Skript zur Vorlesung

Einführung in die Algebra und Zahlentheorie II

im Rahmen der Lehrerweiterbildung

Dozent: V.Schulze

FU Berlin Sommer 2020

Einführung in die Algebra und Zahlentheorie II

Inhaltsverzeichnis

(Seitenzahl in Klammern)

Kap. 1 Gruppen

Kap. 2 Ringe

Kap. 3 Ganzzahlige Kongruenzen

Kap. 4 Polynome

Kap. 5 Körper

Literatur

Ergänzende und vertiefende Literatur zur Vorlesung:

V. Schulze ; Skript Algebra und Zahlentheorie

J. Wolfart ; Zahlentheorie und Algebra

K. Meyberg ; Algebra

M. Artin ; Algebra

Anmerkung: In den 4 aufgeführten Texten ist der Stoff umfangreicher und weniger ausführlich dargestellt als im vorliegenden Skript.

Das Skript ist gedacht als Begleittext zu einer Vorlesung 'Einführung in die Algebra und Zahlentheorie II' im Rahmen der Lehrerweiterbildung im Umfang von ca. 18 Doppelstunden.

Kap. 1 Gruppen

§1 Grundlagen

Im Skript wird nur sehr wenig als bekannt vorausgesetzt. Zunächst werden einige wichtige und häufig verwendete Grundlagen dargestellt.
Wie allgemein in der Mathematik üblich werden folgende Bezeichnungen verwendet:

$\mathbb{N} := \{1, 2, 3, \ldots\}$ Menge der natürlichen Zahlen,
$\mathbb{Z} := \{0, 1, -1, 2, -2, \ldots\}$ Menge der ganzen Zahlen,
$\mathbb{Q} := \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$ Menge der rationalen Zahlen,
$\mathbb{R} :=$ Menge der reellen Zahlen.
$\emptyset$ = Leere Menge; $|M|$ = Anzahl der Elemente der endlichen Menge M.

Def 1.1 (Relationen)
Seien X, Y zwei nichtleere Mengen.
$X \times Y := \{(x, y) \mid x \in X, y \in Y\}$ heißt Cartesisches Produkt von X und Y.

Eine Teilmenge R von $X \times Y$ heißt Relation zwischen X und Y; im Fall $X = Y$ auch Relation auf X.

Übliche Schreibweise für $(x, y) \in R$: $x \sim y$ oder $x \overset{R}{\sim} y$.
Für R schreibt man häufig auch $\sim$.
Für $(x, y) \notin R$ wird auch $x \not\sim y$ geschrieben.

Bsp 1.1

Sei P eine Menge von Personen
und V eine Menge von Vereinen.
Dann ist $R := \{(p,v) \mid p \in P \text{ ist Mitglied im Verein } v \in V\} \subseteq P \times V$
eine Relation zwischen P und V.

Bsp 1.2.
Auf $\mathbb{Z}$ wird eine Relation $\sim$ definiert durch

$$a \sim b :\Leftrightarrow a-b \text{ ist Vielfaches von } 3 \text{ in } \mathbb{Z}.$$

Zum Beispiel gilt $3 \sim 15$ oder $3 \sim -21$, $5 \sim 2$
aber $5 \not\sim -2$.

Bsp 1.3. Auf $\mathbb{Z}$ wird eine Relation definiert durch

$$R := \{(1,2), (2,2)\}$$

(d.h. es gilt $1 \sim 2$ und $2 \sim 2$).

Der Begriff der Relation ist sehr allgemein.
Von besonderem Interesse sind Relationen, die gewisse
Zusatzeigenschaften besitzen.

Def 1.2 (Äquivalenzrelation)
Sei $\sim$ eine Relation auf der Menge X. Dann:

$\sim$ heißt Äquivalenzrelation $:\Leftrightarrow$ (i) $x \sim x$ für alle $x \in X$ (Reflexivität)
(ii) $x \sim y \Rightarrow y \sim x$ (Symmetrie)
(iii) $x \sim y, y \sim z \Rightarrow x \sim z$ (Transitivität).

Bem. 1.1

(i) In Beispiel 1.2 ist $\sim$ eine Äquivalenzrelation. (Bew. als Übung)

(ii) In Beispiel 1.3 ist R keine Äquivalenzrelation;

z.B. gilt $(1,2) \in R$, $(2,1) \notin R$; also ist R nicht symmetrisch;

$(1,1) \notin R$; also ist R nicht reflexiv;

R ist aber transitiv (es gilt $1 \sim 2, 2 \sim 2 \Rightarrow 1 \sim 2$

und $2 \sim 2, 2 \sim 2 \Rightarrow 2 \sim 2$)

Bem. 1.2 (Äquivalenzrelationen und Partitionen)

Es sei $\sim$ eine Äquivalenzralation auf X und $a \in X$. Dann:

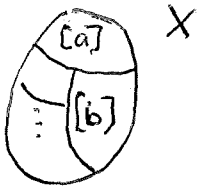
$[a] := \{x \in X \mid a \sim x\}$ hißt die von a erzeugte Äquivalenzklasse.

