Einführung in die Algebra und Zahlentheorie

Eine Vorlesung gehalten von
Volker Schulze[1]
an der FU Berlin

Wintersemester 2002/2003

[1]Den Hörern und Herrn Swerling verdanke ich eine Reihe von Korrekturen und Verbesserungsvorschlägen. Mein Dank gilt Herrn Swerling auch für die Erarbeitung des LaTeX-Files.

Inhaltsverzeichnis

Kapitel 1

Gruppen

1.1 Algebraische Strukturen

Algebra ist die Theorie der algebraischen Strukturen. In der Vorlesung werden aber nur Gruppen, Ringe und Körper behandelt und einige zahlentheoretische Anwendungen.

Definition 1.1. Relation
Seien X, Y Mengen, $R \subseteq X \times Y$.
(R, X, Y) oder auch einfach R heißt (zweistellige) Relation zwischen X und Y.
R wird häufig mit $\sim$ bezeichnet.
Im Fall $X = Y$ heißt R auch Relation auf X.
Für $(x, y) \in R$ schreibt man auch $xRy,\ x \sim_R y$ oder $x \sim y$.
Analog werden n-stellige Relationen definiert als Teilmenge eines Cartesischen Produktes $X_1 \times \cdots \times X_n$.

Beispiel 1.2. Sei P eine Menge von Personen, V eine Menge von Vereinen. Die Mitgliedschaftsbeziehungen werden beschrieben durch die Relation

$$R := \{(x, y) | x \in P \text{ ist Mitglied im Verein } y \in V\} \subseteq P \times V.$$

Definition 1.3. Äquivalenzrelation
Sei $\sim$ Relation auf X.
$\sim$ heißt Äquivalenzrelation, wenn für alle $a, b, c \in X$ gilt:

$$\begin{aligned} a \sim a & \quad \text{(Reflexivität)} \\ a \sim b \Rightarrow b \sim a & \quad \text{(Symmetrie)} \\ a \sim b \wedge b \sim c \Rightarrow a \sim c & \quad \text{(Transitivität)} \end{aligned}$$

Definition 1.4. Äquivalenzklasse
Sei $\sim$ Äquivalenzrelation auf X, $a \in X$. Dann heißt die Teilmenge

$$\{b \in X | b \sim a\} =: [a] \subseteq X$$

die von a erzeugte Äquivalenz-Klasse.

Satz 1.5.
Seien $a, b \in X$. Dann gilt $[a] = [b]$ oder $[a] \cap [b] = \emptyset$
(zwei Äquivalenz-Klassen sind entweder gleich, oder elementefremd).

Beweis.

Fall 1 $[a] \cap [b] = \emptyset$. Der Satz ist trivialerweise erfüllt.

Fall 2 $[a] \cap [b] \neq \emptyset$. Dann $\exists c \in [a] \cap [b]$. Für dieses c gilt
$(c \sim a) \wedge (c \sim b)$. Aus der Symmetrie und Transitivität von $\sim$ folgt $a \sim b$.
Nun wird $[a] \subseteq [b]$ gezeigt.
Aus $d \in [a]$ folgt $d \sim a$ und wegen $a \sim b$ und der Transitivität von $\sim$ weiter $d \sim b$, also $d \in [b]$.
Analog folgt $[a] \supseteq [b]$. □

Definition 1.6. Partition
Sei X eine Menge, T eine Menge von Teilmengen von X.
T heißt Partition von X falls gilt:

1. die Elemente von T sind paarweise disjunkt, und
2. die Vereinigung der Elemente von T ist X.

Satz 1.7. Jede Partition T einer Menge X induziert eine Äquivalenzrelation auf X durch

$$a \sim b :\Leftrightarrow \exists T_1 \in T : (a \in T_1 \wedge b \in T_1).$$

Definition 1.8. Abbildung
Sei (f, A, B) eine Relation.
(f, A, B) heißt Abbildung von A nach B, wenn gilt:
Zu jedem $a \in A$ existiert genau ein $b \in B$ mit $(a, b) \in f$.
Schreibweise: $f : A \to B$, $f(a) := b$ oder $a \mapsto_f b$.

Definition 1.9. Surjektiv
Die Abbildung $f : A \to B$ heißt surjektiv, falls zu jedem $b \in B$ mindestens ein $a \in A$ existiert mit $f(a) = b$.

Definition 1.10. Injektiv
Die Abbildung $f : A \to B$ heißt injektiv, falls zu jedem $b \in B$ höchstens ein $a \in A$ existiert mit $f(a) = b$.

Definition 1.11. Bijektiv
Die Abbildung $f : A \to B$ heißt bijektiv, falls zu jedem $b \in B$ genau ein $a \in A$ existiert mit $f(a) = b$. (Also falls f sowohl surjektiv als auch injektiv ist).

Definition 1.12. Komposition
Seien $f : A \to B,\ g : B \to C$ zwei Abbildungen.
Als Komposition von f und g bezeichnet man die Abbildung $g \circ f : A \to C$, definiert durch $g \circ f(a) := g(f(a))$ für alle $a \in A$.

Bemerkung 1.13. Seien $f : A \to B,\ g : C \to D$ zwei Abbildungen.
Nach Definition 1.8 sind f und g gleich genau dann, wenn gilt:
$A = C,\ B = D$ und $f(a) = g(a)$ für alle $a \in A$.

Definition 1.14. Verknüpfung
Seien X, Y nicht leere Mengen.
Eine Abbildung $f : Y \times X \to X$ heißt 2-stellige Verknüpfung auf X.
Falls $Y \neq X$, heißt f äußere Verknüpfung auf X mit Operatorenbereich Y.
Falls $Y = X$, heißt f innere Verknüpfung auf X.
Analog werden n-stellige Verknüpfungen auf X definiert.
In diesem Skript sind alle Verknüpfungen 2-stellig, wenn nicht explizit anders vereinbart.
Sind $x \in X$ und $y \in Y$, so wird für das „Verknüpfungsergebnis“ $f(x, y)$ in der Regel yfx geschrieben.

Beispiel 1.15. Die Addition und Multiplikation in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ sind innere Verknüpfungen.

Definition 1.16. kommutativ
Eine Verknüpfung $\circ$ auf X heißt kommutativ, falls
$a \circ b = b \circ a$ für alle $a, b \in X$.

Definition 1.17. Assoziativ
Eine Verknüpfung $\circ$ auf X heißt assoziativ, falls
$((a \circ b) \circ c) = (a \circ (b \circ c))$ für alle $a, b, c \in X$.

Bemerkung 1.18.
Ist $\circ$ eine assoziative Verknüpfung auf X, und $x_1, \ldots, x_n \in X$, so nimmt $x_1 \circ \cdots \circ x_n$ bei jeder Beklammerung denselben Wert an (Siehe Übung).

Definition 1.19. Algebraische Struktur
Seien X eine Menge, I eine nicht leere Indexmenge und $V := \{f_i | i \in I\}$ eine (nicht leere) Menge von (nicht notwendig zweistelligen) Verknüpfungen auf X. Dann heißt (X, V) algebraische Struktur.
Ist $V = \{f_1 \dots f_n\}$ endlich, so schreibt man für (X, V) auch $(X, f_1, \dots, f_n)$.
Die Anzahl der Elemente von X heißt Ordnung der algebraischen Struktur (in Zeichen $|X|$ oder Ord X). Die Ordnung kann auch unendlich sein. Man spricht jeweils von einer endlichen oder unendlichen algebraischen Struktur.

Definition 1.20. Verknüpfungstafel, Verknüpfungsmatrix
Seien $X := \{a_1, \dots, a_n\}$ eine endliche Menge und $\circ$ eine innere Verknüpfung auf X. Der algebraischen Struktur $(X, \circ)$ wird eine Verknüpfungstafel wie folgt zugeordnet:

$\circ$	a_1	$\cdots$	a_j	$\cdots$	a_n
a_1	$a_1 \circ a_1$	$\cdots$	$a_1 \circ a_j$	$\cdots$	$a_1 \circ a_n$
$\vdots$	$\vdots$	$\cdot$	$\cdot$	$\cdot$	$\vdots$
a_i	$a_i \circ a_1$	$\cdot$	$a_i \circ a_j$	$\cdot$	$a_i \circ a_n$
$\vdots$	$\vdots$	$\cdot$	$\cdot$	$\cdot$	$\vdots$
a_n	$a_n \circ a_1$	$\cdots$	$a_n \circ a_j$	$\cdots$	$a_n \circ a_n$

Die Matrix

$$\begin{pmatrix} a_1 \circ a_1 & \cdots & a_1 \circ a_j & \cdots & a_1 \circ a_n \\ \vdots & \cdot & \cdot & \cdot & \vdots \\ a_i \circ a_1 & \cdot & a_i \circ a_j & \cdot & a_i \circ a_n \\ \vdots & \cdot & \cdot & \cdot & \vdots \\ a_n \circ a_1 & \cdots & a_n \circ a_j & \cdots & a_n \circ a_n \end{pmatrix}$$

heißt Verknüpfungsmatrix.

Definition 1.21. Isomorph
Zwei algebraische Strukturen (X, V) und (X', V') heißen isomorph (in Zeichen: $(X, V) \cong (X', V')$), wenn gilt:
Es existieren bijektive Abbildungen $\varphi : X \to X'$ mit $x \mapsto x'$ und $\psi : V \to V'$ mit $\circ \mapsto \otimes$, sodaß gilt:

1. $\circ$ ist innere Verknüpfung von $V \Leftrightarrow \otimes$ ist innere Verknüpfung von V'
2. Ist $\circ$ äußere Verknüpfung, so besitzen $\circ$ und $\otimes$ denselben Operatorenbereich Y.
3. $\varphi(x_1 \circ x_2) = x_1' \otimes x_2'$ für alle $x_1, x_2 \in X$ und alle innere Verknüpfungen aus V.

4. $\varphi(y \circ x) = y \otimes x'$ für alle $x \in X,\ y \in Y$ und alle äußere Verknüpfungen aus V.

In der Algebra beschäftigt man sich mit algebraischen Strukturen. In der Vorlesung werden aber nur Gruppen, Ringe und Körper behandelt.

1.2 Gruppen

Definition 1.22. Halbgruppe, Gruppe
Sei $(G, \circ)$ eine algebraische Struktur.
$(G, \circ)$ heißt Halbgruppe, wenn $\circ$ assoziativ ist.
Eine Halbgruppe $(G, \circ)$ heißt Gruppe wenn:

1. Es existiert ein Element $e \in G$, mit $e \circ g = g$ für alle $g \in G$ (e heißt dann linksneutrales Element von $(G, \circ)$).

2. Zu jedem $g \in G$ existiert ein $g' \in G$ mit $g' \circ g = e$ (g' heißt dann linksinverses Element zu g in $(G, \circ)$).

Eine Gruppe $(G, \circ)$ heißt abelsch (oder kommutativ), falls $\circ$ kommutativ ist.

Beispiel 1.23.
$(\mathbb{Z},\ \cdot)$, $(\mathbb{N}, +)$ und $(\mathbb{R}, \cdot)$ sind Halbgruppen.
$(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ und $(2\mathbb{Z}, +)$ sind (abelsche) Gruppen.
Sei M Menge; $P_M := \{f \mid f : M \to M$ bijektive Abbildung$\}$. Dann ist $(P_M, \circ)$ eine Gruppe.

Satz 1.24.
Sei $(G, \circ)$ Gruppe, e linkneutrales Element. Dann gilt:

1. Ein Linksinverses von g ist auch Rechtsinverses von g.
   Das heißt: $g' \circ g = e \Rightarrow g \circ g' = e$.
   g' heißt: auch Inverses von g.

2. Eine linkneutrales Element ist auch rechtsneutrales Element.
   Das heißt: $e \circ g = g \Rightarrow g \circ e = g$.
   e heißt auch neutrales Element oder Eins(element) in G.

3. Seien $a, b \in G$. Dann sind $a \circ x = b$ und $x \circ a = b$ in G eindeutig lösbar.

4. e ist eindeutig bestimmt.

5. Jedes $g \in G$ besitzt genau ein Inverses (das mit g^{-1} bezeichnet wird).

6. Für jedes $g \in G$ gilt $(g^{-1})^{-1} = g$.

7. Für beliebige $g_1, \ldots, g_n \in G$ gilt $(g_1 \circ \cdots \circ g_n)^{-1} = g_n^{-1} \circ \cdots \circ g_1^{-1}$.

Beweis.

1. Zu zeigen: $g \circ g' = e$.
   Sei g'' ein Linksinverses von g'. Dann folgt
   $e = g'' \circ g' = g'' \circ (g' \circ g) \circ g' = (g'' \circ g') \circ (g \circ g') = e \circ (g \circ g') = g \circ g'$.

2. $g \circ e = g \circ (g' \circ g) = (g \circ g') \circ g = e \circ g = g$.
   Man beachte, daß das vorletzte Gleichheitszeichen wegen (1) gilt.

3. Eine Lösung von $a \circ x = b$ ist offenbar $a' \circ b$. Sind x_1, x_2 Lösungen von $a \circ x = b$, so folgt $a \circ x_1 = a \circ x_2 (= b)$, also $a' \circ a \circ x_1 = a' \circ a \circ x_2$ und damit $x_1 = x_2$.
   Die Aussage über $x \circ a = b$ läßt sich analog beweisen.

4. Nach Definition existiert eine Eins e. Jede Eins ist Lösung von $x \circ e = e$. Nach dem vorherigen Teil des Satzes ist die Lösung eindeutig bestimmt.

5. Jedes $g \in G$ besitzt genau ein Inverses als Lösung von $x \circ g = e$.

6. $(g^{-1})^{-1}$ und g sind beide Lösungen von $x \circ g^{-1} = e$ nach dem ersten Teil des Satzes, nach dem dritten Teil sind dann beide Elemente gleich.

7. Wegen der Assoziativität von $\circ$ ist $(g_n^{-1} \circ \cdots \circ g_1^{-1}) \circ (g_1 \circ \cdots \circ g_n) = e$, und nach dem vierten Teil des Satzes ist das Inverse eindeutig. □

Bemerkung 1.25.

1. Bei additiver Schreibweise wird das neutrale Element einer Gruppe i.A. mit 0 bezeichnet und g^{-1} wird mit $-g$ bezeichnet. Bei multiplikativer Schreibweise wird das neutrale Element i.A. mit 1 bezeichnet.

2. In Definition 1.22 kann man auch analog ein rechtsneutrales Element und Rechtsinverse fordern und einen dem Satz 1.24 entsprechenden Satz beweisen.

3. Es gibt Halbgruppen, die eine Rechtseins und Linksinverse besitzen, aber keine Gruppe sind; z.B.:
   $(H, \circ)$ mit $H = \{e, a\}$; $e \circ e = e$, $e \circ a = e$, $a \circ e = a$, $a \circ a = a$.

Satz 1.26. Sei $(G, \circ)$ Halbgruppe. Dann gilt:

$(G, \circ)$ ist Gruppe $\Leftrightarrow \forall a, b \in G : a \circ x = b$ und $x \circ a = b$ sind in G lösbar.

Beweis. $\Rightarrow$: nach Satz 1.24.
$\Leftarrow$: $(G, \circ)$ ist Halbgruppe, also ist $G \neq \emptyset$ und es existiert ein $g \in G$. Nach Voraussetzung existiert ein $e \in G$ mit $e \circ g = g$ als Lösung von $x \circ g = g$.
Sei $a \in G$ beliebig. Dann existiert (nach Voraussetzung) ein $b \in G$ mit $a = g \circ b$ als Lösung von $a = g \circ x$.
Es folgt $e \circ a = e \circ (g \circ b) = (e \circ g) \circ b = g \circ b = a$. e ist also linksneutral.
Für jedes $g \in G$ ist eine Lösung von $x \circ g = e$ linksinverses Element von g. □

Definition 1.27. Regulär (Kürzungsregel)
Eine Halbgruppe $(H, \cdot)$ heißt regulär, wenn für alle $a, x, y \in H$ gilt:
$(a \cdot x = a \cdot y \Rightarrow x = y)$ und $(x \cdot a = y \cdot a \Rightarrow x = y)$.

Satz 1.28. Jede endliche reguläre Halbgruppe ist Gruppe.

Beweis.
Seien $(H, \cdot)$ eine endliche reguläre Halbgruppe, $a \in H$ beliebig aber fest,
$f : H \to H,\ f(x) := x \cdot a$ und $g : H \to H,\ g(x) := a \cdot x$ Abbildungen. f und g sind injektiv (wegen der Regulärität), also bijektiv (da H endlich ist). Also sind $x \cdot a = b$ und $a \cdot x = b$ lösbar für alle $a, b \in H$. Nach Satz 1.26 folgt die Behauptung. □

Bemerkung 1.29.

1. $(\mathbb{N}, +)$ ist reguläre Halbgruppe, die nicht Gruppe ist.
2. Eine Unterhalbgruppe einer Gruppe ist stets regulär.

Beispiel 1.30. Seien $(K, +, \cdot)$ Körper, $n \in \mathbb{N}$.
Sei $\mathrm{Gl}(n, K)$ die Menge aller $n \times n$ Matrizen mit Elementen aus K und Determinante nicht Null.
Sei $\mathrm{Sl}(n, K)$ die Menge aller $n \times n$ Matrizen mit Elementen aus K und Determinante Eins.
Dann sind $(\mathrm{Gl}(n, K), \cdot)$, $(\mathrm{Sl}(n, K), \cdot)$ Gruppen.

Beispiel 1.31. Seien $(G, \circ)$ endliche Halbgruppe, $G = \{a_1, \ldots, a_n\}$, M die zugehörige Verknüpfungsmatrix.
Dann gilt:

$$\circ \text{ kommutativ} \Leftrightarrow M \text{ ist symmetrisch.}$$
$$a_i \circ x = b \text{ lösbar} \Leftrightarrow \text{In der } i\text{-ten Zeile von } M \text{ tritt } b \text{ auf.}$$

Nach Satz 1.26 folgt:
$(G, \circ)$ ist Gruppe$\Leftrightarrow$In jeder Zeile und Spalte der Verknüpfungsmatrix tritt jedes Element aus G genau einmal auf.

Beispiel 1.32. Gruppen mit kleiner Ordnung

1. Bis auf Isomorphie existiert nur eine Gruppe der Ordnung 1, nämlich $(G, \circ)$ mit $G = \{e\}$ und $e \circ e = e$.

2. Bis auf Isomorphie existiert nur eine Gruppe der Ordnung 2, nämlich $(G, \circ)$ mit $G = \{e, a\}$ und der Verknüpfungstafel:

$\circ$	e	a
e	e	a
a	a	e

3. Bis auf Isomorphie existiert nur eine Gruppe der Ordnung 3, nämlich $(G, \circ)$ mit $G = \{e, a, b\}$ und der Verknüpfungstafel:

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. Versucht man für eine Gruppe der Ordnung 4, alle möglichen Verknüpfungstafeln aufzustellen, so erhält man wegen Beispiel 1.31 die folgenden Möglichkeiten (e ist das neutrale Element):

$\circ_1$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\circ_2$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\circ_3$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\circ_4$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Durch probieren läßt sich feststellen, daß alle vier algebraischen Strukturen das Assoziativgesetz erfüllen.
Vertauscht man in $\circ_2$ a und b, so erhält man $\circ_3$. Vertauscht man in $\circ_4$ c und b, so erhält man $\circ_3$. Damit sind die Gruppen mit $\circ_2, \circ_3$ und $\circ_4$ isomorph. Also gibt es bis auf Isomorphie genau 2 Gruppen der Ordnung 4:

Die Kleinsche Vierergruppe: $(G, \circ_1)$ mit $G = \{e, a, b, c\}$ heißt Kleinsche Vierergruppe. Quadrate sind stets e. Das Produkt zweier nicht neutraler Elemente ist immer das dritte nicht neutrale Element. Die Kleinsche Vierergruppe ist abelsch.

Die Zyklische Gruppe der Ordnung 4: (Siehe Definition 1.50 auf Seite 17.) Schreibt man in$(G, \circ_3)$ statt $\{e, a, b, c\}$, die Menge

$\{0,1,2,3\}$, so erhält man die additive Gruppe $\mathbb{Z}$ modolo 4.
Das Verknüpfungsergebnis zweier Elemente erhält man dann durch Addition in $\mathbb{Z}$, Division durch vier, und Bildung des Restes.

Bemerkung 1.33.
$(\mathbb{Z},+)$ und $(2\mathbb{Z},+)$ sind Gruppen, und $f:\mathbb{Z}\to 2\mathbb{Z},\ f(z)=2\cdot z$ ist Isomorphismus obwohl $2\mathbb{Z}\subsetneq\mathbb{Z}$. Siehe Definition 1.21 auf Seite 8.

1.3 Untergruppen, Normalteiler

Definition 1.34. Untergruppe
Sei $(G,\circ)$ eine Gruppe, $U\subseteq G$. Sei U abgeschlossen bezüglich $\circ$, das heißt: Für alle $u_1,u_2\in U$ gilt $u_1\circ u_2\in U$. Dann lässt sich $\circ$ (genauer: Die Einschränkung von $\circ$ auf $U\times U$) auffassen als Verknüpfung auf U.
$(U,\circ)$ heißt *Untergruppe* von $(G,\circ)$, falls $(U,\circ)$ eine Gruppe ist.
Für $(U,\circ)$ schreibt man häufig einfach U.

Bemerkung 1.35.

1. Seien $(G,\circ)$ eine Gruppe mit neutralem Element e, U eine Untergruppe. Dann ist e auch neutrales Element von U.

   Beweis. Sei e' neutrales Element von U.
   Dann gilt $e'\circ e'=e'$ und $e'\circ e=e'$. Nach Satz 1.24.3 ist $e'\circ x=e'$ eindeutig lösbar, also $e=e'$. □

2. Der Durchschnitt beliebig vieler Untergruppen einer Gruppe ist auch eine Untergruppe dieser Gruppe.

3. Die Vereinigung zweier Untergruppen ist nicht unbedingt eine Untergruppe.

   Beweis. Seien $(G,\circ)$ Gruppe;$U_1,\ U_2$ Untergruppen von $(G,\circ)$ mit $U_1\not\subseteq U_2,\ U_2\not\subseteq U_1,\ g_1\in U_1\setminus U_2,\ g_2\in U_2\setminus U_1$.
   Dann gilt $g_1\circ g_2\notin U_1\cup U_2$.
   Angenommen $g_1\circ g_2=u_1\in U_1$.
   Dann ist $g_2=g_1^{-1}\circ u_1\in U_1$ im Widerspruch zur Voraussetzung.
   Analog läßt sich zeigen $g_1\circ g_2\notin U_2$. □

Satz 1.36. Untergruppenkriterien
Sei $(G,\cdot)$ eine Gruppe, $U\subseteq G,\ U\neq\emptyset$. Dann gilt:

$$U \text{ ist Untergruppe} \Leftrightarrow (a,b\in U\Rightarrow a\cdot b^{-1}\in U)$$

Beweis. $\Rightarrow$: Klar.
$\Leftarrow$: Zu zeigen:

1. $e \in U$
2. $\forall u \in U : \ u^{-1} \in U$
3. $\forall a, b \in U : \ a \cdot b \in U$
4. $\cdot$ (auf U beschränkt) ist assoziativ.

Der Beweis dieser Aussagen ergibt sich wie folgt:

1. U ist nicht leer, also existiert ein $u \in U$, also ist $u \cdot u^{-1} = e \in U$
2. $e, u \in U \Rightarrow e \cdot u^{-1} = u^{-1} \in U$.
3. $a, b \in U \Rightarrow a, b^{-1} \in U$, also $a \cdot (b^{-1})^{-1} = a \cdot b \in U$.
4. Die Assoziativität von $\cdot$ auf U folgt aus der Assoziativität auf G. □

Definition 1.37. Nebenklasse
Seien $(G, \cdot)$ eine Gruppe, $a \in G$ und U eine Untergruppe von G.
$a \cdot U := \{a \cdot u | u \in U\}$ heißt die von a erzeugte Linksnebenklasse von U.
$U \cdot a := \{u \cdot a | u \in U\}$ heißt die von a erzeugte Rechtsnebenklasse von U.

Satz 1.38. Sei U Untergruppe von $(G, \cdot)$. Dann gilt:

1. Zwei Linksnebenklassen von U sind gleich oder elementefremd.
2. Die Linksnebenklassen von U bilden eine Partition von G.

Die beiden Aussagen gelten analog für die Rechtsnebenklassen.

Beweis.

1. Seien $a, b \in G$ und $c \in a \cdot U \cap b \cdot U$.
   Dann existieren $u_1, u_2 \in U$ mit $c = a \cdot u_1 = b \cdot u_2$.
   Für beliebiges $a \cdot u \in a \cdot U$ gilt $a \cdot u = a \cdot u_1 \cdot u_1^{-1} \cdot u = b \cdot (u_2 \cdot u_1^{-1} \cdot u) \in b \cdot U$.
   Also ist $a \cdot U \subseteq b \cdot U$ (analog erhält man $bU \subseteq aU$).
2. Für beliebiges $a \in G$ gilt $a = a \cdot e \in aU$. □

Bemerkung 1.39. Seien $(G,\cdot)$ Gruppe, U Untergruppe und $G = \bigcup_{i\in I} g_i \cdot U$ die Zerlegung von G in paarweise verschiedene Linksnebenklassen von U.
Dann heißt $\{g_i | i \in I\}$ vollständiges Repräsentantensystem der Linksnebenklassen von U in G.
Dann ist $G = \bigcup_{i\in I} U \cdot g_i^{-1}$ die Zerlegung von G in paarweise verschiedene Rechtsnebenklassen von U.
Genauer gilt: Die Abbildung $f : \{g_i \cdot U | i \in I\} \to \{U \cdot g_i^{-1} | i \in I\}$ definiert durch $g_i \cdot U \mapsto U \cdot g_i^{-1}$ ist bijektiv.
Es gibt also genausoviele Linksnebenklassen wie Rechtsnebenklassen von U (auch wenn es unendlich viele gibt).
Die Anzahl der Links- oder Rechtsnebenklassen heißt Index von U in G (in Zeichen: $[G : U]$).

Beweis. Wir beweisen zunächst $\bigcup_{i\in I} U \cdot g_i^{-1} = G$.
$\bigcup_{i\in I} U \cdot g_i^{-1} \subset G$ ist trivial.
Für jedes $g \in G$ existieren nach Voraussetzung $i \in I$ und $u \in U$ mit
$g^{-1} = g_i \cdot u$.
Daraus folgt $g = u^{-1} \cdot g_i^{-1} \in U \cdot g_i^{-1}$, also $\bigcup_{i\in I} U \cdot g_i^{-1} \supset G$.
Zu zeigen bleibt, daß $U \cdot g_i^{-1}$ für $i \in I$ paarweise verschiedene Rechtsnebenklassen sind.
Aus Satz 1.38 folgt, daß zwei Rechtsnebenklassen paarweise disjunkt oder gleich sind.
Angenommen $U \cdot g_i^{-1} = U \cdot g_j^{-1}$; dann existieren $u_1, u_2 \in U$ mit $u_1 \cdot g_i^{-1} = u_2 \cdot g_j^{-1}$. Daraus folgt $g_i^{-1} = u_1^{-1} \cdot u_2 \cdot g_j^{-1}$.
Also $g_j = g_i \cdot u_1^{-1} \cdot u_2$ und nach Satz 1.38 ist dann $g_i \cdot U = g_j \cdot U$.
Nach Voraussetzung ist dann $i = j$, also alle $U \cdot g_{i\in I}$ sind paarweise verschieden. □

Bemerkung 1.40. Seien $(G,\cdot)$ Gruppe, U Untergruppe und $g \in G$. Dann gilt: $\varphi : U \to g \cdot U$ definiert durch $\varphi(u) := g \cdot u$ und $\psi : U \to U \cdot g$ definiert durch $\psi(u) := u \cdot g$ sind bijektiv.
Ist G endlich, so hat jede Nebenklasse von U gleich viele Elemente wie U selbst.

Satz 1.41. Lagrange (1736 - 1813)
Seien $(G,\cdot)$ endliche Gruppe, U Untergruppe. Dann gilt:

$$|G| = |U| \cdot [G : U].$$

Speziell ist $|U|$ ein Teiler von $|G|$ (in Zeichen $|U| \Big| |G|$).

Beweis. Sei $g_{i\in I}$ ein vollständiges Repräsentantensystem der Linksnebenklassen von U. Nach Bemerkung 1.40 ist die Abbildung $(i,u) \mapsto g_i \cdot u$

von $I \times U$ nach G bijektiv, also $|I| \cdot |U| = |G|$. Aber $|I| = [G : U]$, also $|G| = |U| \cdot [G : U]$. □

Definition 1.42. Normalteiler
Sei $(G, \cdot)$ Gruppe, U Untergruppe.
U heißt Normalteiler (NT) von G (in Zeichen: $U \lhd G$), wenn gilt:
$g \cdot U = U \cdot g$ für alle $g \in G$.
(Achtung: Gefordert wird die Gleichheit der entsprechenden Nebenklassen, nicht die Gleichheit $g \cdot u = u \cdot g$ für alle $g \in G,\ u \in U$.)

Beispiel 1.43. Jede Gruppe $(G, \circ)$ hat die sogenannten trivialen Normalteiler $\{e\}$ und G.

Bemerkung 1.44. Seien U Untergruppe von G,
N Normalteiler von G mit $N \subseteq U$.
Dann ist N Normalteiler von U, und die Menge der Nebenklassen von N in U ist Teilmenge der Nebenklassen von N in G.

Beweis.

N ist Normalteiler von $G \Leftrightarrow gN = Ng$ für alle $g \in G$
N ist Normalteiler von $U \Leftrightarrow gN = Ng$ für alle $g \in U$ □

Satz 1.45. Normalteiler-Kriterien
Sei $(G, \cdot)$ Gruppe, U Untergruppe. Dann sind die folgenden Aussagen äquivalent:

1. $g \cdot U = U \cdot g$ für alle $g \in G$ (U ist Normalteiler von G).
2. $g \cdot U \cdot g^{-1} = U$ für alle $g \in G$.
3. $g \cdot U \cdot g^{-1} \subseteq U$ für alle $g \in G$.

Beweis. 1 $\Leftrightarrow$ 2: trivial.
2 $\Rightarrow$ 3: trivial.
3 $\Rightarrow$ 2: Nach Voraussetzung gilt $gUg^{-1} \subseteq U$ für alle $g \in G$.
Dann gilt für alle $g \in G$ auch $g^{-1}Ug \subseteq U$ und damit auch $U \subseteq gUg^{-1}$. □

Satz 1.46. Jede Untergruppe vom Index 2 ist Normalteiler.

Beweis. Sei $g \in G$, $g \notin U$. Dann folgt $G = U \cup gU = U \cup Ug$. □

Satz 1.47. Ist $(G, \cdot)$ abelsche Gruppe, so ist jede Untergruppe Normalteiler (klar nach Definition).

Bemerkung 1.48. Sei $(G, \circ)$ die Gruppe aller Permutationen von $\{1, 2, 3\}$, also $|G| = 6$.
Dann ist $U = \{id, (1, 2)\}$ eine Untergruppe.
Es gilt $U \circ (2, 3) = \{(2, 3), (3, 1, 2)\} \neq (2, 3) \circ U = \{(2, 3), (1, 3, 2)\}$, also ist U nicht Normalteiler von G.

1.4 Zyklische Gruppen

Definition 1.49. Erzeugendensystem
Sei $(G, \cdot)$ eine Gruppe, $E \subseteq G$, $E^{-1} := \{g^{-1} | g \in E\}$.
E heißt Erzeugendensystem von G, wenn sich jedes $g \in G$ als Produkt endlich vieler Elemente aus $E \cup E^{-1}$ darstellen läßt.

Definition 1.50. Zyklisch
Die Gruppe $(G, \cdot)$ heißt zyklisch (oder zyklische Gruppe), falls G ein einelementiges Erzeugendensystem besitzt.

Beispiel 1.51.

1. $(\mathbb{Z}, +)$ ist zyklisch mit 1 als erzeugendes Element.

2. Seien $n \in \mathbb{N}$ fest gewählt,
   $\zeta_n := \cos\left(\frac{2\pi}{n}\right) + i \cdot sin\left(\frac{2\pi}{n}\right)$ (n-te Einheitswurzel),
   $E_n := \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$.
   Dann ist $(E_n, \cdot)$ zyklische Gruppe der Ordnung n mit ζ_n als erzeugendem Element (Gruppe der n-ten Einheitswurzeln).

3. Im Beispiel 4 auf Seite 12 wurde eine zyklische Gruppe der Ordnung 4 betrachtet.

Bemerkung 1.52. Seien $(G, \cdot)$ eine endliche Gruppe, $g \in G$ und m die kleinste natürliche Zahl mit $g^m = g^i$, für ein i mit $0 \leq i < m$. Dann gilt:

1. $g^m = e$. (m heißt Ordnung von g, auch Ord g geschrieben.)

   Beweis. Aus $g^m = g^i$ folgt $g^{m-i} = g^0 (= e)$.
   Wegen der Minimalitätseigenschaft von m folgt $i = 0$.

2. $< g >:= \{e, g, g^2, \ldots, g^{m-1}\}$ ist eine zyklische Untergruppe von G.

3. $g^i \cdot g^{m-i} = e$

Satz 1.53. Seien $(G, \cdot)$ eine endliche Gruppe und $g \in G$. Dann gilt:

1. Ord g ist Teiler von $|G|$.

2. $g^{|G|} = e$.

Beweis. Zum Beweis beider Aussagen betrachte die Untergruppe $< g >$ und wende Satz 1.41 (Lagrange) an.

Satz 1.54. Sei p eine Primzahl und $(G, \cdot)$ eine Gruppe der Ordnung p.
Dann ist $(G, \cdot)$ zyklisch und wird erzeugt von einem beliebigen $g \in G$, mit $g \neq e$ (nach Satz 1.53.1).
Bis auf Isomorphie gibt es also genau eine Gruppe der Ordnung p.

