Algebra und Zahlentheorie

Ulrich Bunke*

14. Juli 2004

Inhaltsverzeichnis

*Göttingen, bunke@uni-math.gwdg.de

1 Gruppen und Symmetrien

1.1 Strukturen und strukturerhaltende Abbildungen

1.1.1 Motivation

Wir wollen Gruppen als Mengen von Tranformationen beschreiben. Die natürlichen Tranformationen zwischen unstrukturierten Mengen sind beliebige Abbildungen. Interessante Teilmengen von Abbildung werden dadurch ausgezeichnet, daß sie mit zusätzlichen Strukturen auf den Mengen verträglich sein sollen. Diese zusätzlichen Strukturen können von recht unterschiedlicher Bauart sein. Entsprechend unterschiedlich sehen im Detail auch die Bedingungen an die Transformationen aus. In den folgenden Abschnitten betrachten wir einige Beispiele.

1.1.2 Funktionen

Wir fixieren eine Menge F. In diesem Abschnitt betrachten wir die Strukturen, welche durch F-wertige Abbildungen gegeben werden.

Definition 1.1. *Eine durch F gefärbte Menge ist ein Paar (X, f) aus einer Menge X und einer Abbildung $f : X \to F$.*

Seien (X, f) und (Y, g) zwei F-gefärbte Mengen.

Definition 1.2. *Eine Abbilddung $\phi : X \to Y$ ist färbungserhaltend, wenn $g \circ \phi = f$ gilt.*

Aufgabe 1.1. *Sei $A := \{a,b,c,d,e\}$ und $B := \{x,y,z\}$. Wir betrachten die Färbungen*

a	b	c	d
1	1	2	2

x	y	z
1	2	2

durch $R := \{1,2\}$. Bestimmen Sie alle färbunserhaltenden Abbildungen $A \to B$.

1.1.3 Relationen

Sei $T := \{falsch, wahr\}$.

Definition 1.3. *Eine Relation R auf einer Menge X ist eine Färbung von $X \times X$ durch T.*

Natürlich kann eine Relation auch wie üblich durch die Angabe der Teilmenge $\{(x,y) \in X \times X | R(x,y) = wahr\}$ beschrieben werden.

Seien (X,R) und (Y,S) Mengen mit ausgezeichneten Relationen.

Definition 1.4. *Eine Abbildung $\phi : X \to Y$ ist mit den Relationen verträglich, falls $R = S \circ (\phi \times \phi)$ gilt.*

Aufgabe 1.2. *Wir betrachten die Teilmenge $A := \{1,2,3,4,5,6,7\} \subset \mathbb{N}$ mit den induzierten Relationen $>$ und $\geq$. Beschreiben Sie in beiden Fällen alle relationserhaltenden Abbildungen $A \to A$*

1.1.4 Graphen

Für eine Menge V bezeichne $P^2(V)$ die Menge der ungeordneten Paare von Elementen aus V.

Ist zu Beispiel $A = \{a,b\}$, dann ist $P^2(A) = \{(a,a),(b,b),(a,b)\}$.

Ist $f : V \to W$ eine Abbildung, so erhalten wir eine induzierte Abbildung $P^2(F) : P^2(V) \to P^2(W)$ durch $P^2(f)(a,b) := (f(a), f(b))$.

Definition 1.5. *Ein Graph ist Tripel (V,E,r), wobei V die Menge der Punkte, E die Menge der Seiten, und $r : E \to P^2(V)$ die Endpunkte der Seiten festlegt.*

Seien (V,E,r) und (W,F,s) zwei Graphen.

Definition 1.6. *Eine Morphismus $\phi : (V,E,r) \to (W,F,s)$ von Graphen ist durch zwei Abbildungen $\phi : V \to W$, $\psi : E \to F$ mit $P^2(\phi) \circ r = s \circ \psi$ gegeben*

Aufgabe 1.3. *Sei $E := \mathbb{Z}$, $V := \mathbb{Z}$, und $e : E \to P^2(V)$ durch $r(n) = \{n, n+2\}$ gegeben. Bestimmen Sie alle Morphismen $(V,E,r) \to (V,E,r)$.*

1.1.5 Abstände

Ein Abstand d auf einer Menge X wird durch eine Abbildung $d : X \times X \to [0,\infty]$ gegeben, welche die Abstandsaxiome erfüllt.

Definition 1.7. *Ein metrischer Raum (X,d) ist eine Menge X mit einem ausgezeichneten Abstand d.*

Definition 1.8. *Seien (X,d_X) und (Y,d_Y) metrische Räume. Eine Abbildung $\phi : X \to Y$ ist eine Isometrie, falls $d_Y \circ (\phi \times \phi) = d_X$ gilt.*

Aufgabe 1.4. *Seien $X = \{(x,y) \in \mathbb{R}^2 | |x| + |y| \leq 1\}$ und $Y := \mathbb{R}^2$. mit dem euklidischen Abstand. Bestimmen Sie alle isometrischen Abbildungen $X \to Y$.*

1.1.6 Binäre Operationen

Definition 1.9. *Eine Verknüpfung auf einer Menge M ist eine Abbildung $m : M \times M \to M$.*

Definition 1.10. *Eine Morphismus $\phi : (M,m) \to (N,n)$ von Mengen mit Verknüpfung ist eine Abbildung $\phi : M \to N$ derart, daß $n \circ (\phi \times \phi) = \phi \circ m$ gilt.*

Aufgabe 1.5. *Wir betrachten die Menge $\mathbb{N}$ mit der Verknüpfung*

$$m(x,y) := \begin{pmatrix} x+y & x+y \leq 10 \\ 10 & x+y > 10 \end{pmatrix} .$$

Bestimmen Sie alle verknüfungserhaltenden Abbildungen.

1.1.7 Lineare Strukturen

Sei K ein Körper. Ein Vektorraum über K ist ein Tripel $(V,+,\bullet)$, wobei $+ : V \times V \to V$ die Vektoraddition und $\bullet : K \times V \to V$ die skalare Multiplikation ist. Diese Operationen erfüllen die Vektorraumaxiome.

Definition 1.11. *Eine lineare Abbildung zwischen Vektorräumen $(V,+_V,\bullet_V)$ und $(W,+_W,\bullet_W)$ ist eine Abbildung $\phi : V \to W$ derart, daß $\phi \circ +_V = +_W \circ (\phi \times \phi)$ und $\phi \circ \bullet_V = \bullet_W \circ (\mathtt{id}_K \times \phi)$ gilt.*

Aufgabe 1.6. *Sei $K = F_3$ der Körper mit drei Elementen. Wieviele Elemente hat die Menge der linearen Abbildungen $F_3^2 \to F_3^3$.*

1.1.8 Begriff der Kategorie

Wir fassen die obigen Beispiele in dem Begriff der Kategorie zusammen. Eine Kategorie $\mathcal{C}$ beinhaltet die folgenden Strukturen:

1. die (Klasse der) Objekte $\mathtt{ob}(\mathcal{C})$
2. für je zwei Objekte $A, B \in \mathtt{ob}(\mathcal{C})$ eine Menge von Morphismen $\mathtt{Hom}_{\mathcal{C}}(A,B)$,
3. für jedes Objekt einen Identitätsmorphismus $\mathtt{id}_A \in \mathtt{Hom}_{\mathcal{C}}(A,A)$
4. für je drei Objekte eine Komposition

$$\mathtt{Hom}_{\mathcal{C}}(B,C) \circ \mathtt{Hom}_{\mathcal{C}}(A,B) \to \mathtt{Hom}_{\mathcal{C}}(A,C) \ .$$

Dabei gelten folgende Eigenschaften.

1. Die Komposition ist assoziativ, d.h. es gilt $(f \circ g) \circ h = f \circ (g \circ h)$ für komponierbare Morphismen.
2. Die Identitätsmorphismen erfüllen $\mathtt{id}_B \circ f = f$ und $f \circ \mathtt{id}_A = f$ für $f \in \mathtt{Hom}_{\mathcal{C}}(A,B)$.

In allen Beispielen oben haben wir Kategorien beschrieben.

1.2 Gruppen von Automorphismen

1.2.1 Invertierbare Morphismen

Wir betrachten eine Kategorie $\mathcal{C}$ und ein Objekt $A \in \mathtt{ob}(A)$.

Definition 1.12. *Ein $f \in \mathtt{Hom}_{\mathcal{C}}(A,A)$ heißt Automorphismus, falls es Morphismen $g_l, g_r \in \mathtt{Hom}_{\mathcal{C}}(A,A)$ (Links- und Rechtsinverses) mit $g_l \circ f = f \circ g_r = \mathtt{id}_A$ gibt.*

Lemma 1.13. *Sei f ein Automorphismus. Dann gilt:*

1. $g_l = g_r$.

2. *Das Rechtsinverse g_r eines Automorphismus f ist eindeutig bestimmt. Wir schreiben auch $f^{-1} := g_r$.*

3. *Die Komposition von Automorphismen ist ein Automorphismus.*

4. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

5. $\mathtt{id}_A$ *ist ein Automorphismus.*

Definition 1.14. *Die Gruppe der Automorphismen von A ist die Teilmenge*

$$\mathtt{Aut}_{\mathcal{C}}(A) := \{f \in \mathtt{Hom}_{\mathcal{C}}(A,A) | f \textit{ Automorphismus}\} \subset \mathtt{Hom}_{\mathcal{C}}(A,A)$$

.

1.2.2 Permutationen - die Gruppen S_n

Wir betrachten die Kategorie der Mengen und Abbildungen $\mathtt{sets}$. Sei $A \in \mathtt{ob}(\mathtt{sets})$. Dann besteht $\mathtt{Aut}_{\mathtt{sets}}(A)$ aus den Bijektionen $A \to A$. Wir schreiben oft $S(A) := \mathtt{Aut}_{\mathtt{sets}}(A)$ für die symmetrische Gruppe von A. Ist $A = \{1,2,\ldots,n\} \subset \mathbb{N}$, so schreiben wir $S_n := S(A)$. Weiterhin schreiben wir $1 := \mathtt{id}_{\{1,\ldots,n\}}$.

Sei $A = \{a,b,c,d\}$. Dann kann ein Element $f \in S(A)$ durch eine Wertetabelle dargestellt werden.

x	a	b	c	d
$f(x)$	b	c	a	d

.

Eine kürzere Schreibweise für dieses Element ist die Zyklendarstellung

$$(abc)\ .$$

Hier ein weiteres Beispiel $h \in S_9$.

x	1	2	3	4	5	6	7	8	9
$h(x)$	2	4	6	5	1	7	3	8	9

.

In Zyklen ist dieses Element das Produkt

$$(1,2,4,5) \circ (3,6,7)\ .$$

Wir betrachten $(1,2),(2,3) \in S_3$. Dann gilt

$$(1,2) \circ (2,3) = (1,2,3), \quad (2,3) \circ (1,2) = (1,3,2)\ .$$

Das Ergebnis der Komposition kann also durchaus von der Reihenfolge abhängen.

Aufgabe 1.7. *Wir betrachten S_9. Finden Sie Darstellungen als Produkt von Zyklen von*

$$f := \begin{array}{|c|c|c|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 1 & 3 & 2 & 4 & 6 & 9 & 7 & 8 & 5 \\ \hline \end{array}, \quad g := \begin{array}{|c|c|c|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 2 & 3 & 4 & 7 & 6 & 1 & 8 & 9 & 5 \\ \hline \end{array}.$$

Bestimmen Sie das Produkt $f \circ g$ und geben Sie eine möglichst kurze Darstellung als Produkt von Zyklen an.

Bestimmen Sie das Inverse von $h := (1,2,4) \circ (5,6,8)$. Geben Sie die Wertetabelle von $(1,3,4,6) \circ (6,5,3)$ an.

Aufgabe 1.8. *Sei A endlich. Bestimmen Sie die Anzahl der Elemente von $S(A)$. Bestimmen Sie die Zahl*

$$\mathtt{max}_{f \in S(A)} \mathtt{min} \{ m \in \mathbb{N} | f^m = 1 \} .$$

Für welche $n \in N$ gibt es Elemente $1 \neq x \in S(A)$ mit $x^n = 1$.

1.2.3 Isometrien - die Gruppen D_n

Wir betrachten die Kategorie met der metrischen Räume und Isometrien.

Lemma 1.15. *Ist $A \in \mathtt{ob}(\mathtt{met})$ eine endliche Menge, so gilt $\mathtt{Hom}_{\mathtt{met}}(A,A) = \mathtt{Aut}_{\mathtt{met}}(A,A)$.*

Das ist jedoch nicht mehr richtig für unendliche Mengen. Als Beispiel betrachten wir $\mathbb{N}$ mit dem Abstand $d(n,m) := |n-m|$. Dann ist $f : \mathbb{N} \to \mathbb{N}$, $f(n) = n+1$, eine Isometrie, aber kein Automorphismus.

Wir betrachten die Teilmenge $\mu_n \subset \mathbb{C}$,

$$\mu_n := \{ \exp(2\pi i \frac{m}{n}) | m = 0, 1, \ldots, n-1 \}$$

der n-ten Einheitswurzeln mit dem induzierten euklidischen Abstand.

Definition 1.16. *Die Diedergruppe D_n wird durch $D_n := \mathtt{Aut}_{\mathtt{met}}(\mu_n)$ definiert.*

Sei $r = \exp(2\pi i \frac{1}{n})$. Die komplexe Multiplikation $\mathbb{C} \to \mathbb{C}$, $z \mapsto rz$, ist isometrisch auf $\mathbb{C}$ und erhält μ_n. Wir erhalten Elemente $1, r, \ldots r^{n-1} \in D_n$. Die komplexe Konjugation $\mathbb{C} \to \mathbb{C}$, $z \mapsto s(z) := \bar{z}$, ist isometrisch und erhält μ_n. Wir erhalten ein Element $s \in D_n$.

Lemma 1.17. *Die Liste der Elemente von D_n ist*

$$\{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\} .$$

Aufgabe 1.9. *Bestimmen Sie die Multiplikationstabelle von D_5. Bestimmen Sie für jedes Element von D_5 die Menge der Fixpunkte in μ_n.*

1.2.4 Die Gruppen C_n

Wir betrachten die Menge $X_n := \{1, 2, \ldots, n\} \subset \mathbb{N}$. Auf dieser Menge führen wir die Relation der zyklischen Nachfolge ein. Sie wird durch die Teilmenge $\{(1,2), (2,3), \ldots, (n-1, n), (n, 1)\} \subset X_n \times X_n$ gegeben. Wir betrachten X_n als ein Objekt der Kategorie der Mengen mit ausgezeichneten Relationen $\mathtt{set} + \mathtt{rel}$.

Definition 1.18. *Wir definieren die zyklische Gruppe C_n durch*

$$C_n := \mathtt{Aut}_{\mathtt{set}+\mathtt{rel}}(X_n) .$$

Sei $r \in S(X_n)$ durch den Zyklus $r = (1, \ldots, n)$ gegeben. Dann gilt $r \in C_n$.

Lemma 1.19. *Die Liste der Elemente von C_n ist $\{1, r, \ldots, r^{n-1}\}$.*

Aufgabe 1.10. *Für welche $n \in \mathbb{N}$ existiert ein $1 \neq x \in C_{30}$ mit $x^n = 1$.*

Beantworten Sie diese Frage für alle zyklischen Gruppen C_m.

1.2.5 Lineare Isomorphismen - die Gruppen $GL(n, K)$

Sei K ein Körper. Wir betrachten die Kategorie $K - \mathtt{vect}$ der Vektorräume über K.

Definition 1.20. *Für $V \in K - \mathtt{vect}$ definieren wir*

$$\mathtt{GL}(V) := \mathtt{Aut}_{K-\mathtt{vect}}(V) .$$

Insbesondere setzen wir

$$\mathtt{GL}(n, K) := \mathtt{GL}(K^n) .$$

Die Elemente von $GL(n, K)$ können als Matrizen dargestellt werden. Die Verknüpfung ist dann gerade die Matrixmultiplikation. Als Beispiel betrachten wir den Körper $F_2 = \{0, 1\}$ und die Gruppe $GL(2, F_2)$.

Lemma 1.21. *Die Liste der Elemente von* $GL(2,F_2)$ *ist*

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

Aufgabe 1.11. *Sei* F_3 *der Körper mit drei Elementen. Bestimmen Sie die Liste der Elemente von* $GL(2,F_3)$.

1.3 Abstrakte Gruppen

1.3.1 Gruppenaxiome

Definition 1.22. *Ein Monoid* $(M,\circ,1)$ *ist eine Menge mit Verknüpfung* $(M,\circ)$ *mit einem ausgezeichneten* 1*-Element, so daß*

1. $\circ$ *associativ ist, d.h.* $x\circ(y\circ z)=(x\circ y)\circ z$ *gilt, und*
2. $1\circ x=x\circ 1=x$ *gilt.*

Definition 1.23. *Eine Gruppe ist ein Monoid* $(G,\circ,1)$*, in welchem jedes Element invertierbar ist, d.h. zu jedem* $x\in M$ *Elemente* $y_l,y_r\in M$ *mit* $x\circ y_r=y_l\circ x=1$ *existieren.*

Sei G eine Gruppe.

Lemma 1.24. *In einer Gruppe besitzt jedes Element ein eindeutig bestimmtes Linksinverses. Dieses ist dann auch ein Rechtsinverses.*

Es gibt also eine Bijektion $(\dots)^{-1}:G\to G$ welche jedem Element sein Inverses zuordnet.

Ist $A\in\mathcal{C}$ ein Objekt einer Kategorie, dann ist $\mathtt{Aut}_{\mathcal{C}}(A)$ eine Gruppe.

Ist G eine Gruppe und $1\in U\subset G$ eine unter der Verknüpfung und der Bildung des Inversen abgeschlossene Teilmenge, so ist U selbst eine Gruppe. Wir sagen, daß U eine Untergruppe von G ist.

Eine (abstrakte) Gruppe ist nicht in natürlicher Weise Gruppe von Automorphismen eines Objektes einer Kategorie. Unter einer Darstellung versteht man eine Realisierung

einer Gruppe als Untergruppe (durch einen Isomorphismus) von Automorphismen eines Objektes einer Kategorie. Je nach Kategorie spricht man dann von Permutationsdarstellungen (`sets`) oder linearen Darstellungen ($K-$`vect`). Wir werden sehen, daß jede Gruppe solche Darstellungen besitzt. (Zu beachten ist, daß wir später das Wort Darstellung in einer anderen Bedeutung verwenden werden.)

1.3.2 Die Kategorie der Gruppen

Gruppen sind spezielle Mengen mit Verknüpfung. Mit `groups` bezeichnen wir die Kategorie der Gruppen und Homomorphismen.

In `groups` haben wir beispielsweise einen injektiven Homomorphismus $C_n \to D_n$, welcher dem Element $r^k \in C_n$ das Element $r^k \in D_n$ zuordnet.

Aufgabe 1.12. *Sei G eine Gruppe. Bestimme alle Homomorphismen $\mathbb{Z} \to G$.*

Aufgabe 1.13. *Bestimme alle Homomorphismen $\mathbb{Q} \to \mathbb{Z}$.*

Lemma 1.25. *Sei $f : H \to G$ ein Homomorphismus von Gruppen. Dann gilt:*

1. $\mathtt{ker}(f) := \{h \in H | f(h) = 1\}$ *ist eine Untergruppe von H.*
2. $\mathtt{im}(f) := f(H)$ *ist eine Untergruppe von G.*

Aufgabe 1.14. *Zeige, daß $GL(2, F_2)$ zu S_3 isomorph ist.*

Aufgabe 1.15. *Zeige, daß*

$$U = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3), 1\}$$

eine Untergruppe von S_4 ist.