$[a]$ enthäll also alle Elemente aus X, die in Relation zu a stehen.

(i) Stets gilt $a \in [a]$, da $\sim$ als Äquivalenzrelation reflexiv ist.

Bekanntlich gilt:
Zwei Äquivalenzklassen sind gleich oder elementefremd.

Zusammen folgt:
Die Äquivalenzklassen von $\sim$ bilden eine Partition von X.
(dh: Die Vereinigung aller Äquivalenzklassen von $\sim$ ist X,
der Durchschnitt zweier verschiedener Äquivalenzklassen ist leer.)



(ii) Jede Partition von X definiert (auf natürliche Weise) eine Äquivalenzrelation auf X; genauer:
Sei P eine Partition von X (dh. P ist eine Menge von Teilmengen von X; die Vereinigung all dieser Teilmengen ist X und der Durchschnitt zweier verschiedener Teilmengen ist leer.
Dann wird eine Äquivalenzrelation auf X definiert durch

$x \sim y :\Leftrightarrow$ x und y liegen in derselben Teilmenge aus P.

Def. 1.3 (Abbildungen)

(i) Seien A, B nichtleere Mengen.

Eine Abbildung $f: A \to B$ ist eine Vorschrift, die jedem $a \in A$ genau ein $b \in B$ als Bild zuordnet.
Schreibweise: $f(a) = b$ oder $a \overset{f}{\mapsto} b$
Übersetzt man diese umgangssprachliche Formulierung in die Sprache der Mengenlehre, so erhält man:

Eine Abbildung $f: A \to B$ ist eine Relation $f \subseteq A \times B$ mit der Eigenschaft:

Zu jedem $a \in A$ existiert genau ein $b \in B$ mit $(a, b) \in f$.

(ii) $f: A \to B$ heißt injektiv, wenn gilt:

$$a \neq b \Rightarrow f(a) \neq f(b)$$

oder gleichwertig: $f(a) = f(b) \Rightarrow a = b$

In Worten: Verschiedene Elemente aus A besitzen verschiedene Bilder.
oder: Ein $b \in B$ tritt als Bild von höchstens einem $a \in A$ auf.

(iii) $f: A \to B$ heißt surjektiv, wenn gilt:

Zu jedem $b \in B$ existiert mindestens ein $a \in A$ mit $f(a) = b$.

In Worten: Jedes $b \in B$ tritt als Bild auf von mindestens einem $a \in A$.

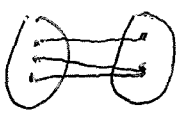
(iii') $f: A \to B$ heißt bijektiv, wenn $f: A \to B$ injektiv und surjektiv ist.

Für $f: A \to B$ schreibt man auch $A \overset{f}{\longrightarrow} B$.

(iv) Zwei Abbildungen $f: A \to B$ und $g: C \to D$ heißen gleich, wenn gilt $A = C, B = D$ und $f(a) = g(a)$ f.a. $a \in A$.

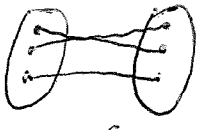
Beispiel 1.4

(i) $A \overset{f}{\to} B$ surjektiv, nicht injektiv

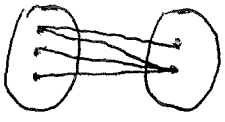


(ii) $A \overset{f}{\to} B$ injektiv, nicht surjektiv

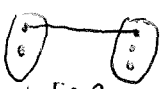
(iii) $A \overset{f}{\to} B$ bijektiv



(iv) $A \to B$ Keine Abbildung (ein Element darf nicht 2 Bilder haben)



(v) $A \overset{f}{\to} B$ Keine Abbildung (jedes Element muß ein Bild besitzen)



Bem 1.3 Ist $f: A \to B$ bijektiv, so existiert die Umkehrabbildung $f^{-1}: B \to A$, die ebenfalls bijektiv ist.

§2 Verknüpfungen

Def 2.1

(i) Es sei X eine nichtleere Menge.
Eine Abbildung $\circ : X \times X \to X$ heißt (innere) Verknüpfung $\circ$ auf X.
Das Bild von (x_1, x_2) bezüglich $\circ$ wird i.a. mit $x_1 \circ x_2$ bezeichnet.
$x_1 \circ x_2$ heißt Verknüpfungsergebnis von x_1 und x_2.
In Worten: Jedem Paar von Elementen aus X wird durch $\circ$ ein eindeutig bestimmtes Element aus X als Verknüpfungsergebnis zugeordnet.
Man beachte speziell: Das Verknüpfungsergebnis muß wieder in X liegen.