Satz 1.55. Jede Untergruppe einer zyklischen Gruppe ist selbst auch zyklisch.

Beweis. Seien $(G, \cdot)$ zyklische Gruppe mit erzeugendem Element g, U Untergruppe von G.
Dann existiert ein minimales $i \in \mathbb{N}$[1] mit $g^i \in U$.
Wir beweisen, daß g^i die Untergruppe U erzeugt:
Sei $g^m \in U$ beliebig gegeben.
Dann liefert die Division mit Rest eine Gleichung der Form $m = q \cdot i + r$ mit $0 \leq r < i$.
Daraus folgt $\underbrace{g^m}_{\in U} = \underbrace{(g^i)^q}_{\in U} \cdot g^r$, also $g^r \in U$ und damit $r = 0$.
Damit ist $g^m = (g^i)^q$. □

Satz 1.56. Seien $(G, \cdot)$ eine Gruppe, $\lambda \in \mathbb{Z}$ und $a \in G$ besitze die Ordnung n. Dann gilt:

$$a^\lambda = e \Leftrightarrow n | \lambda$$

Beweis. Division von λ durch n mit Rest liefert eine Gleichung der Form $\lambda = \mu \cdot n + r$ mit $\mu \in \mathbb{Z}$, $0 \leq r < n$. Dann gilt: $a^\lambda = e \Leftrightarrow a^r = e \Leftrightarrow r = 0$. □

Satz 1.57. Sei $(G, \cdot)$ Gruppe und $a \in G$ besitze die Ordnung n.
Dann besitzt a^m die Ordnung $\frac{n}{\mathrm{ggT}(n,m)}$.

Beweis. Gesucht ist die kleinste natürliche Zahl q mit $(a^m)^q = e$.
Nach Satz 1.56 muß $m \cdot q$ Vielfaches von n sein und $m \cdot q$ ist trivialerweise Vielfaches von m. Das kleinste gemeinsame Vielfache von n und m ist $\frac{n \cdot m}{ggT(n,m)}$. □

Satz 1.58.
Sei g erzeugendes Element der zyklischen Gruppe $(G, \cdot)$ mit $|G| = n \in \mathbb{N}$.
Dann besitzt G zu jedem $d \in \mathbb{N}$ mit $d | n$ genau eine Untergruppe U_d der Ordnung d. U_d wird erzeugt von $g^{\frac{n}{d}}$ (U_d ist also zyklisch).
Weitere Untergruppen besitzt $(G, \cdot)$ nicht.

Beweis. Nach Satz 1.55 besitzt G nur zyklische Untergruppen.
Nach Satz 1.57 erzeugt $g^{\frac{n}{d}}$ eine Untergruppe U_d der Ordnung d für jedes $d | n$.

[1] Dabei ist $\mathbb{N}$ definiert durch $\mathbb{N} := \{1, 2, 3, \dots\}$.

Seien nun U_d und $U'_d := < g^\lambda >$ Untergruppen der Ordnung d.
Zu zeigen ist: $U'_d = U_d$.
Nach Satz 1.57 ist $\frac{n}{\text{ggT}(\lambda,n)} = d$, also ist λ Vielfaches von $\frac{n}{d}$.
Also liegt g^λ in der von $g^{\frac{n}{d}}$ erzeugten Untergruppe U_d.
Es folgt $U'_d \subseteq U_d$, also auch $U'_d = U_d$. □

Satz 1.59. Seien $(G, \cdot)$ eine abelsche Gruppe und $a, b \in$ G mit teilerfremder Ordnung.
Dann ist Ord $a \cdot b =$ Ord $a \cdot$ Ord b.

Beweis. Seien n die Ordnung von a und m die Ordnung von b.
Offenbar ist $(a \cdot b)^{n \cdot m} = a^{n \cdot m} \cdot b^{n \cdot m} = e$ (weil $(G, \cdot)$ abelsch ist).
Sei $(a \cdot b)^\lambda = a^\lambda \cdot b^\lambda = e$.
Dann folgt $a^{\lambda \cdot n} \cdot b^{\lambda \cdot n} = b^{\lambda \cdot n} = e$.
Nach Satz 1.56 ist $\lambda \cdot n$ Vielfaches von m, und wegen der Voraussetzung $\text{ggT}(n, m) = 1$ ist auch λ Vielfaches von m.
Analog ist λ Vielfaches von n. Wegen $\text{ggT}(n, m) = 1$ ist dann λ auch Vielfaches von $n \cdot m$. □

1.5 Permutationsgruppen

Definition 1.60. Transformation, Permutation
Seien M eine nicht leere Menge und $\varphi : M \to M$ eine bijektive Abbildung. Dann heißt φ Transformation von M. Ist M endlich, so heißt φ auch Permutation von M.

Bemerkung 1.61. Transformationsgruppe
Sei M eine nicht leere Menge, S_M die Menge aller Transformationen von M. Dann ist $(S_M, \circ)$ eine Gruppe.
Eine Untergruppe von S_M heißt Transformationsgruppe von M.
$(S_n, \circ)$ bezeichnet die Gruppe aller Permutationen einer Menge von n Elementen. Sie ist bis auf Isomorphie eindeutig und heißt Permutationsgruppe vom Index n (oder symmetrische Gruppe vom Index n).
Es gilt $|S_n| = n!$

Satz 1.62. Jede Gruppe $(G, \cdot)$ ist zu einer Transformationsgruppe isomorph.
Genauer: Für beliebiges $a \in G$ sei $f_a : G \to G$ definiert durch $f_a(g) := a \cdot g$.
Dann gilt:

1. f_a ist bijektiv.
2. Sei $F_G := \{f_a | a \in G\}$. Dann ist $(F_G, \circ)$ eine Gruppe. (Als Untergruppe von $(S_G, \circ)$, also auch Transformationsgruppe.)

3. $\varphi : G \to F_G$ definiert durch $\varphi(g) := f_g$ ist ein Gruppen-Isomorphismus.

Beweis.

1. klar
2. (a) Die Komposition ist assoziativ.
   (b) $f_e = id$ ist neutrales Element.
   (c) Es gilt $f_{a^{-1}} \circ f_a = id$. Also ist $f_{a^{-1}}$ Linksinverses zu f_a.
   (d) Für $f_a, f_b \in F_G$ gilt $f_a \circ f_b = f_{a \cdot b} \in F_G$.
3. Trivialerweise ist φ surjektiv. Ferner gilt:
   $f_g = f_{g'} \Rightarrow g = f_g(e) = f_{g'}(e) = g'$. Also φ ist injektiv.
   Unter Verwendung von 2(d) erhält man
   $\varphi(a \cdot b) = f_{a \cdot b} = f_a \circ f_b = \varphi(a) \circ \varphi(b)$.
   Also φ ist Homomorphismus. □

Eigenschaften von Permutationen

Sei $n \in \mathbb{N},\ n > 1$ und $f \in S_n$. Eine Möglichkeit f darzustellen ist

die Funktionstafel: $\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$

Spezielle Permutationen sind Zyklen. Ein Zyklus $(a_1, \dots, a_m)$ der Länge m ist definiert durch

$$a_1 \mapsto a_2 \mapsto \dots \mapsto a_m \mapsto a_1$$

wobei die von $a_1, \dots, a_m$ verschiedene Elemente auf sich abgebildet werden.

Definition 1.63. Transposition
Ein Zyklus der länge 2 heißt Transposition.
Eine Transposition vertauscht also zwei Elemente und läßt die anderen fest.

Ohne Beweis benutzen wir aus der Linearen Algebra:

Bemerkung 1.64. Signum

1. Jede Permutation ist Produkt elementefremder Zyklen (eindeutig bis auf die Reihenfolge).
2. Jede Permutation ist Produkt von Transpositionen (nicht eindeutig).
3. Sei $\pi \in S_n$ mit $\pi = t_1 \circ \dots \circ t_m = s_1 \circ \dots \circ s_{m'};\ t_i,\ s_j$ Transpositionen. Dann folgt $(-1)^m = (-1)^{m'}$.

$\operatorname{sgn} \pi := (-1)^m$ heißt Signum, Signatur oder Parität von π.
π heißt gerade, falls $\operatorname{sgn} \pi = 1$ und π heißt ungerade, falls $\operatorname{sgn} \pi = -1$.

Bemerkung 1.65.

1. $\operatorname{sgn} \mathrm{id} = 1$ (beachte: $\mathrm{id} = (1,2)(2,1)$).

2. $\operatorname{sgn} \pi = \operatorname{sgn} \pi^{-1}$.
   (Beachte: Ist $\pi = t_1 \circ \cdots \circ t_k$ eine Darstellung von π als Produkt von Transpositionen, so folgt $\pi^{-1} = t_k \circ \cdots \circ t_1$ wegen $t_i^2 = \mathrm{id}$.)

3. $\operatorname{sgn} (\pi_1 \circ \pi_2) = \operatorname{sgn} \pi_1 \cdot \operatorname{sgn} \pi_2$.

Satz 1.66. Alternierende Gruppe
$A_n := \{\pi \in S_n | \operatorname{sgn} \pi = 1\}$ ist Untergruppe von S_n und heißt alternierende Gruppe vom Index n. Es gilt $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ (da $\varphi : A_n \to S_n \setminus A_n$ definiert durch $\varphi(\pi) := (1,2) \circ \pi$ bijektiv ist), also ist $[S_n : A_n] = 2$ und damit ist A_n Normalteiler von S_n (nach Satz 1.46).

1.6 Beispiele von Gruppen

Satz 1.67. Quaternionengruppe
Seien

$$e := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i' := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ k := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Dann bilden die 8 komplexen Matrizen $\pm e,\ \pm i',\ \pm j,\ \pm k$ bezüglich der Matrizenmultiplikation eine nichtkommutative Gruppe $(G, \cdot)$. Diese Gruppe heißt Quaternionengruppe.

Beweis. Es gilt:

1. $(i')^2 = j^2 = k^2 = -e$.

2. $i' \cdot j = k$.
   $j \cdot i' = -k$.

3. $j \cdot k = i'$.
   $k \cdot j = -i'$.

4. $k \cdot i' = j$.
   $i' \cdot k = -j$.

Also ist $\cdot$ eine nicht kommutative Verknüpfung auf G. Die Matrizenmultiplikation ist assoziativ, also ist $(G, \cdot)$ eine Halbgruppe. Offenbar ist e neutrales Element. Die oben angegebenen Verknüpfungsergebnisse zeigen auch, daß jedes Element ein Inverses besitzt. □

Die Quaternionengruppe spielt eine Rolle bei der Konstruktion des Quaternionenschiefkörpers in Ergänzung 2.78.

Satz 1.68. Seien

$$\pi_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & (n-1) & n \\ 1 & n & (n-1) & (n-2) & \dots & 3 & 2 \end{pmatrix} \in S_n \text{ und}$$

$$\pi_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & (n-1) & n \\ 2 & 3 & 4 & \dots & & n & 1 \end{pmatrix} \in S_n.$$

Dann gilt:

1. $\pi_2 \circ \pi_1 = \pi_1 \circ \pi_2^{-1}$
2. Die von π_1 und π_2 erzeugte Untergruppe von $(S_n, \cdot)$ hat für $n \geq 3$ die Ordnung $2n$ und ist nicht kommutativ.

Sie heißt Diedergruppe von Index n und wird mit D_n bezeichnet.

Beweis.

1. Gezeigt wird $\pi_2 \circ \pi_1 \circ \pi_2 = \pi_1$.
   Es gilt $\pi_2 \circ \pi_1 \circ \pi_2(1) = 1 = \pi_1(1)$;
   $\pi_2 \circ \pi_1 \circ \pi_2(n) = 2 = \pi_1(n)$.
   Für $i \neq 1, n$ gilt $\pi_2 \circ \pi_1 \circ \pi_2(i) = \pi_2 \circ \pi_1(i+1) = \pi_2(n-(i-1)) = n - i + 2 = \pi_1(i)$.

2. Offenbar besitzt π_1 die Ordnung 2, π_2 die Ordnung n. Wegen 1 kann also D_n $(n \geq 3)$ nicht kommutativ sein. Wegen 1 gilt $\pi_2 \circ \pi_1 = \pi_1 \circ \pi_2^{n-1}$. Die gesuchte Gruppe enthält also nur die Elemente

   $$\pi_1^\lambda \circ \pi_2^\mu, \ 0 \leq \lambda \leq 1, \ 0 \leq \mu \leq n-1.$$

   Zu zeigen bleibt noch, daß diese Elemente paarweise verschieden sind.
   Dazu nehmen wir $\pi_1^\lambda \circ \pi_2^\mu = \pi_1^{\lambda'} \circ \pi_2^{\mu'}$ an.
   Ist $\lambda = \lambda'$, so folgt $\mu = \mu'$, also die Behauptung.
   Ist $\lambda \neq \lambda'$, etwa $\lambda = 0, \ \lambda' = 1$, so folgt $\pi_1 = \pi_2^{\mu - \mu'}$.
   Wegen $\pi_1(1) = 1 = \pi_2^{\mu-\mu'}(1)$ gilt $\pi_2^{\mu-\mu'} = \mathrm{id}$, also $\mu' = \mu$.
   Daraus folgt $\pi_1^\lambda = \pi_1^{\lambda'}$, also $\lambda = \lambda'$ im Widerspruch zur Voraussetzung.

□

Bemerkung 1.69. D_n $(n \geq 3)$ besitzt eine einfache geometrische Deutung. Die Ecken eines regelmäßigen n-Ecks seien etwa im Uhrzeigersinn mit $1, 2, \ldots, n$ durchnummeriert. Der Mittelpunkt des n-Ecks sei M.
Dann bedeutet π_1 eine Spiegelung an der durch 1 und M bestimmmten Symmetrieachse und π_2 eine Drehung um M im Uhrzeigersinn um $\frac{2\pi}{n}$.

1.7 Gruppenhomomorphismen

Definition 1.70. Seien $(G, \circ)$, $(H, \cdot)$ Gruppen und $\varphi : G \to H$ eine Abbildung.
$\varphi : G \to H$ heißt (Gruppen-) Homomorphismus, wenn φ relationstreu ist; das heißt:

$$\varphi(a \circ b) = \varphi(a) \cdot \varphi(b) \text{ für alle } a, b \in G.$$

$\varphi : G \to H$ heißt (Gruppen-) Isomorphismus, falls φ außerdem bijektiv ist (vergleiche Definition 1.21 auf Seite 8).
Ein (Gruppen-) Isomorphismus $\varphi : G \to G$ heißt Automorphismus (von G).
Existiert ein (Gruppen-) Isomorphismus $\varphi : G \to H$, so heißen G und H isomorphe Gruppen (in Zeichen: $G \cong H$).

Einfache Eigenschaften von Gruppenhomomorphismen sind zusammengefaßt in

Satz 1.71. (Gruppen-) Homomorphismen
Seien $(G, \circ)$, $(H, \cdot)$ Gruppen mit neutralen Elementen e, e' und $\varphi : G \to H$ Homomorphismus. Dann gilt:

1. $\varphi(e) = e'$ und $\varphi(g^{-1}) = \varphi(g)^{-1}$ für alle $g \in G$.

2. U Untergruppe von $G \Rightarrow \varphi(U)$ Untergruppe von H.
   Insbesondere ist $\varphi(G)$ Untergruppe von H.
   N Normalteiler von $G \Rightarrow \varphi(N)$ Normalteiler von $\varphi(G)$.

3. V Untergruppe von $H \Rightarrow \varphi^{-1}(V)$ Untergruppe von G.
   V Normalteiler von $H \Rightarrow \varphi^{-1}(V)$ Normalteiler von G.
   Insbesondere ist $\varphi^{-1}(\{e'\})$ (der Kern von φ) Normalteiler von G.

4. G ist abelsch $\Rightarrow \varphi(G)$ ist abelsch.

5. G ist zyklisch $\Rightarrow \varphi(G)$ ist zyklisch.
   Genauer: Erzeugt g die Gruppe G, so erzeugt $\varphi(g)$ die Gruppe $\varphi(G)$.

6. φ Isomorphismus $\Rightarrow \varphi^{-1}$ Isomorphismus.

7. Sind $\varphi_1 : G \to H,\ \varphi_2 : H \to S$ Homomorphismen, so auch $\varphi_1 \circ \varphi_2 : G \to S$.

8. Sei $Aut\ G := \{\varphi | \varphi : G \to G \text{ ist Automorhismus}\}$.
   Dann ist $(Aut\ G, \circ)$ eine Gruppe und heißt Automorphismengruppe von G.

9. Seien $x \in G,\ \varphi_x : G \to G$ definiert durch $\varphi_x(g) := x \circ g \circ x^{-1}$.
   Dann ist φ_x ein Automorphismus von G.
   φ_x heißt innerer Automorphismus von G.

10. Die inneren Automorphismen von G bilden eine Untergruppe von Aut G (sogar einen Normalteiler, siehe Übungen).

11. φ injektiv $\Leftrightarrow$ Ker $\varphi = \{e\}$.

Satz 1.72. Faktorgruppe
Seien $(G, \circ)$ Gruppe, N Normalteiler von G und $G/N := \{aN | a \in G\}$ (in Worten: G nach N) die Menge der Nebenklassen von N. Dann gilt:

1. Durch $(aN) \cdot (bN) := (a \circ b)N$ wird eine Verknüpfung $\cdot$ auf G/N definiert.

2. $(G/N, \cdot)$ ist eine Gruppe (die Faktorgruppe G nach N).

Beweis.

1. Zu zeigen ist, daß das Verknüpfungsergebnis unabhängig von der Wahl der Repräsentanten der Nebenklassen ist (also wohldefiniert ist):
   Seien $aN = a'N,\ bN = b'N$.
   Dann wird $(a \circ b)N = (a' \circ b')N$ gezeigt.
   Für geeignete $n_1, n_2 \in N$ gilt $a = a' \circ n_1,\ b = b' \circ n_2$.
   Dann folgt $a \circ b = a' \circ n_1 \circ b' \circ n_2$.
   Da N Normalteiler ist gilt $n_1 \circ b' = b' \circ n_1'$ für geeignetes $n_1' \in N$.
   Es folgt $a \circ b = a' \circ b' \circ \underbrace{n_1' \circ n_1}_{\in N} \in (a' \circ b')N$. Also $(a \circ b)N = (a' \circ b')N$.

2. $eN = N$ ist neutrales Element.
   $a^{-1}N$ ist zu aN invers.
   Die Assoziativität von $\cdot$ folgt direkt aus der Assoziativität von $\circ$. $\square$

Beispiel 1.73. Sei $n \in \mathbb{N}$.
Dann ist $n\mathbb{Z} := \{n \cdot z | z \in \mathbb{Z}\}$ eine Untergruppe der kommutativen Gruppe $(\mathbb{Z}, +)$, also auch Normalteiler.
Die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ hat die Elemente $\{n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$ und wird erzeugt von $1 + n\mathbb{Z}$, ist also zyklisch.

Der folgende Satz ist ein wichtiges Hilfsmittel in der Gruppentheorie.

Satz 1.74. Kanonischer Homomorphismus, Homomorphiesatz

1. Kanonischer Homomorphismus
   Seien $(G, \circ)$ Gruppe, N Normalteiler von G.
   Dann ist $\psi : G \to G/N$ definiert durch $\psi(g) := gN$ ein surjektiver Homomorphismus mit Ker $\psi = N$.

2. Homomorphiesatz
   Sei $\varphi : G \to H$ Gruppenhomomorphismus.
   Dann ist $f : G/(\text{Ker } \varphi) \to \varphi(G)$ definiert durch $f(a\text{Ker } \varphi) := \varphi(a)$ ein Isomorphismus.
   Bemerkung: Ker φ ist Normalteiler.

Beweis.

1. ψ ist relationstreu wegen
   $\psi(g_1 \circ g_2) = (g_1 \circ g_2)N = g_1N \cdot g_2N = \psi(g_1) \cdot \psi(g_2)$.
   Der Rest ist klar.

2. Zunächst wird gezeigt, daß f wohldefiniert ist. Sei $a\text{Ker } \varphi = a'\text{Ker } \varphi$.
   Dann ist $\varphi(a) = \varphi(a')$ zu zeigen:
   Für ein geeignetes $g \in \text{Ker } \varphi$ gilt $a = a' \circ g$.
   Es folgt $\varphi(a) = \varphi(a' \circ g) = \varphi(a') \cdot \varphi(g) = \varphi(a')$.
   Ferner ist f surjektiv, da ein beliebiges Element $\varphi(a) \in \varphi(G)$ als Urbild $a\text{Ker } \varphi$ besitzt.
   f ist offenbar relationstreu, also Homomorphismus.
   f ist injektiv, da der Kern trivial ist. □

Bemerkung 1.75.
Ist G eine unendliche zyklische Gruppe, so ist $G \cong \mathbb{Z}$.
Ist G eine endliche zyklische Gruppe der Ordnung $n < \infty$, so ist $G \cong \mathbb{Z}_n$.

Beweis. Sei g erzeugendes Element von G.
Dann ist $\varphi : \mathbb{Z} \to G$ definiert durch $\varphi(z) := g^z$ ein surjektiver Homomorphismus.
Im Fall $|G| = \infty$ ist der Kern trivial.

Im Fall $|G| = n < \infty$ ist der Kern $n\mathbb{Z}$.
Nach dem Homomorphiesatz (Satz 1.74) folgt die Behauptung. □

Satz 1.76. Reduktionssatz oder 1. Isomorphiesatz
Seien $(G, \cdot)$ Gruppe, U Untergruppe, N Normalteiler, von G
$UN := \{u \cdot n | u \in U,\ n \in N\}$. Dann gilt:

1. UN ist Untergruppe von G, und zwar die kleinste Untergruppe die $U \cup N$ enthält.

2. $U \cap N$ ist Normalteiler von U und N ist Normalteiler von UN.

3. $UN/N \cong U/(U \cap N)$

Beweis.

1. Seien $u_1n_1, u_2n_2 \in UN$ mit $u_1, u_2 \in U$ und $n_1, n_2 \in N$. Dann gilt $(u_1n_1)(u_2n_2)^{-1} = u_1 \underbrace{n_1n_2^{-1}}_{\in N} u_2^{-1} = u_1u_2^{-1} \cdot n_3 \in UN$ für ein geeignetes $n_3 \in N$ (wegen $u_2^{-1}N = Nu_2^{-1}$). Nach Satz 1.36 (Untergruppenkriterium) auf Seite 13 folgt die Behauptung.

2. Nach dem Homomorphiesatz ist $\varphi : G \to G/N$ definiert durch $\varphi(g) := gN$ ein surjektiver Homomorphismus mit N als Kern.
   Sei φ' die Einschränkung von φ auf U.
   Dann ist $\varphi' : U \to G/N$ ein Homomorphismus mit $N \cap U$ als Kern.
   Nach Satz 1.71.3 ist dann $N \cap U$ Normaltieler von U.
   Sei φ'' die Einschränkung von φ auf UN.
   Dann ist $\varphi'' : UN \to G/N$ ein Homomorphismus mit N als Kern.
   Nach Satz 1.71.3 ist dann N Normaltieler von UN.

3. $\psi : U \to UN/N$ definiert durch $\psi(u) := uN$ ist surjektiver Homomorphismus mit $N \cap U$ als Kern.
   Nach dem Homomorphiesatz sind $U/(U \cap N)$ und UN/N Isomorph. □

Satz 1.77. Kürzungssatz oder 2. Isomorphiesatz
Sei $(G, \cdot)$ eine Gruppe, $U \subseteq V$ seien Normalteiler von G.
(U ist Normalteiler von V nach Bemerkung 1.44.) Dann gilt:

1. V/U ist Normalteiler von G/U.

2. $G/V \cong G/U \big/ V/U$.

Beweis. Sei $\varphi : G/U \to G/V$ definiert durch $\varphi(gU) := gV$.
Dann ist φ wohldefiniert, denn es gilt:
$gU = g'U \Rightarrow g \in g'U \subseteq g'V \Rightarrow gV = g'V$.
φ ist Homomorphismus.
φ ist surjektiv.
Ker $(\varphi) = V/U$. Nach Satz 1.71.3 ist V/U Normalteiler von G/U, und nach Satz 1.74 auf Seite 25 folgt die Behauptung 2. □

1.8 Normalisator, Zentralisator

Definition 1.78. Konjugiert
Seien $(G, \cdot)$ eine Gruppe; $g, g' \in G$; U, U' Untergruppen von G.
Dann werden eine Relation $\sim$ auf G und eine Relation $\sim$ auf der Menge der Untergruppen von G definiert durch

$$g \sim g' :\Leftrightarrow \exists x \in G \text{ mit } g = xg'x^{-1}$$
$$U \sim U' :\Leftrightarrow \exists x \in G \text{ mit } U = xU'x^{-1}.$$

g und g' heißen konjugiert, falls $g \sim g'$.
U und U' heißen konjugiert, falls $U \sim U'$.

Bemerkung 1.79. $\sim$ ist Äquivalenzrelation auf G.
$\sim$ ist Äquivalenzrelation auf der Menge der Untergruppen von G.

Beweis.
Es gilt $g = ege^{-1}$, also $g \sim g$.
$g \sim g' \Rightarrow g = xg'x^{-1}$ für ein geeignetes $x \in G \Rightarrow g' = x^{-1}gx \Rightarrow g' \sim g$.
Gelte $g_1 \sim g_2$, $g_2 \sim g_3$; etwa $g_1 = xg_2x^{-1}$, $g_2 = yg_3y^{-1}$ mit $x, y \in G$.
Dann folgt $g_1 = xyg_3 \underbrace{y^{-1}x^{-1}}_{(xy)^{-1}}$, also $g_1 \sim g_3$.
(Für Untergruppen analog).

Definition 1.80. Normalisator
Seien $(G, \cdot)$ eine Gruppe, $g \in G$, U Untergruppe von G.
Dann heißt $M_g := \{m \in G | mgm^{-1} = g\}$ Normalisator von g
und $M_U := \{m \in G | mUm^{-1} = U\}$ Normalisator von U.
(beachte: $mUm^{-1} = U \Leftrightarrow mU = Um$.)

Satz 1.81. Sei $(G, \cdot)$ eine Gruppe, $g \in G$, M_g der Normalisator von g. Dann gilt:

1. M_g ist Untergruppe von G.

2. $mgm^{-1} = ngn^{-1} \Leftrightarrow mM_g = nM_g$.

3. Die Anzahl der verschiedenen zu g konjugierten Elemente ist $[G : M_g]$; also Teiler von $|G|$, falls $|G|$ endlich.

Beweis.

1. (a) $e \in M_g$.
   (b) $m_1, m_2 \in M_g \Rightarrow m_1 m_2 g \underbrace{(m_1 m_2)^{-1}}_{m_2^{-1} m_1^{-1}} = g \Rightarrow m_1 \cdot m_2 \in M_g$.
   (c) $m \in M_g \Rightarrow mgm^{-1} = g \Rightarrow m^{-1}gm = g \Rightarrow m^{-1} \in M_g$.

2. $mgm^{-1} = ngn^{-1} \Leftrightarrow n^{-1}mg \underbrace{m^{-1}n}_{(n^{-1}m)^{-1}} = g \Leftrightarrow n^{-1}m \in M_g \Leftrightarrow mM_g = nM_g$.

3. Folgt aus 1. und 2.

Analog zu Satz 1.81 gilt:

Satz 1.82.
Seien $(G, \cdot)$ eine Gruppe, U eine Untergruppe von G, M_U der Normalisator von U. Dann gilt:

1. M_U ist Untergruppe von G (genauer: größte Untergruppe von G, in der U Normalteiler ist).

2. $mUm^{-1} = nUn^{-1} \Leftrightarrow mM_U = nM_U$.

3. Die Anzahl der verschiedenen zu U konjugierten Untergruppen ist $[G : M_U]$; also Teiler von $|G|$, falls $|G|$ endlich.

Beweis. analog zu Satz 1.81.

Definition 1.83. Zentralisator
Seien $(G, \cdot)$ eine Gruppe, $M \subseteq G$.
Dann heißt $Z_M := \{g \in G | \underbrace{gmg^{-1} = m}_{(\Leftrightarrow gm = mg)} \ \forall m \in M\}$ der Zentralisator von M.
Speziell heißt $Z_G = \{g \in G | gmg^{-1} = m \ \forall m \in G\}$ das Zentrum von G.

Bemerkung 1.84. Der Zentralisator von M ist eine Untergruppe von G.
Das Zentrum Z_G von G enthält genau alle Elemente $g \in G$ mit $gm = mg$ für alle $m \in G$.
Also gilt: $Z_G = G \Leftrightarrow G$ abelsch.
Das Zentrum ist ein Normalteiler von G.

1.9 Direkte Produkte, abelsche Gruppen

Seien $(G_1, \cdot)$, $(G_2, \cdot)$ zwei Gruppen. Definiere auf $G_1 \times G_2$ eine Verknüpfung $\cdot$ durch

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2').$$

Dann ist $(G_1 \times G_2, \cdot)$ eine Gruppe (das direkte Produkt von G_1 und G_2). Analog wird das direkte Produkt endlich vieler Gruppen gebildet.

Bemerkung 1.85. Das direkte Produkt abelscher Gruppen ist abelsch.

Satz 1.86. Seien $(G_1, \cdot)$, $(G_2, \cdot)$ zyklische Gruppen und endlich. Dann gilt:

$$(G_1 \times G_2, \cdot) \text{ ist zyklisch} \Leftrightarrow \mathrm{ggT}(|G_1|, |G_2|) = 1.$$

Beweis. Sei g_i erzeugendes Element von G_i für $i \in \{1, 2\}$, also $g_i^{\alpha_i} = e_i$ genau dann, wenn $|G_i| | \alpha_i$.
Sei zunächst $\mathrm{ggT}(|G_1|, |G_2|) = d > 1$.
Dann ist $v := \frac{|G_1| \cdot |G_2|}{d}$ Vielfaches von $|G_1|$ und $|G_2|$, und für ein beliebiges Element $(g_1^{\alpha_1}, g_2^{\alpha_2}) \in G_1 \times G_2$ folgt $(g_1^{\alpha_1}, g_2^{\alpha_2})^v = (g_1^{\alpha_1 \cdot v}, g_2^{\alpha_2 \cdot v}) = (e_1, e_2)$.
Also ist $(G_1 \times G_2)$ nicht zyklisch.
Sei nun $\mathrm{ggT}(|G_1|, |G_2|) = 1$ und $(g_1, g_2)^\lambda = (e_1, e_2)$. Dann ist λ Vielfaches von $|G_1|$ und $|G_2|$, also auch von $|G_1| \cdot |G_2|$. (g_1, g_2) erzeugt also $G_1 \times G_2$.

Satz 1.87. Seien $(G_n, \cdot)$ zyklische Gruppe der Ordnung $n = p_1^{a_1} \cdots p_r^{a_r}$, p_i paarweise verschiedene Primzahlen, $a_i \in \mathbb{N}$.
Dann ist $(G_n, \cdot)$ isomorph zu einem direkten Produkt zyklischer Gruppen $(G_{p_i^{a_i}}, \cdot)$ der Ordnung $p_i^{a_i}$:

$$G_n \cong G_{p_1^{a_1}} \times \cdots \times G_{p_r^{a_r}}.$$

Beweis. Nach Satz 1.86 ist $(G_{p_1^{a_1}} \times \cdots \times G_{p_r^{a_r}}, \cdot)$ zyklisch von der Ordnung n. Andererseits gibt es bis auf Isomorphie nur eine zyklische Gruppe der Ordnung n nach Bemerkung 1.75.

Satz 1.88. Hauptsatz über endlich erzeugte abelsche Gruppen.
Jede endlich erzeugte abelsche Gruppe ist isomorph zu einem direkten Produkt zyklischer Gruppen.
Zusammen mit Satz 1.87 ergibt sich:
Jede endliche abelsche Gruppe ist isomorph zu einem direkten Produkt zyklischer Gruppen von Primzahlpotenzordnung.
Darüber hinaus sind die Faktoren bis auf die Reihenfolge eindeutig bestimmt.

Beweis. Siehe [2] durch vollständige Induktion, [3] im Rahmen der Modultheorie.

Beispiel 1.89.
Seien p eine Primzahl, $(G_p, \cdot)$ zyklische Gruppe der Ordnung p, $(G_{p^2}, \cdot)$ zyklische Gruppe der Ordnung p^2.
Dann sind $(G_{p^2}, \cdot), (G_p \times G_p, \cdot)$ die einzigen abelschen Gruppen der Ordnung p^2 (bis auf Isomorphie).
Der Beweis folgt direkt aus Satz 1.88.

Satz 1.90. Inneres Direktes Produkt
Seien N_1, N_2 Normalteiler der Gruppe $(G, \cdot)$ mit $N_1 \cap N_2 = \{e\}$ und $N_1 \cdot N_2 := \{n_1 \cdot n_2 | n_1 \in N_1, n_2 \in N_2\} = G$. Dann gilt:

1. Jedes $g \in G$ läßt sich eindeutig darstellen in der Form $g = n_1 \cdot n_2$ mit $n_1 \in N_1, n_2 \in N_2$.
2. $n_1 \cdot n_2 = n_2 \cdot n_1$ für alle $n_1 \in N_1, n_2 \in N_2$.
3. $\varphi : G \to N_1 \times N_2$ definiert durch $\varphi(g) := (n_1, n_2)$ für alle $g = n_1 \cdot n_2 \in G$ ist ein Isomorphismus.
   Man sagt kurz: G ist inneres direktes Produkt von N_1, N_2.

Beweis.