Aufgabe 1.16. *Bestimmen Sie alle Untergruppen von C_{12}.*

Sei G eine Gruppe und $h \in G$.

Lemma 1.26. *Dann definiert die Abbildung $\alpha_h : G \to G$, $g \mapsto \alpha_h(g) := g^h :=:= hgh^{-1}$ einen Automorphismus $\alpha_g \in \mathtt{Aut}_{groups}(G)$.*

Lemma 1.27. *Ist $f \in Hom_{groups}(G,H)$ und $U \subset G$ eine Untergruppe, dann ist $f(U) = \{f(u) | u \in U\}$ eine Untergruppe von H.*

1.3.3 Generatoren und Relationen

Sei G eine Gruppe und $S \subset G$ eine Teilmenge.

Definition 1.28. *Wir sagen, daß S die Gruppe G erzeugt, wenn man jedes Element aus G durch eine endliche Verknüpfung von Elementen aus S erhalten kann.*

Aufgabe 1.17. *Verifizieren Sie: Die Menge* $S := \{(2,3),(3,4)\}$ *erzeugt die Gruppe* $\mathbb{Z}^2$*, nicht aber* $T := \{(5,3),(1,1)\}$*. Bestimmen Sie die Gruppe, die von T erzeugt wird.*

Aufgabe 1.18. *Sei A eine endliche Menge. Zeigen Sie, daß die Gruppe* $S(A)$ *die Zyklen der Länge zwei erzeugt wird.*

Aufgabe 1.19. *Berechnen Sie Größe minimaler Erzeugendensysteme folgender Gruppen*

1. S_n
2. D_n
3. $GL(2,F_2)$
4. $GL(2,F_3)$

Definition 1.29. *Sei S eine Menge. Die Elemente von*

$$W_n(S) := \underbrace{S \times \cdots \times S}_{n\times}$$

werden auch Worte der Länge n im Alphabet S genannt. Wir verabreden, daß $W_0 := \{1\}$ *gilt und setzen* $W(S) := \bigcup_{n\geq 0} W_n(S)$.

Sei $S = \{a := (1,2)\circ(3,4), b := (2,3), c := (1,2,3)\} \subset S_4$. Dann sind (a,a,b) und (a,b,c,a) Worte der Länge 3 und 4 im Alphabet S.

Ist $S \subset G$ Teilmenge eine Gruppe (oder allgemeiner Menge mit Verknüpfung), so gibt es eine Abbildung

$$m : W(S) \to G, (a_1,\ldots,a_n) \mapsto a_1 \circ \cdots \circ a_n \ .$$

Diese Abbildung ist genau dann surjektiv, wenn S die Gruppe G erzeugt.

Definition 1.30. *Die Menge der Relationen ist die Teilmenge*

$$R(S) := \{w \in W(S) | r(w) = e\} .$$

Aufgabe 1.20. *Bestimmen Sie alle Relationen der Länge höchstens vier für* $S := \{(1,2),(2,3)\} \subset \mathbb{Z}^2$.

Aufgabe 1.21. *Bestimmen Sie alle Relationen der Länge höchstens vier in* $S = \{(1,2),(1,3,4)\} \subset S_4$.

1.3.4 Freie Gruppen

Sei T eine Menge. Wir betrachten dann die Menge $\hat{T} = T \times \{1,-1\}$. Wir schreiben $t := (t,1)$ und $t^{-1} := (t,-1)$.

Definition 1.31. *Ein Wort* $w = (t_1^{\varepsilon_1}, \ldots, t_n^{\varepsilon_n})$, $\varepsilon_i \in \{1,-1\}$, *heißt reduziert, wenn aus* $t_i = t_{i+1}$ *die Relation* $\varepsilon_i = \varepsilon_{i+1}$ *folgt.*

Sei $T = \{a,b,c\}$. Dann sind (a,b) und (a,b,a^{-1},c) reduziert, nicht aber (a,b^{-1},b,a). Ist T eine Teilmenge einer Gruppe, so ist klar, daß $m(a,b^{-1},b,a) = m(a,a)$ gilt.

Definition 1.32. *Wir definieren die Reduktionsabbidlung*

$$\mathtt{Red} : W(\hat{T}) \to W(\hat{T})$$

durch folgende Vorschrift. Sei $w = (t_1^{\varepsilon_1}, \ldots, t_n^{\varepsilon_n}) \in W(\hat{T})$. *Ist w reduziert, dann setzen wir* $\mathtt{Red}(w) := w$. *Ist w nicht reduziert, dann sei* $j := \mathtt{min}\{i | t_i = t_{i+1} \text{ und } \varepsilon_i \neq \varepsilon_{i+1}\}$ *und*

$$\mathtt{Red}(w) := (t_1^{\varepsilon_1}, t_{j-1}^{\varepsilon_{j-1}}, t_{j+2}^{\varepsilon_{j+2}} \ldots, t_n^{\varepsilon_n}) .$$

Lemma 1.33. *Für jedes* $w \in W(T)$ *ist* $\mathtt{Red}^n(w)$ *für genügend große n reduziert.*

Sei $w = (a,b^{-1},b,a^{-1},a,b,a,a^{-1},b^{-1})$. Dann gilt

n	$\mathtt{Red}(w)$
0	$(a,b^{-1},b,a^{-1},a,b,a,a^{-1},b^{-1})$
1	$(a,a^{-1},a,b,a,a^{-1},b^{-1})$
2	(a,b,a,a^{-1},b^{-1})
3	(a,b,b^{-1})
4	(a)
5	(a)
$\vdots$	$\vdots$

.

Sei $W^{red}(\hat{T}) \subset W(\hat{T})$ die Menge der reduzierten Worte in T.

Definition 1.34. *Wir definieren das Monoid $F(T) := W(\hat{T})^{red}$ mit der Verknüpfung*

$$(t_1^{\varepsilon_1}, \ldots, t_n^{\varepsilon_n}) \circ (s_1^{\delta_1}, \ldots, s_m^{\delta_m}) = (t_1^{\varepsilon_1}, \ldots, t_n^{\varepsilon_n}, s_1^{\delta_1}, \ldots, s_m^{\varepsilon_m})^{red} .$$

Lemma 1.35. *Das Monoid $(F(T), \circ)$ ist eine Gruppe.*

Definition 1.36. *$F(T)$ heißt die freie durch T erzeugte Gruppe. Ist $T_n = \{1, \ldots, n\} \subset \mathbb{N}$, so schreibt man auch $F_n := F(T_n)$ für die freie Gruppe in n Erzeugenden.*

Lemma 1.37. *Ist G eine Gruppe und $T \subset G$, so induziert $m : F(T) \to G$ einen Gruppenhomomorphismus.*

Die Menge T erzeugt G genau dann, wenn dieser Homomorphismus surjektiv ist.

Definition 1.38. *Eine Gruppe G heißt frei, wenn es eine Teilmenge $T \subset G$ gibt, für welche $m : F(T) \to G$ ein Isomorphismus ist.*

Sei T eine Menge. Wir konstruieren einen Graphen G wie folgt. Die Menge der Punkte des Graphen sei $V := F(T)$. Wir setzen weiter

$$E := \{(x, y) \in V \times V | x^{-1} \circ y \in T\} .$$

Die Abbildung $r : E \to P^2(V)$ ist durch $r(x, y) = \{x, y\}$ gegeben. Sei $\mathtt{Aut}(G)$ die Gruppe der Automorphismen des Graphen G.

Aufgabe 1.22. *Finde eine Einbettung $F(T) \to \mathtt{Aut}(G)$.*

1.3.5 Funktoren

Die Konstruktion F der freien Gruppe ordnet jeder Menge eine Gruppe zu. Ist $\phi : T \to S$ eine Abbildung, dann erhalten wir eine induzierte Abbildung $\hat{\phi} : \hat{T} \to \hat{S}$ und schließlich einen Homomorphismus $F(\phi) : F(T) \to F(S)$, indem wir $\hat{\phi}$ auf die Einträge der Worte anwenden. Es gilt dabei $F(\phi) \circ F(\psi) = F(\phi \circ \psi)$. Dies ist ein Beispiel eines Funktors

$$F : \mathtt{sets} \to \mathtt{groups} .$$

Definition 1.39. *Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ besteht aus folgenden Strukturen:*

1. *eine Zuordnung* $F : \mathtt{ob}(\mathcal{C}) \to \mathtt{ob}(\mathcal{D})$,

2. *für je zwei Objekte* $A, B \in \mathtt{ob}(\mathcal{C})$ *eine Abbildung* $F : \mathtt{Hom}_{\mathcal{C}}(A,B) \to \mathtt{Hom}_{\mathcal{D}}(F(A),F(B))$.

Diese Abbildung soll dabei die Verknüpfung erhalten.

Aufgabe 1.23. *Zeige, daß ein Funktor Gruppenhomomorphismen* $F : \mathtt{Aut}_{\mathcal{C}}(A) \to \mathtt{Aut}_{\mathcal{D}}(F(A))$ *induziert.*

Die freie Gruppe $F(T)$ hat folgende universelle Eigenschaft.

Lemma 1.40. *Ist G eine Gruppe und* $f : T \to G$ *eine Abbildung. Dann gibt es genau eine Fortsetzung von* f *zu einem Gruppenhomomorphismus* $F(f) : F(T) \to G$.

Sei $\mathcal{F} : \mathtt{groups} \to \mathtt{sets}$ der Funktor, welcher die Gruppenstruktur vergißt. Dann gilt auf natürliche Weise

$$\mathtt{Hom}_{\mathtt{groups}}(F(T),G) \cong \mathtt{Hom}_{\mathtt{sets}}(T,\mathcal{F}(G)) \ .$$

Man sagt, daß der Funktor F zu $\mathcal{F}$ linksadjungiert ist. In der Tat kann man F so definieren (bis auf Isomorphie).

Aufgabe 1.24. *Eine Gruppe, welche gleichzeitig abelsch und frei ist, ist isomorph zu* $\mathbb{Z}$.

1.3.6 Darstellung als Permutationsgruppe

Jede Gruppe kann als Untergruppe einer Permutationsgruppe dargestellt werden. Sei G eine Gruppe. Dann indiziert jedes Element $g \in G$ durch Linksmultiplikation eine Bijektion $\phi(g) : G \to G$.

Lemma 1.41. *Die Abbildung* $\phi : G \to \mathtt{Aut}_{\mathtt{sets}}(G)$ *ist ein injektiver Gruppenhomomorphismus.*

Insbesondere kann jede endliche Gruppe injektiv in eine Permutationsgruppe eingebettet werden.

1.3.7 Lineare Darstellung

Wir fixieren einen Körper K. Sei X eine Menge. Dann ist $K(X)$ der von X erzeugte Vektorraum. Der Vektorraum $X(k)$ kommt mit einer Einbettung $X \hookrightarrow K(X)$ als Basis. Jedes Element in $K(X)$ hat eine eindeutige Darstellung $\sum_{x\in X} \lambda(x)x$, wobei die Abbildung $\lambda : X \to K$ für fast alle Punkte den Wert Null annimmt.

Ist $K(f) : X \to Y$ eine Abbildung, so erhalten wir eine eindeutige lineare Fortsetzung $K(f) : K(X) \to K(Y)$ durch $K(f)(\sum_{x\in X} \lambda(x)) = \sum_{x\in X} \lambda(x) f(x)$.

Durch K wird ein Funktor $K : \mathtt{sets} \to K - \mathtt{vect}$ beschrieben. In der Tat gilt für jeden K-Vektorraum V auf natürliche Weise

$$\mathtt{Hom}_{K-\mathtt{vect}}(K(X), V) \cong \mathtt{Hom}_{\mathtt{sets}}(X, \mathcal{F}(V)) \ ,$$

wobei hier $\mathcal{F} : K - \mathtt{vect} \to \mathtt{sets}$ die Vektorraumstruktur vergißt.

Wir definieren nun eine Abbildung

$$\phi : G \to \mathtt{GL}(K(G))$$

durch

$$\phi(g)(\sum_{x\in X} \lambda(x)x) = \sum_{x\in X} \lambda(x) g \circ x \ .$$

Lemma 1.42. *Die Abbildung ϕ ist ein wohldefinierter injektiver Gruppenhomomorphismus*

$$G \to \mathtt{GL}(K(G)) \ .$$

Wir sehen also, daß jede Gruppe eine Darstellung als Untergruppe von $GL(V)$ für einen geeigneten Vektorraum besitzt.

Insbesondere besitzt jede endliche Gruppe eine Darstellung als Untergruppe von $\mathtt{GL}(n, K)$ für ein geeignetes n, zum Beispiel $n = |G|$.

2 Struktur von Gruppen

2.1 Untergruppen, Normalteiler, etc

2.1.1 Untergruppen und Nebenklassen

Sei G eine Gruppe.

Definition 2.1. *Eine Teilmenge $U \subset G$ heißt Untergruppe, wenn*

1. *U unter der Verknüpfung abgeschlossen ist,*
2. *$1 \in U$ gilt*
3. *für $u \in U$ auch $u^{-1} \in U$ gilt.*

Untergruppen entstehen z.B. so:

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \to G$ ist eine Untergruppe.
2. Der Kern $\mathtt{ker}(f) \subset G$ eines Homomorphismus $f : G \to H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S >:= m(F(S)) \subset G$ die von S erzeugte Untergruppe.
4. Der Durchschnitt $U := \bigcap_i U_i$ über eine Familie $(U_i)_i$ von Untergruppen ist eine Untergruppe.
5. Sei $G \to \mathtt{Aut}_{\mathtt{sets}}(A)$ eine Wirkung. Für $a \in A$ sei $G_a := \{g \in G | ga = a\}$ der Stabilisator. Dann ist $G_a \subset G$ eine Untergruppe.

2.1.2 Normalteiler

Wir betrachten eine Gruppe, welche auf einer Menge A wirkt. Dann erhalten wir eine Relation:

$$a \sim b \Leftrightarrow \exists g \in G | ga = b \ .$$

Lemma 2.2. *Diese Relation ist eine Äquivalenzrelation.*

Definition 2.3. *Mit $G\backslash A$ bezeichnen wir die Menge der Äquivalenzklassen bezüglich $\sim$.*

Wir haben eine Abbildung $p : A \to G\backslash A$, welche jedem $a \in A$ die von a repräsentierte Klasse $Ga := [a] \in G\backslash A$ zuordnet.

Die Abbildung $p : A \to G\backslash A$ hat die folgende Eigenschaft.

Lemma 2.4. *Für jede Menge B und Abbildung $f : A \to B$ mit der Eigenschaft, daß $f(ga) = a$ für all $g \in G$, gibt es genau eine Abbildung $\bar{f} : G\backslash A \to B$ mit $\bar{f} \circ p = f$.*

$p : A \to G\backslash A$ ist der Quotient einer G-Wirkung in der Kategorie `sets`. Die in Lemma 2.4 gezeigt Eigenschaft wird benutzt, um Quotienten von G-Wirkungen in anderen Kategorien zu charakterisieren.

Aufgabe 2.1. *Sei $p \in \mathbb{N}$ und $G := p\mathbb{Z} \subset \mathbb{Z}$ Die Gruppe G wirke auf der Menge $A := \mathbb{Z}$ durch $(n,a) \mapsto a+n$. Bestimmen Sie die Menge der Äquivalenzklassen $\mathbb{Z}/p\mathbb{Z} := G\backslash A$.*

Aufgabe 2.2. *Die Gruppe $Gl(3,F_2)$ wirkt auf F^3. Bestimmen Sie die Menge $GL(3,F_2)\backslash F_2^3$.*

Aufgabe 2.3. *Die Gruppe $Gl(3,F_2)$ wirkt auf der Menge $P(F^3)$ der eindimensionalen Unterräume von F_2^3. Bestimmen Sie die Menge $GL(3,F_2)\backslash F_2^3$.*

Sei $U \subset G$ eine Untergruppe. Die Gruppe U kann auf G durch links und durch Rechtsmultiplikation wirken:

$$(u,g) \mapsto ug, \quad (u,g) \mapsto gu^{-1} .$$

Wir schreiben den Quotienten nach der Rechtwirkung suggestiv als G/U.

Wir fragen nun, unter welchen Umständen die durch die (Links)Wirkung von U induzierte Äquivalenzrelation mit der Gruppenmultiplikation verträglich ist. Verträglich bedeutet hier:

$$g \sim g', h \sim h' \Rightarrow gh \sim g'h' .$$

Diese Verträglichkeit ist von Bedeutung, weil sie die Definition einer Verknüpfung $\circ : U\backslash G \times U\backslash \to U\backslash$ durch $[g] \circ [h] := [g \circ h]$ erlaubt.

Definition 2.5. *Die Untergruppe $U \subset G$ heißt Normalteiler, wenn die durch die Linkswirkung auf G induzierte Relation mit der Verknüpfung von G verträglich ist.*

Lemma 2.6. *Wenn U ein Normalteiler ist, dann gilt:*

1. *Für jedes $g \in G$ ist $gU = Ug$.*

2. *Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.*

3. *G/U ist mit der induzierten Wirkung eine Gruppe*

Lemma 2.7.

Der Kern eines Homomorphismus ist ein Normalteiler.

Jedes Untergruppe einer abelschen Gruppe ist ein Normalteiler.

Ein Durchschnitt $\cap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.

Insbesondere ist also $p\mathbb{Z} \subset \mathbb{Z}$ ein Normalteiler.

Definition 2.8. *Wir haben eine Gruppe $\mathbb{Z}/p\mathbb{Z}$.*

Aufgabe 2.4. *Zeige, daß $\mathbb{Z}/p\mathbb{Z}$ zur zyklischen Gruppe C_p isomorph ist.*

Aufgabe 2.5. *Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ zur additiven Gruppe von F_p isomorph.*

Sei A eine endliche Menge. Wir konstruieren einen Homomorphismus $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$ durch folgende Vorschrift. Wir betrachten den Vektorraum $\mathbb{Q}(A)$. Wir haben eine lineare Darstellung $\rho : S(A) \to GL(\mathbb{Q}(A))$. Wir erhalten einen Homomorphismus $S(A) \to \mathbb{Q}^*$ durch $g \mapsto \det(\rho(g))$. Wir wissen, daß $S(A)$ durch die Zyklen der Länge zwei erzeugt wird. Sei $A = \{a, b, \dots\}$ und $g = (ab)$. Die Matrix von $\rho(g)$ in der Standardbasis von $\mathbb{Q}(A)$ ist

$$\left(\begin{array}{cc|c} 0 & 1 & 0 \\ 1 & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right).$$

Also gilt $\det(\rho(g)) = -1$. Wir sehen, daß $\sigma(S(A)) \subset \{1, -1\}$ und $\sigma(g) = 1$ genau dann gilt, wenn sich g durch eine gerade Anzahl von Zyklen der Länge zwei darstellen läßt.

Definition 2.9. *Wir definieren*

$$\sigma(g) = \begin{cases} 0 & \det(\rho(g)) = 1 \\ 1 & \det(\rho(g)) = -1 \end{cases} \in \mathbb{Z}/2\mathbb{Z}.$$

Definition 2.10. *Wir definieren die alternierende Gruppe $Alt(A) \subset S(A)$ als den Kern von $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$.*

Wir schreiben Alt_n für $Alt(\{1,\ldots,n\})$.