(ii) Seien X, Y zwei verschiedene nichtleere Mengen.
Eine Abbildung $\circ : Y \times X \to X$ heißt äußere Verknüpfung von X.

(iii) Eine Verknüpfung $\circ$ auf X heißt assoziativ, wenn gilt:
$(x_1 \circ x_2) \circ x_3 = x_1 \circ (x_2 \circ x_3)$ für alle $x_1, x_2, x_3 \in X$.

(iv) Eine Verknüpfung $\circ$ auf X heißt kommutativ, wenn gilt:
$x_1 \circ x_2 = x_2 \circ x_1$ für alle $x_1, x_2 \in X$.

Bem 2.1

Ist $\circ$ eine assoziative Verknüpfung auf X und $x_1, \dots, x_n \in X, n \geq 3$; so nimmt $x_1 \circ \dots \circ x_n$ bei jeder Beklammerung denselben Wert an (Beweis durch vollständige Induktion nach n).

Bsp 2.1

(i) Die übliche Addition $+$ definiert eine Verknüpfung auf $\mathbb{Z}$:
$(a,b) \longrightarrow a+b$.
Analog gilt dies für die Multiplikation.
Analog gilt dies natürlich auch, wenn $\mathbb{Z}$ ersetzt wird durch $\mathbb{N}$, $\mathbb{Q}$ oder $\mathbb{R}$.

(ii) Die Verknüpfung $\circ$ auf $\mathbb{N}$ sei def. durch $a \circ b = 1$ für alle $a, b \in \mathbb{N}$.
$\circ$ ist assoziativ und kommutativ.

(iii) Sei $M = \{a, b\}$ und die Verknüpfung $+$ auf M definiert durch
$a+a = b$, $a+b = a$, $b+a = a$, $b+b = b$.
Dann ist $+$ kommutativ und assoziativ.

Bem 2.2

Sei $M = \{a_1, \dots, a_n\}$ eine endliche Menge und $\circ$ eine Verknüpfung auf M.
Dann lassen sich die Verknüpfungsergebnisse übersichtlich darstellen in der sog. Verknüpfungstafel

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

Bsp 2.2 Zum Beispiel ist die Verknüpfungstafel von $\circ$ in Bsp 2.1 (iii)

$+$	a	b
a	b	a
b	a	b

Auf $M = \{a, b\}$ lassen sich insgesamt 2^4 verschiedene Verknüpfungen definieren; an jeder der 4 "Stellen" der Verknüpfungstafel gibt es 2 Möglichkeiten.

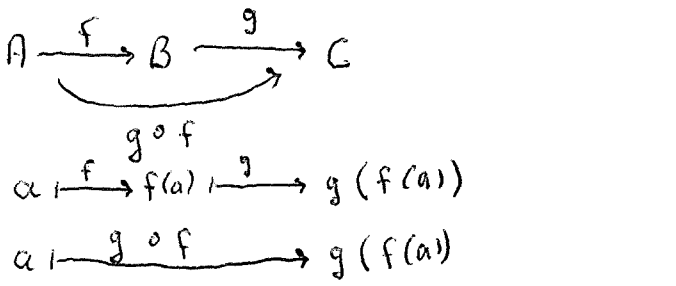
Bem 2.3 (Hintereinanderschaltung von Abbildungen)

(i) Gegeben seien die drei Abbildungen

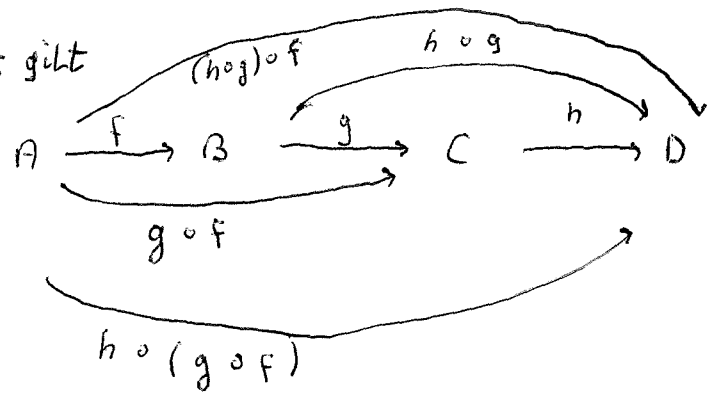
$$f: A \to B, \quad g: B \to C \text{ und } h: C \to D.$$

Dann ist die Abbildung $g \circ f: A \to C$ definiert durch

$$g \circ f(a) := g(f(a)).$$



(ii) Es gilt



und $(h \circ g) \circ f(a) = h \circ g(f(a)) = h(g(f(a)))$,

$h \circ (g \circ f)(a) = h(g \circ f(a)) = h(g(f(a)))$.

Also ist $(h \circ g) \circ f = h \circ (g \circ f)$

(iii) Sei A eine nichtleere Menge und F die Menge aller Abbildungen von A nach A.