1. Die Existenz der Darstellung ist klar nach Voraussetzung.
   Gelte $n_1 \cdot n_2 = n_1' \cdot n_2'$ mit $n_1, n_1' \in N_1$ und $n_2, n_2' \in N_2$.
   Dann folgt $n_1'^{-1} \cdot n_1 = n_2' \cdot n_2^{-1} \in N_1 \cap N_2$, also $n_1'^{-1} \cdot n_1 = e = n_2' \cdot n_2^{-1}$, und damit $n_1 = n_1', n_2 = n_2'$.
2. $n_1 n_2 = n_2 n_1$ ist gleichwertig mit $n_2^{-1} n_1 n_2 n_1^{-1} = e$.
   Andererseits gilt $n_2^{-1} \underbrace{n_1 n_2 n_1^{-1}}_{\in N_2} \in N_2$ und $\underbrace{n_2^{-1} n_1 n_2}_{\in N_1} n_1^{-1} \in N_1$.
3. Folgt aus 1 und 2.

1.10 Einbettung von Halbgruppen in Gruppen

Sei $(H, \cdot)$ Halbgruppe, also $\cdot$ ist assoziative Verknüpfung. Untersucht werden soll die Frage, wann eine Gruppe $(G, \cdot)$ existiert, die eine zu H isomorphe Halbgruppe enthält.
Existiert eine solche Gruppe $(G, \cdot)$, so ist $(H, \cdot)$ regulär.
Die Umkehrung gilt nicht (siehe [1] Seite 115), aber es gilt:

Satz 1.91.
Sei $(H, \cdot)$ kommutative, reguläre Halbgruppe.
Dann existiert eine Gruppe $(G, \cdot)$, die eine zu $(H, \cdot)$ isomorphe Halbgruppe enthält.

Beweis. Um einen Leitfaden für die Konstruktion von $(G,\cdot)$ zu bekommen, führen wir die folgende Vorbetrachtung durch.
Wir nehmen an, daß $(G,\cdot)$ eine Gruppe ist, die H enthält.
Da H abelsch ist, gelten für alle $a,b \in H$ die Gleichungen $ab = ba$ und $b^{-1}a = ab^{-1}$.
Dann ist $U := \{ab^{-1} | a,b \in H\}$ eine Untergruppe von G nach Satz 1.36 (Untergruppenkriterium) auf Seite 13.
Ferner gilt $H \subseteq U$ weil $\underbrace{aa}_{\in H} a^{-1} = a \in U$ für alle $a \in H$, und U ist eine minimale Untergruppe von G mit $H \subseteq U$.
Da H abelsch ist, gilt $ab = ba$, also $b^{-1}a = ab^{-1}$.
Ausserdem gilt $ab^{-1} = cd^{-1} \Leftrightarrow ad = bc$.
Wir nehmen uns U als Vorbild für die Konstruktion der gesuchten Gruppe $(G,\cdot)$.
Sei $M := H \times H$.
Auf M wird eine Relation $\sim$ definiert durch

$$(a,b) \sim (c,d) :\Leftrightarrow ad = bc.$$

Es ist leicht zu zeigen, daß $\sim$ Äquivalenzrelation ist.
$[a,b]$ bezeichne die von (a,b) erzeugte Äquivalenzklasse.
Sei G die Menge der Äquivalenzklassen.
Auf G wird eine Verknüpfung $\cdot$ definiert durch

$$[a,b] \cdot [c,d] := [ac, bd].$$

Die Zuordnung ist wohldefiniert, denn aus $(a,b) \sim (a',b') \wedge (c,d) \sim (c'd')$ also $ab' = a'b \wedge cd' = dc'$ folgt $acb'd' = bda'c'$ also $(ac,bd) \sim (a'c', b'd')$.
$(G,\cdot)$ ist Gruppe. Die Assoziativität ist offenbar erfüllt.
$[a,a]$ ist neutrales Element.
$[a,b]$ ist zu $[b,a]$ invers.
Es bleibt noch zu zeigen, daß $(G,\cdot)$ eine zu $(H,\cdot)$ isomorphe Halbgruppe enthält.
Seien $h \in H$ beliebig aber fest, $T := \{[ah,h] | a \in H\}$.
Dann ist T Unterhalbgruppe von $(G,\cdot)$, denn für beliebige $[ah,h], [bh,h] \in T$ gilt $[ah,h] \cdot [bh,h] = [abh^2, h^2] = [abh, h] \in T$.
Ferner ist $f : H \to T$ definiert durch $f(a) := [ah,h]$ surjektiv, injektiv
(wegen $[ah,h] = [bh,h] \Leftrightarrow ah^2 = bh^2 \Leftrightarrow a = b$)
und Homomorphismus (wegen $[ah,h] \cdot [bh,h] = [abh,h]$); also Isomorphismus.

Bemerkung 1.92. Die im Beweis konstruierte Gruppe G ist minimal in dem folgenden Sinn: Eine echte Untergruppe von G enthält T nicht.

Bemerkung 1.93. Als wichtigen Spezialfall von Satz 1.91 erhält man die Konstruktion von $(\mathbb{Z}, +)$ aus $(\mathbb{N}, +)$.
Hierbei wird davon ausgegangen, daß $(\mathbb{N}, +)$ eine kommutative reguläre Halbgruppe ist.
Auf eine axiomatische Beschreibung von $\mathbb{N}$ und den axiomatischen Aufbau des Zahlensystems wird im Kapitel 2 genauer eingegangen, wenn die Begriffe Integritätsbereich und Quotientenkörper zur Verfügung stehen.

Kapitel 2

Ringe

2.1 Grundbegriffe der Ringtheorie

Definition 2.1. Ring
Seien R Menge und $+, \cdot$ Verknüpfungen auf R.
$(R, +, \cdot)$ heißt Ring, wenn gilt:

1. $(R, +)$ ist abelsche Gruppe.
2. $(R, \cdot)$ ist Halbgruppe.
3. Es gilt $a(b + c) = ab + ac$ und $(b + c)a = ba + ca$ für alle $a, b, c \in R$. (Distributivgesetze)
   (Wie üblich soll $\cdot$ stets stärker binden als $+$, zum Beispiel gilt $a \cdot b + c = (a \cdot b) + c$.)

Der Ring heißt kommutativ, falls $\cdot$ kommutativ ist.
$1 \in R$ heißt Eins, falls $a \cdot 1 = 1 \cdot a = a$ für alle $a \in R$.
0 bezeichnet stets das neutrale Element von $(R, +)$.

Bemerkung 2.2.

1. Ein Ring R besitzt höchstens eine Eins (wegen $1' = 1 \cdot 1' = 1$).
2. Ein $a \in R$ besitzt höchstens ein multiplikatives Inverses.
   Ist nämlich c Rechtsinverses zu a und b Linksinverses zu a, so folgt $c = (ba)c = b(ac) = b$.
3. Ein $a \in R$ kann mehrere Rechtsinverse besitzen (siehe Übung).
   In diesem Fall hat aber a kein Linksinverses.
4. Die Definition von Unterringen erfolgt analog zu der von Untergruppen.

5. Der Durchschnitt von Unterringen eines Ringes ist auch Unterring.

Beispiel 2.3.

1. $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit Eins.
2. $(2\mathbb{Z}, +, \cdot)$ ist kommutativer Ring ohne Eins.
3. $(\{0\}, +, \cdot)$ ist kommutativer Ring mit Eins (der Nullring).
4. $R := \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ ist Unterring von $(\mathbb{R}, +, \cdot)$.
5. Seien $(R, +, \cdot)$ Ring, $n \in \mathbb{N}$, R_M die Menge aller $n \times n$ Matrizen über R.
   Dann ist $(R_M, +, \cdot)$ Ring (voller Matrizenring über R).
6. Seien $(R, +, \cdot)$ Ring, S eine nicht leere Menge,
   $R_S := \{f | f : S \to R \text{ Abbildung}\}$.
   Definiert man auf R_S zwei Verknüpfungen + und $\cdot$ durch
   $$(f + g)(s) := f(s) + g(s) \text{ und}$$
   $$(f \cdot g)(s) := f(s) \cdot g(s) \text{ für alle } s \in S,$$
   so ist $(R_S, +, \cdot)$ Ring.
7. Seien $(R_1, +, \cdot)$, $(R_2, +, \cdot)$ Ringe.
   Definiert man zwei Verknüpfungen + und $\cdot$ auf $R_1 \times R_2$ als die komponentenweise Addition und Multiplikation, also
   $$(r_1, r_2) + (r_1', r_2') := (r_1 + r_1', r_2 + r_2')$$
   $$(r_1, r_2) \cdot (r_1', r_2') := (r_1 \cdot r_1', r_2 \cdot r_2'),$$
   so ist $(R_1 \times R_2, +, \cdot)$ Ring (direktes Produkt von R_1 und R_2).
   Analog erhält man das direkte Produkt endlich vieler Ringe.
   Ist $1 \in R$, so ist $(1, 1)$ Eins im direkten Produkt $(R \times R, +, \cdot)$, und $(1, 0)$ ist Eins im Unterring $\{(r, 0) | r \in R\}$.

Satz 2.4. In einem Ring R gilt:

1. $a \cdot 0 = 0 \cdot a = 0$ für alle $a \in R$.
   $(a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 = 0)$
2. Ist $R \neq \{0\}$, $1 \in R$ so folgt $1 \neq 0$. (für $a \neq 0$ ist $a \cdot 1 = a$, $a \cdot 0 = 0$)
3. $a(-b) = (-a)b = -(ab)$ für alle $a, b \in R$.
   (Zum Beispiel gilt: $ab + a(-b) = a(b - b) = 0$ also $-ab = a(-b)$)

4. $a(b-c) = ab - (ac),\ (b-c)a = ba - ca$ für alle $a, b, c \in R$.

Definition 2.5. Nullteilerfrei
Ein Ring $(R, +, \cdot)$ heißt nullteilerfrei, wenn für alle $a, b \in R$ gilt:
$ab = 0 \Rightarrow (a = 0$ oder $b = 0)$.

Definition 2.6. Integritätsbereich
Ein kommutativer, nullteilerfreier Ring $(R, +, \cdot)$ mit $R \neq \{0\}$ heißt Integritätsbereich.

Bemerkung 2.7. In einem nullteilerfreien Ring gilt die Kürzungsregel:

$$a \neq 0,\ ab = ac \Rightarrow b = c$$
$$a \neq 0,\ ba = ca \Rightarrow b = c$$

Beweis. $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$

Bemerkung 2.8. Sei $(R, +, \cdot)$ nullteilerfreier Ring, 1_R Einselement von R, U Unterring mit $U \neq \{0\}$ und Einselement 1_U.
Dann ist $1_R = 1_U$. (Beachte Beispiel 2.3.7 auf Seite 34.)

Beweis. Unter Verwendung von Bemerkung 2.7 ergibt sich:

$$1_R \cdot 1_U = 1_U \cdot 1_U \Rightarrow 1_R = 1_U.$$

Definition 2.9. Charakteristik
Sei $(R, +, \cdot)$ Ring mit Eins, $|R| > 1$. Dann sei
Char $R := 0$, falls jede endliche Summe $1 + 1 + \cdots + 1 \neq 0$ und
Char $R := n$, falls $n \in \mathbb{N}$ minimal ist mit $\underbrace{1 + 1 + \cdots + 1}_{n-\text{mal}} = 0$.
Char R heißt Charakteristik von R.

Bemerkung 2.10. Seien $(R, +, \cdot)$ nullteilerfreier Ring mit Eins,
$R \neq \{0\},$ Char $R \neq 0$.

1. Dann ist Char R eine Primzahl.

2. Ist $(R, +, \cdot)$ kommutativ und Char $R = p$ Primzahl, so gilt:

$$(a + b)^p = a^p + b^p.$$

Beweis.

1. Annahme: Char $R = n = ab$ mit $1 < a, b < n$.
   Dann folgt aus dem Distributivgesetz
   $\underbrace{(1 + \cdots + 1)}_{a-\text{mal}} \cdot \underbrace{(1 + \cdots + 1)}_{b-\text{mal}} = \underbrace{(1 + \cdots + 1)}_{n-\text{mal}} = 0$, wegen der Nullteilerfreiheit also
   $\underbrace{(1 + \cdots + 1)}_{a-\text{mal}} = 0$ oder $\underbrace{(1 + \cdots + 1)}_{b-\text{mal}} = 0$ im Widerspruch zur Definition von n.

2. Nach Voraussetzung gilt im Ring R die Gleichung $p = 0$, also ist auch jedes Ganzzahlige Vielfache von p gleich 0. (Dabei bedeutet p die p-fache Addition von 1 mit sich selbst.)
   Nach dem Distributivgesetz gilt

   $$(a + b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p.$$

   Ferner ist $\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$ für $1 \leq i < p$ ein Vielfaches von p, da sich der Faktor p im Zähler nicht herauskürzt (weil p prim ist).

Definition 2.11. Einheit
Seien $(R, +, \cdot)$ Ring mit Eins, $R \neq \{0\}$, $a \in R$.
a heißt Einheit von R, wenn a ein multiplikatives Inverses b besitzt
(das heißt: $ab = ba = 1$).
a heißt dann auch invertierbar in R.

Bemerkung 2.12. Sei $(R, +, \cdot)$ Ring mit Eins und $R \neq \{0\}$.
Dann ist 0 nicht Einheit von R, denn es gilt $0 \cdot a = 0 \neq 1$ für alle $a \in R$.
(Siehe Satz 2.4.2)

Satz 2.13. Einheitengruppe
Seien $(R, +, \cdot)$ Ring mit Eins, $E_R := \{r \in R | r \text{ ist Einheit von } R\}$.
Dann ist $(E_R, \cdot)$ Gruppe und heißt Einheitengruppe von R.

Beweis.

1. $1 \in E_R$
2. $a \in E_R \Rightarrow a^{-1} \in E_R$.
3. $a, b \in E_R \Rightarrow abb^{-1}a^{-1} = 1 \Rightarrow ab \in E_R$.

Definition 2.14. Schiefkörper, Körper
Seien $(R, +, \cdot)$ Ring mit Eins, $R \neq \{0\}$.
$(R, +, \cdot)$ heißt Schiefkörper oder Divisorenring, wenn $(R \backslash \{0\}, \cdot)$ Gruppe ist.
Ein kommutativer Schiefkörper heißt Körper.

Satz 2.15. Ein endlicher nullteilerfreier Ring $(R, +, \cdot)$ mit $R \neq \{0\}$ ist Schiefkörper.
Jeder endliche Integritätsbereich ist also Körper.

Beweis. Seien $(R, +, \cdot)$ endlicher nullteilerfreier Ring mit $R \neq \{0\}$.
Dann ist $(R \setminus \{0\}, \cdot)$ endliche reguläre Halbgruppe nach Bemerkung 2.7.
Nach Satz 1.28 folgt die Behauptung.

Satz 2.16. Wedderburn
Jeder endliche Schiefkörper ist Körper.

Beweis. Siehe [4] Seite 67.

Satz 2.17. In Körpern gilt (der Nenner sei $\neq 0$):

$$\frac{a}{b} = \frac{ac}{bc}, \ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \ \frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}, \ \frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}.$$

Dabei sei $\frac{a}{b} := a : b := a \cdot b^{-1}$ wie üblich.

Bemerkung 2.18. Jeder Körper ist nullteilerfrei.

Beweis. Aus $ab = 0$ und $a \neq 0$ folgt $a^{-1}ab = b = 0$.

Bemerkung 2.19. Seien $(R, +, \cdot)$ Ring, $S \subseteq R$.
$[S]$ bezeichne den Durchschnitt aller Unterringe, die S enthalten.
Dann ist $[S]$ Unterring von R.
$[S]$ ist der kleinste Unterring von R, welcher S enthält.
$[S]$ heißt der von S erzeugte Unterring.
Zum Beispiel gilt: $[\emptyset] = \{0\}$.
Im Fall $S \neq \emptyset$ enthält $[S]$ genau alle endlichen Summen von endlichen Produkten von Elementen aus S, wobei die Summanden auch negative Vorzeichen haben dürfen.

2.2 Ideale, Restklassenringe, Ringhomomorphismen

Definition 2.20. (Ring-)Homomorphismus
Seien $(R_1, +, \cdot)$, $(R_2, +, \cdot)$ Ringe.
Eine Abbildung $f : R_1 \longrightarrow R_2$ heißt (Ring-)Homomorphismus, wenn gilt:

$$\begin{aligned} f(a + b) &= f(a) + f(b) \quad \text{und} \\ f(a \cdot b) &= f(a) \cdot f(b) \quad \text{für alle } a, b \in R_1 \end{aligned}$$

Ein bijektiver (Ring-)Homomorphismus heißt (Ring-)Isomorphismus.
$R_1 \cong R_2 :\Leftrightarrow$ Es existiert ein Isomorphismus $\varphi : R_1 \to R_2$.

Bemerkung 2.21.

1. Sei $(R_1 \times R_2, +, \cdot)$ das direkte Produkt der Ringe $(R_1, +, \cdot), (R_2, +, \cdot)$. $\varphi : R_1 \to R_1 \times R_2$ definiert durch $\varphi(r_1) := (r_1, 0)$ ist ein Ring-Homomorphismus.
   Ist $1 \in R_1,\ 1' \in R_2$, so gilt $\varphi(1) = (1,0) \neq (1,1')$. Ein Homomorphismus muß die Eins also nicht immer auf die Eins abbilden.

2. Sei $\varphi : R \to R'$ surjektiver Homomorphismus und $1 \in R$, so ist $\varphi(1)$ Eins in R' (wegen $\varphi(r) \cdot \varphi(1) = \varphi(r \cdot 1) = \varphi(r) = \varphi(1) \cdot \varphi(r)$).

3. Ist φ Ring-Isomorphismus, dann ist auch φ^{-1} Ring-Isomorphismus (Beweis analog wie bei Gruppen).

4. Sei $\varphi : R \to R'$ ein Ring-Homomorphismus.
   Dann gilt: φ injektiv $\Leftrightarrow$ Ker $\varphi = \{0\}$.

   Beweis. Klar, da φ ein Gruppen-Homomorphismus von $(R, +)$ ist (nach Satz 1.71.11).

Definition 2.22. Ideal
Seien $(R, +, \cdot)$ Ring, $(\mathfrak{a}, +)$ Untergruppe von $(R, +)$.
$\mathfrak{a}$ heißt Linksideal von R, wenn gilt: $r \in R,\ a \in \mathfrak{a} \Rightarrow r \cdot a \in \mathfrak{a}$.
$\mathfrak{a}$ heißt Rechtsideal von R, wenn gilt: $r \in R,\ a \in \mathfrak{a} \Rightarrow a \cdot r \in \mathfrak{a}$.
$\mathfrak{a}$ heißt Ideal von R, wenn $\mathfrak{a}$ Rechts- und Linksideal ist.

Bemerkung 2.23.

1. Jeder Ring $(R, +, \cdot)$ besitzt die trivialen Ideale $\{0\}, R$.

2. $\mathfrak{a}$ Ideal von $R \Rightarrow \mathfrak{a}$ Unterring von R.

3. $n\mathbb{Z} := \{n \cdot z | z \in \mathbb{Z}\}$ ist Ideal von $(\mathbb{Z}, +, \cdot)$ für jedes $n \in \mathbb{N}$.

4. Sei $\mathfrak{a}$ Ideal von R.
   Existiert eine Einheit $\varepsilon \in \mathfrak{a}$, so ist $\mathfrak{a} = R$, denn für alle $r \in R$ gilt: $r = (r\varepsilon^{-1})\varepsilon \in \mathfrak{a}$.
   Körper besitzen also nur die trivialen Ideale.

5. Seien $f : R_1 \to R_2$ Ringhomomorphismus, $\mathfrak{a}$ Ideal von R_2.
   Dann ist $f^{-1}(\mathfrak{a}) := \{a \in R_1 | f(a) \in \mathfrak{a}\}$ Ideal von R_1.
   Speziell ist Ker f Ideal von R_1.

Beweis. $f^{-1}(\mathfrak{a})$ ist Gruppe bezüglich $+$ (nach Satz 1.71.3.
Seien $r \in R_1,\ a \in f^{-1}(\mathfrak{a})$. Dann folgt
$f(r \cdot a) = f(r) \cdot \underbrace{f(a)}_{\in \mathfrak{a}} \in \mathfrak{a}$, also $r \cdot a \in f^{-1}(\mathfrak{a})$.

Bemerkung 2.24. Restklassenring, Kongruenz
Seien $(R, +, \cdot)$ Ring, $\mathfrak{a}$ Ideal von R.
Dann ist $\mathfrak{a}$ Normalteiler der Gruppe $(R, +)$, da $(R, +)$ abelsch ist.
Sei $(R/\mathfrak{a}, +)$ die Faktorgruppe. Sie ist abelsch, da $(R, +)$ abelsch ist.
Auf $R/\mathfrak{a}$ wird eine multiplikativ geschriebene Verknüpfung $\cdot$ definiert durch:

$$(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) = a \cdot b + \mathfrak{a} \text{ für alle } (a + \mathfrak{a}), (b + \mathfrak{a}) \in R/\mathfrak{a}.$$

Die Zuordnungsvorschrift ist wohldefiniert, denn aus $a + \mathfrak{a} = a' + \mathfrak{a}$ und $b + \mathfrak{a} = b' + \mathfrak{a}$, also aus $a = a' + x$ und $b = b' + y$ mit geeigneten $x, y \in \mathfrak{a}$ folgt $ab = a'b' + \underbrace{a'y + b'x + xy}_{\in \mathfrak{a}}$, also $ab + \mathfrak{a} = a'b' + \mathfrak{a}$.
Dann ist $(R/\mathfrak{a}, +, \cdot)$ Ring.
Der Ring $(R/\mathfrak{a}, +, \cdot)$ heißt Restklassenring R nach $\mathfrak{a}$.
Auf R wird eine Äquivalenzrelation $\equiv \pmod{\mathfrak{a}}$ definiert durch:

$$a \equiv b (\mathrm{mod}\ \mathfrak{a}) \Leftrightarrow a - b \in \mathfrak{a}$$

Offenbar gilt: $a \equiv b (\mathrm{mod}\ \mathfrak{a}) \Leftrightarrow a + \mathfrak{a} = b + \mathfrak{a}$.
Sprechweise für $a \equiv b \pmod{\mathfrak{a}}$: a ist kongruent b modolo $\mathfrak{a}$.
Rechenregeln für Kongruenzen:

$$\begin{array}{l} a_1 \equiv b_1 (\mathrm{mod}\ \mathfrak{a}) \\ a_2 \equiv b_2 (\mathrm{mod}\ \mathfrak{a}) \end{array} \Rightarrow \begin{array}{r} a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod}\ \mathfrak{a}) \\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 (\mathrm{mod}\ \mathfrak{a}) \end{array}$$

Der Beweis dieser Rechenregeln ergibt sich aus der Wohldefiniertheit von $+$ und $\cdot$ in $R/\mathfrak{a}$.

Satz 2.25. Kanonischer Homomorphismus, Homomorphiesatz für Ringe

1. Kanonischer Homomorphismus
   Seien $(R, +, \cdot)$ Ring, $\mathfrak{a}$ Ideal von R.
   Dann ist $\varphi : R \to R/\mathfrak{a}$ definiert durch $\varphi(r) := r + \mathfrak{a}$ ein surjektiver Homomorphismus mit $\mathrm{Ker}\ \varphi = \mathfrak{a}$.

2. Homomorphiesatz für Ringe
   Sei $\varphi : R_1 \to R_2$ Ring-Homomorphismus.
   Dann ist $f : R_1/\mathrm{Ker}\ \varphi \to \varphi(R_1)$ definiert durch $f(r + \mathrm{Ker}\ \varphi) := \varphi(r)$ ein Isomorphismus.

Beweis.

1. φ ist ein surjektiver Gruppen-Homomorphismus mit Ker $\varphi = \mathfrak{a}$ nach Satz 1.74 (Homomorphiesatz für Gruppen).
   Die Relationstreue bezüglich $\cdot$ ist trivial.

2. f ist Gruppen-Isomorphismus nach Satz 1.74.
   Ferner gilt $f(\underbrace{(r_1 + \text{Ker } \varphi)(r_2 + \text{Ker } \varphi)}_{r_1 r_2 + \text{Ker } \varphi}) = \underbrace{\varphi(r_1)}_{f(r_1 + \text{Ker } \varphi)} \cdot \underbrace{\varphi(r_2)}_{f(r_2 + \text{Ker } \varphi)}$.

Bemerkung 2.26. Sei $(K, +, \cdot)$ Körper, $(R, +, \cdot)$ Ring, $\varphi : K \to R$ Ring-Homomorphismus.
Dann gilt $\varphi(K) \cong K$ oder $\varphi(K) \cong \{0\}$.

Beweis. Folgt aus Satz 2.25, Bemerkung 2.23.4 und Bemerkung 2.23.5.

Bemerkung 2.27. Primkörper
Seien $(K, +, \cdot)$ Körper und $f_1 : \mathbb{Z} \to K$ definiert durch

$$f_1(n) := \begin{cases} \underbrace{1 + \cdots + 1}_{n-\text{mal}}, & \text{falls } n > 0 \\ \underbrace{-(1 + \cdots + 1)}_{n-\text{mal}}, & \text{falls } n < 0 \\ 0, & \text{falls } n = 0 \end{cases}$$

1. Sei Char $K = 0$ und $f : \mathbb{Q} \to K$ definiert durch $f(\frac{a}{b}) := \frac{f_1(a)}{f_1(b)}$, für alle $a \in \mathbb{Z},\ b \in \mathbb{N}$.
   Dann ist f injektiv, und K enthält einen zu $\mathbb{Q}$ isomorphen Teilkörper $f(\mathbb{Q})$.
   Dieser Körper heißt Primkörper von K.

2. Sei Char $K = p$.
   Dann ist f_1 ein Homomorphismus mit dem Kern $p\mathbb{Z}$, und K enthält einen zu $\mathbb{Z}/p\mathbb{Z}$ isomorphen Teilkörper $f_1(\mathbb{Z})$ (man beachte, daß $\mathbb{Z}/p\mathbb{Z}$ nach Satz 2.31 ein Körper ist).
   Der Körper $f_1(\mathbb{Z})$ heißt Primkörper von K.

3. Der Primkörper besitzt keine nicht trivialen Teilkörper.

2.3 Grundlagen der Zahlentheorie

Seien $n \in \mathbb{N},\ n > 1$ und $n\mathbb{Z} := \{z \cdot n | z \in \mathbb{Z}\}$ das von n in $\mathbb{Z}$ erzeugte Ideal.
Wir betrachten den Restklassenring $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

Offenbar gilt $\mathbb{Z}_n = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$.
Die Elemente von $\mathbb{Z}_n$ heißen Restklassen mod n.
$\mathbb{Z}_n$ enthält also genau n Elemente.
Seien $a, b \in \mathbb{Z}$. Für $a = b \pmod{n\mathbb{Z}}$ wird kurz $a \equiv b \pmod{n}$ geschrieben.
Dann gilt: $a \equiv b \pmod{n} \Leftrightarrow a - b \in n\mathbb{Z} \Leftrightarrow \exists \lambda \in \mathbb{Z} : a - b = \lambda n \Leftrightarrow n|(a-b)$.

Bemerkung 2.28.

1. Entsprechend den Regeln für Kongruenzen aus Bemerkung 2.24 gilt:
   $$a_1 \equiv b_1 (\mathrm{mod}\ n) \wedge a_2 \equiv b_2 (\mathrm{mod}\ n) \Rightarrow \begin{cases} a_1 + a_2 & \equiv b_1 + b_2 (\mathrm{mod}\ n) \\ a_1 \cdot a_2 & \equiv b_1 \cdot b_2 (\mathrm{mod}\ n) \end{cases}$$
2. Sei $f(x) = c_0 + c_1 x + \cdots + c_m x^m$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$. Dann gilt:
   $a \equiv b (\mathrm{mod}\ n) \Rightarrow f(a) \equiv f(b) (\mathrm{mod}\ n)$.

Beispiel 2.29. Keine natürliche Zahl der Form $7 + 8k,\ k \in \mathbb{N}$ ist Summe dreier ganzzahliger Quadrate, denn aus $a^2 + b^2 + c^2 = 7 + 8k$ folgt $a^2 + b^2 + c^2 = 7 (\mathrm{mod}\ 8)$. Aber $0, 1, 4 (\mathrm{mod}\ 8)$ sind die einzigen Quadrate modolo 8, die Summe dreier Quadrate kann also nicht kongruent 7 modolo 8 sein.

Beispiel 2.30. $2 \cdot 5 \equiv 0 (\mathrm{mod}\ 10),\ 2 \not\equiv 0 (\mathrm{mod}\ 10),\ 5 \not\equiv 0 (\mathrm{mod}\ 10)$.
Also ist $\mathbb{Z}_{10}$ nicht nullteilerfrei.

Satz 2.31. $\mathbb{Z}_n$ ist nullteilerfrei$\Leftrightarrow n$ ist Primzahl $\Leftrightarrow \mathbb{Z}_n$ ist Körper.

Beweis. Ist n nicht Primzahl, etwa $a \cdot b = n$ mit $1 < a, b < n$, so folgt $a \cdot b \equiv 0 (\mathrm{mod}\ n),\ a \not\equiv 0 (\mathrm{mod}\ n),\ b \not\equiv 0 (\mathrm{mod}\ n)$. $\mathbb{Z}_n$ ist also nicht nullteilerfrei.
Ist n Primzahl und $a \cdot b = 0 (\mathrm{mod}\ n)$, also $n|a \cdot b$,
so folgt $n|a$ oder $n|b$, also $a \equiv 0 (\mathrm{mod}\ n)$ oder $b \equiv 0 (\mathrm{mod}\ n)$.
Ist $\mathbb{Z}_n$ nullteilerfrei, so ist nach Satz 2.15 auf Seite 37 $\mathbb{Z}_n$ Körper. Andererseits ist jeder Körper nullteilerfrei. □

Beispiel 2.32. $2 \cdot 5 \equiv 2 \cdot 2 (\mathrm{mod}\ 6)$, aber $5 \not\equiv 2 (\mathrm{mod}\ 6)$
also gilt in $\mathbb{Z}_6$ nicht die Kürzungsregel.

Satz 2.33. $ax \equiv ay (\mathrm{mod}\ n) \Leftrightarrow x \equiv y (\mathrm{mod}\ \frac{n}{\mathrm{ggT}(a,n)})$.
Speziel gilt für $\mathrm{ggT}(a, n) = 1 : ax \equiv ay (\mathrm{mod}\ n) \Leftrightarrow x \equiv y (\mathrm{mod}\ n)$.

Beweis. $\Rightarrow$:
Aus $n|(ax - ay)$ folgt $\frac{n}{\mathrm{ggT}(a,n)}|(x-y) \cdot \frac{a}{\mathrm{ggT}(a,n)}$, und wegen der Teilerfremdheit von $\frac{n}{\mathrm{ggT}(a,n)}$ und $\frac{a}{\mathrm{ggT}(a,n)}$ folgt $\frac{n}{\mathrm{ggT}(a,n)}|(x-y)$.
$\Leftarrow$: trivial.

Definition 2.34. Vollständiges Restsystem mod n
Eine Menge $\{a_1, \ldots, a_n\} \subseteq \mathbb{Z}$ heißt vollständiges Restsystem mod n, wenn sie aus jeder Restklasse mod n genau ein Element enthält.
Für beliebiges $a \in \mathbb{Z}$ ist zum Beispiel $\{a, a+1, \ldots, a+(n-1)\}$ ein vollständiges Restsystem mod n.

Definition 2.35. Prime Restklasse
Ist $\mathrm{ggT}(a, n) = 1$, so ist jedes Element der Restklasse $a(\mathrm{mod}\ n)$ zu n teilerfremd. Deshalb ist die folgende Begriffsbildung sinnvoll:
$a(\mathrm{mod}\ n)$ heißt prime Restklasse mod n, wenn $\mathrm{ggT}(a, n) = 1$ ist.
Eine Menge$\{a_1, \ldots, a_m\} \subseteq \mathbb{Z}$ heißt vollständiges primes Restsystem mod n, wenn sie aus jeder primen Restklasse mod n genau ein Element enthält.

Definition 2.36. Eulersche φ-Funktion
Die Eulersche φ-Funktion bildet jede natürliche Zahl n auf die Anzahl der primen Restklassen mod n ab.

$$\varphi : \mathbb{N} \to \mathbb{N},\ \varphi(n) := \sum_{\substack{1 \le i \le n \\ \mathrm{ggT}(i,n)=1}} 1$$

Bemerkung 2.37. Sei p Primzahl, $k \in \mathbb{N}$. Dann gilt

$$\varphi(p) = p - 1 \quad \text{und} \quad \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Satz 2.38. Die primen Restklassen mod n bilden die Einheitengruppe von $\mathbb{Z}_n$. Sie wird mit $\mathbb{P}_n$ bezeichnet.

Beweis. Die Einheiten sind offenbar prime Restklassen.
$\mathbb{P}_n$ ist bezüglich der Multiplikation eine Halbgruppe, und nach Satz 2.33 regulär. Aus Satz 1.28 folgt die Behauptung.
Zur Berechnung der Inversen läßt sich der später zu behandelnde Euklidische Algorithmus gut verwenden.

Satz 2.39. Euler, Fermat
Seien $a \in \mathbb{Z},\ n \in \mathbb{N}$ und $\mathrm{ggT}(a, n) = 1$.
Dann gilt $a^{\varphi(n)} \equiv 1(\mathrm{mod}\ n)$.
Speziell folgt der kleine Satz von Fermat:
Seien p eine Primzahl, $a \in \mathbb{Z}$ und $\mathrm{ggT}(a, p) = 1$.
Dann gilt $a^{p-1} \equiv 1(\mathrm{mod}\ p)$.

Beweis. Der Satz von Euler ist ein Sonderfall von Satz 1.53 auf Seite 17.

