamma \mapsto \beta \mapsto \alpha$ auf der Nullstellenmenge $\{\alpha, \beta, \gamma\}$.

Definition 14.4. Es sei K ein Körper und A eine kommutative K-Algebra. Zwei über K algebraische Elemente $\alpha, \beta \in A$ heißen *konjugiert*, wenn ihre Minimalpolynome übereinstimmen.

Satz 14.5. *Es sei $K \subseteq L$ eine endliche Körpererweiterung und es seien α und β konjugierte Elemente aus L. Es sei L der Zerfällungskörper des gemeinsamen Minimalpolynoms F dieser beiden Elemente. Dann gibt es einen K-Algebraautomorphismus φ von L mit $\varphi(\alpha) = \beta$.*

Beweis. Zunächst gibt es wegen

$$K[\alpha] \cong K[X]/(F) \cong K[\beta]$$

einen K-Algebrahomomorphismus φ von $K[\alpha]$ nach $K[\beta]$. Der Körper L ist über diesen beiden Unterkörpern der Zerfällungskörper von F. Daher gibt es nach Satz 11.6 einen K-Algebraautomorphismus von L nach L, der φ fortsetzt. □

14.2. **Das Lemma von Dedekind.**

Die Menge der Charaktere auf einem Monoid G in einen Körper K, also $\mathrm{Char}\,(G, K)$, ist selbst ein Monoid, und zwar ein Untermonoid des Abbildungsmonoids von G nach $K^\times$. Da Charaktere insbesondere Abbildungen von G nach K sind, kann man von Linearkombinationen von Charakteren sprechen. Diese sind im Allgemeinen keine Charaktere mehr. Es gilt die folgende bemerkenswerte Aussage, das *Lemma von Dedekind*.

Richard Dedekind (1831-1916)

Satz 14.6. *Es sei G ein Monoid, K ein Körper und*

$$\chi_1, \ldots, \chi_n \in \mathrm{Char}\,(G, K)$$

seien n Charaktere. Dann sind diese Charaktere linear unabhängig (als Elemente in $\mathrm{Abb}\,(G, K)$*).*

Beweis. Es sei

$$a_1\chi_1 + \cdots + a_n\chi_n = 0,$$

wobei die χ_i verschiedene Charaktere seien und alle $a_i \in K$ von 0 verschieden seien. Darüber hinaus sei n minimal gewählt mit dieser Eigenschaft. Wegen $\chi(e_G) = 1$ ist ein einzelner Charakter nicht die Nullabbildung, also linear unabhängig und somit ist zumindest $n \geq 2$. Wegen $\chi_1 \neq \chi_2$ gibt es auch ein $g \in G$ mit

$\chi_1(g) \neq \chi_2(g)$. Wir behaupten die Gleichheit (wieder von Abbildungen von G nach K)

$$a_1\chi_1(g)\chi_1 + \cdots + a_n\chi_n(g)\chi_n = 0.$$

Für ein beliebiges $h \in G$ ist nämlich

$$\begin{aligned}(a_1\chi_1(g)\chi_1 + \cdots + a_n\chi_n(g)\chi_n)(h) &= a_1\chi_1(g)\chi_1(h) + \cdots + a_n\chi_n(g)\chi_n(h)\\ &= a_1\chi_1(g\cdot h) + \cdots + a_n\chi_n(g\cdot h)\\ &= 0\end{aligned}$$

wegen der Ausgangsgleichung. Wenn man vom $\chi_1(g)$-fachen der Ausgangsgleichung die zweite Gleichung abzieht, so kann man χ_1 elimineren und erhält eine nichttriviale (wegen $a_2 \neq 0$ und der Wahl von g) lineare Relation zwischen $\chi_2, \ldots, \chi_n$ im Widerspruch zur Minimalitätseigenschaft von n. □

14.3. **Galoiserweiterungen.**

Aus dem Lemma von Dedekind ergibt sich eine direkte Abschätzung zwischen der Ordnung der Galoisgruppe und dem Grad einer endlichen Körpererweiterung.

Satz 14.7. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist*

$$\#(\mathrm{Gal}\,(L|K)) \leq \mathrm{grad}_K\, L.$$

Beweis. Nach Satz 10.16 ist $\#(\mathrm{Gal}\,(L|K))$ endlich. Wir setzen

$$m = \#(\mathrm{Gal}\,(L|K))$$

und $n = \mathrm{grad}_K\, L$ und müssen $m \leq n$ zeigen. Nehmen wir also $m > n$ an. Es sei $v_1, \ldots, v_n$ eine K-Basis von L und die Elemente in der Galoisgruppe seien $\varphi_1, \ldots, \varphi_m$. Wir betrachten die Matrix

$$\begin{pmatrix}\varphi_1(v_1) & \cdots & \varphi_m(v_1)\\ \vdots & \ddots & \vdots\\ \varphi_1(v_n) & \cdots & \varphi_m(v_n)\end{pmatrix}.$$

Ihr Rang ist maximal gleich n, da sie nur n Zeilen besitzt. Daher gibt es eine nichttriviale Relation zwischen den m Spalten, sagen wir

$$b_1\begin{pmatrix}\varphi_1(v_1)\\ \vdots\\ \varphi_1(v_n)\end{pmatrix} + \cdots + b_m\begin{pmatrix}\varphi_m(v_1)\\ \vdots\\ \varphi_m(v_n)\end{pmatrix} = 0,$$

wobei nicht alle b_j gleich 0 sind. Wir betrachten nun

$$\sum_{j=1}^{m} b_j \varphi_j \,,$$

wobei wir die Automorphismen φ_j als Charaktere von $L^\times$ nach $L^\times$ auffassen. Für ein beliebiges Element $v \in L$ schreiben wir $v = \sum_{i=1}^{n} a_i v_i$. Mit diesen Bezeichnungen gilt

$$\begin{aligned}
\left(\sum_{j=1}^{m} b_j \varphi_j\right)(v) &= \left(\sum_{j=1}^{m} b_j \varphi_j\right)\left(\sum_{i=1}^{n} a_i v_i\right) \\
&= \sum_{j=1}^{m} b_j \left(\varphi_j \left(\sum_{i=1}^{n} a_i v_i\right)\right) \\
&= \sum_{j=1}^{m} b_j \left(\sum_{i=1}^{n} a_i \varphi_j(v_i)\right) \\
&= \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{m} b_j \varphi_j(v_i)\right) \\
&= 0,
\end{aligned}$$

da ja wegen der obigen linearen Abhängigkeit die Zeilensummen

$$\sum_{j=1}^{m} b_j \varphi_j(v_i) \;=\; 0$$

sind für jedes i. Also liegt eine nicht-triviale Relation zwischen Charakteren vor, was nach Satz 14.6 nicht sein kann. □

Eine wichtige Frage ist, wann in der vorstehenden Abschätzung Gleichheit vorliegt, wann es also so viele Automorphismen wie möglich gibt. Dies machen wir zur Grundlage der folgenden Definition. Wir werden später noch viele äquivalente Eigenschaften kennenlernen.

Definition 14.8. Sei $K \subseteq L$ eine endliche Körpererweiterung. Sie heißt eine *Galoiserweiterung*, wenn

$$\#(\mathrm{Gal}\,(L|K)) \;=\; \mathrm{grad}_K\, L$$

gilt.

Lemma 14.9. *Es sei K ein Körper mit einer Charakteristik $\neq 2$ und sei $K \subseteq L$ eine quadratische Körpererweiterung. Dann ist $K \subseteq L$ eine Galoiserweiterung.*

Beweis. Siehe Aufgabe 14.13. □

Die vorstehende Aussage ist ein Spezialfall der Aussage, dass graduierte Körpererweiterungen unter der Voraussetzung, dass hinreichend viele Einheitswurzeln im Grundkörper vorhanden sind, Galois-Erweiterungen sind. Dazu brauchen wir ein vorbereitendes Lemma.

Lemma 14.10. *Es sei G eine endliche kommutative Gruppe mit dem Exponenten m, und es sei K ein Körper, der eine primitive m-te Einheitswurzel besitzt. Dann sind G und $G^\vee$ isomorphe*[11] *Gruppen.*

Beweis. Nach Lemma 12.14 (2) und Satz Anhang 4.2. kann man annehmen, dass $G = \mathbb{Z}/(n)$ eine endliche zyklische Gruppe ist, und dass K eine n-te primitive Einheitswurzel besitzt. Jeder Gruppenhomomorphismus

$$\varphi\colon G \longrightarrow K^\times$$

ist durch $\zeta = \varphi(1)$ eindeutig festgelegt, und wegen

$$\zeta^n = (\varphi(1))^n = \varphi(n) = \varphi(0) = 1$$

ist ζ eine n-te Einheitswurzel. Umgekehrt kann man zu jeder n-ten Einheitswurzel ζ durch die Zuordnung $1 \mapsto \zeta$ nach Lemma 4.4 und Satz 5.10 einen Gruppenhomomorphismus von $\mathbb{Z}/(n)$ nach $K^\times$ definieren. Die Menge der n-ten Einheitswurzeln ist, da eine primitive Einheitswurzel vorhanden ist, eine zyklische Gruppe der Ordnung n. Also gibt es n solche Homomorphismen. Wenn ζ eine primitive Einheitswurzel ist, dann besitzt der durch $1 \mapsto \zeta$ festgelegte Homomorphismus die Ordnung n und ist damit ein Erzeuger der Charaktergruppe, also $(\mathbb{Z}/(n))^\vee \cong \mathbb{Z}/(n)$. □

Satz 14.11. *Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Der Körper K enthalte eine m-te primitive Einheitswurzel, wobei m der Exponent von D sei. Dann ist $K \subseteq L$ eine Galoiserweiterung mit Galoisgruppe $D^\vee = \mathrm{Char}\,(D, K)$.*

Beweis. Die Voraussetzung über die primitiven Einheitswurzeln in Verbindung mit Lemma 14.10 und Lemma 12.10 (2) sichern

$$\#(D^\vee) = \#(D) = \mathrm{grad}_K\, L.$$

Nach Lemma 12.15 ist

$$\#(D^\vee) \leq \#(\mathrm{Gal}\,(L|K)).$$

Also ist

$$\mathrm{grad}_K\, L \leq \#(\mathrm{Gal}\,(L|K)),$$

und somit haben wir nach Satz 14.7 hier Gleichheit, also liegt eine Galoiserweiterung vor. Damit ist auch der nach Lemma 12.15 injektive Gruppenhomomorphismus

$$D^\vee \longrightarrow \mathrm{Gal}\,(L|K)$$

bijektiv. □

[11] Diese Isomorphie ist nicht kanonisch, es gibt keine natürliche Beziehung zwischen den Elementen aus G und den Charaktern auf G.

Beispiel 14.12. Sei $n \in \mathbb{N}_+$ und sei K ein Körper, der eine n-te primitive Einheitswurzel enthält. Es sei $a \in K$ derart, dass das Polynom $X^n - a$ irreduzibel sei. Dann ist

$$K \subseteq L = K[X]/(X^n - a)$$

eine nach Beispiel 9.5 $D = \mathbb{Z}/(n)$-graduierte Körpererweiterung, und nach Satz 14.11 handelt es sich um eine Galoiserweiterung mit Galoisgruppe

$$\mathrm{Gal}(L|K) = D^\vee \cong \mathbb{Z}/(n).$$

Dabei ist L auch der Zerfällungskörper von $X^n - a$. Wenn x die Restklasse von X bezeichnet, so sind die n verschiedenen Nullstellen dieses Polynoms gleich

$$\zeta x \text{ mit } \zeta \in \mu_n(K) = \{z \in K | \, z^n = 1\},$$

die allesamt homogene Elemente der Stufe $1 \in D$ sind. Ein Charakter $\chi \in D^\vee$ bzw. der zugehörige Automorphismus φ_χ operiert gemäß Lemma 14.2 auf dieser Nullstellenmenge M (die nichtkanonisch isomorph zu $\mu_n(K)$ ist) durch

$$\varphi_\chi \colon M \longrightarrow M, \, \zeta x \longmapsto \chi(1)\zeta x.$$

Die graduierende Gruppe D, sein Charakterdual $D^\vee$, die Gruppe der n-ten Einheitswurzeln $\mu_n(K)$, die Galoisgruppe $\mathrm{Gal}(L|K)$ und die Nullstellenmenge M bestehen aus n Elementen, die Permutationsgruppe von M besteht somit aus $n!$ Elementen. Zu je zwei Nullstellen $x_1 = \zeta_1 x$ und $x_2 = \zeta_2 x$ gibt es einen eindeutigen Charakter bzw. Automorphismus, dessen zugehörige Permutation x_1 in x_2 überführt, nämlich derjenige Charakter χ mit $\chi(1) = \zeta_2 \zeta_1^{-1}$.

Bei $K = \mathbb{Q}$ und $L = \mathbb{Q}[\mathrm{i}] = \mathbb{Q}[X]/(X^2 + 1)$ sind $M = \{\mathrm{i}, -\mathrm{i}\}$ die beiden Nullstellen und der nichtkonstante Charakter vertauscht die beiden Nullstellen. Wegen $2! = 2$ rührt jede Permutation von einem Automorphismus bzw. einem Charakter her.

Bei $K = \mathbb{Q}[\mathrm{i}]$ und $X^4 - 3 \in K[X]$ ist $L = K[X]/(X^4 - 3)$ eine $\mathbb{Z}/(4)$-graduierte Körpererweiterung. Die vier Nullstellen sind $\sqrt[4]{3}$, $-\sqrt[4]{3}$, $\mathrm{i}\sqrt[4]{3}$ und $-\mathrm{i}\sqrt[4]{3}$. Die Irreduzibilität von $X^4 - 3$ ergibt sich dadurch, dass das Produkt von je zwei Linearfaktoren nicht zu $K[X]$ gehört. Jeder Charakter χ ist durch $\chi(1)$ bestimmt und die zugehörige Permutation auf der Nullstellenmenge ist die Multiplikation mit $\chi(1)$. Bei $\chi(1) = -1$ ist das die Permutation $\sqrt[4]{3} \leftrightarrow -\sqrt[4]{3}$, $\mathrm{i}\sqrt[4]{3} \leftrightarrow -\mathrm{i}\sqrt[4]{3}$, bei $\chi(1) = \mathrm{i}$ ist das die Permutation $\sqrt[4]{3} \mapsto \mathrm{i}\sqrt[4]{3} \mapsto -\sqrt[4]{3} \mapsto -\mathrm{i}\sqrt[4]{3}$ und bei $\chi(1) = -\mathrm{i}$ ist das die Permutation $\sqrt[4]{3} \mapsto -\mathrm{i}\sqrt[4]{3} \mapsto -\sqrt[4]{3} \mapsto \mathrm{i}\sqrt[4]{3}$. Unter den 24 Permutationen rühren also nur 4 von einem Charakter her, eine Permutation wie $\sqrt[4]{3} \leftrightarrow \sqrt[4]{3}$, $-\sqrt[4]{3} \leftrightarrow -\sqrt[4]{3}$, und $\mathrm{i}\sqrt[4]{3} \leftrightarrow -\mathrm{i}\sqrt[4]{3}$ z.B. nicht.

14. Arbeitsblatt

14.1. **Aufwärmaufgaben.**

Aufgabe 14.1. Interpretiere Lemma 14.2 für den Fall einer quadratischen Körpererweiterung.

Aufgabe 14.2. Es sei $\mathbb{Q} \subseteq L$ der Zerfällungskörper von X^n-1, also der n-te Kreisteilungskörper über $\mathbb{Q}$ und es sei G die Galoisgruppe der Erweiterung. Zeige, dass bei n ungerade ein natürlicher injektiver Gruppenhomomorphismus $G \to S_{n-1}$ und bei n gerade ein natürlicher injektiver Gruppenhomomorphismus $G \to S_{n-2}$ vorliegt.

Aufgabe 14.3.*

(1) Bestimme die Zerlegung von $X^4 - 7$ in $\mathbb{C}$.
(2) Bestimme den Zerfällungskörper L von $X^4 - 7 \in \mathbb{Q}[X]$.
(3) Bestimme den Grad der Körpererweiterung $\mathbb{Q} \subseteq L$.
(4) Beschreibe, welche Permutationen auf der Nullstellenmenge von $X^4 - 7$ von der Galoisgruppe herrühren.

Aufgabe 14.4. Sei $K \subseteq L$ eine endliche Körpererweiterung mit Galoisgruppe $G = \mathrm{Gal}\,(L|K)$ und sei $K \subseteq M$ eine weitere Körpererweiterung. Es sei E die Menge der K-Algebrahomomorphismen von L nach M. Zeige, dass die Zuordung

$$G \longrightarrow \mathrm{Perm}\,(E),\ \varphi \longmapsto (\iota \mapsto \iota \circ \varphi),$$

ein Gruppenhomomorphismus ist.

Aufgabe 14.5. Es sei M eine Menge und G eine Untergruppe der Menge aller Bijektionen von M nach M. Es sei $T \subseteq M$ eine Teilmenge mit der Eigenschaft, dass jedes $\varphi \in G$ die Menge T in sich selbst überführt. Zeige, dass die Abbildung

$$\psi\colon\ G \longrightarrow \mathrm{Perm}\,(T),\ \varphi \longmapsto \varphi|_T,$$

ein Gruppenhomomorphismus ist. Man gebe Beispiel für solche Situationen, wo ψ (nicht) injektiv, (nicht) surjektiv ist.

Aufgabe 14.6. Zeige, dass jede Isometrie des $\mathbb{R}^n$ eine Selbstabbildung der $(n-1)$-dimensionalen Sphäre

$$S^{n-1} = \{P \in \mathbb{R}^n |\ ||P|| = 1\}$$

induziert.

Aufgabe 14.7. Beschreibe die Wirkungsweise der eigentlichen Würfelgruppe auf der Menge der Ecken, der Kantenmenge, der Menge der Seitenmittelpunkte, der Raumdiagonalen durch geeignete Gruppenhomorphismen.

Aufgabe 14.8. Betrachte die Menge $\mu_4(\mathbb{C})$ der vierten Einheitswurzeln in $\mathbb{C}$. Welche sind untereinander über $\mathbb{Q}$ konjugiert?

Aufgabe 14.9.*

Es sei $K \subseteq L$ eine endliche Körpererweiterung und seien $f, g \in L$ konjugierte Elemente. Zeige, dass dann $N(f) = N(g)$ und $S(f) = S(g)$ gilt.

Aufgabe 14.10. Sei $n \in \mathbb{N}_+$. Zeige, dass die n Vektoren (im $\mathbb{C}^n$)

$$(1, \zeta, \zeta^2, \ldots, \zeta^{n-1}), \zeta \in \mu_n(\mathbb{C}),$$

linear unabhängig sind.

Aufgabe 14.11. Begründe mit dem Lemma von Dedekind, dass die reelle Matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

den Rang 4 besitzt.

Aufgabe 14.12. Sei $n \in \mathbb{N}_+$ und sei $\zeta = e^{\frac{2\pi \mathrm{i}}{n}}$. Berechne die Determinante der $(n \times n)$-Matrix

$$((\zeta^{r+s})_{0 \leq r,s \leq n-1})$$

für $n = 1, 2, 3, 4$.

Aufgabe 14.13. Es sei K ein Körper mit einer Charakteristik $\neq 2$ und sei $K \subseteq L$ eine quadratische Körpererweiterung. Zeige, dass $K \subseteq L$ eine Galoiserweiterung ist.

Aufgabe 14.14. Zeige, dass die quadratische Körpererweiterung $\mathbb{F}_2 \subseteq \mathbb{F}_4$ eine Galoiserweiterung ist.

Aufgabe 14.15. Zeige, dass die quadratische Körpererweiterung $\mathbb{F}_2(X) \subseteq \mathbb{F}_2(X)[T]/(T^2 - X)$ keine Galoiserweiterung ist.

Aufgabe 14.16. Sei $K \subseteq L$ eine endliche Körpererweiterung und sei $\mu_n(L)$ (zu $n \in \mathbb{N}_+$) die Gruppe der n-ten Einheitswurzeln in L. Zeige, dass es zu jedem n einen natürlichen Gruppenhomomorphismus

$$\operatorname{Gal}(L|K) \longrightarrow \operatorname{Aut}(\mu_n(L))$$

gibt.

Bei einer endlichen Körpererweiterung $K \subseteq L$ kann man jeden K-Algebraautomorphismus von L - also jedes Element der Galoisgruppe - als eine bijektive K-lineare Abbildung

$$L \cong K^n \longrightarrow L \cong K^n$$

auffassen und kann daher die Begriffe der linearen Algebra darauf anwenden. Damit hat man insbesondere den Begriff der Determinante zur Verfügung.

Aufgabe 14.17. Sei $K \subseteq L$ eine endliche Körpererweiterung mit Galoisgruppe $G = \operatorname{Gal}(L|K)$. Zeige, dass die Abbildung

$$G \longrightarrow K^\times,\ \varphi \longmapsto \det \varphi,$$

ein Gruppenhomomorphismus ist.

Aufgabe 14.18. Sei D eine endliche kommutative Gruppe mit der zugehörigen Charaktergruppe $D^\vee$ in einen Körper K. Zeige, dass die Abbildung

$$D^\vee \longrightarrow K^\times,\ \chi \longmapsto \prod_{d \in D} \chi(d),$$

ein Gruppenhomomorphismus ist.

14.2. **Aufgaben zum Abgeben.**

Aufgabe 14.19. (3 Punkte)

Es sei K ein Körper und sei

$$\varphi\colon\ K \longrightarrow K$$

ein Körperautomorphismus. Zeige, dass die Abbildung

$$K[X] \longrightarrow K[X],\ \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} \varphi(a_i) X^i,$$

ein Ringautomorphismus des Polynomrings $K[X]$ ist.

Aufgabe 14.20. (2 Punkte)

Sei D eine endliche kommutative Gruppe und sei $K \subseteq L$ eine D-graduierte Körpererweiterung. Beweise für $\chi \in D^\vee$ die Gleichheit

$$\prod_{d \in D} \chi(d) \ = \ \det \varphi_\chi,$$

wobei φ_χ den zugehörigen K-Automorphismus von L bezeichnet (siehe Lemma 12.15).

Aufgabe 14.21. (2 Punkte)

Betrachte die Menge $\mu_8(\mathbb{C})$ der achten Einheitswurzeln in $\mathbb{C}$. Welche sind untereinander über $\mathbb{Q}$ konjugiert?

Aufgabe 14.22. (5 Punkte)

Sei D eine endliche zyklische Gruppe der Ordnung n mit der zugehörigen Charaktergruppe $D^\vee$ mit Werten in einem Körper K.

a) Zeige, dass der Gruppenhomomorphismus

$$\psi\colon \ D^\vee \longrightarrow K^\times, \, \chi \longmapsto \prod_{d \in D} \chi(d),$$

nur die Werte 1 und -1 annehmen kann.

b) Es sei vorausgesetzt, dass K eine n-te primitive Einheitswurzel enthält. Zeige, dass ψ genau dann den Wert -1 annimmt, wenn n gerade ist.

Aufgabe 14.23. (3 Punkte)

Es sei $q \in \mathbb{Q}$ eine rationale Zahl, die in $\mathbb{Q}$ keine dritte Wurzel besitzt, so dass $\mathbb{Q} \subseteq L = \mathbb{Q}[X]/(X^3 - q)$ eine Körpererweiterung vom Grad 3 ist. Zeige, dass das Polynom $X^3 - q$ in L genau eine Nullstelle hat und dass diese Körpererweiterung nicht galoissch ist.

15. Vorlesung - Normale Körpererweiterungen

15.1. **Normale Körpererweiterungen.**

Ein irreduzibles Polynom $F \in K[X]$ hat in dem Erweiterungskörper

$$K \ \subseteq \ L \ := \ K[X]/(F)$$

eine Nullstelle, nämlich die Restklasse x von X und damit in $L[X]$ auch den Linearfaktor $X - x$. Es besteht aber kein Grund, warum das Polynom F über L in Linearfaktoren zerfallen sollte. Vielmehr handelt es sich um eine erweiterungstheoretische Besonderheit, wenn mit einer Nullstelle bereits schon alle Nullstellen vollzählig vorhanden sind.

Definition 15.1. Eine Körpererweiterung $K \subseteq L$ heißt *normal*, wenn es zu jedem $x \in L$ ein Polynom $F \in K[X]$, $F \neq 0$, mit $F(x) = 0$ gibt, das über L zerfällt.

Eine normale Körpererweiterung ist insbesondere algebraisch. Wir werden gleich noch dazu äquivalente Eigenschaften kennenlernen. Einfache Eigenschaften von normalen Erweiterungen werden im folgenden Lemma zusammengefasst.

Lemma 15.2. (1) *Die Identität ist eine normale Körpererweiterung.*
(2) *Jede quadratische Körpererweiterung ist normal.*
(3) *Wenn $K \subseteq L$ eine normale Körpererweiterung ist und $K \subseteq M \subseteq L$ ein Zwischenkörper, so ist auch $M \subseteq L$ normal.*
(4) *Eine Erweiterung von endlichen Körpern ist normal.*

Beweis. (1) ist trivial. (2). Sei $x \in L$ mit dem Minimalpolynom F, das den Grad 1 oder 2 besitzt. In $L[X]$ besitzt F einen Linearfaktor, der andere Faktor ist wegen der Gradbedingung konstant oder auch ein Linearfaktor. (3). Zu jedem $x \in L$ gibt es ein Polynom $F \in K[X]$, $F \neq 0$, mit $F(x) = 0$, das über $L[X]$ zerfällt. Wegen $K[X] \subseteq M[X]$ gilt diese Eigenschaft auch für $M \subseteq L$. (4). Nach (3) können wir sofort eine Körpererweiterung $\mathbb{Z}/(p) \subseteq \mathbb{F}_q$ mit einer Primzahl p und einer Primzahlpotenz $q = p^e$ betrachten. Jedes Element $x \in \mathbb{F}_q$ ist nach dem Satz von Lagrange eine Nullstelle des Polynoms $X^q - X$, so dass dieses Polynom über $\mathbb{F}_q$ zerfällt. □

Beispiel 15.3. Das Polynom $X^3 - 3X + 1 \in \mathbb{Q}[X]$ ist irreduzibel nach Aufgabe 3.16 und definiert daher eine Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

vom Grad 3. Die Restklasse von X in L sei mit α bezeichnet. Nach Aufgabe 11.7 sind auch die Elemente aus L

$$\beta = \alpha^2 - 2$$

und

$$\gamma = -\alpha^2 - \alpha + 2$$

Nullstellen der definierenden Gleichung und daher zerfällt das Polynom bereits über L. Daher ist die Körpererweiterung normal nach Satz 15.4 (3).

Satz 15.4. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent.*

(1) *Die Körpererweiterung ist normal.*
(2) *Wenn ein irreduzibles Polynom $P \in K[X]$ eine Nullstelle in L besitzt, so zerfällt es in $L[X]$.*
(3) *Es gibt ein K-Algebraerzeugendensystem $x_i \in L$, $i \in I$, von L und über L zerfallende Polynome $F_i \in K[X]$, $F_i \neq 0$, $i \in I$, mit $F_i(x_i) = 0$.*

(4) *Für jede Körpererweiterung $L \subseteq M$ und jeden K-Algebrahomomorphismus*

$$\varphi\colon L \longrightarrow M$$

ist $\varphi(L) \subseteq L$.

Beweis. (1) $\Rightarrow$ (2). Sei $P \in K[X]$ irreduzibel und $P(x) = 0$. Dann ist P nach Lemma 7.12 das Minimalpolynom zu x. Nach (1) gibt es ein über L zerfallendes Polynom F mit $F(x) = 0$. Da F ein Vielfaches von P ist, muss auch P über L zerfallen. (2) $\Rightarrow$ (1). Zu $x \in L$ gehört das Minimalpolynom P, das nach Lemma 7.12 irreduzibel ist und nach Voraussetzung (2) über L in Linearfaktoren zerfällt. (2) $\Rightarrow$ (3). Die Familie aller Elemente mit ihren Minimalpolynomen besitzt diese Eigenschaft. (3) $\Rightarrow$ (4). Seien $L \subseteq M$ und $\varphi\colon L \to M$ gegeben. Sei $x_i \in L$ ein Element aus der erzeugenden Familie und sei $F_i \neq 0$ das zugehörige zerfallende Polynom mit $F_i(x) = 0$, das wir als irreduzibel annehmen dürfen. Es ist

$$F_i(\varphi(x_i)) = \varphi(F_i(x_i)) = \varphi(0) = 0,$$

daher ist $\varphi(x_i) \in M$ eine Nullstelle des über L zerfallenden Polynoms F_i. Das heißt aber, dass $\varphi(x_i) \in L$ ist. Diese Zugehörigkeit gilt dann für alle $x \in L$, da sie für ein Algebraerzeugendensystem gilt. (4) $\Rightarrow$ (2). Sei $P \in K[X]$ irreduzibel und sei $x \in L$ mit $P(x) = 0$. Wir können nach Lemma 7.12 annehmen, dass P das Minimalpolynom von x ist. Wir setzen $x_1 = x$ und ergänzen dies zu einem endlichen K-Algebraerzeugendensystem von L, sagen wir

$$L = K[x_1, \ldots, x_n].$$

Es seien $P_1 = P, P_2, \ldots, P_n$ die Minimalpolynome von x_i über K. Wir betrachten das Produkt $F = P_1 \cdots P_n$ und den Zerfällungskörper M von F über L, der zugleich der Zerfällungskörper über K ist. Sei $y \in M$ eine Nullstelle von P. Wir müssen $y \in L$ zeigen. Es gibt einen K-Isomorphismus

$$\varphi\colon K[x] \cong K[X]/(P) \longrightarrow K[y]$$

mit $\varphi(x) = y$. Der Körper M ist der Zerfällungskörper von F über $K[x]$ als auch über $K[y]$. Daher gibt es nach Satz 11.6 ein kommutatives Diagramm

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi} & K[y] \\ \downarrow & & \downarrow \\ M & \xrightarrow{\tilde{\varphi}} & M \end{array}$$

mit einem K-Isomorphismus $\tilde{\varphi}$. Nach Voraussetzung ist dabei $\tilde{\varphi}(L) \subseteq L$, also ist $y = \varphi(x) \in L$. □

Bemerkung 15.5. Insbesondere die zweite Eigenschaft von Satz 15.4 zeigt, dass es sich hierbei um eine recht starke Eigenschaft handelt. Wenn man mit einem Primpolynom $P \in K[X]$ startet und sich den Restklassenkörper $L = K[X]/(P)$ anschaut, so besitzt P in L eine Nullstelle, nämlich die Restklasse x von X. Daher gilt in $L[X]$ die Beziehung $P = (X - x)Q$ mit

einem Polynom $Q \in L[X]$. Es gibt aber keinen allgemeinen Grund, warum Q über L in Linearfaktoren zerfallen sollte.

Wir geben ein Beispiel, das zeigt, dass die Verkettung von normalen Körpererweiterungen nicht normal sein muss.

Beispiel 15.6. Wir betrachten die Körperkette $\mathbb{Q} \subseteq M \subseteq L$, wobei $M = \mathbb{Q}(\sqrt{3})$ und $L = M(\sqrt{1+\sqrt{3}})$ ist. Das sind zwei quadratische Körpererweiterungen, die beide nach Lemma 15.2 (2) normal sind. Wir setzen $u = \sqrt{1+\sqrt{3}}$, und dieses Element erzeugt L über $\mathbb{Q}$. Wir können L als einen Unterkörper von $\mathbb{R}$ auffassen, indem wir für $\sqrt{3}$ und dann für $\sqrt{1+\sqrt{3}}$ die positiven reellen Wurzeln wählen. Wir haben

$$u^4 - 2u^2 - 2 = (u^2-1)^2 - 3 = 0,$$

d.h. das Polynom X^4-2X^2-2 wird von u annulliert. Dieses Polynom besitzt über L die Zerlegung

$$\begin{aligned} X^4 - 2X^2 - 2 &= \left(X^2-1\right)^2 - 3 \\ &= \left(X^2 - 1 - \sqrt{3}\right)\left(X^2 - 1 + \sqrt{3}\right) \\ &= \left(X^2 - u^2\right)\left(X^2 - 1 + \sqrt{3}\right) \\ &= (X-u)(X+u)\left(X^2 - 1 + \sqrt{3}\right). \end{aligned}$$

Wegen $L \subseteq \mathbb{R}$ und $\sqrt{3} - 1 > 0$ ist das hintere quadratische Polynom über L unzerlegbar. Dieses Polynom zerfällt also über L nicht in Linearfaktoren und somit ist $\mathbb{Q} \subseteq L$ nicht normal.

Wir setzen weiterhin voraus, dass eine endliche Körpererweiterung vorliegt. Dann sind die normalen Körpererweiterungen genau die Zerfällungskörper von Polynomen.

Satz 15.7. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist $K \subseteq L$ genau dann eine normale Körpererweiterung, wenn L Zerfällungskörper eines Polynoms $F \in K[X]$ ist.*

Beweis. Sei $K \subseteq L$ normal. Wegen der vorausgesetzten Endlichkeit ist $L = K[x_1, \ldots, x_n]$. Zu x_i sei $F_i \in K[X]$ das Minimalpolynom. Wegen der Normalität zerfällt jedes F_i in $L[X]$ in Linearfaktoren. Daher ist L der Zerfällungskörper des Produktes $F = F_1 \cdots F_n$. Sei nun $L = Z(F)$ ein Zerfällungskörper, und sei $F = (X-\alpha_1)\cdots(X-\alpha_n)$ die Faktorzerlegung zu den Nullstellen $\alpha_i \in L$, die den Körper L erzeugen. Wir werden das Kriterium Satz 15.4 (4) anwenden. Sei also $L \subseteq M$ eine Körpererweiterung und sei

$$\varphi\colon L \longrightarrow M$$

ein K-Algebrahomomorphismus. Es ist dann

$$F(\varphi(\alpha_i)) = \varphi(F(\alpha_i)) = 0,$$

da sich die Koeffizienten von F nicht ändern (vergleiche Lemma 10.15), und somit gehört $\varphi(\alpha_i)$ zur Nullstellenmenge $\{\alpha_1, \ldots, \alpha_n\}$ und damit insbesondere zu L. Daher gilt generell $\varphi(L) \subseteq L$. □

Korollar 15.8. *Sei $K \subseteq L$ eine endliche normale Körpererweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Es sei $\varphi\colon M \to L$ ein K-Algebrahomomorphismus. Dann besitzt φ eine Fortsetzung zu einem Automorphismus auf L.*

Beweis. Aufgrund von Satz 15.7 wissen wir, dass L der Zerfällungskörper eines Polynoms $F \in K[X]$ ist. L ist auch der Zerfällungskörper von $F \in M[X]$. Sei $M' = \varphi(M)$ das isomorphe Bild von M in L unter φ. Somit ist L auch der Zerfällungskörper von $F \in M'[X]$. Daher gibt es nach Satz 11.6 einen Isomorphismus $\tilde{\varphi}\colon L \to L$, der mit den Abbildungen $M \to L$ und $M \xrightarrow{\varphi} M' \to L$ verträglich ist. □

Korollar 15.9. *Sei $K \subseteq L$ eine endliche normale Körpererweiterung und es seien $\alpha, \beta \in L$. Dann sind α und β genau dann konjugiert, wenn es einen K-Automorphismus $\varphi\colon L \to L$ mit $\varphi(\alpha) = \beta$ gibt.*

Beweis. Wenn es einen K-Automorphismus φ mit $\varphi(\alpha) = \beta$ gibt, so induziert dieser einen Isomorphismus $K[\alpha] \to K[\beta]$. Da diese erzeugten Unterkörper jeweils durch die Minimalpolynome von α bzw. β festgelegt sind, müssen die Minimalpolynome übereinstimmen. Also sind α und β konjugiert. Wenn umgekehrt[12] die beiden Elemente konjugiert sind, so gibt es einen K-Isomorphismus $K[\alpha] \to K[\beta]$. Mit der Inklusion $K[\beta] \subseteq L$ führt dies zu einem K-Homomorphismus

$$K[\alpha] \longrightarrow L,$$

den man nach Korollar 15.8 zu einem Automorphismus auf L fortsetzen kann. □

In der nichtnormalen Erweiterung $\mathbb{Q} \subseteq L$ aus Beispiel 15.6 sind $\sqrt{3}$ und $-\sqrt{3}$ zueinander konjugiert (und es gibt einen Automorphismus $\mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{3}] = \mathbb{Q}[-\sqrt{3}]$, der $\sqrt{3}$ in $-\sqrt{3}$ überführt), es gibt aber keinen Automorphismus $L \to L$, der $\sqrt{3}$ in $-\sqrt{3}$ überführt. Aufgrund der Faktorzerlegung des Minimalpolynoms zu u sind die Identität und die durch $u \mapsto -u$ festgelegte Abbildung die einzigen Automorphismen, und beide sind eingeschränkt auf $\mathbb{Q}[\sqrt{3}]$ die Identität.

Korollar 15.10. *Sei $K \subseteq L$ eine endliche normale Körpererweiterung und sei M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann ist $K \subseteq M$ genau dann normal, wenn für jeden K-Algebraautomorphismus*

$$\varphi\colon L \longrightarrow L$$

die Beziehung $\varphi(M) \subseteq M$ gilt.

[12] Die Umkehrung folgt auch aus Satz 14.5.