Dann wird auf F eine Verknüpfung $\circ$ definiert durch die Hintereinanderschaltung von Abbildungen.

Nach (i) gilt

$$(h \circ g) \circ f = h \circ (g \circ f),$$

die Verknüpfung $\circ$ ist also assoziativ.

§3 Halbgruppen und Gruppen

Def. 3.1 Es sei A eine nichtleere Menge,
seien $o_1, \dots, o_n$ Verknüpfungen auf A $(n \geq 1)$.
Dann heißt $(A, o_1, \dots, o_n)$ algebraische Struktur.

Der Begriff der Verknüpfung ist sehr allgemein.
In der Regel werden in der Mathematik Verknüpfungen betrachtet, die gewisse Zusatzeigenschaften besitzen.

Def. 3.2 (Halbgruppe)
Es sei H eine nichtleere Menge und $\circ$ eine assoziative Verknüpfung auf H.
Dann heißt $(H, \circ)$ Halbgruppe

Bsp 3.1 $(\mathbb{N}, +), (\mathbb{Z}, \cdot), (\mathbb{Z}, +), (\mathbb{R}, \cdot)$ sind Beispiele für Halbgruppen.

Def. 3.3 (Gruppe)
Es sei $(G, \circ)$ eine Halbgruppe.
Dann heißt $(G, \circ)$ Gruppe, wenn gilt:
(i) Es existiert ein Element $e \in G$ mit $e \circ g = g \circ e = g$ für alle $g \in G$.
(ii) Zu jedem $g \in G$ existiert ein Element $g^{-1} \in G$ mit
$$g^{-1} \circ g = g \circ g^{-1} = e.$$
e heißt neutrales Element der Gruppe $(G, \circ)$
g^{-1} heißt das zu g inverse Element (die Bezeichnung ist sinnvoll, denn wir werden noch sehen: g^{-1} ist eindeutig bestimmt).
$(G, \circ)$ heißt kommutative (oder abelsche) Gruppe, wenn $\circ$ kommutativ ist.

Bem 3.1

(i) Wird die Verknüpfung der Gruppe mit + bezeichnet, so wird das neutrale Element in der Regel mit 0 bezeichnet und das zu g inverse Element mit $-g$.

(ii) Wird die Verknüpfung der Gruppe mit $\cdot$ bezeichnet, so wird das neutrale Element in der Regel mit 1 bezeichnet und das zu g inverse Element auch mit $\frac{1}{g}$.

Bem 3.2 (ohne Beweis)

Es gibt unterschiedliche Möglichkeiten Gruppen zu definieren, auch in der Literatur wird dies unterschiedlich gemacht.

Es gilt:

Die folgenden Aussagen sind äquivalent:

(i) $(G,\circ)$ ist eine Gruppe (im Sinne von Def. 3.3)

(ii) $(G,\circ)$ ist Halbgruppe und es gilt:

(a) Es existiert ein $e \in G$ mit $e \circ g = g$ für alle $g \in G$ (e heißt Linksneutrales Element)

(b) Zu jedem $g \in G$ existiert ein $\tilde{g}^{-1} \in G$ mit $\tilde{g}^{-1} \circ g = e$ ($\tilde{g}^{-1}$ heißt linksinverses Element von G).

(In (a) und (b) kann "links" auch durch "rechts" ersetzt werden; aber es darf nicht "gemischt" werden (s. Aufgabe 3 in den Übungen)

(iii) $(G,\circ)$ ist eine Halbgruppe und es gilt:

(a) Für $a,b \in G$ ist $x \circ a = b$ stets lösbar; d.h. es existiert ein $x_0 \in G$ mit $x_0 \circ a = b$.

(b) Für $a,b \in G$ ist $a \circ x = b$ stets lösbar; d.h. es existiert ein $x_0 \in G$ mit $a \circ x_0 = b$.

Beispiel 3.1

Beispiele für Gruppen sind $(\mathbb{Z},+), (\mathbb{R},+), (\mathbb{Q},+)$.

Keine Gruppen sind $(\mathbb{Q},\cdot), (\mathbb{R},\cdot)$ (hier ist 1 neutrales Element, aber 0 besitzt kein Inverses)

$(\mathbb{N},+)$, $(\mathbb{Z},\cdot)$ sind keine Gruppen.

$(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ sind Gruppen.

Bem 3.3

Es sei $(G,\circ)$ eine Gruppe. Dann gilt:

(i) Das neutrale Element e der Gruppe ist eindeutig bestimmt.

(ii) Seien $a,b \in G$ gegeben.

Dann ist $x \circ a = b$ in G eindeutig lösbar,

und $a \circ x = b$ in G eindeutig lösbar.

(iii) Das zu $g \in G$ inverse Element g^{-1} ist eindeutig bestimmt.