Satz 2.40. Der Chinesische Restsatz
Seien $n_1, \ldots, n_r \in \mathbb{N}$ paarweise teilerfremd und $n := n_1 \cdots n_r$. Dann ist $\mathbb{Z}_n$ isomorph zum direkten Produkt der Restklassenringe $\mathbb{Z}_{n_1}, \ldots, \mathbb{Z}_{n_r}$. (Siehe Beispiel 2.3.7 auf Seite 34)
Genauer gilt:

1. $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ definiert durch
   $\varphi(a \pmod n) := (a \pmod{n_1}, \ldots, a \pmod{n_r})$ ist ein (Ring-) Isomorphismus.

2. $\varphi^* : \mathbb{P}_n \to \mathbb{P}_{n_1} \times \cdots \times \mathbb{P}_{n_r}$ definiert durch
   $\varphi^*(a \pmod n) := (a \pmod{n_1}, \ldots, a \pmod{n_r})$ ist ein (Gruppen-) Isomorphismus.

Beweis.

1. Trivialerweise ist φ wohldefiniert, und ein Homomorphismus.
   Da $n_1, \ldots, n_r$ paarweise teilerfremd sind, ist der Kern von φ trivial, also ist φ injektiv.
   Wegen $|\mathbb{Z}_n| = |\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}|$ ist φ dann auch surjektiv.

2. Ist $\mathrm{ggT}(a, n) = 1$, so ist auch $\mathrm{ggT}(a, n_i) = 1$ für $1 \leq i \leq r$, also ist φ^* wohldefiniert.
   Offenbar ist φ^* Homomorphismus.
   φ^* ist die Einschränkung von φ auf $\mathbb{P}_n$; mit φ ist also auch φ injektiv.
   Ein beliebiges Element aus $\mathbb{P}_{n_1} \times \cdots \times \mathbb{P}_{n_r}$ besitzt nach dem 1. Teil des Satzes genau ein Urbild, und dieses liegt offenbar in $\mathbb{P}_n$.

Folgerung 2.41. Seien $n_1, \ldots, n_r \in \mathbb{N}$ paarweise teilerfremd und $a_1, \ldots, a_r \in \mathbb{Z}$ beliebig. Dann gilt:

1. $\exists a \in \mathbb{Z} : a \equiv a_i \pmod{n_i}$ für $1 \leq i \leq r$.

2. $a' \equiv a_i \pmod{n_i}$ für $1 \leq i \leq r \Leftrightarrow a \equiv a' \pmod{n_1 \cdots n_r}$.

Beweis.

1. Nach Satz 2.40.2 existiert ein $a \in \mathbb{Z}$ mit
   $\varphi(a \pmod{n_1 \cdots n_r}) = (a_1 \pmod{n_1}, \ldots, a_r \pmod{n_r})$.
   Dann erfüllt a die geforderten Kongruenzbedingungen.

2. a ist modolo $n_1 \cdots n_r$ eindeutig bestimmt, da φ injektiv ist.

Folgerung 2.42. Seien $n, m \in \mathbb{N}$ mit $\text{ggT}(n, m) = 1$.
Dann gilt für die Eulersche φ-Funktion:

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m).$$

Zusammen mit Bemerkung 2.37 folgt:
Ist $n = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung von n, so gilt

$$\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}) = p_1^{e_1-1} \cdots p_r^{e_r-1} \cdot (p_1 - 1) \cdots (p_r - 1).$$

Beweis. $\varphi(n \cdot m) = |\mathbb{P}_{n \cdot m}| = |\mathbb{P}_n| \cdot |\mathbb{P}_m| = \varphi(n) \cdot \varphi(m)$.

Definition 2.43. Primitivwurzel
Seien $n \in \mathbb{N}$, $a \in \mathbb{Z}_n$. a heißt Primitivwurzel $\pmod n$, falls Ord $a = \varphi(n)$, das heißt $a \pmod n$ erzeugt $\mathbb{P}_n$ (die Gruppe der primen Restklassen).

Bemerkung 2.44. Eine Primitivwurzel $\pmod n$ existiert genau dann, wenn $\mathbb{P}_n$ zyklisch ist. (Siehe auch Bemerkung 2.46.)

Beispiel 2.45.

1. 2 ist Primitivwurzel mod 3.

2. 3 ist Primitivwurzel mod 7.

   Beweis. Es gilt $3^2 \equiv 2 \pmod 7$ und $3^3 \equiv 6 \pmod 7$, also ist Ord $(3 \pmod 7) > 3$.
   Die Ordnung von $\mathbb{P}_7$ ist 6.
   Nach Satz 1.53 is Ord 3(mod 7) Teiler von 6.
   Die einzigen Teiler von 6 sind 1,2,3,6; also ist Ord 3(mod 7) = 6.

3. 2 ist nicht Primitivwurzel (mod 7), denn $2^3 \equiv 1 (\text{mod } 7)$.

Bemerkung 2.46.

1. Es ist kein einfaches Verfahren bekannt, nach dem eine Primitivwurzel mod p bestimmt werden kann.
   Das Probeverfahren liefert natürlich eine Primitivwurzel nach endlich vielen Schritten, das sind jedoch oft zu viele Schritte um anwendbar zu sein.

2. Vermutung von Artin: Sei $a \in \mathbb{Z}$ nicht Quadratzahl. Dann gibt es unendlich viele Primzahlen p, für die a Primitivwurzel mod p ist.

3. Die prime Restklassengruppe $\mathbb{P}_m$ ist zyklisch genau für
   $m = 1, 2, 4, p^\alpha, 2p^\alpha$, wobei $p > 2$ Primzahl ist und $\alpha \in \mathbb{N}$
   (Beweis siehe [8]). Siehe auch Satz 4.29 für den Fall $m = p$.

Satz 2.47. Sei $n = \sum_{i=0}^{r} a_i \cdot 10^i$ die 10-adische (dezimal) Darstellung von n.
Die a_i heißen Ziffern von n.
$q(n) := \sum_{i=0}^{r} a_i$ heißt Quersumme von n.
$q^*(n) := \sum_{i=0}^{r} (-1)^i a_i$ heißt alternierende Quersumme von n.
Es gilt:

1. Dreier-Probe

   (a) $3|n \Leftrightarrow 3|q(n)$.

   (b) $q(n_1 \cdot n_2) \equiv q(n_1) \cdot q(n_2) (\text{mod } 3)$.

   (c) $q(n_1 + n_2) \equiv q(n_1) + q(n_2) (\text{mod } 3)$.

   Multipliziert man oder addiert man zwei natürliche Zahlen, so kann man relativ leicht testen, ob die vorletzte oder letzte Kongruenz erfüllt ist. Ist dies nicht der Fall, so hat man sich verrechnet.
   Dieses Verfahren nennt man Dreier-Probe.

2. Neuner-Probe

   (a) $9|n \Leftrightarrow 9|q(n)$.

   (b) $q(n_1 \cdot n_2) \equiv q(n_1) \cdot q(n_2) (\text{mod } 9)$.

   (c) $q(n_1 + n_2) \equiv q(n_1) + q(n_2) (\text{mod } 9)$.

3. Elfer-Probe

   (a) $11|n \Leftrightarrow 11|q^*(n)$.

   (b) $q^*(n_1 \cdot n_2) \equiv q^*(n_1) \cdot q^*(n_2) (\text{mod } 11)$.

   (c) $q^*(n_1 + n_2) \equiv q^*(n_1) + q^*(n_2) (\text{mod } 11)$.

Beweis.
1: Rechne mod 3, beachte $10 \equiv 1 (\text{mod } 3)$.
4: Rechne mod 9, beachte $10 \equiv 1 (\text{mod } 9)$.
5: Rechne mod 11, beachte $10 \equiv -1 (\text{mod } 11),\ 10^i \equiv (-1)^i \ (\text{mod } 11)$.

2.4 Einbettung von Integritätsbereichen in Körper

Ist $(R, +, \cdot)$ ein Ring mit $R \neq \{0\}$, welcher in einem Körper enthalten ist, so ist $(R, +, \cdot)$ kommutativer Ring und nullteilerfrei, also Integritätsbereich.
Umgekehrt gilt:

Satz 2.48. Sei $(R, +, \cdot)$ Integritätsbereich.
Dann existiert ein Körper $(K, +, \cdot)$, der einen zu R isomorphen Teilring enthält.
Sprechweise: R läßt sich in einen Körper K einbetten.

Beweis. Um einen Leitfaden für die Konstruktion von $(K, +, \cdot)$ zu bekommen, führen wir die folgende Vorbetrachtung durch.
Wir nehmen an, daß $(K, +, \cdot)$ ein Körper ist, welcher R enthält.
Dann ist $T := \{\frac{a}{b} | a, b \in R,\ b \neq 0\}$ ein Teilkörper von $(K, +, \cdot)$.
Ferner gilt $T \supseteq R$, und T ist minimaler Teilkörper von $(K, +, \cdot)$ mit dieser Eigenschaft.
Außerdem gilt $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$.
Wir nehmen T als Vorbild für die Konstruktion des gesuchten Körpers.

Sei $M := R \times R_0,\ R_0 := R \backslash \{0\}$.
Definiere auf M eine Relation $\sim$ durch $(a, b) \sim (c, d) :\Leftrightarrow ad = bc$.
Dann ist $\sim$ Äquivalenzrelation.
Seien K die Menge der Äquivalenzklassen, $[a, b]$ die von (a, b) erzeugte Äquivalenzklasse.
Definiere auf K zwei Verknüpfungen durch:

$$[a, b] \cdot [c, d] := [ac, bd] \qquad \text{und}$$
$$[a, b] + [c, d] := [ad + bc, bd].$$

Nachrechnen bestätigt, daß beide Verknüpfungen wohldefiniert sind.
Dann ist $(K, +, \cdot)$ ein Körper, das Nullement ist $[0, r]$, das Einselement ist $[r, r]$ und das Inverse zu $[a, b]$ ist $[b, a]$ für $[a, b] \neq [0, r]$.
Sei $r \in R,\ r \neq 0$ beliebig aber fest.
Dann ist $f : R \to K$ definiert durch $f(a) := [ar, r]$ ein injektiver Ringhomomorphismus, also $f(R) \cong R$ nach dem Homomorphiesatz für Ringe (siehe Seite 39).

Definition 2.49. Quotientenkörper
Sei der Integritätsbereich R Unterring des Körpers K. Dann heißt K Quotientenkörper von R, wenn R in keinem echten Unterkörper von K enthalten ist.

Bemerkung 2.50. Der im Beweis von Satz 2.48 konstruierte Körper K ist Quotientenkörper von $f(R)$.

Bemerkung 2.51. Ist K der Quotientenkörper von R, so läßt sich K darstellen in der Form:

$$K = \{\frac{a}{b} | a, b \in R,\ b \neq 0\} \text{ mit } \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

Bemerkung 2.52. Sei $(K, +, \cdot)$ der im Beweis von Satz 2.48 konstruierte Quotientenkörper von $(R, +, \cdot)$.
„Identifiziert" man R mit $f(R)$, so läßt sich R als Unterring von $(K, +, \cdot)$ auffassen. Dies wurde in der obigen Bemerkung gemacht, und wir werden es auch später häufig tun.
Unter „identifizieren" soll das folgende Prozeß verstanden werden:
Sei $\varphi : R \to R'$ ein injektiver Ringhomomorphismus.
Dann soll R' ersetzt werden durch einen zu R' isomorphen Ring R'', welche R als Unterring enthält. Wir gehen hier nicht weiter darauf ein, wie dies genau gemacht wird.

Beispiel 2.53. Als wichtigen Spezialfall erhält man die Konstruktion von $(\mathbb{Q}, +, \cdot)$ aus $(\mathbb{Z}, +, \cdot)$.

Bemerkung 2.54. Die Konstruktion von Satz 2.48 läßt sich wie folgt verallgemeinern:
Es sei $(R, +, \cdot)$ ein kommutativer Ring, $R \neq \{0\}$.
Ferner sei $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge von R (das heißt: $a, b \in S \Rightarrow a \cdot b \in S$), die keine Nullteiler enthält
(das heißt: $(s \in S \wedge r \in R \wedge r \cdot s = 0) \Rightarrow (r = 0 \vee s = 0)$).
Dann läßt sich $(R, +, \cdot)$ einbetten in einen Ring $(R_S, +, \cdot)$ mit Eins, in dem alle $s \in S$ invertierbar sind.
R_S läßt sich darstellen in der Form

$$R_S = \{\frac{r}{s} | r \in R, s \in S\}$$

mit $\frac{r_1}{s_1} = \frac{r_2}{s_2} \Leftrightarrow r_1 s_2 = r_2 s_1$.
R_S heißt Lokalisation von R nach S

2.5 Der Aufbau des Zahlensystems

Bisher wurden in der Vorlesung Grundeigenschaften der natürlichen Zahlen und rationalen Zahlen, die intuitiv klar sind, als bekannt vorausgesetzt und ohne weitere Begründung verwendet. Eine Rechtfertigung hierfür ergibt sich aus dem axiomatischen Aufbau des Zahlensystems, der in diesem Paragraphen kurz, und zum Teil ohne Beweis, skizziert werden soll. Eine ausführliche Darstellung findet man in [6].

Definition 2.55. Peano-Struktur
$(\mathbb{N}, 1, *)$ heißt Peano-Stuktur, wenn gilt:

1. $\mathbb{N}$ ist eine nichtleere Menge,

2. $1 \in \mathbb{N}$ ist ein ausgezeichnetes Element aus $\mathbb{N}$,

3. $*$ ist eine Abbildung $* : \mathbb{N} \to \mathbb{N},\ n \mapsto n^*$,
   so daß $(\mathbb{N}, 1, *)$ die folgenden Peano-Axiome erfüllt:

   P_1: Es existiert kein $x \in \mathbb{N}$ mit $x^* = 1$.

   P_2: $x^* = y^* \Rightarrow x = y$ (Das heißt $*$ ist injektiv.)

   P_3: Für jede Teilmenge $T \subseteq \mathbb{N}$ mit $1 \in T$ gilt:
   $(x \in T \Rightarrow x^* \in T) \Rightarrow T = \mathbb{N}$.

Bemerkung 2.56.

1. Jedes $n \in \mathbb{N}$ läßt sich anschaulich interpretieren als eine gewisse Anzahl entsprechend der intuitiven Vorstellung von den natürlichen Zahlen.

2. Die Abbildung $*$ beschreibt das Weiterzählen.

3. n^* heißt Nachfolger von n.

4. P_3 sichert das Prinzip der vollständigen Induktion.

Satz 2.57. (Ohne Beweis) Es existiert eine Peano-Struktur

Satz 2.58. (Ohne Beweis) Die Peano-Struktur ist bis auf Isomorphie eindeutig bestimmt. Das heißt:
Ist $(\widetilde{\mathbb{N}}, \widetilde{1}, \widetilde{*})$ eine weitere Peano-Struktur, so existiert eine bijektive Abbildung $f : \begin{matrix} \mathbb{N} \to \widetilde{\mathbb{N}} \\ n \mapsto \widetilde{n} \end{matrix}$ mit $f(1) = \widetilde{1},\ f(n^*) = \widetilde{n}^{\widetilde{*}}$.

Bemerkung 2.59. Im Folgenden sei $(\mathbb{N}, 1, *)$ stets eine festgewählte Peano-Struktur.
$\mathbb{N} = \{1, 1^* = 2, 2^* = 3, \dots\}$ heißt Menge der natürlichen Zahlen.

Damit sind die natürliche Zahlen charakterisiert.
Wir definieren nun zwei Verknüpfungen auf $\mathbb{N}$.

Definition 2.60.

1. $(n + 1) := n^*$
   $n + m^* := (n + m)^*$

2. $n \cdot 1 := n$
   $n \cdot m^* := n \cdot m + n$

Bemerkung 2.61. (Ohne Beweis) Durch Definition 2.60 werden auf $\mathbb{N}$ zwei Verknüpfungen $+$ und $\cdot$ definiert.
Es gilt:

1. $(\mathbb{N}, +)$ ist eine kommutative, reguläre Halbgruppe.
2. $(\mathbb{N}, \cdot)$ ist eine kommutative, reguläre Halbgruppe, 1 ist Einselement.
3. $(\mathbb{N}, +, \cdot)$ erfüllt das Distributivgesetz.

Wichtig ist noch die übliche Ordnungsrelation auf $\mathbb{N}$.

Definition 2.62. $x \leq y :\Leftrightarrow \exists z \in \mathbb{N} : x + z = y \vee x = y$.
Die übliche Schreibweise $y \geq x$ soll $x \leq y$ bedeuten.

Satz 2.63. (Ohne Beweis) $(\mathbb{N}, \leq)$ ist eine wohlgeordnete Menge mit 1 als kleinstem Element. Das heißt es gilt:

1. $a \leq b \wedge b \leq c \Rightarrow a \leq c$.
2. $a \leq b \wedge b \leq a \Rightarrow a = b$.
3. $\forall a, b \in \mathbb{N} : a \leq b \vee b \leq a$.
4. Jede nichtleere Teilmenge $T \subseteq \mathbb{N}$ enthält ein kleinstes Element t.
   (Das heißt es gilt: $t \leq t'$ für alle $t' \in T$.

Im nächsten Schritt erfolgt die Erweiterung von $\mathbb{N}$ auf $\mathbb{Z}$.

Satz 2.64. $(\mathbb{N}, +, \cdot)$ läßt sich bis auf Isomorphie eindeutig erweitern zu einem Integritätsbereich $(\mathbb{Z}, +, \cdot)$ mit $\mathbb{Z} = \mathbb{N} \dot\cup \{0\} \dot\cup -\mathbb{N}$ wobei $-\mathbb{N} := \{-n | n \in \mathbb{N}\}$.

Beweis. Die Konstruktion von $(\mathbb{Z}, +)$ aus $(\mathbb{N}, +)$ wird in Bemerkung 1.93 beschrieben.
Aus der Konstruktion ergibt sich

$$\mathbb{Z} = \mathbb{N} \dot\cup \{0\} \dot\cup -\mathbb{N}. \tag{2.1}$$

Ist nämlich $a \in \mathbb{N}$ neutrales Element in $(\mathbb{Z}, +)$, so folgt $a^* = a + 1 = 1$ im Widerspruch zu P_1. Also gilt: $0 \notin \mathbb{N}$.
Für $n \in \mathbb{N}$ gilt dann auch $-n \notin \mathbb{N}$, sonst würde $n + (-n) = 0 \in \mathbb{N}$ gelten.
Ferner haben verschiedene $n \in \mathbb{N}$ in der Gruppe $(\mathbb{Z}, +)$ verschiedene Inverse.
Nach Gleichung 2.1 und Satz 2.4 gibt es nur eine Möglichkeit die Multiplikation von $\mathbb{N}$ auf $\mathbb{Z}$ fortzusetzen, so daß $(\mathbb{Z}, +, \cdot)$ zu einem kommutativen Ring wird. Durch Fallunterscheidung läßt sich leicht nachprüfen, daß diese Möglichkeit tatsächlich einen kommutativen Ring $(\mathbb{Z}, +, \cdot)$ liefert.

Für $a, b \in \mathbb{N}$ gilt $a \cdot b \in \mathbb{N}$, also insbesondere $a \cdot b \neq 0$. Hieraus folgt leicht, daß $(\mathbb{Z}, +, \cdot)$ nullteilerfrei ist.

Die Ordnungsrelation $\leq$ von $\mathbb{N}$ wird auf $\mathbb{Z}$ übertragen durch

$$x \leq y :\Leftrightarrow y - x \in \mathbb{N} \cup \{0\}.$$

Wie üblich wird definiert

$$x < y :\Leftrightarrow (x \leq \wedge x \neq y).$$

Satz 2.65. (Ohne Beweis) $(\mathbb{Z}, +, \cdot, \leq)$ ist ein Integritätsbereich, der archimedisch angeordnet ist. Das heißt:

1. Für jedes $a \in \mathbb{Z}$ gilt genau eine der Relationen $a > 0,\ a = 0,\ -a > 0$.
2. $a > 0 \wedge b > 0 \Rightarrow a + b > 0 \wedge a \cdot b > 0$.
3. $0 < a < b \Rightarrow \exists n \in \mathbb{N} : a \cdot n > b$.

Aus $(\mathbb{Z}, +, \cdot)$ erhält man durch Bildung des Quotientenkörpers den Körper $(\mathbb{Q}, +, \cdot)$ der rationalen Zahlen. Es läßt sich leicht zeigen, daß man die Anordnung $\leq$ von $\mathbb{Z}$ auf genau eine Weise zu einer Anordnung $\leq$ des Körpers $\mathbb{Q}$ fortsetzen kann, nämlich durch

$$0 \leq \frac{a}{b} :\Leftrightarrow 0 \leq a \cdot b, \quad \frac{a}{b} \leq \frac{c}{d} :\Leftrightarrow 0 \leq \frac{c}{d} - \frac{a}{b}, \qquad \forall a, b, c, d \in \mathbb{Z} \text{ mit } b, d \neq 0.$$

Der Übergang von $\mathbb{Q}$ zum Körper $\mathbb{R}$ der reellen Zahlen erfolgt mit Hilfe von Cauchyfolgen.
Sei M die Menge aller rationalen Cauchyfolgen. Durch komponentenweise Addition und Multiplikation wird M zu einem Ring $(M, +, \cdot)$.
Sei A die Menge aller Elemente aus M die gegen 0 konvergieren.
Dann ist A ein Ideal von M.
Der Restklassenring $\mathbb{R} := M/A$ ist ein Körper.
Als Übungsaufgabe weise man für ein beliebiges Element $\neq 0$ die Existenz eines Inversen nach.
Dies ist der Körper der reellen Zahlen.
Die Abbildung von $\mathbb{Q}$ nach $\mathbb{R}$, die jedem $q \in \mathbb{Q}$ als Bild die Nebenklasse von A zuordnet, die die konstante Folge $(q)_{n \in N}$ als Repräsentant hat, ist eine Einbettung von $\mathbb{Q}$ in $\mathbb{R}$.
Jede Nebenklasse aus $\mathbb{R}$ besitzt einen Repräsentanten der Form

$$(a_0, a_0 + \frac{a_1}{10}, a_0 + \frac{a_1}{10} + \frac{a_2}{100}, \dots), \text{ mit } a_0 \in \mathbb{Z},\ a_i \in \{0, 1, \dots 9\} \text{ für } i \in \mathbb{N}.$$

Die zugehörige reelle Zahl kann man auch in der Dezimaldarstellung $a_0, a_1a_2a_3\ldots$ schreiben. Existiert für eine reelle Zahl $r = a_0, a_1a_2\ldots$ ein minimales $i \in \mathbb{N}$ mit $a_j = 9$ für alle $j \geq i$ (also $a_{i-1} < 9$ oder $i = 1$), so besitzt r auch die Dezimaldarstellung

$$r = a_0, a_1a_2\ldots a_{i-2}(a_{i-1}+1)000\ldots.$$

Umgekehrt, existiert für eine reelle Zahl $s = a_0, a_1a_2\ldots$ ein $a_i > 0$ mit $a_j = 0$ für alle $j > i$, so besitzt s auch die Dezimaldarstellung

$$s = a_0, a_1\ldots a_{i-1}(a_i-1)999\ldots.$$

Zum Beispiel gilt: $1 = 0,999\ldots$.
Tritt keiner dieser beiden Fälle ein, so ist die Dezimaldarstellung eindeutig.

Die Ordnungsrelation $\leq$ wird von $\mathbb{Q}$ auf $\mathbb{R}$ fortgesetzt, indem für alle $r = ((a_n)_{n\in\mathbb{N}} + A) \in \mathbb{R},\ r_1, r_2 \in \mathbb{R}$ definiert wird:

$$\begin{aligned} 0 \leq r &:\Leftrightarrow (r = 0 \vee 0 \leq a_n \text{ für unendlich viele } n \in \mathbb{N}),\\ r_1 \leq r_2 &:\Leftrightarrow 0 \leq r_2 - r_1. \end{aligned}$$

Satz 2.66. (Ohne Beweis) $(\mathbb{R}, +, \cdot, \leq)$ ist ein archimedisch angeordneter Körper, der vollständig ist (das heißt jede Cauchy Folge ist konvergent).
Bis auf Isomorphie ist $\mathbb{R}$ hierdurch eindeutig bestimmt.

Definiert man auf $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ zwei Verknüpfungen durch

$$\begin{aligned} (a_1, a_2) + (b_1, b_2) &:= (a_1 + b_1, a_2 + b_2)\\ (a_1, a_2) \cdot (b_1, b_2) &:= (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1), \end{aligned}$$

so erhält man den Körper der komplexen Zahlen. Setzt man
$r := (r, 0)$ und $i := (0, 1)$, so gilt $a + bi = (a, 0) + (b, 0)(0, 1)$.
Hieraus ergibt sich die übliche Schreibweise für komplexe Zahlen.
Man kann den Körper der komplexen Zahlen auch als Zerfällungskörper von $x^2 + 1$ über $\mathbb{R}$ auffassen (siehe Kapitel 4).

2.6 Polynomringe

Definition 2.67. Polynom
Seien $(R, +, \cdot)$ Ring, $R \neq \{0\},\ \mathbb{N}_0 := \mathbb{N} \cup \{0\}$.
Eine Abbildung $f : \mathbb{N}_0 \to R$, für die $f(n) \neq 0$ für nur endlich viele $n \in \mathbb{N}_0$ gilt, heißt Polynom über R.

Seien $a_i := f(i)$ für alle $i \in \mathbb{N}$, $a_i = 0$ für alle $i > n$.
Dann schreibt man f üblicherweise in der Form

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

Die Reihenfolge der Summanden wird gelegentlich auch vertauscht.
a_i heißt Koeffizient von x^i des Polynoms f.
Summanden mit Koeffizient 0 können, müssen aber nicht, aufgeführt werden.
Ist $a_i = 1$, so schreibt man für $a_i x^i$ auch x^i.
Für a_0 schreibt man auch $a_0 x^0$.
Die „Unbestimmte" x kann durch ein anderes Symbol ersetzt werden, etwa durch y.

Bemerkung 2.68. Das Polynom f ist eindeutig durch seine Koeffizienten bestimmt.
Das Polynom, dessen Koeffizienten sämtlich 0 sind, heißt Nullpolynom und wird mit 0 bezeichnet.
Seien f nicht das Nullpolynom, $n \in \mathbb{N}_0$ maximal mit $f(n) = a_n \neq 0$.
Dann heißt n der Grad von f und f heißt normiert falls $a_n = 1$.
Außerdem heißt a_n höchster Koeffizient von f.
Ist $1 \in R$, so ist x ein Polynom über R.
Für den Grad von f schreibt man grad f.

Bemerkung 2.69. Seien $(R, +, \cdot)$ Ring, $R[x]$ die Menge aller Polynome über R.
Auf $R[x]$ werden zwei Verknüpfungen $+$ und $\cdot$ definiert wie folgt:
Für alle $f, g \in R[x]$ sei

$$\begin{aligned} f + g : \mathbb{N}_0 \to R \text{ definiert durch } (f+g)(n) &:= f(n) + g(n) \\ f \cdot g : \mathbb{N}_0 \to R \text{ definiert durch } (f \cdot g)(n) &:= \textstyle\sum_{i=0}^{n} f(i) \cdot g(n-i) \end{aligned}$$

$f \cdot g$ ist wieder ein Polynom, denn für $m >$ grad $f +$ grad g gilt $f \cdot g(m) = 0$.

Bemerkung 2.70. Sei $(R, +, \cdot)$ Ring, $R \neq \{0\}$.
Dann ist auch $(R[x], +, \cdot)$ Ring (der Polynomring über R).
Ist $(R, +, \cdot)$ kommutativ, so auch $(R[x], +, \cdot)$.

Beweis. Nichttrivial ist nur das Assoziativgesetz bezüglich $\cdot$.

$$((f \cdot g) \cdot h)(n) = \sum_{i+j=n} (f \cdot g)(i) \cdot h(j) = \sum_{l+k+j=n} f(l) \cdot g(k) \cdot h(j) = (f \cdot (g \cdot h))(n).$$

Bemerkung 2.71. $R[x]$ enthält einen zu R isomorphen Teilring

$$R' := \{a_0 x^0 | a_0 \in R\}.$$

Identifiziert man R mit R', so kann man R als Teilring von $R[x]$ auffassen.

Bemerkung 2.72. Man kann den Polynomring $R[x][y]$ bilden.
Es gilt $R[x][y] \cong R[y][x]$. Man schreibt auch $R[x, y]$.
Analog kann man $R[x_1, \ldots, x_n]$ bilden, den Polynomring in n Unbestimmten.

Bemerkung 2.73. Seien $(R, +, \cdot)$ Ring, $R[[x]]$ die Menge aller Abbildungen $f : \mathbb{N}_0 \to R$.
Definiert man analog zu Bemerkung 2.69 zwei Verknüpfungen $+$ und $\cdot$ auf $R[[x]]$, so erhält man ebenfalls einen Ring (Ring der formalen Potenzreihen über R).

Bemerkung 2.74. Seien $(R, +, \cdot)$ Ring, $R \neq \{0\}$, $(S, \cdot)$ Halbgruppe mit $S \cap R = \emptyset$.
Sei $R[S] := \{f : S \to R | f(s) \neq 0$ für nur endlich viele $s \in S\}$.
Definiere auf $R[S]$ zwei Verknüpfungen durch

$$\begin{aligned}(f + g)(s) &:= f(s) + g(s)\\ (f \cdot g)(s) &:= \sum_{\substack{s_1 \cdot s_2 = s\\ s_1, s_2 \in S}} f(s_1) \cdot f(s_2).\end{aligned}$$

Dann ist $(R[S], +, \cdot)$ Ring (der Halbgruppenring von S über R).
Für die Halbgruppe $(\mathbb{N}_0, +)$ erhält man den Polynomring über R aus Bemerkung 2.70.

Bemerkung 2.75. Mit $(R, +, \cdot)$ ist auch der Polynomring $(R[x], +, \cdot)$ Integritätsbereich.
Dann existiert auch der Quotientenkörper

$$R(x) := \{\frac{f}{g} | f, g \in R[x], g \neq 0\}.$$

Bemerkung 2.76. Sei $f = a_n x^n + \cdots + a_0 \in R[x]$.
$\widetilde{f} : R \to R$ sei definiert durch $\widetilde{f}(r) := a_n r^n + \cdots + a_1 r + a_0 =: f(r)$.
Dann heißt $\widetilde{f}$ Polynomabbildung von f. Gelegentlich wird $\widetilde{f}$ auch mit f bezeichnet.
Verschiedene Polynome können dieselbe Polynomabbildung besitzen; zum Beispiel haben $0, x^2 - x \in \mathbb{Z}_2[x]$ beide die Nullabbildung als Polynomabbildung.

Sehr häufig gebraucht wird

Satz 2.77. Einsetzungshomomorphismus
Seien $(R, +, \cdot)$ kommutativer Ring, $r \in R$.

Dann ist $\varphi : R[x] \to R$ definiert durch $\varphi(f) := \widetilde{f}(r)$ ein Ringhomomorphismus.
Eine Gleichung mit Elementen aus $R[x]$ geht über in eine Gleichung mit Elementen aus R, wenn x durch r ersetzt wird.

Beweis. Es gilt $(\widetilde{f+g})(r) = \widetilde{f}(r) + \widetilde{g}(r)$, da die Gruppe $(R,+)$ kommutativ ist.
Sei $f = a_0 + a_1x + \cdots + a_sx^s,\ g = b_0 + b_1x + \cdots + b_tx^t$.
Dann gilt $\widetilde{f}(r) = a_0 + a_1r + \cdots + a_sr^s \wedge \widetilde{g}(r) = b_0 + b_1r + \cdots + b_tr^t$.
Also $\widetilde{f}(r) \cdot \widetilde{g}(r) = \sum_{n=0}^{r+t} \left(\sum_{i+j=n} a_ib_j \right) r^n = (\widetilde{f \cdot g})(r)$.
Man beachte, daß das vorletzte Gleichheitszeichen wegen der kommutativität des Rings R gilt.

Ergänzung 2.78. Satz 2.77 gilt nicht für beliebige Ringe.
Als Beispiel betrachten wir den sogenannten Quaternionen Schiefkörper.
Für $v, u \in \mathbb{C}$ betrachte man die 2×2 Matrix $M(u,v) := \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$.
Dann ist $Q := \{M(u,v) | u, v \in \mathbb{C}\}$ ein Ring.

Es gilt $M(u,v) - M(x,y) = M(u-x, v-y)$,
$M(u,v) \cdot M(x,y) = M(ux - v\bar{y}, uy + v\bar{x})$,
$M(1,0)$ ist Einselement,
zu $M(u,v) \neq M(0,0)$ ist $M(\frac{\bar{u}}{|u|^2+|v|^2}, \frac{-v}{|u|^2+|v|^2})$ das Inverse.