Aufgabe 2.6. *Bestimmen Sie Alt_n für $n = 2,3,4$.*

Aufgabe 2.7. *Zeigen Sie, daß $S(A)/Alt(A) \cong \mathbb{Z}/2\mathbb{Z}$.*

Aufgabe 2.8. *Seien $U \subset N \subset G$ Normalteiler. Dann ist das Bild von in G/U ein Normalteiler.*

2.1.3 Definition von Gruppen durch Erzeuger und Relationen

Sei G eine Gruppe und $R \subset G$ eine Teilmenge. Mit $< R > \subset G$ bezeichnen wir die von R erzeugt Untergruppe. Im allgemeinen ist diese kein Normalteiler.

Lemma 2.11. *Die Gruppe $< R >$ ist der Durchschnitt*

$$< R >= \cap_{R \subset U} U$$

aller R enthaltenden Untergruppen von G.

Definition 2.12. *Der von R erzeugte Normalteiler $<< R >>$ ist der Durchschnitt*

$$<< R >>= \cap_{R \subset N} N$$

aller R-enthaltenden Normalteiler von G.

Sei T eine Menge. Dann haben wir die freie Gruppe $F(T)$ über T. Die Menge $F(T)$ ist die Menge der reduzierten Worte $W^{red}(\hat{T})$ in $\hat{T} = \{T \times \{1,-1\}$.

Sei $R \subset W^{red}(\hat{T})$ eine Menge von reduzierten Worten.

Definition 2.13. *Die durch T mit den Relationen R erzeugte Gruppe $< T|R >$ ist durch $F(T)/ << R >>$ definiert.*

Das Paar (T,R) heißt auch Präsentation der Gruppe.

Aufgabe 2.9. *Sei $T = \{a\}$, $p \in \mathbb{N}$ und $R = \{a^p\}$. Zeige, daß $< T|R >$ zu $\mathbb{Z}/p\mathbb{Z}$ isomorph ist.*

Aufgabe 2.10. *Sei* $T_1 = \{a,b\}$ *und* $R_1 = \{aba^{-1}b^{-1}, a^2, b^3\}$ *und* $T_2 = \{c\}$ *und* $R_1 = \{c^6\}$. *Zeigen Sie, daß* $< T_1, R_1 > \cong < T_2 | R_2 > \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *gilt.*

Aufgabe 2.11. *Sei* $T_1 = \{a,b\}$ *und* $R_1 = \{aba^{-1}b^{-1}, a^2, b^2\}$ *und* $T_2 = \{c\}$ *und* $R_1 = \{c^4\}$. *Zeigen Sie, daß* $< T_1, R_1 > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *und* $< T_2 | R_2 > \cong \mathbb{Z}/4\mathbb{Z}$, *gilt, diese beiden Gruppen aber nicht isomorph sind.*

Aufgabe 2.12. *Sei* $T = \{s,r\}$ *und* $R = \{s^2, t^n, sts^{-1}t\}$. *Zeigen Sie, daß* $< T | R > \cong D_n$ *gilt.*

Aufgabe 2.13. *Sei* $T = \{a,b\}$ *und* $R = \{aba^{-1}b^{-1}\}$. *Zeige, daß die Gruppe* $< T | R >$ *zu* $\mathbb{Z}^2$ *isomorph ist.*

Aufgabe 2.14. *Sei* $T = \{(1,2),1,3),(2,3)\} \subset S_3$. *Bestimmen Sie eine möglichst kleine Menge* $R \subset F(T)$ *derart, daß die natürliche Abbildung* $m : F(T) \to S_3$ *über einen Isomorphismus* $< T, R > \cong S_3$ *faktorisiert.*

2.1.4 Wortproblem u.ä.

Sei G eine Gruppe und $S \subset G$ eine Teilmenge. Das Wortproblem ist das folgende.

Seien zwei Worte $w, v \in W(S)$ **gegeben. Gilt dann** $m(w) = m(v)$**. Finde einen Algorithmus, diese Frage zu entscheiden.**

Beispiel : Sei $G = F(S)$ und $w, v \in W(\hat{S})$. Es gilt dann $m(w) = m(v)$ genau dann, wenn $w^{red} = v^{red}$. Der Algorithmus:

1. reduziere (Definition 1.32) v, w
2. Vergleiche die Ergebnisse : $v^{red} \stackrel{?}{=} w^{red}$

Jedes Wort in $W(S)$ hat eine Länge. Für die freie Gruppe über S kann das Wortproblem gelöst werden, weil wir eine Vorschrift haben, mit welcher die Länge eines Wortes verkleinert werden kann, ohne das dargestellt Gruppenelement zu ändern, und welche schließlich ein Ergebnis liefert, welches nur von diesem Element abhängt, nämlich das Element selbst als reduziertes Wort.

Ein verwandtes Problem ist das folgende. Seien T_i, $i = 0,1$ Mengen und R_i eine Menge von Relationen in $W^{red}(\hat{T})$.

Entscheide (mit einem Algorithmus), ob $< T_0 | R_0 > \cong < T_1 | R_1 >$ **gilt.**

2.1.5 Kompositionsreihen

Definition 2.14. *Ein maximaler Normalteiler von G ist ein echter Normalteiler $N \subset G$ derart, daß der einzige N enthaltende Normalteiler die Gruppe G selbst ist.*

Definition 2.15. *Eine Gruppe heißt einfach, wenn die triviale Untergruppe ein maximaler Normalteiler ist.*

Definition 2.16. *Eine aufsteigende Folge von Untergruppen*

$$1 = U_0 \subset U_1 \subset \cdots \subset U_{a-1} \subset U_a = G$$

heißt Kompositionsreihe, wenn A_{i-1} ein maximaler Normalteiler in A_i ist.

Die Kompositionsfaktoren A_i/A_{i-1} sind einfache Gruppen.

Satz 2.17 (Jordan-Hölder). *Seien*

$$1 = U_0 \subset U_1 \subset \cdots \subset U_{a-1} \subset U_a = G$$

und

$$1 = V_0 \subset V_1 \subset \cdots \subset V_{b-1} \subset V_b = G$$

zwei Kompositionsreihen von G. Dann gilt $a = b$ und es gibt eine Permutation $\sigma \in S_a$ derart, daß $A_{\sigma(i)}/V_{\sigma(i)-1} \cong V_i/V_{i-1}$.

Aufgabe 2.15. *Bestimmen Sie die Kompositionsfaktoren der Gruppen S_3 und S_4.*

Aufgabe 2.16. *Bestimmen Sie die Kompositionsfaktoren der Gruppe $GL(2, F_2)$.*

Aufgabe 2.17. *Bestimmen Sie die Kompositionsfaktoren der Gruppen $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

2.1.6 Gruppenordnung

Definition 2.18. *Die Ordnung $|G| \in \mathbb{N}$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.*

So gilt zum Beispiel $|S_n| = n!$, $Alt_n = \frac{n!}{2}$, $D_n = 2n$, $|C_n = n$ und $|GL(2, F_2)| = 6$.

Satz 2.19 (Lagrange). *Ist $U \subset G$ eine Untergruppe, so gilt $|G| = |U||G/U|$.*

Proof. Wir behaupten, daß $|gU| = |U|$ für alle Nebenklassen. In der Tat definiert die Multiplikation mit g eine Bijektion $U \to gU$. □

Folgerung 2.20. *Ist $U \subset G$ eine Untergruppe, so teilt $|U|$ die Gruppenordnung.*

Aufgabe 2.18. *Bestimmen Sie alle Untergruppen von $\mathbb{Z}/12\mathbb{Z}$.*

Aufgabe 2.19. *Bestimmen Sie alle Untergruppen von Alt_4.*

2.1.7 Die Kompositionsfaktoren der Permutationsgruppen

Wir hatten schon gesehen, daß S_n eine normale Untergruppe vom Index 2 besitzt, nämlich Alt_n.

Satz 2.21. *Ist $n \geq 5$, so ist Alt_n einfach.*

Proof. Wir zeigen zuerst, daß Alt_n von 3-Zyklen erzeugt wird. Wir nutzen dazu aus, daß jedes Element von Alt_n als Produkt eine geraden Zahl von Transpositionen dargestellt werden kann. Weiter nutzen wir $(a,b)(a,c) = (a,b,c)$ und $(a,b)(c,d) = (a,b,c)(a,d,c)$.

Sei nun $N \subset Alt_n$ ein nicht-trivialer Normalteiler. Wenn N einen 3-Zyklus $g = (a,b,c)$ enthält, dann sind wegen $hgh^{-1} = (a',b',c')$ für $h = (a,a')(b,b'),(c,c')$ alle 3-Zyklen in N enthalten. Da N nicht-trivial ist, darf N also keine 3-Zyklen enthalten.

Sei $g = (a_1,a_2,a_3,a_4,\dots)(\dots)\dots(\dots) \in Alt_n$ (disjunkte Zyklenzerlegung). Sei weiter $h := (a_1,a_2,a_3)$. Dann gilt

$$g' = h^{-1}gh = (a_2,a_3,a_1,a_4,\dots)(\dots)\dots(\dots) \in N\,.$$

Wir haben damit $g^{-1}g' = (a_1,a_2,a_4) \in N$, was unmöglich ist.

Wir sehen, daß N also nur Element mit disjunkter Zyklenzerlegung enthält, deren Faktoren die Länge 2 oder 3 haben. In einer solchen Zerlegung kann nicht genau ein 3-Zyklus auftreten (betrachte das Quadrat).

Wenn $N \ni g = (a,b,c)(a',b',c')(\dots)\dots(\dots)$, dann enthält $g' = h^{-1}gh = (a,a',c,b,c')(\dots)\dots(\dots)$ einen 5-Zyklus. Damit ist jedes Element von Alt_n ein (disjuktes) Produkt einer geraden Anzahl von Transpositionen.

$N \ni g = (a,b)(a',b')$, dann gilt $(a,c)(a',b') = (a,c,b)^{-1}g(a,c,b) \in N$ für alle $c \in A^g$ (gibts wegen $n \geq 5$) . Es gilt $gg' = (a,b,c)$, was unmöglich ist.

Sei nun $N \ni g = (a_1,b_1)(a_2,b_2)(a_3,b_3)(a_4,b_4)\dots$. Dann ist $g' = h^{-1}gh \in N$ mit $h = (a_2,b_1)(a_3,b_2)$. Es gilt $gg' = (a_1,a_3,b_2)(a_2,b_3,b_1)$, und das hatten wir schon ausgeschlossen. □

Also sind die Kompositionsfaktoren von S_n durch

$$\{\mathbb{Z}/2\mathbb{Z}, Alt_n\}$$

gegeben.

Wir bestimmen nun die Kompositionsfaktoren von S_3 und S_4.

Die Gruppe Alt_3 ist offensichtlich isomorph zur zyklischen Gruppe $\mathbb{Z}/3\mathbb{Z}$ mit dem Erzeuger $(1,2,3)$.

Damit ist $\{\mathbb{Z}/2\mathbb{Z}, Z/3\mathbb{Z}\}$ die Liste der Kompositionsfaktoren von S_3.

Wir betrachten nun die Gruppe Alt_4. Wir betrachten alle Elemente der Ordnung zwei in Alt_4. Hier ist die Liste:

$$U = \{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),1\}\,.$$

Durch nachrechnen zeigen wir, daß diese Menge eine Untergruppe ist. Nach Definition ist diese Untergruppe Invariant unter Konjugation und folglich ein Normalteiler. Es gilt $|Alt_4/U| = 3$.

Das Element $(1,2,3) \in Alt_4$ hat Ordnung 3. Seine Klasse in Alt_4/U ist nicht trivial und erzeugt die Gruppe Alt_4/U welche damit zu $\mathbb{Z}/3\mathbb{Z}$ isomorph ist. Insbesondere ist U also maximal.

Wir rechnen nun weiter nach, daß die Gruppe U abelsch ist. Folglich ist $V := \{1,(1,2)(3,4)\}$ ein maximaler Normalteiler in U welcher isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist. Der Quotient U/V ist auch isomorph zu $\mathbb{Z}/2\mathbb{Z}$ und wird von der Klasse von $(1,3)(2,4)$ erzeugt.

Damit ist die Liste der Kompositionsfaktoren von S_4 durch

$$\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}\}$$

gegeben.

2.1.8 Direkte und semidirekte Produkte

Seien G, H Gruppen.

Definition 2.22. *Die Gruppe $G \times H$ ist die Menge $G \times H$ mit Verknüpfung $(g_0, h_0) \circ (g_1, h_1) = (g_0 \circ h_0, g_1 \circ h_1)$ und dem Einselement $1 = (1,1)$.*

Lemma 2.23. *Das Produkt $G \times H$ ist wohldefiniert.*

Aufgabe 2.20. *Zeige, daß $G \times H$ zusammen mit den Projektionen $\mathtt{pr}_1 : G \times H \to G$ und $\mathtt{pr}_2 : G \times H \to H$ das kategorielle Produkt in* `groups` *repräsentiert.*

Wir haben zwei Einbettungen $G \to G \times H$, $g \mapsto (g,1)$ und $H \to G \times H$, $h \mapsto (1,h)$. Die Bilder sind Normalteiler und es gilt $G = G \times H/H$ und $H = G \times H/G$. Beachte, daß die Bilder von G und H in $G \times H$ kommutieren.

Die Rollen von G und H sind hier völlig gleichwertig.

Eine etwas allgemeinere Situation ist die folgende. Sei $\rho : H \to \mathtt{Aut}(G)$ ein Homomorphismus. Dann können wir auf $G \times H$ die folgende Verknüpfung definieren.

$$(g_0, h_0) \circ_\rho (g_1, h_1) = (g_0 \circ h_0, g_1^{h_0} \circ h_1) \ .$$

Lemma 2.24. *1. $G \times\!| H := (G \times H, \circ_\rho, (1,1))$ ist eine Gruppe.*

2. $G \to G \times\!| H$ ist eine Einbettung eines Normalteilers.

3. $H \to G \times\!| H$ ist eine Einbettung einer Untergruppe.

4. $G \times\!| H \to H$ ist ein Homomorphismus.

Definition 2.25. *$G \times\!| H$ heißt das semidirekte Produkt von G und H bezüglich ρ.*

Wenn ρ der triviale Homomorphismus ist, dann stimmt das semidirekte mit dem direkten Produkt überein.

Aufgabe 2.21. *Schreibe* $S_3 = \mathbb{Z}/3\mathbb{Z} \times | \mathbb{Z}/2\mathbb{Z}$

Aufgabe 2.22. *Schreibe* $D_n = C_n \times | \mathbb{Z}/2\mathbb{Z}$.

Lemma 2.26. *Die Liste der Kompositionsfaktoren von* $G \times | H$ *ist die Vereinigung der Listen der Kompositionsfaktoren von* G *und* H.

2.1.9 Die Struktur zyklischer Gruppen

Definition 2.27. *Eine Gruppe* G *heißt zyklisch, wenn sie von einem Element erzeugt werden kann.*

Lemma 2.28. *Alle Untergruppen von* $\mathbb{Z}$ *sind zyklisch.*

Proof. Sei $G \subset \mathbb{Z}$ eine Untergruppe. Sei $n \in \mathbb{N}$ minimal mit $n \in G$. Dann ist $< n > \subset G$.

Sei $k \in G$. Dann gilt $k = an + b$ mit eindeutigem $a \in \mathbb{Z}$ und $b \in \{0, 1, \ldots n-1\}$. Also gilt $b = k - na \in G$, damit $b = 0$ und $k \in < n >$. Wir haben also $G \subset < n >$. □

Lemma 2.29. *Jede endliche zyklische Gruppe ist zu* $\mathbb{Z}/n\mathbb{Z}$ *für ein geeignetes eindeutig bestimmtes* $n \in \mathbb{N}$ *isomorph.*

Proof. Ist G zyklisch und $g \in G$ ein Erzeuger, so gibt es einen surjektiven Homomorphismus $q : \mathbb{Z} \cong F_1 \to G$, welcher 1 auf g abbildet. Sei $n \in \mathbb{Z}$ ein Erzeuger von $\ker(q)$. Dann ist n minimal mit $g^n = 0$. Es gilt $G = \mathbb{Z}/n\mathbb{Z}$. □

Lemma 2.30. *Sei* G *eine endliche Gruppe und* $g, h \in G$ *kommutierende Elemente mit teilerfremder Ordnung. Dann definiert* $(g^r, h^s) \mapsto g^r h^s$ *einen Isomorphismus* $< g > \times < h > \cong < g, h >$. *Inbesondere gilt* $o(gh) = o(g)o(h)$.

Dieses Lemma ist im allgemeinen falsch, wenn die Ordnungen von g, h nicht Teilerfremd sind.

Sei $G = < g >$ eine endliche zyklische Gruppe.

Lemma 2.31. *Die Untergruppen von* G *sind die Gruppen* $< g^l >$ *für alle Teiler* l *von* N

Proof. Wir schreiben $G = \mathbb{Z}/n\mathbb{Z}$. Dann sind die Untergruppen die Bilder von $m\mathbb{Z} \subset n\mathbb{Z}$ gegeben. Diese Inklusion gilt aber genau dann, wenn $n|m$. □

Definition 2.32. *Eine endliche Gruppe ist eine p-Gruppe, wenn $|G| = p^e$ für ein geeignetes $e \in \mathbb{N}$ gilt.*

Folgerung 2.33. *Jede zyklische Gruppe G ist isomorph zu einem Produkt $\times_{p||G|} G_p$. zyklischer p-Gruppen.*

2.1.10 Die Struktur endlicher abelscher Gruppen

Sei G eine endliche abelsche Gruppe.

Lemma 2.34. *Ist $U \subset G$ eine zyklische Untergruppe maximaler Ordnung, dann gilt $o(g)||U|$ für alle $g \in G$.*

Proof. Sei $g \in G$. Sei $p \in \mathbb{N}$ eine Primzahl und $r \in \mathbb{N}$ derart, daß $p^r|o(g)$. Sei $|U| = p^e m$ für $e, m \in \mathbb{N}$ mit $(p,m) = 1$. Wir wählen $a \in < g >$ und $b \in U$ mit $o(a) = p^r$ und $o(b) = m$. Dann ist $o(ab) = p^r m$. Da U maximale Ordnung hatte, gilt $r = e$. □

Lemma 2.35. *Ist $U \subset G$ eine maximale zyklische Untergruppe, so gibt es eine komplementäre Untergruppe $V \subset G$ so daß $G = U \times V$ ist.*

Proof. Wir beweisen durch Induktion nach der Ordnung von G. Ist $U = G$, so setzt man $V = \{1\}$.

Sei $U \neq G$. Sei $y \in G \setminus U$ ein Element minimaler Ordnung. Da $< y^p > \subset_{\neq} < y >$ für jeden Primteiler von $o(y)$ gilt $< y^p > \subset U$. Sei $U =< u >$. Da $o(y)||U|$ gilt, hat U eine genau Untergruppe $< v >$ der Ordnung $o(y)$. Die Gruppe $< v^p >$ ist damit eine Untergruppe der Ordnung $\frac{o(y)}{p} = | < y^p > |$ in $< u^p >$, also $< v^p > = < y^p >$.

Sei $u^{pi} = y^p$ für ein geeignetes i. Dann gilt $(u^{-i}y)^p = 1$. Da $u^{-i}y \in G \setminus U$, gilt $o(y) = p$.