Beweis. Wenn $K \subseteq M$ normal ist, so gilt die Homomorphismuseigenschaft aufgrund von Satz 15.4 (4). Zur Umkehrung verwenden wir das Kriterium Satz 15.4 (2). Sei also $P \in K[X]$ ein irreduzibles (normiertes) Polynom, das in M eine Nullstelle, sagen wir α, besitzt. Dieses Polynom zerfällt über L in Linearfaktoren, und wir müssen zeigen, dass die zugehörigen Nullstellen zu M gehören. Sei $\beta \in L$ eine weitere Nullstelle von P. Wegen der Irreduzibilität und Lemma 7.12 ist P das Minimalpolynom von α und auch von β, d.h. die beiden Elemente sind konjugiert. Nach Korollar 15.9 gibt es daher einen K-Automorphismus $\varphi\colon L \to L$ mit $\varphi(\alpha) = \beta$. Nach Voraussetzung ist $\beta \in M$. □

Beispiel 15.11. Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{7}, \sqrt{-3}] = \mathbb{Q}[\sqrt[3]{7}, \eta] =: L,$$

wobei

$$\eta = \frac{-1+\sqrt{3}\mathrm{i}}{2}$$

die dritte primitive Einheitswurzel ist und wobei wir mit $\sqrt[3]{7}$ die reelle Zahl meinen. Dies ist eine Erweiterung vom Grad 6, wie die Kette

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{7}] =: M \subseteq L$$

zeigt. Die Erweiterung $\mathbb{Q} \subseteq M$ ist nicht normal, da die beiden anderen dritten Wurzeln der 7, nämlich $\sqrt[3]{7}\eta$ und $\sqrt[3]{7}\eta^2$, nicht zu M gehören, weil sie nicht reell sind. Sie gehören aber zu L und da mit $\sqrt{-3}$ auch $-\sqrt{-3}$ zu L gehört ist nach Satz 15.4 (3) die Gesamterweiterung $\mathbb{Q} \subseteq L$ normal. Nach Korollar 15.10 muss es $\mathbb{Q}$-Automorphismen $\varphi\colon L \to L$ mit $\varphi(M) \neq M$ geben. In der Tat gibt es einen Automorphismus φ auf L, der η auf sich selbst und $\sqrt[3]{7}$ auf $\sqrt[3]{7}\eta$ abbildet. Dabei ist

$$M' = \varphi(M) = \mathbb{Q}[\sqrt[3]{7}\eta] \neq M.$$

15. Arbeitsblatt

15.1. **Aufwärmaufgaben.**

Aufgabe 15.1.*

Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad 3 und es sei $\mathbb{Q} \subseteq L$ eine Körpererweiterung, in der F in Linearfaktoren zerfällt. Zeige, dass die Nullstellen von F in L nicht die Form $\alpha, \alpha+\beta, \alpha+\gamma$ mit rationalen Zahlen β, γ haben können.

Aufgabe 15.2. Zeige, dass man in Satz 15.4 (2) nicht auf die Bedingung der Irreduzibilität verzichten kann.

Aufgabe 15.3. Zeige, dass man in Satz 15.4 die äquivalenten Bedingungen durch die folgende Eigenschaft ergänzen kann:

Zu jeder Körpererweiterung $K \subseteq M$ und zu zwei K-Algebrahomomorphismen

$$\varphi_1, \varphi_2 \colon L \longrightarrow M$$

ist $\varphi_1(L) = \varphi_2(L)$.

Aufgabe 15.4.*

Sei $\mathbb{Q} \subseteq K$ eine endliche normale Körpererweiterung und sei

$$\kappa \colon \mathbb{C} \longrightarrow \mathbb{C}$$

die komplexe Konjugation.

a) Zeige, dass $\kappa(K) \subseteq K$ gilt.

b) Zeige, dass $\kappa|_K = \mathrm{Id}_K$ genau dann gilt, wenn $K \subseteq \mathbb{R}$ ist.

Aufgabe 15.5. Es sei $q \in \mathbb{Q}$ eine rationale Zahl, die in $\mathbb{Q}$ keine dritte Wurzel besitzt, so dass $\mathbb{Q} \subseteq L = \mathbb{Q}[X]/(X^3 - q)$ eine Körpererweiterung vom Grad 3 ist. Zeige anhand der verschiedenen äquivalenten Formulierungen von Satz 15.4, dass diese Körpererweiterung nicht normal ist. Man gebe die verschiedenen Einbettungen von L in $\mathbb{C}$ an.

Aufgabe 15.6. Sei $K \subseteq L$ eine endliche normale Körpererweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper, der über K nicht normal sei. Zeige, dass es einen weiteren Zwischenkörper $M' \neq M$ gibt, der zu M isomorph ist.

Aufgabe 15.7. Wir betrachten die Körpererweiterung $\mathbb{Q} \subseteq M$ aus Beispiel 15.6. Zeige anhand der verschiedenen äquivalenten Formulierungen von Satz 15.4, dass diese Körpererweiterung nicht normal ist.

Aufgabe 15.8. Finde für den Körper L aus Beispiel 14.9 eine endliche Körpererweiterung $L \subseteq L'$ mit $L' \subseteq \mathbb{C}$ und so, dass L' über $\mathbb{Q}$ normal ist. Beschreibe einen $\mathbb{Q}$-Automorphismus $\varphi \colon L' \to L'$ mit $\varphi(L) \neq L$.

Aufgabe 15.9. Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Zu jedem Primpotenzteiler p^r von $\#(D)$ enthalte K eine p^r-te primitive Einheitswurzel. Zeige, dass $K \subseteq L$ eine separable Körpererweiterung ist.

Aufgabe 15.10. Bestimme für die Körpererweiterung $\mathbb{F}_3 \subseteq \mathbb{F}_9$, welche Elemente aus $\mathbb{F}_9$ untereinander konjugiert sind.

15.2. **Aufgaben zum Abgeben.**

Aufgabe 15.11. (4 Punkte)

Man gebe in jeder Charakteristik Beispiele für eine normale Körpererweiterung $K \subseteq L$ vom Grad 3.

Aufgabe 15.12. (3 Punkte)

Sei $K \subseteq L$ eine endliche Körpererweiterung und seien M_1, M_2 Zwischenkörper, die beide über K normal seien. Zeige, dass auch $K \subseteq M_1 \cap M_2$ normal ist.

Aufgabe 15.13. (4 Punkte)

Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Zu jedem Primpotenzteiler p^r von $\#(D)$ enthalte K eine p^r-te primitive Einheitswurzel. Zeige, dass $K \subseteq L$ eine normale Körpererweiterung ist.

Aufgabe 15.14. (4 Punkte)

Sei $K \subseteq L$ eine endliche normale und separable Körpererweiterung. Es sei $x \in L$ mit $x^n = a \in K$, wobei $\operatorname{grad}_K K(x) = n$ sei. Zeige, dass L n verschiedene n-te Einheitswurzeln besitzt.

Aufgabe 15.15. Bestimme für die Körpererweiterung $\mathbb{F}_2 \subseteq \mathbb{F}_8$, welche Elemente aus $\mathbb{F}_8$ untereinander konjugiert sind.

16. Vorlesung - Fixkörper

16.1. **Fixkörper.**

Definition 16.1. Es sei L ein Körper und $H \subseteq \operatorname{Aut}(L)$ eine Untergruppe der Automorphismengruppe von L. Dann heißt

$$\operatorname{Fix}(H) = \{x \in L | \varphi(x) = x \text{ für alle } \varphi \in H\}$$

der *Fixkörper* zu H.

Es ist unmittelbar klar, dass es sich dabei um einen Unterkörper von L handelt. Dies gilt auch dann, wenn H eine beliebige Menge von Ringendomorphismen ist, die nicht notwendigerweise bijektiv sein müssen.

Bemerkung 16.2. Zur trivialen Untergruppe $\{\mathrm{Id}\} \subseteq \mathrm{Aut}\,(L)$ gehört der Fixkörper L, und für jede andere Untergruppe ist der Fixkörper ein echter Unterkörper. Den Fixkörper zur gesamten Automorphismengruppe kann man dagegen nicht einfach charakterisieren (es ist nicht immer der Primkörper).

Lemma 16.3. *Es sei L ein Körper und $G = \mathrm{Aut}\,(L)$ die Automorphismengruppe von L. Dann gelten folgende Eigenschaften.*

(1) *Für Untergruppen $H_1 \subseteq H_2 \subseteq G$ ist $\mathrm{Fix}\,(H_1) \supseteq \mathrm{Fix}\,(H_2)$.*
(2) *Für Unterkörper $M_1 \subseteq M_2 \subseteq L$ ist $\mathrm{Gal}\,(L|M_1) \supseteq \mathrm{Gal}\,(L|M_2)$.*
(3) *Für eine Untergruppe $H \subseteq G$ ist $H \subseteq \mathrm{Gal}\,(L|\,\mathrm{Fix}\,(H))$.*
(4) *Für einen Unterkörper $M \subseteq L$ ist $M \subseteq \mathrm{Fix}\,(\mathrm{Gal}\,(L|M))$.*

Beweis. Siehe Aufgabe 16.3. □

16.2. **Charakterisierung von Galoiserweiterungen.**

Wir streben eine umfassende Charakterisierung von Galoiserweiterungen an, was einige Vorbereitungen erfordert.

Lemma 16.4. *Es sei L ein Körper und sei $H \subseteq \mathrm{Aut}\,(L)$ eine endliche Untergruppe der Automorphismengruppe von L. Es sei $K = \mathrm{Fix}\,(H)$. Dann ist $K \subseteq L$ eine algebraische Körpererweiterung, die normal und separabel ist. Für jedes $x \in L$ ist der Grad des Minimalpolynoms von x über K maximal gleich $\#(H)$.*

Beweis. Sei $x \in L$ fixiert. Wir betrachten die endliche Menge

$$M = \{\varphi(x)|\, \varphi \in H\} = \{x_1, \ldots, x_n\},$$

wobei $x_1 = x$ sei. Wir setzen

$$F := (X-x_1)(X-x_2)\cdots(X-x_n) = a_0+a_1X+a_2X^2+\cdots+a_{n-1}X^{n-1}+X^n$$

($\in L[X]$). Es ist $F(x) = 0$. Wir zeigen zuerst, dass die Koeffizienten a_i dieses Polynoms zu K gehören. Sei dazu $\varphi \in H$. Dann ist

$$\sum_{i=0}^{n} \varphi(a_i)X^i = \prod_{i=1}^{n}(X - \varphi(x_i)) = \prod_{i=1}^{n}(X - x_i) = \sum_{i=0}^{n} a_iX^i.$$

Daher ist $\varphi(a_i) = a_i$. Somit gehören die Koeffizienten zum Fixkörper $K = \mathrm{Fix}\,(H)$ und daher ist $F \in K[X]$. Dies bedeutet, dass x algebraisch über K ist, und dass sein Minimalpolynom einen Grad

$$\leq \mathrm{Grad}\,(F) = n = \#(M) \leq \#(H)$$

besitzt. Da F über L in Linearfaktoren zerfällt, und da alle Nullstellen von F einfach sind, ist die Erweiterung normal und separabel. □

Emil Artin (1898-1962)

Der folgende Satz heißt *Satz von Artin.*

Satz 16.5. *Es sei L ein Körper und sei $H \subseteq \mathrm{Aut}\,(L)$ eine endliche Untergruppe der Automorphismengruppe von L. Es sei $K = \mathrm{Fix}\,(H)$. Dann ist*

$$\mathrm{grad}_K\, L = \#(H).$$

Insbesondere ist $K \subseteq L$ eine Galoiserweiterung mit Galoisgruppe H.

Beweis. Nehmen wir an, dass $\#(H) < \mathrm{grad}_K\, L$ ist. Wir können annehmen, dass L endlich über K ist, da wir L durch einen (über K endlichen) Zwischenkörper der Form $K[\varphi(x_i), \varphi \in H, i = 1, \ldots, n]$ mit beliebig hohem Grad ersetzen können. Nach Lemma 16.4 ist die Körpererweiterung separabel und nach dem Satz vom primitiven Element kann man $L = K[x]$ schreiben. Dabei ist der Grad des Minimalpolynoms von x gleich dem Grad der Körpererweiterung, so dass sich ein Widerspruch zu Lemma 16.4 ergibt. Also ist $K \subseteq L$ eine endliche Körpererweiterung mit $\#(H) \geq \mathrm{grad}_K\, L$. Nach Satz 14.7 muss hierbei Gleichheit gelten. Die Inklusion $H \subseteq \mathrm{Gal}\,(L|K)$ ist trivial. Da H nach Satz 14.7 schon die maximal mögliche Anzahl von K-Automorphismen enthält, gilt hier Gleichheit. □

Der nächste Satz fasst die verschiedenen Charakterisierungen einer Galoiserweiterung zusammen.

Satz 16.6. *Sei $K \subseteq L$ eine endliche Körpererweiterung und sei $G = \mathrm{Gal}\,(L|K)$ die Galoisgruppe. Dann sind folgende Eigenschaften äquivalent.*

(1) *Die Körpererweiterung $K \subseteq L$ ist eine Galoiserweiterung.*
(2) *Es ist $\mathrm{Fix}\,(G) = K$.*

(3) *Die Körpererweiterung $K \subseteq L$ ist normal und separabel.*
(4) *L ist Zerfällungskörper eines separablen Polynoms $F \in K[X]$.*

Beweis. Zum Beweis der Implikation von (1) nach (2) betrachten wir die Körperkette $K \subseteq \operatorname{Fix}(G) \subseteq L$. Nach der Gradformel und da eine Galoiserweiterung vorliegt ist

$$\operatorname{grad}_K \operatorname{Fix}(G) \cdot \operatorname{grad}_{\operatorname{Fix}(G)} L = \operatorname{grad}_K L = \#(G).$$

Nach dem Satz von Artin ist $\operatorname{grad}_{\operatorname{Fix}(G)} L = \#(G)$, also ist $\operatorname{grad}_K \operatorname{Fix}(G) = 1$. Die Implikation von (2) nach (3) folgt aus Lemma 16.4. Die Äquivalenz von (3) und (4) ergibt sich sofort aus Satz 15.7. Sei nun (3) erfüllt. Wir schreiben $L = K[x_1, \ldots, x_m]$. Die Minimalpolynome $F_i \in K[X]$ der x_i zerfallen wegen der Normalität in $L[X]$ in Linearfaktoren. Daher können wir Lemma 13.7 mit $M = L$ anwenden und erhalten $n = \operatorname{grad}_K L$ Einbettungen von L nach L (über K), und somit besitzt die Galoisgruppe n Elemente. □

Korollar 16.7. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann ist auch $M \subseteq L$ eine Galoiserweiterung.*

Beweis. Nach Lemma 15.2 (3) ist $M \subseteq L$ eine normale Körpererweiterung. Nach Lemma 13.5 ist sie auch separabel. Somit handelt es sich aufgrund von Satz 16.6 um eine Galoiserweiterung. □

In der vorstehenden Situation ist die Körpererweiterung $K \subseteq M$ im Allgemeinen nicht galoissch.

16.3. **Endliche Körper als Galoiserweiterung.**

Wir besprechen zuerst endliche Körper im Rahmen der Galoistheorie.

Zu jeder Primzahl p und jedem Exponenten m gibt es nach Satz 11.11 einen eindeutig bestimmten endlichen Körper mit p^m Elementen.

Lemma 16.8. *Sei L ein endlicher Körper der Charakteristik p. Dann ist der Frobeniushomomorphismus*

$$\Phi\colon L \longrightarrow L,\ x \longmapsto x^p,$$

ein Automorphismus, dessen Fixkörper $\mathbb{Z}/(p)$ ist.

Beweis. Der Frobeniushomomorphismus ist stets ein Ringhomomorphismus. Die Injektivität ergibt sich aus Korollar 6.8, und daraus ergibt sich die Surjektivität wegen der Endlichkeit aus Lemma 10.5 (Analysis (Osnabrück 2014-2016)). Wegen $\Phi(1) = 1$ werden die Elemente aus $\mathbb{Z}/(p)$ auf sich selbst abgebildet. Daher gibt es p Elemente in K mit $x^p = x$. Mehr kann es wegen Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) nicht geben. □

Satz 16.9. *Es sei p eine Primzahl und $m \in \mathbb{N}$, $q = p^m$. Dann ist die Körpererweiterung $\mathbb{F}_p \subseteq \mathbb{F}_q$ eine Galoiserweiterung mit einer zyklischen Galoisgruppe der Ordnung m, die vom Frobeniushomomorphismus erzeugt wird.*

Beweis. Es sei

$$\Phi\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$$

der Frobeniushomomorphismus, der nach Lemma 16.8 ein $\mathbb{F}_p$-Automorphismus ist. Daher sind auch die Iterationen Φ^k Automorphismen, und zwar gilt

$$\Phi^k(x) = x^{p^k}.$$

Bei $k = m$ ist nach Korollar 4.17 $x^{p^m} = x$ für alle $x \in \mathbb{F}_q$, also ist $\Phi^m = \mathrm{Id}$. Für $k < m$ kann Φ^k nicht die Identität sein, da dies sofort Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) widersprechen würde. Also gibt es m verschiedene Potenzen des Frobeniusautomorphismus. Nach Satz 14.7 kann es keine weiteren Automorphismen geben und die Körpererweiterung ist galoissch mit der vom Frobenius erzeugten Gruppe als Galoisgruppe. □

Korollar 16.10. *Es sei p eine Primzahl und $m, n \in \mathbb{N}_+$. Es seien K und L endliche Körper mit p^m bzw. p^n Elementen. Dann ist K genau dann ein Unterkörper von L, wenn m ein Teiler von n ist. In diesem Fall ist $K \subseteq L$ eine Galoiserweiterung vom Grad n/m mit einer zyklischen Galoisgruppe der Ordnung n/m, die von der m-ten Iteration des Frobenius erzeugt wird.*

Beweis. Sei $q = p^m$. Wenn K ein Unterkörper von L ist, so ist L ein K-Vektorraum einer gewissen endlichen Dimension. Daher muss die Elementanzahl von L eine Potenz von q sein. Aus

$$p^n = q^k = (p^m)^k = p^{mk}$$

ergibt sich sofort, dass n ein Vielfaches von m ist. Sei umgekehrt m ein Teiler von n. Die Frobeniusiteration Φ^m auf L erzeugt eine Untergruppe H der nach Satz 16.9 zyklischen Galoisgruppe von $\mathbb{F}_p \subseteq L$. Die Ordnung von H ist n/m. Es sei $M = \mathrm{Fix}\,(H) \subseteq L$ der zugehörige Fixkörper. Dann besitzt die Körpererweiterung $M \subseteq L$ nach Korollar 16.7 den Grad n/m und somit besitzt $\mathbb{F}_p \subseteq M$ den Grad m. Daher besitzt M gerade p^m Elemente und ist daher wegen Satz 11.11 isomorph zu K. □

16. Arbeitsblatt

16.1. **Aufwärmaufgaben.**

Aufgabe 16.1. Es sei L ein Körper und M eine Menge von Ringhomomorphismen von L nach L. Zeige, dass die Menge

$$\{x \in L |\, \varphi(x) = x \text{ für alle } \varphi \in M\}$$

ein Unterkörper von L ist.

Aufgabe 16.2. Es sei L ein Körper, es sei M eine Menge von Automorphismen von L nach L und es sei H die von M erzeugte Untergruppe der Automorphismengruppe. Zeige die Gleichheit

$$\operatorname{Fix}(H) = \{x \in L | \varphi(x) = x \text{ für alle } \varphi \in M\} .$$

Aufgabe 16.3. Es sei L ein Körper und $G = \operatorname{Aut} L$ die Automorphismengruppe von L. Begründe die folgenden Beziehungen.

(1) Für Untergruppen $H_1 \subseteq H_2 \subseteq G$ ist $\operatorname{Fix}(H_1) \supseteq \operatorname{Fix}(H_2)$.
(2) Für Unterkörper $M_1 \subseteq M_2 \subseteq L$ ist $\operatorname{Gal}(L|M_1) \supseteq \operatorname{Gal}(L|M_2)$.
(3) Für eine Untergruppe $H \subseteq G$ ist $H \subseteq \operatorname{Gal}(L|\operatorname{Fix}(H))$.
(4) Für einen Unterkörper $M \subseteq L$ ist $M \subseteq \operatorname{Fix}(\operatorname{Gal}(L|M))$.

Aufgabe 16.4. Es sei K ein Körper und H eine endliche Gruppe von Körperautomorphismen. Sei $x \in K$. Zeige, dass

$$\sum_{\varphi \in H} \varphi(x) \text{ und } \prod_{\varphi \in H} \varphi(x)$$

zum Fixkörper $\operatorname{Fix}(H)$ gehören.

Aufgabe 16.5. Es sei L ein Körper und sei

$$\varphi\colon L \longrightarrow L$$

ein Automorphismus. Zeige, dass die Einschränkung von φ auf den Primkörper von L die Identität ist.

Aufgabe 16.6. Beweise Lemma 11.8 mit Hilfe von Fixkörpern.

Aufgabe 16.7. Es sei p eine Primzahl und $q = p^e$, $e \geq 1$, eine Primzahlpotenz. Beweise mit Hilfe der verschiedenen äquivalenten Eigenschaften aus Satz 16.6, dass die Körpererweiterung $\mathbb{F}_p \subseteq \mathbb{F}_q$ galoissch ist.

Aufgabe 16.8. Bestimme die Matrix des Frobeniushomomorphismus

$$\Phi : \mathbb{F}_q \to \mathbb{F}_q$$

bezüglich einer geeigneten $\mathbb{F}_p$-Basis von $\mathbb{F}_q$ für $p = 2$ und $q = 4$ bzw. $q = 8$.

Aufgabe 16.9.*

Bestimme die Matrix des Frobeniushomomorphismus

$$\Phi\colon \mathbb{F}_{49} \longrightarrow \mathbb{F}_{49}$$

bezüglich einer geeigneten $\mathbb{F}_7$-Basis von $\mathbb{F}_{49}$.

Aufgabe 16.10. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass zwischen $\varphi \in \mathrm{Gal}\,(L|K)$ und der Multiplikationsabbildung μ_f, $f \in L$, beide aufgefasst als K-lineare Abbildung von L nach L, weder die Beziehung

$$\mu_{\varphi(f)} = \mu_f \circ \varphi$$

noch die Beziehung

$$\mu_{\varphi(f)} = \varphi \circ \mu_f$$

gelten muss.

Aufgabe 16.11.*

Sei $K \subseteq L$ eine endliche Körpererweiterung und es sei $\varphi \in \mathrm{Gal}\,(L|K)$ ein K-Automorphismus. Zeige, dass für die Multiplikationsabbildungen zu $f \in L$ die Beziehung

$$\mu_{\varphi(f)} = \varphi \circ \mu_f \circ \varphi^{-1}$$

gilt.

16.2. **Aufgaben zum Abgeben.**

Aufgabe 16.12. (3 Punkte)

Es seien L und L' isomorphe Körper. Zeige, dass dann auch die Automorphismengruppen $\mathrm{Aut}\,(L)$ und $\mathrm{Aut}\,(L')$ in natürlicher Weise zueinander isomorph sind.

Aufgabe 16.13. (4 Punkte)

Bestimme die Körperautomorphismen von $\mathbb{R}$.

Aufgabe 16.14. (3 Punkte)

Bestimme die Matrix des Frobeniushomomorphismus

$$\Phi\colon\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$$

bezüglich einer geeigneten $\mathbb{F}_p$-Basis von $\mathbb{F}_q$ für $p = 3$ und $q = 9$ bzw. $q = 27$.

Aufgabe 16.15. (5 Punkte)

Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit einer zyklischen Galoisgruppe. Zeige, dass für jeden Zwischenkörper M auch die Erweiterung $K \subseteq M$ galoissch ist mit einer ebenfalls zyklischen Galoisgruppe.

17. Vorlesung - Die Galoiskorrespondenz

17.1. **Die Galoiskorrespondenz.**

Der folgende Satz heißt auch *Hauptsatz der Galoistheorie* oder *Satz über die Galoiskorrespondenz*. Er stiftet eine unmittelbare Beziehung zwischen den Zwischenkörpern einer endlichen Galoiserweiterung und Untergruppen der Galoisgruppe. Er bildet die Grundlage dafür, gruppentheoretische Aussagen auf Körpererweiterungen anzuwenden.

Satz 17.1. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit der Galoisgruppe $G = \operatorname{Gal}(L|K)$. Dann sind die Zuordnungen*

$$M \longmapsto \operatorname{Gal}(L|M) \text{ und } H \longmapsto \operatorname{Fix}(H)$$

zueinander inverse Abbildungen zwischen der Menge der Zwischenkörper M, $K \subseteq M \subseteq L$, und der Menge der Untergruppen von G. Bei dieser Korrespondenz werden die Inklusionen umgekehrt.

Beweis. Diese Abbildungen sind wohldefiniert und kehren nach Lemma 16.3 die Inklusion um. Sei M ein Zwischenkörper. Nach Korollar 16.7 ist $M \subseteq L$ eine Galoiserweiterung, also ist $\operatorname{Fix}(\operatorname{Gal}(L|M)) = M$ nach Satz 16.6. Sei nun H vorgegeben mit dem Fixkörper $M = \operatorname{Fix}(H)$. Nach dem Satz von Artin ist $M \subseteq L$ eine Galoiserweiterung mit Galoisgruppe $H = \operatorname{Gal}(L|M)$. □

Für einen Automorphismus $\varphi \in \operatorname{Gal}(L|K)$ und einen Zwischenkörper M, $K \subseteq M \subseteq L$, ist $M' = \varphi(M)$ wieder ein Zwischenkörper, der zu M K-isomorph ist. Zwischen den zugehörigen Galoisgruppen $\operatorname{Gal}(L|M)$ und $\operatorname{Gal}(L|M')$ gilt die folgende Beziehung.

Satz 17.2. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und sei M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Es sei $\psi \in G = \operatorname{Gal}(L|K)$ und $M' = \psi(M)$. Dann gilt in der Galoisgruppe G die Beziehung*

$$\operatorname{Gal}(L|M') = \psi \operatorname{Gal}(L|M)\psi^{-1}.$$

Beweis. Sei $\varphi \in \operatorname{Gal}(L|M')$. Wir schreiben $\varphi = \psi(\psi^{-1}\varphi\psi)\psi^{-1}$ und müssen zeigen, dass $\psi^{-1}\varphi\psi$ zu $\operatorname{Gal}(L|M)$ gehört. Sei dazu $x \in M$. Dann ist

$$\left(\psi^{-1}\varphi\psi\right)(x) = \psi^{-1}(\varphi(\psi(x))).$$

Dabei gehört $\psi(x) \in M'$ und somit ist $\varphi(\psi(x)) = \psi(x)$. Also ist

$$\psi^{-1}(\varphi(\psi(x))) = \psi^{-1}(\psi(x)) = x.$$

Die umgekehrte Inklusion ergibt sich genauso bzw. folgt direkt daraus, dass beide Gruppen die gleiche Anzahl besitzen. □

Diese Aussage bedeutet, dass für konjugierte Zwischenkörper M und M' in einer Galoiserweiterung auch ihre zugehörigen Galoisgruppen zueinander konjugiert sind im Sinne der folgenden Definition.

Definition 17.3. Zwei Untergruppen $H_1, H_2 \subseteq G$ heißen zueinander *konjugiert*, wenn es einen inneren Automorphismus

$$\kappa_h \colon G \longrightarrow G,\, g \longmapsto hgh^{-1},$$

gibt, der eine Isomorphie zwischen H_1 und H_2 stiftet.

Korollar 17.4. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und sei M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann sind folgende Aussagen äquivalent.*

(1) *Für alle $\psi \in \mathrm{Gal}\,(L|K)$ ist $\psi(M) = M$.*
(2) *Die Untergruppe $\mathrm{Gal}\,(L|M) \subseteq \mathrm{Gal}\,(L|K)$ ist nur zu sich selbst konjugiert.*

Beweis. Siehe Aufgabe 17.13. □

Wir wissen nach Korollar 16.7, dass bei einer Galoiserweiterung $K \subseteq L$ und einem Zwischenkörper $K \subseteq M \subseteq L$ auch die hintere Erweiterung $M \subseteq L$ galoissch ist. Die Erweiterung $K \subseteq M$ muss hingegen nicht galoisch sein, vielmehr liefert die folgende Aussage ein Kriterium.

Satz 17.5. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann gelten folgende Aussagen.*

(1) *Die Körpererweiterung $K \subseteq M$ ist genau dann eine Galoiserweiterung, wenn die Untergruppe $\mathrm{Gal}\,(L|M) \subseteq \mathrm{Gal}\,(L|K)$ ein Normalteiler ist.*
(2) *Sei $K \subseteq M$ eine Galoiserweiterung. Dann besteht zwischen den Galoisgruppen die natürliche Restklassenbeziehung*

$$\mathrm{Gal}\,(M|K) = \mathrm{Gal}\,(L|K)/\mathrm{Gal}\,(L|M).$$

Bei dieser Zuordnung wird ein Automorphismus $\varphi \in \mathrm{Gal}\,(L|K)$ auf M eingeschränkt.

Beweis. (1). Da die Körpererweiterung $K \subseteq M$ separabel ist, muss aufgrund von Satz 16.6 nur die Normalität betrachtet werden. Nach Satz 15.4 (4) ist die Körpererweiterung $K \subseteq M$ genau dann normal, wenn jeder K-Automorphismus von L den Unterkörper M in sich selbst überführt. Dies ist wegen Korollar 17.4 genau dann der Fall, wenn $\mathrm{Gal}\,(L|M)$ unter jeder Konjugation auf sich selbst abgebildet wird, also nach Lemma 5.4 ein Normalteiler ist. (2). Sei nun $K \subseteq M$ normal. Dann ist $\varphi(M) = M$ für jedes $\varphi \in \mathrm{Gal}\,(L|K)$ und somit gibt es eine natürliche Abbildung

$$\mathrm{Gal}\,(L|K) \longrightarrow \mathrm{Gal}\,(M|K),\, \varphi \longmapsto \varphi|_M.$$

Diese ist offensichtlich ein Gruppenhomomorphismus. Aufgrund von Satz 15.4 gibt es für einen Automorphismus $\psi \in \mathrm{Gal}\,(M|K)$ eine Fortsetzung zu einem Automorphismus $\tilde{\psi} \in \mathrm{Gal}\,(L|K)$. Daher ist der Gruppenhomomorphismus surjektiv. Der Kern davon ist offenbar $\mathrm{Gal}\,(L|M)$, so dass sich die behauptete Isomorphie aus Korollar 5.11 ergibt. □

17.2. **Beispiele zur Galoiskorrespondenz.**

Die zuletzt genannte Aussage ist natürlich im Fall, dass eine Galoiserweiterung mit abelscher Galoisgruppe vorliegt, unmittelbar anwendbar. In dieser Situation ist also jeder Zwischenkörper über dem Grundkörper galoissch.

Beispiel 17.6. Es sei $\mathbb{F}_p \subseteq \mathbb{F}_q$ mit $q = p^n$ eine Körpererweiterung endlicher Körper. Nach Satz 16.9 ist dies eine Galoiserweiterung mit zyklischer Galoisgruppe der Ordnung n, die vom Frobeniushomomorphismus Φ erzeugt wird. Die Galoisgruppe ist also isomorph zu $\mathbb{Z}/(n)$. Die Untergruppen von $\mathbb{Z}/(n)$ sind von der Form

$$H = \langle m \rangle = \{0, m, 2m, \ldots, (k-1)m\}$$

mit einem Teiler m von n, wobei $k = \frac{n}{m}$ die Ordnung der Untergruppe ist. Der zugehörige Fixkörper ist der Fixkörper zu Φ^m, der nach Korollar 16.10 isomorph zu $\mathbb{F}_{p^m}$ ist, und H ist die Galoisgruppe von $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

Zu jeder Untergruppe $H = \langle m \rangle$ gibt es die Restklassenabbildung

$$\mathbb{Z}/(n) \longrightarrow (\mathbb{Z}/(n))/H \cong \mathbb{Z}/(m).$$

Gemäß Satz 17.5 ist die Restklassengruppe dabei die Galoisgruppe von $\mathbb{F}_p \subseteq \mathbb{F}_{p^m}$, und der Frobenius Φ von $\mathbb{F}_{p^n}$ wird dabei auf den Frobenius von $\mathbb{F}_{p^m}$ eingeschränkt.

Insbesondere hängen die Anzahl und die Inklusionsbeziehungen der Zwischenkörper von $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ nur von n und nicht von der Primzahl ab.

Proposition 17.7. *Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Der Körper K enthalte eine m-te primitive Einheitswurzel, wobei m der Exponent von D sei. Dann ist jeder Zwischenkörper M, $K \subseteq M \subseteq L$, von der Form $M = \bigoplus_{d \in E} L_d$ mit einer eindeutig bestimmten Untergruppe $E \subseteq D$.*

Beweis. Die Körpererweiterung $K \subseteq L$ ist nach Satz 14.11 eine Galoiserweiterung mit Galoisgruppe $G = \mathrm{Char}\,(D, K)$. Da K hinreichend viele Einheitswurzeln besitzt, entsprechen sich die Untergruppen von D und von G über die Charakter-Korrespondenz

$$E \longmapsto E^\perp = \{\chi \in G |\, \chi(d) = 1 \text{ für alle } d \in E\}$$

und

$$H \longmapsto H^\perp = \{d \in D |\, \chi(d) = 1 \text{ für alle } \chi \in H\}\ .$$

Zu jeder Untergruppe $E \subseteq D$ ist $\bigoplus_{d \in E} L_d$ ein Zwischenkörper. Da wegen der Galoiskorrespondenz die Anzahl der Zwischenkörper mit der Anzahl der Untergruppen der Galoisgruppe, und diese mit der Anzahl der Untergruppen in D übereinstimmt, ist jeder Zwischenkörper von dieser Form und insbesondere graduiert. □

Zu einer Untergruppe $H \subseteq G$ ist dabei

$$\mathrm{Fix}\,(H) \;=\; \bigoplus_{d \in H^\perp} L_d,$$

und zu einem Unterkörper $M = L_E = \bigoplus_{d \in E} L_d$ ist

$$\mathrm{Gal}\,(L|M) \;=\; E^\perp \;=\; \{\chi \in D^\vee |\, \chi(d) = 1 \text{ für alle } d \in E\}\,.$$

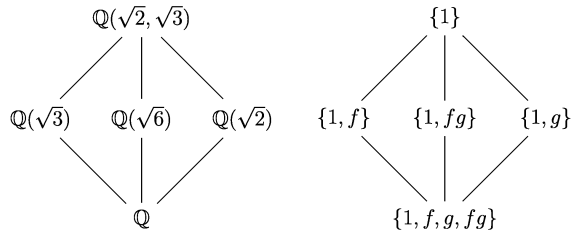
Die Galoisgruppe von

$$M \;=\; L_E$$

über K ist gleich

$$\mathrm{Gal}\,(M|K) \;=\; E^\vee \;=\; D^\vee / E^\perp.$$

Die bijektive Beziehung zwischen Zwischenkörpern und Untergruppen der graduierenden Gruppe im Galoisfall wird manchmal auch als *Kogaloiskorrespondenz* bezeichnet. Bei ihr werden Inklusionen erhalten und drehen sich nicht wie bei der Galoiskorrespondenz um (bei der Bijektion zwischen Untergruppen und ihrem Charakterdual drehen sich die Inklusionen um).



Beispiel 17.8. Wir knüpfen an Beispiel 12.8 an. Aufgrund von Satz 14.11 liegt eine Galoiserweiterung vor. Die graduierende Gruppe ist $D = \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Neben der trivialen Untergruppe und D selbst gibt es noch die drei Untergruppen $\{(0,0),(1,0)\}$, $\{(0,0),(0,1)\}$, $\{(0,0),(1,1)\}$, die den Zwischenkörpern

$$\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{6}),\ L$$

entsprechen. Wegen Proposition 17.7 gibt es keine weiteren Zwischenkörper. Die Galoisgruppe ist $G = D^\vee \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$ nach Satz 14.11. Zur Untergruppe $E = \{(0,0),(1,0)\} \subseteq D$ gehört dabei $E^\perp$ (das der Galoisgruppe $\mathrm{Gal}\,(L_E|\mathbb{Q})$ entspricht), das aus dem konstanten Charakter und der Abbildung

$$\chi\colon\ D \longrightarrow \mathbb{Q}^\times$$

besteht, die E auf 1 und $D \setminus E$ auf -1 abbildet. Dazu gehört wiederum der durch

$$1 \longmapsto 1,\ \sqrt{2} \longmapsto \sqrt{2},\ \sqrt{3} \longmapsto -\sqrt{3},\ \sqrt{6} \longmapsto -\sqrt{6}$$

festgelegte $\mathbb{Q}$-Automorphismus φ.

Beispiel 17.9. Wir betrachten die $\mathbb{Z}/(6)$-graduierte Körpererweiterung

$$\mathbb{Q} \subseteq L = \mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}] = \mathbb{Q}[\sqrt[6]{-108}] = \mathbb{Q}[X]/(X^6 + 108).$$

Die Graduierung ist durch $L_i = \mathbb{Q} \cdot x^i$ mit $x = \sqrt[6]{-108} = \sqrt[3]{2} \cdot \sqrt{-3}$ gegeben. Es ist $\sqrt{-3} = -\frac{1}{6}x^3$ und $\sqrt[3]{2} = \frac{1}{18}x^4$. Da es in $\mathbb{Q}$ keine primitive dritte Einheitswurzel gibt, ist $\mathrm{Char}\,(\mathbb{Z}/(6), \mathbb{Q}^\times) \cong \mathbb{Z}/(2)$ und daher gibt es nur zwei homogene Automorphismen (somit ist dies auch keine Kummererweiterung.[13]). Dennoch handelt es sich um eine Galoiserweiterung. Zunächst gehört

$$\zeta_3 = \frac{-1 + \sqrt{-3}}{2} = \frac{-6 - x^3}{12}$$

zu L und es ist $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) = L_0 \oplus L_3$. Ein weiterer (mit der Graduierung verträglicher) Zwischenkörper ist $\mathbb{Q}\left(\sqrt[3]{2}\right) = L_0 \oplus L_2 \oplus L_4$. Die durch $x^i \mapsto (-1)^i x^i$ gegebene Abbildung ist ein homogener Automorphismus φ mit $\varphi^2 = \mathrm{Id}$. Aber auch die Zuordnung $x^i \mapsto (\zeta_3)^i x^i$ definiert einen (nicht-homogenen) Automorphismus ψ mit $\psi^3 = \mathrm{Id}$. Es gibt also insgesamt 6 Automorphismen und daher liegt eine Galoiserweiterung vor. Dabei ist

$$(\varphi \circ \psi)(x) = \varphi(\psi(x)) = \varphi(\zeta_3 x) = \varphi\left(\frac{-6x - x^4}{12}\right) = \frac{6x - x^4}{12}$$

und

$$(\psi \circ \varphi)(x) = \psi(\varphi(x)) = \psi(-x) = -\psi(x) = -\frac{-6x - x^4}{12} = \frac{6x + x^4}{12}.$$

Daher ist die Galoisgruppe nicht kommutativ, und es muss $\mathrm{Gal}\,(L|\mathbb{Q}) = S_3$ sein. Der Körper $\psi\left(\mathbb{Q}\left(\sqrt[3]{2}\right)\right)$ ist ein nichthomogener Zwischenkörper.