Also ist $(Q, +, \cdot)$ Schiefkörper (der Qaternionenschiefkörper).
Setze $j := M(0,1)$. Dann gilt $M(u,v) = M(u,0) + M(v,0) \cdot j$.
Die Abbildung $f : \mathbb{C} \to Q$ definiert durch $f(u) := M(u,0)$ ist ein injektiver Homomorphismus.
Identifiziert man $\mathbb{C}$ mit seinem Bild in Q, so kann $\mathbb{C}$ als Teilkörper von Q aufgefaßt werden.
Dann gilt $Q = \{u + vj | u, v \in \mathbb{C}\}$, und

$$\begin{aligned} (u + vj) + (x + yj) &= (u + x) + (v + y)j \\ (u + vj) \cdot (x + yj) &= (ux - v\bar{y}) + (uy - v\bar{x})j. \end{aligned}$$

Schreibt man die Elemente aus C in der Form $z = a + bi;\ a, b \in \mathbb{R};\ i^2 = -1$ und setzt man $k := i \cdot j$, so gilt:

$$\begin{aligned} Q &= \{a_1 + a_2i + a_3j + a_4k | a_1, \ldots, a_4 \in \mathbb{R}\}, \\ i^2 &= j^2 = k^2 = -1, \\ ij &= -ji = k, \\ jk &= -kj = i, \\ ki &= -ik = j. \end{aligned}$$

Man beachte die Analogie dieser Rechenregeln zur Quaternionengruppe aus Satz 1.67 auf Seite 21.
Satz 2.77 gilt nicht für Q.
Für $f = ix \in Q[x],\ g = x \in Q[x]$, also $g \cdot f = ix^2$ gilt

$$\widetilde{g}(j) \cdot \widetilde{f}(j) = j \cdot i \cdot j = -j^2 i = i,$$
$$\widetilde{g \cdot f}(j) = i \cdot j^2 = -i.$$

Bemerkung 2.79. Kanonische Fortsetzung
Sei $\varphi : R_1 \to R_2$ Ringhomomorphismus. Dann ist

$$\widetilde{\varphi} : R_1[x] \to R_2[x] \text{ definiert durch}$$
$$\widetilde{\varphi}(a_0 + \cdots + a_n x^n) := \varphi(a_0) + \cdots + \varphi(a_n) x^n$$

ebenfalls Ringhomomorphismus.
Ist φ bijektiv, so auch $\widetilde{\varphi}$.

2.7 Division von Polynomen

Satz 2.80. Seien $(K, +, \cdot)$ Körper; $f, g \in K[x];\ g \neq 0$.
Dann existieren Polynome $q, r \in K[x]$ mit

$$f = q \cdot g + r,\ r = 0 \vee \text{grad } r < \text{grad } g.$$

Beweis.
Ist grad $f <$ grad g oder $f = 0$, so wähle man $q = 0$.
Sei also grad $f \geq$ grad g.
Der Beweis wird geführt durch vollständige Induktion nach grad f.
Induktionsbeginn:
Im Fall grad $f = 0$ wähle man q=0, falls grad $g > 0$ und $q = g^{-1} f$, falls grad $g = 0$.
Der Schluß auf n:
Annahme:
Für alle $f \in K[x]$ mit grad $f < n$ gilt die Behauptung.
Seien $f = a_n x^n + \cdots + a_0,\ g = b_m x^m + \cdots + b_0,\ n \geq m,\ a_n \neq 0,\ b_m \neq 0$.
Sei $h := f - x^{n-m} \cdot \frac{a_n}{b_m} \cdot g$.
Dann gilt entweder $h = 0$ (und es folgt die Behauptung)
oder grad $h <$ grad f.
Im zweiten Fall existieren nach Induktionsvoraussetzung $q, r \in K[x]$ mit $h = q \cdot g + r,\ r = 0$ oder grad $r <$ grad g, und es folgt $f = (\frac{a_n}{b_m} x^{n-m} + q) + r$. □

Bemerkung 2.81. Der Beweis von Satz 2.80 läßt sich übertragen, wenn $(K, +, \cdot)$ Ring ist mit $1 \in K$ und g normiert oder der höchste Koeffizient von g Einheit ist.

2.8 Nullstellen von Polynomen

Satz 2.82. Seien $(R, +, \cdot)$ kommutativer Ring, $1 \in R,\ f \in R[x],\ \alpha \in R$ mit $f(\alpha) = 0$ (genauer $\widetilde{f}(\alpha) = 0$, wobei $\widetilde{f}$ die zu f gehörige Polynomabbildung ist), also α ist Nullstelle von $f(x),\ f \neq 0$.
Dann existiert genau ein $q \in R[x]$ mit $f = (x - \alpha) \cdot q,\ \text{grad } f = \text{grad } q + 1$.

Beweis.
Existenz: Der Divisionsalgorithmus für Polynome (Satz 2.80) liefert eine Gleichung der Form

$$f = q(x - \alpha) + r$$

mit $r = 0$ oder grad $r <$ grad $(x - \alpha)$, also ist r konstant. Der Einsetzungshomomorphismus (Satz 2.77) liefert $0 = f(\alpha) = q(\alpha) \cdot 0 + r$, also $r = 0$.
Eindeutigkeit: Aus $(x - \alpha) \cdot q - (x - \alpha) \cdot q^* = 0$ folgt $(x - \alpha) \cdot (q - q^*) = 0$ (Nullpolynom), also $q = q^*$. Es gilt grad $f =$ grad $q + 1$. □

Definition 2.83. k-fache Nullstelle
Seien $(R, +, \cdot)$ kommutativer Ring, $1 \in R,\ f \in R[x],\ f \neq 0,\ \alpha \in R$.
α heißt k-fache Nullstelle von f, wenn gilt

$$f = (x - \alpha)^k \cdot q$$

für ein $q \in R[x]$ mit $q(\alpha) \neq 0$.

Bemerkung 2.84. In Definition 2.83 sind k und q durch f eindeutig bestimmt. Dies ergibt sich analog zum Beweis von Satz 2.80.

Bemerkung 2.85. Seien I Integritätsbereich, $1 \in I,\ f \in I[x],\ f \neq 0$,
$\alpha_i \quad r_i$-fache Nullstellen von f für $i = 1, \ldots, s$ und α_i paarweise verschieden.
Dann läßt sich f darstellen in der Form

$$f = \prod_{i=1}^{s} (x - \alpha_i)^{r_i} \cdot q.$$

Dabei ist $q \in I[x]$ eindeutig bestimmt. Ferner gilt $q(\alpha_i) \neq 0$ für $i = 1, \ldots, s$.

Beweis. Die Existenz der Darstellung ergibt sich durch vollständige Induktion nach der Anzahl der „abgespaltenen" Linearfaktoren.
Die Eindeutigkeit von $q \in I[x]$ ergibt sich analog zum Beweis von Satz 2.82 unter Anwendung von Bemerkung 2.84.

Bemerkung 2.86. Sei $(I, +, \cdot)$ Integritätsbereich, $1 \in I,\ f \in I[x],\ f \neq 0$.
Dann besitzt f höchstens grad f Nullstellen. Dabei zählen k-fache Nullstellen als k Nullstellen.

Beweis. Vergleiche die Grade auf beiden Seiten der Gleichung in Bemerkung 2.85.

Bemerkung 2.87.

1. Bemerkung 2.86 gilt nicht für beliebige kommutative Ringe.
   Zum Beispiel besitzt $x^3 - x \in \mathbb{Z}_6[x]$ 6 Nullstellen.

2. Bemerkung 2.86 gilt nicht für beliebige Schiefkörper. Man beachte, daß zum Beweis der Einsetzungshomomorphismus benutzt wird. Ist Q der Quaternionenschiefkörper, so besitzt $x^2+1 \in Q[x]$ die Nullstellen i, j, k.
   Siehe Ergänzung 2.78 auf Seite 54.

Bemerkung 2.88. Formale Ableitung
Seien $(I, +, \cdot)$ Integritätsbereich, $1 \in I$, $f = a_n x^n + \cdots + a_0 \in I[x]$.
Setze $f' := a_n \cdot n \cdot x^{n-1} + \cdots + a_1 \in I[x]$. f' heißt formale Ableitung von f.
$a_m \cdot m$ bezeichne die m-fache Summe von a_m mit sich selbst.
Dann gilt

$$(f+g)' = f' + g',$$
$$(f \cdot g)' = f \cdot g' + f' \cdot g.$$

Der Beweis sei als Übung empfohlen.
Sei α Nullstelle von f. Dann gilt:

$$\alpha \text{ ist 1-fache Nullstelle von } f \Leftrightarrow f'(\alpha) \neq 0.$$

Allgemeiner gilt falls Char $I = 0$:

$$\alpha \text{ ist } n\text{-fache Nullstelle von } f \Leftrightarrow \alpha \text{ ist } (n-1)\text{-fache Nullstelle von } f'.$$

Beweis.
Sei $f = (x - \alpha) \cdot g$.
Dann folgt $f' = (x - \alpha)g' + g$.
Also ist $f'(\alpha) = 0$ gleichwertig mit $g(\alpha) = 0$.
Die Verallgemeinerung ergibt sich analog.

Folgerung 2.89. $x^{p^n} - x \in I[x]$ besitzt keine mehrfachen Nullstellen, falls Char $I = p$.

Satz 2.90.
Seien $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $\alpha \in \mathbb{Q}$ mit $f(\alpha) = 0$, $\alpha = \frac{r}{s}$, $r \in \mathbb{Z}$, $s \in \mathbb{N}$, $\mathrm{ggT}(r, s) = 1$.
Dann ist $s | a_n$ und $r | a_0$.
Im Fall $a_n = 1$ ist also $\alpha \in \mathbb{Z}$ und $\alpha | a_0$.

Beweis. Es gilt $s^n \cdot f(\frac{r}{s}) = 0 = a_n r^n + a_{n-1} s r^{n-1} + \cdots + a_0 s^n$, also $s | a_n r^n$ und damit $s | a_n$ und $r | a_0$.

Beispiel 2.91. Als mögliche Nullstellen von $x^5 + x + 2 \in \mathbb{Q}[x]$ kommen nach Satz 2.90 höchstens die Elemente $0, \pm 1, \pm 2$ in Frage (tatsächlich ist -1 die einzige Nullstelle in $\mathbb{Q}$).

Kapitel 3

Ideale in Kommutativen Ringen

In diesem Kapitel seien alle Ringe kommutativ!

3.1 Summe und Produkt von Idealen

Sei $(R, +, \cdot)$ kommutativer Ring. Nach Definition 2.22 heißt $\mathfrak{a} \subseteq R$ Ideal von R, wenn gilt: $(\mathfrak{a}, +)$ ist Gruppe und $(r \in R,\ a \in \mathfrak{a} \Rightarrow r \cdot a \in \mathfrak{a})$.

Bemerkung 3.1.
Der Durchschnitt von Idealen von R ist wieder Ideal von R.

Definition 3.2. Hauptideal, Erzeugendensystem
Seien $(R, +, \cdot)$ kommutativer Ring, $M \subseteq R$. Dann bezeichnet

$$(M) := \bigcap_{\substack{M \subseteq \mathfrak{a} \\ \mathfrak{a} \text{ ist Ideal von } R}} \mathfrak{a}$$

das kleinste Ideal von R, welches M umfaßt, und M heißt Erzeugendensystem des Ideals (M).
Ein Ideal $\mathfrak{a}$ heißt Hauptideal von R, wenn $\mathfrak{a}$ von einem Element erzeugt wird.

Bemerkung 3.3. Seien $(R, +, \cdot)$ kommutativer Ring, $M \subseteq R$.
Ist $M = \emptyset$, so gilt $(M) = \{0\}$.
Ist $M \neq \emptyset$, so enthält (M) genau alle endlichen Summen der Form

$$\sum_{i=1}^{n} r_i m_i + \sum_{j=1}^{s} k_j m'_j$$

wobei $r_i \in R;\ m_i, m'_j \in M;\ k_j \in \mathbb{Z}$ und
$k \cdot m := \underbrace{m + \cdots + m}_{(k-mal)}$, falls $k > 0$

$k \cdot m := 0$, falls $k = 0$
$k \cdot m := \underbrace{-m - \cdots - m}_{(k-mal)}$, falls $k < 0$.
Im Fall $1 \in R$ enthält (M) genau alle endlichen Summen der Form

$$\sum_{i=1}^{n} r_i m_i \qquad r_i \in R,\ m_i \in M.$$

Beispiel 3.4.

1. Sei $1 \in R$. Dann gilt:
   - $(a) = \{\lambda \cdot a | \lambda \in R\}$.
   - $(1) = R$.
   - $(a) = R \Leftrightarrow a$ ist Einheit.
   - $(a, b) = (a, b, -b) = (a, -b) = (a, a + b)$.
2. In $\mathbb{Z}$ gilt: $(6, -9, 21) = (6, -9, 21, -3) = (3)$.
3. In $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ gilt
   $(2, 1 + \sqrt{-5}) = (2, -1 - \sqrt{-5}) = (2, 1 - \sqrt{-5})$.

Definition 3.5. Summenideal
Seien $\mathfrak{a}_i$ $(i \in I)$ Ideale von R.
Dann bezeichnet $\sum_{i \in I} \mathfrak{a}_i$ das kleinste Ideal, welches alle $\mathfrak{a}_i$ enthält.

Bemerkung 3.6. Die obige Definition des Summenideals ist sinnvoll nach Bemerkung 3.1. Sonst existiert das kleinste Ideal eventuell nicht.
$\sum_{i \in I} \mathfrak{a}_i$ enthält genau alle endlichen Summen der Form

$$a_1 + \cdots + a_n,$$

wobei a_i aus einem der Ideale $\mathfrak{a}_i$ stammt.

Beispiel 3.7. In $\mathbb{Z}$ gilt

- $(6) + (9) = (6, 9) = (3)$.
- $(2) + (3) = (2, 3) = (1)$.

Generell gilt

- $\mathfrak{a} + \mathfrak{b} = (\mathfrak{a} \cup \mathfrak{b})$.
- $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$.

Definition 3.8. Produktideal
Seien $\mathfrak{a},\ \mathfrak{b}$ Ideale von R.
Dann bezeichnet $\mathfrak{a} \cdot \mathfrak{b}$ das kleinste Ideal, welches $\{a \cdot b | a \in \mathfrak{a},\ b \in \mathfrak{b}\}$ enthält.

Bemerkung 3.9. $\mathfrak{a} \cdot \mathfrak{b}$ enthält genau alle endlichen Summen der Form

$$\sum a_i b_i \text{ mit } a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}.$$

Bemerkung 3.10. Für Ideale $\mathfrak{a},\ \mathfrak{b}$ gilt stets $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

Bemerkung 3.11. Seien $(R, +, \cdot)$ kommutativer Ring; $A, B \subseteq R$,
$\mathfrak{a} := (A)$,
$\mathfrak{b} := (B)$,
$A \cdot B := \{a \cdot b | a \in A,\ b \in B\}$.
Dann gilt $\mathfrak{a} \cdot \mathfrak{b} = (A \cdot B)$.
Ist A Erzeugendensystem von $\mathfrak{a}$, B Erzeugendensystem von $\mathfrak{b}$, so ist $A \cdot B$ Erzeugendensystem von $\mathfrak{a} \cdot \mathfrak{b}$.

Beweis. Folgt aus Bemerkung 3.3.

Beispiel 3.12. Betrachte das Ideal $\mathfrak{a} := (2, 1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$.
Dann gilt $\mathfrak{a}^2 := \mathfrak{a} \cdot \mathfrak{a} = (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) = (4, 2 + 2\sqrt{-5}, 6) = (2)$.

Bemerkung 3.13. Für Ideale eines kommutativen Ringes gilt:

1. $(\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c})$.
2. $\mathfrak{a} \cdot \sum_{i \in I} \mathfrak{b}_i = \sum_{i \in I} \mathfrak{a} \cdot \mathfrak{b}_i$.

3.2 Teilbarkeit in Integritätsbereichen

Definition 3.14. Seien $(R, +, \cdot)$ Integritätsbereich mit $1 \in R$; $a, b \in R$; E die Gruppe der Einheiten von R.

1. $a \sim b :\Leftrightarrow \exists \varepsilon \in E$ mit $a = \varepsilon \cdot b$
   Sprechweise: a und b sind assoziiert.
2. a $\Big|$ b (in R):$\Leftrightarrow \exists c \in R$ mit $a \cdot c = b$.

Bemerkung 3.15. $\sim$ ist eine Äquivalenzrelation auf R.

Beweis.
$a \sim a$, da $1 \in E$.
Sei $a \sim b$, etwa $a = \varepsilon \cdot b$. Dann folgt $b = a \cdot \varepsilon^{-1}$, also $b \sim a$.
Aus $a \sim b \wedge b \sim c$, etwa $a = \varepsilon_1 b,\ b = \varepsilon_2 c$ folgt $a = \varepsilon_1 \cdot \varepsilon_2 c$, also $a \sim c$.

Bemerkung 3.16.

1. Gilt $a|b$ in R, $a \sim a'$ und $b \sim b'$, so folgt $a'|b'$.
2. $a \sim b \Leftrightarrow a|b$ und $b|a$.

Beispiel 3.17. Die Einheiten in $\mathbb{Z}$ sind ± 1.

Beispiel 3.18. Wir betrachten den Ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ und die Abbildung $N : \mathbb{C} \to \mathbb{R}$, $N(z) = z \cdot \bar{z}$ für alle $z \in \mathbb{C}$.
Bekanntlich gilt $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$ (N heißt Normabbildung).
Für die Einheiten in $\mathbb{Z}[\sqrt{-5}]$ gilt:

1. $\varepsilon \in \mathbb{Z}[\sqrt{-5}]$ Einheit $\Leftrightarrow N(\varepsilon) = 1$
2. Die Einheiten von $\mathbb{Z}[\sqrt{-5}]$ sind ± 1.

Beweis.

1. $N(\varepsilon) = \varepsilon \cdot \bar{\varepsilon} = 1 \Rightarrow \bar{\varepsilon}$ ist zu ε invers.
   Ist ε Einheit, so gilt $N(\varepsilon \cdot \varepsilon^{-1}) = 1 = N(\varepsilon) \cdot N(\varepsilon^{-1})$,
   $N(\varepsilon) \in \mathbb{N}$, $N(\varepsilon^{-1}) \in \mathbb{N}$, also folgt die Behauptung.
2. Klar.

Beispiel 3.19. Im Ring $\mathbb{Z}[i] := \{a + bi | a, b \in \mathbb{Z}\}$ gilt:
$\varepsilon \in \mathbb{Z}[i]$ ist Einheit $\Leftrightarrow N(\varepsilon) = 1$.
Die Einheiten von $\mathbb{Z}[i]$ sind ± 1, $\pm i$.

Teilbarkeitsbeziehungen in Integritätsbereichen lassen sich idealtheoretisch ausdrücken. Dies besagt der wichtige, aber leicht zu beweisende

Satz 3.20. Seien $(R, +, \cdot)$ Integritätsbereich, $1 \in R$; $a, b \in R$. Dann gilt:

1. $(a) \subseteq (b) \Leftrightarrow b|a$.
2. $(a) = (b) \Leftrightarrow a|b$ und $b|a \Leftrightarrow a \sim b$
3. ε Einheit $\Leftrightarrow \varepsilon|a$ für alle $a \in R$
4. $\varepsilon|1 \Leftrightarrow \varepsilon$ ist Einheit.
5. $a \in (b) \Leftrightarrow b|a$

Definition 3.21. Sei $(R, +, \cdot)$ Integritätsbereich, $1 \in R, a \in R, a \neq 0$, a nicht Einheit.
Dann wird definiert:

1. a unzerlegbar (in R) $:\Leftrightarrow (a = b \cdot c \Rightarrow b$ Einheit oder c Einheit)
   a besitzt nur die trivialen Teiler, also nur Einheiten und zu a assoziierte Elemente als Teiler.

2. a Primelement (in R) $:\Leftrightarrow (a|b \cdot c \Rightarrow a|b \vee a|c)$.

3. Sei $f \in R[x], f \neq 0, gradf > 0$.
   f reduzibel (über R oder in $R[x]$) $:\Leftrightarrow$ f ist darstellbar als Produkt zweier nicht konstanter Polynome aus $R[x]$.
   f irreduzibel (über R oder in $R[x]$) $:\Leftrightarrow$ f ist nicht darstellbar als Produkt zweier nicht konstanter Polynome aus $R[x]$.

Beispiel 3.22. $2x^2 + 2 \in \mathbb{Z}[x]$ ist irreduzibel, da das Polynom in $\mathbb{Z}$ offenbar keine Nullstellen besitzt, aber nicht unzerlegbar (eine nichttriviale Zerlegung ist $2(x^2 + 1)$).

Satz 3.23. Jedes Primelement ist unzerlegbar (Beispiel 3.25 zeigt, daß die Umkehrung falsch ist).

Beweis. Sei p Primelement und gelte $p = b \cdot c$. O.B.d.A. folgt $p|b$, etwa $p \cdot r = b$ für ein $r \in R$.
Dann ist $p = p \cdot r \cdot c$, also $r \cdot c = 1$ und damit c Einheit.

Beispiel 3.24. In $(\mathbb{Z}, +, \cdot)$ sind genau die Primzahlen $\pm 2, \pm 3, ...$ die Primelemente und auch die unzerlegbaren Elemente. Die Begriffe Primelement und unzerlegbares Element fallen in diesem Fall zusammen. Dies ist intuitiv klar. Ein Beweis folgt in Abschnitt 3.3.

Beispiel 3.25.

1. In $\mathbb{Z}[\sqrt{-5}]$ ist die 2 unzerlegbar. Aus $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ folgt durch Anwendung der Normabbildung $4 = N(2) = (a^2 + 5b^2)(c^2 + 5d^2)$, also $b = d = 0$ und $a = \pm 2, c = \pm 1$ oder $a = \pm 1, c = \pm 2$.

2. In $\mathbb{Z}[\sqrt{-5}]$ ist 2 nicht Primelement. Es gilt nämlich
   $2|6, 6 = (1+\sqrt{-5})(1-\sqrt{-5})$, aber $2 \nmid (1 \pm \sqrt{-5})$ (da $\frac{1 \pm \sqrt{-5}}{2} \notin \mathbb{Z}[\sqrt{-5}]$).

Beispiel 3.26. Ist $p \in R$ Primelement, so ist auch jedes zu p assoziierte Element Primelement.
Die Aussage gilt analog für unzerlegbare Elemente.

Satz 3.27. Seien $(R, +, \cdot)$ Integritätsbereich; $1, r \in R$; $r \neq 0$, r nicht Einheit.
Dann gilt:
r ist unzerlegbar $\Leftrightarrow (r)$ ist maximal unter den Hauptidealen $\neq R$ von R.
Das heißt: $((r) \subseteq (a) \subseteq R) \Rightarrow ((a) = (r)$ oder $(a) = R)$.

Beweis. $\Rightarrow$:
Sei r unzerlegbar. Dann ist r auch nicht Einheit. Dann ist $(r) \neq R(= (1))$ (nach Satz 3.20.2).
Gelte $(r) \subseteq (a) \subseteq R$.
Dann $\exists b \in R$ mit $r = a \cdot b$.
Da r als unzerlegbar angenommen wird, folgt: a ist Einheit (also $(a) = R$) oder b ist Einheit (also $(r) = (a)$) nach Satz 3.20.2.
$\Leftarrow$: Sei $(r) \neq R$ maximal unter den Hauptidealen.
Gelte $r = a \cdot b$. Dann folgt (nach Satz 3.20.1) $(r) \subseteq (a)$ und aufgrund der Voraussetzung $(r) = (a)$ oder $R = (a)$.
Im 1. Fall folgt, daß b Einheit ist (Satz 3.20.2).
Im 2. Fall folgt, daß a Einheit ist.

3.3 Euklidische-, Hauptideal- und ZPE-Ringe

Betrachtet werden in diesem Abschnitt Integritätsbereiche mit Eins mit speziellen Eigenschaften.

Definition 3.28. Sei R Integritätsbereich mit Eins. R heißt Hauptidealring, wenn jedes Ideal von R Hauptideal ist (also von einem Element erzeugt wird).

Definition 3.29. Sei R ein Integritätsbereich mit Eins.
R heißt ZPE-Ring, wenn für jedes $r \in R$, $r \neq 0$, r nicht Einheit, gilt:

1. r ist Produkt unzerlegbarer Elemente.

2. Gilt $r = p_1 \cdots p_t = q_1 \cdots q_s$, mit $p_1, \ldots, p_t, q_1, \ldots, q_s$ unzerlegbar, so folgt $t = s$ und bei geeigneter Numerierung $p_i \sim q_i$.
   (d.h. die Darstellung von r als Produkt unzerlegbarer Elemente ist im wesentlichen eindeutig).

Bemerkung 3.30. Sei R ZPE-Ring und $r \in R$. Dann gilt:
r ist unzerlegbar $\Leftrightarrow$ r ist Primelement.

Beweis. $\Leftarrow$: nach Satz 3.23
$\Rightarrow$: Sei r unzerlegbar.
Gelte $r|a \cdot b$, etwa $r \cdot c = a \cdot b$.
In der Zerlegung von $a \cdot b$ in ein Produkt unzerlegbarer Elemente tritt nach Definition 3.29 ein zu r assoziierter Faktor auf. Dies ist dann auch der Fall bei einem der Faktoren a oder b, etwa bei b. Dann folgt $r|b$.

Bemerkung 3.31. $\mathbf{Z}[\sqrt{-5}]$ ist kein ZPE-Ring, denn nach Beispiel 3.25 ist 2 unzerlegbar, aber nicht Primelement.

Zum Beispiel erhält man durch $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ zwei verschiedene Darstellungen von 6 als Produkt unzerlegbarer Elemente. Mit Hilfe der Normabbildung läßt sich leicht zeigen, daß jedes Element $\neq 0$, welches nicht Einheit ist, als Produkt unzerlegbarer Elemente darstellbar ist.

Satz 3.32. Jeder Hauptidealring ist ZPE-Ring.
(In den Übungen wird gezeigt, daß die Umkehrung falsch ist.)

Als Vorbereitung für den Beweis werden 2 Lemmata benötigt.

Lemma 3.33. Sei R Hauptidealring. Dann wird jede aufsteigende Kette $(a_0) \subseteq (a_1) \subseteq \ldots$ von Idealen konstant.
Das heißt, es existiert ein $j \in \mathbb{N}$ mit $(a_j) = (a_{j+1}) = (a_{j+2}) = \ldots$. (Die Aussage gilt analog für Integritätsbereiche mit Eins, in denen jedes Ideal von endlich vielen Elementen erzeugt wird (Noethersche Ringe)).

Beweis. Offenbar ist $\bigcup_{i=0}^{\infty}(a_i)$ Ideal in R, etwa von der Form (b).
Dann gilt $b \in (a_j)$ für ein geeignetes j, also $(b) \subseteq (a_j)$.
Hieraus folgt die Behauptung. □

Lemma 3.34. Sei R Hauptidealring. Dann ist jedes unzerlegbare Element Primelement.

Beweis. Sei p unzerlegbar, gelte $p|a \cdot b,\ p \nmid a$, also $a \notin (p)$.
Nach Satz 3.27 folgt $(p, a) = (1)$.
Dann gilt $1 = \lambda \cdot p + \mu \cdot a$ für geeignete $\lambda, \mu \in R$, also $b = \lambda p \cdot b + \mu \cdot \underbrace{a \cdot b}_{\text{Vielfaches von } p}$
und damit $p|b$. □

Beweis von Satz 3.32 Existenz einer Zerlegung (mit Hilfe von Lemma 3.33):
Sei $a_0 \in R$, $a_0 \neq 0$, a_0 nicht Einheit.
Annahme: a_0 ist nicht Produkt unzerlegbarer Elemente; speziell ist dann a_0 nicht unzerlegbar.
Gelte $a_0 = a_1 \cdot b_1$; a_1, b_1 nicht Einheiten, also $(a_0) \subsetneqq (a_1)$, $(a_0) \subsetneqq (b_1)$ (nach Satz 3.20 auf Seite 62). Aufgrund der Annahme ist mindestens einer der Faktoren a_1, b_1 ebenfalls nicht Produkt unzerlegbarer Elemente; etwa a_1. Führt man dieselbe Überlegung anstelle von a_0 nun für a_1 durch, so erhält man ein $a_2 \in R$ mit $(a_1) \subsetneqq (a_2)$, a_2 nicht Produkt unzerlegbarer Elemente.
Fortführung liefert eine Folge von Idealen $(a_0) \subsetneqq (a_1) \subsetneqq \ldots$ im Widerspruch zu Lemma 3.33.
(Bei dieser Schlußweise wird das Auswahlaxiom benutzt:
Betrachte die Menge aller Elemente aus R, die nicht Produkt unzerlegbarer

Elemente sind.
Ordne jedem dieser Elemente r die Menge T_r aller Teiler zu, die nicht Produkt unzerlegbarer Elemente sind.
Dann wird eine Auswahlfunktion für die Menge der Mengen T_r benötigt.)
Eindeutigkeit der Zerlegung (mit Hilfe von Lemma 3.34):
Gelte $a = p_1 \cdots p_r = q_1 \cdots q_s$ für unzerlegbare Elemente $p_1, \ldots, p_r, q_1, \ldots, q_s$; speziell $p_1 | q_1 \cdots q_s$.
Nach Lemma 3.34 sind die p_j auch Primelemente, also folgt $p_1 | q_j$ für ein geeignetes j. Da q_j unzerlegbar ist, folgt $p_1 \sim q_j$.
Kürzen und Wiederhohlung der Schlußweise liefert die Behauptung.

Definition 3.35. Sei R Integritätsbereich mit $1 \in R$.
R heißt Euklidischer Ring, wenn eine Abbildung $f : R \setminus \{0\} \to \mathbb{N}_0$ existiert mit:
Zu $a, b \in R$ mit $b \neq 0$ existieren Elemente $q, r \in R$ mit
$a = q \cdot b + r$, wobei $r = 0$ oder $f(r) < f(b)$.
f heißt Euklidische (Norm-)Abbildung von R.

Bemerkung 3.36. $(\mathbb{Z}, +, \cdot)$ ist ein Euklidischer Ring, $f : \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0$ definiert durch $f(z) := |z|$ ist eine Euklidische Abbildung von $\mathbb{Z}$.
(Dies ist aufgrund der intuitiven Vorstellung von $\mathbb{Z}$ klar. Für einen exakten Beweis verwendet man, daß $(\mathbb{Z}, +, \cdot, \leq)$ ein archimedisch angeordneter Ring ist.)
Sei $(K, +, \cdot)$ ein Körper.
Dann ist der Polynomring $K[x]$ Euklidischer Ring und $f : K[x] \setminus \{0\} \to \mathbb{N}_0$ definiert durch $f(g(x)) := \operatorname{grad} g(x)$ ist eine Euklidische Abbildung von $K[x]$ nach Satz 2.80 auf Seite 55.
Natürlich kann ein Ring mehrere Euklidische Abbildungen besitzen.

Satz 3.37. Jeder Euklidische Ring ist Hauptidealring.
(Die Umkehrung ist falsch, zum Beispiel für $\mathbb{Z}[\sqrt{-19}]$, ohne Beweis.)

Beweis. Sei $\mathfrak{a} \neq (0)$ Ideal von R.
Wähle $a \in \mathfrak{a},\ a \neq 0$, so daß $f(a) \leq f(b)$ für alle $b \in \mathfrak{a},\ b \neq 0$.
Gezeigt wird dann $\mathfrak{a} = (a)$. Trivial ist $(a) \subseteq \mathfrak{a}$.
Sei $b \in \mathfrak{a}$ beliebig. Nach Voraussetzung existieren Elemente $q, r \in R$ mit $b = q \cdot a + r$ mit $r = 0$ oder $f(r) < f(a)$.
Aus $r = b - q \cdot a \in \mathfrak{a}$ und der Minimalität von $f(a)$ folgt $r = 0$, also $b \in (a)$. □

Bemerkung 3.38. Sei $(K, +, \cdot)$ Körper, $K[x]$ der Polynomring in einer Unbestimmten.
Dann ist $K[x]$ Hauptidealring, also auch ZPE-Ring (siehe Satz 3.32, Bemerkung 3.36 und Satz 3.37).

Beispiel 3.39. $\mathbb{Z}[i] := \{a + bi | a, b \in \mathbb{Z}\}$ ist ein Euklidischer Ring.
$N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}_0$ definiert durch $N(a + bi) := a^2 + b^2$ ist eine Euklidische Abbildung von $\mathbb{Z}[i]$.
Seien $\alpha, \beta \in \mathbb{Z}[i];\ \beta \neq 0$.
Dann ist zu zeigen: Es existiert ein $q \in \mathbb{Z}[i]$ mit $N(\alpha - q\beta) < N(\beta)$ beziehungsweise $N(\frac{\alpha}{\beta} - q) < 1$ (beachte, daß N multiplikativ ist, das heißt $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ für alle $\alpha, \beta \in \mathbb{Z}[i]$).
Die letzte Bedingung bedeutet geometrisch in der Gaußschen Zahlenebene, daß es zu $\frac{\alpha}{\beta}$ einen Gitterpunkt q mit ganzzahligem Real- und Imaginärteil gibt mit Abstand kleiner als eins von $\frac{\alpha}{\beta}$. Dies ist klar.

Bemerkung 3.40. Sei R Integritätsbereich, $1 \in R,\ M \subseteq R,\ M \neq \emptyset$.
$d \in R$ heißt ggT von M, wenn gilt:

$$\begin{aligned} &d|m \text{ für alle } m \in M \\ &d'|m \text{ für alle } m \in M \Rightarrow d'|d. \end{aligned}$$

Ein ggT existiert nicht immer (siehe Übung).
Es gilt:

$$\begin{aligned} d_1, d_2 \text{ ggT von } M \Rightarrow d_1|d_2 \wedge d_2|d_1 &\underset{\text{siehe Satz 3.20.2}}{\Rightarrow} d_1 \sim d_2 \\ d_1 \text{ ggT von } M \wedge d_1 \sim d_2 &\underset{\text{siehe Bemerkung 3.16}}{\Rightarrow} d_2 \text{ ggT von } M. \end{aligned}$$

Bemerkung 3.41. Sei $(R, +, \cdot)$ ZPE-Ring, $r \in R$.
Mit r ist auch jedes zu r assoziierte Element Primelement.
$\mathbb{P}_R$ enthalte aus jeder Äquivalenzklasse assoziierter Primelemente genau einen Vertreter.
Sei $a \in R,\ a \neq 0$.
Dann läßt sich a eindeutig darstellen in der Form

$$a = \varepsilon \cdot \prod_{p \in \mathbb{P}_R} p^{\nu_p(a)} \quad \text{mit} \quad \begin{cases} \nu_p(a) \in \mathbb{N}_0 \\ \nu_p(a) \neq 0 \text{ für nur endlich viele } p \\ \varepsilon \text{ Einheit.} \end{cases}$$

Sei $M \subseteq R,\ M \neq \emptyset$.
Dann besitzt M einen ggT, nämlich $\prod_{p \in \mathbb{P}_R} p^{\min\{\nu_p(a) | a \in M\}}$.