Sei $N =< y >$. Dann gilt $N \cap U = 1$. Wir setzen $\bar{G} = G/N$. Ist $x \in G$, dann gilt $o([x]) = \mathtt{min}\{n \in \mathbb{N} | x^n \in U\} \leq o(x)$. Insbesondere gilt $o([u]) = o(u)$. Somit ist $\bar{U} =< [u] >$ eine

maximale zyklische Untergruppe von $\bar{G}$. Sei $\bar{V} \subset \bar{G}$ ein Komplement (Induktionsvoraussetzung), also $\bar{G} = \bar{U} \times \bar{V}$. Wir schreiben $\bar{V} = V/N$ für $N \subset V \subset G$. Dann ist V ein Komplement von U. □

Folgerung 2.36. *Jede endliche abelsche Gruppe ist isomorph zu einem Produkt zyklischer Gruppen.*

Folgerung 2.37. *Jede endliche abelsche Gruppe ist isomorph zu einem Produkt zyklischer p-Gruppen.*

Das heißt, die allgemeine Form einer endlichen abelschen Gruppe ist

$$G \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

wobei p_i Primzahlen und $e_i \in \mathbb{N}$ sind.

3 Ringe

3.1 Allgemeine Begriffe

3.1.1 Definition und Beispiele von Ringen

Definition 3.1. *Ein kommutativer Ring mit Eins ist ein Tupel $(R, +, \circ, 0, 1)$, aus einer nicht-leeren Menge R und Verknüpfungen $+$ und $\circ$ derart,daß*

1. $(R, +, 0)$ *eine abelsche Gruppe ist,*
2. $(R, \circ, 1)$ *ein abelsches Monoid ist,*
3. *und die Operationen $+$ und $\circ$ vermöge des Distributivgesetzes*

$$a \circ (b + c) = a \circ b + a \circ c$$

verträglich sind.

Wir werden das Symbol $\circ$ für die Multiplikation gewöhnlich weglassen. Im folgenden werden einfach von Ringen sprechen. Hier sind Beispiele:

1. Jeder Körper ist ein Ring.
2. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring.
3. Ist X eine Menge und R ein Ring, dann die Menge der Funktionen $R^X = \{f : X \to R\}$ ein Ring mit $(f+g)(x) = f(x)+g(x)$, $(fg)(x) = f(x)g(x)$
4. Ist G eine endliche abelsche Gruppe, dann $R(G) := R^G$ mit der Addition $(f+g)(x) := f(x)+g(x)$ und der Multiplikation $(fg)(x) = \sum_{y\in G} f(y)g(y^{-1}x)$ ein Ring.

3.1.2 Polynomringe

Wir betrachten zuerst den Körper $\mathbb{R}$. Ein Polynom $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ kann als eine Funktion $p : \mathbb{R} \to \mathbb{R}$ aufgefaßt werden. Insbesondere ist der Polynomring $\mathbb{R}[x]$ ein Untering von $\mathbb{R}^{\mathbb{R}}$.

Für andere Körper gilt dies nicht. Es gilt beispielsweise

$$x = x^2 : \mathbb{F}_2 \to \mathbb{F}_2 \ .$$

Wir werden daher $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ nicht als Funktion sondern als Folge $(a_0, \ldots, a_n, 0, 0, \ldots)$ betrachten.

Sei R ein Ring.

Definition 3.2. *Die unterliegende additive Gruppe des Polynomringes $R[x]$ ist die Gruppe der Abbildungen $a : \mathbb{N} \to R$, welche nur an endlich vielen Stellen von Null verschiedene Werte annehmen. Das Produkt wird durch*

$$(a \circ b)_n := \sum_{k,l\in\mathbb{N}, k+l=n} a_k b_l$$

definiert.

Man kann $R[x]$ als den (Halb)Gruppenring von $\mathbb{N}$ auffassen.

Lemma 3.3. *Der Ring $R[x]$ ist wohldefiniert.*

Definition 3.4. *Der Grad eines Polynoms $0 \neq a \in R[x]$ wird durch*

$$\deg(a) = \mathtt{max}\{n \in \mathbb{N} | a_n \neq 0\}$$

definiert. Wir setzen $\deg(0) = -\infty$.

Lemma 3.5. *Es gilt:*

1. $\deg(ab) \leq \deg(a) + \deg(b)$
2. $\deg(a+b) \leq \texttt{max}\{\deg(a), \deg(b)\}$.

Aufgabe 3.1. *Ist K ein Körper, so gilt* $\deg(ab) = \deg(a) + \deg(b)$.

3.1.3 Quadratische Ringe

Sei $D \in \mathbb{Z}$ kein Quadrat (also etwa $D = -1$ oder $D = 2$). Wir wählen eine Wurzel $\sqrt{D} \in \mathbb{C}$.

Definition 3.6. *Wir definieren* $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} | a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

Lemma 3.7. *Mit den von* $\mathbb{C}$ *induzierten Operationen ist* $\mathbb{Z}[\sqrt{D}]$ *ist ein Ring.*

Definition 3.8. *Wir definieren* $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} | a, b \in \mathbb{Q}\} \subset \mathbb{C}$.

Lemma 3.9. *Mit den von* $\mathbb{C}$ *induzierten Operationen ist* $\mathbb{Q}(\sqrt{D})$ *ist ein Körper.*

3.1.4 Integritätsbereiche

Sei R ein Ring.

Definition 3.10. *Ein Element* $a \in R$ *heißt Nullteiler, falls es ein* $b \neq 0$ *mit* $ab = 0$ *gibt.*

Aufgabe 3.2. *Sei X eine Menge. bestimmen Sie die Nullteiler von* $\mathbb{R}^X$.

Definition 3.11. *Ein Integritätsbereich ist ein Ring, der keine nichttrivialen Nullteiler enthält.*

Die ganzen Zahlen bilden eine Integritätsbereich. Allgemeiner sind alle Unterringe von Körpern Integritätsbereiche, so etwa $\mathbb{Z}[\sqrt{D}]$.

Lemma 3.12. *Ist R ein Integritätsbereich, so ist der Polynomring* $R[x]$ *ein Integritätsbereich.*

3.1.5 Teilen und prime Elemente

Sei R ein Ring

Definition 3.13. *1. Seien $a, b \in R$. Wenn es $c \in R$ mit $ac = b$ gibt, so sagen wir, daß a ein Teiler von b ist $(a|b)$.*

2. *Sei $M \subset R$ eine Teilmenge. Eine Element $a \in R$ heißt größter gemeinsamer Teiler von M ($a \in g.g.T(M)$), falls jedes $b \in R$, welches alle $m \in M$ teilt, auch a teilt.*

3. *$a \in R$ ist eine Einheit, wenn $a|1$.*

4. *$0 \neq b \in R$ ist irreduzibel, wenn b keine Einheit ist und aus $b = ac$ folgt, daß a oder c eine Einheit in R ist. ist.*

5. *$0 \neq p \in R$ ist prim, wenn p keine Einheit ist und aus $p|ab$ folgt, daß $p|a$ oder $p|b$.*

Lemma 3.14. *Die Einheiten von $\mathbb{Z}$ sind $\{1, -1\}$.*

Aufgabe 3.3. *Bestimmmen in $\mathbb{Z}$ einen $g.g.T(\{120, 50, 96\})$.*

Aufgabe 3.4. *Bestimmen Sie in $\mathbb{R}[x]$ einen größten gemeinsamen Teiler von ...*

Lemma 3.15. *Die Einheiten von $K[x]$ sind $K^* = K \setminus \{0\}$.*

Lemma 3.16. *Die Einheiten eines Ringes bilden eine abelsche Gruppe unter der Multipikation.*

Aufgabe 3.5. *Bestimmen Sie die Einheiten in $\mathbb{Z}[i]$.*

Aufgabe 3.6. *Ist $D < -1$, so hat $\mathbb{Z}[\sqrt{D}]$ nur die Einheiten ± 1.*

3.1.6 Die Einheiten in $\mathbb{Z}[\sqrt{D}]$

Sei $D \in \mathbb{Z}$ quadratfrei. Wir betrachten den Ringhomomorphismus

$$\overline{(\dots)} : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}] \ ,$$

$$\overline{a + b\sqrt{D}} := a - b\sqrt{D} \ .$$

Wir betrachten die Norm

$$N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z} \ ,$$

$$N(x) := x\bar{x} \ .$$

Diese Bildung ist hilfreich, um die Einheiten in $\mathbb{Z}[\sqrt{D}]$ zu studieren. Sei zunächst $D<0$. Dann ist $\mathbb{Z}[\sqrt{D}] \subset \mathbb{C}$ ein Gitter mit Basis $1, \sqrt{D}$. Die Norm N ist die Einschränkung der Norm von $\mathbb{C}$, $z \mapsto |z|^2$. Insbesondere ist $\{x \in \mathbb{Z}[\sqrt{D}] | N(x) < C\}$ endlich für jedes $C \in \mathbb{R}$.

Wenn $x \in \mathbb{Z}[\sqrt{D}]$ eine Einheit ist, dann muß $N(x) = 1$ gelten. Wir schließen:

Lemma 3.17. *Wenn $D < 0$, so ist die Gruppe der Einheiten von $\mathbb{Z}[\sqrt{D}]$ endlich.*

Dies steht im Gegensatz zum Fall $D > 0$. Wir definieren eine Einbettung als Gitter

$$\mathbb{Z}[\sqrt{D}] \to \mathbb{R}^2$$

durch $x \mapsto (x, \bar{x})$. Die Norm ist dann die Einschränkung des hyperbolischen Produktes

$$(x, y) \mapsto xy \ .$$

Lemma 3.18. *Wenn $D > 0$, dann ist die Gruppe der Einheiten in $\mathbb{Z}[\sqrt{D}]$ unendlich.*

Proof. Wir müssen zeigen, daß es unendlich viele Elemente mit $N(x) = 1$ gilt. Diese sind alle Einheiten.

Wir nehmen zuerst an, daß es ein $r > 0$ gibt, so daß

$$\sharp\{x \in \mathbb{Z}[\sqrt{D}] | N(x) \leq r\} = \infty \ . \tag{1}$$

Dann führen wir eine Äquivalenzrelation $\sim_r$ auf $\mathbb{Z}[\sqrt{D}]$ ein durch $x \sim_r y$ falls $r | x - y$. Es gibt nur endlich viele Klassen bezüglich $\sim_r$. Wenn $N(x) = N(y) = r$ und $x \sim_r y$, dann ist $x/y \in \mathbb{Z}[\sqrt{D}]$ eine Einheit. In der Tat gilt

$$x/y = x\bar{y}/N(y) = x\bar{y}/r = y\bar{y}/r + (x-y)\bar{y}/r = 1 + \frac{(x-y)}{r}\bar{y} \ .$$

Wir zerlegen die Menge aller Elemente der Norm r in Äquivalenzklassen bezüglich $\sim_r$. Eine dieser Klassen ist unendlich.

Es bleibt nur noch (1) zu zeigen. Wir betrachten das Rechteck $R(u) \subset \mathbb{R}^2$ mit den Eckpunkten $(\pm u, \pm r/u)$ mit der Fläche $4r^2$. Wenn $4r^2$ größer als die $4x$ die Fläche der Fundamentalmasche des Gitters ist, muß es in diesem einen Gitterpunkt $\neq 0$ geben. Wir betrachten jetzt immer größere Werte von u. Auf der y-Achse liegen keine Gitterpunkte. Damit erhalten wir undendlich viele Gitterpunkte mit $N(x) \leq r$. □

[1]

[1] Dieser Abschnitt ist zu verbessern : Siehe Behandlung der Pellschen Gleichung im Skript von Maus.

3.1.7 Homomorphismen

Seien R, S Ringe.

Definition 3.19. *Eine Homomorphismus $\phi : R \to S$ ist eine Abbildung, welche Homomorphismen der additiven abelschen Gruppen und der multiplikativen Monoide induziert.*

Lemma 3.20. *Der Kern eines Homomorphismus $\phi : R \to S$ ist eine Untergruppe, welche abgeschlossen unter der Multiplikation mit Elementen aus R ist.*

Definition 3.21. *Ein Ideal $I \subset R$ ist eine Untergruppe, welche abgeschlossen unter der Multiplikation mit Elementen aus R ist.*

Lemma 3.22. *Ist $I \subset R$ ein Ideal, so läßt sich auf der Gruppe R/I eine Multiplikation vertreterweise definieren so daß R/I die Struktur eines Ringes bekommt. Die Projektion $R \to R/I$ ist ein Homomorphismus von Ringen mit dem Kern I.*

Sei $n \in \mathbb{Z}$. Die Menge $(n) := n\mathbb{Z} \subset \mathbb{Z}$ ist ein Ideal.

Lemma 3.23. *Der Quotient $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Integritätbereich, wenn n eine Primzahl ist.*

Aufgabe 3.7. *Zeige, daß für jede Primzahl $p \in \mathbb{Z}$ der Ring $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist.*

Aufgabe 3.8. *Bestimmen Sie die Einheiten in $\mathbb{Z}/n\mathbb{Z}$.*

3.2 Euklidische Ringe, Euklidischer Algorithmus und Hauptideale

3.2.1 Hauptideale

Sei R ein Ring.

Definition 3.24. *Ein Ideal $I \subset R$ heißt Hauptideal, wenn es ein $a \in R$ mit $I = aR$ gibt. Wir schreiben dann auch $(a) := I$.*

Definition 3.25. *Ein Ring heißt Hauptidealring, wenn alle seine Ideale Hauptideale sind.*

Wir werden sehen, daß $\mathbb{Z}$ und $K[x]$ für einen Körper Hauptidealringe sind.

Lemma 3.26. *Ein Ring ist genau dann ein Hauptidealring, wenn für jede Teilmenge ein größter gemeinsamer Teiler der Form $a = a_1m_1 + \cdots + a_rm_r$ mit $a_i \in R$ und $m_i \in M$ existiert.*

Proof. Sei R ein Hauptidealring. Sei (M) das von M erzeugte Ideal. Dann gibt es ein $a \in R$ mit $(M) = (a)$. Insbesondere Teilt a alle Elemente von M. Wenn jetzt $b \in R$ alle $m \in M$ teilt, so auch a. Folglich ist a ein größter gemeinsamer Teiler von M.

Umgekehrt, wenn $a = a_1m_1 + \cdots + a_rm_r$ ein größter gemeinsamer Teiler von M ist, so gilt offensichtlich $(M) = (a)$. □

3.2.2 Euklidische Ringe

Sei R ein Ring.

Definition 3.27. *Eine Höhe auf R ist eine Abbildung $H : R \setminus \{0\} \to \mathbb{N} \cup 0$ mit: Für alle $a, b \in R$ existieren $q, r \in R$ mit $a = bq + r$ und $H(r) < H(b)$ oder $r = 0$.*

Lemma 3.28. *Durch $\mathbb{Z} \ni n \mapsto |n|$ wird eine Höhe auf $\mathbb{Z}$ definiert.*

Lemma 3.29. *Durch $K[x] \ni p \mapsto \deg(p)$ wird eine Höhe auf $K[x]$ definiert.*

Proof. Seien $f, g \in K[x]$. Gilt $\deg(f) < \deg(g)$, so schreiben wir

$$f = 0g + r$$

mit $f = r$. Es gilt $\deg(r) < \deg(g)$. Sei nun $n := \deg(f) \geq \deg(g)$. Wir schreiben $f = f_nx^n + \ldots f_0$ und $g = g_mx^m + \ldots g_0$. Wir beweisen mit Induktion nach n. Ist $n = 0$, so schreiben wir $f = \frac{f_0}{g_0}g + 0$ und es gilt $\deg(g) > \deg(0)$. Ist $n > 0$, so setzen wir $h := f - \frac{f_n}{g_m}X^{n-m}g$. Dann gilt $\deg(h) < n$ und nach Induktionsvoraussetzung

$$h = qg + r$$

mit $\deg(g) > \deg(r)$. Daraus folgt

$$f = (q + \frac{f_n}{g_m}X^{n-m})g + r\,.$$

□

In diesem Fall ist die Darstellung $f = qg + r$ sogar eindeutig.

Lemma 3.30. *Der Ring $\mathbb{Z}[i]$ ist ein euklidischer Ring mit der Höhe $a+bi := a^2+b^2 = |a+bi|^2$.*

Proof. Sei $z \in \mathbb{Z}[i]$. Wir suchen q mit $|f-qg| < |g|$. In der Tat ist diese Bedingung zu $|\frac{f}{g} - q| < 1$ äquivalent. Wir finden q durch elementar-geometrische Betrachtungen. □

Aufgabe 3.9. *Welche der folgenden Ringe sind Euklidisch.*

1. $\mathbb{Z}[\sqrt{-2}]$.
2. $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.
3. $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

Aufgabe 3.10. *Zeige, daß $\mathbb{Z}[\sqrt{2}]$ euklidisch ist mit der Höhe $H(a+b\sqrt{2}) = a^2-2b^2$.*

Lemma 3.31. *Ein Euklidischer Ring (R,H) ist ein Hauptidealring.*

Proof. Sei $I \subset R$ ein Ideal. Wir wählen ein $0 \neq g \in I$ mit $H(g)$ minimal. Ist $f \in I$ so gilt

$$f = qg + r$$

mit $H(r) < H(g)$. Wegen $r \in I$ gilt $r = 0$. □

Folgerung 3.32. *In einem Euklidischen Ring hat jede Teilmenge einen g.g.T.*

Folgerung 3.33. *Für einen Körper K ist $K[x]$ ein Hauptidealring.*

3.2.3 Euklidischer Algorithmus

Sei R ein Euklidischer Ring mit Höhe H.

Lemma 3.34. *Für $\{a,b\} \in R$ wird der g.g.T durch folgenden Algorithmus bestimmt.*

1. *$f := a$ und $g := b$*
2. *$f = qg + r$ mit $N(g) > N(r)$*
3. *Wenn $r = 0$ so ist $g = g.g.T\{a,b\}$. Sonst $f := g$ und $g := r$ und gehe zu 2.*

Proof. Sei (r_n) die Folge der Werte von r, die von diesem Algorithmus erzeugt werden. Dann ist $(N(r_n))$ streng monoton fallend. Folglich bricht der Algorithmus ab. Seien (f_n) und (g_n) die erzeugten Folgen. Dann gilt $g.g.T(f_{n+1}, g_{n+1}) = g.g.T(f_n, g_n)$. □

Aufgabe 3.11. *Bestimmen Sie in $\mathbb{Z}[i]$ einen g.g.T von $\{1+5i, -1+5i\}$*

3.2.4 Polynome und Nullstellen

Sei R ein Ring. Dann ist $R[x]$ nicht notwendig Euklidisch, aber es gilt folgende schwächere Version.

Lemma 3.35. *Seien $f, g \in R[x]$ und sei $g = g_m x^m + \cdots + g_0$ und g_m eine Einheit. Dann existieren $q, r \in R[x]$ mit* $\deg(g) > \deg(r)$ *und*

$$f = qg + r\,.$$

Lemma 3.36. *Sei $f \in R[x]$ und $w \in R$ mit $f(w) = 0$. Dann gilt $f(x) = (x-w)g$ für ein $g \in R[x]$.*

Proof. Wir schreiben $f = (x-w)q + r$. Dann gilt $\deg(r) < 0$ und $r(w) = 0$, also $r = 0$. □

Lemma 3.37. *Sei R ein Integritätsbereich und $f[x] \in R[x]$. Dann hat f höchstens* $\deg(n)$ *paarweise verschiedene Nullstellen.*

Folgerung 3.38. *Ist R ein unendlicher Integritätsbereich, so ist die Abbildung $R[x] \to R^R$ injektiv.*

3.3 Primfaktorzerlegungen

3.3.1 Irreduzible und prime Elemente

Definition 3.39. *In einem Integritätsbereich R heißen $a, b \in R$ genau dann assoziiert, wenn $a = eb$ für eine Einheit $e \in R$ gilt. Wir schreiben diese Äquivalenzrelation als $a \sim b$.*

Sei R ein Integritätsbereich und $p \in R$ prim.