17. Arbeitsblatt

17.1. **Aufwärmaufgaben.**

Aufgabe 17.1. Es sei p eine Primzahl und sei $K \subseteq L$ eine Körpererweiterung vom Grad p. Zeige, dass die Galoisgruppe von L über K entweder genau eine oder genau zwei Untergruppen besitzt. Wie viele Zwischenkörper besitzt die Körpererweiterung, wann ist die Erweiterung galoissch?

Aufgabe 17.2. Es sei $K \subseteq L$ eine endliche Körpererweiterung mit Galoisgruppe $\mathrm{Gal}\,(L|K)$. Zeige, dass die Zuordnung

$$H \longmapsto \mathrm{Fix}\,(H)\,,$$

die einer Untergruppe ihren Fixkörper zuordnet, stets injektiv ist.

[13] Siehe die nächste Vorlesung.

Aufgabe 17.3. Sei p eine Primzahl. Erstelle Inklusionsdiagramme für die Zwischenkörper der Körpererweiterung $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ für $n = 4, 6, 8, 12$. Wie sehen die zugehörigen Inklusionsdiagramme der Untergruppen der Galoisgruppe aus?

Aufgabe 17.4. Es sei $K \subseteq L$ eine Galoiserweiterung mit Galoisgruppe

$$\mathrm{Gal}\,(L|K) \cong (\mathbb{Z}/(p))^n,$$

wobei p eine Primzahl sei. Bestimme die Untergruppen der Galoisgruppen und skizziere ein Inklusionsdiagramm für die Untergruppen, die Zwischenkörper und die Potenzmenge von $\{1, \ldots, n\}$.

Aufgabe 17.5. Bestimme die Nullstellen von $X^6 + 108$ in Beispiel 17.9 und beschreibe, wie die Automorphismen auf diesen Nullstellen wirken. Welche Nullstellen sind konjugiert?

Aufgabe 17.6. Bestimme die Zwischenkörper in Beispiel 17.9.

Aufgabe 17.7.*

Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G und es seien $H_1, H_2 \subseteq G$ Untergruppen mit den zugehörigen Fixkörpern $K_1 = \mathrm{Fix}\,(H_1)$ und $K_2 = \mathrm{Fix}\,(H_2)$. Zeige, dass der Durchschnitt $K_1 \cap K_2$ gleich dem Fixkörper zu H ist, wobei H die von H_1 und H_2 erzeugte Untergruppe bezeichnet (das ist die kleinste Untergruppe von G, die sowohl H_1 als auch H_2 enthält).

Aufgabe 17.8. Es sei $\mathbb{F}_q$ ein endlicher Körper. Beschreibe den Frobeniushomomorphismus als Abbildung von $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)$ in sich selbst. Woran erkennt man nach dieser Übersetzung die Bijektivität des Frobenius? Wie sehen die Iterationen aus? Wie kann man die Fixelemente zu einer solchen Iteration als Kern beschreiben?

Aufgabe 17.9. Wir betrachten den Körper $\mathbb{F}_9$ mit 9 Elementen. Für welche Untergruppen $H \subseteq \mathbb{F}_9^\times$ ist $H \cup \{0\}$ ein Körper, für welche nicht?

Eine Gruppe heißt *einfach*, wenn sie genau zwei Normalteiler enthält (nämlich sich selbst und die triviale Gruppe).

Aufgabe 17.10. Es sei $K \subseteq L$ eine Galoiserweiterung derart, dass die Galoisgruppe einfach sei. Zeige, dass ein Zwischenkörper M, $K \subseteq M \subseteq L$, nur dann galoissch über K ist, wenn er gleich K oder L ist.

Aufgabe 17.11. Sei G eine einfache, nicht kommutative Gruppe. Zeige, dass G eine Untergruppe besitzt, die kein Normalteiler ist.

Aufgabe 17.12. Es seien $K \subseteq L$ und $R \subseteq S$ Galoiserweiterungen derart, dass ihre Galoisgruppen $\mathrm{Gal}\,(L|K)$ und $\mathrm{Gal}\,(S|R)$ isomorph sind. Stifte eine inklusionserhaltende Bijektion zwischen den Zwischenkörper der ersten und den Zwischenkörpern der zweiten Erweiterung.

17.2. **Aufgaben zum Abgeben.**

Aufgabe 17.13. (3 Punkte)

Es sei $K \subseteq L$ eine endliche Galoiserweiterung und sei M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) Für alle $\psi \in \mathrm{Gal}\,(L|K)$ ist $\psi(M) = M$.
(2) Die Untergruppe $\mathrm{Gal}\,(L|M) \subseteq \mathrm{Gal}\,(L|K)$ ist nur zu sich selbst konjugiert.

Aufgabe 17.14. (3 Punkte)

Zeige, dass $X^4-5 \in \mathbb{Q}[\mathrm{i}][X]$ irreduzibel ist. Zeige, dass die Körpererweiterung

$$\mathbb{Q}[\mathrm{i}] \subseteq \mathbb{Q}[\mathrm{i}][X]/\left(X^4-5\right)$$

galoissch ist, bestimme die Galoisgruppe und sämtliche Zwischenkörper.

Aufgabe 17.15. (3 Punkte)

Es sei S_3 die Gruppe der bijektiven Abbildungen auf einer dreielementigen Menge. Bestimme die Untergruppen von S_3 und welche zueinander konjugiert sind. Welche Untergruppen sind Normalteiler? Man gebe eine Galoiserweiterung mit Galoisgruppe S_3 an und bestimme die zu den Untergruppen gehörenden Zwischenkörper.

Aufgabe 17.16. (3 Punkte)

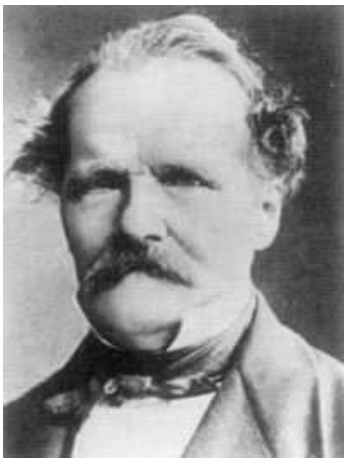
Sei G eine zyklische Gruppe. Zeige, dass G genau dann einfach ist, wenn G endlich und ihre Ordnung eine Primzahl ist.

Aufgabe 17.17. (3 Punkte)

Es sei K ein Körper und $F \in K[X]$ ein irreduzibles separables Polynom. Es sei vorausgesetzt, dass die Galoisgruppe des Zerfällungskörpers L von F kommutativ sei. Zeige, dass dann $L \cong K[X]/(F)$ ist.

18. Vorlesung - Kummererweiterungen

18.1. **Kummererweiterungen.**



Ernst Eduard Kummer (1810-1893)

Wir haben in der letzten Vorlesung gesehen, dass sich einige Eigenschaften einer Galoiserweiterung vereinfachen, wenn die Galoisgruppe abelsch ist. Beispielsweise ist dann jeder Zwischenkörper selbst galoissch über dem Grundkörper. Man spricht von *abelschen Galoiserweiterungen*.[14] Wichtige Beispiele solcher abelschen Körpererweiterungen sind Erweiterungen von endlichen Körpern und graduierte Körpererweiterungen, wenn hinreichend viele Einheitswurzeln im Grundkörper vorhanden sind.[15] Unter dieser Bedingung folgt umgekehrt, dass sich eine abelsche Erweiterung graduieren lässt. Dies ist der Inhalt der Kummertheorie.

Definition 18.1. Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Eine Galoiserweiterung $K \subseteq L$ heißt eine *Kummererweiterung* zum Exponenten m, wenn ihre Galoisgruppe abelsch und ihr Exponent ein Teiler von m ist.

Satz 18.2. *Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann gelten folgende Aussagen.*

(1) *Wenn $L = \bigoplus_{d \in D} L_d$ eine D-graduierte Körpererweiterung ist, so ist $K \subseteq L$ eine Kummererweiterung zum Exponenten m.*
(2) *Sei $K \subseteq L$ eine Kummererweiterung zum Exponenten m mit Galoisgruppe G. Es sei $D = \operatorname{Char}(G, K)$ die Charaktergruppe von G. Zu*

[14] Es ist eine generelle Bezeichnungsphilosophie, dass ein Eigenschaftswort zu einer Galoiserweiterung sich auf die Galoisgruppe bezieht.

[15] Eine weitere wichtige Beispielsklasse sind die Kreisteilungskörper, siehe die beiden nächsten Vorlesungen.

$\delta \in D$ *sei*[16]

$$L_\delta = \{x \in L | \, \varphi(x) = \delta(\varphi) \cdot x \text{ für alle } \varphi \in G\}.$$

Dann ist $L = \bigoplus_{\delta \in D} L_\delta$ *eine* D*-graduierte Körpererweiterung.*

Beweis. (1). Dies ist eine Neuformulierung von Satz 14.11. (2). Nach Satz Anhang 8.3 sind sämtliche Automorphismen $\varphi \in G = \mathrm{Gal}\,(L|K)$ diagonalisierbar. Da die Galoisgruppe abelsch ist, folgt aus Satz Anhang 8.4. die simultane Diagonalisierbarkeit aller Automorphismen $\varphi_1, \ldots, \varphi_n$ $(n = \#(G))$. Das heißt, dass man $L = \bigoplus_{i=1}^n L_i$ mit eindimensionalen K-Untervektorräumen L_i schreiben kann, die unter jedem $\varphi \in \mathrm{Gal}\,(L|K)$ auf sich abgebildet werden. Zu jedem L_i und jedem φ ist dabei $\varphi(x) = \zeta_{i,\varphi} \cdot x$ für jedes $x \in L_i$, das Element $\zeta_{i,\varphi}$ beschreibt also den Eigenwert von φ auf L_i. Die Zuordnung

$$\delta_i \colon G \longrightarrow K^\times, \, \varphi \longmapsto \zeta_{i,\varphi},$$

ist dabei ein Charakter. Es ist $L_i \subseteq L_{\delta_i}$, da ja L_i die zu δ_i gehörende Eigenraumbedingung erfüllt. Wegen

$$n = \mathrm{grad}_K L = \#(G) = \#(D)$$

ist $L_i = L_{\delta_i}$ und jeder Charakter δ tritt als ein δ_i auf. Also ist $L = \bigoplus_{\delta \in D} L_\delta$. Die Stufe zum konstanten Charakter ist K. Für $x_1 \in L_{\delta_1}$ und $x_2 \in L_{\delta_2}$ und $\varphi \in G$ ist

$$\begin{aligned} \varphi(x_1 x_2) &= \varphi(x_1)\varphi(x_2) \\ &= \delta_1(\varphi) x_1 \delta_2(\varphi) x_2 \\ &= \delta_1(\varphi)\delta_2(\varphi) x_1 x_2 \\ &= (\delta_1 \cdot \delta_2)(\varphi) x_1 x_2, \end{aligned}$$

also $x_1 x_2 \in L_{\delta_1 \cdot \delta_2}$, so dass in der Tat eine graduierte Körpererweiterung vorliegt. □

Ein Beispiel wie $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-3}, \sqrt[3]{7}]$ zeigt, dass eine graduierte Körpererweiterung galoissch sein kann mit einer nichtkommutativen Galoisgruppe.

Korollar 18.3. *Sei* $m \in \mathbb{N}$ *und sei* K *ein Körper, der eine* m*-te primitive Einheitswurzel enthält. Es sei* $K \subseteq L$ *eine Kummererweiterung zum Exponenten* m *mit Galoisgruppe* G*, zugehöriger Charaktergruppe*

$$D = \mathrm{Char}\,(G, K)$$

und zugehöriger Graduierung

$$L = \bigoplus_{d \in D} L_d.$$

[16]Hier orientiert sich die Indizierung - entgegen der sonst üblichen additiven Schreibweise für eine graduierende Gruppe - an der multiplikativen Struktur von $\mathrm{Char}\,(G, K)$. Insbesondere ist L_1 die Stufe zum neutralen Element.

Es seien $H^\times$ die homogenen Elemente $\neq 0$ von L. Dann ist die natürliche Inklusion

$$H^\times \longrightarrow \left\{a \in L^\times \mid a^m \in K\right\}$$

ein Gruppenisomorphismus.

Beweis. Die Charaktergruppe $D = \operatorname{Char}(G, K)$ besitzt wegen der Voraussetzung über die Einheitswurzeln nach Lemma 14.10 den gleichen Exponenten wie G. Für ein homogenes Element $x \in L_d$ gilt also insbesondere $x^m \in L_{dm} = L_0 = K$,[17] so dass die linke Menge eine Teilmenge der rechten ist. Die Multiplikation ist links und rechts gleich, so dass eine Untergruppe vorliegt. Zum Nachweis der Surjektivität sei $a \in L^\times$ mit $a^m \in K$ vorgegeben. Wir zeigen, dass ein solches Element einen Charakter der Galoisgruppe definiert. Zu $\varphi \in \operatorname{Gal}(L|K)$ ist

$$\left(\frac{\varphi(a)}{a}\right)^m = \frac{(\varphi(a))^m}{a^m} = \frac{\varphi(a^m)}{a^m} = \frac{a^m}{a^m} = 1.$$

Der Bruch $\delta_a(\varphi) = \frac{\varphi(a)}{a}$ ist also eine m-te Einheitswurzel und gehört somit zu $K^\times$. Für zwei Automorphismen $\varphi, \psi \in \operatorname{Gal}(L|K)$ ist dabei

$$\begin{aligned}
\frac{(\varphi \circ \psi)(a)}{a} &= \frac{\varphi(\psi(a))}{a} \\
&= \frac{\varphi(a)}{a} \cdot \frac{\varphi(\psi(a))}{\varphi(a)} \\
&= \frac{\varphi(a)}{a} \cdot \varphi\left(\frac{\psi(a)}{a}\right) \\
&= \frac{\varphi(a)}{a} \cdot \frac{\psi(a)}{a},
\end{aligned}$$

so dass

$$\delta_a \colon \operatorname{Gal}(L|K) \longrightarrow K^\times,\ \varphi \longmapsto \frac{\varphi(a)}{a},$$

ein Charakter ist. Wegen $\varphi(a) = \frac{\varphi(a)}{a} a = \delta_a(\varphi) a$ ist $a \in L_{\delta_a}$, also homogen. □

Korollar 18.4. *Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Es sei $K \subseteq L$ eine Kummererweiterung zum Exponenten m. Dann ist $K \subseteq L$ eine Radikalerweiterung.*

Beweis. Dies folgt direkt aus Satz 18.2 und aus Lemma 12.10 (5). □

Innerhalb der Radikalerweiterungen sind die Kummererweiterungen speziell, nämlich von der folgenden Gestalt.

[17] Hier verwenden wir wieder additive Schreibweise.

Satz 18.5. *Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Es sei $K \subseteq L$ eine Körpererweiterung. Dann ist $K \subseteq L$ genau dann eine Kummererweiterung zum Exponenten m, wenn es eine Beschreibung*

$$L = K\left(\sqrt[m]{a_1}, \ldots, \sqrt[m]{a_r}\right)$$

mit $a_i \in K$ gibt.

Beweis. Aus Satz 18.2 und Lemma 12.10 (3) folgt, dass eine Kummererweiterung die angegebene Radikaldarstellung besitzt. Zum Beweis der Umkehrung sei $L = K(x_1, \ldots, x_r)$ mit $x_i^m = a_i \in K$. Wir müssen zeigen, dass diese Erweiterung galoissch mit abelscher Galoisgruppe ist. Es sei $\zeta \in K$ eine primitive m-te Einheitswurzel. Die Produkte $\zeta^\ell x_i$ erfüllen ebenfalls $\left(\zeta^\ell x_i\right)^m = a_i$. Da man die x_i als von 0 verschieden annehmen kann, und ζ primitiv ist, sind diese Produkte für jedes i untereinander verschieden. Dies bedeutet, dass die Polynome $X^m - a_1, \ldots, X^m - a_r$ über L in verschiedene Linearfaktoren zerfallen. Damit ist L der Zerfällungskörper dieser separablen Polynome, so dass nach Satz 16.6 eine Galoiserweiterung vorliegt. Sei $G = \mathrm{Gal}(L|K)$ die Galoisgruppe dieser Erweiterung. Für jedes $\varphi \in G$ und jedes i ist $\varphi(x_i)$ ebenfalls eine Lösung der Gleichung $X^m = a_i$ und daher ist $\varphi(x_i) = \zeta^\ell x_i$ mit einem gewissen (von φ und i abhängigen) ℓ. Für zwei Automorphismen $\varphi_1, \varphi_2 \in G$ ist daher

$$(\varphi_1 \circ \varphi_2)(x_i) = \varphi_1(\varphi_2(x_i)) = \varphi_1(\zeta^{\ell_2} x_i) = \zeta^{\ell_2}\varphi_1(x_i) = \zeta^{\ell_2}\zeta^{\ell_1} x_i = \zeta^{\ell_2+\ell_1} x_i.$$

Somit wirken die Automorphismen auf dem Erzeugendensystem kommutativ und daher ist $\varphi_1 \circ \varphi_2 = \varphi_2 \circ \varphi_1$. Damit ist die Galoisgruppe abelsch. Für jedes x_i ist ferner

$$\varphi^m(x_i) = \left(\zeta^\ell\right)^m x_i = x_i$$

mit einem gewissen ℓ. Also ist $\varphi^m = \mathrm{Id}$, so dass m ein Vielfaches des Exponenten ist. □

Beispiel 18.6. Der achte Kreisteilungskörper über $\mathbb{Q}$, also die (siehe Beipiel 9.15) (mehrfach) graduierte Körpererweiterung

$$\mathbb{Q} \subseteq L = K_8 = \mathbb{Q}[\mathrm{i}, \sqrt{2}] = \mathbb{Q}[X]/(X^4 + 1)$$

ist eine Kummererweiterung zum Exponenten 2 mit Galoisgruppe $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Die gemäß Satz 18.2 zugehörige $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$-Graduierung ist

$$\mathbb{Q} \oplus \mathbb{Q}\mathrm{i} \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\mathrm{i}\sqrt{2}\,.$$

Nach Korollar 18.3 gilt $H^\times = \{a \in L^\times \mid a^2 \in \mathbb{Q}\}$, d.h. die Menge der rationalen Quadratwurzeln von L sind einfach beschreibbar. Es gibt aber auch noch weitere Wurzeln aus rationalen Zahlen in L, beispielsweise die achte Einheitswurzel ζ_8, die eine vierte Wurzel von -1 ist.

18.2. **Das Lemma von Gauss und das Eisensteinkriterium.**

In der nächsten Vorlesung werden wir uns mit Kreisteilungskörpern beschäftigen. Dazu brauchen wir einige wichtige Irreduzibilitätskriterien für Polynome aus $\mathbb{Q}[X]$.

Die folgende Aussage heißt *Lemma von Gauß*.

Lemma 18.7. *Es sei $f \in \mathbb{Z}[X]$ ein nichtkonstantes Polynom derart, dass in $\mathbb{Z}[X]$ nur Faktorzerlegungen $f = gh$ mit $g \in \mathbb{Z}$ oder $h \in \mathbb{Z}$ möglich sind. Dann ist f irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Nehmen wir an, es gebe eine nicht-triviale Faktorzerlegung $f = gh$ mit nicht-konstanten Polynomen $g, h \in \mathbb{Q}[X]$. Sowohl in g als auch in h kommen nur endlich viele Nenner aus $\mathbb{Z}$ vor, so dass man mit einem gemeinsamen Hauptnenner $r \in \mathbb{Z}$ multiplizieren kann und somit eine Darstellung $rf = \tilde{g}\tilde{h}$ mit $\tilde{g}, \tilde{h} \in \mathbb{Z}[X]$ erhält. Dabei haben sich die Grade der beteiligten Polynome nicht geändert. Es sei $r = p_1 \cdots p_n$ die Primfaktorzerlegung von r. Nach Aufgabe 3.19 ist p_1 auch im Polynomring $\mathbb{Z}[X]$ prim. Da es das Produkt $\tilde{g}\tilde{h}$ teilt, muss es einen der Faktoren teilen, sagen wir $\tilde{h}$. Dann kann man mit p_1 kürzen und erhält eine Gleichung der Form

$$r'f = \tilde{g}\tilde{h}'.$$

Dabei ändern sich wieder die Grade nicht. So kann man sukzessive alle Primfaktoren wegkürzen und erhält schließlich eine Zerlegung

$$f = g'h'$$

mit nicht konstanten Polynomen $h', g' \in \mathbb{Z}[X]$ im Widerspruch zur Voraussetzung. □

Lemma 18.8. *Sei R ein Integritätsbereich und sei $F = \sum_{i=0}^{n} c_i X^i \in R[X]$ ein Polynom. Es sei $p \in R$ ein Primelement mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, alle anderen Koeffizienten teilt, aber dass p^2 nicht den konstanten Koeffizienten c_0 teilt. Dann besitzt F keine Zerlegung $F = GH$ mit nicht-konstanten Polynomen $G, H \in R[X]$.*

Beweis. Sei angenommen, dass es eine Zerlegung $F = GH$ mit nicht-konstanten Polynomen $G, H \in R[X]$ gebe, und sei $G = \sum_{i=0}^{k} a_i X^i$ und $H = \sum_{j=0}^{m} b_j X^j$. Dann ist $c_0 = a_0 b_0$ und dies ist ein Vielfaches von p, aber nicht von p^2. Da p prim ist, teilt es einen der Faktoren, sagen wir a_0, aber nicht den anderen. Es ist nicht jeder Koeffizient von G ein Vielfaches von p, da sonst G und damit auch F ein Vielfaches von p wäre, was aber aufgrund der Bedingung an den Leitkoeffizienten ausgeschlossen ist. Es sei r der kleinste Index derart, dass a_r kein Vielfaches von p ist. Es ist $r \leq \operatorname{grad}(G) < \operatorname{grad}(F)$, da H nicht konstant ist. Wir betrachten den Koeffizienten c_r, für den

$$c_r = a_0 b_r + a_1 b_{r-1} + \cdots + a_{r-1} b_1 + a_r b_0$$

gilt. Hierbei sind c_r und alle Summanden $a_i b_{r-i}$, $i = 0, \ldots, r-1$, Vielfache von p. Daher muss auch der letzte Summand $a_r b_0$ ein Vielfaches von p sein. Dies ist aber ein Widerspruch, da $p \nmid a_r$ und $p \nmid b_0$. □

Das folgende Kriterium für die Irreduzibilität von Polynomen heißt *Eisenstein-Kriterium*.

Satz 18.9. *Es sei $F = \sum_{i=0}^{n} c_i X^i \in \mathbb{Z}[X]$ ein Polynom. Es sei $p \in \mathbb{Z}$ eine Primzahl mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, aber alle anderen Koeffizienten teilt, aber dass p^2 nicht den konstanten Koeffizienten c_0 teilt. Dann ist F irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Dies folgt aus Lemma 18.8 und Lemma 18.7. □

18. Arbeitsblatt

18.1. **Aufwärmaufgaben.**

Aufgabe 18.1. Sei $K \subseteq L$ eine endliche Körpererweiterung und sei $\varphi \in \mathrm{Gal}\,(L|K)$ ein K-Automorphismus. Es sei λ ein Eigenwert von φ. Zeige, dass λ eine Einheitswurzel ist.

Aufgabe 18.2. Sei $K \subseteq L$ eine endliche Körpererweiterung und sei $\delta \in G^\vee$ ein Charakter auf der Galoisgruppe $G = \mathrm{Gal}\,(L|K)$. Man mache sich die Gleichheit

$$L_\delta = \{x \in L |\, \varphi(x) = \delta(\varphi) \cdot x \text{ für alle } \varphi \in G\} = \bigcap_{\varphi \in G} \mathrm{Eig}_{\delta(\varphi)}\,(\varphi)$$

klar.

Aufgabe 18.3. Bestimme die Eigenwerte und die Eigenräume des Frobeniushomomorphismus auf $\mathbb{F}_{125}$.

Aufgabe 18.4. Bestimme die Eigenwerte und die Eigenräume des Frobeniushomomorphismus auf $\mathbb{F}_{p^p}$.

Aufgabe 18.5. Zeige, dass die Körpererweiterung $\mathbb{Z}/(13) \subseteq \mathbb{F}_{2197}$ eine Kummererweiterung zum Exponenten 3 ist.

Aufgabe 18.6. Bestimme die Matrizen zu sämtlichen Körperautomorphismen in Beispiel 17.9 bezüglich einer geeigneten Basis.

Aufgabe 18.7.*

Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Der Körper K enthalte eine m-te primitive Einheitswurzel, wobei m der Exponent von D sei. Zeige, dass es ein Element $v \in L$ derart gibt, dass die Menge

$$\{\varphi(v) | \, \varphi \in \mathrm{Gal}\,(L|K)\}$$

eine K-Basis von L bildet.

Aufgabe 18.8.*

Sei $D = \mathbb{Z}/(n)$ und sei K ein Körper, der eine n-te primitive Einheitswurzel ζ enthält. Es sei L eine D-graduierte Körpererweiterung von K. Beschreibe die Matrizen der K-Algebraautomorphismen auf L (also die Elemente der Galoisgruppe $\mathrm{Gal}\,(L|K)$) bezüglich einer geeigneten K-Basis von L.

Aufgabe 18.9.*

(1) Bestimme den Zerfällungskörper L zum Polynom $X^4 - 7 \in \mathbb{Q}[X]$.
(2) Was ist der Grad $\mathbb{Q} \subseteq L$?
(3) Ist die Körpererweiterung graduierbar (mit welcher graduierenden Gruppe?).
(4) Was sind die homogenen Automorphismen, welche Gruppe bilden sie?
(5) Ist die Galoisgruppe $\mathrm{Gal}\,(L|\mathbb{Q})$ abelsch?
(6) Handelt es sich um eine Kummererweiterung (zu welchem Exponenten)?

Aufgabe 18.10. Es sei $\zeta_n \in \mathbb{C}$ eine n-te primitive Einheitswurzel, und $K = \mathbb{Q}[\zeta_n]$ der zugehörige Kreisteilungskörper. Zeige, dass es galoissche Körpererweiterungen $K \subseteq L$ gibt, deren Galoisgruppe zyklisch der Ordnung n ist.

Aufgabe 18.11. Es seien $F, G \in \mathbb{Z}[X]$ normierte Polynome mit der Eigenschaft, dass $F = GH$ ist mit $H \in \mathbb{Q}[X]$. Zeige, dass $H \in \mathbb{Z}[X]$ ist.

Aufgabe 18.12. Formuliere und beweise das „verschobene Eisensteinkriterium“. Man gebe auch ein Beispiel eines Polynoms $P \in \mathbb{Q}[X]$, wo man die Irreduzibilität nicht mit dem Eisensteinkriterium, aber mit dem verschobenen Eisensteinkriterium nachweisen kann.

Aufgabe 18.13. Formuliere und beweise das *umgekehrte Eisensteinkriterium*, bei dem die Rollen des Leitkoeffizienten und des konstanten Koeffizienten vertauscht werden.

Aufgabe 18.14. Wende eine Form des *Eisensteinkriteriums* an, um die Irreduzibilität der folgenden Polynome aus $\mathbb{Q}[X]$ nachzuweisen.

(1) $X^4 + 2X^2 + 2$,
(2) $20X^5 - 15X^4 + 125X^3 - 10X + 4$,
(3) $X^4 + 9$.

Aufgabe 18.15. Zeige mit Hilfe des verschobenen Eisensteinkriteriums, dass das Polynom $X^3 - 3X - 1$ irreduzibel in $\mathbb{Q}[X]$ ist.

Aufgabe 18.16. Zeige, dass das Polynom $X^3 + 2X^2 - 5$ in $\mathbb{Q}[X]$ irreduzibel ist.

Aufgabe 18.17. Zeige, dass ein Polynom der Form $X^n - p^2 \in \mathbb{Q}[X]$ mit einer Primzahl p im Allgemeinen nicht irreduzibel ist.

18.2. **Aufgaben zum Abgeben.**

Aufgabe 18.18. (1 Punkt)

Es sei p eine Primzahl. Zeige, dass die Polynome $X^n - p \in \mathbb{Q}[X]$ für jedes $n \geq 1$ irreduzibel sind.

Aufgabe 18.19. (6 Punkte)

Es sei p eine Primzahl. Betrachte das Polynom

$$P = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1.$$

Zeige, dass P irreduzibel in $\mathbb{Q}[X]$ ist.

Aufgabe 18.20. (3 Punkte)

Betrachte das Polynom

$$P = x^6 - 5x^5 + 11x^4 - 13x^3 + 9x^2 - 3x + 1.$$

Zeige, dass P irreduzibel in $\mathbb{Q}[X]$ ist.

Aufgabe 18.21. (4 Punkte)

Bestimme, ob die beiden folgenden Polynome in $\mathbb{Q}[x,y]$ irreduzibel sind.

a) $y^4+3x^2y^2+4x^7y+2x$.

b) $y^6+3xy^4+3x^2y^2+x^3$.

Aufgabe 18.22. (3 Punkte)

Bestimme die Eigenwerte und die Eigenräume des Frobeniushomomorphismus auf $\mathbb{F}_{343}$.

19. Vorlesung - Kreisteilungskörper

19.1. **Kreisteilungskörper.**

Definition 19.1. Der n-te *Kreisteilungskörper* ist der Zerfällungskörper des Polynoms

$$X^n-1$$

über $\mathbb{Q}$.

Offenbar ist 1 eine Nullstelle von X^n-1. Daher kann man X^n-1 durch $X-1$ teilen und erhält, wie man schnell nachrechnen kann,

$$X^n-1 = (X-1)\left(X^{n-1}+X^{n-2}+\cdots+X+1\right).$$

Wegen $1\in\mathbb{Q}$ ist daher der n-te Kreisteilungskörper auch der Zerfällungskörper von

$$X^{n-1}+X^{n-2}+\cdots+X+1\,.$$

Es gibt auch Kreisteilungskörper über anderen Körpern, da es ja stets Zerfällungskörper gibt. Wir beschränken uns aber weitgehend auf die Kreisteilungskörper über $\mathbb{Q}$, die wir auch mit K_n bezeichnen. Da X^n-1 auf die in der zweiten Vorlesung beschriebenen Art über $\mathbb{C}$ in Linearfaktoren zerfällt, kann man K_n als Unterkörper von $\mathbb{C}$ realisieren, und zwar ist K_n der von allen n-ten Einheitswurzeln erzeugte Unterkörper von $\mathbb{C}$. Dieser wird sogar schon von einer einzigen primitiven Einheitswurzel erzeugt.

Lemma 19.2. *Sei $n\in\mathbb{N}_+$. Dann wird der n-te Kreisteilungskörper über $\mathbb{Q}$ von $e^{2\pi\mathrm{i}/n}$ erzeugt. Der n-te Kreisteilungskörper ist also*

$$K_n = \mathbb{Q}\left(e^{2\pi\mathrm{i}/n}\right) = \mathbb{Q}[e^{2\pi\mathrm{i}/n}].$$

Insbesondere ist jeder Kreisteilungskörper eine einfache Körpererweiterung von $\mathbb{Q}$.[18]

Beweis. Es sei K_n der n-te Kreisteilungskörper über $\mathbb{Q}$. Wegen $\left(e^{2\pi\mathrm{i}/n}\right)^n = 1$ ist $\mathbb{Q}[e^{2\pi\mathrm{i}/n}]\subseteq K_n$. Wegen $\left(e^{2\pi\mathrm{i}/n}\right)^k = e^{2\pi\mathrm{i}k/n}$ gehören auch alle anderen Einheitswurzeln zu $\mathbb{Q}[e^{2\pi\mathrm{i}/n}]$, also ist $\mathbb{Q}[e^{2\pi\mathrm{i}/n}] = K_n$. □

[18]Dies ist natürlich auch klar aufgrund des Satzes vom primitiven Element.

Statt $e^{\frac{2\pi \mathrm{i}}{n}}$ kann man auch jede andere n-te primitive Einheitswurzel aus $\mathbb{C}$ als Erzeuger nehmen.

Beispiel 19.3. Wir bestimmen einige Kreisteilungskörper für kleine n. Bei $n = 1$ oder 2 ist der Kreisteilungskörper gleich $\mathbb{Q}$. Bei $n = 3$ ist

$$X^3 - 1 = (X-1)\left(X^2 + X + 1\right)$$

und der zweite Faktor zerfällt

$$X^2 + X + 1 = \left(X + \frac{1}{2} - \mathrm{i}\frac{\sqrt{3}}{2}\right)\left(X + \frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}\right).$$

Daher ist der dritte Kreisteilungskörper der von $\sqrt{-3} = \sqrt{3}\mathrm{i}$ erzeugte Körper, es ist also $K_3 = \mathbb{Q}[\sqrt{-3}]$ eine quadratische Körpererweiterung der rationalen Zahlen.

Bei $n = 4$ ist natürlich

$$\begin{aligned} X^4 - 1 &= \left(X^2 - 1\right)\left(X^2 + 1\right) \\ &= (X-1)(X+1)\left(X^2+1\right) \\ &= (X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i}). \end{aligned}$$

Der vierte Kreisteilungskörper ist somit $\mathbb{Q}[\mathrm{i}] \cong \mathbb{Q}[X]/(X^2+1)$, also ebenfalls eine quadratische Körpererweiterung von $\mathbb{Q}$.

Lemma 19.4. *Sei p eine Primzahl. Dann ist der p-te Kreisteilungskörper gleich*

$$\mathbb{Q}[X]/\left(X^{p-1} + X^{p-2} + \cdots + X^1 + 1\right).$$

Insbesondere besitzt der p-te Kreisteilungskörper den Grad $p-1$ über $\mathbb{Q}$.

Beweis. Der p-te Kreisteilungskörper wird nach Lemma 19.2 von $e^{2\pi \mathrm{i}/p}$ erzeugt, er ist also isomorph zu $\mathbb{Q}[X]/(P)$, wobei P das Minimalpolynom von $e^{2\pi \mathrm{i}/p}$ bezeichnet. Als Einheitswurzel ist $e^{2\pi \mathrm{i}/p}$ eine Nullstelle von $X^p - 1$ und wegen $e^{2\pi \mathrm{i}/p} \neq 1$ ist $e^{2\pi \mathrm{i}/p}$ eine Nullstelle von $X^{p-1} + X^{p-2} + \cdots + X^1 + 1$. Das Polynom $X^{p-1} + X^{p-2} + \cdots + X^1 + 1$ ist irreduzibel nach Aufgabe 18.19 und daher handelt es sich nach Lemma 7.12 (2) um das Minimalpolynom von $e^{2\pi \mathrm{i}/p}$. □

Beispiel 19.5. Der fünfte Kreisteilungskörper wird von der komplexen Zahl $e^{2\pi \mathrm{i}/5}$ erzeugt. Er hat aufgrund von Lemma 19.4 die Gestalt

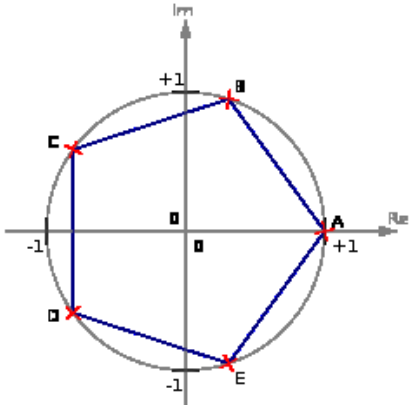
$$K_5 \cong \mathbb{Q}[X]/\left(X^4 + X^3 + X^2 + X + 1\right),$$

wobei die Variable X als $e^{2\pi \mathrm{i}/5}$ (oder eine andere primitive Einheitswurzel) zu interpretieren ist. Sei $x = e^{2\pi \mathrm{i}/5}$ und setze $u = 2x^4 + 2x + 1$. Aus Symmetriegründen muss dies eine reelle Zahl sein. Es ist

$$\begin{aligned} u^2 &= 4x^8 + 4x^2 + 1 + 8x^5 + 4x^4 + 4x \\ &= 4x^3 + 4x^2 + 1 + 8 + 4x^4 + 4x \\ &= 5 + 4\left(x^4 + x^3 + x^2 + x + 1\right) \\ &= 5. \end{aligned}$$

Es ist also $u = \sqrt{5}$ (die positive Wurzel) und somit haben wir eine Folge von quadratischen Körpererweiterungen

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}] \subset K_5.$$



Weiter unten werden wir für jedes n die Minimalpolynome der primitiven n-ten Einheitswurzeln bestimmen.

19.2. **Die Eulersche Funktion.**

Zur Bestimmung der Galoisgruppe des n-ten Kreisteilungskörpers sind die Einheiten im Restklassenring $\mathbb{Z}/(n)$ entscheidend.

Definition 19.6. Zu einer natürlichen Zahl n bezeichnet $\varphi(n)$ die Anzahl der Elemente von $(\mathbb{Z}/(n))^\times$. Man nennt $\varphi(n)$ die *Eulersche Funktion.*

Die Zahl $\varphi(n)$ gibt also an, wie viele natürliche Zahlen k, $1 \leq k \leq n$, teilerfremd zu n sind. In einem Körper, in dem es überhaupt eine n-te primitive Einheitswurzel gibt, gibt es genau $\varphi(n)$ primitive Einheitswurzeln, da dann die Gruppe der n-ten Einheitswurzeln isomorph zur zyklischen Gruppe der Ordnung n ist. Für eine Primzahl p ist $\varphi(p) = p - 1$.