(iv) Für $g_1, \dots, g_n \in G$ gilt

$$(g_1 \circ \dots \circ g_n)^{-1} = g_n^{-1} \circ \dots \circ g_1^{-1}.$$

(v) Für $g \in G$ ist $(g^{-1})^{-1} = g$.

Beweis:

(i) Annahme: e und e' sind neutrale Elemente der Gruppe.

Dann gilt: $e = e' \circ e = e'$.
(e' ist neutrales Element; e ist neutrales Element)

(ii) Offenbar ist $b \circ a^{-1}$ Lösung von $x \circ a = b$.

Ist x_0 Lösung von $x \circ a = b$, so gilt $x_0 \circ a = b$.

Es folgt $x_0 = b \circ a^{-1}$

Also ist $x \circ a = b$ in G eindeutig lösbar.

Der Beweis für die Aussage über die Gleichung $a \circ x = b$ erfolgt analog.

(iii) Nach (ii) ist g^{-1} eindeutig bestimmt als Lösung von $x \circ g = e$.

(iv) Zu zeigen ist

$$(g_n^{-1} \circ \dots \circ g_1^{-1}) \circ (g_1 \circ \dots \circ g_n) = e.$$

Es gilt das Assoziativgesetz, nach Bem 2.1 darf beliebig geklammert werden. Also ist

$$g_n^{-1} \circ \dots \circ \underbrace{g_2^{-1} \circ \underbrace{(g_1^{-1} \circ g_1)}_{=e} \circ g_2}_{=e} \circ \dots \circ g_n = e.$$

(v) g und $(g^{-1})^{-1}$ sind Lösungen der Gleichung $g^{-1} \circ x = e$.

Nach (ii) folgt $g = (g^{-1})^{-1}$.

Bem 3.4 Sei $(G, \circ)$ eine Gruppe und seien $a, b, c \in G$.

Dann gilt:

$a \circ b = a \circ c \Rightarrow b = c$ und analog: $b \circ a = c \circ a \Rightarrow b = c$

Dies ergibt sich durch Multiplikation der linken Gleichung mit a^{-1}.

Sprechweise: In einer Gruppe darf gekürzt werden.

Def 3.4 Es sei $(G, \circ)$ ein Gruppe.

Ist $\circ$ kommutativ, so heißt $(G, \circ)$ kommutative Gruppe oder abelsche Gruppe.

§4 Endliche Gruppen

Def 4.1

Eine Gruppe $(G,\circ)$ heißt endliche Gruppe, wenn G eine endliche Menge ist.
Besitzt G n Elemente, so heißt $(G,\circ)$ Gruppe der Ordnung n.

Bsp 4.1

Sei $\mathbb{Z}_2 := \{0,1\}$.
Auf $\mathbb{Z}_2$ wird eine Verknüpfung $+$ definiert durch

$0+0 := 0$
$0+1 := 1$
$1+0 := 1$
$1+1 := 0$.

Die zugehörige Verknüpfungstafel (s. Bem 2.2)

ist also

$+$	0	1
0	0	1
1	1	0

offenbar ist 0 neutrales Element;
0 zu 0 invers und 1 zu 1 invers.
Es gilt das Assoziativgesetz; dies läßt sich bestätigen, indem alle (endlich vielen) Möglichkeiten einzeln überprüft werden.
Also ist $(\mathbb{Z}_2, +)$ eine Gruppe (der Ordnung 2).

Bem 4.1

Es sei $G := \{g_1, \dots, g_n\}$ eine endliche Menge und $(G, \circ)$ eine (endliche) ~~Gruppe~~ Halbgruppe.

Die Verknüpfungstafel von $(G, \circ)$ ist dann (s. Bem 2.2)

$\circ$	g_1	$\cdots$	g_j	$\cdots$	g_n	
g_1						
$\vdots$						
g_i	$\cdots\cdots$		$g_i \circ g_j$	$\cdots$		$\leftarrow$ i-te Zeile
$\vdots$						
g_n						

$\uparrow$ j-te Spalte

Dann gilt:
$(G, \circ)$ ist Gruppe gdw in jeder Zeile und in jeder Spalte der Verknüpfungstafel jedes Element aus G auftritt.

Bew:
$\Rightarrow$: wir betrachten die i-te Zeile und ein beliebiges $a \in G$.
Zu zeigen ist: a tritt in der i-ten Zeile auf.
Nach Bem 3.3 ist $g_i \circ x = a$ in der Gruppe lösbar, etwa durch g_j. Dann tritt a auf in der i-ten Zeile an der j-ten Stelle.
Für die Spalten kann eine analoge Betrachtung durchgeführt werden.

$\Leftarrow$: Nach Bem 3.2(iii') genügt es zu zeigen:
Für $a, b \in G$ sind $x \circ a = b$ und $a \circ x = b$ lösbar.
Ist $a = g_j$ und b an der i-ten Stelle der j-ten Spalte, so ist g_i Lösung von $x \circ a = b$.
Ist $a = g_i$ und b an der j-ten Stelle der i-ten Zeile, so ist g_j Lösung von $a \circ x = b$.