Lemma 3.40. *1. p is irreduzibel.*

2. Ist $p \sim p'$ so ist p' auch prim.

3. Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.

4. Wenn $p|a_1 \dots a_k$, so existiert ein $i \in R$ mit $p|a_i$.

Im allgemeinen sind irreduzible Elemente nicht prim.

Dazu berachten wir den Ring $R = \mathbb{Z}[\sqrt{-5}]$. In diesem Ring gilt

$$6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5}) .$$

Wir zeigen, daß $a = 2,3,(1+\sqrt{-5}),(1-\sqrt{-5})$ irreduzibel sind. Dazu betrachten wir die Normen $|a|^2 = 4,9,6,6$. Wenn nun $r \in \mathbb{Z}[\sqrt{-5}]$ ein echter Teiler von a ist, so müßte $1 \neq |r|^2 | 4,9,6,6$ gelten, also $|r|^2 = 2$ oder $|r|^2 = 3$. Wir schreiben $r = x+y\sqrt{-5}$. Dann gilt $x^2+5y^2 = 2$ oder $x^2+5y^2 = 3$. Diese Gleichungen haben keine ganzzahligen Lösungen.

Es gilt $2|(1+\sqrt{-5}),(1-\sqrt{-5})$ aber nicht $2|(1+\sqrt{-5})$ oder $2|(1-\sqrt{-5})$. Folglich ist 2 zwar irreduzibel, aber nicht prim.

3.3.2 Die primen Gaußschen Zahlen

Im folgenden brauchen wir das folgende Lemma.

Lemma 3.41 (Satz von Wilson). *Für jede Primzahl gilt*

$$(p-1)! \equiv -1 (\mod p) .$$

Proof. Für $p = 2$ gilt das Lemma. Wir betrachten den Körper $\mathbb{Z}/p\mathbb{Z}$. Das Polynom $x^2 - 1 = (x-1)(x+1)$ hat genau zwei verschiedene Nullstellen. Folglich hat $(\mathbb{Z}/p\mathbb{Z})^*$ genau zwei Elemente der Ordnung 2, nämlich 1 und -1. $x = (p-1)!$ ist das Produkt aller Elemente von $(\mathbb{Z}/p\mathbb{Z})^*$. Kürze jeden Faktor von $(p-1)!$ mit seinem Inversen. Dann bleibt das nichttriviale Element der Ordnung 2 übrig. □

Satz 3.42. *Die Primelemente von $\mathbb{Z}[i]$ sind assoziiert zu*

1. $\pi = 1+i$

2. $\pi = a+bi$, $a^2+b^2 = p$, $p \equiv 1(\mod 4)$, $a > |b| > 0$

3. $\pi = p$, $p \equiv 3(\mod 4)$

(p ist prim in $\mathbb{Z}$).

Proof. Die Zahlen in 1. und 2. sind prim, da $N(\pi)$ prim ist. Die Zahlen in 3. sind prim, da $N(p) = p^2 = N(\alpha)N(\beta)$ impliziert $N(\alpha) = p = a^2+b^2 \equiv 1(\mod 4)$.

Sei $\pi \in \mathbb{Z}[i]$ prim. Dann ist $N(\pi) = \pi\bar{\pi} = p_1 \dots p_r$. Folglich $\pi | p_i$ für ein i. Sei $p := p_i$. Also $N(\pi)|N(p) = p^2$. Wenn $N(\pi) = p^2$, dann ist $\pi \sim p$. Wenn $p \equiv 1(\mod 4)$, so ist p nicht prim. In der Tat sei $p = 4n+1$. Dann $p|((2n!)^2+1)$ und $((2n!)^2+1) = ((2n)!+i)((2n)!-i)$. Aber p teilt keinen der Faktoren. Um dies einzusehen,

$$-1 \overset{Wilson}{\equiv} (p-1)! = [1.2.\dots.(2n)][(p-1)(p-2)\dots(p-2n)] \equiv (2n)!(-1)^{2n}(2n)!(\mod p).$$

Sei nun $N(p) = p$. Dann ist π vom Typ 2., oder falls $p = 2$, vom Typ 1.

3.3.3 Zerfallverhalten von Primzahlen

Wir betrachten zwei Integritätsbereiche $\mathbb{Z} \subset, R = \mathbb{Z}[\sqrt{D}]$ oder $R = \mathbb{Z}[\omega_D]$ für $\omega_D = \frac{1+\sqrt{D}}{2}$ falls $4|(D-1)$. Sei $p \in \mathbb{Z}$ eine Primzahl.

Definition 3.43. *1. p ist verzweigt, wenn $p = \pi\bar{\pi}$ für ein Primelement $\pi \in R$ mit $\pi \sim \bar{\pi}$ gilt.*

2. *p ist zerlegt, wenn $p = \pi\bar{\pi}$ für zwei nicht assoziierte Primelemente $\pi, \bar{\pi}$ in R.*

3. *p ist träge, wenn p in R prim bleibt.*

Wir betrachten den Ring $R = \mathbb{Z}[\omega_{-3}]$.

Satz 3.44. *Sei $p \in \mathbb{Z}$ prim.*

1. *p ist genau dann verzweigt, wenn $p = 3$.*

2. *p ist genau dann zerlegt, wenn $p = a^2+ab+b^2$ (oder äquivalent $4p = c^2+3b^2$).*

3. *In allen weiteren Fällen ist p träge.*

Proof. Sei p verzweigt. Dann gilt $p = \pi\bar{\pi}$ mit $N(\pi) = p$ und $\pi \sim \bar{\pi}$. Die Einheiten von R sind ω_{-3}^n, $n = 0, \ldots, 5$. Wir schreiben $\pi = a + b\omega_{-3}$ und untersuchen $\bar{\pi} = a + b - b\omega_{-3} = \omega_{-3}^n \pi$. In jedem Fall schließen wir $N(\pi) = p$ aus, falls $p \neq 3$. Fall $p = 3$, so ist $\pi = 1 - 2\omega_{-3}$.

Wenn sich $p = \pi\bar{\pi}$, dann gilt $N(\pi) = p$, also $p = a^2 + ab + b^2$. Wegen $4a^2 + 4ab + 4b^2 = (2a + b)^2 + 3b^2$ gilt auch die zweite Darstellung. Ist $p \neq 3$, dann ist $\pi \not\sim \bar{\pi}$.

3.3.4 Faktorielle Ringe I

Sei R ein Integritätsbereich und $a \in R$.

Definition 3.45. *Das Element a hat eine im wesentlichen eindeutige Zerlegung in irreduzible Elemente, wenn $a = p_1 \ldots p_r$ für irreduzible Elemente p_i gilt, und wenn für jede andere solche Darstellung $a = q_1 \ldots q_s$ gilt:*

1. *$r = s$*
2. *Es existiert eine Permutation $\sigma \in S_r$ mit $p_{\sigma(i)} \sim q_i$ für alle $i = 1, \ldots r$.*

Das Beispiel $R = \mathbb{Z}[\sqrt{-5}]$ und

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

zeigt, daß 6 zwar eine Zerlegung als Produkt irreduzibler Elemente besitzt, diese Zerlegung aber nicht wesentlich eindeutig ist.

Definition 3.46. *Ein Integritätsbereich heißt faktoriell, wenn jedes von Null verschiedene Element eine im wesentlichen eindeutige Zerlegung in irreduzible Elemente besitzt.*

Wir werden später zeigen, daß $\mathbb{Z}$ faktoriell ist. Wir schon oben gezeigt, ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell.

3.3.5 Teilerketten

Wir betrachten einen Integritätbereich R und $a \in R$.

Definition 3.47. *1. Eine Teilerkette von a ist eine Folge $(a_i)_{i\in\mathbb{N}}$ mit $a_{i+1}|a_i$ für alle $i \in \mathbb{N}$.*

2. Wir sagen, daß in R der Teilerkettensatz gilt, wenn für jedes $a \in R$ und jede Teilerkette $(a_i)_{i\in R}$ von a ein $n \in \mathbb{N}$ existiert, so daß für $i \geq n$ auch $a_i|a_{i+1}$ gilt.

Lemma 3.48. *Wenn in R der Teilerkettensatz gilt, dann besitzt jedes von Null verschiedene Element eine Zerlegung in irreduzible Elemente.*

Satz 3.49. *In den folgenden Ringen gilt der Teilerkettensatz.*

1. $\mathbb{Z}$,
2. $K[X]$ *für einen Körper* K,
3. $\mathbb{Z}[\sqrt{D}]$
4. R *Hauptidealring*
5. R *Euklidischer Ring*
6. $R[X]$, *wenn Teilerkettensatz für* R *gilt.*

Proof. Zu 4.: Sei R Hauptidealring. Sei $a \in R$ und $(a_i)_{i\in\mathbb{N}}$ eine Teilerkette. Dann haben wir eine Folge von Hauptidealen

$$(a_1) \subset (a_2) \subset \dots .$$

Nun ist $I := \cup_i (a_i)$ ein Ideal und damit ein Hauptideal, also $I = (d)$. Dann gilt aber $d \in (a_n)$ für ein n und deshalb $(d) \subset (a_n)$. Folglich $(a_i) = (a_{i+1})$ für $i \geq n$. □

3.3.6 Faktorielle Ringe II

Sei R ein Integritätsbereich und $a \in R$.

Lemma 3.50. *Seien $a = p_1 \dots p_r$ und $a = q_1 \dots q_s$ Zerlegungen in prime Elemente, dann gilt $r = s$ und $p_i \sim q_i$ (nach geeigneter Umnumerierung).*

Lemma 3.51. *In einem Hauptidealring R sind alle irreduziblen Elemente prim.*

Proof. Sei $p \in R$ irreduzibel und $p|ab$ für $a,b \in R$. Wenn $p \not| a$ so gilt $g.g.T.(p,a) = 1$. Also gibt es nach Lemma 3.26 eine Darstellung $1 = xp + ya$ für $x,y \in R$. Also $b = xbp + yab$ woraus $p|b$ folgt. □

Satz 3.52. *Sei R ein Integritätsbereich. Dann ist R genau dann faktoriell, wenn in R der Teilerkettensatz gilt und alle irreduziblen Elemente prim sind.*

Proof. Die Rückrichtung folgt aus 3.50. Sei nun R faktoriell. Sei $p \in R$ irreduzibel und $p|ab$. Dann gibt irreduzible Zerlegungen $a = p_1 \dots p_r$ und $b = q_1 \dots q_s$. Insbesondere ist auch $ab = p_1 \dots p_r q_1 \dots q_s$ eine solche Zerlegung. Wir schreiben $ab = pc$ und $z = r_1 \dots r_t$. Dann $p_1 \dots p_r q_1 \dots q_s = p r_1 \dots r_t$. Aus der Eindeutigkeit der Zerlegung folgt, daß $p \sim p_i$ oder $p \sim q_i$ für geeignetes i. Damit gilt $p|a$ oder $p|b$. Wir schließen nun den Teilerkettensatz durch abzählen der Primfaktoren. □

Satz 3.53. *Hauptidealringe sind faktoriell.*

Folgerung 3.54.

1. *$\mathbb{Z}$ ist faktoriell.*
2. *Euklidische Ringe sind faktoriell.*
3. *$K[x]$ für einen Körper K ist faktoriell.*

3.4 Restklassenringe von $\mathbb{Z}$

3.4.1 Kongruenzen

Sei $m \in \mathbb{Z}$, $(m) \subset \mathbb{Z}$ das von m erzeugte Hauptideal und und $\mathbb{Z}/(m)$ der dazugehörige Restklassenring. Wir schreiben Elemente dieses Ringes in der Form $[a]$, $a \in \mathbb{Z}$. Die Gleichung $[a] = [b]$ is gleichbedeutend mit $a \equiv b(\mod m)$.

Lemma 3.55.

1. *Die Gleichung $[a]x = 1$ ist in $\mathbb{Z}/(m)$ genau dann lösbar, wenn $g.g.T.(a,m) = 1$.*
2. *Die Gleichung $[a]x = [b]$ st in $\mathbb{Z}/(m)$ genau dann lösbar, wenn für $d := g.g.T(a,m)$ gilt $d|b$.*
3. *Wenn $d|b$, so gibt es d verschiedene Lösungen.*

Proof. 1. schon gezeigt.

Zu 2.: Notwendigkeit der Bedingung klar. Für die andere Richtung schreiben wir $d = au + mv$ und $b = dw$. Es gilt $g.g.T(w,a) = 1$. Dann gilt $b = wau + wmv$, also $x = [wu]$.

Sei $df = m$ und $a = zd$. Die Lösungen erfüllen auch $[z]_f[x]_f = [w]_f$. Wegen $g.g.T(f,z) = 1$ gilt $[x]_f = [z]_f^{-1}[w]_f$. Die Menge $\{[x] \in \mathbb{Z}/(m) | [x]_f = [z]_f^{-1}[w]_f\}$ hat d Elemente. □

Wir geben uns jetzt $m_1, \ldots, m_r \in \mathbb{Z}$ paarweise teilerfremd vor. Seien weiter $a_1, \ldots a_r \in \mathbb{Z}$ gegeben.

Satz 3.56 (Chinesischer Restsatz). *Es existiert ein $x \in \mathbb{Z}$ mit*

$$x \equiv a_i (\mod m_i) \quad i = 1, \ldots r \, .$$

Die Klasse $[x] \in \mathbb{Z}/(m)$ ist eindeutig bestimmt mit $m = m_1 \ldots m_r$.

Proof. Es reicht, das folgende Problem zu lösen:

$$x \equiv 1 (\mod m_1) \text{ und } x \equiv 0 (\mod m_i) \quad i > 1 \, .$$

Sei $nm_1 = m$. Dann gilt $g.g.T.(n, m_1) = 1$. Sei $qm_1 \equiv 1 (\mod n)$. Setze $x = qn$.

Wenn x, y Lösungen sind, dann gilt $m_i | (x - y)$, $i = 1, \ldots r$. Daraus folgt $m | x - y$. □

Dieser Satz gilt für jeden Hauptidealring an der Stelle von Z mit dem gleichen Beweis. Wir haben folgende Konsequenz.

Folgerung 3.57. *Die Abbildung*

$$x \mapsto ([x]_{m_1}, \ldots, [x]_{m_r})$$

induziert einen Isomorphismus

$$\mathbb{Z}/(m) \xrightarrow{\sim} \mathbb{Z}/(m_1) \times \cdots \times \mathbb{Z}/(m_r) \, .$$

3.4.2 Die Einheiten in $\mathbb{Z}/(m)$

Sei $m \in \mathbb{Z}$. Die Einheiten von $\mathbb{Z}/(m)$ sind genau die Klassen $[a]$ mit $g.g.T(a,m) = 1$.

Definition 3.58. *Wir definieren* $\varphi(m) \in \mathbb{N}$ *als die Anzahl der Einheiten in* $\mathbb{Z}/(m)$.

Es gilt offensichtlich

1. $\varphi(1) = 1$.
2. $\varphi(p) = p - 1$ für eine Primzahl $m := p \in \mathbb{Z}$.
3. $\varphi(p^n) = p^{n-1}(p-1)$ für eine Primzahl $p \in \mathbb{Z}$.

(In 3. beschreibt $\varphi(p^n)$ die Menge aller Klassen $[a]$, wobei a kein Vielfaches von p ist.)

Lemma 3.59. *Es gilt* $\varphi(m) = m\prod_{p|m}(1-\frac{1}{p})$.

Proof. Sei $m := \prod_{i=1}^{r} p_i^{l_i}$. Sei $M := \{1,\ldots,m\}$ und sei $M_i \subset M$ die Menge aller durch p_i teilbaren Zahlen. Sei $V := M \setminus \{M_1 \cup \ldots M_r\}$. Dann ist $\varphi(m) = |V|$. Wir haben

$$\begin{aligned} |V| &= |M| - \sum_i |M_i| + \sum_{i<j} |M_i \cap M_j| \\ &\quad - \sum_{i<j<k} |M_i \cap M_j \cap M_k| + \cdots + (-1)^r |M_1 \cap \cdots \cap M_r| \\ &= m - \sum_i \frac{m}{p_i} + \sum_{i<j} \frac{m}{p_i p_j} \\ &\quad - \sum_{i<j<k} \frac{m}{p_i p_j p_k} + \cdots + (-1)^r \frac{m}{p_1 \cdots p_r} \\ &= m \prod_i (1 - \frac{1}{p_1}) \; . \end{aligned}$$

□

Folgerung 3.60. *Wenn* $g.g.T(m,n) = 1$, *so gilt* $\varphi(mn) = \varphi(m)\varphi(n)$.

Lemma 3.61 (Euler-Fermat). *Sei* $m \in \mathbb{Z}$ *und* $a \in \mathbb{Z}$ *prim zu m. Dann gilt* $a^{\varphi(m)} \equiv 1 (\mod m)$.

Proof. Es gilt $|Z/(m)^*| = \varphi(m)$. Da $[a] \in Z/(m)^*$, so gilt $[a]^{\varphi(m)} = 1$. □
(Bemerkung: Sei G abelsch mit $|G| = m$. Dann ist $g^m = 1$ für jedes $g \in G$. In der Tat ist $\prod_{a\in G} a = \prod_{a\in G}(ga) = g^m \prod_{a\in G}\cdot$)

Folgerung 3.62 (Fermat). *Für eine Primzahl* $p \in \mathbb{Z}$ *und jedes* $a \in \mathbb{Z}$ *mit* $p \not| a$ *gilt* $a^p \equiv a (\mod (m)$.

Sei q prim und $F_q = \mathbb{Z}/(q)$.

Lemma 3.63. *Die Gruppe der Einheiten $\mathbb{F}_q^*$ ist zyklisch.*

Proof. Sei $|\mathbb{F}_q^*| = \prod_p p^{e_p}$ die Primzerlegung. Dann haben wir einen Isomorphismus

$$\prod_p G_{p^e} \cong \mathbb{F}_q^* ,$$

wobei G_{p^e} eine p-Gruppe ist und vorerst jede Primzahl mehrfach vorkommen kann.

Sei $G \subset \mathbb{F}_q^*$ eine Untergruppe der Ordnung p. Dann gilt $x^p = 1$ für alle $x \in G$. Diese Gleichung hat höchstens p Lösungen. Also ist $G \subset G_{p^e}$ durch p eindeutig bestimmt. Es folgt, daß G_{p^e} zyklisch ist. Damit ist aber $\mathbb{F}_q$ zyklisch. □

Aufgabe 3.12. *Finden Sie ein Erzeugendes von $\mathbb{F}_p^*$ für $p = 97$ und $p = 13$.*

Lemma 3.64. *Sei K ein Körper und $U \subset K^*$ endlich. Dann ist U zyklisch.*

Proof. Argument wie für . $|U| = \prod_p p^{e_p}$, $U \cong \prod_p G_{p^e}$. $G \subset U$ ist durch $|G| = p$ eindeutig. □

3.4.3 Bestimmung von Inversen

Wir zeigen nun, wie man Inverse in $\mathbb{Z}/(m)^*$ mit dem Euklidischen Algorithmus bestimmen kann.

Sei a zu m teilerfremd. Dann ist $[a] \in \mathbb{Z}/(m)^*$. Wir suchen $[b] \in Z/(m)^*$ mit $[a][b] = 1$, also $1 = ab + rm$. Wir benutzen dazu den Euklidischen Algorithmus. Seien $u, v \in \mathbb{Z}$ vorgegeben. Dann liefert der Algorithmus eine Folge $F(u,v) := (w_n)$ durch folgende Vorschrift

1. $w_1 := u$
2. $w_2 := v$
3. Bestimme w_{n+2} durch $w_n = x_{n+1} w_{n+1} + w_{n+2}$ mit $0 \leq w_{n+3} < |w_{n+1}|$.