Bemerkung 3.42. Seien $(R, +, \cdot)$ Hauptidealring, $M \subseteq R,\ M \neq \emptyset$.
Für das von M erzeugte Ideal gelte $(M) = (d)$.
Dann ist d ein ggT von M.

Dies ergibt sich wie folgt: Klar gilt $d|m$ für alle $m \in M$.
Gilt $d'|m$ für alle $m \in M$, so folgt $M \subseteq (d')$, also auch $(d) = (M) \subseteq (d')$, also $d'|d$.
Ferner läßt sich d darstellen in der Form

$$d = \lambda_1 m_1 + \cdots + \lambda_t m_t \text{ mit } \lambda_i \in R,\ m_i \in M \text{ (nach Bemerkung 3.3).}$$

Dies liefert allerdings keine Methode zur Bestimmung der λ_i (vergleiche mit Satz 3.45).

Bemerkung 3.43. Seien R Integritätsbereich, $1 \in R$, $H \subseteq R$, H Hauptidealring und Unterring von R.
Sei $d \in H$ ein ggT von $\{a, b\} \subseteq H$ in H.
Dann ist d auch ein ggT von $\{a, b\}$ in R.

Beweis. $d|a$ und $d|b$ ist klar.
Sei $\delta \in R$ und $\delta|a,\ \delta|b$.
Dann folgt auch $\delta|d$ in R, da sich (nach Bemerkung 3.42) d darstellen läßt in der Form $d = \lambda_1 a + \lambda_2 b$ mit $\lambda_1, \lambda_2 \in H$. □

Interessante Spezialfälle von Bemerkung 3.43 werden zusammengefaßt in

Bemerkung 3.44. Seien $K \subseteq E$ Körper, also $K[x] \subseteq E[x]$ Hauptidealringe nach Bemerkung 3.38.
Seien $f, g \in K[x]$. Dann gilt:

1. Ist d ggT von $\{f, g\}$ in $K[x]$, so ist d auch ggT von $\{f, g\}$ in $E[x]$.

2. Besitzen f und g in E eine gemeinsame Nullstelle α, so besitzen f und g in $K[x]$ einen gemeinsamen nicht konstanten Teiler, denn es gilt:
   Nach Satz 2.82 ist $(x-\alpha)$ gemeinsamer Teiler von f und g in $E[x]$, also ist eine Konstante aus K nicht ggT von f und g in $K[x]$ (nach Teil 1).

3. Sei $f \in K[x]$ irreduzibel, $f' \neq 0$.
   Dann besitzt f in E keine mehrfache Nullstelle.

   Beweis. Ist $\alpha \in E$ mehrfache Nullstelle von f, so gilt $f'(\alpha) = 0$ (nach Bemerkung 2.88 auf Seite 57), also ist $(x - \alpha)$ gemeinsamer Teiler von f und f' in $E[x]$.
   Also besitzen (nach Teil 2) f und f' einen nichtkonstanten gemeinsamen Teiler in $K[x]$ im Widerspruch zur Irreduzibilität von f. □

4. Nach Bemerkung 2.88 auf Seite 57 folgt:
   Sei $f(x) \in K[x]$, $f(x)$ zerfalle in $E[x]$ in ein Produkt von Linearfaktoren. Dann gilt

   $$f \text{ besitzt in } E \text{ keine mehrfache Nullstellen} \Leftrightarrow \text{ggT}(f(x), f'(x)) = 1.$$

Satz 3.45. Euklidischer Algorithmus
Seien $(R, +, \cdot)$ Euklidischer Ring und $f : R\backslash\{0\} \to \mathbb{N}_0$ euklidische Abbildung von R.
Seien $a_1, a_2 \in R$ mit $a_1 \neq 0,\ a_2 \neq 0$. Gelte

$$(*) \begin{cases} a_1 = q_1 \cdot a_2 + a_3, & f(a_3) < f(a_2), \\ a_2 = q_2 \cdot a_3 + a_4, & f(a_4) < f(a_3), \\ \quad\vdots & \\ a_{n-2} = q_{n-2} \cdot a_{n-1} + a_n, & f(a_n) < f(a_{n-1}), \\ a_{n-1} = q_{n-1} \cdot a_n + a_{n+1}, & f(a_{n+1}) < f(a_n), \\ a_n = q_n \cdot a_{n+1} + 0. & \end{cases}$$

(Nach endlich vielen Schritten erhält man stets den Rest 0.)
Dann gilt

1. a_{n+1} ist ein ggT von $\{a_1, a_2\}$.

2. Durch Einsetzen in $(*)$ lassen sich $\lambda_1, \lambda_2 \in R$ berechnen mit $a_{n+1} = \lambda_1 a_1 + \lambda_2 a_2$
   (Man beginne bei der vorletzten Gleichung.)

Beweis.

1. Es gilt $a_{n+1}|a_n$ (letzte Gleichung), also auch $a_{n+1}|a_{n-1}$ (vorletzte Gleichung). Fortführung liefert $a_{n+1}|a_2$ (zweite Gleichung), also auch $a_{n+1}|a_1$ (erste Gleichung).
   Gelte $d|a_1 \wedge d|a_2$. Dann folgt $d|a_3$ (erste Gleichung), also auch $d|a_4$ (zweite Gleichung). Fortführung liefert $d|a_{n+1}$ (vorletzte Gleichung).

2. Trivial.

Folgerung 3.46. Die ganzzahlige Gleichung $ax + by = m$ ist in $\mathbb{Z}$ lösbar genau dann, wenn m Vielfaches vom $\mathrm{ggT}(a, b)$ ist.

Das nächste Ziel in diesem Abschnitt ist der Beweis, daß der Polynomring $R[x]$ ZPE-Ring ist, falls R ZPE-Ring ist.

Definition 3.47. Primitiv
Sei R ZPE-Ring und $f = a_n x^n + \cdots + a_0 \in R[x]$ Polynom mit Koeffizienten aus R.
Dann heißt f primitiv, falls 1 ggT der Koeffizienten von f ist (der ggT existiert nach Bemerkung 3.41).

Bemerkung 3.48.
Seien R ZPE-Ring, K Quotientenkörper von R, $g \in K[x]$.
Dann existiert ein $a \in K$, so daß $a \cdot g \in R[x]$ primitiv ist.
Bis auf einen Einheitsfaktor aus R ist a eindeutig bestimmt.

Beweis. Ergibt sich aus der Definition von ZPE-Ringen.

Lemma 3.49. Gaußsches Lemma
Sei R ZPE-Ring und seien $f, g \in R[x]$.
Sind f und g primitiv, so auch $f \cdot g$.

Beweis. Seien

$$\begin{aligned} f &= a_n x^n + \cdots + a_0 \in R[x], \qquad a_n \neq 0, \\ g &= b_m x^m + \cdots + b_0 \in R[x], \qquad b_m \neq 0. \\ f \cdot g &= c_{n+m} x^{n+m} + \cdots + c_0 \in R[x]. \end{aligned}$$

Wir nehmen an, daß ein Primelement $p \in R$ existiert mit $p | c_i$ für alle i.
Nach Voraussetzung existiert ein kleinstes i mit $p \nmid a_i$.
Nach Voraussetzung existiert ein kleinstes j mit $p \nmid b_j$.
Nach Voraussetzung gilt $p | c_{i+j}$.
Andererseits gilt $c_{i+j} = \underbrace{a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots}_{\text{Vielfaches von } p} + a_i b_j + \underbrace{\cdots + a_{i+j} b_0}_{\text{Vielfaches von } p}$,
also $p \nmid c_{i+j}$.

Besonders wichtig für den Spezialfall $R = \mathbb{Z}$ ist

Satz 3.50. Seien R ZPE-Ring, K Quotientenkörper von R und $f \in R[x]$.
Dann gilt

$$f \text{ irreduzibel in } R[x] \Leftrightarrow f \text{ irreduzibel in } K[x]$$

Beweis. $\Leftarrow$ klar.
$\Rightarrow$: Gelte $f = g \cdot h$ in $K[x]$.
Sei $g = g^* \cdot g_1$, $g_1 \in R[x]$ primitiv, $g^* \in K$ (nach Bemerkung 3.48).
Sei $h = h^* \cdot h_1$, $h_1 \in R[x]$ primitiv, $h^* \in K$ (nach Bemerkung 3.48).
Dann folgt $f = g^* \cdot h^* \cdot g_1 \cdot h_1$.
Nach dem Gaußschen Lemma ist $g_1 \cdot h_1$ primitiv, andererseits gilt $f \in R[x]$ also folgt $g^* \cdot h^* \in R$.
Man erhält also eine Zerlegung von f in $R[x]$.

Satz 3.51. Ist R ZPE-Ring, so ist auch der Polynomring $R[x]$ ZPE-Ring.

Beweis. Es sei zunächst darauf hingewiesen, daß die unzerlegbaren Elemente von $R[x]$ genau die unzerlegbaren Elemente von R und die irreduziblen,

primitiven Polynome aus $R[x]$ sind.
Sei $f \in R[x]$ gegeben, f nicht Einheit in $R[x]$, $f \neq 0$.
Ist $f \in R$, so ist die „eindeutige Faktorzerlegung" in unzerlegbare Elemente klar, da R ZPE-Ring ist.
Sei f nicht aus R. Die Existenz einer Zerlegung von f in ein Produkt unzerlegbarer Elemente ist klar (man beachte grad $g \cdot h =$ grad $g +$ grad h).
Gelte $f = p_1 \cdot p_2 \cdots g_1 \cdot g_2 \cdots g_r = q_1 \cdot q_2 \cdots h_1 \cdot h_2 \cdots h_s$; p_i, q_j aus R unzerlegbar, g_i, h_i aus $R[x]$ primitiv und irreduzibel.
Nach Bemerkung 3.48 und Lemma 3.49 folgt $p_1 \cdot p_2 \cdots \sim q_1 \cdot q_2 \cdots$, und da R ZPE-Ring ist, weiter $p_1 \sim q_1,\ p_2 \sim q_2, \ldots$ bei geeigneter Numerierung.
Durch Kürzen erhält man aus der obigen Gleichung $\varepsilon \cdot g_1 \cdots g_r = h_1 \cdots h_s$, ε Einheit.
Man betrachte diese Gleichung in $K[x]$, wobei K Quotientenkörper von R ist und beachte, daß $K[x]$ Euklidischer Ring ist, also auch ZPE-Ring.
Dann folgt $r = s$ und $g_i \sim h_i$ in $K[x]$ bei geeigneter Numerierung.
Also existieren Elemente $c_i \in K$ mit $g_i = c_i \cdot h_i$.
Da $g_i,\ h_i$ in $R[x]$ primitiv sein sollten, folgt nach Bemerkung 3.48, daß $c_i \in R$ Einheit ist.
Also ist auch $g_i \sim h_i$ in $R[x]$.

Bemerkung 3.52. Eine Satz 3.51 entsprechende Aussage gilt für Hauptidealringe nicht.
Zum Beispiel ist $(2, x)$ kein Hauptideal in $\mathbb{Z}[x]$ (siehe Übung).
Ist K Körper, so ist $K[x]$ Euklidischer Ring.

3.4 Lineare und Quadratische Kongruenzen

Wir betrachten in diesem Paragraphen speziell ganzzahlige Kongruenzen.
Zunächst eine Bemerkung allgemein über Polynomkongruenzen.

Bemerkung 3.53. Seien $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd; $m := m_1 \cdots m_r$.
Ferner sei $f(x) \in \mathbb{Z}[x]$ ein Polynom mit ganzzahligen Koeffizienten.
Dann gilt offenbar:

$$f(c) \equiv 0 \pmod{m} \Rightarrow f(c) \equiv 0 \pmod{m_i} \text{ für } i = 1, \ldots, r.$$

Nach dem Chinesischen Restsatz (genauer: nach Folgerung 2.41) gilt ferner:

$$\left.\begin{array}{rl} f(c_i) \equiv 0 & \pmod{m_i} \text{ für } i = 1, \ldots, r \\ c \equiv c_i & \pmod{m_i} \text{ für } i = 1, \ldots, r \end{array}\right\} \Rightarrow f(c) \equiv 0 \pmod{m}.$$

Bei Vorgabe der c_i ist $c \pmod m$ eindeutig bestimmt.
Also folgt:
Die Anzahl der $\pmod m$ verschiedenen Lösungen von $f(x) \equiv 0 \pmod m$ ist gleich dem Produkt der entsprechenden Lösungsanzahlen von $f(x) \equiv 0 \pmod{m_i}$ für $i = 1, \ldots, r$.

Satz 3.54. Lineare Kongruenzen

1. $ax \equiv b \pmod m$ lösbar $\Leftrightarrow \mathrm{ggT}(a, m) | b$

2. Sei x_0 eine Lösung von $ax \equiv b \pmod m$.
   Dann erhält man alle $\pmod m$ verschiedenen Lösungen durch

$$x_0 + \lambda \frac{m}{\mathrm{ggT}(a, m)}, \ \lambda = 0, 1, \ldots, \ \mathrm{ggT}(a, m) - 1.$$

   Speziell: Im Fall $\mathrm{ggT}(a, m) = 1$ besitzt $ax \equiv b \pmod m$ modolo m genau eine Lösung.

Beweis.

1. $ax \equiv b \pmod m$ lösbar $\Leftrightarrow$ Es existieren $x_0, \lambda \in \mathbb{Z}$ mit $a \cdot x_0 - b = \lambda \cdot m$.
   Nach Folgerung 3.46 ist dies gleichwertig mit $\mathrm{ggT}(a, m) | b$.
   Beachte: Ein solches x_0 findet man nach endlich vielen Schritten durch Probieren oder durch Anwendung des Euklidischen Algorithmus.

2. $<>$

$$\begin{aligned} y_0 \text{ Lösung von } ax \equiv b \pmod m &\Leftrightarrow ax_0 \equiv ay_0 \pmod m \\ &\Leftrightarrow \ x_0 \equiv \ y_0 \pmod{\frac{m}{\mathrm{ggT}(a, m)}}. \end{aligned}$$

   Die letzte Äquivalenz ergibt sich aus Satz 2.33.

Folgerung 3.55. Wilson
Sei $n \in \mathbb{N}$. Dann gilt:

$$n \text{ Primzahl } \Leftrightarrow (n-1)! \equiv -1 \pmod n$$

Beweis. Sei zunächst n nicht Primzahl, etwa $n = a \cdot b, \ 1 < a, \ 1 < b$.
Dann ist $(n-1)! \pmod n$ offenbar nicht prime Restklasse $\pmod n$ im Gegensatz zu $-1 \pmod n$.
Sei nun n Primzahl. Nach Satz 3.54 existiert zu jedem $i \in \{1, 2, \ldots, n-1\}$ genau ein $j \in \{1, 2, \ldots, n-1\}$ mit $i \cdot j \equiv 1 \pmod n$. Andererseits folgt aus $i^2 \equiv 1 \pmod n$ unmittelbar $(i-1)(i+1) = 0 \pmod n$ und, da n Primzahl ist, $i \equiv 1 \pmod n$ oder $i \equiv -1 \pmod n$.
Hieraus folgt die Behauptung.

Untersucht werden soll nun die Lösbarkeit einer quadratischen Kongruenz der Form

$$x^2 \equiv a \pmod{p};\ p > 2 \text{ Primzahl}, a \in \mathbb{Z},\ p \nmid a.$$

Definition 3.56. Legendre-Symbol
Seien $a \in \mathbb{Z},\ p > 2$ Primzahl. Dann wird das Legendre-Symbol $\left(\frac{a}{p}\right)$ definiert durch

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } x^2 \equiv a \pmod{p} \text{ lösbar und } p \nmid a \\ -1 & \text{falls } x^2 \equiv a \pmod{p} \text{ nicht lösbar und } p \nmid a \\ 0 & \text{falls } p|a \end{cases}$$

Im Fall $\left(\frac{a}{p}\right) = 1$ heißt a Quadratischer Rest $\mod p$ (QR $\mod p$);
Im Fall $\left(\frac{a}{p}\right) = -1$ heißt a Quadratischer Nichtrest $\mod p$ (QNR $\mod p$).

Einige einfache Eigenschaften des Legendre-Symbols werden zusammengestellt in

Satz 3.57. Sei p Primzahl, $p \neq 2$.

1. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{a^2}{p}\right) = 1$, falls $p \nmid a$
   $\left(\frac{1}{p}\right) = 1$
3. $\left(\frac{a}{p}\right) = 1 \Rightarrow x^2 \equiv a \pmod{p}$ besitzt genau 2 Lösungen
4. Sei g Primitivwurzel $\mod p$ und $a \equiv g^{\text{ind}(a)} \pmod{p}$.
   (Dabei ist $\text{ind}(a) \mod p - 1$ eindeutig bestimmt.)
   Dann gilt:
   $$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } 2|\text{ind}(a) \\ -1 & \text{falls } 2 \nmid \text{ind}(a). \end{cases}$$
5. Jedes vollständige prime Restsystem $\mod p$ enthält genau $\frac{p-1}{2}$ QR $\mod p$, nämlich $g^0, g^2, \ldots, g^{p-3}$ und genau $\frac{p-1}{2}$ QNR $\mod p$, nämlich $g^1, g^3, \ldots, g^{p-2}$ (dabei sei g PW $\mod p$).

Beweis.

1. Trivial.
2. Trivial.
3. Ist x_0 Lösung von $x^2 \equiv a \pmod{p}$, so gilt $x^2 - x_0^2 \equiv (x - x_0)(x + x_0) \equiv 0 \pmod{p}$, und $-x_0$ ist die einzige weitere Lösung.
4. Ist $2|\mathrm{ind}(a)$, so folgt $(g^{\frac{\mathrm{ind}(a)}{2}})^2 \equiv a \pmod{p}$, also $\left(\frac{a}{p}\right) = 1$.
   Sei $\left(\frac{a}{p}\right) = 1$, etwa $x^2 \equiv a \pmod{p}$, $x \equiv g^\alpha \pmod{p}$, so folgt $\mathrm{ind}(a) \equiv 2\alpha \pmod{(p-1)}$, also $2|\mathrm{ind}(a)$.
5. Klar nach 4.

Aus Satz 3.57.4 folgt

Satz 3.58. Multiplikativität des Legendre-Symbols
Sei $p \neq 2$ Primzahl und $a, b \in \mathbb{Z}$ mit $p \nmid a$, $p \nmid b$. Dann gilt:

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

Bemerkung 3.59. Zur Berechnung des Legendre-Symbols genügt es also, $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{q}{p}\right)$ zu kennen, wobei $p \neq q$ ungerade Primzahlen sind.

Satz 3.60.

1. Euler Kriterium
   Sei $p > 2$ Primzahl, $p \nmid a$. Dann gilt $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
2. 1. Ergänzung zum quadratischen Reziprozitätsgesetz
   Sei $p > 2$ Primzahl. Dann gilt

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 4 \\ -1 & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

Beweis.

1. Sei $\left(\frac{a}{p}\right) = 1$, etwa $x_0^2 \equiv a \pmod{p}$.
   Dann folgt $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \pmod{p}$ nach Satz 2.39.
   Sei $\left(\frac{a}{p}\right) = -1$. Dann ist nach Satz 3.57.1 $\mathrm{ind}(a)$ ungerade, etwa $a \equiv$

$g^{2\alpha+1} \pmod p$ für eine PW g.
Es folgt $a^{\frac{p-1}{2}} \equiv g^{(p-1)\alpha} \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod p$ nach Satz 2.39.
Nun ist aber $g^{\frac{p-1}{2}} \equiv -1 \pmod p$, denn nach Satz 2.39 ist $g^{\frac{p-1}{2}}$ Lösung von $x^2 - 1 \equiv (x-1)(x+1) \equiv 0 \pmod p$.

2. Folgt aus Teil 1. für $a = -1$.

Satz 3.61. 2. Ergänzung zum quadratischen Reziprozitätsgesetz (Ohne Beweis)
Sei $p > 2$ Primzahl. Dann gilt

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \pmod 8 \\ -1 & \text{falls } p \equiv \pm 3 \pmod 8. \end{cases}$$

Sind p und q ungerade Primzahlen mit $p \neq q$, so ist ein einfacher Ausdruck für $\left(\frac{p}{q}\right)$ nicht bekannt.

Allerdings besteht ein einfacher Zusammenhang zwischen $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$.

Satz 3.62. Quadratisches Reziprozitätsgesetz (ohne Beweis)
Seien p und q zwei verschiedene Primzahlen > 2. Dann gilt:

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 4 \text{ oder } q \equiv 1 \pmod 4 \\ -1 & \text{sonst} \end{cases}$$

Beispiel 3.63.

$$\left(\frac{15}{23}\right) = \left(\frac{3}{23}\right) \cdot \left(\frac{5}{23}\right) = -\left(\frac{23}{3}\right) \cdot \left(\frac{23}{5}\right) = -\left(\frac{2}{3}\right) \cdot \left(\frac{3}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

3.5 Primzahlen

Nach Paragraph 3.3 ist $(\mathbb{Z}, +, \cdot)$ ein ZPE-Ring.
Die Primelemente von $\mathbb{Z}$ sind $\pm 2,\ \pm 3,\ \pm 5,\ \pm 7,\ \pm 11, \ldots$.
Die positiven Primelemente von $\mathbb{Z}$ heißen Primzahlen.
Sei $\mathbb{P} := \{2, 3, 5, 7, 11, \ldots\}$ die Menge aller Primzahlen und p_n die $n-$te Primzahl.
$\pi : \mathbb{R}^+ \to \mathbb{N} \cup \{0\}$ definiert durch $\pi(x) := \sum_{\substack{p \leq x \\ p \in \mathbb{P}}} 1$ heißt Primzahlfunktion.
$\pi(x)$ gibt also die Anzahl aller Primzahlen $\leq x$ an.

Satz 3.64. Es gibt unendlich viele Primzahlen.
Genauer gilt:

1. $p_n \leq 2^{(2^{n-1})}$ für alle $n \in \mathbb{N}$.
2. $\pi(n) > \ln\ln n$ für alle $n \in \mathbb{N}$.

Beweis. (nach Euklid)

1. Seien $p_1, \ldots, p_n$ die ersten n Primzahlen.
   Dann gilt $p_i \nmid (p_1 \cdots p_n + 1)$ für $i = 1, \ldots, n$.
   Jede natürliche Zahl läßt sich als Produkt von Primzahlen darstellen, da $\mathbb{Z}$ ZPE-Ring ist.
   Jeder Primfaktor von $(p_1 \cdots p_n + 1)$ ist $\leq (p_1 \cdots p_n + 1)$.
   Also existiert p_{n+1}, und es gilt $p_{n+1} \leq (p_1 \cdots p_n + 1)$.
   Hieraus ergibt sich die Behauptung durch vollständige Induktion.
2. Sei $n \in \mathbb{N},\ n \geq 2$ gegeben und $k \in \mathbb{Z}$ so gewählt, daß $2^{(2^{k-1})} \leq n < 2^{2^k}$.
   Dann folgt $\ln\ln n < k \leq \pi(^{(2^{k-1})}) \leq \pi(n)$
   (mit diesem Ansatz erhält man aus einer oberen Abschätzung für p_n eine untere Abschätzung für $\pi(n)$).

Satz 3.65. Sieb des Eratosthenes
Sei $n \in \mathbb{N},\ n \geq 2$ gegeben.
Betrachte die Zahlen $1, 2, 3, \ldots n$.

1. Streiche 1.
2. Unterstreiche die kleinste nicht gestrichene und nicht unterstrichene Zahl und streiche alle echten Vielfachen davon.
3. Wiederhole Schritt 2 bis eine Zahl $> \sqrt{n}$ unterstrichen ist.

Behauptung: Die nicht gestrichenen Zahlen sind genau die Primzahlen $\leq n$.
(„Ausgesiebt" werden alle Zahlen, die echtes Vielfaches einer Primzahl sind.)

Beweis. Offenbar werden Primzahlen $\leq n$ nicht gestrichen.
Sei $m \leq n$ und m nicht Primzahl.
Dann besitzt m einen Primteiler $p \leq \sqrt{n}$, und als echtes Vielfaches von p wird m gestrichen.

Die Abschätzungen in Satz 3.64 lassen sich wesentlich verbessern. Es gilt

Satz 3.66. Primzahlsatz (ohne Beweis)

$$\pi(x) \sim \frac{x}{\ln x} \qquad \text{(das heißt: } \lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1\text{);}$$

$$p_n \sim n \ln n \qquad \text{(das heißt: } \lim_{n\to\infty} \frac{p_n}{n \cdot \ln n} = 1\text{).}$$

3.6 Irreduzibilitätskriterien

Bereits bewiesen wurde (siehe Satz 3.50)

Bemerkung 3.67. Seien R ZPE-Ring, K Quotientenkörper von R, $f \in R[x]$.
Dann gilt:

$$f \text{ irreduzibel in } R[x] \Leftrightarrow f \text{ irreduzibel in } K[x].$$

Speziell für $f \in \mathbb{Z}[x]$:

$$f \text{ irreduzibel in } \mathbb{Z}[x] \Leftrightarrow f \text{ irreduzibel in } \mathbb{Q}[x].$$

Beispiel 3.68.
$x^2 - 2$ irreduzibel in $\mathbb{Q}[x]$ ($\sqrt{2}$ ist nicht rational)
$x^2 - 2$ nicht irreduzibel in $\mathbb{R}[x]$

Bemerkung 3.69.
Seien $(R, +, \cdot)$ Integritätsbereich, $1 \in R,\ f \in R[x],\ a \in R$.
Dann gilt:

$$f(x) \text{ irreduzibel in } R[x] \Leftrightarrow f(x+a) \text{ irreduzibel in } R[x].$$

Beweis. Es ist leicht nachzurechnen,
daß aus $f = g \cdot h$ folgt $f(x+a) = g(x+a) \cdot h(x+a)$.

Bemerkung 3.70. Sei $f \in R[x],\ f = a_n x^n + \cdots + a_0$.
Ferner seien $m \in \mathbb{N}$ gegeben und $a_n \not\equiv 0 \pmod{m}$.
Weiter sei $\widetilde{f} := \overline{a_n} x^n + \cdots + \overline{a_0} \in \mathbb{Z}_m[x]$.
Dabei bezeichne $\overline{a_i}$ die Restklasse $a_i \pmod{m}$. Dann gilt:

$$\widetilde{f} \text{ irreduzibel in } \mathbb{Z}_m[x] \Rightarrow f \text{ irreduzibel in } \mathbb{Z}[x].$$

Beweis. Die Abbildung $\widetilde{\phi} : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ definiert durch
$\widetilde{\phi}(d_r x^r + \cdots + d_0) := \overline{d_r} x^r + \cdots + \overline{d_0}$ ist ein Homomorphismus (siehe Bemerkung 2.79).
Aus der Zerlegung

$$f = a_n x^n + \cdots + a_0 = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0) \text{ in } \mathbb{Z}[x]$$

erhält man also die Zerlegung

$$\widetilde{f} = \overline{a_n} x^n + \cdots + \overline{a_0} = (\overline{b_r} x^r + \cdots + \overline{b_0})(\overline{c_s} x^s + \cdots + \overline{c_0}) \text{ in } \mathbb{Z}_m[x].$$

Wegen $\overline{a_n} \neq \overline{0}$ und $a_n = b_r \cdot c_s$ folgt $\overline{b}_r \neq \overline{0}$, $\overline{c}_s \neq \overline{0}$.
Ist die Zerlegung in $\mathbb{Z}[x]$ nicht trivial, so ist auch die Zerlegung in $\mathbb{Z}_m[x]$ nicht trivial.

Beispiel 3.71. $x^3 - 8x^2 + 17x - 135$ ist irreduzibel in $\mathbb{Z}_2[x]$ (besitzt keine Nullstelle), also auch irreduzibel in $\mathbb{Z}[x]$.
Dies läßt sich auch direkt nachweisen (mit Hilfe von Satz 2.90).

Satz 3.72. Eisensteinkriterium
Sei R ZPE-Ring, $f = a_n x^n + \cdots + a_0 \in R[x]$, $n \geq 1$, $a_n \neq 0$.
Ferner existiere ein Primelement $p \in R$ mit $p \nmid a_n$, $p | a_{n-1}, \ \ldots \ , p | a_0$, $p^2 \nmid a_0$.
Dann ist f irreduzibel in $R[x]$ (und nach Bemerkung 3.67 auch in $K[x]$, wenn K Quotientenkörper von R ist).

Beweis.
Gelte $f = a_n x^n + \cdots + a_0 = g \cdot h = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0) \in R[x]$.
Dann ist zu zeigen, daß g oder h konstant ist.
Es gilt $a_0 = b_0 \cdot c_0$.
Nach Voraussetzung teilt p genau eine der Zahlen b_0 oder c_0, etwa $p | b_0, \ p \nmid c_0$.
Weiter ist nach Voraussetzung $p \nmid a_n$ und $a_n = b_r \cdot c_s$, also auch $p \nmid b_r$.
Demnach existiert ein Index m mit $p | b_0, \ \ldots, \ p | b_{m-1}, p \nmid b_m$ (grad $g \geq m$).
Es folgt $a_m = \underbrace{b_m \cdot c_0}_{\text{nicht Vielfaches von } p} + \underbrace{b_{m-1}c_1 + \cdots + b_0 c_m}_{\text{Vielfaches von } p}$, also $p \nmid a_m$.
Aus der Voraussetzung des Satzes folgt weiter $m = n$, also grad $g \geq n$.
Dies ist nur dann möglich, wenn h konstant ist.

Beispiel 3.73.

1. $3x^5 + 2x^3 - 4x^2 + 2 \in \mathbb{Z}[x]$ ist irreduzibel (wähle $p = 2$).

2. $x^n - p \in \mathbb{Z}[x]$ ($n \in \mathbb{N}$, p Primzahl) ist irreduzibel.
   Speziell folgt: $x^n - p$ hat in $\mathbb{Q}$ keine Nullstelle, also ist $\sqrt[n]{p}$ irrational.

3. Sei p Primzahl.
   Dann ist $\phi_p(x) := x^{p-1} + xy'^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ irreduzibel.
   $\phi_p(x)$ heißt p-tes Kreisteilungspolynom.

   Beweis. Es gilt

$$\begin{aligned} \phi_p(x) &= \frac{x^p - 1}{x - 1} \\ \phi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \underbrace{\binom{p}{p-1}}_{=p} x^0. \end{aligned}$$

   $\phi_p(x+1)$ ist irreduzibel in $\mathbb{Z}[x]$ nach Satz 3.72, also auch $\phi_p(x)$ nach Bemerkung 3.69.

3.7 Primideale, Maximale Ideale

Definition 3.74. Primideal, maximales Ideal
Seien $(R,+,\cdot)$ kommutativer Ring; $\mathfrak{a}$ Ideal von R und $\mathfrak{a} \neq R$.

1. $\mathfrak{a}$ heißt Primideal, wenn gilt:

$$a \cdot b \in \mathfrak{a} \Rightarrow (a \in \mathfrak{a} \vee b \in \mathfrak{a}).$$

2. $\mathfrak{a}$ heißt maximales Ideal, wenn gilt:

$$(\mathfrak{b} \text{ Ideal}, \mathfrak{a} \subseteq \mathfrak{b} \subseteq R) \Rightarrow (\mathfrak{b} = \mathfrak{a} \vee \mathfrak{b} = R).$$

Bemerkung 3.75. Seien $(R,+,\cdot)$ Integritätsbereich, $1 \in R$, $p \in R$, p nicht Einheit, $p \neq 0$. Dann gilt:

$$\begin{aligned} p \text{ Primelement} &\underset{\text{Definition 3.21}}{\Leftrightarrow} \Big(p|a \cdot b \Rightarrow (p|a \vee p|b)\Big) \\ &\underset{\text{Satz 3.20}}{\Leftrightarrow} \Big((a \cdot b) \subseteq (p) \Rightarrow \Big((a) \subseteq (p) \vee (b) \subseteq (p)\Big)\Big) \\ &\Leftrightarrow \Big(a \cdot b \in (p) \Rightarrow \Big(a \in (p) \vee b \in (p)\Big)\Big) \\ &\underset{\text{Definition 3.74}}{\Leftrightarrow} (p) \text{ Primideal.} \end{aligned}$$

Satz 3.76. Sei $(R,+,\cdot)$ kommutativer Ring; $\mathfrak{p}$ Ideal von R, $\mathfrak{p} \neq R$.
Dann gilt:

$$\mathfrak{p} \text{ Primideal} \Leftrightarrow R/\mathfrak{p} \text{ nullteilerfrei.}$$

Beweis. $\Rightarrow$: Sei $(a+\mathfrak{p}) \cdot (b+\mathfrak{p}) = a \cdot b + \mathfrak{p} = 0 + \mathfrak{p}$, also $a \cdot b \in \mathfrak{p}$.
Nach Voraussetzung folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, also $a+\mathfrak{p}$ oder $b+\mathfrak{p}$ Null in $R/\mathfrak{p}$.
$\Leftarrow$: Sei $a \cdot b \in \mathfrak{p}$, also $a \cdot b + \mathfrak{p} = (a+\mathfrak{p})(b+\mathfrak{p}) = 0 + \mathfrak{p}$.
Nach Voraussetzung folgt $a+\mathfrak{p}$ oder $b+\mathfrak{p}$ Null in $R/\mathfrak{p}$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

Satz 3.77. Sei $(R,+,\cdot)$ kommutativer Ring, $1 \in R$, $\mathfrak{m}$ Ideal von R, $\mathfrak{m} \neq R$.
Dann gilt:

$$\mathfrak{m} \text{ maximales Ideal} \Leftrightarrow R/\mathfrak{m} \text{ Körper.}$$

Beweis. $\Rightarrow$: Sei $a+\mathfrak{m}$ nicht Null in $R/\mathfrak{m}$, also $a \notin \mathfrak{m}$.
Dann folgt $(a,\mathfrak{m}) = R$, und es existieren $m \in \mathfrak{m}$, $b \in R$ mit $1 = m + b \cdot a$ (Bemerkung 3.3).
Also ist $(b+\mathfrak{m})(a+\mathfrak{m}) = 1+\mathfrak{m}$. Das heißt: $b+\mathfrak{m}$ ist zu $a+\mathfrak{m}$ in $R/\mathfrak{m}$ invers.
$\Leftarrow$: Sei $\mathfrak{a}$ ein Ideal mit $\mathfrak{m} \subsetneq \mathfrak{a} \subseteq R$.
Gezeigt wird: $\mathfrak{a} = R$.
Sei $a \in \mathfrak{a}$ mit $a \notin \mathfrak{m}$.