Bem 4.2

(i) Die Bedingungen in Bem. 4.1 lassen sich an Hand der Verknüpfungstafel leicht überprüfen; nicht aber das Assoziativgesetz.

(ii) Offenbar gilt:
Sei $\circ$ eine Verknüpfung auf einer endlichen Menge M.
Dann ist $\circ$ Kommutativ gdw die Verknüpfungstafel symmetrisch zur Hauptdiagonalen ist.

Bem 4.3

(i) Bis auf Schreibweise gibt es genau eine Gruppe der Ordnung 1, nämlich $(G,\circ)$ mit $G=\{e\}$ und $e\circ e = e$.

(ii) Die Verknüpfungstafel einer Gruppe $(G,\circ)$ der Ordnung 2 mit $G=\{e,a\}$ und dem neutralen Element e ist festgelegt durch

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

(nach Bem 4.1)

Es gibt also höchstens eine Gruppe der Ordnung 2 (bis auf Schreibweise).
Man kann in endlich vielen Schritten überprüfen, ob die Verknüpfung $\circ$ assoziativ ist; also ist $(G,\circ)$ eine Gruppe.

Bis auf Schreibweise gibt es also genau eine Gruppe der Ordnung 2.

Ändert man die Bezeichnung und ersetzt e durch 0 und a durch 1, $\circ$ durch $+$, so erhält man die Gruppe aus Bsp 4.1

(iii) Analog zu (ii) erhält man:
Bis auf Schreibweise gibt es genau eine Gruppe der Ordnung 3;
Ist $(G,\circ)$ Gruppe der Ordnung 3 und e das neutrale Element, $G=\{e,a,b\}$, so erhält man die Verknüpfungstafel

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

Die erste Zeile und 1. Spalte ergibt sich, da e neutrales Element ist. Dann bleibt für $a\circ b$ nur e und auch der Rest ist festgelegt.

(iv) Analog erhält man: Bis auf Schreibweise gibt es genau 2 Gruppen der Ordnung 4

§5 Permutationen und Gruppen

Def. 5.1

Es sei $M = \{m_1, \dots, m_n\}$ eine endliche Menge und $\pi : M \to M$ eine bijektive Abbildung.

Dann heißt π Permutation (von M).

Schreibweise für π, aus der die Zuordnungsvorschrift für π hervorgeht:

$$\begin{pmatrix} a_1 & \dots & a_n \\ \pi(a_1) & \dots & \pi(a_n) \end{pmatrix} \qquad (*)$$

beachte unter jedem Element steht das Bild.

Natürlich kann die Reihenfolge der $a_1, \dots, a_n$ auch anders gewählt werden, die Permutation bleibt dieselbe.

Anmerkung: Da π bijektiv ist, tritt jedes Element aus M in der zweiten Zeile von $(*)$ (genau ein Mal) auf.

Bsp 5.1

$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$, $\pi_2 = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ sind Permutationen;

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

Z.B. bildet π_1 die Zahl 3 auf 4 ab.

Bem 5.1

(i) Die Hintereinanderschaltung bijektiver Abbildungen ist bijektiv.

(ii) Eine bijektive Abbildung besitzt eine Umkehrabbildung, diese ist auch wieder bijektiv (s. Bem 1.3).

(iii) Die Hintereinanderschaltung von Permutationen wird auch als Produkt bezeichnet.

Bsp 5.2

Mit den Bezeichnungen aus Bsp. 5.1 gilt

$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$;

$1 \xmapsto{\pi_1} 3 \xmapsto{\pi_2} 3$
$2 \xmapsto{\pi_1} 2 \xmapsto{\pi_2} 1$
$3 \xmapsto{\pi_1} 4 \xmapsto{\pi_2} 4$
$4 \xmapsto{\pi_1} 1 \xmapsto{\pi_2} 2$;

$\pi_1^2 = \pi_1 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$;

$\pi_1^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id$ (Identität, die jedes Element auf sich abbildet.) ;

$\pi_1^{-1} = \pi_1^2$ (da $\pi_1 \circ \pi_1^2 = id$, s.o.),
$(\pi_1^2)^{-1} = \pi_1$ (da $\pi_1^0 \circ \pi_1 = id$).

Bem. 5.2

Sei $M = \{a_1, \dots, a_n\}$ eine Menge von n Elementen.

Sei S_n die Menge aller Permutationen von M.

$\circ$ bezeichne die Hintereinanderschaltung von Abbildungen.

Dann ist $(S_n, \circ)$ eine Gruppe (bezeichnet als symmetrische Gruppe vom Index n),
das neutrale Element dieser Gruppe ist die Abb. id, die jedes Element auf sich abbildet (mit id bezeichnet)

Bew klar nach Bem 2.3 (iii) und Bem 5.1.