Wir haben

$$\begin{aligned} w_n &= w_{n-2} - x_{n-1}w_{n-1} \\ &= w_{n-2} - x_{n-1}(w_{n-3} - x_{n-2}w_{n-2}) \\ &= (1+x_{n-2})w_{n-2} - x_{n-1}w_{n-3} \\ &= (1+x_{n-2})(w_{n-4} - x_{n-3}w_{n-3}) - x_{n-1}w_{n-3} \\ &= (1+x_{n-2})w_{n-4} - ((1+x_{n-2})x_{n-3} + x_{n-1})w_{n-3} \\ &\vdots \\ &= c_1w_1 + c_2w_2 \ . \end{aligned}$$

Wir betrachten nun die Folge $(w_n) = F(m,a)$. Wegen $g.g.T.(m,a) = 1$ gilt $w_n = 1$ für ein geeignetes n. Mit dem obigen Verfahren erhalten wir

$$1 = c_1m + c_2a \ .$$

Also gilt für $[c_2][a] = 1$ in $\mathbb{Z}/(m)$.

Beispiel: $m = 37$ und $a = 12$. Wir rechnen

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4$, $x_2 = 3$, $w_3 = 4$
4. $11 = 2.4 + 3$, $x_3 = 2$, $w_4 = 3$
5. $4 = 1.3 + 1$, $x_4 = 1$, $w_5 = 1$

Wir haben also $n = 5$

$$1 = (1+2)37 - ((1+2)3+1)11 = 3.37 - 10.11$$

Also gilt $[10]_{37}[11]_{37} = [1]_{37}$.

Aufgabe 3.13. *Bestimmen Sie ein Inverses von* $[7]_{71}$ *in* $\mathbb{Z}/(71)$.

3.4.4 Der RSA-Algorithmus

Bob will Nachrichten empfangen. Jeder Sender soll in die Lage versetzt werden, zu verschlüsseln, jedoch soll nur Bob entschlüsseln können.

Bob geht wie folgt vor.

Er bestimmt zwei sehr große Primzahlen p,q und setzt $m = pq$. Er berechnet $\varphi(m) = (p-1)(q-1)$. Die Nachrichten werden Elemente $[x]_m \in \mathbb{Z}/(m)$sein für welche x klein gegen p,q ist. Solche x sind dann prim zu p,q.

Bob bestimmt weiter eine Zahl e mit $g.g.T(e,\varphi(m))$. Er kann mit dem euklidischen Algorithmus ein d finden so daß

$$[e]_{\varphi(m)}[d]_{\varphi(m)} = [1]_{\varphi(m)} \ .$$

Bob veröffentlicht nun das Paar (m,e).

Alice möchte Bob eine Nachricht $x \in \mathbb{Z}/(m)$ übermitteln. Sie kennt (wie alle Mithörer) das Paar (m,e). Sie wird $y := x^e$ senden.

Um zu entschlüsseln, bildet Bob $z := y^d$. Da x zu $m = pq$ prim ist, gilt in $\mathbb{Z}/(m)$

$$z = x^{ed} = x^{1+\varphi(m)r} = x \ \ .$$

Warum können die Mithörer den Wert von x nicht bestimmen. Das liegt daran, daß sie zwar m, aber nicht p und q kennen und damit $\varphi(m)$ nicht berechnen können und folglich d nicht zur Verfügung haben. Die Sicherheit des Verfahrens beruht auf der Schwierigkeit, die Primfaktoren von m zu bestimmen und auf der Schwierigkeit, in $\mathbb{Z}/(m)$ eine e-te Wurzel zu finden.

Aufgabe 3.14. *Bob veröffentlicht* $m := 492929$ *und* $e := 7$. *Ein Angreifer fängt die Nachricht* 170859375 *von Alice ab. Welchen Inhalt hatte sie ?*

3.5 Algebraische Gleichungen

3.5.1 Reduktion modulo m

Wir betrachten ein Polynom $f(x_1,\ldots,x_n)$ mit ganzen Koeffizienten. Dann ergibt sich die Frage, ob die Gleichung $f = 0$ ganzzahlige Lösungen $(a_1,\ldots,a_n) \in \mathbb{Z}^n$ besitzt.

Sei $m \in \mathbb{Z}$. Wir können die Reduktion $[f]_m$ von f modulo m betrachten. Sei

$$N_f(m) := \sharp\{([a_1]_m, \ldots, [a_n]_m) \in (\mathbb{Z}/(m))^n | [f]_m([a_1]_m, \ldots, [a_n]_m) = 0\} .$$

Wenn $f = 0$ eine ganze Lösung $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ hat, dann ist $([a_1]_m, \ldots, [a_n]_m)$ eine Lösung von $[f]_m = 0$.

Lemma 3.65. *Eine notwendige Bedingung für die Lösbarkeit von $f = 0$ ist die Lösbarkeit von $[f]_m = 0$ für alle $m \in \mathbb{N}$.*

Sei $m = m_1 m_2$ und $g.g.T.(m_1, m_2) = 1$.

Lemma 3.66. *Es gilt $N_f(m) = N_f(m_1)N_f(m_2)$.*

Proof. Der chinesische Restsatz gibt einen Isomorphismus

$$\mathbb{Z}/(m) \cong Z/(m_1) \times \mathbb{Z}/(m_2) .$$

Wir erhalten einen induzierten Isomorphismus

$$\{[f]_m = 0\} \cong \{[f_{m_1} = 0\} \times \{[f]_{m_2} = 0\} .$$

□

Sei $m = \prod_p p^{e_p}$ die Primfaktorenzerlegung.

Lemma 3.67. *Es gilt*

$$N_f(m) = \prod_p N_f(p^{e_p}) .$$

3.5.2 Mehr über $N_f(p^e)$

Wir betrachten dazu zwei Beispiele.

Sei $f(x) = x^2 + 1$ und $p = 5$. Dann ist $\{[f]_5 = 0\} = \{[2]_5, [-2]_5\}$. Wir setzen $x_0 = 2$. Wir suchen ein Element von $\{[f]_{5^2} = 0\}$ der Form $[x_0 + 5x_1]_{5^2}$. Einsetzen ergibt

$$0 \equiv (2 + 5x_1)^2 + 1 \equiv 4 + 20x_1 + 1 \equiv 5(1 + 4x_1) \mod 5^2 .$$

Wir finden $x_1 = 1$. Wir suchen nun ein Element von $\{[f]_{5^3} = 0\}$ der Form

$$[x_0 + 5x_1 + 5^2 x_2]_{5^3} .$$

Einsetzen ergibt

$$0 \equiv 49 + 100x_2 + 1 \equiv 25(2 + 4x_3) \mod 5^3 .$$

Wir finden $x_3 = 2$.

Wenn wir eine Lösung $[f]_{5^e}([a]_{p^e}) = 0$ mit $[a]_5 = 2$ haben, dann machen wir den Ansatz $b = a + 5^e x_e$ für eine Lösung von $[f]_{5^{e+1}}([b]_{p^{e+1}})$. Wir erhalten

$$0 \equiv a^2 + 25^e a x_e + 1 \equiv 5^e(c + 4x_e)$$

mit $c = (a^2+1)/5^e$. Wegen $g.g.T.(4,5) = 1$ existiert eine Lösung x_4 von $c + 4x_e \equiv 0 \mod 5$. Wir können o.B.d.A $x_e \in \{0, 1, \ldots 4\}$ nehmen.

Wenn wir dieses Verfahren fortsetzen, so erhalten wir eine Lösung

$$a = x_0 + x_1 5 + x_2 5^2 + x_3 5^3 \ldots$$

von $[f]_{5^\infty}([a]_{5^\infty}) = 0$, wobei diese Aussage präziese mit der Konvergenz in den 5-adischen Zahlen verstanden werden kann.

Wir betrachten nun die gleiche Gleichung $f(x) = x^2 + 1$ für $p = 2$. Wir wählen $x_0 := 1$ und machen den Ansatz $b = x_1 + 2x_2$ für eine Lösung von $[f]_{2^2}([b]_{2^2}) = 0$. Es ergibt sich

$$0 \equiv 1 + 4x_2 \mod 2^2 .$$

Diese Bedingung hat keine Lösung.

Der Unterschied der beiden Fälle ist der folgende. Es gilt

$$[f']_5(2) = [4]_5 \neq 0$$

aber

$$[f']_2(1) = [0]_2 .$$

Lemma 3.68. *Sei $p \in \mathbb{Z}$ prim, $n, k \in \mathbb{N}$, $0 \leq 2k < n$, und $f \in \mathbb{Z}[x]$. Sei weiterhin $x \in \mathbb{Z}$ mit*

$$\begin{aligned} f(x) &\equiv 0 \mod p^n \\ f'(x) &\equiv 0 \mod p^k \\ f'(x) &\not\equiv 0 \mod p^{k+1} . \end{aligned}$$

Dann gibt es ein modulo p^{n-k+1} eindeutig bestimmtes $y \in \mathbb{Z}$ derart, daß

$$\begin{aligned} f(y) &\equiv 0 \mod p^{n+1} \\ f'(y) &\equiv 0 \mod p^{k} \\ f'(x) &\not\equiv 0 \mod p^{k+1} \\ y &\equiv x \mod p^{n-k} . \end{aligned}$$

Proof. Wir setzen $y = x + zp^{n-k}$. Taylorentwicklung um x ergibt

$$f(y) = f(x) + p^{n-k} z f'(x) + r p^{2(n-k)} .$$

Es folgt wegen $n+1 \leq 2(n-k)$

$$f(y) \equiv f(x) + p^{n-k} z f'(x) \mod p^{n+1} .$$

Wir schreiben $f(x) = p^n b$ und $f'(x) = p^k c$ mit $p \not| c$. Dann gilt

$$f(y) \equiv p^n (b + zc) \mod p^{n+1} .$$

Also muß $b + zc \equiv 0 \mod p$ gelten, wodurch z eindeutig $\mod p$ bestimmt wird. □

3.5.3 Quadratische Reste

Wir betrachten die Gleichung

$$x^2 - a \equiv 0 \mod m$$

unter der Voraussetzung $g.g.T.(m,a) = 1$.

Definition 3.69. *Wenn diese Gleichung eine Lösung hat, so heißt a quadratischer Rest (QR) modulo m. Andernfalls ist a ein quadratischer Nichtrest (QNR) modulo m*

Sei $m = \prod_p p^{e_p}$ die Primzerlegung von m.

Lemma 3.70. *1. a ist QR modulo m genau dann, wenn a ein QR modulo p^{e_p} für alle Primfaktoren p von m ist.*

2. Ist $p > 2$, dann ist a ein QR modulo p^e genau dann, wenn a ein QR modulo p ist.

3. *Ist $p = 2$, dann ist a ein QR modulo 2^e genau dann, wenn a ein QR modulo $2^{\min(e,3)}$ ist.*

Proof. 1. folgt aus 3.66.

Für $f(x) = x^2 - a$ gilt $f'(x) = 2x$. Ist $y^2 - a \equiv 0 \mod p$, so gilt $f'(y)y \equiv 2a \mod p$, also $f'(y) \not\equiv 0 \mod p$ für $p > 2$. Die 2. Behauptung folgt aus 3.68.

Ist $p = 2$, so gilt $f'(y) = 2y \equiv 0 \mod 2$. Ist $y^2 - a \equiv 0 \mod 4$, so gilt $f'(y)y \equiv 2a \mod 4$, also $f'(y) \not\equiv 0 \mod 4$.

Wenn $e > 3$ ist, dann wenden wir 3.68 für $n \geq e$ und $k = 1$ an. □

Es ergeben sich die folgenden Fragen:

1. Gegeben sei eine Primzahl $p > 2$. Bestimme die QR modulo p.
2. Gegeben sei a. Bestimme alle p, für welche a ein QR modulo p ist.

Sei $a, p \in \mathbb{Z}$, $p \neq 2$ eine Primzahl, und $p \not| a$.

Definition 3.71. *Das Legendresymbol wird durch*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ ist QR modulo } p \\ -1 & a \text{ ist QNR modulo } p \end{cases}$$

definiert.

Offensichtlich hängt $\left(\frac{a}{p}\right)$ nur von $[a]_p$ ab.

Lemma 3.72. *1.* **[Eulerkriterium]** *Es gilt*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p\ .$$

2. *Wenn a, b prim zu p sind, dann gilt*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)\ .$$

Proof. Wir betrachten den Homomorphismus. $\phi : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $\phi(x) := x^2$. Es gilt $\mathtt{ker}(\phi) = \{[1]_p, [-1]_p\}$. Das Bild von ϕ ist die Untergruppe der quadratischen Reste modulo p. Es gilt $[\mathbb{F}_p^* : \mathtt{im}(\phi)] = 2$. Wir erhalten somit einen Isomorphismus

$$\psi : \mathbb{F}_p^*/\mathtt{im}(\phi) \xrightarrow{\sim} \{1, -1\} .$$

Es gilt nach Definition

$$\psi([a]) = \left(\frac{a}{p}\right) .$$

Es folgt 2.

Wir betrachten nun den Homomorphismus $\kappa : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $\kappa(x) := x^{\frac{p-1}{2}}$. Es gilt (nach 3.62) $\kappa(x)^2 = x^{p-1} = 1$. Folglich ist $\kappa(x) \in \{1, -1\}$.

Die Gruppe $\mathbb{F}_p^*$ ist zyklisch (3.4.2) und hat damit nur eine Untergruppe vom Index 2. Da $[\mathbb{F}_p^* : \mathtt{ker}(\kappa)] = 2$ gilt, muß $\mathtt{ker}(\kappa) = \mathtt{im}(\phi)$ gelten. Dies zeigt 1. □

3.5.4 Das quadratische Reziprozitätsgesetz

Sei $2 \neq p \in \mathbb{Z}$ prim. Sei $a = (-1)^\nu \prod_q q^{e_q}$. Dann gilt

$$\left(\frac{a}{p}\right) = \left(\frac{(-1)^\nu}{p}\right) \left(\frac{2}{p}\right) \prod_{p \neq 2} \left(\frac{q}{p}\right) .$$

Die ersten beiden Faktoren berechnen wir direkt in den folgenden beiden Sätzen. Die restlichen sind Objekt des quadratischen Reziprozitätsgesetzes.

Lemma 3.73 (1. Ergänzungssatz). *Es gilt* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Proof. Eulerkriterium 3.72. □

Lemma 3.74 (2. Ergänzungssatz). *Es gilt* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof. Nach dem Eulerkriterium gilt

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \mod p .$$

Wir benutzen nun die folgende Aussage (welche wir später beweisen werden).

Es gibt eine Körpererweiterung $\mathbb{F}_p \subset L$ derart, daß L eine primitive achte Einheitswurzel ζ enthält.

Es gilt also $\zeta^8 = 1$, $\zeta^4 = -1$ und $\zeta^2 = -\zeta^{-2}$. Wir setzen $\alpha := \zeta - \zeta^{-1}$. Dann gilt $\alpha^2 = \zeta^2 + \zeta^{-2} + 2 = 2$.

Da L die Charakteristik p hat, ist $x \mapsto x^p$ ein Automorphismus. Es gilt $\alpha^p = \zeta^p + \zeta^{-p}$. Wenn $p \equiv \pm 5 \mod 8$, dann ist $\alpha^p = -\alpha$, und wenn $p \equiv \pm 1 \mod 8$, dann ist $\alpha^p = \alpha$. Folglich gilt

$$\alpha^{p-1} = (-1)^{\frac{p^2-1}{8}} .$$

Wir schließen (in L)

$$2^{\frac{p-1}{2}} = \alpha^{p-1} = (-1)^{\frac{p^2-1}{8}} .$$

□

Satz 3.75 (Quadratisches Reziprozitätsgesetz). *Seien p, q verschiedene ungerade Primzahlen. Dann gilt*

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

Proof. Nach dem Eulerkriterium gilt

$$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \mod p .$$

Wir werden (in einem Erweiterungskörper L) ein α konstruieren mit

$$\alpha^2 = (-1)^{\frac{q-1}{2}} q \quad , \alpha^{p-1} = \left(\frac{p}{q}\right) .$$

Dann folgt (in L)

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

Wir benutzen einen Erweiterungskörper $\mathbb{F}_p \subset l$, welcher eine primitive q-te Einheitswurzel ζ enthält. Es gilt (diese Zahl erfüllt $\zeta x = x$)

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

Wir setzen $\left(\frac{0}{p}\right) := 0$ (in den Symbolen und im Exponenten von ζ rechnen wir in $\mathbb{F}_q$ und außen in L) und definieren

$$\alpha := \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \zeta^x .$$

$$\begin{aligned}\alpha^2 &= \sum_{x,y\in\mathbb{F}_p}\left(\frac{xy}{q}\right)\zeta^{x+y}\\ &= \sum_{u\in\mathbb{F}_q}\zeta^u\left(\sum_{x\in\mathbb{F}_q}\left(\frac{x(u-x)}{q}\right)\right).\end{aligned}$$

Für $x\neq 0$ gilt

$$\left(\frac{x(u-x)}{q}\right)=\left(\frac{-x^2}{q}\right)\left(\frac{1-x^{-1}u}{q}\right)=(-1)^{\frac{q-1}{2}}\left(\frac{1-x^{-1}u}{q}\right).$$

Also $\alpha^2=(-1)^{\frac{q-1}{2}}\sum_{u\in\mathbb{F}_q}c_u\zeta^u$ mit

$$c_u=\sum_{x\in\mathbb{F}_q^*}\left(\frac{1-x^{-1}u}{q}\right).$$

Falls $u=0$, so $c_u=q-1$. Wenn $u\neq 0$, so durchläuft $1-x^{-1}u$ genau $\mathbb{F}_q\setminus\{1\}$. Die Anzahl der QR wie QNR ist $\frac{q-1}{2}$. Es gilt daher $c_u=-1$. Damit

$$\alpha^2=(-1)^{\frac{q-1}{2}}(q-1-\sum_{x\in\mathbb{F}_q^*}\zeta^x)=(-1)^{\frac{q-1}{2}}q\,.$$

Wir rechnen nun

$$\begin{aligned}\alpha^p &= \sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)^p\zeta^{px}\\ &= \sum_{u\in\mathbb{F}_q}\left(\frac{p^{-1}x}{q}\right)\zeta^u\\ &= \left(\frac{p^{-1}}{q}\right)\alpha\\ &= \left(\frac{p}{q}\right)\alpha\end{aligned}$$

□

3.5.5 Anwendung des Quadratischen Reziprozitätsgesetzes

Ist 37 ein QR bezüglich 103 ? Wir berechnen

$$\begin{aligned}\left(\frac{37}{103}\right) &= \left(\frac{103}{37}\right)\\ &= \left(\frac{29}{37}\right)\\ &= \left(\frac{37}{29}\right)\\ &= \left(\frac{8}{29}\right)\\ &= \left(\frac{2}{29}\right)\\ &= -1\,.\end{aligned}$$

Hier ist ein anderes Beispiel. Ist 24 ein QR bezüglich 31 ?

$$\begin{aligned}\left(\frac{24}{31}\right) &= \left(\frac{2^3}{31}\right)\left(\frac{3}{31}\right)\\ &= \left(\frac{2}{31}\right)\left(\frac{3}{31}\right)\\ &= -\left(\frac{31}{3}\right)\\ &= -\left(\frac{1}{3}\right)\\ &= -1\end{aligned}$$

Hier sind die Quadrate $\mod 31$

$$\{1,4,9,16,25,5,18,2,10,7,28,20,14,10,8\}\,.$$

Wir rechnen

$$\begin{aligned}\left(\frac{10}{31}\right) &= \left(\frac{2}{31}\right)\left(\frac{5}{31}\right)\\ &= \left(\frac{5}{31}\right)\\ &= -\left(\frac{31}{5}\right)\\ &= \left(\frac{1}{5}\right)\\ &= 1\end{aligned}$$

Aufgabe 3.15. *Untersuchen Sie, ob* 14 *ein QR bezüglich* 310 *ist.*

3.5.6 Verzweigung von Primzahlen in $\mathbb{Z}[\sqrt{D}]$

Sei $D \in \mathbb{Z}$ quadratfrei und

$$R := \begin{cases} \mathbb{Z}[\sqrt{D}] & D \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases} .$$

Wir nehmen an, daß R faktoriell ist. Wenn $D < 0$, dann gilt

$$D \in \{-1,-2,-3,-5,-7,-11,-19,-43,-67,-163\} .$$

Es wird vermutet, daß R für undendlich viele $D > 0$ faktoriell ist.