Lemma 19.7. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung*

$$n = p_1^{r_1} \cdots p_k^{r_k}$$

(die p_i seien also verschieden und $r_i \geq 1$). Dann ist

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k}) = (p_1 - 1)p_1^{r_1 - 1} \cdots (p_k - 1)p_k^{r_k - 1}.$$

Beweis. Siehe Aufgabe 19.4. □

19.3. **Kreisteilungspolynome.**

Definition 19.8. Sei $n \in \mathbb{N}_+$ und seien $z_1, \ldots, z_{\varphi(n)}$ die primitiven komplexen Einheitswurzeln. Dann heißt das Polynom

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - z_i) \in \mathbb{C}[X]$$

das n-te *Kreisteilungspolynom*.

Nach Konstruktion hat das n-te Kreisteilungspolynom den Grad $\varphi(n)$.

Lemma 19.9. *Sei $n \in \mathbb{N}_+$. Dann gilt in $\mathbb{C}[X]$ die Gleichung*

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Beweis. Jede der n verschiedenen n-ten Einheitswurzeln besitzt eine Ordnung d, die ein Teiler von n ist. Eine n-te Einheitswurzel der Ordnung d ist eine primitive d-te Einheitswurzel. Die Aussage folgt daher aus

$$\begin{aligned} X^n - 1 &= \prod_{z \text{ ist } n\text{-te Einheitswurzel}} (X - z) \\ &= \prod_{d|n} \left(\prod_{z \text{ ist primitive } d\text{-te Einheitswurzel}} (X - z) \right) \\ &= \prod_{d|n} \Phi_d. \end{aligned}$$

□

Lemma 19.10. *Die Koeffizienten der Kreisteilungspolynome liegen in $\mathbb{Z}$.*

Beweis. Induktion über n. Für $n = 1$ ist $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Für beliebiges n betrachten wir die in Lemma 19.9 bewiesene Darstellung

$$X^n - 1 = \prod_{d|n} \Phi_d = \left(\prod_{d|n,\, d \neq n} \Phi_d \right) \cdot \Phi_n.$$

Der linke Faktor ist ein normiertes Polynom und er besitzt nach der Induktionsvoraussetzung Koeffizienten in $\mathbb{Z}$. Daraus folgt mit Aufgabe 18.11, dass auch Φ_n Koeffizienten in $\mathbb{Z}$ besitzt. □

Grundlegend ist die folgende Aussage.

Satz 19.11. *Die Kreisteilungspolynome Φ_n sind irreduzibel über $\mathbb{Q}$.*

Beweis. Nehmen wir an, dass Φ_n nicht irreduzibel über $\mathbb{Q}$ ist. Dann gibt es nach Lemma 18.7 eine Zerlegung $\Phi_n = FG$ mit normierten Polynomen

$F, G \in \mathbb{Z}[X]$ von kleinerem Grad. Wir fixieren eine primitive n-te Einheitswurzel ζ. Dann ist nach Definition der Kreisteilungspolynome $\Phi_n(\zeta) = 0$ und daher ist (ohne Einschränkung) $F(\zeta) = 0$. Wir können annehmen, dass F irreduzibel und normiert ist, also das Minimalpolynom von ζ ist.Wir werden zeigen, dass jede primitive n-te Einheitswurzel ebenfalls eine Nullstelle von F ist. Dann folgt aus Gradgründen $\operatorname{grad}(F) = \varphi(n) = \operatorname{grad}(\Phi_n)$ im Widerspruch zur Reduzibilität. Jede primitive Einheitswurzel kann man als ζ^k mit einer zu n teilerfremden Zahl k schreiben. Es genügt dabei, den Fall ζ^p mit einer zu n teilerfremden Primzahl p zu betrachten, da sich jedes ζ^k sukzessive als p-Potenz von ζ erhalten lässt (wobei man ζ sukzessive durch ζ^p ersetzt und $F(\zeta^p) = 0$ verwendet). Nehmen wir also an, dass $F(\zeta^p) \neq 0$ ist. Dann muss $G(\zeta^p) = 0$ sein. Daher ist ζ eine Nullstelle des Polynoms $G(X^p)$ und daher gilt $FH = G(X^p)$ mit $H \in \mathbb{Q}[X]$, da ja F das Minimalpolynom von ζ ist. Wegen Aufgabe 18.11 gehören die Koeffizienten von H zu $\mathbb{Z}$. Wir betrachten nun die Polynome Φ_n, F, G, H modulo p, also als Polynome in $\mathbb{Z}/(p)[X]$, wobei wir dafür $\overline{\Phi_n}, \overline{F}$ usw. schreiben. Aufgrund des Frobeniushomomorphismus in Charakteristik p und wegen des kleinen Fermat'schen Satzes gilt

$$\overline{G}(X^p) = \left(\overline{G}(X)\right)^p.$$

Daher ist

$$\overline{FH} = \overline{G}(X^p) = (\overline{G}(X))^p.$$

Sei nun $\mathbb{Z}/(p) \subseteq L$ der Zerfällungskörper von $X^n - 1$ über $\mathbb{Z}/(p)$, so dass über L insbesondere auch $\overline{\Phi_n}$ und damit auch $\overline{F}$ in Linearfaktoren zerfällt. Sei $u \in L$ eine Nullstelle von $\overline{F}$. Dann ist u wegen der obigen Teilbarkeitsbeziehung auch eine Nullstelle von $\overline{G}$. Wegen $\overline{\Phi_n} = \overline{FG}$ ist dann u eine mehrfache Nullstelle von $\overline{\Phi_n}$. Damit besitzt auch $X^n - 1$ eine mehrfache Nullstelle in L. Nach dem formalen Ableitungskriterium ist aber $(X^n - 1)' = (n \bmod p)X^{n-1}$ und dieser Koeffizient ist wegen der vorausgesetzten Teilerfremdheit nicht 0. Also erzeugt das Polynom $X^n - 1$ und seine Ableitung das Einheitsideal, so dass es nach Aufgabe 11.28 keine mehrfache Nullstellen geben kann und wir einen Widerspruch erhalten. □

Korollar 19.12. *Der n-te Kreisteilungskörper K_n über $\mathbb{Q}$ hat die Beschreibung*

$$K_n = \mathbb{Q}[X]/(\Phi_n),$$

wobei Φ_n das n-te Kreisteilungspolynom bezeichnet. Der Grad des n-ten Kreisteilungskörpers ist $\varphi(n)$.

Beweis. Es ist $K_n = \mathbb{Q}[\zeta]$, wobei ζ eine primitive n-te Einheitswurzel ist. Nach Definition des Kreisteilungspolynoms ist $\Phi_n(\zeta) = 0$ und nach Satz 19.11 ist das Kreisteilungspolynom irreduzibel, so dass es sich um das Minimalpolynom von ζ handeln muss. Also ist nach Satz 7.11 $K_n \cong \mathbb{Q}[X]/(\Phi_n)$. □

Das im vorstehenden Beweis verwendete Beweisverfahren nennt man *Reduktion zu positiver Charakteristik*.

19. Arbeitsblatt

19.1. **Aufwärmaufgaben.**

Aufgabe 19.1.*

Bestimme die Primfaktorzerlegung des Polynoms $X^6 - 1$ über den Körpern $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(7)$ und $\mathbb{Z}/(5)$.

Aufgabe 19.2. Berechne die Werte der eulerschen Funktion $\varphi(n)$ für $n \leq 20$.

Man diskutiere dabei auch die Einheitenversion des Chinesischen Restsatzes, siehe Anhang 4.

Aufgabe 19.3. Zeige, dass die eulersche Funktion φ für natürliche Zahlen n, m die Eigenschaft

$$\varphi(\mathrm{ggT}(m,n)) \cdot \varphi(\mathrm{kgV}(m,n)) \;=\; \varphi(n) \cdot \varphi(m)$$

erfüllt.

Aufgabe 19.4.*

Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung

$$n \;=\; p_1^{r_1} \cdots p_k^{r_k}.$$

Zeige, dass dann

$$\varphi(n) \;=\; \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k}) \;=\; (p_1 - 1) p_1^{r_1 - 1} \cdots (p_k - 1) p_k^{r_k - 1}$$

gilt.

Aufgabe 19.5.*

Sei $a \in \mathbb{N}$. Zeige, dass die eulersche Funktion φ die Gleichheit

$$\varphi(a^n) \;=\; a^{n-1} \varphi(a)$$

für $n \geq 1$ erfüllt.

Aufgabe 19.6. Beweise die *eulersche Formel* für die eulersche Funktion, das ist die Aussage, dass

$$\varphi(n) = n \cdot \prod_{p|n,\ p \text{ prim}} \left(1 - \frac{1}{p}\right)$$

gilt.

Aufgabe 19.7. Sei $\varphi(n)$ die Eulersche Funktion. Zeige die Abschätzung

$$\varphi(n) \geq \frac{\sqrt{n}}{2}.$$

Aufgabe 19.8. Bestimme für $n = 1, 2, \ldots, 10$ die primitiven komplexen Einheitswurzeln ζ_n^k, mit $\zeta_n = e^{2\pi \mathrm{i}/n}$.

Aufgabe 19.9. Schreibe den 5-ten Kreisteilungskörper K_5 als quadratische Körpererweiterung von $\mathbb{Q}[\sqrt{5}]$.

Aufgabe 19.10. Es sei L der neunte Kreisteilungskörper über $\mathbb{Q}$. Zeige

$$L \cap \mathbb{R} \cong \mathbb{Q}[X]/\left(X^3 - 3X + 1\right).$$

Aufgabe 19.11.* Es sei K_n der n-te Kreisteilungskörper über $\mathbb{Q}$ und

$$R_n = K_n \cap \mathbb{R}.$$

Zeige, dass bei $n \geq 2$ die Körpererweiterung $R_n \subseteq K_n$ den Grad 2 besitzt.

Aufgabe 19.12. Es sei $n \in \mathbb{N}$ ungerade. Zeige, dass der n-te Kreisteilungskörper mit dem $2n$-ten Kreisteilungskörper übereinstimmt.

Aufgabe 19.13. Bestimme die Kreisteilungspolynome Φ_n für $n \leq 15$.

Aufgabe 19.14. Bestimme für $n \leq 12$, welche der n-ten Einheitswurzeln in K_n zueinander konjugiert sind.

Aufgabe 19.15. Zeige, dass für $n \geq 2$ der konstante Koeffizient der Kreisteilungspolynome Φ_n immer 1 ist.

Aufgabe 19.16.*

Es sei $\mathbb{Q} \subseteq K_n$ (in $\mathbb{C}$) der n-te Kreisteilungskörper und sei ζ eine n-te primitive Einheitswurzel. Wir betrachten die Elemente ζ^i, $i \in (\mathbb{Z}/(n))^\times$.

a) Zeige, dass für eine Primzahl $n = p$ diese Elemente eine $\mathbb{Q}$-Basis von K_n bilden.

b) Sei p eine Primzahl und $n = p^2$. Zeige, dass diese Elemente keine $\mathbb{Q}$-Basis von K_n bilden.

Aufgabe 19.17. Es sei $n \in \mathbb{N}$, $\mathbb{Q} \subseteq K_n$ der n-te Kreisteilungskörper und sei ζ eine n-te primitive Einheitswurzel.

(1) Zeige, dass für jedes k die (benachbarten) Einheitswurzeln
$$\zeta^k, \zeta^{k+1}, \ldots, \zeta^{k+\varphi(n)-1}$$
eine $\mathbb{Q}$-Basis von K_n.
(2) Bilden die primitiven n-ten Einheitswurzeln stets eine $\mathbb{Q}$-Basis von K_n?

Aufgabe 19.18. Bestimme die Norm und die Spur der n-ten komplexen Einheitswurzeln im n-ten Kreisteilungskörper.

Über einem beliebigen Körper K werden Kreisteilungskörper folgendermaßen definiert.

Es sei K ein Körper und $n \in \mathbb{N}$. Der n-te *Kreisteilungskörper über K* ist der Zerfällungskörper des Polynoms
$$X^n - 1$$
über K.

Aufgabe 19.19. Sei p eine Primzahl und $q = p^e$, $e \geq 1$, eine Primzahlpotenz. Zeige, dass der $(q-1)$-te Kreisteilungskörper über $\mathbb{F}_p$ gleich $\mathbb{F}_q$ ist.

Aufgabe 19.20. Erstelle eine Tabelle, die für die ersten zwölf Primzahlen p und für $n = 1, \ldots, 12$ angibt, welcher endliche Körper $\mathbb{F}_{p^e}$ der n-te Kreisteilungskörper über $\mathbb{F}_p$ ist.

(Man trage die Exponenten e ein; es empfiehlt sich zur Probe, die Zeilen und Spalten unabhängig voneinander durchzurechnen.)

p	1	2	3	4	5	6	7	8	9	10	11	12
2	1	1	2	1	4							
3	1											
5	1											
7	1											
11	1											
13	1											
17	1											
19	1											
23	1											
29	1											
31	1											
37	1											

Aufgabe 19.21. Es sei Φ_n das n-te Kreisteilungspolynom und es sei p eine zu n teilerfremde Primzahl. Es sei K ein Körper der Charakteristik p, in dem es eine n-te primitive Einheitswurzel ζ gebe. Zeige, dass das Produkt

$$\prod_{0<i<n,\ i,n \text{ teilerfremd}} (X - \zeta^i)$$

zu $\mathbb{Z}/(p)[X]$ gehört und mit $\Phi_n \bmod p$ übereinstimmt.

Aufgabe 19.22. Man lege eine Tabelle an, die für Primzahlen $p \leq 13$ zeigt, wie die Primfaktorzerlegung der Kreisteilungspolynome in $\mathbb{Z}/(p)[X]$ aussieht.

19.2. **Aufgaben zum Abgeben.**

Aufgabe 19.23. (4 Punkte)

Sei $\varphi(n)$ die Eulersche Funktion. Zeige, dass die Folge $\frac{\varphi(n)}{n}$, $n \in \mathbb{N}$, sowohl in 1 als auch in $\frac{1}{3}$ einen Häufungspunkt besitzt.

Aufgabe 19.24. (4 Punkte)

Zeige, dass das achte Kreisteilungspolynom $X^4 + 1$ über allen endlichen Primkörpern $\mathbb{F}_p$ reduzibel ist.

Hinweis: Zeige, dass $\mathbb{F}_{p^2}$ für $p \neq 2$ bereits eine primitive achte Einheitswurzel enthält.

Aufgabe 19.25. (4 Punkte)

Es sei p eine Primzahl und n eine natürliche Zahl, die wir als $n = kp^a$ schreiben mit k und p teilerfremd. Zeige, dass der n-te Kreisteilungskörper über $\mathbb{F}_p$ gleich $\mathbb{F}_q$ ist (mit $q = p^e$), wobei q die minimale echte Potenz von p mit der Eigenschaft ist, dass $q-1$ ein Vielfaches von k ist. Zeige insbesondere, dass es ein solches q gibt.

Aufgabe 19.26. (2 Punkte)

Bestimme die Kreisteilungskörper über $\mathbb{R}$.

Aufgabe 19.27. (4 Punkte)

Wir betrachten die Tabelle, die für kleine p und n die endlichen Kreisteilungskörper beschreibt.

p	1	2	3	4	5	6	7	8	9	10	11	12
2	1	1	2	1	4	2	3	1	6	4	10	2
3	1	1	1	2	4	1	6	2	1	4	5	2
5	1	1	2	1	1	2	6	2	6	1	5	2
7	1	1	1	2	4	1	1	2	3	4	10	2
11	1	1	2	2	1	2	3	2	6	1	1	2
13	1	1	1	1	4	1	2	2	3	4	10	1
17	1	1	2	1	4	2	6	1	2	4	10	2
19	1	1	1	2	2	1	6	2	1	2	10	2
23	1	1	2	2	4	2	3	2	6	4	1	2
29	1	1	2	1	2	2	1	2	6	2	10	2
31	1	1	1	2	1	1	6	2	3	1	5	2
37	1	1	1	1	4	1	3	2	1	4	5	1

Begründe die folgenden (mehr oder weniger sichtbaren) Eigenschaften der Tabelle.

a) Für jedes n sind die Einträge in der n-ten Spalte $\leq \varphi(n)$.

b) Für jedes p kommt in der p-ten Zeile die 1 unendlich oft vor.

In der folgenden Aufgabe soll eine Eigenschaft bewiesen werden, die in der Tabelle über Kreisteilungspolynome modulo p sichtbar wurde.

Aufgabe 19.28. (6 Punkte)

Es sei Φ_n das n-te Kreisteilungspolynom und es sei p eine Primzahl. Zeige, dass das Polynom $(\Phi_n \bmod p) \in \mathbb{Z}/(p)[X]$ das Produkt von irreduziblen Polynomen ist, die alle den gleichen Grad besitzen.

Tipp: Reduziere auf den Fall, wo n und p teilerfremd ist.

20. Vorlesung - Kreisteilungskörper II

In dieser Vorlesung möchten wir zunächst nachweisen, dass es sich bei einem Kreisteilungskörper über $\mathbb{Q}$ um eine Galoiserweiterung handelt, deren Galoisgruppe abelsch ist und eine Struktur besitzt, die unmittelbar mit den Einheitswurzeln zusammenhängt.

20.1. **Kreisteilungskörper als Galoiserweiterung.**

Wir kommen nun zur Galoiseigenschaft der Kreisteilungskörper über $\mathbb{Q}$.

Satz 20.1. *Es sei K_n der n-te Kreisteilungskörper. Dann ist $\mathbb{Q} \subseteq K_n$ eine Galoiserweiterung mit der Galoisgruppe*

$$\operatorname{Gal}(K_n|\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times .$$

Dabei entspricht der Einheit $a \in (\mathbb{Z}/(n))^\times$ derjenige Automorphismus $\varphi_a \in \operatorname{Gal}(K_n|\mathbb{Q})$, der eine n-te Einheitswurzel ζ auf ζ^a abbildet.

Beweis. Nach Korollar 19.12 ist

$$K_n = \mathbb{Q}[X]/(\Phi_n),$$

wobei Φ_n das n-te Kreisteilungspolynom ist. Dieses ist das Produkt $\Phi_n = \prod_{i=1}^{\varphi(n)}(X - z_i)$ über alle primitiven Einheitswurzeln und damit vom Grad $\varphi(n)$. Da der Kreisteilungskörper all diese primitiven Einheitswurzeln enthält, zerfällt das Kreisteilungspolynom über K_n in Linearfaktoren und daher ist K_n der Zerfällungskörper des Kreisteilungspolynoms und somit nach Satz 16.6 eine Galoiserweiterung.

Es sei nun ζ eine primitive n-te Einheitswurzel, und zwar diejenige, die bei der obigen Restklassenidentifizierung der Variablen X entspricht. Zu $a \in (\mathbb{Z}/(n))^\times$ ist ζ^a ebenfalls eine primitive Einheitswurzel. Wir betrachten den Einsetzungshomomorphismus

$$\mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]/(\Phi_n),\ X \longmapsto \zeta^a.$$

Dieser ist surjektiv, da ζ^a den Kreisteilungskörper erzeugt. Wegen $\Phi_n(\zeta^a) = 0$ induziert dies einen Automorphismus

$$\mathbb{Q}[X]/(\Phi_n) \longrightarrow \mathbb{Q}[X]/(\Phi_n),\ \zeta \longmapsto \zeta^a.$$

Dadurch erhalten wir eine Zuordnung

$$(\mathbb{Z}/(n))^\times \longrightarrow \operatorname{Gal}(K_n|\mathbb{Q}),\ a \longmapsto \varphi_a.$$

Für $a, a' \in (\mathbb{Z}/(n))^\times$ ist

$$\varphi_{aa'}(\zeta) = \zeta^{aa'} = \left(\zeta^{a'}\right)^a = \varphi_a\left(\zeta^{a'}\right) = \varphi_a(\varphi_{a'}(\zeta)) = (\varphi_a \circ \varphi_{a'})(\zeta),$$

so dass $\varphi_{aa'} = \varphi_a \circ \varphi_{a'}$ gilt (da die Automorphismen auf dem Erzeuger ζ festgelegt sind). Die Zuordnung ist also ein Gruppenhomomorphismus. Für

verschiedene Einheiten $a \neq a'$ ist $\zeta^a \neq \zeta^{a'}$ und somit $\varphi_a \neq \varphi_{a'}$. Die Abbildung ist also injektiv. Da es links und rechts $\varphi(n)$ Elemente gibt, ist die Abbildung eine Bijektion. □

Beispiel 20.2. Wir betrachten den achten Kreisteilungskörper K_8. Die Einheitengruppe $(\mathbb{Z}/(8))^\times$ ist $\{1,3,5,7\}$, wobei $3,5,7$ die Ordnung 2 besitzen. Die nach Satz 20.1 zugehörigen Körperautomorphismen sind neben der Identität die Abbildungen φ_3, φ_5, φ_7, die auf den Einheitswurzeln (ζ sei eine primitive achte Einheitswurzel) folgendermaßen wirken.

$$\varphi_3 : \zeta \longleftrightarrow \zeta^3,\ \zeta^2 = \mathrm{i} \longleftrightarrow \zeta^6 = -\mathrm{i},\ \zeta^5 \longleftrightarrow \zeta^7\,,$$

$$\varphi_5 : \zeta \longleftrightarrow \zeta^5,\ \mathrm{i} = \zeta^2 \longleftrightarrow \zeta^{10} = \mathrm{i},\ \zeta^3 \longleftrightarrow \zeta^7,\ -\mathrm{i} \longleftrightarrow -\mathrm{i}\,,$$

und

$$\varphi_7 : \zeta \longleftrightarrow \zeta^7,\ \mathrm{i} = \zeta^2 \longleftrightarrow \zeta^{14} = -\mathrm{i},\ \zeta^3 \longleftrightarrow \zeta^5\,.$$

Korollar 20.3. *Zu jeder endlichen abelschen Gruppe G gibt es eine endliche Galoiserweiterung $\mathbb{Q} \subseteq L$, deren Galoisgruppe gleich G ist.*

Beweis. Nach einem Satz, den wir hier nicht beweisen, lässt sich G als Restklassengruppe einer Einheitengruppe $(\mathbb{Z}/(n))^\times$ auffassen. Es sei

$$q\colon\ (\mathbb{Z}/(n))^\times \longrightarrow G$$

der zugehörige surjektive Restklassenhomomorphismus und H der Kern davon. Nach Satz 20.1 ist $(\mathbb{Z}/(n))^\times$ die Galoisgruppe der n-ten Kreisteilungserweiterung $\mathbb{Q} \subseteq K_n$. Es sei $M \subseteq K_n$ der Fixkörper zu H. Nach Satz 17.5 ist $\mathbb{Q} \subseteq M$ eine Galoiserweiterung mit Galoisgruppe G. □

Es ist ein offenes Problem, ob jede endliche Gruppe als Galoisgruppe einer Galoiserweiterung von $\mathbb{Q}$ auftritt. Diese Fragestellung gehört zur sogenannten *inversen Galoistheorie*.

20.2. **Galoiseigenschaften des Kompositums.**

Wir betrachten eine wichtige Konstruktion, das sogenannte Kompositum.

Definition 20.4. Sei $K \subseteq L$ eine Körpererweiterung und seien $K \subseteq M_1, M_2 \subseteq L$ zwei Zwischenkörper. Dann nennt man den von M_1 und M_2 erzeugten Unterkörper das *Kompositum* der beiden Körper (in L). Es wird mit M_1M_2 bezeichnet.

Das Kompositum hängt vom Oberkörper ab. Wenn man von endlichen Körpererweiterungen $K \subseteq M_1$ und $K \subseteq M_2$ ausgeht, so sichert Aufgabe 10.11, dass es überhaupt einen gemeinsamen Oberkörper gibt.

Lemma 20.5. *Es sei $K \subseteq L$ eine endliche separable Körpererweiterung und sei $K \subseteq K'$ eine weitere Körpererweiterung mit dem gemeinsamen Oberkörper M, in dem das Kompositum $L' = LK'$ gebildet sei. Dann ist $K' \subseteq L'$ ebenfalls eine endliche separable Körpererweiterung.*

Beweis. Es sei $K \subseteq L = K[x_1, \ldots, x_n]$ separabel, und seien $F_i \in K[X]$ die zu x_i gehörigen (separablen) Minimalpolynome. Dann ist $L' = K'[x_1, \ldots, x_n]$ und die Minimalpolynome G_i der x_i über K' sind in $K'[X]$ Teiler der F_i und daher selbst separabel. Nach Satz 13.11 ist $K' \subseteq L'$ eine separable Körpererweiterung. □

Lemma 20.6. *Es sei $K \subseteq L$ eine endliche normale Körpererweiterung und sei $K \subseteq K'$ eine weitere Körpererweiterung mit dem gemeinsamen Oberkörper M, in dem das Kompositum $L' = LK'$ gebildet sei. Dann ist $K' \subseteq L'$ ebenfalls eine normale Körpererweiterung.*

Beweis. Wir können $L = K[x_1, \ldots, x_n]$ schreiben, und wir wissen, dass es zugehörige Polynome $F_i \in K[X]$ mit $F_i(x_i) = 0$ gibt, die über L zerfallen. Daher ist $L' = K'[x_1, \ldots, x_n]$ und dieselben Polynome, aufgefasst in $K'[X]$, erfüllen die gleichen Eigenschaften. Aus Satz 15.4 (3) ergibt sich die Normalität. □

Aus diesen zwei Lemmata ergibt sich der folgende Satz, der für die Charakterisierung der auflösbaren Körpererweiterungen wichtig ist.

Satz 20.7. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und sei $K \subseteq K'$ eine weitere Körpererweiterung mit dem gemeinsamen Oberkörper M, in dem das Kompositum $L' = LK'$ gebildet sei. Dann ist $K' \subseteq L'$ ebenfalls eine endliche Galoiserweiterung, und für ihre Galoisgruppe gilt die natürliche Isomorphie*

$$\mathrm{Gal}\,(L'|K') \cong \mathrm{Gal}\,(L|L \cap K').$$

Beweis. Die Erweiterung $K' \subseteq L'$ ist normal nach Lemma 20.6 und separabel nach Lemma 20.5, also eine Galoiserweiterung aufgrund von Satz 16.6. Zur Berechnung der Galoisgruppe gehen wir von der Einschränkungsabbildung

$$\Psi\colon\ \mathrm{Gal}\,(L'|K') \longrightarrow \mathrm{Gal}\,(L|K),\ \varphi \longmapsto \varphi|_L,$$

aus, die wegen der Normalität von $K \subseteq L$ nach Satz 15.4 (4) ein wohldefinierter Gruppenhomomorphismus ist. Es sei $\varphi \in \mathrm{Gal}\,(L'|K')$ ein Automorphismus, dessen Bild unter diesem Homomorphismus trivial sei, also $\varphi|_L = \mathrm{Id}_L$. Da auch $\varphi|_{K'} = \mathrm{Id}_{K'}$ gilt, ist φ auf dem Kompositum $L' = LK'$ die Identität, also das neutrale Element. Daher ist Ψ nach dem Kernkriterium injektiv. Das Bild von Ψ ist eine Untergruppe $H = \mathrm{bild}\,\Psi \subseteq \mathrm{Gal}\,(L|K)$. Aufgrund der Galoiskorrespondenz gibt es einen Zwischenkörper Z, $K \subseteq$

$Z \subseteq L$, mit $H = \mathrm{Gal}\,(L|Z)$, und zwar ist Z der Fixkörper von H. Es liegt also insgesamt die Situation

$$\mathrm{Gal}\,(L'|K') \xrightarrow{\cong} \mathrm{bild}\,\Psi = H = \mathrm{Gal}\,(L|Z) \subseteq \mathrm{Gal}\,(L|K)$$

vor. Wir behaupten $L \cap K' = Z$. Für jedes $\varphi \in \mathrm{Gal}\,(L'|K')$ ist $\varphi|_{K'} = \mathrm{Id}_{K'}$, und daher ist auch $(\varphi|_L)|_{L\cap K'} = \mathrm{Id}_{L\cap K'}$. Also ist $L \cap K' \subseteq Z$. Wenn $x \in Z$ ist, so bedeutet dies, dass für jedes $\varphi \in \mathrm{Gal}\,(L'|K')$ die Gleichheit $(\varphi|_L)(x) = x$ gilt. Dann ist aber $x \in K'$ nach Satz 16.6, da $K' \subseteq L'$ eine Galoiserweiterung ist. Somit ist $x \in L \cap K'$. Insgesamt ist also

$$\mathrm{Gal}\,(L'|K') \cong \mathrm{bild}\,\Psi = \mathrm{Gal}\,(L|L \cap K').$$

□

20. Arbeitsblatt

20.1. **Aufwärmaufgaben.**

Aufgabe 20.1. Bestimme für jedes $n = 1, 2, \ldots, 10$, für welche k der durch

$$\zeta_n \mapsto \zeta_n^k$$

festgelegte Automorphismus des Kreisteilungskörpers K_n ein Erzeuger der Galoisgruppe ist.

Aufgabe 20.2. Es sei K_n der n-te Kreisteilungskörper über $\mathbb{Q}$. Zeige, dass derjenige Automophismus von K_n, der der Einheit $-1 \in (\mathbb{Z}/(n))^\times$ entspricht, die Einschränkung der komplexen Konjugation ist.

Aufgabe 20.3. Es sei n eine durch 4 teilbare Zahl, W_n die Menge der n-ten komplexen Einheitswurzeln und K_n der n-te Kreisteilungskörper.

(1) Definiert die Spiegelung an der imaginären Achse eine Permutation von W_n?
(2) Definiert die Spiegelung an der imaginären Achse eine $\mathbb{Q}$-lineare Abbildung auf K_n?
(3) Definiert die Spiegelung an der imaginären Achse einen $\mathbb{Q}$-Körperautomorphismus auf K_n?

Aufgabe 20.4. Es sei $\zeta = e^{2\pi \mathrm{i}/10}$. Bestimme den (alle?) Körperautomorphismus $K_{10} \to K_{10}$, der ζ^3 auf ζ^7 abbildet. Wohin wird ζ^9 abgebildet?

Aufgabe 20.5.*

Wir betrachten den fünften Kreisteilungskörper K_5 mit der $\mathbb{Q}$-Basis $1, \zeta, \zeta^2, \zeta^3$, wobei $\zeta = e^{2\pi \mathrm{i}/5}$ ist.

(1) Bestimme die Multiplikationsmatrizen zu ζ^i, $i = 0, 1, 2, 3$, bezüglich dieser Basis.
(2) Bestimme die Matrizen zu den Elementen der Galoisgruppe Gal $(K_5|\mathbb{Q})$ bezüglich dieser Basis.

Aufgabe 20.6.*

Bestimme die Zwischenkörper des 7-ten Kreisteilungskörpers K_7. Dabei soll jeweils eine Restklassendarstellung explizit angegeben werden.

Aufgabe 20.7. Bestimme für $n \leq 12$, wie viele Unterkörper der n-te Kreisteilungskörper K_n besitzt und wie viele davon selbst Kreisteilungskörper sind.

Aufgabe 20.8. Es sei $\mathbb{Q} \subseteq K_n$ ein Kreisteilungskörper und $L \subseteq K_n$ ein Zwischenkörper. Zeige, dass $\mathbb{Q} \subseteq L$ eine abelsche Körpererweiterung ist, also eine Galoiserweiterung, deren Galoisgruppe abelsch ist.

Ein schwieriger Satz, der *Satz von Kronecker-Weber*, besagt umgekehrt, dass man jede abelsche Körpererweiterung von $\mathbb{Q}$ als Unterkörper eines Kreisteilungskörpers realisieren kann.

Aufgabe 20.9.*

Realisiere die folgenden Gruppen als Galoisgruppe einer geeigneten Körpererweiterung $\mathbb{Q} \subseteq L$.

(1) $\mathbb{Z}/(4)$,
(2) $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$,
(3) $\mathbb{Z}/(2) \times \mathbb{Z}/(4)$,
(4) $\mathbb{Z}/(8)$.

Aufgabe 20.10. Zeige, dass das Kompositum K_1K_2 zu zwei Körpererweiterungen $K \subseteq K_1$ und $K \subseteq K_2$ vom gewählten Oberkörper abhängen kann.

Aufgabe 20.11. Es seien $K \subseteq K_1$ und $K \subseteq K_2$ zwei Körpererweiterungen vom Grad d_1 bzw. d_2. Es sei K_1K_2 das in einem Oberkörper gebildete Kompositum. Zeige, dass die Abschätzung $\operatorname{grad}_K K_1K_2 \leq d_1d_2$ gilt.

Aufgabe 20.12. Es sei K ein Körper und es seien $K \subseteq K_1 \cong K[X]/F(X)$ und $K \subseteq K_2 \cong K[Y]/G(Y)$ zwei endliche einfache Körpererweiterungen von K.

a) Zeige, dass die K-Algebra $A = K[X,Y]/(F,G)$ kein Körper sein muss.

b) Es sei K_1K_2 das in einem gemeinsamen Oberkörper gebildete Kompositum. Zeige, dass es einen surjektiven K-Algebrahomomorphismus von A nach K_1K_2 gibt.

Aufgabe 20.13. Es sei p eine Primzahl und sei $\mathbb{F}_{q_1}$ der Körper mit $q_1 = p^{e_1}$ und $\mathbb{F}_{q_2}$ der Körper mit $q_2 = p^{e_2}$ Elementen. Zeige, dass das Kompositum (unabhängig vom gewählten Oberkörper) von $\mathbb{F}_{q_1}$ und $\mathbb{F}_{q_2}$ gleich $\mathbb{F}_q$ mit $q = p^e$ und $e = \mathrm{kgV}\,(e_1, e_2)$ ist.

Aufgabe 20.14. Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G und es seien $H_1, H_2 \subseteq G$ Untergruppen mit den zugehörigen Fixkörpern $K_1 = \mathrm{Fix}\,(H_1)$ und $K_2 = \mathrm{Fix}\,(H_2)$. Zeige, dass das Kompositum K_1K_2 gleich dem Fixkörper von $H_1 \cap H_2$ ist.

Eine geordnete Menge $(M, \leq)$ mit der Eigenschaft, dass für je zwei Elemente $x, y \in M$ ein Infimum $x \sqcap y$ und ein Supremum $x \sqcup y$ existiert, heißt *Verband*.

In den beiden folgenden Aufgaben geht es insbesondere auch darum, jeweils die Verknüpfungen $\sqcap$ und $\sqcup$ zu definieren.

Aufgabe 20.15. Zeige, dass die Menge der Untergruppen einer Gruppe G mit der Inklusion einen Verband bildet.

Aufgabe 20.16. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass die Menge der Zwischenkörper mit der Inklusion einen Verband bildet.

Aufgabe 20.17. Es sei $K \subseteq L$ eine Galoiserweiterung. Es sei V der Verband der Zwischenkörper der Erweiterung und sei W der Verband der Untergruppen der Galoisgruppe $\mathrm{Gal}\,(L|K)$. Zeige, dass durch die Galoiskorrespondenz eine bijektive antimonotone Abbildung zwischen den Verbänden V und W gegeben ist.

20.2. **Aufgaben zum Abgeben.**

Aufgabe 20.18. (3 Punkte)

Es sei K_n der n-te Kreisteilungskörper, $n \geq 3$. Zeige, dass es einen Zwischenkörper L, $\mathbb{Q} \subseteq L \subseteq K_n$, gibt, der eine quadratische Körpererweiterung von $\mathbb{Q}$ ist.

Aufgabe 20.19. (2 Punkte)

Es seien K_{n_1} und K_{n_2} zwei Kreisteilungskörper über $\mathbb{Q}$. Zeige, dass das Kompositum (unabhängig vom gewählten Oberkörper) von K_{n_1} und K_{n_2} gleich K_n ist, wobei $n = \text{kgV}\,(n_1, n_2)$ ist.

Aufgabe 20.20. (3 Punkte)

Es seien m und n teilerfremde natürliche Zahlen. Zeige, dass das n-te Kreisteilungspolynom über dem m-ten Kreisteilungskörper K_m irreduzibel ist.

Aufgabe 20.21. (3 Punkte)

Es sei K ein Körper der Charakteristik 0 und sei $K \subseteq K(\zeta)$ die Adjunktion einer n-ten primitiven Einheitswurzel. Zeige mit Hilfe von Satz 20.7 und der Theorie der Kreisteilungskörper (über $\mathbb{Q}$), dass $K \subseteq K(\zeta)$ eine Galoiserweiterung ist, deren Galoisgruppe abelsch ist.

Aufgabe 20.22. (4 Punkte)

Es sei K ein Körper und es seien $K \subseteq K_1 \cong K[X]/F(X)$ und $K \subseteq K_2 \cong K[Y]/G(Y)$ zwei endliche einfache Körpererweiterungen von K, deren Grade teilerfremd seien. Zeige, dass die K-Algebra $A = K[X,Y]/(F,G)$ ein Körper ist.

Aufgabe 20.23. (6 Punkte)

Zu $n \geq 3$ sei F_n der Flächeninhalt eines in den Einheitskreis eingeschriebenen gleichmäßigen n-Eckes. Zeige $F_n \leq F_{n+1}$.

21. Vorlesung - Auflösbare Gruppen

In den nächsten drei Vorlesungen möchten wir auflösbare Körpererweiterungen galoistheoretisch charakterisieren und insbesondere zeigen, dass nicht jede Körpererweiterung auflösbar ist, also sich nicht jedes Polynom durch (sukzessive) Radikale (auf) lösen lässt. In dieser Vorlesung bereiten wir dazu das gruppentheoretische Fundament.