In $R/\mathfrak{m}$ besitzt $a+\mathfrak{m}$ nach Voraussetzung ein Inverses, etwa $b+\mathfrak{m}$.
Dann folgt $a \cdot b + \mathfrak{m} = 1 + \mathfrak{m}$, also $a \cdot b - 1 \in \mathfrak{m} \subseteq \mathfrak{a}$.
Wegen $a \in \mathfrak{a}$ ist auch $a \cdot b \in \mathfrak{a}$, also $1 \in \mathfrak{a}$, woraus $\mathfrak{a} = R$ folgt.

Bemerkung 3.78. Da jeder Körper nullteilerfrei ist, ist nach Satz 3.76 und Satz 3.77 in einem kommutativen Ring mit Eins jedes maximale Ideal Primideal.

Bemerkung 3.79. In $2\mathbb{Z}$ ist (4) maximales Ideal; $2\mathbb{Z}/(4)$ ist nicht nullteilerfrei wegen $(2+(4))(2+(4)) = 0+(4)$; erst recht ist $2\mathbb{Z}/(4)$ kein Körper (beachte: $1 \notin 2\mathbb{Z}$).

Satz 3.80. Seien $(R,+,\cdot)$ kommutativer Ring, $1 \in R$, $\mathfrak{a}$ Ideal von R, $\mathfrak{a} \neq R$. Dann besitzt R ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subseteq \mathfrak{m}$.

Beweis. Sei $M := \{\mathfrak{b} \supseteq \mathfrak{a} | \mathfrak{b} \text{ Ideal von } R, \mathfrak{b} \neq R\}$ und M geordnet bezüglich der Inklusion.
Dann ist M nicht leer wegen $\mathfrak{a} \in M$.
Sei K eine Kette von M. Dann besitzt K die obere Schranke $\sigma := \bigcup_{\tau \in K} \tau$
(offenbar ist σ Ideal, $\sigma \supseteq \mathfrak{a}$ und $1 \notin \sigma$; also $\sigma \in M$).
Nach dem Zornschen Lemma[1] besitzt M ein maximales Element $\mathfrak{m}$.
Dieses ist offenbar ein maximales Ideal, welches $\mathfrak{a}$ enthält.

---

[1] Voraussetzungen für das Zornsche Lemma:

Geordnete Menge $(M, \leq)$ heißt geordnete Menge, falls gilt:

1. $a \leq a$ für alle $a \in M$. (Reflexivität)
2. $(a \leq b \wedge b \leq a) \Rightarrow a = b$ für alle $a, b \in M$. (Antisymmetrie)
3. $(a \leq b \wedge b \leq c) \Rightarrow a \leq c$ für alle $a, b, c \in M$ (Transitivität)

Kette Eine geordnete Menge $(M, \leq)$ heißt Kette oder vollständig geordnete Menge, falls zusätzlich gilt: $a \leq b \vee b \leq a$ für alle $a, b \in M$.

Obere Schranke Seien $(M, \leq)$ eine geordnete Menge, $U \subseteq M$.
Ein Element $s \in M$ heißt obere Schranke von U, falls gilt: $k \leq s$ für alle $u \in U$.

Maximales Element Sei $(M, \leq)$ eine geordnete Menge. Ein Element $m \in M$ heißt maximales element, falls gilt: $m \leq a \Rightarrow m = a$ für alle $a \in M$.

Zornsche Lemma: Sei $(M, \leq)$ eine nicht leere, geordnete Menge.
Besitzt jede Kette $K \subseteq M$ eine obere Schranke s in M, dann besitzt M ein maximales Element m.

Kapitel 4

Elementare Körpertheorie

4.1 Körpererweiterungen

Es seien $(E, +, \cdot)$ ein Ring mit 1 und K Teilkörper von E.
Dann läßt sich E auf natürliche Weise auffassen als K-Vektorraum (dabei sei das Produkt von Skalar mit Vektor definiert durch das Produkt in E).
$[E : K]$ bezeichne die Dimension des K-Vektorraums E (Grad der Erweiterung $E : K$).
Interessant ist vor allem der Spezialfall, bei dem E Körper ist.
Grundlegend ist

Satz 4.1. Seien $K \subseteq S \subseteq E$ Körper. Dann gilt:

1. Ist $[S : K]$ unendlich, so ist auch $[E : K]$ unendlich.

2. Ist $[E : S]$ unendlich, so ist auch $[E : K]$ unendlich.

3. Sind $[E : S]$ und $[S : K]$ endlich, so auch $[E : K]$, und es gilt

$$[E : K] = [E : S] \cdot [S : K]. \qquad \text{(Körpergrad-Formel)}$$

   Genauer: Seien $\{\alpha_1, \ldots, \alpha_n\}$ Basis von $S : K$,
   $\{\beta_1, \ldots, \beta_m\}$ Basis von $E : S$.
   Dann ist $B := \{\alpha_i \beta_j | 1 \leq i \leq n,\ 1 \leq j \leq m\}$ Basis von $E : K$.

Beweis.

1. Nach Voraussetzung besitzt E einen Unterraum S unendlicher Dimension.
   Dann besitzt auch E unendliche Dimension (Lineare Algebra).

2. Sei B eine (unendliche) Basis des S-VR E, speziell B linear unabhängig über S.
   Dann ist B erst recht linear unabhänging über K.

3. Zu zeigen: B Erzeugenden-System von $E : K$.
   Sei $\gamma \in E$ beliebig gegeben.
   Dann läßt sich γ darstellen in der Form $\gamma = \sum_{j=1}^{m} s_j \beta_j$, $s_j \in S$.
   Die s_j lassen sich darstellen in der Form $s_j = \sum_{i=1}^{n} k_{ij} \alpha_i$, $k_{ij} \in K$.
   Also ist γ Linearkombination von Elementen aus B mit Koeffizienten aus K.
   Zu zeigen: B linear unabhängig über K.

$$0 = \sum_{i,j} \underbrace{k_{ij}}_{\in K} \alpha_i \beta_j = \sum_j (\underbrace{\sum_i k_{ij} \alpha_i}_{\in S}) \beta_j$$

   Da $\{\beta_1, \ldots, \beta_m\}$ Basis von E über S ist, folgt $\sum_i k_{ij} \alpha_i = 0$ für alle j.
   Da $\{\alpha_1, \ldots, \alpha_n\}$ Basis von S über K ist, folgt $k_{ij} = 0$ für alle i, j.

Bemerkung 4.2. Ringadjunktion, Körperadjunktion
Sei I Integritätsbereich, $1 \in I$.
Sei I_1 Teilbereich von I, $1 \in I_1$.
Sei $M \subseteq I$.
Dann wird definiert

$$I_1[M] := \bigcap_{\substack{R \supseteq I_1 \cup M \\ R \text{ Unterring von } I}} R$$

(kleinster Unterring von I, welcher I_1 und M enthält).
Natürlich ist $I_1[M]$ Integritätsbereich.
$I_1[M]$ enthält genau alle endlichen Summen von Elementen der Form

$$i \cdot m_1^{a_1} \cdots m_r^{a_r} \text{ mit } i \in I_1,\ m_i \in M,\ a_i \in \mathbb{N} \cup \{0\}.$$

$I_1(M)$ bezeichne den Quotientenkörper von $I_1[M]$.
$I_1(M)$ enthält genau alle Elemente der Form $\frac{a}{b}$ mit $a, b \in I_1[M],\ b \neq 0$.
Der Übergang $I_1 \to I_1[M]$ heißt Ringadjunktion.
Der Übergang $I_1 \to I_1(M)$ heißt Körperadjunktion.

Spezialfälle

1. Seien $K \subseteq E$ Körper, $M \subseteq E$.
   Dann ist $K(M)$ der kleinste Teilkörper von E, welcher K und M enthält.

2. $K_1, K_2 \subseteq E$ seien Körper. Dann gilt $K_1(K_2) = K_2(K_1)$.

3. Sei $K[x]$ Polynomring über dem Körper K.
   Dann kann $K[x]$ auch aufgefaßt werden als Ringadjunktion von x zu K.
   (Die Bezeichnungen stimmen überein.)
   $K(x)$ ist der Quotientenkörper von $K[x]$.

Beispiel 4.3.

1. $\mathbb{Q}[i] = \{a + bi | a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$.
   $\{1, i\}$ ist eine Basis des $\mathbb{Q}$-VR $\mathbb{Q}[i]$, also ist $[\mathbb{Q}[i] : \mathbb{Q}] = 2$.
   Ferner gilt $\mathbb{Q}[i] = \mathbb{Q}(i)$ (wegen $\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$, falls $a + bi \neq 0$.

2. Sei $K[x]$ Polynomring über dem Körper K.
   Dann ist $\{1, x, x^2, \dots\}$ eine Basis von $K[x] : K$.

Es gilt der wichtige

Satz 4.4. Seien $K \subseteq E$ Körper und sei $M \subseteq E$.
Ist $[K[M] : K]$ endlich, so gilt $K[M] = K(M)$.

Beweis. Sei $a \in K[M],\ a \neq 0$.
Gesucht wird ein zu a in $K[M]$ multiplikatives Inverses.
Betrachte die Abbildung

$$\begin{aligned} \varphi : K[M] &\to K[M] \text{ definiert durch} \\ \varphi(\alpha) &:= a \cdot \alpha \text{ für alle } \alpha \in K[M]. \end{aligned}$$

Dann ist φ lineare Abbildung des K-VR $K[M]$ in sich.
φ ist injektiv, denn aus $\varphi(\alpha) = \varphi(\alpha')$ folgt $a \cdot \alpha = a \cdot \alpha'$ also $\alpha = \alpha'$ (durch Multiplikation mit $a^{-1} \in E$).
Dann ist φ auch surjektiv, da $[K[M] : K]$ als endlich vorausgesetzt wurde (lineare Algebra).
Also existiert ein $\alpha \in K[M]$ mit $\varphi(\alpha) = a\alpha = 1$.

4.2 Algebraische und Transzendente Erweiterungen

Definition 4.5. Algebraisch, Transzendent
Seien $K \subseteq E$ Körper.
$E : K$ heißt endliche Körpererweiterung, falls $[E : K]$ endlich ist.
$\alpha \in E$ heißt algebraisch über K, wenn ein Polynom $f \in K[x],\ f \neq 0$, existiert mit $f(\alpha) = 0$ (sonst heißt α transzendent über K).
$E : K$ heißt algebraische Körpererweiterung, wenn jedes $\alpha \in E$ algebraisch über K ist.

Bemerkung 4.6. Sei $\alpha \in E$ algebraisch über K.
Dann existiert genau ein normiertes Polynom $p \in K[x]$ kleinsten Grades mit $p(\alpha) = 0,\ p \neq 0$ (andernfalls wäre die Differenz zweier solcher Polynome ein Polynom $\neq 0$ kleineren Grades, welches α als Nullstelle besitzt).
Das Polynom ist irreduzibel in $K[x]$.
Es heißt definierendes Polynom von α über K oder Minimalpolynom von α über K und wird bezeichnet mit $\mathrm{Irr}(\alpha, K)$.
Besitzt $\mathrm{Irr}(\alpha, K)$ den Grad n, so heißt α algebraisch vom Grad n über K.

Bemerkung 4.7. Sei $\alpha \in E$ algebraisch über K, $f \in K[x],\ f \neq 0,\ f(\alpha) = 0$.
Dann gilt $\mathrm{Irr}(\alpha, K) | f$ in $K[x]$.
Also gilt: Ist $f(x) \in K[x]$ irreduzibel, $f(\alpha) = 0$ und $f(x)$ normiert, so ist $f(x) = \mathrm{Irr}(\alpha, K)$.

Beweis. Division von f durch $\mathrm{Irr}(\alpha, K)$ mit Rest liefert eine Gleichung der Form $f = q \cdot \mathrm{Irr}(\alpha, K) + r$ mit $r = 0$ oder grad $r <$ grad $\mathrm{Irr}(\alpha, K)$.
Der Einsetzungshomomorphismus liefert $r(\alpha) = 0$.
Es folgt $r = 0$.

Satz 4.8. Jede endliche Körpererweiterung $E : K$ ist algebraisch.
(Die Umkehrung ist falsch, siehe Übung.)

Beweis. Seien $[E : K] = n \in \mathbb{N}$ und $\alpha \in E$.
Dann sind $1, \alpha, \ldots \alpha^n$ linear abhängig über K.
Gelte $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$; $a_i \in K[x]$, nicht alle $a_i = 0$.
Dann ist α Nullstelle von $f(x) = a_0 + \cdots + a_n x^n \in K[x],\ f \neq 0$.

Satz 4.9. Seien $K \subseteq E$ Körper, $\alpha \in E$. Dann gilt:

$$\alpha \text{ transzendent über } K \Rightarrow K[\alpha] \cong K[x] \text{ (Polynomring über } K).$$

Beweis. Betrachte den Einsetzungshomomorphismus $\varphi_\alpha : K[x] \to K[\alpha]$ definiert durch $\varphi_\alpha(f) := f(\alpha)$.
Da α transzendent ist über K, folgt Ker $\varphi_\alpha = \{0\}$.
Ferner ist φ_α surjektiv.
Die Behauptung folgt nach dem Homomorphie-Satz für Ringe.

Satz 4.10. Seien $K \subseteq E$ Körper, $\alpha \in E$ algebraisch über K. Dann gilt:

1. $K[\alpha] \cong K[x]/(\mathrm{Irr}(\alpha, K)$.

2. Sei $n := \mathrm{grad}\ \mathrm{Irr}(\alpha, K)$.
   Dann ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Basis von $K[\alpha] : K$.
   (Speziell ist $K[\alpha] : K$ endlich.)

3. $K[\alpha] = K(\alpha)$. (Das heißt: $K[\alpha]$ ist ein Körper.)

Beweis.

1. Nach Bemerkung 4.7 ist $(\mathrm{Irr}(\alpha, K))$ der Kern des Einsetzungshomomorphismus φ_α, und nach dem Homomorphiesatz für Ringe folgt die Behauptung.

2. $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist linear unabhängig über K, denn aus $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$, $a_i \in K$, folgt für $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in K[x]$ die Gleichung $f(\alpha) = 0$ und wegen grad $f < n$ weiter $f = 0$; das heißt: $a_i = 0$ für alle i.
   $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist ein Erzeugenden-System des K-VR $K[\alpha]$:
   Sei $b_0 + \cdots + b_s\alpha^s \in K[\alpha]$ beliebig gegeben.
   Setze $f := b_0 + \cdots + b_s x^s$.
   Der Divisionsalgorithmus liefert eine Gleichung der Form
   $f = q \cdot \mathrm{Irr}(\alpha, K) + r$ mit $r = 0$ oder grad $r < n$.
   Der Einsetzungshomomorphismus liefert $f(\alpha) = r(\alpha)$.
   Es folgt die Behauptung, da $r(\alpha)$ Linearkombination der Elemente $1, \alpha, \ldots, \alpha^{n-1}$ mit Koeffizienten aus K ist.

3. Es werden drei Beweise geführt:

   (a) Nach Satz 4.4 und Teil 2.

   (b) $\mathrm{Irr}(\alpha, K)$ ist unzerlegbar in $K[x]$; $K[x]$ ist Euklidischer Ring, (Bemerkung 3.36) also auch Hauptidealring (Satz 3.37), also ist $(\mathrm{Irr}(\alpha, K))$ maximales Ideal in $K[x]$ (Satz 3.27).
   Dann ist $K[x]/(\mathrm{Irr}(\alpha, K))$ Körper (Satz 3.77) und nach Teil 1 folgt die Behauptung.

(c) (Konstruktive Berechnung der Inversen mit Hilfe des Euklidischen Algorithmus)
Sei $\beta \in K[\alpha],\ \beta \neq 0$, etwa $\beta = f(\alpha)$, $f \in K[\alpha]$, grad $f < n$ (nach Teil 2).
Es folgt $\mathrm{Irr}(\alpha, K) \nmid f$ und damit $1 = \mathrm{ggT}\{\mathrm{Irr}(\alpha, K), f\}$.
Mit Hilfe des Euklidischen Algorithmus berechne man $\lambda, \mu \in K[x]$ mit $f \cdot \mu + \mathrm{Irr}(\alpha, K) \cdot \lambda = 1$.
Der Einsetzungshomomorphismus für α liefert $f(\alpha) \cdot \mu(\alpha) = 1$.

Nach Satz 4.8 und Satz 4.10 folgt

Bemerkung 4.11. Seien $K \subseteq E$ Körper, $\alpha \in E$ algebraisch über K.
Dann ist $K[\alpha]$ algebraisch über K.

Bemerkung 4.12. Seien $K \subseteq S \subseteq E$ Körper, $\alpha \in E$ algebraisch über K.
Dann ist α algebraisch über S (klar nach Definition).

Bemerkung 4.13. Seien $K \subseteq S \subseteq E$ Körper, S algebraisch über K, $\alpha \in E$ algebraisch über S.
Dann ist α algebraisch über K.

Beweis. Sei α Nullstelle von $f = a_0 + \cdots + a_n x^n \in S[x]$.
Dann ist $K(a_0, \ldots, a_n) : K$ endlich, denn für alle i ist a_i algebraisch über $K(a_0, \ldots, a_{i-1})$ (nach Bemerkung 4.12), also $K(a_0, \ldots, a_i) : K(a_0, \ldots, a_{i-1})$ endlich (nach Satz 4.10) und damit auch $K(a_0, \ldots, a_n) : K$ endlich (nach Satz 4.1).
Ferner ist auch $K(a_0, \ldots, a_n, \alpha) : K(a_0, \ldots, a_n)$ endlich (Satz 4.10).
Dann ist auch $K(a_0, \ldots, a_n, \alpha) : K$ endlich (Satz 4.1), und nach Satz 4.8 folgt die Behauptung.

Satz 4.14. Seien $K \subseteq E$ Körper. Dann gilt:
$E : K$ endlich $\Leftrightarrow$ es existieren endlich viele über K algebraische Elemente $\alpha_1, \ldots, \alpha_n \in E$ mit $E = K(\alpha_1, \ldots, \alpha_n)$.

Beweis. $\Rightarrow$: Wähle α_i so daß $K \subsetneqq K(\alpha_1) \subsetneqq \ldots$.
Aufgrund der Körpergradformel erhält man nach endlich vielen Schritten E.
$\Leftarrow$: Es gilt: $K(\alpha_1) : K$ endlich, $K(\alpha_1\alpha_2) : K(\alpha_1)$ endlich, $\ldots$.
Die Behauptung folgt nach der Körpergradformel.

Bemerkung 4.15. Seien $K \subseteq E$ Körper.
Dann ist $A(K) := \{\alpha \in E | \alpha \text{ algebraisch über } K\}$ ein Körper (der algebraische Abschluß oder die algebraische Hülle von K in E).

Beweis. Seien $a, b \in A(K)$.
Dann ist $K(a, b) : K$ endlich (Satz 4.10), also auch algebraisch (Satz 3.54).
Es folgt $a \pm b \in A(K)$, $a \cdot b \in A(K)$ und $a^{-1} \in A(K)$, falls $a \neq 0$.

4.3 Konstruktionen mit Zirkel und Lineal

Untersucht werden soll das folgende Problem:
Es seien Punkte in der Ebene gegeben.
Welche neuen Punkte lassen sich daraus mit Zirkel und Lineal konstruieren?

Präzisierung der Problemstellung:
Sei P_0 eine Menge von gegebenen Punkten in der Ebene;
P_0 enthalte mindestens zwei Punkte.
Lege in der Ebene ein Cartesisches Koordinatensystem fest (also eine Orthonormalbasis B).
Identifiziere die Punkte der Ebene mit den zugehörigen Koordinaten, also mit den Elementen $(x, y) \in \mathbb{R}^2$.
Im allgemeinen legt man das Koordinatensystem so, daß $(0,0), (0,1)$ gegebene Punkte sind (das heißt: die Einheitsstrecke ist gegeben).

Es sind folgende Operationen erlaubt:

(L) Lineal: Ziehe durch zwei verschiedene Punkte von P_0 eine Gerade.

(Z) Zirkel: Ziehe um einen Punkt aus P_0 einen Kreis, wobei der Radius Abstand zweier Punkte aus P_0 ist.

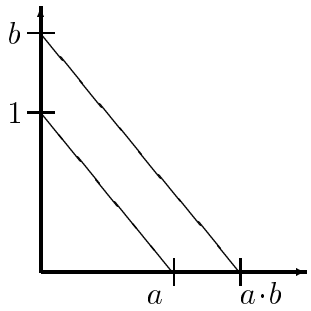
Die Schnittpunkte von Geraden und Kreisen, die man mit zwei Operationen erhalten kann, heißen im ersten Schritt aus P_0 konstruierbare Punkte.
Algebraisch lassen sich die Koordinaten dieser Punkte beschreiben als Lösungen gewisser Gleichungssysteme.
Ein Punkt $p \in \mathbb{R}^2$ heißt aus P_0 konstruierbar, falls es endlich viele Punkte $p_1, p_2, \ldots, p_n = p$ gibt, so daß p_i im ersten Schritt aus $P_0 \cup \{p_1, \ldots, p_{i-1}\}$ konstruierbar ist für $i = 1, \ldots, n$.
Ein Element $a \in \mathbb{R}$ heißt konstruierbar aus P_0, wenn der Punkt $(a, 0)$ konstruierbar ist.
Ein Element $a \in \mathbb{R}$ heißt konstruierbar, wenn der Punkt $(a, 0)$ aus $\{(0,0), (0,1)\}$ konstruierbar ist.

Bemerkung 4.16.

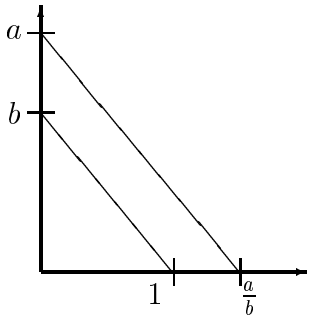
$$(a, b) \in \mathbb{R}^2 \text{ aus } P_0 \text{ konstruierbar } \Leftrightarrow a, b \text{ aus } P_0 \text{ konstruierbar}$$

Bemerkung 4.17. $a, b \in \mathbb{R}$ konstruierbar aus $P_0 \Rightarrow a + b,\ a \cdot b,\ \frac{a}{b}$ (für $b \neq 0$), $\sqrt{a}$ konstruierbar aus P_0.

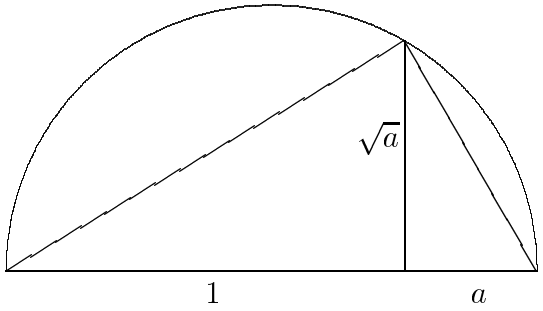
Beweis.



Die Konstruktion von $a \cdot b$ ergibt sich aus dem Strahlensatz.



Die Konstruktion von $\frac{a}{b}$ $(b \neq 0)$ ergibt sich ebenfalls aus dem Strahlensatz.



Die Konstruktion von $\sqrt{a}$ ergibt sich aus dem Höhensatz.

Satz 4.18. Sei $M \subseteq \mathbb{R}$, $1 \in M$, $\alpha \in \mathbb{R}$.

1. Dann sind alle Elemente aus dem Körper $\mathbb{Q}(M)$ aus M konstruierbar (nach Bemerkung 4.17).

2. α aus M konstruierbar $\Leftrightarrow$ Es existiert ein endlicher Körperturm $\mathbb{Q}(M) =: K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ mit $\alpha \in K_n$ und $[K_i : K_{i-1}] = 2$ für alle $i \in \{1, \ldots, n\}$.

Nach Satz 4.10 hat K_i die Form $K_i = K_{i-1}(\sqrt{\beta_{i-1}}),\ \beta_{i-1} \in K_{i-1}$.
K_i entsteht also durch Adjunktion der Nullstelle eines geeigneten quadratischen Polynoms mit Koeffizienten aus K_{i-1}.
Speziell: $\alpha \in \mathbb{R}$ Konstruierbar $\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}]$ ist Potenz von 2.
Die Umkehrung ist falsch (ohne Beweis).

Beweis.

1. Klar.

2. Schnittpunkte von Geraden und Kreisen haben Koordinaten, die Lösungen quadratischer oder linearer Gleichungen sind.

Beispiel 4.19. 1. Quadratur des Kreises
Gegeben sei ein Kreis mit dem Radius 1 (das heißt die beiden Punkte $(0,0),\ (0,1)$).
Aufgabe: Konstruiere ein Quadrat mit gleichem Flächeninhalt (mit Zirkel und Lineal).
Zur Lösung ist $\sqrt{\pi}$ zu konstruieren.
Dies ist jedoch unmöglich, da $\sqrt{\pi}$ transzendent über $\mathbb{Q}$ ist (ohne Beweis), also $[\mathbb{Q}(\sqrt{\pi}) : Q] = \infty$.

2. Delisches Problem
Gegeben sei ein Würfel mit der Kantenlänge 1.
Aufgabe: Konstruiere die Kantenlänge eines Würfels mit doppeltem Volumen (mit Zirkel und Lineal).
Zur Lösung ist $\sqrt[3]{2}$ zu konstruieren.
Dies ist jedoch unmöglich, da $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist (nach Satz 4.10).
Beachte, daß $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ ist nach dem Eisensteinkriterium.

3. Dreiteilung eines Winkels
Behauptung: Es sei eine Strecke der Länge 1 gegeben.
Dann läßt sich nicht jeder Winkel α mit Zirkel und Lineal in drei gleich große Winkel teilen.

Beweis. Sei ein Winkel 3α gegeben durch die Strecke der Länge $\cos(3\alpha)$.
Zeigen: Bei geeigneter Wahl von α läßt sich $\cos\alpha$ nicht konstruieren aus $\{1, \cos 3\alpha\}$.
Zunächst gilt nach der Formel von de Moivre: $\cos 3\alpha + i \sin 3\alpha = (\cos\alpha + i \sin\alpha)^3$.
Vergleich des Realteils liefert $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Für $\alpha = 20°$, also $\cos 3\alpha = \frac{1}{2}$, erhält man speziell $\frac{1}{2} = 4x^3 - 3x$ oder $8x^3 - 6x - 1 = 0$.
$8x^3 - 6x - 1 = 0$ ist irreduzibel, da das Polynom nach Satz 2.90 keine Nullstellen in $\mathbb{Q}$ besitzt. Also ist $[\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$ und $\cos 20°$ ist nicht konstruierbar.
(Also ist auch das regelmäßige 18-Eck nicht konstruierbar.)

4.4 Zerfällungskörper

Es seien $(K, +, \cdot)$ ein Körper, $f \in K[x]$.
Gesucht wird ein Körper $E \supseteq K$, über dem f in Linearfaktoren zerfällt.
Zunächst wird ein Körper $E \supseteq K$ gesucht, in dem f eine Nullstelle besitzt.

Vorbemerkung

Seien $E \supseteq K$ Körper, $\alpha \in E$ algebraisch über K.
Dann gilt (nach Satz 4.10):

$$K(\alpha) = K[\alpha] \cong K[x]/(\mathrm{Irr}(\alpha, K)).$$

Also ist $K[\alpha]/(\mathrm{Irr}(\alpha, K))$ ein Körper, welcher K enthält (bis auf Isomorphie), und in dem $\mathrm{Irr}(\alpha, K)$ eine Nullstelle besitzt.
Ferner ist $1, \alpha, \ldots, \alpha^{n-1}$ Basis von $K(\alpha) : K$, wobei $n := \mathrm{grad}\ \mathrm{Irr}(\alpha, K)$.

Satz 4.20. Seien $(K, +, \cdot)$ Körper, $p \in K[x]$ irreduzibel (speziell nicht konstant). Dann existiert eine Körpererweiterung $L : K$ mit $[L : K] = \mathrm{grad}\ p$, in der p eine Nullstelle besitzt.

Beweis.
Entsprechend der Vorbemerkung wird der Körper $K[x]/(p)$ betrachtet.
$\varphi : K \to K[x]/(p)$ definiert durch $\varphi(k) := k + (p)$ ist ein injektiver Homomorphismus.
$K[x]/(p)$ enthält also einen zu K isomorphen Teilkörper $\{k + (p) | k \in K\}$, welcher mit K identifiziert wird.
Dann besitzt p in $K[x]/(p)$ die Nullstelle $x + (p)$. Dies ergibt sich wie folgt:
Ersetzt man in $p(x) = \underbrace{a_0}_{=a_0+(p)} + \cdots + \underbrace{a_n}_{=a_n+(p)} x^n \in K[x]$ die Unbestimmte x durch das Element $x + (p) \in K[x]/(p)$, so erhält man das Element

$$(a_0+(p))+(a_1+(p))(x+(p))+\cdots+(a_n+(p))(x+(p))^n = {}^1p(x)+(p) = 0+(p),$$

[1] Beachte die Rechenregeln im Restklassenkörper $K[x]/(p)$; Multiplikation und Addition ist repräsentantenweise vorzunehmen.

also die Null in $K[x]/(p)$.
Ferner wird gezeigt:
$1 + (p), x + (p), \ldots, x^{n-1} + (p)$ ist eine Basis von $K[x]/(p) : K$, wobei $n := \text{grad } p(x)$. (Dies ergibt sich auch direkt aus Satz 4.10).
Die lineare Unabhängigkeit ergibt sich aus $a_0 + \cdots + a_{n-1}x^{n-1} \notin (p)$ für beliebige $a_i \in K$.
Sei $f + (p)$ ($f \in K[x]$) beliebig aus $K[x]/(p)$ gegeben.
Division von f durch p liefert nach dem Euklidischen Algorithmus eine Gleichung der Form $f = q \cdot p + r$ mit $r = 0$ oder grad $r <$ grad p.
Es folgt $f + (p) = r + (p)$ und $r + (p)$ ist Linearkombination der $1 + (p), \ldots, x^{n-1} + (p)$ mit Koeffizienten aus K.

Folgerung 4.21. Es seien $(K, +, \cdot)$ ein Körper und $f \in K[x]$ ein nicht konstantes Polynom.
Dann existiert eine Körpererweiterung E von K, über der f in Linearfaktoren zerfällt.

Beweis. Besitzt f eine Nullstelle in E, so läßt sich von f in $E[x]$ ein Linearfaktor abspalten (nach Satz 2.82).
Zum Beweis zerlege man f in ein Produkt irreduzibler Faktoren und wende Satz 4.20 wiederholt an.

Definition 4.22. Zerfällungskörper
Seien $(K, +, \cdot)$ Körper, $f \in K[x]$.
Eine Körpererweiterung E von K heißt Zerfällungskörper von f über K, wenn gilt:

1. Es existieren $\alpha \in K$, $\alpha_1, \ldots, \alpha_n \in E$ mit $f = \alpha(x - \alpha_1) \cdots (x - \alpha_n)$ (f zerfällt über E in Linearfaktoren).

2. $E = K(\alpha_1, \ldots, \alpha_n)$.

E ist also minimale Körpererweiterung von K, über der f in Linearfaktoren zerfällt.

Bemerkung 4.23. Ist $(K, +, \cdot)$ Körper und $f \in K[x]$, so existiert ein Zerfällungskörper von f über K.

Beispiel 4.24. $\mathbb{Q}(\sqrt{2})$ ist Zerfällungskörper von $x^2 - 2$ über $\mathbb{Q}$.