Wir setzen

$$d := \begin{cases} & 4D \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases} .$$

Lemma 3.76. *Eine Primzahl $p \in \mathbb{Z}$ ist genau dann träge in R, wenn $p \nmid d$ und d ein QR modulo p ist.*

Proof. Wir betrachten den Fall $D \not\equiv 1 \mod 4$. Sei $p \in \mathbb{Z}$ prim, $p \neq 2$.

Sei p nicht träge, also $p = \pi\bar{\pi}$, $\pi = a + b\sqrt{D}$. Es gilt nicht $p|a$ und $p|b$ (sonst wäre π nicht prim). Dann gilt $N(\pi) = p = a^2 - Db^2$. Es folgt

$$a^2 \equiv Db^2 \mod p .$$

Damit gilt $p \nmid d$ und d ist ein QR modulo p oder aber $p|d$.

Sei nun umgekehrt $p \nmid d$ und d ein QR modulo p. Dann ist d und auch D ein QR modulo p^2. Wir betrachten eine Lösung $x \in \mathbb{Z}$ von $x^2 \equiv D \mod p^2$. Es gilt $p \nmid x$, da andernfalls $p^2|D$, also D nicht quadratfrei wäre. Es gilt

$$p|(x+\sqrt{D})(x-\sqrt{D}) .$$

Da $p \nmid x$, gilt $p \nmid (x+\sqrt{D})$ oder $p \nmid (x-\sqrt{D})$. Folglich muß sich p zerlegen in $p = \pi\bar{\pi}$, also ist p nicht träge.

Wenn $p|d$, dann gilt $p|\sqrt{D}\sqrt{D}$ und $p \nmid \sqrt{D}$. Wir schließen wieder, daß $p = \pi\bar{\pi}$, also p nicht träge ist.

Sei nun $p = 2$ und $2|(a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - Db^2$. Diese Gleichung kann man immer durch geeignete Wahl von a, b erfüllen. Wenn $D \equiv 1 \mod 2$, dann ist $a \equiv 1 \mod 2$

oder $b \equiv 1 \mod 2$. In beiden Fällen gilt $2 \not| (a + b\sqrt{D})$ und $2 \not| (a - b\sqrt{D})$. Folglich kann 2 nie träge sein.

Wir haben damit gezeigt, daß $p \in \mathbb{Z}$ genau dann träge ist, wenn $p \not| d$ und p ein *QNR* modulo d ist.

4 Körpererweiterungen

4.1 Konstruktion von Körpererweiterungen

4.1.1 Körpererweiterungen und Teilkörper

Sei K ein Körper.

Definition 4.1. *Unter einer Körpererweiterung von K verstehen wir einen Körper L mit einer Einbettung $K \hookrightarrow L$. In der Regel identifizieren wir K mit dem Bild dieser Einbettung.*

Sei $K \subset L$ eine Körpererweiterung. Dann ist L ein K-Vektorraum.

Definition 4.2. *Wir definieren den Grad dieser Erweiterung als*

$$[L : K] = \deg_K(L) := \dim_K(L) \ .$$

Lemma 4.3. *Ist $L \subset M$ eine Erweiterung, dann ist auch die Komposition $K \subset M$ eine Körpererweiterung und es gilt*

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

Es gilt $[L : K] = 1$ genau dann, wenn $L = K$.

Hier ist eine Konstruktion von Körpererweiterung.

Sei $k \subset K$ ein Teilkörper. Seien weiter $\alpha_1, \ldots, \alpha_r \in K$.

Definition 4.4. *Wir definieren den Körper $k(\alpha_1, \ldots, \alpha_r), \subset K$ als den kleinsten Unterkörper von K, welcher sowohl α_i, $i = 1, \ldots, r$ als auch k enthält.*

Es gilt also

$$k(\alpha_1,\ldots,\alpha_r) = \cap_l l \ ,$$

wobei l alle Unterkörper von K mit $k \cup \{\alpha_1,\ldots,\alpha_r\} \subset l$ durchläuft.

Sei $\alpha \in L$.

Lemma 4.5. *Es gilt* $k(\alpha) = \{\frac{g(\alpha)}{f(\alpha)} | f,g \in k[x], f(\alpha) \neq 0\}$.

Proof. Sei M die rechte Seite. Es gilt $M \subset k(\alpha)$. Wir müssen zeigen, daß M ein Körper ist. □

Sei $D \in \mathbb{Z}$ quadratfrei und $\alpha = \sqrt{D}$. Dann haben wir

$$\mathbb{Q}[\sqrt{D}] = \{a + b\alpha | a,b \in \mathbb{Q}\}$$

als Unterkörper $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{C}$ konstruiert.

4.1.2 Zerfällungskörper I

Sei $f \in K[x]$ ein nichtkonstantes Polynom und $K \subset L$. Wir betrachten $K[x] \subset L[x]$.

Definition 4.6. *f zerfällt über L, falls in $L[x]$ gilt*

$$f = \prod_{i=1}^{\deg(f)} (x - a_i) \ .$$

Jedes Polynom in $\mathbb{Q}[x]$ zerfällt über $\mathbb{C}$.

Definition 4.7. *Die Erweiterung $K \subset L$ heißt Zerfällungskörper von f, falls es keinen Zwischenkörper $K \subset M \subset L$ gibt, so daß f über M zerfällt.*

Sei $f = x^2 + 5 \in \mathbb{Q}[x]$. Dann zerfällt f über $\mathbb{Q}[\sqrt{-5}]$. Es gilt

$$f = (x - \sqrt{-5})(x + \sqrt{-5}) \ .$$

In der Tat ist dieser Körper ein Zerfällungskörper von f. Um dies einzusehen, betrachten wird den Grad der Erweiterung.

Sei $\mathbb{Q} \subset K \subset \mathbb{C}$ und $f \in K[x]$. Seien $\alpha_1,\ldots,\alpha_r$ die komplexen Nullstellen von f.

Lemma 4.8. *f zerfällt über der Erweiterung $K \subset K(\alpha_1,\ldots,\alpha_r) \subset \mathbb{C}$. Insbesondere besitzt f einen Zerfällungskörper $K \subset L \subset K(\alpha_1,\ldots,\alpha_r)$.*

Im nächsten Abschnitt werden wir diese Aussage auf beliebige Körper K verallgemeinern.

4.1.3 Adjunktion von Nullstellen

Sei K ein Körper. Dann ist $K[x]$ ein euklidisch und damit Hauptidealring. Ist $I \subset K[x]$ ein echtes Ideal, so gilt $I = (f)$ für ein geeignetes $f \in K[x]$. Sei

$$0 \to I \to K[x] \to K[x]/I \to 0 \; .$$

Lemma 4.9. *Der Ring $K[x]/I$ ist genau dann ein Körper, wenn f irreduzibel ist.*

Proof. Sei $0 \neq [g] \in K[x]/I$. Dann gilt $g.g.T(g,f) = 1$. Damit existieren $a,b \in K[x]$ mit $1 = ag + bf$. Folglich gilt $[a][g] = 1 \in K[x]/I$. □

Die Projektion $K \to K[x] \to K[x]/I$ ist eine Einbettung. Wir erhalten damit eine Körpererweiterung

$$K \subset K_f := K[x]/I \; .$$

Lemma 4.10. *Die Klassen der Polynome $[1],[x],\ldots,[x^{\deg(f)-1}]$ bilden eine Basis von K_f über K. Insbesondere gilt $[K_f : K] = \deg(f)$.*

Proof. O.B.d.A gilt $f = x^{\deg(f)} + a_{\deg(f)-1}x^{\deg(f)-1} + \cdots + a_0$, also

$$[x^{\deg f}] = -a_{\deg(f)-1}[x^{\deg(f)-1}] - \cdots - a_0 \; .$$

Sei $m \geq \deg(f)$. Dann schreiben wir $[x^m] = [x^{m-\deg(f)}](-a_{\deg(f)-1}[x^{\deg(f)-1}] - \cdots - a_0)$. Wir sehen induktiv, daß man alle $[x^m]$ für $m \geq \deg(f)$ als Linearkombinationen der Klassen $[1],[x],\ldots,[x^{\deg(f)-1}]$ schreiben kann.

Andererseits sind $[1],[x],\ldots,[x^{\deg(f)-1}]$ linear unabhängig. In der Tat, wenn

$$c_1 + \cdots + c_{\deg(f)-1}x^{\deg(f)-1} = gf \; ,$$

dann ist $c_i = 0$ für alle $i = 0,\ldots,\deg(f)-1$. □

Wir betrachten die Erweiterung $K \subset K_f$ für ein irreduzibles $f \in K[x]$. Sei $\alpha = [x] \in K_f$.

Lemma 4.11. *Es gilt in K_f daß $f(\alpha) = 0$.*

Lemma 4.12. *Sei K ein Körper und $f \in K[x]$. Dann existiert eine Erweiterung $K \subset L$ so daß f über L zerfällt. In der Tat kann man L mit $[L : K] < \deg(f)!$ finden.*

Proof. Wir führen Induktion nach $\deg(f)$ durch. Sei $f = pq$ mit irreduziblen q. Dann gilt in $K_q[x]$ daß $q = gh$, wobei g zerfällt und $\deg(ph) = \deg(f) - \deg(g)$. Nach Induktionsvoraussetzung gibt es eine Erweiterung $K_q \subset L$ mit $[L : K_q] < (\deg(f) - \deg(g))!$ derart, daß ph über L zerfällt. Damit zerfällt auch f über L. Es gilt

$$[L : K] = [L : L_q][L_q : K] \leq (\deg(f) - \deg(g))!\deg(q) \leq \deg(f)! \; .$$

□

4.1.4 Zerfällungskörper II

Sei K ein Körper und $f \in K[x]$ irreduzibel. Sei $K \subset L$ eine Erweiterung und $\alpha \in L$ eine Nullstelle von f. Wir erhalten einen Homomorphismus $\phi_\alpha : K_f \to K(\alpha)$ durch

$$\phi_\alpha([g]) := g(\alpha) \; .$$

Lemma 4.13. *$\phi_\alpha : K_f \to K(\alpha)$ ist ein Isomorphismus.*

Proof. K_f ist Körper. Daraus folgt die Injektivität. Es gilt $\alpha \in \mathtt{im}(\phi_\alpha)$, $K \subset \mathtt{im}(\phi_\alpha)$. Da $K(\alpha)$ minimal mit $K \subset K(\alpha)$ und $\alpha \in K(\alpha)$ ist, folgt die Surjektivität von ϕ_α. □

Sei $\phi : K \to K'$ ein Isomorphismus. Sei f' das Bild von f unter dem induzierten Isomorphismus $\Phi : K[x] \to K'[x]$. Sei $K' \subset L'$ eine Erweiterung von K' und α' eine Nullstelle von f'.

Beachte, daß es keine Beziehung zwischen L und L' geben muß.

Lemma 4.14. *Es gibt genau eine Ausdehnung $\hat{\phi} : K(\alpha) \to K'(\alpha')$ von ϕ mit $\phi(\alpha) = \alpha'$.*

Proof.

$$\hat{\phi} : K(\alpha) \xrightarrow{\sim} K_f \xrightarrow{\bar{\Phi}} K'_{f'} \xrightarrow{\sim} K'(\alpha') \; .$$

□

Lemma 4.15. *Sei $f \in K[x]$, $\phi : K \to K'$ ein Isomorphismus, und $\Phi : K[x] \to K'[x]$ seine Ausdehnung. Seien $K \subset L$ und $K' \subset L'$ Zerfällungskörper von f und $\Phi(f)$. Dann existiert ein Isomorphismus $\psi : L \to L'$ mit $\psi_{|K} = \phi$ derart, daß $\phi(\{\alpha \in L | f(\alpha) = 0\}) = \{\alpha' \in L' | f(\alpha') = 0\}$.*

Proof. Induktion nach der Anzahl $r_{L,K}(f)$ der Nullstellen von f in $L \setminus K$. Für $r = 0$ ist die Aussage klar.

Sei $\alpha \in L$ Nullstelle von f. Sei $f = gh \in K[x]$ derart, daß g irreduzibel und $g(\alpha) = 0$. Sei $\alpha' \in L'$ Nullstelle von $\Phi(g)$ in L'. Wir erhalten $\tilde{\psi} : K(\alpha) \to K'(\alpha')$ derart mit $\tilde{\psi}_{|K} = \phi$. Es gilt $r_{L,K(alpha)}(f) < r_{L,K}(f)$. Wir ersetzen nun K, K' durch $K(\alpha), K'(\alpha')$. Nach Induktionsvoraussetzung finden wir die weitere Ausdehnung ψ. □

Folgerung 4.16. *Ist $f \in K[x]$ und sind $K \subset L$ und $K \subset L'$ zerfällungskörper von f. Dann gibt es einen Isomorphismus $\phi : L \to L'$ mit $\phi | K = \mathtt{id}_K$.*

4.2 Irreduzible Polynome

4.2.1 Primitive Elemente

Wir haben desöfteren vorausgesetzt, daß $f \in K[x]$ irreduzibel sei. Im folgenden wollen einige Methoden kennenlernen, mit denen man diese Voraussetzung nachprüfen kann.

Sei $R \subset K$ ein faktorieller Unterring mit $K = \{\frac{a}{b} | a, b \in R, b \neq 0\}$. Sei $f = a_n x^n + \cdots + a_0$.

Definition 4.17. *Der Inhalt von f sei $I(f) = g.g.T.(a_0, \ldots, a_n)$. Wenn $I(f) = 1$, so nennen wir f primitiv.*

Lemma 4.18. *Es gilt $I(fg) = I(f)I(g)$.*

Proof. Sei $a \in I(f)$ und $b \in I(g)$, $f = af_0$ und $g = bg_0$. Dann sind f_0 und g_0 primitiv. Es genügt zu zeigen, daß $f_0 g_0$ primitiv ist.

Sei $p \in R$ prim. Seien $f_0 = a_n x^n + \cdots + a_0$ und $g_0 = b_m x^m + \cdots + b_0$. Seien l, k minimal mit $p \not| a_k$ und $p \not| b_l$. Sei $fg = c_{n+m} x^{n+m} + \cdots + c_0$. Dann gilt $c_{l+k} = \sum_{i+j=l+k} a_i b_j$. Es gilt $p \not| c_{l+k}$.

Also muß $f_0 g_0$ primitiv sein. □

Lemma 4.19. *Wenn $h \in K[x]$, $g \in R[x]$ primitiv und $f = gh \in R[x]$ ist, dann gilt $h \in R[x]$.*

Proof. Wenn $f = 0$, so gilt $h = 0$. Wenn $f \neq 0$, dann gilt $f = af_0$, f_0 primitiv. Sei $k \in R$ derart, daß $kh \in R[x]$. Wir schreiben $kh = dh_0$ mit $I(h_0) = 1$. Dann gilt $akf_0 = kf = kgh = dgh_0$. Es folgt $ak \in I(kf) = I(dgh_0) = dI(gh_0) = d$. Also gilt $k|d$. Wir schließen $h = \frac{d}{k} h_0 \in R[x]$. □

Lemma 4.20. *Ist $f \in R[x]$ irreduzibel, so auch in $K[x]$.*

Proof. Sei $f \in R[x]$ irreduzibel. Dann ist f primitiv. Sei $f = gh \in K[x]$. Dann gilt $\deg(g) > 0$ und $\deg(h) > 0$. Sei $g = rg_0$, $r \in K$, g_0 primitiv. Dann gilt $f = (rh)g_0$. Folglich $rh \in R[x]$. Dann wäre aber f nicht in $R[x]$ irreduzibel. □

4.2.2 Satz von Gauß

Sei R ein faktorieller Ring.

Lemma 4.21. *$R[x]$ is faktoriell.*

Proof. In R gilt der Teilerkettensatz. Damit gilt er auch in $R[x]$. Wir müssen zeigen, daß jedes irredzible Element $f \in R[x]$ prim ist. f ist primitiv und in $K[x]$ irreduzibel. Da $K[x]$ ein Hauptidealring und damit faktoriell ist, ist f in $K[x]$ prim.

Sei $f|gh$ in $K[x]$ mit $g, h \in R[x]$. Dann gilt $f|g$ oder $f|h$. Sei also $g = fl$ mit $l \in K[x]$. Dann gilt bereits $l \in R[x]$. Also $f|g$ in $R[x]$. □

So ist z.B. der Ring $\mathbb{Z}[x]$ faktoriell.

4.2.3 Kriterien für Irreduzibilität

Wir betrachten zuerst das Eisensteinkriterium. Sei R faktoriell mit dem Quotientenkörper K. Sei $p \in R$ prim und $f = a_n x^n + \cdots + a_0 \in R[x]$, $n > 0$. Es gelte $p|a_0, \ldots, p|a_{n-1}$ und $p^2 \not| a_0$ und $p \not| a_n$.

Lemma 4.22. *f ist in $K[x]$ irreduzibel.*

Proof. Zeigen, daß $f \in R[x]$ irreduzibel ist.

Sei $f = gh$ echte Zerlegung, $\deg(g) > 0$ und $\deg(h) > 0$. Sei $g = b_m x^m + \cdots + b_0$ und $h = c_l x^l + \cdots + c_0$. Da $p \not| f$, gilt auch $p \not| g$ und $p \not| h$. Sei i, j minimal mit $p \not| b_i$ und $p \not| c_j$. Dann gilt $p \not| a_{i+j}$. Also $i + j = n$, $i = m$ und $j = l$. Damit $p|c_0$ und $p|b_0$, also $p^2|a_0$. Widerspruch. □

Dieses Lemma kann direkt auf $x^n + px + p$ oder $x^n - p$ in $\mathbb{Z}[x]$ angewendet werden. Die Irreduzibilität des letzteren zeigt, daß $p^{1/n} \notin \mathbb{Q}$.

Hier ist eine weitere Anwendung. Sei $f = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + 1$. Wir definieren

$$g(x) := f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \sum_{n=1}^{p} \binom{p}{n} x^{n-1} .$$

Man kann das Lemma auf g anwenden. Mit g ist aber auch f irreduzibel.

Sei $I \subset R$ ein Ideal derart daß R/I ein Integritätsbereich ist. Sei $f = a_n x^n + \cdots + a_0 \in R[x]$ primitiv mit $a_n \notin I$. Sei $\bar{R} = R/I$ und $\bar{f} \in \bar{R}[x]$ das Bild von f unter $R[x] \to \bar{R}[x]$.