21.1. **Auflösbare Gruppen.**

Definition 21.1. Eine Gruppe G heißt *auflösbar*, wenn es eine Filtrierung

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = G$$

derart gibt, dass G_i ein Normalteiler in G_{i+1} ist und die Restklassengruppe G_{i+1}/G_i abelsch ist (für jedes $i = 0, \ldots, k-1$).

Die in dieser Definition auftretende Filtrierung nennt man auch eine *auflösende Filtrierung*. Eine kommutative Gruppe ist natürlich auflösbar, wie die triviale Filtrierung $\{e\} \subseteq G$ zeigt. Die Permutationsgruppe S_3 ist auflösbar, wie die Untergruppe $\mathbb{Z}/(3) \cong A_3 \subset S_3$ mit der Restklassengruppe $\mathbb{Z}/(2)$ zeigt.

Lemma 21.2. *Es sei G eine auflösbare Gruppe. Dann ist auch jede Untergruppe $H \subseteq G$ auflösbar.*

Beweis. Wir gehen von einer auflösenden Filtrierung

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = G$$

aus, d.h., dass die G_i Normalteiler in G_{i+1} und die Restklassengruppen G_{i+1}/G_i kommutativ sind. Die Untergruppe $H \subseteq G$ besitzt durch $H_i = H \cap G_i$ eine induzierte Filtrierung. Dabei liegt das kommutative Diagramm

$$\begin{array}{ccc} H \cap G_i & \longrightarrow & H \cap G_{i+1} \\ \downarrow & & \downarrow \\ G_i & \longrightarrow & G_{i+1} \end{array}$$

vor. Wir betrachten den Homomorphismus

$$f\colon H \cap G_{i+1} \longrightarrow G_{i+1}/G_i.$$

Der Kern von f ist offenbar $H \cap G_i$. Daher ist H_i nach Lemma 5.6 ein Normalteiler in H_{i+1}, und der Quotient H_{i+1}/H_i ist nach Satz 5.12 eine Untergruppe von G_{i+1}/G_i und damit kommutativ. Also bilden die H_i eine auflösende Filtrierung von H. □

Lemma 21.3. *Es sei G eine Gruppe, $N \subseteq G$ ein Normalteiler und G/N die zugehörige Restklassengruppe. Dann ist G genau dann auflösbar, wenn dies für N und G/N gilt.*

Beweis. Sei zunächst G auflösbar. Nach Lemma 21.2 ist $N \subseteq G$ auflösbar. Betrachten wir also die Restklassengruppe $H = G/N$ und fixieren wir eine auflösende Filtrierung

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = G.$$

Es sei

$$q\colon G \longrightarrow H$$

der Restklassenhomomorphismus. Wir setzen $H_i = q(G_i)$, dies ist eine Filtrierung von H mit Untergruppen. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccc} G_i & \longrightarrow & G_{i+1} \\ \downarrow & & \downarrow \\ H_i & \longrightarrow & H_{i+1}\,, \end{array}$$

wobei die vertikalen Homomorphismen surjektiv sind. Wir behaupten, dass H_i ein Normalteiler in H_{i+1} ist, und ziehen dazu Lemma 5.4 heran. Sei also $h \in H_i$ und $x \in H_{i+1}$, die wir durch $\tilde{h} \in G_i$ bzw. $\tilde{x} \in G_{i+1}$ repräsentieren. Dann ist $xhx^{-1} = q\left(\tilde{x}\tilde{h}\tilde{x}^{-1}\right)$ und wegen der Normalität von G_i in G_{i+1} ist $\tilde{x}\tilde{h}\tilde{x}^{-1} \in G_i$ und somit $xhx^{-1} \in H_i$. Wir betrachten die zusammengesetzte surjektive Abbildung

$$G_{i+1} \longrightarrow H_{i+1} \longrightarrow H_{i+1}/H_i\,.$$

Da G_i zum Kern dieser Abbildung gehört, gibt es aufgrund von Satz 5.10 eine surjektive Abbildung

$$G_{i+1}/G_i \longrightarrow H_{i+1}/H_i,$$

weshalb H_{i+1}/H_i ebenfalls kommutativ ist.

Seien nun N und $H = G/N$ auflösbar, sei $q\colon\, G \to G/N$ der Restklassenhomomorphismus und seien

$$\{e\} = N_0 \subseteq N_1 \subseteq N_2 \subseteq \ldots \subseteq N_{k-1} \subseteq N_k = N$$

und

$$\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots \subseteq H_{\ell-1} \subseteq H_\ell = H$$

auflösende Filtrierungen. Wir ergänzen die Filtrierung von N durch die Urbilder $G_j = q^{-1}(H_j)$ zu einer Filtrierung von G. Die surjektive Abbildung

$$G_{j+1} \longrightarrow H_{j+1} \longrightarrow H_{j+1}/H_j$$

besitzt den Kern G_j und zeigt, dass G_j ein Normalteiler in G_{j+1} mit kommutativer Restklassengruppe ist. □

Die Definition einer auflösbaren Gruppe legt nicht nahe, wie man eine solche Filtrierung finden könnte. Ein systematischer Weg, eine solche Filtrierung zu finden, falls es denn eine gibt, wird durch iterierte Kommutatorgruppen gegeben. Ein Kommutator ist ein Element der Form $aba^{-1}b^{-1}$.

Definition 21.4. Zu einer Gruppe G heißt die von allen Kommutatoren $aba^{-1}b^{-1}$, $a, b \in G$, erzeugte Untergruppe die *Kommutatorgruppe* von G. Sie wird mit $K(G)$ bezeichnet.

Lemma 21.5. *Es sei G eine Gruppe und $K(G)$ ihre Kommutatorgruppe. Dann gelten folgende Aussagen.*

(1) *$K(G)$ ist ein Normalteiler in G.*
(2) *Die Restklassengruppe $G/K(G)$ ist abelsch.*

(3) *Die Gruppe G ist genau dann abelsch, wenn $K(G)$ trivial ist.*

Beweis. (1). Es ist zu zeigen, dass für jedes $x \in G$ der Automorphismus

$$G \longrightarrow G,\ g \longmapsto xgx^{-1},$$

die Untergruppe $K(G)$ in sich selbst überführt. Für einen Kommutator $aba^{-1}b^{-1}$ ist

$$\begin{aligned} xaba^{-1}b^{-1}x^{-1} &= \left(xax^{-1}\right)\left(xbx^{-1}\right)\left(xa^{-1}x^{-1}\right)\left(xb^{-1}x^{-1}\right) \\ &= \left(xax^{-1}\right)\left(xbx^{-1}\right)\left(xax^{-1}\right)^{-1}\left(xbx^{-1}\right)^{-1} \end{aligned}$$

wieder ein Kommutator. Daher wird auch jedes Produkt von Kommutatoren auf ein Produkt von Kommutatoren abgebildet und somit ist $xK(G)x^{-1} \subseteq K(G)$. (2). In der Restklassengruppe $G/K(G)$ ist

$$[a][b] = [a][b][b^{-1}a^{-1}ba] = [a][b][b^{-1}][a^{-1}][b][a] = [b][a].$$

(3). Eine Gruppe ist genau dann abelsch, wenn sämtliche Kommutatoren trivial sind. □

Definition 21.6. Es sei G eine Gruppe. Die i-te *iterierte Kommutatoruntergruppe* wird induktiv durch

$$K^0(G) = G \text{ und } K^i(G) = K(K^{i-1}(G))$$

definiert.

Die erste Kommutatorgruppe ist einfach die Kommutatorgruppe, die zweite Kommutatorgruppe ist die Kommutatorgruppe der Kommutatorgruppe, u.s.w. Dies ergibt insgesamt eine absteigende Filtrierung

$$G \supseteq K(G) \supseteq K^2(G) \supseteq K^3(G) \supseteq \dots .$$

Diese Filtrierung kann unendlich absteigend sein oder aber stationär werden, d.h. es kann $K^i(G) = K^{i+1}(G)$ gelten. Die Auflösbarkeit einer Gruppe kann mit dieser Filtrierung folgendermaßen charakterisiert werden.

Lemma 21.7. *Eine Gruppe G ist genau dann auflösbar, wenn es ein i derart gibt, dass die i-te iterierte Kommutatorgruppe $K^i(G)$ trivial wird.*

Beweis. Wenn die Filtrierung der iterierten Kommutatorgruppen trivial wird, sagen wir

$$G \supseteq K(G) \supseteq K^2(G) \supseteq \dots \supseteq K^{i-1}(G) \supseteq K^i(G) = \{e\},$$

so liegt unmittelbar eine auflösende Filtrierung vor, da ja

$$K^{j+1}(G) = K(K^j(G)) \subseteq K^j(G)$$

nach Lemma 21.5 ein Normalteiler ist mit einer abelschen Restklassengruppe. Sei nun G auflösbar. Wir zeigen durch Induktion über die Anzahl k der beteiligten Untergruppen in einer auflösenden Filtrierung von G, dass die Filtrierung der iterierten Kommutatorgruppen trivial wird. Dabei sind die Fälle $k = 0, 1$ klar. Wir betrachten die Untergruppe $G_{k-1} \subset G_k = G$ in

der Filtrierung. Da die Restklassengruppe G/G_{k-1} kommutativ ist, wird die Kommutatorgruppe $K(G)$ unter der Restklassenabbildung auf 0 abgebildet und daher ist $K(G) \subseteq G_{k-1}$. Dabei besitzt natürlich G_{k-1} eine auflösende Filtrierung mit $k-1$ Untergruppen, und der Beweis zu Lemma 21.2 zeigt, dass dies auch für die Untergruppe $K(G)$ gilt. Nach Induktionsvoraussetzung wird also die Filtrierung von $K(G)$ durch die iterierten Kommutatorgruppen trivial. □

Lemma 21.8. *Für $n \leq 4$ sind die Permutationsgruppen S_n auflösbar.*

Beweis. Siehe Aufgabe 21.9. □

Lemma 21.9. *Für $n \geq 5$ sind die Permutationsgruppen S_n nicht auflösbar.*

Beweis. Wir betrachten eine Filtrierung

$$G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = S_n$$

derart, dass die $G_i \subseteq G_{i+1}$ Normalteiler sind mit kommutativen Restklassengruppen. Wir werden zeigen, dass jedes G_i sämtliche Dreierzykel (also Permutationen, bei denen drei Elemente zyklisch vertauscht werden, und alle übrigen festgelassen werden), enthält. Daher kann diese Filtrierung nicht bei der trivialen Gruppe enden, also ist $G_0 \neq \{e\}$. Die Aussage über die Dreierzykel beweisen wir durch absteigende Induktion, wobei der Fall $G_k = S_n$ klar ist. Sei also vorausgesetzt, dass G_{i+1} alle Dreierzykel enthält. Sei $\langle z_1, z_2, z_3 \rangle$ ein Dreierzyklus (mit verschiedenen Elementen $z_1, z_2, z_3 \in \{1, \ldots, n\}$.) Wegen $n \geq 5$ gibt es noch zwei weitere Elemente $x, y \in \{1, \ldots, n\}$, die von z_1, z_2, z_3 und untereinander verschieden sind. Nach Induktionsvoraussetzung gehören die Dreierzykel

$$\sigma = \langle z_1, z_2, x \rangle \text{ und } \tau = \langle z_1, z_3, y \rangle$$

zu G_{i+1}. Eine elementare Überlegung zeigt

$$\langle z_1, z_2, z_3 \rangle = \langle z_3, y, z_2 \rangle \circ \langle z_1, y, z_3 \rangle = (\sigma\tau\sigma^{-1}) \circ \tau^{-1} = \sigma\tau\sigma^{-1}\tau^{-1}.$$

Dieses Element wird unter der Restklassenabbildung

$$G_{i+1} \longrightarrow G_{i+1}/G_i$$

auf das neutrale Element abgebildet, da ja die Restklassengruppe kommutativ ist. Also ist $\langle z_1, z_2, z_3 \rangle \in G_i$. □

21. Arbeitsblatt

21.1. **Aufwärmaufgaben.**

Aufgabe 21.1. Untersuche für jede Filtrierung von S_3 mit Untergruppen, ob eine auflösende Filtrierung vorliegt oder nicht.

Aufgabe 21.2. Sei G eine Gruppe. Zeige, dass G genau dann kommutativ ist, wenn die Kommutatoruntergruppe $K(G)$ trivial ist.

Aufgabe 21.3. Seien G und H Gruppen und sei

$$\varphi\colon G \longrightarrow H$$

ein Gruppenhomomorphismus. Zeige die Beziehung $\varphi(K(G)) \subseteq K(H)$.

Die folgende Aussage heißt Satz von Cayley.

Jede Gruppe lässt sich als Untergruppe einer Permutationsgruppe realisieren. Jede endliche Gruppe lässt sich als Untergruppe einer endlichen Permutationsgruppe realisieren.

Aufgabe 21.4. Beweise den Satz von Cayley für Gruppen.

Aufgabe 21.5. Sei G eine einfache, nicht kommutative Gruppe. Zeige, dass G nicht auflösbar ist.

Wir erwähnen, dass die alternierenden Gruppen A_n, $n \geq 5$, einfach sind (das ist eine nichttriviale Aussage). Dies bedeutet, dass die Permutationsgruppen S_n, $n \geq 5$, nur die alternierende Gruppe als Normalteiler enthalten.

Aufgabe 21.6. Sei A_n eine alternierende Gruppe mit $n \geq 4$. Zeige, dass A_n nicht kommutativ ist.

Eine Gruppe G heißt *perfekt*, wenn sie gleich ihrer eigenen Kommutatoruntergruppe ist, also wenn $G = K(G)$ gilt.

Aufgabe 21.7. Sei G eine einfache, nicht kommutative Gruppe. Zeige, dass G perfekt ist.

Nach Aufgabe 5.12 ist das Zentrum $Z_1 = Z = Z(G)$ einer Gruppe G ein Normalteiler in G. Folglich gibt es eine Restklassengruppe $G/Z(G)$, die selbst wiederum ein Zentrum besitzt. Das Urbild dieser Gruppe in G wird mit Z_2 bezeichnet; sie ist wieder ein Normalteiler in G, so dass man eine Filtration

$$0 \subseteq Z_1 \subseteq Z_2 \subseteq Z_3 \subseteq \cdots$$

von Normalteilern in G erhält. Diese Filtration nennt man *Zentralreihe*.

Eine Gruppe G heißt *nilpotent*, wenn ihre Zentralreihe bei G endet, d.h. wenn G mit einer iterierten Zentrumsgruppe $Z_n(G)$ übereinstimmt.

Aufgabe 21.8. Zeige, dass eine nilpotente Gruppe auflösbar ist.

21.2. **Aufgaben zum Abgeben.**

Aufgabe 21.9. (4 Punkte)

Zeige, dass für $n \leq 4$ die Permutationsgruppen S_n auflösbar sind.

Aufgabe 21.10. (3 Punkte)

Es sei G eine endliche Gruppe, für die jede Untergruppe ein Normalteiler sei. Zeige, dass G auflösbar ist.

Aufgabe 21.11. (2 Punkte)

Zeige, dass jede gerade Permutation $\sigma \in S_n$, $n \geq 3$, ein Produkt aus Dreierzykeln ist.

Aufgabe 21.12. (3 Punkte)

Zeige: Keine der alternierenden Gruppen A_n besitzt eine Untergruppe vom Index zwei.

Hinweis: Aufgabe 21.11 hilft.

Aufgabe 21.13. (3 Punkte)

Sei G eine Gruppe mit Zentrum $Z(G)$. Zeige:

(1) G ist genau dann abelsch, wenn $G/Z(G)$ zyklisch ist.
(2) Der Index von $Z(G)$ in G ist keine Primzahl.
(3) Ist G von der Ordnung pq für zwei Primzahlen p und q, so ist G abelsch oder $Z(G)$ trivial.

Aufgabe 21.14. (4 Punkte)

Sei K ein Körper mit mindestens 4 Elementen. Zeige, dass $\mathrm{SL}_2(K)$ perfekt ist.

Tipp: Es gibt ein $x \in K$ mit $x^2 - 1 \neq 0$.

Aufgabe 21.15. (4 Punkte)

Sei K ein Körper. Zeige, dass $\mathrm{SL}_2(K)$ von

$$\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in K\} \cup \{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \mid c \in K\}$$

erzeugt wird.

22. Vorlesung - Auflösbare Körpererweiterungen

22.1. Die normale Hülle.

Definition 22.1. Es sei $K \subseteq L$ eine algebraische Körpererweiterung. Man nennt einen Körper N mit $L \subseteq N$ eine *normale Hülle* von L über K, wenn N der gemeinsame Zerfällungskörper aller Minimalpolynome von Elementen aus L ist.

Lemma 22.2. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann existiert die normale Hülle $L \subseteq N$.*

Beweis. Es sei $L = K(x_1, \ldots, x_n)$ und seien $P_1, \ldots, P_n$ die zugehörigen Minimalpolynome. Wir setzen $P = P_1 \cdots P_n$, und es sei N der Zerfällungskörper von P über L. Nach Satz 15.7 ist die Körpererweiterung $K \subseteq N$ normal. □

22.2. Auflösbare Körpererweiterungen.

Wir kommen nun zu einer Ausgangsfrage der Galoistheorie zurück, nämlich zur Frage, ob man für jedes gegebene Polynom $P \in \mathbb{Q}[X]$ eine Kette von einfachen Radikalerweiterungen $\mathbb{Q} \subseteq K_1 \subseteq \ldots \subseteq K_n = K$ finden kann, so dass K die Nullstellen von P enthält. Dies ist die körpertheoretische Variante der Frage, ob es entsprechend zur Lösungsformel von Cardano auch für höhere Grade eine Lösung mit Radikalen gibt. Diese Fragestellung führt zu den folgenden Begriffen.

Definition 22.3. Eine Körpererweiterung $K \subseteq L$ heißt *auflösbar*, wenn es eine Radikalerweiterung $K \subseteq M$ mit $L \subseteq M$ gibt.

Definition 22.4. Es sei K ein Körper und $F \in K[X]$ ein Polynom. Man sagt, dass das Polynom F *auflösbar* ist (bzw., dass die Gleichung $F(x) = 0$ *auflösbar* ist), wenn die Körpererweiterung $K \subseteq Z(F)$ auflösbar ist.

Wir erinnern daran, dass eine Radikalerweiterung aus einer Kette von einfachen Radikalerweiterungen besteht, wobei eine einfache Radikalerweiterung durch die Adjunktion einer gewissen Wurzel eines Elements gegeben ist.[19] Eine Radikalerweiterung

$$K \subseteq L$$

nennt man eine *m-Radikalerweiterung*, wenn es eine Körperkette aus einfachen Radikalerweiterungen $L_{i+1} = L_i(x_i)$ gibt, wobei die Beziehung $x_i^m \in L_i$ gilt. Jede Radikalerweiterung ist eine *m-Radikalerweiterung* für viele m, beispielsweise kann man jedes gemeinsame Vielfache der Einzelexponenten der beteiligten einfachen Radikalerweiterungen nehmen. Ein solches m hat (ähnlich wie der Exponent bei Kummererweiterungen) lediglich die Funktion,

[19] Man beachte, dass eine einfache Radikalerweiterung *nicht* das gleiche ist wie eine Radikalerweiterung, die zugleich eine einfache Körpererweiterung ist.

gewisse numerische Daten durch eine „gemeinsame Schranke“ zu kontrollieren.

Lemma 22.5. *Es sei $K \subseteq L$ eine m-Radikalerweiterung. Dann ist auch die normale Hülle N von L eine m-Radikalerweiterung von K.*

Beweis. Es sei eine Körperkette aus einfachen Radikalerweiterungen gegeben, also

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_n = L$$

mit $L_{i+1} = L_i(x_i)$ und $x_i^m \in L_i$. Wir zeigen durch Induktion über n, dass die normale Hülle von L über K ebenfalls eine m-Radikalerweiterung ist. Bei $n = 0$ ist nichts zu zeigen. Wir nehmen also an, dass die Aussage schon für kleinere Zahlen $n' < n$ bewiesen sei. Es sei $L \subseteq N$ die normale Hülle, die die normale Hülle N_{n-1} von L_{n-1} enthält. Nach Induktionsvoraussetzung ist $K \subseteq N_{n-1}$ eine m-Radikalerweiterung. In N_{n-1} zerfallen die Minimalpolynome der x_i, $i \leq n-2$, und in N zerfallen die Minimalpolynome der x_i, $i \leq n-1$. Daher ist $N = N_{n-1}(\alpha_1, \ldots, \alpha_k)$, wobei die α_j die Nullstellen des Minimalpolynoms von x_{n-1} sind. Wegen $x_{n-1}^m = a_{n-1} \in L_{n-1}$ sind diese α_j auch Nullstellen des Polynoms $X^m - a_{n-1}$. □

Wir kommen nun zur gruppentheoretischen Charakterisierung von auflösbaren Körpererweiterungen. Dabei beschränken wir uns auf Charakteristik 0. Dies sichert, dass es zu jeder Zahl n primitive n-te Einheitswurzeln in einem Erweiterungskörper gibt. Durch die Hinzunahme von Einheitswurzeln können wir auf eine Situation hin transformieren, in der wir mittels Kummertheorie aus der Kommutativität von gewissen Galoisgruppen auf die Existenz von Wurzeln schließen können.

Satz 22.6. *Es sei K ein Körper der Charakteristik 0 und sei $K \subseteq L$ eine Galoiserweiterung. Dann ist die Körpererweiterung $K \subseteq L$ genau dann auflösbar, wenn ihre Galoisgruppe $\mathrm{Gal}\,(L|K)$ auflösbar ist.*

Beweis. Es sei zuerst die Körpererweiterung $K \subseteq L$ auflösbar, und zwar sei $L \subseteq M$ eine Körpererweiterung derart, dass $K \subseteq M$ eine Radikalerweiterung ist. Es sei m dabei ein gemeinsamer „Radikalexponent“ der beteiligten einfachen Radikalerweiterungen. Da wir in Charakteristik 0 sind, können wir zu M eine m-te primitive Einheitswurzel ζ adjungieren und erhalten eine m-Radikalerweiterung $K \subseteq M' = M(\zeta)$. Wir ersetzen M' durch seine normale Hülle M'', die nach Lemma 22.5 ebenfalls eine m-Radikalerweiterung von K ist. Da wir in Charakteristik 0 sind, ist $K \subseteq M''$ eine Galoiserweiterung. Wir können also davon ausgehen, dass eine Kette

$$K = L_0 \subseteq K(\zeta) = L_1 \subseteq L_2 \subseteq \ldots \subseteq L_k = M$$

vorliegt, wobei $K \subseteq M$ galoissch ist und wo die sukzessiven Körpererweiterungen $L_i \subseteq L_{i+1}$ einfache Radikalerweiterungen sind. Es sei $G =$

$\mathrm{Gal}\,(M|K)$ und wir setzen

$$G_i \,=\, \mathrm{Gal}\,(M|L_i).$$

Dabei gelten nach Lemma 16.3 (2) die natürlichen Inklusionen

$$G_k \,=\, \{\mathrm{Id}\} \,\subseteq\, G_{k-1} \,\subseteq\, G_{k-2} \,\subseteq \ldots \subseteq\, G_1 \,\subseteq\, G_0 \,=\, G.$$

Da die Zwischenerweiterungen $L_i \,\subseteq\, L_{i+1}$ für $i \,\geq\, 1$ einfache Radikalerweiterungen und in L_1 die benötigten Einheitswurzeln vorhanden sind, folgt aus Satz 18.5, dass es sich um Galoiserweiterungen mit abelscher Galoisgruppe handelt. Aufgrund von Satz 17.5 (2) sind daher die G_{i+1} Normalteiler in G_i und die Restklassengruppen G_i/G_{i+1} sind kommutativ. Die Erweiterung $K \,\subseteq\, K(\zeta) \,=\, L_1$ besitzt nach Aufgabe 20.21 ebenfalls eine abelsche Galoisgruppe. Daher liegt insgesamt eine Filtrierung vor, die G als auflösbar erweist. Da $K \,\subseteq\, L$ eine Galoiserweiterung ist, gilt wieder nach Satz 17.5 die Beziehung

$$\mathrm{Gal}\,(L|K) \,=\, G/\,\mathrm{Gal}\,(M|L),$$

so dass auch $\mathrm{Gal}\,(L|K)$ wegen Lemma 21.3 eine auflösbare Gruppe ist.

Sei nun vorausgesetzt, dass die Galoisgruppe $G \,=\, \mathrm{Gal}\,(L|K)$ auflösbar ist, und sei

$$\{\mathrm{Id}\} \,=\, G_k \,\subseteq\, G_{k-1} \,\subseteq\, G_{k-2} \,\subseteq \ldots \subseteq\, G_1 \,\subseteq\, G_0 \,=\, G$$

eine Filtrierung mit Untergruppen derart, dass jeweils $G_{i+1} \,\subseteq\, G_i$ ein Normalteiler ist mit abelscher Restklassengruppe G_i/G_{i+1}. Wir setzen $L_i \,=\, \mathrm{Fix}\,(G_i)$, so dass nach Lemma 16.3 (1) und Satz 16.6 die Körperkette

$$K \,=\, L_0 \,\subseteq\, L_1 \,\subseteq \ldots \subseteq\, L_k \,=\, L$$

vorliegt. Dabei sind nach Korollar 16.7 die Körpererweiterungen $L_i \,\subseteq\, L$ galoissch, und ihre Galoisgruppen sind G_i gemäß Satz 17.1. Da die G_{i+1} Normalteiler in G_i sind, sind aufgrund von Satz 17.5 die Körpererweiterungen $L_i \,\subseteq\, L_{i+1}$ galoissch mit Galoisgruppe $\mathrm{Gal}\,(L_{i+1}|L_i) \,=\, G_i/G_{i+1}$. Diese sukzessiven Erweiterungen sind also Galoiserweiterungen mit abelscher Galoisgruppe. Es sei m der Exponent von G. Es sei $L \,\subseteq\, M$ ein m-ter Kreisteilungskörper, also ein Zerfällungskörper von $X^m - 1$ über L, und sei $\zeta \,\in\, M$ eine m-te primitive Einheitswurzel. Es ist somit $M \,=\, L(\zeta)$. Wir setzen $M_i \,=\, L_i(\zeta)$ (innerhalb von M) und haben dann die Körperkette

$$K \,\subseteq\, M_0 \,=\, K(\zeta) \,\subseteq\, M_1 \,\subseteq \ldots \subseteq\, M_k \,=\, M.$$

Hierbei gilt $M_{i+1} \,=\, M_i L_{i+1}$. Nach Satz 20.7 ist $M_i \,\subseteq\, M_{i+1}$ ebenfalls galoissch, und es gilt die Untergruppenbeziehung

$$\mathrm{Gal}\,(M_{i+1}|M_i) \,=\, \mathrm{Gal}\,(L_{i+1}|L_{i+1} \cap M_i) \,\subseteq\, \mathrm{Gal}\,(L_{i+1}|L_i),$$

so dass diese Galoisgruppen auch abelsch sind. Da die m-te primitive Einheitswurzel ζ zu M_0 gehört, sind die Erweiterungen $M_i \,\subseteq\, M_{i+1}$ allesamt Kummererweiterungen und damit nach Korollar 18.4 auch Radikalerweiterungen. Da auch $K \,\subseteq\, M_0 \,=\, K(\zeta)$ eine (einfache) Radikalerweiterung ist,

ist insgesamt $K \subseteq M$ eine Radikalerweiterung, die L umfasst. Somit ist $K \subseteq L$ auflösbar. □

Korollar 22.7. *Es sei K ein Körper der Charakteristik 0 und sei $F \in K[X]$ ein Polynom. Dann ist F genau dann auflösbar, wenn die Galoisgruppe $\mathrm{Gal}\,(Z(F)|K)$ des Zerfällungskörpers von F auflösbar ist.*

Beweis. Wegen Satz 16.6 ist $K \subseteq Z(F)$ eine Galoiserweiterung, so dass die Aussage direkt aus Satz 22.6 folgt. □

Ein wichtiges unmittelbares Korollar aus der vorstehenden Charakterisierung ist die Auflösbarkeit mit Radikalen von polynomialen Gleichungen vom Grad vier, wobei man dieses Ergebnis auch direkt über die (recht komplizierten, aber) expliziten Cardanoschen Lösungsformeln zum vierten Grad erhalten kann.

Korollar 22.8. *Es sei K ein Körper der Charakteristik 0 und sei $F \in K[X]$ ein Polynom vom Grad ≤ 4. Dann ist F auflösbar. D.h. es gibt eine Radikalerweiterung $K \subseteq M$, so dass F über M in Linearfaktoren zerfällt.*

Beweis. Es sei L der Zerfällungskörper von F über K, der aufgrund der Voraussetzung über die Charakteristik nach Satz 16.6 eine Galoiserweiterung ist. Sei $G = \mathrm{Gal}\,(L|K)$. Über L besitzt F maximal $d = \mathrm{grad}\,(F)$ Nullstellen. Nach Lemma 14.2 ist G eine Untergruppe der Permutationsgruppe der Nullstellen, also ist jedenfalls $G \subseteq S_4$. Wegen Lemma 21.8 und Lemma 21.2 ist somit G eine auflösbare Gruppe. Aus Satz 22.6 folgt daher die Auflösbarkeit des Zerfällungskörpers über K. □

Das entscheidende Schlussfolgerung aus der obigen Charakterisierung ist aber, dass nicht alle Gleichungen auflösbar sind. Das ist Gegenstand der nächsten Vorlesung.

22. Arbeitsblatt

22.1. **Aufwärmaufgaben.**

Aufgabe 22.1. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass diese Erweiterung genau dann normal ist, wenn die normale Hülle gleich L ist.

Aufgabe 22.2. Es sei K ein Körper und $F \in K[X]$ ein irreduzibles Polynom. Zeige, dass die normale Hülle der Körpererweiterung $K \subseteq K[X]/(F)$ gleich dem Zerfällungskörper von F ist.

Aufgabe 22.3. Es sei $K \subseteq L$ eine auflösbare Körpererweiterung. Es sei $K \subseteq K'$ eine weitere Körpererweiterung und es sei $L' = LK'$ das Kompositum von L und K' (das in einem gewissen Oberkörper gebildet sei). Zeige, dass auch $K' \subseteq L'$ auflösbar ist.

Aufgabe 22.4. Es sei K ein Körper und seien $P, F \in K[X]$ nichtkonstante Polynome. Wir setzen $Q = P(F)$ (in P wird also das Polynom F eingesetzt). Zeige, dass man den Zerfällungskörper von P in den Zerfällungskörper von Q einbetten kann.

Aufgabe 22.5. Es sei K ein Körper und sei $P \in K[X]$ ein auflösbares Polynom. Zeige, dass auch $P(X^n)$ auflösbar ist.

Aufgabe 22.6.*

Es sei $P \in \mathbb{Q}[X]$ ein Polynom vom Grad 3. Zeige mit Mitteln der Galoistheorie, dass P auflösbar ist.

Aufgabe 22.7. Es sei $P \in \mathbb{Q}[X]$ ein Polynom vom Grad 3. Setze die Körpererweiterungen von $\mathbb{Q}$, die sich aus der Cardanoschen Formel ergeben, mit den Körpererweiterungen in Beziehung, die sich aus der Galoistheorie über Satz 22.6 ergeben.

Aufgabe 22.8. Man gebe ein Beispiel für einen Körper K und zerfallende Polynome $F, G \in K[X]$ derart, dass die Einsetzung $F(G)$ nicht zerfällt.

22.2. **Aufgaben zum Abgeben.**

Aufgabe 22.9. (3 Punkte)

Sei n eine ungerade Zahl. Man gebe eine Körpererweiterung $\mathbb{Q} \subseteq L$ vom Grad n derart, dass $\mathrm{Gal}\,(L|\mathbb{Q})$ trivial ist.

Aufgabe 22.10. (2 Punkte)

Es seien $K \subseteq L$ und $L \subseteq M$ auflösbare Körpererweiterungen. Zeige, dass auch $K \subseteq M$ auflösbar ist.

Aufgabe 22.11. (2 Punkte)

Es seien F und G auflösbare Polynome über einem Körper K. Zeige, dass das Produkt FG ebenfalls auflösbar ist.

Aufgabe 22.12. (8 (5+3) Punkte)

Es sei $E \subseteq \mathbb{R}^2$ ein reguläres n-Eck ($n \geq 3$) mit den Eckpunkten $v_1, \ldots, v_n$, und es sei V der von diesen Eckpunkten erzeugte $\mathbb{Q}$-Vektorraum.

a) Zeige die Abschätzungen

$$\varphi(n) \leq \dim_{\mathbb{Q}}(V) \leq \varphi(n) + 1.$$

(Dabei bezeichnet $\varphi(n)$ die eulersche φ-Funktion).

b) Zeige, dass in (a) sowohl links als auch rechts Gleichheit gelten kann.

23. Vorlesung - Der Satz von Abel-Ruffini

23.1. Polynome mit unauflösbarer Galoisgruppe.

Wir möchten nun zeigen, dass gewisse Körpererweiterungen, und zwar die Zerfällungskörper von gewissen Polynomen vom Grad ≥ 5, nicht auflösbar sind. Dazu müssen wir aufgrund der Galoistheorie für auflösbare Körpererweiterungen und den gruppentheoretischen Überlegungen zu den Permutationsgruppen S_n, $n \geq 5$, (Lemma 21.9) lediglich nachweisen, dass diese Permutationsgruppen als Galoisgruppen auftreten. Dazu bedarf es einiger Vorbereitungen über Permutationsgruppen.

Zu einer Permutationsgruppe $S(M)$ auf einer Menge M liefert jede Teilmenge $T \subseteq M$ eine Untergruppe $S(T) \subseteq S(M)$. Man setzt einfach die Permutation auf T durch die Identität auf $M \setminus T$ zu einer Permutation auf ganz M fort.

Lemma 23.1. *Es sei M eine endliche Menge und $T_1, T_2 \subseteq M$ seien Teilmengen mit $T_1 \cap T_2 \neq \emptyset$. Es sei $G \subseteq S(M)$ eine Untergruppe der Permutationsgruppe, die sowohl $S(T_1)$ als auch $S(T_2)$ umfasst. Dann ist $S(T_1 \cup T_2) \subseteq G$.*

Beweis. Jedes Element $\sigma \in S(T_1 \cup T_2)$ lässt sich nach Lemma 18.7 (Lineare Algebra (Osnabrück 2017-2018)) als Produkt von Transpositionen auf $T_1 \cup T_2$ schreiben. Es muss also lediglich gezeigt werden, dass solche Transpositionen zu G gehören. Sei $\sigma \in S(T_1 \cup T_2)$ eine Transposition, und zwar vertausche σ die Elemente a und b, also $\sigma = \langle a, b \rangle$. Wenn beide Elemente zu T_1 (oder zu T_2) gehören, sind wir fertig. Sei also $a \in T_1, a \notin T_2$ und $b \in T_2, b \notin T_1$. Es sei ferner $c \in T_1 \cap T_2$, und c sei von a und b verschieden (sonst gehören beide zu einer der Teilmengen). Dann ist

$$\sigma = \langle a, b \rangle = \langle a, c \rangle \circ \langle b, c \rangle \circ \langle a, c \rangle$$

und diese drei Transpositionen gehören zu $S(T_1)$ oder zu $S(T_2)$ und damit zu G. □

Definition 23.2. Es sei M eine Menge und sei $G = S(M)$ die zugehörige Permutationsgruppe. Eine Untergruppe $H \subseteq G$ heißt *transitiv*, wenn es zu je zwei Elementen $x, y \in M$ ein $\sigma \in H$ mit $\sigma(x) = y$ gibt.

Lemma 23.3. *Es sei p eine Primzahl und S_p die Permutationsgruppe zu $\{1,\ldots,p\}$. Es sei $H \subseteq S_p$ eine transitive Untergruppe, die eine Transposition enthalte. Dann ist $H = S_p$.*

Beweis. Sei $M = \{1,\ldots,p\}$. Wir betrachten Teilmengen $T \subseteq M$ derart, dass $S(T) \subseteq H$ ist, und wollen $T = M$ zeigen. Sei dazu T_1 eine solche Teilmenge mit maximaler Elementanzahl, die wir k nennen. Da es mindestens eine Transposition in H gibt, ist $k \geq 2$. Für jedes $\sigma \in H$ ist $T_\sigma = \sigma(T_1)$ ebenfalls eine k-elementige Menge mit $S(T_\sigma) \subseteq H$. Für $\tau \in S(T_\sigma)$ ist nämlich

$$\tau = \sigma(\sigma^{-1}\tau\sigma)\sigma^{-1},$$

und $\sigma^{-1}\tau\sigma$ ist eine Permutation auf T_1, so dass sie zu H gehört und damit auch $\tau \in H$ gilt. Für Permutationen $\sigma_1, \sigma_2 \in H$ ist entweder $T_{\sigma_1} = T_{\sigma_2}$ oder $T_{\sigma_1} \cap T_{\sigma_2} = \emptyset$, da andernfalls nach Lemma 23.1 $S(T_1 \cup T_2) \subseteq H$ wäre im Widerspruch zur Maximalität von k. Sei nun $x \in M$ vorgegeben und ein $y \in T_1$ fixiert. Aufgrund der Transitivität gibt es ein $\sigma \in H$ mit $\sigma(y) = x$. Dann ist natürlich $x \in T_\sigma$. Das bedeutet, dass die Mengen T_σ, $\sigma \in H$, die Gesamtmenge M überdecken. Wegen der Gleichmächtigkeit dieser Mengen ist p ein Vielfaches von k und somit ist $p = k$, also $M = T_1$. □

Lemma 23.4. *Sei p eine Primzahl und $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad p, das genau $p-2$ reelle Nullstellen besitzt. Dann ist die Galoisgruppe des Zerfällungskörpers $\mathbb{Q} \subseteq Z(F)$ gleich der Permutationsgruppe S_p. Bei $p \geq 5$ ist diese Körpererweiterung nicht auflösbar.*

Beweis. Es seien $\alpha_1,\ldots,\alpha_{p-2}$ die reellen Nullstellen und α_{p-1}, α_p die beiden nichtreellen komplexen Nullstellen. Nach Lemma 14.2 ist die Galoisgruppe $\mathrm{Gal}\,(Z(F)|\mathbb{Q})$ in natürlicher Weise eine Untergruppe der Permutationsgruppe der Nullstellen. Wir zeigen, dass es sich um die volle Permutationsgruppe handelt. Die komplexe Konjugation induziert einen $\mathbb{Q}$-Automorphismus auf L, der die reellen Nullstellen unverändert lässt und die beiden nichtreellen Nullstellen α_{p-1} und α_p ineinander überführt. Daher bewirkt dieser Automorphismus auf den Nullstellen eine Transposition. Da F über $\mathbb{Q}$ irreduzibel ist, ist F für jede Nullstelle das Minimalpolynom und daher sind alle Nullstellen zueinander konjugiert. Nach Satz 14.5 gibt es somit für je zwei Nullstellen α und β einen Automorphismus φ mit $\varphi(\alpha) = \beta$. Damit sind die Voraussetzungen von Lemma 23.3 erfüllt und somit ist die Galoisgruppe die volle Permutationsgruppe. □

Korollar 23.5. *Sei a eine Primzahl und sei*

$$F = X^5 + a^2X^4 - a \in \mathbb{Q}[X].$$

Dann gelten folgende Aussagen.