Zum Nachweis der Eindeutigkeit des Zerfällungskörpers (bis auf Isomorphie) brauchen wir

Satz 4.25. Seien $\varphi : K \to K_1$ ein Körperisomorphismus,
$\widetilde{\varphi} : K[x] \to K_1[x]$ definiert durch $\widetilde{\varphi}(a_0 + \cdots + a_n x^n) := \varphi(a_0) + \cdots + \varphi(a_n)x^n$ die kanonische Fortsetzung. Nach Bemerkung 2.79 (dann ist $\widetilde{\varphi}$ ebenfalls Isomorphismus) und $\widetilde{\varphi}(f) := f_1$.
Seien $f \in K[x]$ irreduzibel,
E Körpererweiterung von K, $\alpha \in E$ Nullstelle von f,
E_1 Körpererweiterung von K_1, $\alpha_1 \in E_1$ Nullstelle von f_1.
Dann läßt sich φ zu einem Isomorphismus

$$\varphi^* : K(\alpha) \to K_1(\alpha_1)$$

mit $\varphi^*(\alpha) = \alpha_1$ fortsetzen.

$$\boxed{\begin{array}{c} K \xrightarrow{\varphi} K_1 \\ K[x] \xrightarrow{\widetilde{\varphi}} K_1[x] \\ K(\alpha) \xrightarrow{\varphi^*} K_1(\alpha_1) \end{array}}$$

Beweis. Sei grad $f = n$.
Dann ist auch grad $f_1 = n$ und f_1 ist irreduzibel über K_1 (da $\widetilde{\varphi}$ Isomorphismus).
Nach Satz 4.10 gilt:

$$\left.\begin{array}{l} \{1, \ldots, \alpha^{n-1}\} \text{ Basis von } K(\alpha) : K; \\ \{1, \ldots, \alpha_1^{n-1}\} \text{ Basis von } K_1(\alpha_1) : K_1. \end{array}\right\} (*)$$

Definiere φ^* durch $\varphi^*(a_0 + \cdots + a_{n-1}\alpha^{n-1}) := \varphi(a_0) + \cdots + \varphi(a_{n-1})\alpha_1^{n-1}$.
Dann gilt

- φ^* ist bijektiv (nach $(*)$).
- φ^* setzt φ fort.
- $\varphi^*(\alpha) = \alpha_1$.
- φ^* ist relationstreu bezüglich $+$.
- φ^* ist relationstreu bezüglich $\cdot$.[2]

[2] Seien $g(\alpha), h(\alpha) \in K(\alpha)$; $g, h \in K[x]$ und sei $g \cdot h = q \cdot f + r$ nach dem Euklidischen Algorithmus.

$$\begin{array}{rrcl} \text{Dann gilt} & \varphi^*(g(\alpha) \cdot h(\alpha)) = & \varphi^*(r(\alpha)) & = r_1(\alpha_1) \text{ und} \\ & \varphi^*(g(\alpha)) \cdot \varphi^*(h(\alpha)) = & g_1(\alpha_1)g_1(\alpha_1) & = r_1(\alpha_1) \text{ wegen} \\ & g_1 \cdot h_1 = & q_1 \cdot f_1 + r_1 & \text{und } f_1(\alpha_1) = 0 \end{array}$$

Setzt man in Satz 4.25 speziell $\varphi = \mathrm{id}$, so erhält man

Folgerung 4.26. Seien $K \subseteq E$ Körper, $f \in K[x]$ irreduzibel und $\alpha_1, \alpha_2 \in E$ Nullstellen von f.
Dann ist $\varphi^* : K(\alpha_1) \to K(\alpha_2)$ definiert durch

$$\varphi^*(a_0 + \cdots + a_{n-1}\alpha_1^{n-1}) := a_0 + \cdots + a_{n-1}\alpha_2^{n-1}$$

ein Isomorphismus mit $\varphi(\alpha_1) = \alpha_2$.

Wiederholte Anwendung von Satz 4.25 liefert

Satz 4.27. Seien $\varphi : K \to K_1$ Körperisomorphismus, $\widetilde{\varphi} : K[x] \to K_1[x]$ die kanonische Fortsetzung, $f \in K[x]$, $f_1 := \widetilde{\varphi}(f)$,
L Zerfällungskörper von f über K,
L_1 Zerfällungskörper von f_1 über K_1.
Dann läßt sich φ zu einem Isomorphismus $\varphi^* : L \to L_1$ fortsetzen.
(Speziell erhält man für $\varphi = \mathrm{id}$, daß der Zerfällungskörper von $f(x) \in K[x]$ bis auf Isomorphie eindeutig ist.)

4.5 Endliche Körper

Satz 4.28. Sei $(K, +, \cdot)$ endlicher Körper (also Körper mit endlich vielen Elementen).
Dann ist $|K|$ Primzahlpotenz.

Beweis. Sei Char $K = p$. Dann ist p Primzahl (Bemerkung 2.10).
Dann ist $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ der Primkörper von K (das heißt: der von 1 erzeugte Unterkörper) bis auf Isomorphie.
Sei $[K : \mathbb{Z}_p] = n$.
Dann besitzt der $\mathbb{Z}_p$-VR K eine Basis mit n Elementen.
Jedes Element aus K läßt sich eindeutig darstellen als Linearkombination durch die n Basiselemente mit Koeffizienten aus $\mathbb{Z}_p$. Die Anzahl aller möglichen Linearkombinationen beträgt genau p^n; also gilt: $|K| = p^n$.

Satz 4.29. Sei $(K, +, \cdot)$ Körper und G eine endliche Untergruppe der multiplikativen Gruppe $(K \setminus \{0\}, \cdot)$ des Körpers.
Dann ist $(G, \cdot)$ zyklische Gruppe.
Speziell ist die multiplikative Gruppe eines endlichen Körpers stets zyklisch.

Zum Beweis wird gebraucht

Lemma 4.30. Sei $(G, \cdot)$ endliche abelsche Gruppe.

1. Dann existiert ein $g \in G$, für dessen Ordnung m gilt: $a^m = e$ für alle $a \in G$.

2. Ferner gilt: $m \leq |G|$ (nach dem Satz von Euler).

Beweis. (von Lemma 4.30)
Sei $g \in G$ ein Element mit maximaler Ordnung m.
Annahme: Es existiert ein $b \in G$, dessen Ordnung n nicht Teiler von m ist; etwa $m = p^r m'$, $n = p^s n'$, $\mathrm{ggT}(m', p) = \mathrm{ggT}(n', p) = 1$, $s > r$ für eine geeignete Primzahl p.
Dann besitzt g^{p^r} die Ordnung m' und $b^{n'}$ die Ordnung p^s (Satz 1.57); also $g^{p^r} b^{n'}$ besitzt die Ordnung $p^s m' > m$ (Satz 1.59). Dies ist ein Widerspruch zur maximalen Wahl von m.

Beweis. (von Satz 4.29)
Nach Lemma 4.30.1 existiert ein $g \in G$ der Ordnung m mit $a^m = 1$ für alle $a \in G$.
Dann ist jedes $a \in G$ Nullstelle von $x^m - 1 \in K[x]$. Es folgt $|G| \leq m$, da $x^m - 1$ höchstens m verschiedene Nullstellen besitzen kann, und nach Lemma 4.30.2 weiter $|G| = m$. Also erzeugt g die Gruppe G.

Satz 4.31. Seien $p \in \mathbb{N}$ Primzahl und $n \in \mathbb{N}$.

1. Bis auf Isomorphie existiert genau ein Körper $\mathrm{GF}(p^n)$ der Ordnung p^n (Galois-Field der Ordnung p^n).

2. Der Zerfällungskörper von $x^{p^n} - x \in \mathbb{Z}_p[x]$ ist ein Körper der Ordnung p^n.

Beweis.

2. Sei K Zerfällungskörper von $x^{p^n} - x \in \mathbb{Z}_p[x]$.
   Das Polynom $x^{p^n} - x$ besitzt keine mehrfache Nullstellen (Bemerkung 2.88).
   Seien $\alpha_1, \ldots, \alpha_{p^n}$ die Nullstellen von $x^{p^n} - x$ in K.
   Es genügt zu zeigen, daß die Nullstellen einen Körper bilden, der $\mathbb{Z}_p$ enthält.
   Nach dem Satz von Fermat ist jedes Element aus $\mathbb{Z}_p$ Nullstelle von $x^{p^n} - x$.
   Mit α ist auch $-\alpha$ Nullstelle von $x^{p^n} - x$. Dies ist klar für $p \neq 2$; im Fall $p = 2$ beachte man $\alpha = -\alpha$.
   Mit α_1, α_2 sind auch $\alpha_1 + \alpha_2$ und $\alpha_1 \cdot \alpha_2$ Nullstellen von $x^{p^n} - x$.
   Mit $\alpha (\neq 0)$ ist auch $\frac{1}{\alpha}$ Nullstelle von $x^{p^n} - x$.

1. Die Existenz folgt aus 2.
   Sei K Körper mit p^n Elementen.
   Dann ist der Primkörper von K isomorph zu $\mathbb{Z}_p$ (nach dem Beweis von Satz 4.28.
   Ferner ist jedes $a \in K$ Nullstelle von $x^{p^n} - x$, denn die multiplikative Gruppe von K hat offenbar die Ordnung $p^n - 1$.
   Also ist K Zerfällungskörper von $x^{p^n} - x \in \mathbb{Z}_p[x]$ und damit bis auf Isomorphie eindeutig.

Bemerkung 4.32. Sei K Körper der Ordnung p^n; $m \in \mathbb{N}$. Dann gilt:

$$K \text{ enthält einen Unterkörper der Ordnung } p^m \Leftrightarrow m|n.$$

Der Beweis wird dem Leser als Übung überlassen. Es wird nochmal auf den Satz von Wedderburn (Seite 37) hingewiesen.

4.6 Endliche Erweiterungen

Definition 4.33. Einfache algebraische Körpererweiterung, primitives Element

Sei $E : K$ eine Körpererweiterung.
$E : K$ heißt einfache Körpererweiterung, wenn ein $\alpha \in K$ existiert mit $K(\alpha) = E$.
$E : K$ heißt einfach, algebraische Körpererweiterung, wenn ein $\alpha \in E$ existiert mit $K(\alpha) = E$, und α algebraisch über K.
Gilt $E = K(\alpha)$, so heißt α primitives Element von $E : K$.

Interessant ist der folgende (in der Vorlesung aber nicht weiter benötigte)

Satz 4.34. Sei $E : K$ eine Körpererweiterung. Dann gilt:
$E : K$ einfach algebraisch $\Leftrightarrow$ Es existieren nur endlich viele Zwischenkörper L mit $K \subseteq L \subseteq E$.

Beweis. $\Leftarrow$:
Vorausgesetzt wird, daß nur endlich viele Zwischenkörper L existieren.
Dann ist $E : K$ algebraisch (ist nämlich $\alpha \in E$ transzendent über K, so gilt $K(\alpha) \supsetneqq K(\alpha^2) \supsetneqq K(\alpha^{2^2}) \supsetneqq K(\alpha^{2^3}) \supsetneqq \ldots$, da $K(\alpha^{2^n})$ genau alle Quotienten von Polynomen in α enthält, bei denen der Exponent von α stets Vielfaches von 2^n ist.
Betrachte einen Körperturm der Form

$$K \subsetneqq K(\alpha_1) \subsetneqq K(\alpha_1, \alpha_2) \subsetneqq \cdots \subsetneqq K(\alpha_1, \ldots, \alpha_r) = E \tag{4.1}$$

Ein solcher existiert, da nach Voraussetzung nur endlich viele Zwischenkörper existieren.
Dann ist $E : K$ endlich (nach der Körpergradformel auf Seite 81 und da jede einzelne Erweiterung endlich ist nach Satz 4.10).
Nun werden zwei Fälle unterschieden.
Ist K endlich, so ist auch E endlich, also die multiplikative Gruppe von E zyklisch, und ein erzeugendes Element ist offenbar primitives Element von $E : K$.
Sei nun K unendlich, und der Körperturm 4.1 so gewählt, daß r minimal ist.
Dann ist $r = 1$ zu zeigen.
Annahme: $r > 1$. Für $c \in K$ sei $\nu_c := \alpha_1 + c\alpha_2$.
Dann existieren $a, b \in K$ mit $K(\nu_a) = K(\nu_b)$, da $|K|$ unendlich und $E : K$ nur endlich viele Zwischenkörper besitzt. Es folgt $\nu_a - \nu_b = \underbrace{(a-b)}_{\in K}\alpha_2 \in K(\nu_a)$,
also $\alpha_2 \in K(\nu_a)$ und damit auch $\alpha_1 = \nu_a - a \cdot \alpha_2 \in K(\nu_a)$.
Dann gilt $K(\alpha_1, \alpha_2) \subseteq K(\nu_a)$ und $E = K(\nu_a, \alpha_3, \ldots, \alpha_r)$ im Widerspruch zur minimalen Wahl von r.
$\Rightarrow$: Sei $E : K$ einfach algebraisch; etwa $E = K(\alpha)$, α algebraisch über K, M ein Zwischenkörper ($K \subseteq M \subseteq E$) und $\mathrm{Irr}(\alpha, M) := m_0 + \cdots + m_r x^r \in M[x]$.
Zunächst wird gezeigt:

$$M = K(m_0, \ldots, m_r) \tag{4.2}$$

(also sind verschiedenen Zwischenkörpern M verschiedene $\mathrm{Irr}(\alpha, M)$ zugeordnet).
Es gilt: $K(m_0, \ldots, m_r) \subseteq M$.
Gezeigt wird: $K(m_0, \ldots, m_r) \supseteq M$:
$\mathrm{Irr}(\alpha, M)$ ist irreduzibel in $M[x]$, also erst recht in $K(m_0, \ldots, m_r)$.
Dann gilt: $[\underbrace{M(\alpha)}_{=E} : M] = \mathrm{grad}\,\mathrm{Irr}(\alpha, M) = [\underbrace{K(m_0, \ldots, m_r, \alpha)}_{=E} : K(m_0, \ldots, m_r)]$, also $M = K(m_0, \ldots, m_r)$.
Der Beweis ergibt sich nun wie folgt:
Es gilt $\mathrm{Irr}(\alpha, M) | \mathrm{Irr}(\alpha, K)$ in $M[x]$, also erst recht $\mathrm{Irr}(\alpha, M) | \mathrm{Irr}(\alpha, K)$ in $E[x]$.
Andererseits besitzt $\mathrm{Irr}(\alpha, K)$ in $E[x]$ nur endlich viele normierte Polynome als Teiler (man beachte, daß $E[x]$ ZPE-Ring ist).
Nach (4.2) folgt die Behauptung.

Definition 4.35. Sei $E : K$ eine Körpererweiterung, $\alpha \in E$ algebraisch über K.
Dann heißt α separabel über K, wenn $\mathrm{Irr}(\alpha, K)$ in seinem Zerfällungskörper nur einfache Nullstellen besitzt.

Ist $E : K$ endlich, so existieren endlich viele über K algebraische Elemente

$\alpha_1, \ldots, \alpha_n \in E$ mit $E = K(\alpha_1, \ldots, \alpha_n)$. Häufig kommt man aus mit der Adjunktion eines Elementes. Dies besagt

Satz 4.36. Satz vom primitiven Element
Sei $E : K$ eine Körpererweiterung.
Seien $\nu_1, \ldots, \nu_r \in E$ separabel über K mit $E = K(\nu_1, \ldots, \nu_r)$.
Dann existiert ein primitives Element $\nu \in E$ mit $E = K(\nu)$.

Beweis. Gezeigt wird: Ist α algebraisch über K, β separabel über K, so existiert ein $\nu \in K(\alpha, \beta)$ mit $K(\alpha, \beta) = K(\nu)$.
Wiederholte Anwendung liefert den Satz (man beachte, daß ν algebraisch über K ist, da $K(\nu) = K(\alpha, \beta)$ über K endlichen Grad besitzt.
Ist K endlich, so auch $K(\alpha, \beta)$ (nämlich $|K(\alpha, \beta)| = |K|^{[K(\alpha,\beta):K]}$) und man wähle für ν ein erzeugendes Element der multiplikativen Gruppe von $K(\alpha, \beta)$ nach Satz 4.29.
Sei nun K nicht endlich.
Ferner seien $p(x) := \mathrm{Irr}(\alpha, K), \quad q(x) := \mathrm{Irr}(\beta, K)$, $F \supseteq K(\alpha, \beta)$ ein Körper, in dem $p \cdot q$ in Linearfaktoren zerfällt (ein solcher existiert nach Bemerkung 4.23),
$p = (x - \alpha_1) \cdots (x - \alpha_r)$; $\alpha = \alpha_1$; $\alpha_i \in F$;
$q = (x - \beta_1) \cdots (x - \beta_l)$; $\beta = \beta_1$; $\beta_i \in F$ paarweise verschieden, da β separabel.
Betrachte die Gleichungen

$$\alpha + x\beta = \alpha_s + x\beta_t \tag{4.3}$$

für alle $1 \leq s \leq r$ und $1 < t \leq l$.
Dies sind endlich viele Gleichungen und jede Gleichung hat in K höchstens eine Lösung. Wegen $|K| = \infty$ existiert also ein $\xi \in K$, welches keine der Gleichungen (4.3) löst.
Gezeigt wird: $\nu := \alpha + \xi\beta$ ist ein primitives Element (der Beweis ist also konstruktiv).
Es gilt: $K(\nu) \subseteq K(\alpha, \beta)$.
Zum Beweis von $K(\nu) \supseteq K(\alpha, \beta)$ wird $\beta \in K(\nu)$ gezeigt (dann folgt auch $\alpha \in K(\nu)$).
Es gilt: $q(x),\ f(x) := p(\nu - \xi x) \in K(\nu)[x]$ zerfallen in $F[x]$ in Linearfaktoren. $q(x), f(x)$ haben beide β also Nullstelle, aber keine weitere gemeinsame Nullstellen (nach Wahl von ξ).
Also haben p, f in $F(x)$ den ggT $(x - \beta)$ (da β separabel über K ist).
Nach Bemerkung 4.7 folgt $\mathrm{Irr}(\beta, K(\nu))|q$, $\mathrm{Irr}(\beta, K(\nu))|f$ in $K(\nu)[x]$ und $\mathrm{Irr}(\beta, K(\nu)) = x - \beta$ und damit $\beta \in K(\nu)$.

Beachte: Im Beweis vom Satz vom primitiven Element kommt man ohne die Separabilitätsanforderung nicht aus. Hierfür gibt es Beispiele.

4.7 Normale und Separabele Erweiterungen

Definition 4.37. Sei $E : K$ Körpererweiterung.
E heist normal über K, wenn gilt:

1. $E : K$ algebraisch
2. Jedes irreduzible Polynom $f \in K[x]$, welches in E eine Nullstelle besitzt (also in $E[x]$ einen Linearfaktor besitzt), zerfällt in $E[x]$ bereits in Linearfaktoren.

Satz 4.38. Sei $E : K$ endliche Körpererweiterung. Dann gilt:

$$E : K \text{ normal} \Leftrightarrow E \text{ ist Zerfällungskörper eines } f \in K[x].$$

Beweis. $\Rightarrow$: Sei $E = K(\alpha_1, \ldots, \alpha_n)$; $\alpha_1, \ldots, \alpha_n$ algebraisch über K.
Nach Voraussetzung zerfällt $\mathrm{Irr}(\alpha_i, K)$ in $E[x]$ in Linearfaktoren für $i = 1, \ldots, n$. Also ist E Zerfällungskörper von $\prod_{i_1}^{n} \mathrm{Irr}(\alpha_i, K)$.
$\Leftarrow$: Sei E Zerfällungskörper von $f \in K[x]$.
Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f in E, also $E = K(\alpha_1, \ldots, \alpha_n)$.
Sei $g \in K[x]$ irreduzibel und $a \in E$ Nullstelle von g.
Sei F Zerfällungskörper von $g \in E[x]$.
Sei $b \in F$ Nullstelle von g.
Dann ist $b \in E$ zu zeigen.
Nach Folgerung 4.26 existiert ein Isomorphismus $\varphi : K(a) \to K(b)$ mit $\varphi(a) = b,\ \varphi_{|K} = \mathrm{id}$.
Es ist

$$\begin{array}{lcll} E(a) = E = K(a, \alpha_1, \ldots, \alpha_n) & & & \text{Zerfällungskörper von } f \text{ über } K(a), \\ E(b) & = & K(b, \alpha_1, \ldots, \alpha_n) & \text{Zerfällungskörper von } f \text{ über } K(b). \end{array}$$

Dann läßt sich φ fortsetzen zu einem Isomorphismus $\varphi^* : E \to E(b)$ (nach Satz 4.27).
Wegen $\varphi^*_{|K} = \mathrm{id}$ ist φ^* lineare Abbildung vom K-VR E in den K-VR $E(b)$, also VR-Isomorphismus.
Es folgt $[E : K] = [E(b) : K]$, da $E : K$ endlich ist als Zerfällungskörper.
Dann ist $E = E(b)$, also $b \in E$.

Bemerkung 4.39. Sei $E : K$ endliche Körpererweiterung.
Dann hat E die Form $E = K(\alpha_1, \ldots, \alpha_n)$; $\alpha_i \in E$ algebraisch über K.
Sei M Zerfällungskörper von $\prod_{i=1}^{n} \mathrm{Irr}(\alpha_i, K)$ über K.
Dann ist M eine normale Erweiterung von K mit $K \subseteq E \subseteq M$ und auch minimal mit dieser Eigenschaft.
M heißt normale Hülle von E über K.

Bemerkung 4.40. Seien $K \subseteq E \subseteq M$ Körper. Ist $M : K$ normal und endlich, so auch $M : E$ nach Satz 4.38.

Beispiel 4.41.

1. $\mathbb{Q}(\sqrt{a}) : \mathbb{Q}$ ist normal als Zerfällungskörper von $x^2 - a$, $a \in \mathbb{Q}$.

2. $\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}$ ist nicht normal ($\sqrt[3]{2}$ bezeichne die reelle 3-te Wurzel), denn $\mathbb{Q}(\sqrt[3]{2})$ enthält nur reelle Zahlen, also nicht alle Nullstellen des nach dem Eisensteinkriterium irreduziblen Polynoms $x^3 - 2 \in \mathbb{Q}[x]$.

Definition 4.42. Seien $(K, +, \cdot)$ Körper, $f \in K[x]$ irreduzibel, $g \in K[x]$.
f heißt separabel über K, wenn f in seinem Zerfällungskörper nur einfache Nullstellen besitzt.
g heißt separabel über K, wenn alle irreduziblen Faktoren von g in $K[x]$ separabel über K sind.
K heißt vollkommen, wenn jedes $f \in K[x]$ separabel über K ist.
$E : K$ heißt separable Körpererweiterung, wenn jedes $\alpha \in E$ separabel über K ist.

Bemerkung 4.43. Sei $E : K$ Körpererweiterung. Dann gilt:
α separabel über $K \Leftrightarrow \mathrm{Irr}(\alpha, K)$ separabel über $K \Leftrightarrow \alpha$ Nullstelle eines separablen Polynoms $f \in k[x]$
(ist α Nullstelle eines separablen Polynoms $f \in K[x]$, so gilt nach Bemerkung 4.7 $\mathrm{Irr}(\alpha, K) | f$ in $K[x]$ und $\mathrm{Irr}(\alpha, K)$ ist separabel).

Bemerkung 4.44. Sei $f \in K[x]$ irreduzibel. Dann gilt:

1. f separabel über $K \Leftrightarrow f' \neq 0$

2. Char $K = 0 \Rightarrow K$ vollkommen

3. f nicht separabel über $K \Rightarrow$ Char $K =: p \neq 0$ und die formale Ableitung f' von f ist das Nullpolynom (und damit Polynom in x^p).

Beweis.

1. $\Rightarrow$: Sei f separabel über K, α Nullstelle von f. Dann ist α einfache Nullstelle von f. Nach Bemerkung 2.88 ist dann $f'(\alpha) \neq 0$ und damit $f' \neq 0$.
   $\Leftarrow$: Sei $f' \neq 0$ und α Nullstelle von f. Dann ist $f'(\alpha) \neq 0$ nach Bemerkung 4.7. (Sonst würde $f | f'$ gelten. Das ist aber wegen grad f' < grad f nicht möglich.) Also ist α einfache Nullstelle von f nach Bemerkung 2.88.

2. Ist Char $K = 0$ und f nicht konstantes Polynom, so ist die formale Ableitung f' von f nicht das Nullpolynom, also folgt nach 1. die Behauptung.

3. Folgt aus 1. und 2.

4.8 Galoistheorie im Überblick

In diesem Paragraphen werden die Hauptergebnisse der Galoistheorie skizziert. Auf Beweise wird weitgehend verzichtet.

Bemerkung 4.45. Galoisgruppe
Sei $L : K$ eine Körpererweiterung. Dann bilden die Automorphismen von L, die K elementenweise festlassen eine Gruppe. Diese wird mit $\mathrm{G}(L : K)$ oder $\mathrm{Gal}(L : K)$ bezeichnet und heißt Galoisgruppe von $L : K$.

Satz 4.46. Sei $L : K$ eine endliche Körpererweiterung. Dann gilt:

$$|\mathrm{Gal}(L : K)| \leq [L : K].$$

Die Aussage ist klar, falls $L : K$ separabel ist. Nach dem Satz vom primitiven Element existiert dann ein $\nu \in L$ mit $L = K(\nu)$, und ein Automorphismus aus $\mathrm{Gal}(L : K)$ bildet ν wieder ab auf eine Nullstelle von $\mathrm{Irr}(\nu, K)$ und durch das Bild von ν ist der Automorphismus bereits festgelegt.

Definition 4.47. Galoissche Erweiterung
Sei $L : K$ eine endliche Körpererweiterung.
$L : K$ heißt galoissche Erweiterung, falls $|\mathrm{Gal}(L : K)| = [L : K]$.

Bemerkung 4.48. Fixpunktkörper
Sei U eine Untergruppe von $\mathrm{Gal}(L : K)$. Dann ist

$$F := \{\alpha \in L | f(\alpha) = \alpha \text{ für alle } f \in U\}$$

ein Zwischenkörper von $L : K$. Er heißt Fixpunktkörper von U.

Satz 4.49. Sei $L : K$ endliche Körpererweiterung. Dann sind äquivalent:

1. $L : K$ ist galoissche Erweiterung

2. K ist der Fixpunktkörper von $\mathrm{Gal}(L : K)$

3. $L : K$ ist normal und separabel

4. L ist Zerfällungskörper eines über K separablen Polynoms $f(x) \in K[x]$.

Folgerung 4.50. Ist $L : K$ galoissche Körpererweiterung und M ein Zwischenkörper.
Dann ist auch $L : M$ galoissche Körpererweiterung.

Sei nun $L : K$ endliche, galoissche Körpererweiterung.
Das Hauptziel dieses Paragraphen besteht darin eine bijektive Korrespondenz zwischen den Untergruppen von $\mathrm{G}(L : K)$ und den Zwischenkörpern von $L : K$ herzuleiten.
Sei $M_Z := \{Z \text{ Körper } | K \subseteq Z \subseteq L\}$ die Menge der Zwischenkörper von $L : K$;
$M_U := \{U | U \text{ Untergruppe von } \mathrm{G}(L : K)\}$ die Menge der Untergruppen von $\mathrm{G}(L : K)$;
$\phi_{Z,U} : M_Z \to M_U$ ordne jedem Zwischenkörper Z die Untergruppe $\mathrm{G}(L : Z)$ von $\mathrm{G}(L : K)$ zu;
$\phi_{U,Z} : M_U \to M_Z$ ordne jeder Untergruppe U den Fixpunktkörper $\{a \in L | \sigma(a) = a \text{ für alle } \sigma \in U\}$ von U zu.
Das Hauptergebnis des nächsten Satzes besagt, daß $\phi_{Z,U}$ und $\phi_{U,Z}$ bijektiv und zueinander invers sind.
Einen Überblick gibt das folgende Schema:

$$\begin{array}{ccccc} L & \longleftrightarrow & \{e\} & & \\ | & & | & & \\ \text{Fixpunktkörper von } Z & \longleftrightarrow & U = \mathrm{G}(L : Z) & & \text{(Galoiskorrespondenz)} \\ | & & | & & \\ K & \longleftrightarrow & \mathrm{G}(L : K) & & \end{array}$$

$\phi_{Z,U} : M_Z \to M_U$, $z \mapsto \mathrm{G}(L : Z)$
$\phi_{U,Z} : M_U \to M_Z$, $u \mapsto$Fixpunktkörper von U.

Satz 4.51. Hauptsatz der Galoistheorie
Mit den obigen Voraussetzungen und Bezeichnungen gilt:

1. $\phi_{U,Z} : M_U \to M_Z$ und $\phi_{Z,U} : M_Z \to M_U$ sind bijektiv und zueinander invers.
   Das heißt:

   (a) Ist $Z \in M_Z$ Zwischenkörper von $L : K$, so ist Z Fixpunktkörper von $\mathrm{G}(L : Z) \in M_U$.

   (b) Ist $U \in M_U$ Untergruppe von $\mathrm{G}(L : K)$ und F der Fixpunktkörper von U, so ist $U = \mathrm{G}(L : F)$.

2. Sind $U_1, U_2 \in M_U$ zwei Untergruppen von $\mathrm{G}(L : K)$ und F_1, F_2 die zugehörigen Fixpunktkörper, so gilt:

$$U_1 \subseteq U_2 \Leftrightarrow F_2 \subseteq F_1.$$

3. Sei $U \in M_U$ eine Untergruppe von $\mathrm{G}(L : K)$ und F der zugehörige Fixpunktkörper. Dann gilt:

$$[L : F] = |U|$$
$$[F : K] = [\mathrm{G}(L : K) : U]$$

4. Sei $U \in M_U$ eine Untergruppe von $\mathrm{G}(L : K)$ und F der zugehörige Fixpunktkörper; $\sigma \in \mathrm{G}(L : K)$.
Dann besitzt $\sigma U \sigma^{-1}$ den Fixpunktkörper $\sigma(F)$.
Das heißt: $(U \leftrightarrow F) \Rightarrow (\sigma U \sigma^{-1} \leftrightarrow \sigma(F))$.

5. Sei $U \in M_U$ eine Untergruppe von $\mathrm{G}(L : K)$ und F der zugehörige Fixpunktkörper. Dann gilt:

   (a) U Normalteiler in $\mathrm{G}(L : K) \Leftrightarrow F : K$ galoissch

   (b) U Normaltieler in $\mathrm{G}(L : K) \Rightarrow \mathrm{G}(F : K) \cong \mathrm{G}(L : K)/\mathrm{G}(L : F)$
   (Beachte $\mathrm{G}(L : F) = U$ nach 5a.)

Mit Hilfe der Galoistheorie läßt sich allgemein die Frage beantworten, wann die Nullstellen eines Polynoms durch „Wurzeln" ausgedrückt werden können. Für quadratische Polynome ist dies möglich nach der bekannten Formel von Vieta ($p - q$-Formel), für kubische nach der Formel von Cardano.
Seit der Mitte des 16. Jahrhunderts kennt man auch eine Formel für Polynome 4. Grades. Nach einer Formel für Polynome vom Grad>4 hat man lange gesucht. 1826 bewies Abel, daß es solche Formeln nicht geben kann.
Zur genauen Beschreibung werden zwei weitere Begriffe benötigt, nämlich den der „Radikalerweiterung" und der „auflösbaren Gruppe".

Definition 4.52. Reine Radikalerweiterung, Radikalerweiterung
Sei $E : K$ Körpererweiterung.

1. $E : K$ reine Radikalerweiterung:$\Leftrightarrow E$ hat die Form $E = K(b)$, wobei b Nullstelle eines $f(x) = x^n - a \in K[x]$ ist.
   Das heißt: E entsteht aus K durch Adjunktion einer n-ten Wurzel eines Elementes $a \in K$;
   die Elemente aus E haben die Form

$$k_0 + k_1 \sqrt[n]{a} + \cdots + k_{n-1} \sqrt[n]{a}^{n-1}, \ k_i \in K.$$

2. $E : K$ Radikalerweiterung:$\Leftrightarrow$ Es existiert eine endliche Körperkette $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = E$.
   wobei $K_{i+1} : K$ reine Radikalerweiterung ist für alle i.
   Das heißt: Die Elemente aus E lassen sich durch „verschachtelte Wurzelausdrücke" von Elementen aus K darstellen.

Definition 4.53. Durch Radikale Auflösbar
Seien $(K, +, \cdot)$ Körper, $f \in K[x]$.
f heißt durch Radikale auflösbar, wenn der Zerfällungskörper von f über K in einer Radikalerweiterung von K enthalten ist.
Das heißt: Die Nullstellen von f lassen sich durch „verschachtelte Wurzelausdrücke" von Elementen aus K darstellen.

Definition 4.54. Auflösbar
Sei $(G, \cdot)$ eine Gruppe.
G heißt auflösbar, wenn Untergruppen $N_0, \ldots, N_l$ von G existieren, so daß gilt:

1. $G = N_0 \supseteq \cdots \supseteq N_l = \{e\}$,
2. N_i ist Normalteiler in $Ni - 1$ und N_{i-1}/N_i ist abelsche Gruppe für $i = 1, \ldots, l$.

Satz 4.55. Sei $(K, +, \cdot)$ Körper mit Char $K = 0$, $f \in K[x]$ und E Zerfällungskörper von f über K. Dann gilt:
f ist über K durch Radikale auflösbar$\Leftrightarrow$ Gal$(E : K)$ ist auflösbar.

Bemerkung 4.56. Sei E Zerfällungskörper von $f \in K[x]$,
seien $\alpha_1, \ldots \alpha_n$ die Nullstellen von f in E, also $E = K(\alpha_1, \ldots \alpha_n)$.
Jedes $\sigma \in$ Gal$(E : K)$ permutiert die Nullstellen von f (da σ Homomorphismus), und σ ist durch diese Permutation bereits festgelegt.
Also ist Gal$(E : K)$ isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

Bemerkung 4.57. Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.
Für $n \leq 4$ ist S_n auflösbar, also ist jedes Polynom $f \in K[x]$ vom Grad$\leq$ durch Radikale auflösbar, falls Char $K = 0$.
Für $n \geq 5$ ist S_n nicht auflösbar.
Es gibt Polynome von Grad 5 (zum Beispiel $x^5 - 6x^3 + 3$), deren Galoisgruppe isomorph ist zu S_5. Diese sind dann nicht durch Radikale auflösbar.

Index

Literaturverzeichnis

[1] Jacobsen: Basic Algebra I und II, W.H. Freeman and Company San Francisco

[2] Hornfeck, Algebra, Walter de Gruyter & Co Berlin 1969

[3] Meyberg

[4] Lidl & Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge 1994

[5] Scheja & Storch: Lehrbuch der Algebra, B.G.Teubner Stuttgart 1994

[6] Oberschelp: Aufbau des Zahlensystems.

[7] Jürgen Wolfart: Zahlentheorie und Algebra, Vieweg 1996

[8] Ivan Niven, H. S. Zuckerman: An Introduction to the Theory of Numbers, Wiley 1980

[9] E. Artin: Algebra

[10] M. Artin: Algebra

[11] Kunz: Algebra

[12] P. M. Cohn: Algebra I und II