Lemma 4.23. *Ist $\bar{f}$ irreduzibel in $\bar{R}[x]$, so ist $f \in K[x]$ irreduzibel.*

Proof. Es reicht zu zeigen, daß $f \in R[x]$ irreduzibel ist. Sei $f = gh$ eine echte Zerlegung. Dann gilt $\deg(g) > 0$ und $\deg(h) > 0$. Dann ist $\bar{f} = \bar{g}\bar{h}$. Wegen $a_n \notin I$ ist $\deg(g) = \deg(\bar{g}) > 0$ und $\deg(\bar{h}) = \deg(h) > 0$. Dann ist $\bar{f} = \bar{g}\bar{h}$ eine echte Zerlegung von $\bar{f}$. □

Hier ist eine Anwendung. Wir betrachten $f = x^5 - x + 1 \in \mathbb{Z}[x]$. Sei $p = 3$. Die Werte von $\bar{f}$ sind

x	0	1	2
$\bar{f}(x)$	1	1	1

.

$\bar{f}$ hat also keinen Linearfaktor. Die Liste der in $\mathbb{F}_3[x]$ irreduziblen Polynome ist

$$x^2+1, x^2+x-1, x^2-x-1 \ .$$

Wir stellen fest, daß $\bar{f}$ durch keines dieser Polynome teilbar ist. Folglich ist $\bar{f}$ irreduzibel und somit auch f.

4.3 Algebraische Erweiterungen

4.3.1 Einheitswurzelkörper

Sei K ein Körper.

Definition 4.24. *Der n-te Einheitswurzelkörper über K ist der Zerfällungskörper K_n von X^n-1. Die Nullstellen von X^n-1 in K_n heißen n-te Einheitswurzeln. Die Erzeugenden der Gruppe μ_n der n-ten Einheitswurzeln heißen primitive Einheitswurzeln.*

Nach Lemma 3.64 ist μ_n zyklisch.

Folgerung 4.25. *Sei K ein Körper und $n \in \mathbb{N}$. Dann gibt es eine Erweiterung $K \subset L$ derart, daß L eine primitive n-te Einheitswurzel enthält.*

Ist $\zeta \in \mu_n$ primitiv, so gilt $K_n = K(\zeta)$.

Ist $\mathtt{char}(K) = p$ und $n = p^e m$ mit $e \geq 1$, so ist

$$x^n - 1 = 0 \Leftrightarrow x^{p^e m} - 1 = 0 \Leftrightarrow (x^m-1)^p = 0 \Leftrightarrow X^m - 1 = 0 \ .$$

Folglich gilt $|\mu_n(K)| \leq m < n$.

Wir betrachten jetzt nur den Fall, daß $\mathtt{char}(K) \not| n$. Dann gilt $f'(\xi) = n\zeta \neq 0$ für $\zeta \in \mu_n$. Die Nullstellen von f sind also einfach und $|\mu_n| = n$. μ_n ist eine Untergruppe von K_n^* und deshalb zyklisch. Es gibt $\varphi(n)$ primitive Einheitswurzeln.

Definition 4.26. *Das n-te Kreisteilungspolynom ist durch*

$$\Phi_n := \prod_{i=1}^{\varphi(n)} (x - \zeta_i)$$

definiert.

Lemma 4.27. *1. Es gilt* $\Phi_n \in \mathbb{Z}[x]$ *falls* $\mathtt{char}(K) = 0$ *und* $\Phi_n \in \mathbb{F}_p[x]$ *falls* $\mathtt{char}(K) = p$.

2. Weiterhin

$$x^n - 1 = \prod_{d|n} \Phi_d \ .$$

Proof. Ist $\xi \in \mu_n$ von Ordnung d, dann ist ξ eine d-te primitive Einheitswurzel und es gilt $\Phi_d(\xi) = 0$. Die Polynome auf beiden Seiten haben den Grad n und n verschiedene gemeinsame Nullstellen. Dies zeigt 2.

Wir zeigen 1. durch Induktion nach n. $n = 1$ ist klar. Sei $n > 1$. Sei $g = \prod_{d|n, d\neq n} \Phi_d$. Dann gilt $\Phi_n g = x^n - 1$. Da g und $x^n - 1$ in $\mathbb{Z}[x]$ (bzw. $\mathbb{F}_p[x]$) gilt, muß (Division mit Rest in $\mathbb{Z}[x]$ oder $\mathbb{F}_p[x]$) auch Φ_n in $\mathbb{Z}[x]$ oder $\mathbb{F}_p[x]$ liegen. □

Lemma 4.28 (Gauß,Dedekind). Φ_n *in* $\mathbb{Q}[x]$ *ist irreduzibel.*

Proof. Zeigen, daß Φ_n in $\mathbb{Z}[x]$ irreduzibel ist. Sei $\Phi_n = fh$ eine Zerlegung.

Sei $\zeta \in \mu_n$ primitiv. Wir können annehmen, daß $f(\zeta) = 0$. Sei $g \in \mathbb{Q}[x]$ von minimalen Grad derart, daß $g(\zeta) = 0$. Dann ist g prim. Es gilt weiter $g|f$ (wäre $g.g.T(f,g) = 1$, dann $1(\zeta) = 0$).

Nach Umnormieren gilt also $\Phi_n = fh$ (setze $h := hf/g$) mit $f(\zeta) = 0$ und f hat minimalen Grad mit dieser Eigenschaft.

Wollen zeigen, daß $f = \Phi_n$. Zeigen dazu: Ist p prim zu n und $f(\xi) = 0$, dann auch $f(\xi^p) = 0$. Die Menge $\{\zeta^{kp} | k \in \mathbb{Z}\}$ durchläuft die primitiven n-ten Einheitswurzeln.

Annahme: $f(\xi^p) \neq 0$. Dann gilt $h(\xi^p) = 0$. Sei $H(x) = h(x^p)$, dann $H(\xi^p) = 0$.

f ist minimal mit $f(\xi^p) = 0$. Also $H = fg$ mit $f, g \in \mathbb{Z}[x]$. Rechnen jetzt modulo p. $\bar{h}^p = \bar{H} = \bar{f}\bar{g}$. Es existiert $1 \neq q \in \mathbb{F}_p[x]$ mit $q = g.g.T(\bar{h}, \bar{f})$. Es gilt $\bar{\Phi}_n = \bar{f}\bar{h}$. Also hat $\bar{\Phi}_n$ mehrfache Nullstelle $u \neq 0$. (nämlich jede von q). Aber $\bar{\Phi}'(nu^{n-1}) \neq 0$. □

4.3.2 Algebraische und Transzendente Erweiterungen

Sei $K \subset L$ eine Erweiterung und $\alpha \in L \setminus K$. Wir haben $\phi_\alpha : K[x] \to L$ durch $\phi_\alpha(f) := f(\alpha)$. Sei $I_\alpha = \texttt{ker}(\phi_\alpha)$. Dann gilt $I_\alpha = (f_\alpha)$.

Definition 4.29. *Das Element α heißt transzendent über K, falls $I_\alpha = 0$. Andernfalls heißt α algebraisch. Der normierte Erzeuger f_α ist in diesem Fall das Minimalpolynom von α.*

Folgerung 4.30. *Ist α transzendent, so gilt $K(\alpha) \cong K[x]$. Andernfalls ist f_α ist irreduzibel und $K(\alpha) \cong K_{f_\alpha}$. Es gilt $[K(\alpha) : K] = \deg(f_\alpha)$.*

Satz 4.31. *1. e ist transzendent.(Hermite, 1873)*

2. π ist transzendent. (Lindemann, 1882)

4.3.3 Automorphismen

Sei $\texttt{char}(K) \not| n$ und $K_n = K(\zeta)$ der n-te Kreisteilungskörper. Sei f ein Minimalpolynom von ζ. Wir haben $K_f = K(\zeta)$. Seien $\zeta_1 := \zeta, \zeta_2, \ldots, \zeta_m$ die Wurzeln von f, $\deg(f) = m$.

Durch $\zeta \mapsto \zeta_i$ wird also ein Automorphismus σ_i von $K(\zeta)/K$ induziert und umgekehrt. In der Tat gilt $K(\zeta) = K(\zeta_i)$.

Definition 4.32. *Sei $Gal(K(\zeta)/K)$ die Gruppe dieser Automorphismen.*

Lemma 4.33. *Es gilt $|Gal(K(\zeta)/K)| = m$. Insbesondere, wenn $K = \mathbb{Q}$ ist, so gilt $|Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = \varphi(n)$.*

Die Gruppe $\mu_n =< \zeta >$ ist zyklisch. Ist $\sigma \in Gal(K(\zeta)/K)$, so induziert σ einen Automorphismus von μ_n, welcher durch $\zeta \mapsto \zeta^{\tau(\sigma)}$ bestimmt ist. Es gilt $\tau(\sigma)^n = 1$ und $\tau(\sigma)$ ist einen Einheit in $\mathbb{Z}/n\mathbb{Z}$. Wir erhalten einen injektiven Homomorphismus

$$\tau : Gal(K(\zeta)/K) \to (\mathbb{Z}/n\mathbb{Z})^* .$$

Ist $K = \mathbb{Q}$, so muß τ wegen $|Gal(K(\zeta)/K)| = |(\mathbb{Z}/n\mathbb{Z})^*|$ ein Isomorphismus sein.

4.4 Ausblicke auf die Galois Theorie und warum es keine Lösungsformel für Gleichungen fünften Grades gibt.

4.4.1 Fixkörper

Sei L ein Körper und $G \subset \mathtt{Aut}(L)$ eine Untergruppe.

Definition 4.34. *Der Fixkörper von G ist durch*

$$L^G = \{x \in L \,|\, \sigma x = x \,\forall \sigma \in G\}$$

Lemma 4.35. *L^G ist ein Körper.*

Lemma 4.36. *Es gilt $[L : L^G] = |G|$.*

4.4.2 Der Hauptsatz der Galoistheorie

Sei $K \subset L$ eine Körpererweiterung.

Definition 4.37. *Wir definieren die Galoisgruppe $Gal(L/K) \subset \mathtt{Aut}(L)$ als*

$$Gal(L/K) = \{\sigma \in \mathtt{Aut}(L) \,|\, \sigma_{|K} = \mathtt{id}_K\} \,.$$

Definition 4.38. *Die Erweiterung $K \subset L$ heißt Galoiserweiterung, falls*

$$L^{Gal(L/K)} = K \,.$$

Eine äquivalente Bedingung ist $[L : K] = |Gal(L/K)|$.

Sei $K \subset L$ eine Galoiserweiterung.

Satz 4.39 (Hauptsatz). *Die Zuordnung, $G \mapsto L^G$, $G \subset Gal(L(K)$ liefert eine inklusionsumkehrende Bijektion zwischen der Menge der Untergruppen von $G \subset Gal(L/K)$ und den Zwischenkörpern $K \subset L^G \subset L$. Dabei ist $K \subset L^G$ eine Galoiserweiterung genau dann, wenn G ein Normalteiler ist, und es gilt $Gal(L^G/K) \cong Gal(L/K)/G$.*

4.4.3 $\mathbb{Q}[\sqrt[3]{2},\zeta]$

Sei $\zeta \in \mathbb{C}$ eine Nullstelle von $f = 1+x+x^2$. Sei weiter $\alpha \in \mathbb{R}$ positiv mit $\alpha^3 = 2$. Wir betrachten den Körper $L = \mathbb{Q}(\alpha,\zeta)$.

Wir haben $\zeta^3 = 1$ und $f = 1+x+x^2 = (x-\zeta)(x-\zeta^2)$. Das Polynom f ist irreduzibel. Folglich induziert $\zeta \mapsto \zeta^2$ einen Automorphismus $\bar{\tau} \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ mit $\bar{\tau}^2 = 1$. Da $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ ist die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ eine Galoiserweiterung.

Es gilt $g := x^3 - 2 = (x-\alpha)(x-\zeta\alpha)(x-\zeta^2\alpha)$. Da $g \in \mathbb{Q}(\zeta)$ irreduzibel ist, haben wir einen Automorphismus $\sigma \in Gal(\mathbb{Q}(\alpha,\zeta)/\mathbb{Q}(\zeta))$, $\sigma(\alpha) = \zeta\alpha$. Es gilt $\sigma^3 = 1$. Wegen $[\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}(\zeta)] = 3$ ist $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\alpha,\zeta)$ eine Galoiserweiterung.

Wir betrachten nun die Erweiterung $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha,\zeta)$. Das Polynom $1+x+x^2$ ist irreduzibel über $\mathbb{Q}(\alpha)$. Somit gibt es einen Automorphismus $\tau \in Gal(\mathbb{Q}(\alpha,\zeta)/\mathbb{Q}(\alpha))$ mit $\tau(\zeta) = \zeta^2$ und $\tau^2 = 1$. Auch diese Erweiterung ist eine Galoiserweiterung.

Es gilt $\tau\sigma\tau\sigma = 1$. Die Gruppe $< \tau,\sigma >$ ist isomorph zur symmetrischen Gruppe S_3 und hat insbesondere 6 Elemente. Wegen $[\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}] = 2.3 = 6$ ist $\mathbb{Q} \subset \mathbb{Q}(\alpha,\zeta)$ eine Galoiserweiterung mit $Gal(\mathbb{Q}(\alpha,\zeta)/\mathbb{Q}) =< \tau,\sigma >$.

Die Untergruppen sind $< \tau >$, $< \sigma\tau\sigma^{-1} >$, $< \sigma^2\tau\sigma^{-2} >$, $< \sigma >$ und entsprechen den Zwischenkörpern $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\zeta\alpha)$, $\mathbb{Q}(\zeta^2\alpha)$, $\mathbb{Q}(\zeta)$. Nur $< \sigma >$ ist ein Normalteiler. Die Klasse $\bar{\tau} = [\tau] \in Gal(\mathbb{Q}(\zeta\alpha)/\mathbb{Q})/ < \sigma >$ erzeugt $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$.

4.4.4 Die Galoisgruppe eines Polynoms

Sei $f \in K[x]$.

Definition 4.40. *f heißt separabel, wenn jeder irreduzible Faktor von f in seinem Zerfällungskörper keine mehrfachen Nullstellen hat.*

Satz 4.41. *Ist $f \in K[x]$ separabel und $K \subset L$ der Zerfällungskörper von f, dann ist $K \subset L$ eine Galoiserweiterung. Sei $G(f) := Gal(L/K)$. Umgekehrt ist jede Galoiserweiterung ein Zerfällungskörper eines separablen Polynoms.*

Wir nehmen an, daß $\mathtt{char}(K) \not| n$ und daß K die n-ten Einheitswurzeln enthält. Sei $a \in K^*$ und $f := x^n - a \in K[x]$.

Satz 4.42. *$Gal(f)$ ist zyklisch.*

Proof. Die Idee ist, daß

$$f = \prod_{i=0}^{n-1} (x - \zeta^i b)$$

für eine Nullstelle b von f, wobei ζ eine n-te primitive Einheitswurzel ist. Wir erhalten einen injektiven Homomorphismus $\kappa : G(f \to \mathbb{Z}/n\mathbb{Z}$ durch $\sigma(b) = \zeta^{\kappa(\sigma)} b$. □

Ein Beispiel dafür ist die Erweiterung $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\alpha, \zeta)$ in 4.4.3.

4.4.5 Radikalerweiterungen

Definition 4.43. *Eine Erweiterung $K \subset L$ heißt Radikalerweiterung, falls es eine Kette von Erweiterungen*

$$K = K_1 \subset K_2 \subset \cdots \subset K_n = L$$

gibt derart, daß $K_{i+1} = K_i(x_i)$ mit $x_i^{n_i} \in K_i$ für geeignete $n_i \in \mathbb{N}$.

Lemma 4.44. *Sei $K \subset L$ eine Radikalerweiterung. Dann gibt es eine Erweiterung $L \subset L'$ derart, daß $K \subset L'$ eine Radikal- und Galoiserweiterung ist.*

Proof. Induktion nach $[L : K]$. Sei $[L : K] \geq 2$. Dann gibt es $K \subset M \subset L$ so daß $L = M(b)$ mit $b^n \in M$. Es gibt nach Induktionsannahme $M \subset M'$ derart, daß $K \subset M'$ Radikal- und Galoiserweiterung ist.

Sei M' Zerfällungskörper von $f \in K[x]$. Setzen

$$g := \prod_{\sigma \in Gal(M'/K)} (x^n - \sigma b^n) \, .$$

Dann gilt $g \in K[x]$. Sei $M' \subset L'$ der Zerfällungskörper von fg. □

Definition 4.45. *$f \in K[x]$ heißt durch Radikale auflösbar, falls es eine Radikalerweiterung $K \subset L$ gibt, in welcher f zerfällt.*

Satz 4.46. *Sei $f \in K[x]$ separabel und gelte $\mathtt{char}(K) = 0$. Dann sind äquivalent:*

1. *$G(f)$ ist auflösbar.*

2. *f ist durch Radikale auflösbar.*

Proof. Zeigen hier nur $2 \Rightarrow 1$. Sei $K \subset L$ eine Radikalerweiterung, in welcher f zerfällt. Wegen 4.44 kann man annehmen, daß $K \subset L$ eine Galoiserweiterung ist.

Sei $K = L_0 \subset L_1 \subset \cdots \subset L_m = L$ mit $L_{i+1} = L_i(b_i)$ mit $b_i^{n_i} \in L_i$. Sei $n = n_0 n_1 \ldots n_{m-1}$. Sei ζ eine primitive Einheitswurzel. Wir setzen $L_i' := L(\zeta)$ und $K' := K(\zeta)$. Wir haben Turm von Galoiserweiterungen

$$K \subset K' \subset L' \ .$$

Wenn $K \subset L$ der Zerfällungskörper von $h \in K[x]$ ist, dann ist $K \subset L'$ der Zerfällungskörper von $h(x^n - 1)$.

Die Erweiterungen $L_i' \subset L_{i+1}'$ sind Galois (siehe 4.42, da L_i' die n_i-te primitive Einheitswurzel enthält).

Haben nun Turm von Galoiserweiterungen

$$K \subset K' \subset L_1' \subset \cdots \subset L_m' = L' \ .$$

Dem entspricht Normalreihe

$$0 \subset Gal(L'/L_{m-1}') \subset \cdots \subset Gal(L'/K') \subset Gal(L'/K) \ .$$

Alle Subquotienten sind zyklisch. Also ist $Gal(L'/K)$ auflösbar.

Sei $K \subset M \subset L'$ der Zerfällungskörper von f. Dann ist $Gal(M/K)$ ein Quotient von $Gal(L'/K)$ und damit auch auflösbar. □

Sei $f = x^5 - 4x + 2$. Nach Eisenstein mit $p = 2$ ist f irreduzibel. Es hat drei verschiedene relle Nullstellen r_1, r_2, r_3 (in der Tat hat f' zwei verschiedene relle Nullstellen). Folglich muß es ein weiteres Paar $\alpha, \bar{\alpha}$ von komplexen Nullstellen haben.

Sei L der Zerfällungskörper von f. Es gilt $[L : \mathbb{Q}] = |G(f)$. Es gilt $G(f) \subset S(r_1, r_2, r_3, \alpha, \bar{\alpha}) \cong S_5$. Es gilt $[\mathbb{Q}(r_1) : \mathbb{Q}] = 5$ (f ist irreduzibel). Damit gilt $5|G(f)$. Folglich enthält $G(f)$ ein Element σ der Ordnung 5. Dieses ist o.B.d.a ein Fünferzyklus. Die komplexe Konjugation liefert eine Involution $\tau = (\alpha, \bar{\alpha}) \in G(f)$. Nun gilt aber $< \sigma, \tau >= S_5$. Die Gruppe S_5 ist nicht auflösbar. Also ist f nicht durch Radikale auflösbar.