(1) *Das Polynom F ist irreduzibel in $\mathbb{Q}[X]$.*
(2) *F besitzt drei reelle Nullstellen und darüber hinaus zwei komplexe nichtreelle Nullstellen.*

(3) *Die Galoisgruppe des Zerfällungskörpers* $\mathbb{Q} \subseteq Z(F)$ *ist die Permutationsgruppe* S_5.
(4) *Die Körpererweiterung* $\mathbb{Q} \subseteq Z(F)$ *ist nicht auflösbar.*

Beweis. (1) ergibt sich aus dem Kriterium von Eisenstein. (2). Wir berechnen einige Funktionswerte von F. Es ist

$$F\left(-a^2\right) = -a^{10} + a^{10} - a = -a < 0,$$

$$F(-1) = -1 + a^2 - a = -1 + a(a-1) > 0,$$

$$F(0) = -a < 0$$

und schließlich

$$F(1) = 1 + a^2 - a > 0.$$

Nach dem Zwischenwertsatz gibt es daher mindestens drei reelle Nullstellen. Die Ableitung von F ist

$$F' = 5X^4 + 4a^2X^3 = 5X^3\left(X + \frac{4}{5}a^2\right)$$

und besitzt die beiden reellen Nullstellen 0 und $-\frac{4}{5}a^2$. Nach dem Mittelwertsatz der Differentialrechnung kann somit F nicht mehr als drei reelle Nullstellen besitzen, da zwischen zwei Nullstellen stets eine Nullstelle der Ableitung liegt. Die Nullstellen der Ableitung sind wegen

$$F\left(-\frac{4}{5}a^2\right) \neq 0$$

(wegen der Irreduzibilität von F über $\mathbb{Q}$) keine Nullstelle von F, so dass F keine mehrfache Nullstelle besitzen kann. Daher muss es zwei weitere komplexe nichtreelle Nullstellen geben. (3) und (4) folgen aus (1), (2) und Lemma 23.4. □

Das erste Beispiel für ein solches Polynom ist $X^5 + 4X^4 - 2$. Durch die Existenz solcher Polynome folgt die allgemeine Unauflösbarkeit für algebraische Gleichungen vom Grad 5 und höher. Diese Aussage heißt *Satz von Abel-Ruffini.*

Satz 23.6. *Für* $n \geq 5$ *gibt es polynomiale Gleichungen (über* $\mathbb{Q}$*) vom Grad* n*, die nicht auflösbar sind.*

Paolo Ruffini (1765-1822)

Niels Henrik Abel (1802-1829)

Beweis. Für $n = 5$ folgt dies direkt aus Korollar 23.5, und für $n \geq 6$ kann man ein unauflösbares Polynom vom Grad 5 einfach mit einem beliebigen Polynom vom Grad $n-5$ multiplizieren. □

23. Arbeitsblatt

23.1. **Aufwärmaufgaben.**

Aufgabe 23.1. Es sei M eine endliche Menge und $T \subseteq M$ eine Teilmenge, und es seien $\mathrm{Perm}(T)$ und $\mathrm{Perm}(M)$ die zugehörigen Permutationsgruppen Zeige, dass durch

$$\Psi\colon\ \mathrm{Perm}(T) \longrightarrow \mathrm{Perm}(M),\ \varphi \longmapsto \tilde{\varphi},$$

mit

$$\tilde{\varphi}(x) = \begin{cases} \varphi(x), \text{ falls } x \in T, \\ x \text{ sonst}, \end{cases}$$

ein injektiver Gruppenhomomorphismus gegeben ist.

Aufgabe 23.2. Zeige, dass zwei Permutationen mit disjunktem Wirkungsbereich vertauschbar sind.

Aufgabe 23.3. Sei M eine endliche Menge und sei σ eine Permutation auf M und $x \in M$. Zeige, dass $\{n \in \mathbb{Z} |\, \sigma^n(x) = x\}$ eine Untergruppe von $\mathbb{Z}$ ist. Den eindeutig bestimmten nichtnegativen Erzeuger dieser Untergruppe bezeichnen wir mit $\mathrm{ord}_x\, \sigma$. Zeige die Beziehung

$$\mathrm{ord}\,(\sigma) = \mathrm{kgV}\,\{\mathrm{ord}_x\, \sigma |\, x \in M\}\,.$$

Aufgabe 23.4. Sei G eine zyklische Gruppe der Ordnung 6. Für welche $n \in \mathbb{N}$ lässt sich G als Untergruppe der Permutationsgruppe S_n realisieren?

Aufgabe 23.5.*

Wir betrachten die endliche Permutationsgruppe S_n zu einer Menge mit n Elementen.

a) Zeige, dass es in S_n Elemente der Ordnung n gibt.

b) Man gebe ein Beispiel für eine Permutationsgruppe S_n und einem Element darin, dessen Ordnung größer als n ist.

Aufgabe 23.6. Zeige, dass in Lemma 23.1 die Voraussetzung, dass die beiden Teilmengen T_1, T_2 nicht disjunkt sind, wesentlich ist.

Aufgabe 23.7. Zeige, dass die alternierende Gruppe $A_n \subseteq S_n$ für $n \geq 3$ eine transitive Untergruppe ist.

Aufgabe 23.8. Bestimme für jede Untergruppe $G \subseteq S_4$ der Permutationsgruppe S_4, ob es sich um eine transitive Untergruppe handelt oder nicht.

Aufgabe 23.9. Es sei $G \subseteq S_n$ eine Untergruppe der Permutationsgruppe S_n. Zeige, dass G genau dann eine transitive Untergruppe ist, wenn es ein Element $z \in \{1, \ldots, n\}$ derart gibt, dass es zu jedem Element $w \in \{1, \ldots, n\}$ eine Permutation $\pi \in G$ mit $\pi(z) = w$ gibt.

Aufgabe 23.10. Es sei $G \subseteq S_n$ eine Untergruppe der Permutationsgruppe S_n. Zeige, dass G genau dann keine transitive Untergruppe ist, wenn es eine echte Zerlegung

$$\{1, \ldots, n\} = S \uplus T$$

derart gibt, dass

$$G \subseteq \mathrm{Perm}\,(S) \times \mathrm{Perm}\,(T) \subseteq S_n$$

gilt.

Aufgabe 23.11. Es sei $G \subseteq S_n$ eine Untergruppe der Permutationsgruppe S_n. Zeige, dass auf $\{1, \ldots, n\}$ durch $x \sim_G y$, falls es ein $\pi \in G$ mit $\pi(x) = y$ gibt, eine Äquivalenzrelation gegeben ist.

Aufgabe 23.12.*

(1) Zeige, dass eine transitive Untergruppe $G \subseteq S_n$ zumindest n Elemente besitzt.
(2) Zeige, dass es eine transitive Untergruppe $G \subseteq S_n$ mit genau n Elementen gibt.

Aufgabe 23.13. Es sei K ein Körper und sei $F \in K[X]$ ein separables irreduzibles Polynom. Es sei L der Zerfällungskörper von F, $G = \mathrm{Gal}\,(L|K)$ seine Galoisgruppe und $\lambda_1, \ldots, \lambda_n$ die Nullstellen von F in L. Nach Lemma 14.2 ist G eine Untergruppe der Permutationsgruppe der Nullstellen. Zeige, dass es sich um eine transitive Untergruppe handelt.

Die folgende Aufgabe zeigt, dass man in Lemma 23.4 auf die Voraussetzung, dass der Grad des Polynoms eine Primzahl ist, nicht verzichten kann.

Aufgabe 23.14.*

Man gebe ein irreduzibles Polynom $F \in \mathbb{Q}[X]$ vom Grad 4 an, das in $\mathbb{C}$ genau zwei reelle Nullstellen hat und dessen Galoisgruppe nicht die S_4 ist.

Aufgabe 23.15. Sei a eine Primzahl, $F = X^5 + a^2X^4 - a \in \mathbb{Q}[X]$ und $L = Z(F)$ der Zerfällungskörper von F. Bestimme den Grad der Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R} \cap L$. Handelt es sich um eine Galoiserweiterung?

Aufgabe 23.16. Sei a eine Primzahl, $F = X^5 + a^2X^4 - a \in \mathbb{Q}[X]$ und $L = Z(F)$ der Zerfällungskörper von F. Es seien $\alpha_1, \ldots, \alpha_5$ die Nullstellen von F in $\mathbb{C}$.

(1) Zeige, dass
$$\sum_{i=1}^{5} \alpha_i \text{ und } \prod_{i=1}^{5} \alpha_i$$
rationale Zahlen sind.
(2) Zeige, dass
$$\prod_{1 \leq i < j \leq 5} (\alpha_i - \alpha_j)$$
zu L^{A_n} gehört, aber nicht zu $\mathbb{Q}$.
(3) Zeige, dass
$$\prod_{1 \leq i < j \leq 5} (\alpha_i - \alpha_j)^2$$
eine rationale Zahl ist.

23.2. **Aufgaben zum Abgeben.**

Aufgabe 23.17. (4 Punkte)

Es sei $n \geq 2$ keine Primzahl. Zeige, dass es eine echte Untergruppe $H \subset S_n$ gibt, die transitiv ist und die mindestens eine Transposition enthält.

Aufgabe 23.18. (3 Punkte)

Eliminiere in $X^5 + a^2X^4 - a$ (mit $a \in \mathbb{Q}$) durch eine geeignete Substitution (einen Variablenwechsel) den Term zum Grad 4.

Aufgabe 23.19. (3 Punkte)

Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad 3 und seien $\alpha, \beta, \gamma \in \mathbb{C}$ die Nullstellen von F. Zeige, dass die Differenzen $\alpha - \beta$ und $\beta - \gamma$ nicht beide aus $\mathbb{Q}$ sein können.

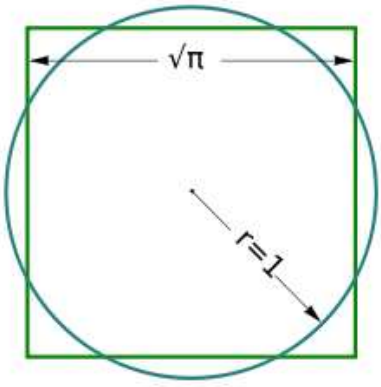
Aufgabe 23.20. (4 Punkte)

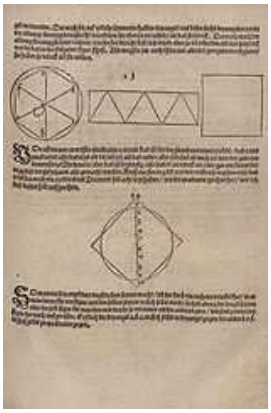
Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad 3. Zeige, dass die Nullstellen von F in $\mathbb{C}$ nicht die Form $\alpha, \alpha^2, \alpha^3$ (mit einem $\alpha \in \mathbb{C}$) haben können.

Aufgabe 23.21. (3 Punkte)

Zeige, dass es ein irreduzibles Polynom $F \in \mathbb{Q}[X]$ vom Grad 4 gibt, dessen Nullstellen in $\mathbb{C}$ die Form $\alpha, \alpha^2, \alpha^3, \alpha^4$ besitzen.

24. Vorlesung - Konstruktionen mit Zirkel und Lineal





Auch Albrecht Dürer hatte Spaß an der Quadratur des Kreises

Unter den drei klassischen Problemen der antiken Mathematik versteht man

(1) die Quadratur des Kreises,
(2) die Dreiteilung des Winkels,
(3) die Würfelverdoppelung.

Dabei sollen diese Konstruktionen ausschließlich mit Zirkel und Lineal durchgeführt werden, wobei dies natürlich präzisiert werden muss. Nach langen vergeblichen Versuchen, solche Konstruktionen zu finden, ergab sich im Laufe des neunzehnten Jahrhunderts die Erkennntnis, dass es keine solche Konstruktionen geben kann. Dies erfordert natürlich, dass man eine Übersicht über alle möglichen Konstruktionen erhalten kann.

24.1. **Konstruktionen mit Zirkel und Lineal.**

Unter der Ebene E verstehen wir im Folgenden die Anschauungsebene, die wir später mit $\mathbb{R}^2 \cong \mathbb{C}$ identifizieren. Zunächst sind die Konstruktionen „koordinatenfrei“. An elementargeometrischen Objekten verwenden wir Punkte, Geraden und Kreise. An elementargeometrischen Gesetzmäßigkeiten verwenden wir, dass zwei verschiedene Punkte eine eindeutige Gerade definieren, dass zwei Geraden entweder identisch sind oder parallel und schnittpunktfrei oder genau einen Schnittpunkt haben, u.s.w.

Definition 24.1. Es sei $M \subseteq E$ eine Teilmenge der Ebene E. Eine Gerade $G \subseteq E$ heißt aus M *elementar konstruierbar*, wenn es zwei Punkte $P, Q \in M$, $P \neq Q$, derart gibt, dass die Verbindungsgerade von P und Q gleich G ist. Ein Kreis $C \subseteq E$ heißt aus M *elementar konstruierbar*, wenn es zwei Punkte $Z, S \in M$, $Z \neq S$, derart gibt, dass der Kreis mit dem Mittelpunkt Z und durch den Punkt S gleich C ist.

Man kann also an zwei Punkte aus der vorgegebenen Menge M das *Lineal anlegen* und die dadurch definierte Gerade zeichnen, und man darf die *Nadelspitze des Zirkels* in einen Punkt der Menge stechen und die *Stiftspitze des Zirkels* an einen weiteren Punkt der Menge anlegen und den Kreis ziehen.

Wenn ein Koordinatensystem vorliegt, und zwei Punkte $P = (p_1, p_2)$ und $Q = (q_1, q_2)$ gegeben sind, so ist die Gleichung der Verbindungsgeraden der beiden Punkte bekanntlich

$$(p_1 - q_1)y + (q_2 - p_2)x + q_1p_2 - q_2p_1 = 0\,.$$

Wenn zwei Punkte $Z = (z_1, z_2)$ und $S = (s_1, s_2)$ gegeben sind, so besitzt der Kreis mit dem Mittelpunkt Z durch den Punkt S die Kreisgleichung

$$(x - z_1)^2 + (y - z_2)^2 - (s_1 - z_1)^2 - (s_2 - z_2)^2 = 0\,.$$

Definition 24.2. Es sei $M \subseteq E$ eine Teilmenge der Ebene E. Dann heißt ein Punkt $P \in E$ aus M *in einem Schritt konstruierbar*, wenn eine der folgenden Möglichkeiten zutrifft.

(1) Es gibt zwei aus M elementar konstruierbare Geraden G_1 und G_2 mit $G_1 \cap G_2 = \{P\}$.

(2) Es gibt eine aus M elementar konstruierbare Gerade G und einen aus M elementar konstruierbaren Kreis C derart, dass P ein Schnittpunkt von G und C ist.
(3) Es gibt zwei aus M elementar konstruierbare Kreise C_1 und C_2 derart, dass P ein Schnittpunkt der beiden Kreise ist.

Definition 24.3. Es sei $M \subseteq E$ eine Teilmenge der Ebene E. Dann heißt ein Punkt $P \in E$ aus M *konstruierbar* (oder *mit Zirkel und Lineal konstruierbar*), wenn es eine Folge von Punkten

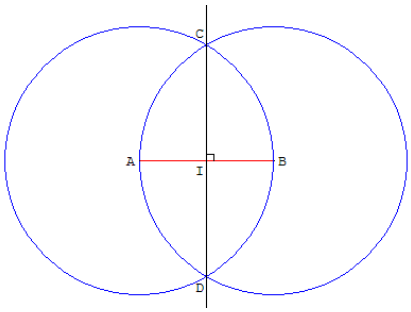
$$P_1, \ldots, P_n = P$$

gibt derart, dass P_i jeweils aus $M \cup \{P_1, \ldots, P_{i-1}\}$ in einem Schritt konstruierbar ist.

Definition 24.4. Eine Zahl $z \in \mathbb{C} \cong E$ heißt *konstruierbar* oder *konstruierbare Zahl*, wenn sie aus der Startmenge $\{0, 1\} \subset \mathbb{R} \subset \mathbb{C}$ mit Zirkel und Lineal konstruierbar ist.

Bemerkung 24.5. Man startet also mit zwei beliebig vorgegebenen Punkten, die man 0 und 1 nennt und die dann die arithmetische Funktion übernehmen, die mit diesen Symbolen verbunden wird. Als erstes kann man die Gerade durch 0 und 1 ziehen, und diese Gerade wird mit den reellen Zahlen $\mathbb{R}$ identifiziert. Wir werden gleich sehen, dass man eine zu $\mathbb{R}$ senkrechte Gerade durch 0 konstruieren kann, mit deren Hilfe ein *kartesisches Koordinatensystem* entsteht und mit dem wir die Ebene mit den komplexen Zahlen $\mathbb{C}$ identifizieren können.

In den folgenden Konstruktionen verwenden wir einige Begrifflichkeiten aus der euklidischen Geometrie, wie Winkel, senkrecht, parallel, Strecke und elementare Grundtatsachen wie die Strahlensätze, Symmetriesätze und den Satz des Pythagoras.



Lemma 24.6. *In der Ebene lassen sich folgende Konstruktionen mit Zirkel und Lineal durchführen.*

(1) *Zu einer Geraden G und zwei Punkten $Q_1, Q_2 \in G$ kann man die zu G senkrechte Gerade zeichnen, die die Strecke zwischen Q_1 und Q_2 halbiert.*
(2) *Zu einer Geraden G und einem Punkt $P \in G$ kann man die zu G senkrechte Gerade durch P zeichnen.*
(3) *Zu einer Geraden G und einem Punkt P kann man die zu G senkrechte Gerade durch P zeichnen.*
(4) *Zu einer gegebenen Geraden G und einem gegebenen Punkt P kann man die Gerade G' durch P zeichnen, die zu G parallel ist.*

Beweis. Wir verwenden im Beweis einige elementargeometrische Grundtatsachen.

(1) Wir zeichnen die beiden Kreise C_1 und C_2 mit dem Mittelpunkt Q_1 durch Q_2 und umgekehrt. Die beiden Schnittpunkte von C_1 und C_2 seien S_1 und S_2. Deren Verbindungsgerade steht senkrecht auf G und halbiert die Strecke zwischen Q_1 und Q_2.
(2) Man zeichnet einen Kreis C mit P als Mittelpunkt und einem beliebigen Radius (dazu braucht man neben P noch einen weiteren Punkt). Es seien Q_1 und Q_2 die beiden Schnittpunkte der Gerade G mit C. Für diese beiden Punkte führen wir die in (1) beschriebene Konstruktion durch. Diese Halbierungsgerade läuft dann durch P und steht senkrecht auf G.
(3) Wenn P auf der Geraden liegt, sind wir schon fertig mit der Konstruktion in (2). Andernfalls zeichnen wir einen Kreis mit P als Mittelpunkt mit einem hinreichend großen Radius derart, dass sich zwei Schnittpunkte Q_1 und Q_2 mit der Geraden ergeben (dafür braucht man, dass mindestens ein weiterer Punkt zur Verfügung steht). Dann führt wieder die erste Konstruktion zum Ziel.
(4) Dafür führt man zuerst die Konstruktion der Senkrechten S durch P wie in (3) beschrieben durch. Mit P und S führt man dann die Konstruktion (2) durch.

□

24.2. **Arithmetische Eigenschaften von konstruierbaren Zahlen.**

Von nun an werden wir stets die Ebene E mit der reellen Zahlenebene $\mathbb{R}^2$ bzw. der komplexen Ebene $\mathbb{C}$ identifizieren. Dies erlaubt es, die geometrischen Objekte und die Konstruktionen mit Hilfe von Koordinaten zu beschreiben.

Lemma 24.7. *Sei $P = (x, y) \in \mathbb{C} \cong \mathbb{R}^2$ ein Punkt in der Ebene. Dann ist P genau dann konstruierbar, wenn die beiden Koordinaten x und y konstruierbar sind.*

Beweis. Zunächst einmal kann man aufgrund der vorgegebenen Punkte die x-Achse und dann wegen Lemma 24.6 die dazu senkrechte Achse durch 0,

also die y-Achse, konstruieren. Es steht also das Achsenkreuz zur Verfügung. Wenn nun P gegeben ist, so kann man aufgrund von Lemma 24.6 (4) die zu den Achsen parallelen Geraden zeichnen und erhält somit die Koordinatenwerte. Den y-Wert kann man dann noch mit einem Kreis mit dem Nullpunkt als Mittelpunkt auf die x-Achse transportieren. Wenn umgekehrt die beiden Koordinaten gegeben sind, so kann man durch diese die senkrechten Geraden zeichnen. Deren Schnittpunkt ist der gesuchte Punkt. □

Lemma 24.8. *Es sei G eine mit 0 und 1 markierte Gerade, die wir mit den reellen Zahlen identifizieren. Es seien zwei Punkte $a, b \in G$ gegeben. Dann gelten folgende Aussagen*

(1) *Die Summe $a + b$ ist (mit Zirkel und Lineal) konstruierbar.*
(2) *Das Produkt ab ist konstruierbar.*
(3) *Bei $b \neq 0$ ist der Quotient a/b konstruierbar.*

Beweis. (1) Wir verwenden eine zu G senkrechte Gerade H durch 0 und darauf einen Punkt $x \neq 0$. Dazu nehmen wir die zu H senkrechte Gerade G' durch x, die also parallel zu G ist. Wir zeichnen die Gerade H', die parallel zu H ist und durch $a \in G$ verläuft. Der Schnittpunkt von H' und G' markieren wir als a', so dass der Abstand von a' zu x gleich a ist. Jetzt zeichnen wir die Gerade L durch b und x und dazu die parallele Gerade L' durch a'. Der Schnittpunkt von L' mit G ist $y = a + b$, da x, b, a', y ein Parallelogramm bilden. Zum Beweis von (2) und (3) verwenden wir wieder die zu G senkrechte Gerade H. Wir schlagen Kreise mit dem Nullpunkt als Mittelpunkt durch 1, a und b und markieren die entsprechenden Punkte auf H als $1'$, a' und b'. Dabei wählt man $1'$ als einen der beiden Schnittpunkte und a' und b' müssen dann auf den entsprechenden Halbgeraden sein. Um das Produkt zu erhalten, zeichnet man die Gerade L durch a und $1'$ und dazu die parallele Gerade L' durch b'. Diese Gerade schneidet G in genau einem Punkt x. Für diesen Punkt gilt nach dem Strahlensatz das Steckenverhältnis

$$\frac{x}{a} = \frac{b'}{1'} = \frac{b}{1}.$$

Also ist $x = ab$. Um den Quotienten $\frac{a}{b}$ bei $b \neq 0$ zu erhalten, zeichnet man die Gerade T durch 1 und b' und dazu parallel die Gerade T' durch a'. Der Schnittpunkt von T' mit G sei z. Aufgrund des Strahlensatzes gilt die Beziehung

$$\frac{a}{b} = \frac{a'}{b'} = z.$$

□

Satz 24.9. *Die Menge der konstruierbaren Zahlen ist ein Unterkörper von $\mathbb{C}$.*

Beweis. Die 0 und die 1 sind als Ausgangsmenge automatisch darin enthalten. Zu einem Punkt P gehört auch der „gegenüberliegende“ Punkt $-P$ dazu,

da man ihn konstruieren kann, indem man die Gerade durch P und 0 und den Kreis mit Mittelpunkt 0 und Radius P zeichnet; der zweite Schnittpunkt von diesem Kreis und dieser Geraden ist $-P$. Die Menge der konstruierbaren Zahlen ist also unter der Bildung des Negativen abgeschlossen.

Aufgrund von Lemma 24.7 kann man sich beim Nachweis der Körpereigenschaften darauf beschränken, dass die reellen konstruierbaren Zahlen einen Körper bilden. Dies folgt aber aus Lemma 24.8. □

24.3. **Konstruktion von Quadratwurzeln.**

Wenn man sich zwei Punkte 0 und 1 vorgibt und man die dadurch definierte Gerade mit $\mathbb{R}$ identifiziert, so wird diese Gerade durch 0 in zwei Hälften (Halbgeraden) unterteilt, wobei man dann diejenige Hälfte, die 1 enthält, als positive Hälfte bezeichnet. Aus solchen positiven reellen Zahlen kann man mit Zirkel und Lineal die Quadratwurzel ziehen.

Lemma 24.10. *Es sei G eine mit zwei Punkten 0 und 1 markierte Gerade, die wir mit den reellen Zahlen identifizieren. Es sei $a \in G_+$ eine positive reelle Zahl. Dann ist die Quadratwurzel $\sqrt{a}$ aus $0, 1, a$ mittels Zirkel und Lineal konstruierbar.*

Beweis. Wir zeichnen den Kreis mit Mittelpunkt 0 durch 1 und markieren den zweiten Schnittpunkt dieses Kreises mit G als -1. Wir halbieren die Strecke zwischen -1 und a gemäß Lemma 24.6 und erhalten den konstruierbaren Punkt $M = \frac{a-1}{2} \in G$. Der Abstand von M zu a als auch zu -1 ist dann $\frac{a+1}{2}$. Wir zeichnen den Kreis mit Mittelpunkt M und Radius $\frac{a+1}{2}$ und markieren einen der Schnittpunkte des Kreises mit der zu G senkrechten Geraden H durch 0 als x. Wir wenden den Satz des Pythagoras auf das Dreieck mit den Ecken $0, x, M$ an. Daraus ergibt sich

$$x^2 = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 = \frac{a^2+2a+1-(a^2-2a+1)}{4} = \frac{4a}{4} = a.$$

Also repräsentiert (der Abstand von 0 zu) x die Quadratwurzel aus a. □

24. Arbeitsblatt

24.1. **Aufwärmaufgaben.**

Aufgabe 24.1.*

Erstelle eine Kreisgleichung für den Kreis im $\mathbb{R}^2$ mit Mittelpunkt $(2, 7)$, der durch den Punkt $(4, -3)$ läuft.

Aufgabe 24.2. Bestimme die Koordinaten der beiden Schnittpunkte der Geraden G und des Kreises K, wobei G durch die Gleichung $2y - 3x + 1 = 0$ und K durch den Mittelpunkt $(2, 2)$ und den Radius 5 gegeben ist.

Aufgabe 24.3.*

Berechne die Schnittpunkte der beiden Kreise K_1 und K_2, wobei K_1 den Mittelpunkt $(3,4)$ und den Radius 6 und K_2 den Mittelpunkt $(-8,1)$ und den Radius 7 besitzt.

Aufgabe 24.4. Es seien P, Q zwei Punkte auf einer Geraden L und M sei eine weitere Gerade durch P. Konstruiere mit Zirkel und Lineal eine *Raute*, so dass P und Q Eckpunkte sind und eine Seite auf M liegt.

Aufgabe 24.5. Es sei D ein Dreieck in der Ebene mit den drei Eckpunkten A, B, C. Zeige, dass man die Höhen, die Mittelsenkrechten, die Winkelhalbierenden und die Seitenhalbierenden mit Zirkel und Lineal konstruieren kann.

Aufgabe 24.6. Es sei ein Dreieck D durch die Eckpunkte A, B, C in der Ebene E mit den Seiten S, T, R gegeben. Es sei ferner eine Strecke S' durch zwei Punkte $P, Q \in E$ gegeben. Konstruiere mit Zirkel und Lineal ein zu D ähnliches (also winkelgleiches) Dreieck D' derart, dass S' eine Seite von D' ist und dass S' der Seite S entspricht.

Aufgabe 24.7. Es sei ein Kreis K und ein Punkt $P \in K$ gegeben. Konstruiere die Tangente an den Kreis durch P.

Aufgabe 24.8. Es sei eine Gerade G und ein Punkt $P \notin G$ gegeben. Konstruiere einen Kreis mit Mittelpunkt P derart, dass die Gerade eine Tangente an den Kreis wird.

Aufgabe 24.9. Es sei $P \in \mathbb{C}$ ein nichtkonstruierbarer Punkt.

a) Zeige, dass es unendlich viele Geraden durch P gibt, auf denen mindestens ein konstruierbarer Punkt liegt.

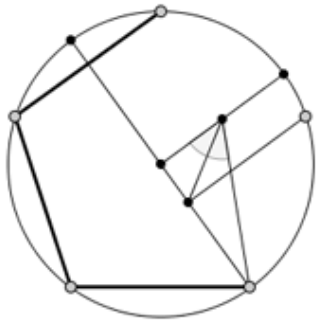
b) Zeige, dass es maximal eine Gerade durch P gibt, auf der es mindestens zwei konstruierbare Punkte gibt.

Aufgabe 24.10. Erläutere geometrisch, warum die 0 das neutrale Element der geometrischen Addition von reellen Zahlen ist.

Aufgabe 24.11. Rekapituliere die Strahlensätze.

Aufgabe 24.12. Es seien P und Q zwei konstruierbare Punkte. Zeige, dass dann auch der Abstand $d(P, Q)$ konstruierbar ist.

Aufgabe 24.13. Beschreibe die Konstruktion mit Zirkel und Lineal eines regelmäßigen Fünfecks, wie sie in der folgenden Animation dargestellt ist.



Konstruktion eines regulären Fünfecks mit Zirkel und Lineal

Aufgabe 24.14.*

Aus einer Menge $T \subseteq E$ seien „wie üblich“ Geraden und Kreise elementar konstruierbar. Als neue Punkte seien allerdings nur die Durchschnitte von einer Geraden mit einer Geraden und von einer Geraden mit einem Kreis erlaubt (also nicht der Durchschnitt von zwei Kreisen). Bestimme die Menge M der Punkte, die aus der Anfangsmenge $\{0, 1\}$ auf diese Weise konstruierbar ist.

24.2. **Aufgaben zum Abgeben.**

Aufgabe 24.15. (5 Punkte)

Berechne die Koordinaten der beiden Schnittpunkte der beiden Kreise K und L, wobei K den Mittelpunkt $(2, 3)$ und den Radius 4 und L den Mittelpunkt $(5, -1)$ und den Radius 7 besitzt.

Aufgabe 24.16. (6 Punkte)

Es sei eine zweielementige Menge $M = \{0, 1\}$ in der Ebene gegeben. Wie viele Punkte lassen sich aus M in einem Schritt, in zwei Schritten und in drei Schritten konstruieren?

Aufgabe 24.17. (2 Punkte)

Erläutere geometrisch, warum die 1 das neutrale Element der geometrischen Multiplikation von reellen Zahlen ist.

Aufgabe 24.18. (2 Punkte)

Erläutere geometrisch, woran die geometrische Division von reellen Zahlen durch 0 scheitert.

Aufgabe 24.19. (3 Punkte)

Bestimme alle Lösungen der Kreisgleichung

$$x^2 + y^2 = 1$$

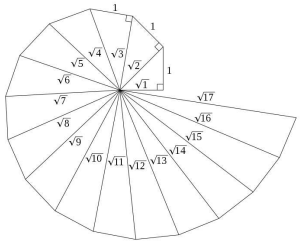
für die Körper $K = \mathbb{Z}/(2)$, $\mathbb{Z}/(5)$ und $\mathbb{Z}/(11)$.

Aufgabe 24.20. (12 Punkte)

Schreibe Computeranimationen, die die in Lemma 24.6 beschriebenen Konstruktionen veranschaulichen (über Commons hochladen).

25. Vorlesung - Die Quadratur des Kreises

25.1. **Die Quadratur des Rechtecks.**



Die Spirale des Theodorus. In dieser Weise kann man alle Quadratwurzeln von natürlichen Zahlen konstruieren.

Korollar 25.1. *Es sei ein Rechteck in der Ebene gegeben. Dann lässt sich mit Zirkel und Lineal ein flächengleiches Quadrat konstruieren.*

Beweis. Die Längen der Rechteckseiten seien a und b. Wir wählen einen Eckpunkt des Rechtecks als Nullpunkt und verwenden die Geraden durch die anliegenden Rechteckseiten als Koordinatenachsen. Wir wählen willkürlich einen Punkt 1 ($\neq 0$) auf einer der Achsen und schlagen einen Kreis um den Nullpunkt durch den Eckpunkt auf der anderen Achse, so dass beide Seitenlängen auf der mit 0 und 1 markierten Achse liegen. Darauf führen wir

die Multiplikation ab nach Lemma 24.8 durch. Aus diesem Produkt zieht man nun gemäß Lemma 24.10 die Quadratwurzel und erhält somit $\sqrt{ab}$. Mit dieser Streckenlänge konstruiert man ein Quadrat, dessen Flächeninhalt gleich dem Flächeninhalt des vorgegebenen Rechtecks ist. □

Man beachte, dass im Beweis der vorstehenden Aussage die Zahl ab (also der Punkt auf der Achse) von der Wahl der 1 abhängt, nicht aber $\sqrt{ab}$ und damit natürlich auch nicht die Seitenlänge des konstruierten Quadrats.

25.2. **Konstruierbare und algebraische Zahlen.**

Wir wollen nun die konstruierbaren Zahlen algebraisch mittels quadratischer Körpererweiterungen charakterisieren. Unter einer reell-quadratischen Körpererweiterung eines Körpers $K \subseteq \mathbb{R}$ verstehen wir eine quadratische Körpererweiterung $K \subseteq K'$ mit $K' \subseteq \mathbb{R}$, die sich also innerhalb der reellen Zahlen abspielt. Eine solche Körpererweiterung ist immer durch die Adjunktion einer Quadratwurzel einer positiven reellen Zahl $\sqrt{c}$ mit $c \in K$, $\sqrt{c} \notin K$ gegeben. Es gilt die Isomorphie

$$K[\sqrt{c}] \cong K[X]/\left(X^2 - c\right).$$

Lemma 25.2. *Sei $K \subseteq \mathbb{R}$ ein Körper. Es sei $P \in \mathbb{C}$ ein Punkt, der sich aus $K^2 = K + K\mathrm{i}$ in einem Schritt konstruieren lässt. Dann liegen die Koordinaten von P in einer reell-quadratischen Körpererweiterung von K.*

Beweis. Wir gehen die drei Möglichkeiten durch, einen Punkt aus K^2 in einem Schritt zu konstruieren. Es sei P der Schnittpunkt von zwei verschiedenen Geraden G_1 und G_2, die über K definiert sind. Es sei also

$$G_1 = \{(x,y) |\, a_1x + b_1y + c_1 = 0\}$$

und

$$G_2 = \{(x,y) |\, a_2x + b_2d + c_2 = 0\}$$

mit $a_1, b_1, c_1, a_2, b_2, c_2 \in K$. Dann gehört der Schnittpunkt zu K^2 und seine Koordinaten gehören zu K. Sei G eine über K definierte Gerade und C ein über K definierter Kreis. Dann ist $G = \{(x,y) |\, ax + by + c = 0\}$ und $C = \{(x,y) |\, (x-r)^2 + (y-s)^2 = d\}$ mit $a, b, c, r, s, d \in K$. Wir können annehmen, dass $b \neq 0$ ist, so dass die Geradengleichung auf die Form $y = ux + v$ gebracht werden kann. Einsetzen von dieser Gleichung in die Kreisgleichung ergibt eine quadratische Gleichung für x über K. Die reellen Koordinaten der (eventuell komplexen) Lösungen davon liegen in einer quadratischen Erweiterung von K. Das gilt dann auch für die zugehörigen Lösungen für y. Seien nun C_1 und C_2 zwei über K definierte verschiedene Kreise. Es seien

$$C_1 = \left\{(x,y) |\, (x-r_1)^2 + (y-s_1)^2 - a_1 = 0\right\}$$

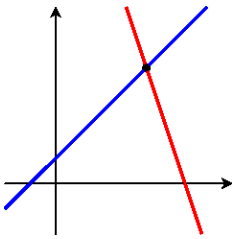
und

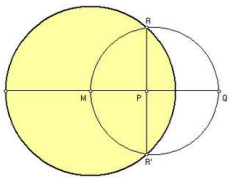
$$C_2 = \left\{(x,y) |\, (x-r_2)^2 + (y-s_2)^2 - a_2 = 0\right\}$$

die Kreisgleichungen. Ein Schnittpunkt der beiden Kreise muss auch jede Linearkombination der beiden Gleichungen erfüllen. Wir betrachten die Differenz der beiden Gleichungen, die die Gestalt

$$x(-2r_1+2r_2)+r_1^2-r_2^2+y(-2s_1+2s_2)+s_1^2-s_2^2-a_1+a_2 \;=\; 0$$

besitzt. D.h. dies ist eine Geradengleichung, und die Schnittpunkte der beiden Kreise stimmen mit den Schnittpunkten eines Kreises mit dieser Geraden überein. Wir sind also wieder im zweiten Fall. □





Beispiel 25.3. Wir betrachten die beiden Kreise mit den Kreisgleichungen

$$x^2+y^2=1 \text{ und } (x-2)^2+y^2=3.$$

Die Differenz der beiden Gleichungen ist

$$x^2-(x-2)^2+2 \;=\; 0$$

bzw.

$$4x=2 \text{ und somit } x=\frac{1}{2}\,.$$

Die Schnittpunkte der beiden Kreise müssen also auch auf der durch $x = \frac{1}{2}$ gegebenen Geraden liegen. Setzt man diese Geradenbedingung in die erste Kreisgleichung ein, so erhält man

$$y^2 \;=\; 1-x^2 \;=\; 1-\frac{1}{4} \;=\; \frac{3}{4},$$

also

$$y \;=\; \pm\frac{\sqrt{3}}{2}.$$

Satz 25.4. *Es sei $P \in \mathbb{C}$ eine komplexe Zahl. Dann ist P eine konstruierbare Zahl genau dann, wenn es eine Kette von reell-quadratischen Körpererweiterungen*

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n$$

derart ist, dass die Koordinaten von P zu K_n gehören.