Bem 5.3

Bekanntlich besitzt die symmetrische Gruppe $(S_n, \circ)$ vom Index n genau $n!$ Elemente (Beweis durch vollständige Induktion)

Bem 5.4 Auf die Bezeichnung der Elemente aus M in Bem 5.2 kommt es nicht an; bis auf Schreibweise erhält man immer dieselbe Gruppe.
Häufig verwendet man $M = \{1, 2, \dots, n\}$.

Bsp 5.3

Sei $M = \{a_1, a_2\}$. Dann ist $S_2 = \left\{ \underbrace{\begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}}_{=id.}, \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} \right\}$

Bsp 5.4

Betrachte π_1 aus Beispiel 5.1 bzw. Beispiel 5.2.

Sei $G := \{ id, \pi_1, \pi_1^2 \}$.

Dann ist $\pi_1^3 = id$, also $\pi_1^{-1} = \pi_1^2$, $(\pi_1^2)^{-1} = \pi_1$

Also ist $(G, \circ)$ eine Gruppe.

Bem 5.5 (Zyklus)

Eine Permutation der Form $\begin{pmatrix} 1 & 2 & 3 & \cdots & (n-1) & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}$

heißt Zyklus (der Länge n).

Es gilt $1 \longmapsto 2$; $2 \longmapsto 3$; $\ldots$; $(n-1) \longmapsto n$; $n \longmapsto 1$.

Offenbar sind $id, \pi, \ldots, \pi^{n-1}$ paarweise verschieden;

es gilt $\pi^n = id$, also $\underbrace{\pi \circ \pi \circ \ldots \circ \pi}_{n\text{-mal}} = id$.

Es folgt $\pi^i \circ \pi^{n-i} = id$, also $(\pi^i)^{-1} = \pi^{n-i}$.

Also ist $(\{id, \pi, \ldots, \pi^{n-1}\}, \circ)$ eine Gruppe (Sprechweise: die von π erzeugte Gruppe).

Bem 5.6 (Permutation als Produkt elementefremder Zyklen)

Gegeben sei eine Permutation π von $M = \{1, \dots, n\}$; also ist $\pi \in S_n$.

Dann läßt sich π darstellen in der folgenden Form:

Wähle ein beliebiges Element aus M; etwa $1 \in M$.

Betrachte den folgenden Zyklus:

$(1, \pi(1), \pi^2(1), \dots, \pi^{m-1}(1))$, wobei $\pi^m(1) = 1$ ist.

Dabei ist m eindeutig bestimmt. Da π bijektiv ist, kann in der Folge der Elemente des Zyklus kein Element mehrfach auftreten und weil M endlich ist, tritt nach endlich vielen Schritten wieder 1 als Bild auf.

Man setze das Verfahren fort und bilde einen neuen Zyklus, als Anfangselement wird ein Element aus M gewählt, das im ersten Zyklus nicht aufgetreten ist (gibt es ein solches Element nicht, so ist man fertig).

Eine Fortführung des Verfahrens liefert eine Darstellung von π als Produkt elementefremder Zyklen (d.h. je 2 verschiedene Zyklen enthalten kein gemeinsames Element).

Die Darstellung ist bis auf die Reihenfolge der Zyklen eindeutig.

Das Produkt der elementefremden Zyklen ist kommutativ.

Bsp 5.5

Für $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 3 & 7 & 5 & 8 & 6 & 4 \end{pmatrix}$

erhält man

$\pi = (1,2) \circ (3) \circ (4,7,6,8)$.

Jede einzelne Klammer ist ein Zyklus.

π ist dargestellt als Produkt elementefremder Zyklen.

Zyklen der Länge 1 können auch weggelassen werden, wenn klar ist welche Grundmenge M zu Grunde liegt.

Bem 5.7 (Transpositionen)

Ein Zyklus der Länge 2 heißt Transposition.
Eine Transposition vertauscht also zwei Elemente.
Also ist das Quadrat einer Transposition stets die Identität.

Es gilt

$$(a_1, \dots, a_n) = (a_1, \dots, a_{n-1}) \circ (a_{n-1}, a_n). \quad (n \geq 3)$$

Dies ist leicht nachzuprüfen; z.B. gilt rechts: $a_{n-1} \mapsto a_n$; $a_n \mapsto a_{n-1} \mapsto a_1$.
Wiederholte Anwendung liefert mit Hilfe von Bem 5.6:

Jede Permutation läßt sich als Produkt von Transpositionen schreiben. Man beachte: Die Darstellung ist nicht eindeutig.

Bei einer gegebenen Permutation π ist die Anzahl der Faktoren allerdings stets gerade (dann heißt π gerade Permutation) oder stets ungerade (dann heißt π ungerade Permutation) (ohne Bew).