Beweis. Es sei $P \in \mathbb{C}$ eine konstruierbare komplexe Zahl. D.h. es gibt eine Folge von Punkten $P_1, \ldots, P_n = P$ derart, dass P_{i+1} aus den Vorgängerpunkten $\{0, 1, P_1, \ldots, P_i\}$ in einem Schritt konstruierbar ist. Es sei $P_i = (a_i, b_i)$ und es sei

$$K_i \;=\; \mathbb{Q}(a_1, b_1, \ldots, a_i, b_i)$$

der von den Koordinaten der Punkte erzeugte Unterkörper von $\mathbb{R}$. Nach Lemma 25.2 liegt K_{i+1} in einer reell-quadratischen Körpererweiterung von K_i (und zwar ist $K_{i+1} = K_i$ oder K_{i+1} ist eine reell-quadratische Körpererweiterung von K_i). Die Koordinaten von P liegen also in K_n, und K_n ist das Endglied in einer Folge von quadratischen Körpererweiterungen von $\mathbb{Q}$. Sei umgekehrt angenommen, dass die Koordinaten eines Punktes $P = (a, b)$ in einer Kette von reell-quadratischen Körpererweiterungen von $\mathbb{Q}$ liegen. Wir zeigen durch Induktion über die Länge der Körperkette, dass die Zahlen in einer solchen Kette aus quadratischen Körpererweiterungen konstruierbar sind. Bei $n = 0$ ist $K_0 = \mathbb{Q}$, und diese Zahlen sind konstruierbar. Sei also schon gezeigt, dass alle Zahlen aus K_n konstruierbar sind, und sei $K_n \subset K_{n+1}$ eine reell-quadratische Körpererweiterung. Nach Lemma 2.7 ist $K_{n+1} = K_n[\sqrt{c}]$ mit einer positiven reellen Zahl $c \in K_n$. Nach Induktionsvoraussetzung ist c konstruierbar und nach Lemma 24.10 ist $\sqrt{c}$ konstruierbar. Daher ist auch jede Zahl $u + v\sqrt{c}$ mit $u, v \in K_n$, konstruierbar. Damit sind die Koordinaten von P konstruierbar und somit ist nach Lemma 24.7 auch P selbst konstruierbar. □

Wir werden in der nächsten Vorlesung zeigen, dass eine komplex-algebraische Zahl z genau dann konstruierbar ist, wenn der Grad des Zerfällungskörpers des Minimalpolynoms von z eine Potenz von 2 ist. Für viele Anwendungen sind allerdings schon die oben vorgestellte Charakterisierung und die folgenden Korollare ausreichend.

Korollar 25.5. *Eine mit Zirkel und Lineal konstruierbare Zahl ist algebraisch.*

Beweis. Dies folgt direkt aus Satz 25.4, aus Satz 2.8 und aus Satz 10.4. □

Korollar 25.6. *Sei $z \in \mathbb{C}$ eine konstruierbare Zahl. Dann ist der Grad des Minimalpolynoms von z eine Potenz von zwei.*

Beweis. Die Koordinaten der konstruierbaren Zahl z liegen nach Satz 25.4 in einer Folge von reell-quadratischen Körpererweiterungen

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n.$$

Diese Kette kann man um die komplex-quadratische Körpererweiterung

$$\begin{array}{rcl} K_n & \subset & K_n[\mathrm{i}] \\ & = & L \end{array}$$

ergänzen mit $z \in L$. Nach der Gradformel ist der Grad von L über $\mathbb{Q}$ gleich 2^{n+1}. Dabei ist $\mathbb{Q}(z) = \mathbb{Q}[z] \subseteq L$ ein Unterkörper und daher ist, wieder nach der Gradformel, der Grad von $\mathbb{Q}[z]$ über $\mathbb{Q}$ ein Teiler von 2^{n+1}, also selbst eine Potenz von 2. □

25.3. **Das Delische Problem.**

Wir kommen zur ersten Konsequenz von unserer systematischen Untersuchung der konstruierbaren Zahlen für die klassischen Konstruktionsprobleme.

Korollar 25.7. *Die Würfelverdopplung mit Zirkel und Lineal ist nicht möglich.*

Beweis. Wir betrachten einen Würfel mit der Kantenlänge 1 und dem Volumen 1. Die Konstruktion eines Würfels mit dem doppelten Volumen würde bedeuten, dass man die neue Kantenlänge, also $2^{1/3}$ mit Zirkel und Lineal konstruieren könnte. Das Minimalpolynom von $2^{1/3}$ ist $X^3 - 2$, da dieses offenbar $2^{1/3}$ annulliert und nach Satz 17.9 irreduzibel ist. Nach Korollar 25.6 ist $2^{1/3}$ nicht konstruierbar, da 3 keine Zweierpotenz ist. □

Die Bewohner der Insel Delos befragten während einer Pestepidemie 430 v. Chr. das Orakel von Delphi. Sie wurden aufgefordert, den würfelförmigen Altar des Apollon zu verdoppeln.

25.4. **Die Quadratur des Kreises.**

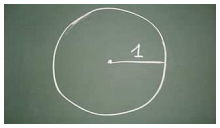
Satz 25.8. *Es ist nicht möglich, zu einem vorgegebenen Kreis ein flächengleiches Quadrat mit Zirkel und Lineal zu konstruieren.*

Beweis. Wenn es ein Konstruktionsverfahren gäbe, so könnte man insbesondere den Einheitskreis mit dem Radius 1 quadrieren, d.h. man könnte ein Quadrat mit der Seitenlänge $\sqrt{\pi}$ mit Zirkel und Lineal konstruieren. Nach Korollar 25.5 muss aber eine konstruierbare Zahl algebraisch sein. Nach dem Satz von Lindemann ist aber π und damit auch $\sqrt{\pi}$ transzendent. □

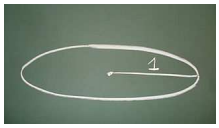
Es gibt natürlich einige geometrische Methoden die Zahl π zu erhalten, z.B. die Abrollmethode und die Schwimmbadmethode.

Beispiel 25.9. Die einfachste Art, die Zahl π geometrisch zu konstruieren, ist die *Abrollmethode*, bei der man einen Kreis mit Durchmesser 1 einmal exakt abrollt. Die zurückgeführte Entfernung ist genau der Kreisumfang, also π.

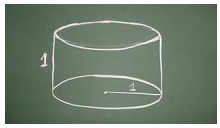
Beispiel 25.10. Man kann die Zahl π auch mit Hilfe von Schwimmbecken und einer idealen Flüssigkeit erhalten.



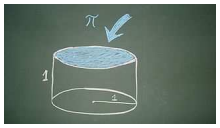
Wir starten mit einem Einheitskreis,



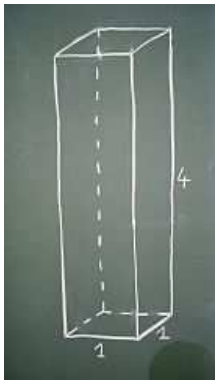
den wir als Grundfläche



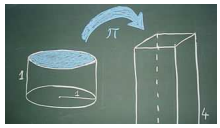
eines Schwimmbeckens der Höhe 1 nehmen.



Das füllen wir randvoll mit Wasser auf.



Wir nehmen ein zweites Schwimmbecken mit quadratischer Grundfläche 1×1 und Höhe 4.



Der Inhalt des ersten Schwimmbeckens wirg

in das zweite Schwimmbecken gegossen.

Der Wasserstand im zweiten Schwimmbecken ist exakt π.

25. Arbeitsblatt

25.1. **Aufwärmaufgaben.**

Aufgabe 25.1. Konstruiere zu einem gegebenen Rechteck mit den Seitenlängen a und b ein flächengleiches Quadrat, wobei eine Seitenlänge als 1 angesetzt werden soll.

Aufgabe 25.2. Zeige, dass man zu einem gegebenen Parallelogramm mit Zirkel und Lineal ein flächengleiches Rechteck derart konstruieren kann, dass eine Seite (von Parallelogramm und Rechteck) übereinstimmt.

Aufgabe 25.3. Zeige, dass man zu einem gegebenen Dreieck mit Zirkel und Lineal ein flächengleiches gleichseitiges Dreieck konstruieren kann.

Aufgabe 25.4. Ist die Zahl, die den „goldenen Schnitt“ beschreibt, eine konstruierbare Zahl?

Aufgabe 25.5. Betrachte ein DinA4-Blatt. Ist das Seitenverhältnis aus langer und kurzer Seitenlänge eine konstruierbare Zahl?

Aufgabe 25.6.*

Skizziere, wie man zu einer quadratischen Gleichung

$$z^2 + pz + q = 0$$

mit $p, q \in \mathbb{R}$ aus den gegebenen Parametern p, q die reellen Lösungen x, y der Gleichung mit Zirkel und Lineal konstruieren kann.

Aufgabe 25.7. Es sei $K \subset K' (\subseteq \mathbb{R})$ eine reell-quadratische Körpererweiterung. Zeige, dass dann auch $K[\mathrm{i}] \subset K'[\mathrm{i}]$ eine quadratische Körpererweiterung ist.

Aufgabe 25.8. Zeige direkt, ohne Bezug auf Koordinaten, dass die Summe von zwei konstruierbaren komplexen Zahlen wieder konstruierbar ist.

Aufgabe 25.9. Betrachte die Tastatur eines Klaviers. Ist das Schwingungsverhältnis von zwei nebeneinander liegendenTasten (bei „gleichstufiger Stimmung“) eine konstruierbare Zahl?

Aufgabe 25.10.*

Es seien $z, w \in \mathbb{C}$ konstruierbare Zahlen. Bestimme, ob die Zahl

$$z^2 - 3z\sqrt{w} + \sqrt{z + w^2} - \frac{5}{7} + 4\sqrt{\sqrt{z} + w} + \sqrt{11}$$

konstruierbar ist.

Aufgabe 25.11. Zeige, dass es Matrizen $M \in \mathrm{Mat}_2(\mathbb{R})$ derart gibt, dass das charakteristische Polynom aus $\mathbb{Q}[X]$ ist, dass in M aber auch transzendente Einträge vorkommen.

Aufgabe 25.12.*

Zeige, dass zu zwei konstruierbaren positiven reellen Zahlen a und b die Potenz a^b nicht konstruierbar sein muss.

Aufgabe 25.13. Zeige, dass es Geraden gibt, auf denen es keinen konstruierbaren Punkt gibt.

Aufgabe 25.14. Begründe elementargeometrisch, dass der Flächeninhalt eines Kreises zu seinem Umfang im Verhältnis Radius halbe steht.

25.2. **Aufgaben zum Abgeben.**

Aufgabe 25.15. (4 Punkte)

Es sei ein Kreis K und ein Punkt P außerhalb des Kreises gegeben. Konstruiere eine der Tangenten an den Kreis, die durch P läuft.

Aufgabe 25.16. (2 Punkte)

Sei $Z \in \mathbb{C}$ eine konstruierbare Zahl und r eine konstruierbare positive reelle Zahl. Zeige, dass dann auch der Kreis mit Mittelpunkt Z und Radius r konstruierbar ist.

Aufgabe 25.17. (3 Punkte)

Es seien P, Q_1, Q_2 drei konstruierbare Punkte derart, dass die Abstände $d(P, Q_1)$ und $d(P, Q_2)$ gleich 1 sind und dass der Winkel zwischen den dadurch definierten Halbgeraden 90 Grad beträgt. Zeige, dass es dann eine affin-lineare Abbildung

$$\varphi\colon\ E = \mathbb{R}^2 \longrightarrow E = \mathbb{R}^2$$

gibt, die 0 auf P, 1 auf Q_1 und i auf Q_2 schickt, und die konstruierbare Punkte in konstruierbare Punkte überführt.

Aufgabe 25.18. (3 Punkte)

Beschreibe die Konstruktion einer reellen Zahl x mit Hilfe von Zirkel und Lineal, deren Abweichung von $\sqrt{\pi}$ kleiner als $0,00001$ ist.

Aufgabe 25.19. (2 Punkte)

Zeige, dass die komplexe Zahl $re^{\mathrm{i}\varphi} = r\,(\cos\varphi, \sin\varphi)$ genau dann konstruierbar ist, wenn r und $e^{\mathrm{i}\varphi}$ konstruierbar sind.

Aufgabe 25.20. (4 Punkte)

Beweise auf zwei verschiedene Arten, dass die komplexe Quadratwurzel einer konstruierbaren komplexen Zahl wieder konstruierbar ist.

26. Vorlesung - Galoistheoretische Charakterisierung von konstr. Zahlen

Wir haben gesehen, dass das Minimalpolynom einer aus $\mathbb{Q}$ konstruierbaren komplexen Zahl eine Zweierpotenz als Grad besitzt. Wir werden hier zeigen, dass eine komplexe algebraische Zahl genau dann konstruierbar ist, wenn der Grad des Zerfällungskörper ihres Minimalpolynoms eine Zweierpotenz ist. Dies erfordert einige einfache gruppentheoretische Vorbereitungen.

26.1. **Konjugationsklassen und Klassengleichung.**

Definition 26.1. Zu einer Gruppe G nennt man die Äquivalenzklassen zur Äquivalenzrelation, bei der zwei Elemente als äquivalent (oder *konjugiert*) gelten, wenn sie durch einen inneren Automorphismus ineinander überführt werden können, die *Konjugationsklassen*.

Zwei Elemente $a, b \in G$ sind also konjugiert, wenn es ein $x \in G$ mit $b = xax^{-1}$ gibt. Den Konjugationsklassen sind wird schon auf dem fünften Arbeitsblatt begegnet.

Die folgende Aussage heißt *Klassengleichung*.

Lemma 26.2. *Sei G eine endliche Gruppe und seien $K_1, \ldots, K_r$ die Konjugationsklassen von G mit mindestens zwei Elementen. Dann ist*

$$\operatorname{ord}(G) = \operatorname{ord}(Z(G)) + \sum_{i=1}^{r} \#(K_i).$$

Beweis. Die Konjugationsklassen sind Äquivalenzklassen, daher bilden sie eine Zerlegung von G. Die Summe der Anzahl der Elemente in den Konjugationsklassen ist daher gleich der Ordnung von G. Die einelementigen Konjugationsklassen entsprechen dabei den Elementen im Zentrum der Gruppe. □

Die Anzahl der Elemente in den einzelnen Konjugationsklassen unterliegt starken Einschränkungen, die das folgende Lemma beinhaltet.

Lemma 26.3. *Sei G eine endliche Gruppe und sei $a \in G$. Dann gelten folgende Aussagen.*

(1) *Die Menge $G_a = \{x \in G | \, xax^{-1} = a\}$ ist eine Untergruppe von G.*
(2) *Sei $K = [a]$ die Konjugationsklasse zu a. Dann ist*
$$\#(K) = \operatorname{ind}_G G_a.$$
(3) *Die Elementanzahl von $K = [a]$ ist ein Teiler von* $\operatorname{ord}(G)$.

Beweis. (1). Es ist klar, dass das neutrale Element zu G_a gehört. Seien $x, y \in G_a$. Dann ist
$$xya(xy)^{-1} = xyay^{-1}x^{-1} = xax^{-1} = a,$$
also $xy \in G_a$. Bei $x \in G_a$ ist $xax^{-1} = a$, was man direkt zu $a = x^{-1}ax$ auflösen kann, was wiederum $x^{-1} \in G_a$ bedeutet. (2). Wir betrachten die Abbildung
$$G \longrightarrow K,\ x \longmapsto xax^{-1}.$$
Da K genau aus allen zu a konjugierten Elementen besteht, ist diese Abbildung surjektiv. Unter dieser Abbildung ist G_a das Urbild von a. Es gilt $xax^{-1} = yay^{-1}$ genau dann, wenn $y^{-1}xax^{-1}y = a$ ist, also genau dann, wenn $y^{-1}x \in G_a$ ist. Das bedeutet, dass die Fasern der Abbildung gerade

die Linksnebenklassen zur Untergruppe G_a sind. Daher ist $\#(K)$ gleich dem Index von G_a in G. (3) folgt aus (2) und Satz 4.16. □

Die Gruppe G_a nennt man auch die *Isotropiegruppe* zu a.

Lemma 26.4. *Es sei p eine Primzahl und G eine endliche Gruppe mit p^r, $r \geq 1$, Elementen. Dann ist das Zentrum Z von G nicht trivial.*

Beweis. Wir gehen von der Klassengleichung aus, also von

$$\operatorname{ord}(G) = \operatorname{ord}(Z) + \sum_{j \in J} n_j,$$

wobei n_j den Index der zu den mehrelementigen Konjugationsklassen C_j gehörenden echten Untergruppen (im Sinne von Lemma 26.3) $G_j \subseteq G$ bezeichnet. Jedes n_j ist nach Lemma 26.3 (3) ein Vielfaches von p. Daher ist auch $\operatorname{ord}(Z)$ ein Vielfaches von p. Somit ist Z nicht trivial. □

26.2. **Galoistheoretische Charakterisierung von konstruierbaren Zahlen.**

Lemma 26.5. *Es sei $K = L_0 \subset L_1 \subset \ldots \subset L_r = L$ eine Kette von quadratischen Körpererweiterungen in $\mathbb{C}$. Dann gibt es eine endliche Galoiserweiterung $K \subseteq M$ in $\mathbb{C}$, die L enthält, und die ebenfalls eine Kette von quadratischen Körpererweiterungen besitzt.*

Beweis. Wir führen Induktion über r, wobei die Fälle $r = 0, 1$ klar sind. Sei also eine Kette von quadratischen Körpererweiterungen

$$K = L_0 \subset L_1 \subset \ldots \subset L_r \subset L_{r+1} = L$$

gegeben. Nach Induktionsvoraussetzung gibt es einen Körper M, $L_r \subseteq M \subseteq \mathbb{C}$, derart, dass $K \subseteq M$ eine Galoiserweiterung ist, die eine Kette von quadratischen Körpererweiterungen besitzt. Als Galoiserweiterung über K ist M nach Satz 16.6 der Zerfällungskörper eines (separablen) Polynoms $F \in K[X]$. Wir können $L_{r+1} = L_r(x)$ mit $x^2 = a \in L_r$ schreiben. Wir betrachten das Polynom

$$H = \prod_{\varphi \in \operatorname{Gal}(M|K)} \left(X^2 - \varphi(a)\right).$$

Die Koeffizienten dieses Polynoms sind invariant unter der Galoisgruppe $\operatorname{Gal}(M|K)$ und gehören daher wegen Satz 16.6 zu K. Sei M' der Zerfällungskörper von H über M in $\mathbb{C}$. Dieser ist insgesamt der Zerfällungskörper vom Produkt FH über K, so dass $K \subseteq M'$ insbesondere eine Galoiserweiterung ist. Nach Konstruktion ist x eine Nullstelle von H, woraus sich $L = L_r(x) \subseteq M'$ ergibt. Nach Induktionsvoraussetzung gibt es eine Kette von quadratischen Körpererweiterungen

$$K = M_0 \subset M_1 \subset \ldots \subset M_s = M.$$

Diese erweitern wir sukzessive zu einer Kette

$$M = M_s \subset M_{s+1} \subset \ldots \subset M_t = M'$$

von quadratischen Körpererweiterungen, wobei $M_{s+i+1} = M_{s+i}\left(\sqrt{\varphi_i(a)}\right)$ sei und φ_i die Automorphismen von $\mathrm{Gal}\,(M|K)$ durchlaufe. □

Satz 26.6. *Es sei $K \subseteq \mathbb{C}$ ein Unterkörper und $z \in \mathbb{C}$. Dann sind folgende Aussagen äquivalent.*

(1) *Die komplexe Zahl z ist aus K konstruierbar.*
(2) *Es gibt in $\mathbb{C}$ eine Körperkette aus quadratischen Körpererweiterungen*

$$K = L_0 \subset L_1 \subset \ldots \subset L_r = L$$

mit $z \in L$.
(3) *Das Element z ist algebraisch über K, und der Grad des Zerfällungskörpers von z über K ist eine Zweierpotenz.*
(4) *Das Element z ist algebraisch über K, und die Ordnung der Galoisgruppe des Zerfällungskörpers von z über K ist eine Zweierpotenz.*
(5) *Es gibt eine endliche Galoiserweiterung $K \subseteq M$ (in $\mathbb{C}$) mit $z \in M$, deren Grad eine Zweierpotenz ist.*

Beweis. Die Äquivalenz von (1) und (2) ergibt sich wie in Satz 25.4. Sei (2) erfüllt. Nach Lemma 26.5 gibt es eine endliche Galoiserweiterung $K \subseteq M$, die L und damit z enthält und die eine Kette von quadratischen Körpererweiterungen besitzt. Nach Satz 2.8 ist dann der Grad von $K \subseteq M$ eine Zweierpotenz. Es sei L' der Zerfällungskörper von z über K. Da M galoissch ist, gilt $L' \subseteq M$, und daher ist auch der Grad von $K \subseteq L'$ eine Zweierpotenz. Die Implikationen von (3) nach (4) und von (4) nach (5) sind klar aufgrund von Satz 16.6. (5) $\Longrightarrow$ (2). Sei nun (5) erfüllt, und eine Galoiserweiterung $K \subseteq M$ in $\mathbb{C}$ mit $z \in M$ gegeben, deren Grad eine Zweierpotenz 2^r ist. Wir zeigen durch Induktion nach r, dass es eine Filtration der Körpererweiterung durch quadratische Körpererweiterungen gibt (also ohne direkten Bezug auf ein z.). Dabei ist der Fall $r = 0$ trivial. Sei also $\mathrm{grad}_K M = 2^r$ ($r \geq 1$) und die Existenz von Körperketten für kleinere Exponenten bereits bewiesen. Nach Satz 16.6 ist dann auch die Ordnung der Galoisgruppe $G = \mathrm{Gal}\,(M|K)$ gleich 2^r. Aufgrund von Lemma 26.4 gibt es ein nichttriviales Zentrum $Z \subseteq G$, so dass es nach dem Hauptsatz für endliche abelsche Gruppen auch eine Untergruppe $H \subseteq Z$ mit zwei Elementen gibt. Als Untergruppe des Zentrums ist H ein Normalteiler in G. Wir betrachten $L = \mathrm{Fix}\,(H) \subseteq M$. Nach Satz 16.6 ist $\mathrm{grad}_L M = 2$ und nach Satz 17.5 ist $K \subseteq L$ eine Galoiserweiterung der Ordnung 2^{r-1} und besitzt nach Induktionsvoraussetzung eine Filtration aus quadratischen Körpererweiterungen. Diese Filtration wird durch $L \subset M$ zu einer solchen Gesamtfiltration ergänzt. □

Bemerkung 26.7. Wir betrachten die konstruierbare Zahl $u = \sqrt{1+\sqrt{3}}$ und knüpfen dabei an Beispiel 14.9 an. Dort wurde gezeigt, dass u das Minimalpolynom $X^4 - 2X^2 - 2$ besitzt, welches über $L = \mathbb{Q}[u]$ die Primfaktorzerlegung

$$X^4 - 2X^2 - 2 \;=\; (X-u)(X+u)\left(X^2 - 1 + \sqrt{3}\right)$$

besitzt. Insbesondere ist L nicht normal, der Zerfällungskörper ist vielmehr $Z = L[\sqrt{1-\sqrt{3}}]$ und hat den Grad 8 über $\mathbb{Q}$. Seine Galoisgruppe ist nicht abelsch, denn andernfalls wäre jeder Zwischenkörper nach Satz 17.5 (1) eine Galoiserweiterung von $\mathbb{Q}$, was aber für L nicht zutrifft.

Abschließend bemerken wir, dass es algebraische Elemente $z \in \mathbb{C}$ gibt, deren Minimalpolynom zwar den Grad 4 besitzt, wo der Grad des Zerfällungskörpers aber keine Zweierpotenz ist. Für ein hinreichend kompliziertes Polynom vom Grad 4 ist nämlich die Galoisgruppe des Zerfällungskörpers gleich der symmetrischen Gruppe S_4 und daher ist der Grad des Zerfällungskörpers gleich 24.

26. Arbeitsblatt

26.1. **Aufwärmaufgaben.**

Aufgabe 26.1. Sei G eine Gruppe. Zeige, dass G genau dann kommutativ ist, wenn alle Konjugationsklassen einelementig sind.

Aufgabe 26.2. Sei G eine endliche Gruppe und seien $x, y \in G$ konjugierte Elemente. Zeige, dass x und y die gleiche Ordnung besitzen.

Aufgabe 26.3. Zeige, dass zwei Permutationen $\sigma, \tau \in S_n$ genau dann konjugiert sind, wenn ihre Zykeldarstellung den gleichen Typ haben, d.h. wenn die Anzahl der Zykel und deren Längen übereinstimmen.

Aufgabe 26.4. Überprüfe die Klassengleichung für die Permutationsgruppen S_2, S_3, S_4, S_5.

Aufgabe 26.5. Überprüfe die Klassengleichung für die eigentliche Würfelgruppe.

Aufgabe 26.6. Bestimme zu jeder Permutation $\pi \in S_n$, $n = 2, 3, 4, 5$, die Isotropiegruppe G_π und die Konjugationsklasse $[\pi]$, und bestätige die Gleichung

$$\operatorname{ord}(G_\pi) \cdot \#([\pi]) = n!$$

aus Lemma 26.3.

Aufgabe 26.7.*

Es sei p eine Primzahl und G eine endliche Gruppe mit p^r Elementen. Zeige, dass G auflösbar ist.

Aufgabe 26.8. Man gebe ein Beispiel für eine endliche Körpererweiterung $\mathbb{Q} \subseteq K$, $K \subseteq \mathbb{C}$, das zeigt, dass zu einem Element $z = a + b\mathrm{i} \in K$ die reellen Koordinaten a und b nicht zu K gehören müssen.

Aufgabe 26.9. Es sei $z \in \mathbb{C}$ eine konstruierbare Zahl. Zeige, dass der erzeugte Unterkörper $\mathbb{Q}(z)$ eine Radikalerweiterung von $\mathbb{Q}$ ist.

Aufgabe 26.10. Es sei $z \in \mathbb{C}$ eine konstruierbare Zahl mit dem Minimalpolynom $F \in \mathbb{Q}[X]$. Zeige, dass jede komplexe Nullstelle von F ebenfalls konstruierbar ist.

Aufgabe 26.11. Es sei $z \in \mathbb{C}$ eine konstruierbare Zahl mit dem Minimalpolynom $F \in \mathbb{Q}[X]$. Zeige, dass der Zerfällungskörper von F eine Radikalerweiterung von $\mathbb{Q}$ ist.

Aufgabe 26.12. Zeige, dass eine konstruierbare Zahl $z \in \mathbb{C}$ in einer auflösbaren Körpererweiterung $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$ liegt.

Aufgabe 26.13. Es sei $K \subseteq L$ eine Galoiserweiterung vom Grad p^r mit einer Primzahl p und $r \geq 1$. Zeige, dass es einen echten Zwischenkörper $K \subset M \subset L$ gibt, der über K eine Galoiserweiterung ist.

Aufgabe 26.14. Es sei $K = L_0 \subset L_1 \subset \ldots \subset L_r = L$ eine Kette von quadratischen Körpererweiterungen in $\mathbb{C}$. Zeige, dass es eine Kette von quadratischen Körpererweiterungen $L = M_0 \subset M_1 \subset \ldots \subset M_s = M$ derart gibt, dass $K \subseteq M$ eine Galoiserweiterung ist.

Aufgabe 26.15. Finde zur Kette aus quadratischen Körpererweiterungen

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}] = L$$

eine Galoiserweiterung $\mathbb{Q} \subseteq M$ minimalen Grades mit $\sqrt[4]{2} \in M$.

26.2. **Aufgaben zum Abgeben.**

Aufgabe 26.16. (4 Punkte)

Es seien $K \subseteq L \subseteq M$ endliche Körpererweiterungen. Es sei $F \in K[X]$ ein irreduzibles Polynom, dass über M in Linearfaktoren zerfalle. Der Zwischenkörper L enthalte keine Nullstelle von F. Folgt daraus, dass F irreduzibel über L ist?

Aufgabe 26.17. (4 Punkte)

Es sei $\mathbb{Q} \subseteq L$ eine Körpererweiterung in $\mathbb{C}$ und es sei $K \subseteq L$ der Unterkörper, der aus allen konstruierbaren Zahlen in L besteht. Zeige, dass für jeden Automorphismus $\varphi \in \mathrm{Gal}\,(L|\mathbb{Q})$ die Beziehung $\varphi(K) \subseteq K$ gilt.

Aufgabe 26.18. (3 Punkte)

Es seien $\alpha_1, \ldots, \alpha_n$ algebraische Zahlen.

a) Zeige, dass es ein irreduzibles Polynom $F \in \mathbb{Q}[X]$ derart gibt, dass man alle α_i als $\mathbb{Q}$-Linearkombination von Potenzen der Nullstellen von F schreiben kann.

b) Zeige, dass es kein irreduzibles Polynom $F \in \mathbb{Q}[X]$ derart geben muss, dass alle α_i Nullstellen von F sind.

Aufgabe 26.19. (5 Punkte)

Sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei $z \in L$ ein Element derart, dass $\varphi(z)$, $\varphi \in G$, eine K-Basis von L bildet. Wir betrachten das Polynom

$$F = \prod_{\varphi \in G} (X - \varphi(z))\,.$$

Zeige, dass die Koeffizienten von F zu K gehören, dass F in $K[X]$ irreduzibel ist und dass L der Zerfällungskörper von F über K ist.

27. Vorlesung - Konstruierbare Einheitswurzeln

27.1. **Konstruierbare Einheitswurzeln.**

Definition 27.1. Sei $n \in \mathbb{N}_+$. Man sagt, dass *das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar* ist, wenn die komplexe Zahl

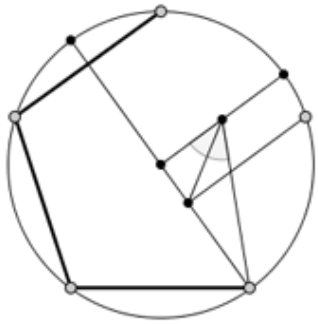
$$e^{2\pi \mathrm{i}/n} = \cos\left(\frac{2\pi}{n}\right) + \mathrm{i}\sin\left(\frac{2\pi}{n}\right)$$

eine konstruierbare Zahl ist.

Die Menge der komplexen Einheitswurzeln $e^{\frac{2\pi ik}{n}}$, $k = 0, \ldots, n-1$, bilden die Eckpunkte eines regelmäßigen n-Ecks, wobei 1 eine Ecke bildet. Alle Eckpunkte liegen auf dem Einheitskreis. Die Ecke $e^{\frac{2\pi i}{n}}$ ist eine primitive Einheitswurzel; wenn diese mit Zirkel und Lineal konstruierbar ist, so sind auch alle weiteren Eckpunkte konstruierbar, da diese ja Potenzen der primitiven Einheitswurzel sind. Das reguläre n-Eck ist genau dann konstruierbar, wenn der n-te Kreisteilungskörper ein Unterkörper der konstruierbaren Zahlen ist.

Bei $n = 1, 2$ kann man sich darüber streiten, ob man von einem regelmäßigen n-Eck sprechen soll, jedenfalls gibt es die zugehörigen Einheitswurzeln und diese sind aus $\mathbb{Q}$, also erst recht konstruierbar. Das regelmäßige Dreieck ist ein gleichseitiges Dreieck und dieses ist konstruierbar nach Beispiel 18.3, da der dritte Kreisteilungskörper eine quadratische Körpererweiterung von $\mathbb{Q}$ ist und die Menge der konstruierbaren Zahlen nach Satz 25.4 unter quadratischen Körpererweiterungen abgeschlossen ist.

(man kann einfacher auch direkt zeigen, dass ein gleichseitiges Dreieck aus seiner Grundseite heraus konstruierbar ist). Das regelmäßige Viereck ist ein Quadrat mit den Eckpunkten $1, \mathrm{i}, -1, -\mathrm{i}$, und dieses ist ebenfalls konstruierbar. Das regelmäßige Fünfeck ist ebenfalls konstruierbar, wie in Beispiel 19.5 in Verbindung mit Satz 25.4 bzw. in Aufgabe 24.13 gezeigt wurde. Wir werden im Folgenden sowohl positive als auch negative Resultate zur Konstruierbarkeit von regelmäßigen n-Ecken vorstellen. Zunächst untersuchen wir den Zusammenhang zwischen der Konstruierbarkeit des n-Ecks und der Konstruierbarkeit des k-Ecks, wenn k ein Teiler von n ist. In diesem Fall lässt sich das regelmßige k-Eck in das regelmäßige n-Eck einschreiben.



Konstruktion eines regulären Fünfecks mit Zirkel und Lineal

Lemma 27.2. *Sei $m = kn$, $m, k, n \in \mathbb{N}_+$. Dann gelten folgende Aussagen.*

(1) *Das regelmäßige 2^r-Eck, $r \in \mathbb{N}$, ist konstruierbar.*
(2) *Wenn das regelmäßige m-Eck konstruierbar ist, so sind auch das regelmäßige n-Eck und das regelmäßige k-Eck konstruierbar.*

(3) *Wenn n und k teilerfremd sind und wenn das regelmäßige n-Eck und das regelmäßige k-Eck konstruierbar sind, so ist auch das regelmäßige m-Eck konstruierbar.*

Beweis. (1) folgt daraus, dass eine Winkelhalbierung stets mit Zirkel und Lineal durchführbar ist. (2). Nach Voraussetzung ist $e^{\frac{2\pi \mathrm{i}}{nk}}$ konstruierbar. Dann ist auch nach Satz 24.9 die Potenz

$$\left(e^{\frac{2\pi \mathrm{i}}{nk}}\right)^n = e^{\frac{2\pi \mathrm{i}}{k}}$$

konstruierbar. (3). Seien nun $e^{\frac{2\pi \mathrm{i}}{n}}$ und $e^{\frac{2\pi \mathrm{i}}{k}}$ konstruierbar und n und k teilerfremd. Nach dem Lemma von Bezout gibt es dann ganze Zahlen r, s mit $rn + sk = 1$. Daher ist auch

$$\left(e^{\frac{2\pi \mathrm{i}}{n}}\right)^s \left(e^{\frac{2\pi \mathrm{i}}{k}}\right)^r = \left(e^{\frac{2\pi \mathrm{i}k}{nk}}\right)^s \left(e^{\frac{2\pi \mathrm{i}n}{nk}}\right)^r = e^{\frac{2\pi \mathrm{i}sk}{nk}} e^{\frac{2\pi \mathrm{i}rn}{nk}} = e^{\frac{2\pi \mathrm{i}(sk+rn)}{nk}} = e^{\frac{2\pi \mathrm{i}}{nk}}$$

konstruierbar. □

Aus diesem Lemma kann man in Zusammenhang mit den oben erwähnten Konstruktionsmöglichkeiten folgern, dass die regelmäßigen $3 \cdot 2^r$-Ecke, die regelmäßigen $5 \cdot 2^r$-Ecke und die regelmäßigen $15 \cdot 2^r$-Ecke für jedes r konstruierbar sind. Wenn man die Zahl als

$$n = 2^r 3^{r_1} \cdots 5^{r_2} \cdot$$

schreibt, so wird mit dem Lemma die Konstruierbarkeit des n-Ecks auf die Konstruierbarkeit des regelmäßigen Ecks zu Prizmahlpotenzen zurückgeführt. Ein entscheidendes notwendiges Kriterium (das sich später auch als hinreichend erweist) für die Konstruierbarkeit wird im folgenden Satz formuliert.

Satz 27.3. *Sei n eine natürliche Zahl derart, dass das regelmäßige n-Eck konstruierbar ist. Dann ist $\varphi(n)$ eine Zweierpotenz.*

Beweis. Die Voraussetzung besagt, dass die primitive Einheitswurzel $\zeta = e^{\frac{2\pi \mathrm{i}}{n}}$ konstruierbar ist. Dann muss nach Korollar 25.6 der Grad des Minimalpolynoms von ζ eine Zweierpotenz sein. Nach Korollar 19.12 ist das Minimalpolynom von ζ das n-te Kreisteilungspolynom, und dieses hat den Grad $\varphi(n)$. Also muss $\varphi(n)$ eine Zweierpotenz sein. □

27.2. **Winkeldreiteilung.**

Wir sind nun in der Lage, das Problem der Winkeldreiteilung zu beantworten.

Korollar 27.4. *Das regelmäßige 9-Eck ist nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Wäre das regelmäßige 9-Eck konstruierbar, so müsste nach Satz 27.3 $\varphi(9)$ eine Zweierpotenz sein. Es ist aber $\varphi(9) = 2 \cdot 3 = 6$. □

Satz 27.5. *Es ist nicht möglich, einen beliebig vorgegebenen Winkel mittels Zirkel und Lineal in drei gleich große Teile zu unterteilen.*

Beweis. Es genügt, einen (konstruierbaren) Winkel α derart anzugeben, dass $\alpha/3$ nicht konstruierbar ist. Wir betrachten $\alpha = 120°$ Grad, welcher konstruierbar ist, da die dritten Einheitswurzeln konstruierbar sind, weil sie nämlich in einer quadratischen Körpererweiterung von $\mathbb{Q}$ liegen. Dagegen ist der Winkel $\alpha/3 = 120°/3 = 40°$ nicht konstruierbar, da andernfalls das regelmäßige 9-Eck konstruierbar wäre, was nach Korollar 27.4 aber nicht der Fall ist. □

Wir geben noch einen weiteren Beweis, dass die Winkeldreiteilung mit Zirkel und Lineal nicht möglich ist, der nicht auf der allgemeinen Irreduzibilität der Kreisteilungspolynome beruht.

Lemma 27.6. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes Polynom vom Grad ≤ 3 ohne Nullstelle in $\mathbb{Z}$. Dann ist F irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Aufgrund von Lemma 18.7 und der Gradvoraussetzung genügt es zu zeigen, dass es keine Faktorzerlegung $F = GH$ in $\mathbb{Z}[X]$ mit $\operatorname{grad}(G) = 1$ geben kann. Sei also angenommen, dass $G = aX+b \in \mathbb{Z}[X]$ ein Teiler von F ist. Der Leitkoeffizient a teilt den Leitkoeffizienten von F, also 1, daher muss $a \in \mathbb{Z}$ eine Einheit sein. Dann ist $a = \pm 1$ und somit ist $\pm b$ eine Nullstelle im Widerspruch zur Voraussetzung. □

Einfache Beispiele wie $F = (2X+1)^2$ zeigen, dass ohne die Voraussetzung normiert die Aussage nicht stimmt. Ob ein ganzzahliges normiertes Polynom ganzzahlige Nullstellen besitzt oder nicht, ist im Allgemeinen einfach zu zeigen. Für n betragsmäßig groß kann man durch eine einfache Abschätzung zeigen, dass es dafür keine Nullstelle geben kann, und für n in einem verbleibenden überschaubaren Bereich kann man durch explizites Ausrechnen feststellen, ob eine Nullstelle vorliegt oder nicht. Die Zerlegung

$$X^4 - 4 = \left(X^2 - 2\right)\left(X^2 + 2\right)$$

zeigt, dass diese Aussage für Grad ≥ 4 nicht gilt.

Bemerkung 27.7. Wir zeigen direkt, dass man den Winkel 20° Grad nicht konstruieren kann (obwohl man 60° Grad konstruieren kann). Aufgrund der *Additionstheoreme für die trigonometrischen Funktionen* gilt

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$$

und damit

$$\begin{aligned}(2\cos 20°)^3 - 3(2\cos 20°) - 1 &= 2\left(4\cos^3 20° - 3\cos 20° - \frac{1}{2}\right)\\ &= 2\left(\cos 60° - \frac{1}{2}\right)\\ &= 0.\end{aligned}$$

Also wird $2\cos 20°$ vom Polynom X^3-3X-1 annulliert. Dieses Polynom hat keine ganzzahlige Nullstelle und ist daher nach Lemma 27.6 irreduzibel. Also muss es nach Lemma 7.12 das Minimalpolynom von $2\cos 20°$ sein. Daher kann $2\cos 20°$ nach Korollar 25.6 nicht konstruierbar sein und damit ebensowenig $\cos 20°$.

27.3. **Fermatsche Primzahlen.**

Die Frage der Konstruierbarkeit von regelmäßigen n-Ecken führt uns zu Fermatschen Primzahlen.

Definition 27.8. Eine Primzahl der Form 2^s+1, wobei s eine positive natürliche Zahl ist, heißt *Fermatsche Primzahl*.

Es ist unbekannt, ob es unendlich viele Fermatsche Primzahlen gibt. Es ist noch nicht mal bekannt, ob es außer den ersten fünf Fermatschen Primzahlen

$$3, 5, 17, 257, 65537$$

überhaupt weitere Fermatschen Primzahlen gibt.

Lemma 27.9. *Bei einer Fermatschen Primzahl 2^s+1 hat der Exponent die Form $s = 2^r$ mit einem $r \in \mathbb{N}$.*

Beweis. Wir schreiben $s = 2^k u$ mit u ungerade. Damit ist

$$2^{2^k u}+1 = \left(2^{2^k}\right)^u + 1.$$

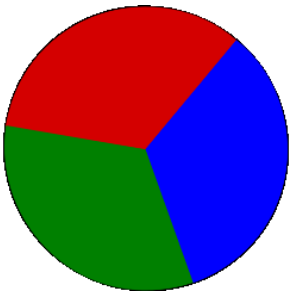
Für ungerades u gilt generell die polynomiale Identität (da -1 eine Nullstelle ist)

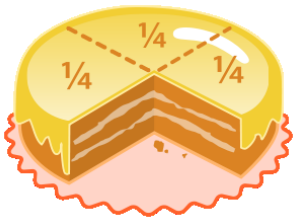
$$X^u+1 = (X+1)\left(X^{u-1}-X^{u-2}+X^{u-3}-\ldots+X^2-X+1\right).$$

Also ist $2^{2^k}+1 \geq 3$ ein Teiler von $2^{2^k u}+1$. Da diese Zahl nach Voraussetzung prim ist, müssen beide Zahlen gleich sein, und dies bedeutet $u = 1$. □

Eine Fermatsche Primzahl ist nach diesem Lemma also insbesondere eine Fermat-Zahl im Sinne der folgenden Definition.

Definition 27.10. Eine Zahl der Form $2^{2^r}+1$, wobei r eine natürliche Zahl ist, heißt *Fermat-Zahl*.





Diese Torte wurde nicht mit Zirkel und Lineal geteilt.

Satz 27.11. *Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt*

$$n = 2^\alpha p_1 \cdots p_k$$

hat, wobei die p_i verschiedene Fermatsche Primzahlen sind.

Beweis. Es sei $n = 2^\alpha p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung von n mit den verschiedenen ungeraden Primzahlen p_i, $i = 1, \ldots, k$, und positiven Exponenten $r_i \geq 1$ (und $\alpha \geq 0$). Nach Satz 27.3 muss die eulersche Funktion eine Zweierpotenz sein, also

$$\varphi(n) = 2^t.$$

Andererseits gilt nach Lemma 19.7 die Beziehung

$$\varphi(n) = 2^{\alpha-1}(p_1 - 1)p_1^{r_1-1} \cdots (p_k - 1)p_k^{r_k-1}$$

(bei $\alpha = 0$ ist der Ausdruck $2^{\alpha-1}$ zu streichen). Da dies eine Zweierpotenz sein muss, dürfen die ungeraden Primzahlen nur mit einem Exponenten 1 (oder 0) auftreten. Ferner muss jede beteiligte Primzahl p die Gestalt $p = 2^s + 1$ haben, also eine Fermatsche Primzahl sein. Für die andere Richtung muss man aufgrund von Lemma 27.2 lediglich zeigen, dass für eine Fermatsche Primzahl $p = 2^s + 1$ das regelmäßige p-Eck konstruierbar ist. Der p-te Kreisteilungskörper besitzt nach Lemma 19.4 den Grad $p - 1 = 2^s$, und dieser ist der Zerfällungskörper des p-ten Kreisteilungspolynoms und wird von der p-ten primitiven Einheitswurzel $\zeta = e^{2\pi \mathrm{i}/p}$ erzeugt. Aufgrund von Satz 26.6 ist somit ζ konstruierbar. □

Aus Satz 27.11 ergibt sich, dass in Satz 27.3 auch die Umkehrung gilt. Man kann Satz 27.11 auch ohne Bezug auf Satz 26.6 beweisen, indem man verwendet, dass ein Kreisteilungskörper eine abelsche Körpererweiterung ist. Wenn dessen Grad eine Zweierpotenz ist, so gibt es aufgrund der Galoiskorrespondenz auch eine Filtrierung mit sukzessiven quadratischen Körpererweiterungen, und die Konstruierbarkeit folgt aus Satz 25.4.

27. Arbeitsblatt

27.1. **Aufwärmaufgaben.**

Aufgabe 27.1. Was ist eigentlich ein „Winkel“?

Aufgabe 27.2. Zeige, dass man jeden vorgegebenen Winkel mittels Zirkel und Lineal halbieren kann.

Aufgabe 27.3. Konstruiere mit Zirkel und Lineal ein regelmäßiges Zwölfeck.

Aufgabe 27.4.*

Zeige, dass es auf dem Einheitskreis unendlich viele konstruierbare Punkte gibt.

Aufgabe 27.5. Zeige auf möglichst viele verschiedene Arten, dass die Menge der konstruierbaren Zahlen auf dem komplexen Einheitskreis dicht liegen.

Aufgabe 27.6. Bestimme für alle $n \leq 30$, ob das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist oder nicht.

Aufgabe 27.7. Man gebe eine Liste aller natürlichen Zahlen n zwischen 100 und 200 mit der Eigenschaft, dass das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar ist.

Aufgabe 27.8. Welche der Winkel

$$10^\circ,\ 20^\circ,\ 30^\circ,\ 40^\circ, \ldots, 350^\circ$$

sind mit Zirkel und Lineal konstruierbar?

Aufgabe 27.9.*

Es sei n eine zu 360 teilerfremde natürliche Zahl. Zeige, dass der Winkel n° nicht mit Zirkel und Lineal konstruierbar ist.

Aufgabe 27.10.*

Man gebe einen Winkel a°, $0 < a < 1$, an, der mit Zirkel und Lineal konstruierbar ist.

Aufgabe 27.11. Es seien P und Q konstruierbare Zahlen. Zeige, dass die Menge der konstruierbaren Strahlen, die von P ausgehen, in einer natürlichen Bijektion zur Menge der konstruierbaren Strahlen steht, die von Q ausgehen.

Aufgabe 27.12. Es sei β ein Winkel, der durch zwei konstruierbare (Halb)-Geraden durch den Nullpunkt gegeben ist. Zeige, dass die Drehung um den Nullpunkt um den Winkel β konstruierbare Punkte in konstruierbare Punkte überführt.

Aufgabe 27.13.*

Es sei $P \in \mathbb{R}^2$ und

$$\varphi\colon\ \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

eine Drehung um den Drehpunkt P um den Winkel β, $0° < \beta < 360°$, mit der Eigenschaft, dass konstruierbare Punkte in konstruierbare Punkte überführt werden.

a) Zeige, dass P ein konstruierbarer Punkt ist.

b) Zeige, dass der Drehwinkel β in dem Sinne konstruierbar ist, dass er als Winkel zwischen zwei konstruierbaren Geraden realisiert werden kann.

Aufgabe 27.14. Zeige, dass ein Kreisteilungskörper K genau dann ein Unterkörper der konstruierbaren Zahlen ist, wenn sein Grad eine Zweierpotenz ist.

Aufgabe 27.15. Bestimme die Galoisgruppe für den Kreisteilungskörper K_{15}.

Aufgabe 27.16. Bestimme die Galoisgruppe für die konstruierbaren Kreisteilungskörper.

Aufgabe 27.17. Es sei p eine Primzahl. Wir betrachten die Körperkette der Kreisteilungskörper

$$\mathbb{Q} \subseteq K_p \subseteq K_{p^2} \subseteq K_{p^3} \subseteq \ldots .$$

Es sei

$$L_p := \bigcup_{r \in \mathbb{N}} K_{p^r}.$$

(1) Zeige, dass L ein Körper ist.
(2) Zeige, dass die Körpererweiterung $\mathbb{Q} \subseteq L$ algebraisch, aber nicht endlich ist.
(3) Für welche Primzahlen p besteht L_p nur aus konstruierbaren Zahlen?

27.2. **Aufgaben zum Abgeben.**

Aufgabe 27.18. (2 Punkte)

Beweise die Formel

$$\cos 3\alpha \ = \ 4\cos^3 \alpha - 3\cos\alpha$$

aus den Additionstheoremen für die trigonometrischen Funktionen.

Aufgabe 27.19. (4 Punkte)

Bestimme die Koordinaten der fünften Einheitswurzeln in $\mathbb{C}$.

Aufgabe 27.20. (4 Punkte)

Zeige, dass es nicht für jede konstruierbare Zahl $z \in \mathbb{C}$ einen Kreisteilungskörper K_n mit $z \in K_n$ gibt.

Aufgabe 27.21. (5 Punkte)

Es sei $n \in \mathbb{N}$ eine natürliche Zahl, für die das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar sei. Es sei eine Strecke S durch zwei Punkte $P, Q \in E$ gegeben. Konstruiere mit Zirkel und Lineal ein regelmäßiges n-Eck R derart, dass S eine der Kanten von R wird.

Tipp: Aufgabe 24.6 kann helfen.

Aufgabe 27.22. (4 Punkte)

Welche der Winkel

$$1^\circ,\ 2^\circ,\ 3^\circ,\ 4^\circ, \ldots, 10^\circ$$

sind mit Zirkel und Lineal konstruierbar?

28. Vorlesung - Transzendenzgrad

In dieser Vorlesung standen endliche Körpererweiterungen der rationalen Zahlen $\mathbb{Q}$ im Mittelpunkt. Zum Abschluss werden wir Körper betrachten, die von den rationalen Zahlen aus nicht algebraisch erfasst werden können, sondern transzendente Elemente enthalten. Diese Eigenschaft haben zwar auch die reellen Zahlen, aber diese lassen sich von den rationalen Zahlen aus als Grenzwerte erfassen (was allerdings kein algebraisches Konzept ist). Hier geht es um transzendente Elemente, die eher den Charakter von Funktionen oder einfach von Variablen haben. Es bestehen enge Beziehungen zur Invariantentheorie, Dimensionstheorie für kommutative Ringe, Funktionenkörper von algebraischen Varietäten.

28.1. **Algebraische Unabhängigkeit.**

Wir haben schon öfters den Körper der rationalen Funktionen $K(X)$, also den Quotientenkörper des Polynomringes in einer Variablen über einem Körper erwähnt. Dort gibt es das Phänomen, dass dieser Körper echte Unterkörper enthält, die zu diesem Körper selbst isomorph sind, und zwar als K-Algebra. Beispielsweise ist der von X^2 erzeugte Unterkörper $K(X^2) \subseteq K(X)$ selbst isomorph zu $K(Y)$ (und damit zu $K(X)$). Der Grad der angegebenen Erweiterung ist 2. In der Tat ist sogar für jedes Polynom $P \in K[X]$, $P \notin K$,

der davon erzeugte Unterkörper isomorph zum Körper der rationalen Funktionen in einer Variablen. Wir fragen uns, wie zu Polynomen $P, Q \in K[X]$, $P, Q \notin K$, der erzeugte Unterkörper $K(P,Q) \subseteq K(X)$ aussieht. Es wird sich herausstellen, dass hierbei stets eine algebraische Abhängigkeit zwischen diesen Polynomen besteht. Es gibt also zwar viele verschiedene, aber isomorphe, Unterkörper von $K(X)$, aber kein Unterkörper, der zum Quotientenkörper von $K[X,Y]$ isomorph wäre. Für solche Quotientenkörper führen wir eine eigene Bezeichnung ein.

Definition 28.1. Es sei K ein Körper. Den Quotientenkörper des Polynomringes $K[X_1, \ldots, X_n]$ nennt man *Körper der rationalen Funktionen in n Variablen*. Er wird mit $K(X_1, \ldots, X_n)$ bezeichnet.

Die Elemente dieses Körpers sind rationale Funktionen in mehreren Variablen, also Quotienten aus Polynomen in mehreren Variablen (wie schon bei Polynomen muss man aber bei einem endlichen Grundkörper vorsichtig sein bei der Identifizierung zwischen Elementen dieses Körpers und Funktionen auf gewissen Punktmengen).

Definition 28.2. Es sei R ein kommutativer Ring und A eine kommutative R-Algebra. Die Elemente $f_1, \ldots, f_n \in A$ heißen *algebraisch unabhängig* (über R), wenn für jedes vom Nullpolynom verschiedene Polynom $P \in R[X_1, \ldots, X_n]$ bei der Einsetzung

$$P(f_1, \ldots, f_n) \neq 0$$

gilt.

Ein einzelnes algebraisch unabhängiges Element ist einfach ein transzendentes Element. Von daher ist die Vorstellung, dass es sich bei einer algebraisch unabhängigen Familie um eine „transzendente Familie“ handelt, sinnvoll. Das Urbeispiel einer algebraisch unabhängigen Familie ist die Variablenfamilie in einem Polynomring $K[X_1, \ldots, X_n]$ bzw. im Körper der rationalen Funktionen $K(X_1, \ldots, X_n)$.

Lemma 28.3. *Es sei A eine kommutative R-Algebra über einem kommutativen Ring R und seien $f_1, \ldots, f_n \in A$ eine Elementfamilie. Dann sind folgende Aussagen äquivalent.*

(1) *Die Elemente $f_1, \ldots, f_n$ sind algebraisch unabhängig.*
(2) *Der Einsetzungshomomorphismus*

$$R[X_1, \ldots, X_n] \longrightarrow A,\ X_i \longmapsto f_i,$$

ist injektiv.
(3) *Der Einsetzungshomomorphismus*

$$R[X_1, \ldots, X_n] \longrightarrow R[f_1, \ldots, f_n],\ X_i \longmapsto f_i,$$

ist bijektiv.

Beweis. Siehe Aufgabe 28.6. □

Eine algebraisch unabhängige Familie ist also dadurch gekennzeichnet, das der Einsetzungshomomorphismus eine R-Algebraisomorphie

$$R[X_1, \ldots, X_n] \longrightarrow R[f_1, \ldots, f_n] \subseteq A$$

definiert. Wenn $R = K$ ein Körper ist, was wir zumeist annehmen werden, so führt dies auch zu einem Körperisomorphismus

$$K(X_1, \ldots, X_n) \longrightarrow K[X_1, \ldots, X_n].$$

28.2. **Transzendenzbasen.**

Definition 28.4. Es sei K ein Grundkörper und $K \subseteq L$ eine Körpererweiterung. Man sagt, dass $f_1, \ldots, f_n \in L$ eine *Transzendenzbasis* von L über K ist, wenn die $f_1, \ldots, f_n$ algebraisch unabhängig sind und $K(f_1, \ldots, f_n) \subseteq L$ eine algebraische Körpererweiterung ist.

Beispiel 28.5. Zum Polynomring $K[X_1, \ldots, X_n]$ über einem Körper K in n Variablen besitzt der Quotientenkörper

$$K(X_1, \ldots, X_n) = Q(K[X_1, \ldots, X_n]),$$

also der rationale Funktionenkörper in n Variablen, die Transzendenzbasis $X_1, \ldots, X_n$, da die Variablen algebraisch unabhängig sind.

Beispiel 28.6. Es sei K ein Körper und $F \in K(X_1, \ldots, X_n)[T]$ ein irreduzibles Polynom, die Koeffizienten des Polynoms sind also rationale Funktionen in den n Variablen $X_1, \ldots, X_n$. Nach Korollar 7.7 ist der Restklassenring

$$L := K(X_1, \ldots, X_n)[T]/(F)$$

ein Körper, und zwar eine endliche Körpererweiterung von $K(X_1, \ldots, X_n)$, deren Grad durch den Grad des Polynoms gegeben ist. Insbesondere bilden die Variablen $X_1, \ldots, X_n$ eine Transzendenzbasis von L.

Wenn eine algebraische Körpererweiterung

$$K(X_1, \ldots, X_n) \subset L$$

vorliegt, so kann es natürlich trotzdem sein, dass L die Form

$$L = K(Y_1, \ldots, Y_n)$$

besitzt, also isomorph zum Körper der rationalen Funktionen ist. Das einfachste Beispiel ergibt sich für $X = Y^2$.

Definition 28.7. Eine Körpererweiterung $K \subseteq L$ heißt *rein transzendent*, wenn es algebraisch unabhängige Elemente $f_1, \ldots, f_n \in L$ mit $L = K(f_1, \ldots, f_n)$ gibt.

Rein transzendent bedeutet also einfach, dass es eine K-Isomorphie zum Körper der rationalen Funktionen gibt. Es ist im Allgemeinen schwierig zu entscheiden, ob ein gegebener Körper rein transzendent ist. Der Quotientenkörper von $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ ist rein transzendent (über $\mathbb{C}$), der Quotientenkörper von $\mathbb{C}[X,Y]/(X^3+Y^3-1)$ ist hingegen nicht rein transzendent.

Wir wollen zeigen, dass die Anzahl der Elemente in einer Transzendenzbasis wohlbestimmt ist. Die Argumentation orientiert sich am Beweis des Satzes der linearen Algebra, dass die Anzahl der Elemente in einer Vektorraumbasis, also die Dimension des Vektorraumes, wohlbestimmt ist.

Lemma 28.8. *Es sei K ein Grundkörper und $K \subseteq L$ eine Körpererweiterung mit endlichen Transzendenzbasen $f_1,\ldots,f_m$ und $g_1,\ldots,g_n$. Dann gibt es zu jedem Element f_i der ersten Transzendenzbasis ein Element g_j der zweiten Transzendenzbasis derart, dass $f_1,\ldots,f_{i-1},g_j,f_{i+1},\ldots,f_m$ ebenfalls eine Transzendenzbasis ist.*

Beweis. Wir zeigen, dass man f_m durch eines der g_j ersetzen kann. Da die Körpererweiterung $K(f_1,\ldots,f_m) \subseteq L$ algebraisch ist, gibt es zu jedem g_j ein irreduzibles Polynom $P_j \in K(f_1,\ldots,f_m)[T]$ mit $P_j(g_j) = 0$. Wir multiplizieren mit dem Hauptnenner sämtlicher Koeffizienten der P_j und können dann annehmen, dass $P_j \in K[f_1,\ldots,f_m][T]$ gilt. Nehmen wir an, dass sämtliche P_j sogar zu $K[f_1,\ldots,f_{m-1}][T]$ gehören. Dann wäre die Körperkette

$$K(f_1,\ldots,f_{m-1}) \subseteq K(g_1,\ldots,g_n) \subseteq L$$

eine nach Aufgabe 10.4 algebraische Erweiterung und insbesondere wäre f_m algebraisch über $K(f_1,\ldots,f_{m-1})$ im Widerspruch zur Voraussetzung, dass die f_i algebraisch unabhängig sind. Es gibt also ein P_j mit $P_j \notin K[f_1,\ldots,f_{m-1}][T]$. Wir schreiben

$$P_j = \sum_{k=0}^{r} \alpha_k T^k$$

mit

$$\alpha_k = \sum_{\ell=0}^{s} \beta_{k,\ell} f_m^\ell$$

und $\beta_{k,\ell} \in K[f_1,\ldots,f_{m-1}]$. Dabei ist zumindest ein $\beta_{k,\ell} \neq 0$ für ein $\ell \geq 1$. Daher können wir die Gleichung $P_j(g_j) = 0$ als eine algebraische Gleichung für f_m über $K[f_1,\ldots,f_{m-1},g_j]$ lesen. Dies bedeutet, dass f_m algebraisch über $K(f_1,\ldots,f_{m-1},g_j)$ ist.

Wir behaupten, dass $f_1,\ldots,f_{m-1},g_j$ eine Transzendenzbasis von L über K ist, wobei wir gerade gezeigt haben, dass L darüber algebraisch ist. Es ist zu zeigen, dass diese Elemente algebraisch unabhängig sind. Wären sie algebraisch abhängig, so müsste g_j algebraisch über $K(f_1,\ldots,f_{m-1})$ sein. Doch dann wäre, wieder wegen der Transitivität von algebraisch, auch f_m algebraisch über $K(f_1,\ldots,f_{m-1})$ im Widerspruch zur Voraussetzung. □

Satz 28.9. *Es sei K ein Grundkörper und $K \subseteq L$ eine Körpererweiterung mit einer endlichen Transzendenzbasis. Dann besitzt jede Transzendenzbasis von L über K gleich viele Elemente.*

Beweis. Es sei m die minimale Zahl derart, dass es eine Transzendenzbasis mit m Elementen gibt. Es sei $f_1, \ldots, f_m$ eine Transzendenzbasis und $g_1, \ldots, g_n$ eine weitere Transzendenzbasis mit

$$n \geq m$$

Elementen. Wir wenden Lemma 28.8 sukzessive an und erhalten Transzendenzbasen

$$g_{j_1}, f_2, \ldots, f_m ,$$

$$g_{j_1}, g_{j_2}, f_3, \ldots, f_m ,$$

$$\ldots$$

$$g_{j_1}, g_{j_2}, g_{j_3}, \ldots, g_{j_{m-1}}, f_m ,$$

$$g_{j_1}, g_{j_2}, g_{j_3}, \ldots, g_{j_{m-1}}, g_{j_m} ,$$

wobei die g_{j_i} Elemente der zweiten Familie sind. Die letzte Familie ist eine Transzendenzbasis mit m Elementen (es kann keine Elementwiederholungen geben wegen der vorausgesetzen Minimalität von m). Bei $n > m$ würde sich ein Widerspruch ergeben, da eine echte Teilfamilie einer Transzendenzbasis keine Transzendenzbasis sein kann, also ist $n = m$. □

28.3. **Der Transzendenzgrad.**

Definition 28.10. Es sei K ein Grundkörper und $K \subseteq L$ eine Körpererweiterung mit einer endlichen Transzendenzbasis. Dann nennt man die Anzahl der Elemente in einer jeden Transzendenzbasis von L über K den *Transzendenzgrad* von L über K. Dafür schreibt man $\operatorname{trdeg}(L/K)$.

Nach Satz 28.9 ist dieser Transzendenzgrad wohldefiniert.

Korollar 28.11. *Es sei K ein Körper. und $K(X_1, \ldots, X_n) \subseteq L$ eine algebraische Körpererweiterung des Körpers der rationalen Funktionen in n Variablen. Dann ist der Transzendenzgrad von L über K gleich n. Insbesondere besitzt der Körper der rationalen Funktionen $K(X_1, \ldots, X_n)$ den Transzendenzgrad n.*

Beweis. Dies folgt direkt daraus, dass die Variablen $X_1, \ldots, X_n$ eine Transzendenzbasis von $K(X_1, \ldots, X_n)$ und von L bilden und dass man nach Satz 28.9 den Transzendenzgrad mit jeder Basis bestimmen kann. □

Korollar 28.12. *Es sei $K \subseteq L$ eine Körpererweiterung und seien $f_1, \ldots, f_n \in L$ Elemente. Dann sind folgende Aussagen äquivalent.*

(1) *Die Elemente $f_1, \ldots, f_n$ sind algebraisch unabhängig.*
(2) *Der Einsetzungshomomorphismus induziert eine K-Algebraisomorphie*
$$K(X_1, \ldots, X_n) \longrightarrow K(f_1, \ldots, f_n),\ X_i \longmapsto f_i,$$
(3) *Es gibt eine K-Algebraisomorphie*
$$K(X_1, \ldots, X_n) \longrightarrow K(f_1, \ldots, f_n).$$

Beweis. Die Äquivalenz von (1) und (2) folgt direkt aus Lemma 28.3. Von (2) nach (3) ist klar, sei also (3) erfüllt. Da eine Isomorphie vorliegt, und der Transzendenzgrad eine (wohldefinierte) invariante einer Körpererweiterung ist, besitzt der Körper $K(f_1, \ldots, f_n)$ den Transzendenzgrad n. Von diesem Körper ist $f_1, \ldots, f_n$ eine Transzendenzbasis und insbesondere algebraisch unabhängig. □

Korollar 28.13. *Es sei $K \subseteq L \subseteq M$ eine Kette von Körpererweiterungen. Dann ist*
$$\operatorname{trdeg}(M/K) = \operatorname{trdeg}(L/K) + \operatorname{trdeg}(M/L).$$

Beweis. Es sei $x_1, \ldots, x_n \in L$ eine Transzendenzbasis von L über K und $y_1, \ldots, y_m \in M$ eine Transzendenzbasis von M über L. Nach Aufgabe 28.13 ist $x_1, \ldots, x_n, y_1, \ldots, y_m$ algebraisch unabhängig über K. Nach Voraussetzung ist $K(x_1, \ldots, x_n) \subseteq L$ algebraisch. Daher ist auch
$$K(x_1, \ldots, x_n, y_1, \ldots, y_m) \subseteq L(y_1, \ldots, y_m)$$
algebraisch. Da auch $L(y_1, \ldots, y_m) \subseteq M$ algebraisch ist, folgt mit Aufgabe 10.4, dass $K(x_1, \ldots, x_n, y_1, \ldots, y_m) \subseteq M$ algebraisch ist. □

Korollar 28.14. *Es sei $K \subseteq L \subseteq M$ eine Kette von Körpererweiterungen. Dann ist*
$$\operatorname{trdeg}(L/K) \leq \operatorname{trdeg}(M/K).$$

Beweis. Dies folgt unmittelbar aus Korollar 28.13. □

28. Arbeitsblatt

28.1. **Übungsaufgaben.**

Aufgabe 28.1. Berechne in $\mathbb{Q}(X, Y)$
$$\frac{7X^2 - XY^3 + Y^4}{5X - \frac{1}{3}Y^4} \cdot \frac{1}{X^2Y^3} + \frac{3X^3 + X^2Y^2 - XY^2}{2 + 4X^3 - X^{257}} \cdot \frac{1}{X^2Y^3} - \frac{1}{7}X^3 + XY + Y^6 + 9$$

Aufgabe 28.2. Es sei $K \subseteq L$ eine algebraische Körpererweiterung. Zeige, dass dann auch die Körpererweiterung

$$K(X_1, \ldots, X_n) \subseteq L(X_1, \ldots, X_n)$$

der rationalen Funktionenkörper algebraisch ist.

Aufgabe 28.3. Zeige, dass eine Unterfamilie einer algebraisch unabhängigen Familie wieder algebraisch unabhängig ist.

Aufgabe 28.4. Es seien $e_1, \ldots, e_n$ positive natürliche Zahlen. Zeige, dass die Familie $X_1^{e_1}, \ldots, X_n^{e_n}$ im Polynomring $K[X, \ldots, X_n]$ über einem Körper K algebraisch unabhängig ist.

Aufgabe 28.5. Zeige, dass die Familie $X+Y, XY$ im Polynomring $K[X, Y]$ über einem Körper K algebraisch unabhängig ist.

Aufgabe 28.6. Es sei A eine kommutative R-Algebra über einem kommutativen Ring R und seien $f_1, \ldots, f_n \in A$ eine Elementfamilie. Zeige, dass folgende Aussagen äquivalent sind.

(1) Die Elemente $f_1, \ldots, f_n$ sind algebraisch unabhängig.
(2) Der Einsetzungshomomorphismus
$$R[X_1, \ldots, X_n] \longrightarrow A,\ X_i \longmapsto f_i,$$
ist injektiv.
(3) Der Einsetzungshomomorphismus
$$R[X_1, \ldots, X_n] \longrightarrow R[f_1, \ldots, f_n],\ X_i \longmapsto f_i,$$
ist bijektiv.

Aufgabe 28.7. Es sei $K[X_1, \ldots, X_n]$ der Polynomring über einem Körper K und seien $n+1$ Polynome $f_1, \ldots, f_{n+1} \in K[X_1, \ldots, X_n]$ gegeben. Zeige, dass diese algebraisch abhängig sind.

Aufgabe 28.8. Es seien $f_1, \ldots, f_n$ Elemente eines Körpers K und seien $f_1, \ldots, f_{n-1}$ algebraisch unabhängig. Zeige, dass die Familie $f_1, \ldots, f_n$ genau dann algebraisch unabhängig ist, wenn f_n transzendent über $K(f_1, \ldots, f_{n-1})$ ist.

Aufgabe 28.9. Besitzt die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$ eine endliche Transzendenzbasis?

Aufgabe 28.10. Es sei $z_1, \ldots, z_n \in \mathbb{R}$ eine Familie von reellen Zahlen. Zeige, dass es daraus eine algebraisch unabhängige Teilfamilie gibt.

Es ist übrigens unbekannt, ob die beiden transzendenten Zahlen e und π algebraisch unabhängig über $\mathbb{Q}$ sind.

Aufgabe 28.11. Es sei $K \subseteq L$ eine Körpererweiterung. Zeige, dass eine echte Unterfamilie einer Transzendenzbasis von L über K keine Transzendenzbasis ist.

Aufgabe 28.12. Es sei $K \subseteq L$ eine Körpererweiterung und $L \subseteq M$ eine algebraische Körpererweiterung. Es sei $f_1, \ldots, f_n \in L$ eine Transzendenzbasis von L über K. Zeige, dass diese Familie auch eine Transzendenzbasis von M über K ist.

Aufgabe 28.13.*

Es seien $K \subseteq L$ und $L \subseteq M$ Körpererweiterungen. Es sei $f_1, \ldots, f_r \in L$ eine algebraisch unabhängig über K und $g_1, \ldots, g_s \in M$ algebraisch unabhängig über L. Zeige, dass die Familie

$$f_1, \ldots, f_r, g_1, \ldots, g_s \in M$$

algebraisch unabhängig über K ist.

Aufgabe 28.14. Es sei K ein Körper der Charakteristik 0 und

$$f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$$

Polynome, die für den Körper der rationalen Funktionen $K(X_1, \ldots, X_n)$ eine Transzendenzbasis über K bilden. Es sei f_n ein Primpolynom. Zeige, dass die Restklassen der $f_1, \ldots, f_{n-1}$ im Quotientenkörper $Q(K[X_1, \ldots, X_n]/(f_n))$ eine Transzendenzbasis bilden.

Aufgabe 28.15. Bestimme den Transzendenzgrad des von den beiden trigonometrischen Funktionen Sinus und Kosinus über $\mathbb{R}$ erzeugten Körpers.

Aufgabe 28.16. Diskutiere Gemeinsamkeiten zwischen dem Konzept lineare Unabhängigkeit (Basis, Dimension) und dem Konzept algebraische Unabhängigkeit (Transzendenzbasis, Transzendenzgrad).

Aufgabe 28.17. Es sei K ein Körper und $L = K(X_1, \ldots, X_n)$ der rationale Funktionenkörper in n Variablen. Es sei $G \subseteq \mathrm{Gal}\,(L|K)$ eine endliche Untergruppe der Galoisgruppe. Zeige, dass der Transzendenzgrad des Fixkörpers L^G über K gleich n ist.

Aufgabe 28.18. Wir betrachten den Funktionenkörper in zwei Variablen $L = K(X,Y)$ über einem Körper K der Charakteristik 0. Die Gruppe $K^\times$ ist eine Untergruppe der Galoisgruppe $\mathrm{Gal}\,(L|K)$, indem man $s \neq 0$ als den durch $X \mapsto sX$, $Y \mapsto sY$ festgelegten Automorphismus auffasst. Bestimme den Fixkörper $K(X,Y)^{K^\times}$ sowie dessen Transzendenzgrad über K.

Aufgabe 28.19. Wir betrachten den Funktionenkörper $L = K(X_1,\ldots,X_n)$ über einem Körper K. Wie betrachten auf der Menge $\mathcal{Z}$ aller Zwischenkörper die Relation, die durch

$$M_1 \sim M_2,$$

falls es einen Zwischenkörper M derart gibt, dass $M_1 \subseteq M$ und $M_2 \subseteq M$ endliche Körpererweiterungen sind, gegeben ist. Zeige, dass es sich dabei um eine Äquivalenzrelation handelt.

Aufgabe 28.20. Man gebe ein Beispiel für Zwischenkörper

$$L, M \subseteq K(X,Y),$$

die den gleichen Transzendenzgrad haben, die aber nicht zueinander äquivalent im Sinne von Aufgabe 28.19 sind.

28.2. **Aufgaben zum Abgeben.**

Aufgabe 28.21. (4 Punkte)

Sei $n \in \mathbb{N}_+$. Betrachte auf dem rationalen Funktionenkörper $\mathbb{C}(X)$ die Gruppe der $\mathbb{C}$-Körperautomorphismen, die durch $X \mapsto \zeta_n X$ erzeugt wird, wobei ζ_n eine primitive n-te Einheitswurzel bezeichnet. Bestimme den Fixkörper $\mathbb{C}(X)^{\mathbb{Z}/(n)}$.

Aufgabe 28.22. (4 Punkte)

Zeige, dass die Familie $X+Y+Z, XY+XZ+YZ, XYZ$ im Polynomring $K[X,Y,Z]$ über einem Körper K algebraisch unabhängig ist.

Aufgabe 28.23. (8 (2+2+4) Punkte)

Es sei K ein Körper und $L = K(X_1,\ldots,X_n)$ der rationale Funktionenkörper in n Variablen. Wir knüpfen an Beispiel 10.12 an.

(1) Zeige, dass es einen natürlichen injektiven Gruppenhomomorphismus

$$\mathrm{GL}_n(K) \longrightarrow \mathrm{Gal}\,(L|K)$$

(2) Zeige, dass dieser nicht surjektiv ist.

(3) Es sei nun zusätzlich vorausgesetzt, dass der Körper K die Charakteristik 0 habe. Zeige für den Fixkörper die Gleichheit

$$L^{\mathrm{GL}_n(K)} = K.$$

Aufgabe 28.24. (1 Punkt)

Es sei $L = K(X_1, \ldots, X_n)$ der rationale Funktionenkörper über einem Körper K. Wie betrachten auf der Menge $\mathcal{Z}$ aller Zwischenkörper die Äquivalenzrelation aus Aufgabe 28.19. Zeige, dass der Transzendenzgrad auf den Äquivalenzklassen wohldefiniert ist.

Aufgabe 28.25. (2 Punkte)

Es sei $L = K(X_1, \ldots, X_n)$ der rationale Funktionenkörper über einem Körper K. Es seien Zwischenkörper

$$K \subseteq M_1, M_2 \subseteq L$$

mit der Eigenschaft gegeben, dass die Körpererweiterungen

$$M_1 \cap M_2 \subseteq M_1, M_2$$

endlich seien. Zeige, dass es dann auch einen Zwischenkörper N derart gibt, dass $M_1, M_2 \subseteq N$ endlich sind.

Abbildungsverzeichnis

 245