Bei der Hintereinander-schaltung von Zyklen schreibt man $\circ$ häufig nicht mit.

Bsp 5.6

(i) $id = (1,2)(1,2)$ ist eine gerade Permutation

(ii) $(1,2,3) = (1,2)(2,3)$ ist eine ungerade Permutation,

(iii) Es gilt

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1,2,3,4) = (1,2,3)(3,4) = (1,2)(2,3)(3,4)$$

Dies ergibt sich aus Bem 5.6 und Bem 5.7.

Es gilt aber auch $\pi = (1,4)(3,1)(2,1)$, was sich leicht nachrechnen läßt (z.B. gilt $1 \mapsto 2 \mapsto 2 \mapsto 2$; $2 \mapsto 1 \mapsto 3 \mapsto 3$).
Schrittweise Darstellung von $\pi = (1,4) \circ (3,1) \circ (2,1)$:

$$\left.\begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{matrix}\right\} \text{Anwendung von } (2,1)$$
$$\left.\begin{matrix} 2 & 3 & 1 & 4 \end{matrix}\right\} \text{Anwendung von } (3,1)$$
$$\left.\begin{matrix} 2 & 3 & 4 & 1 \end{matrix}\right\} \text{Anwendung von } (1,4)$$

Die zweite Zeile von π entsteht, in dem in 3 Schritten jeweils 2 Elemente vertauscht werden.

Der erste Schritt erfolgt so, daß die richtige Zuordnung der 1, also $1 \longmapsto 2$ erreicht wird.

Der zweite Schritt erfolgt so, daß die richtige Zuordnung der 2, also $2 \longmapsto 3$ erreicht wird.

Der dritte Schritt erfolgt so, daß die richtige Zuordnung der 3, also $3 \longmapsto 4$ erreicht wird.

Da π bijektiv ist, ergibt sich die richtige Zuordnung der 4 dann von selbst.

Dieses Verfahren kann natürlich analog angewendet werden auf beliebige Permutationen.

Bem 5.8

Betrachte die symmetrische Gruppe $(S_n, \circ)$ vom Index n, $n \geq 2$.

$id = (12)(12)$ ist eine gerade Permutation (s. Bsp 5.6 (i)).

Offenbar ist das Produkt gerader Permutationen wieder gerade.

Sei $\pi = (a_1, a_2) \cdots (a_{n-1}, a_n)$ Produkt von Transpositionen.

Da eine Transposition zu sich selbst invers ist, folgt nach Bem 3.3 (iv)

$\pi^{-1} = (a_{n-1}, a_n) \cdots (a_1, a_2)$. Es folgt: Ist π gerade, so auch π^{-1}.

Zusammen ergibt sich.

Sei A_n die Menge aller geraden Permutation aus S_n.

Dann ist $(A_n, \circ)$ eine Gruppe (alternierende Gruppe vom Index n).

A_n ist also Untergruppe von $(S_n, \circ)$ (s. Beh. 6.1)

§6 Untergruppen und Nebenklassen

Def 6.1 (Untergruppe)

Es sei $(G,\circ)$ eine Gruppe und $U \subseteq G$ (also U Teilmenge von G).

Sei U abgeschlossen bzgl. der Verknüpfung $\circ$; d.h.

$$u_1, u_2 \in U \Rightarrow u_1 \circ u_2 \in U.$$

Dann läßt sich $\circ$ auffassen als Verknüpfung von U.

Dann heißt $(U,\circ)$ Untergruppe der Gruppe $(G,\circ)$, falls $(U,\circ)$ Gruppe ist.

Für $(U,\circ)$ schreibt man häufig einfach U.

Bem 6.1

(i) Es sei $(G,\circ)$ Gruppe mit dem neutralen Element e und U Untergruppe von $(G,\circ)$.

Dann ist $e \in U$ und e ist neutrales Element von U.

Beweis: Annahme: e' ist das neutrale Element von U.

Dann gilt $e' \circ e' = e' = e \circ e'$, also $e' \circ e' = e \circ e'$.

Multiplikation von rechts mit dem Inversen von e' liefert $e = e'$.

(ii) Der Durchschnitt beliebig vieler Untergruppen einer Gruppe $(G,\circ)$ ist wieder Untergruppe von $(G,\circ)$.

Beweis: klar

Sind z.B. a, b im Durchschnitt, dann sind a, b in jeder Untergruppe und $a \circ b$ ist auch in jeder Untergruppe, also im Durchschnitt.

Bsp 6.1

(i) Sei $n \in \mathbb{N}$. Dann ist $n\mathbb{Z} := \{n \cdot z \mid z \in \mathbb{Z}\}$ Untergruppe der Gruppe $(\mathbb{Z}, +)$.

Speziell sind $2\mathbb{Z}$ und $3\mathbb{Z}$ Untergruppen von $(\mathbb{Z}, +)$; ferner ist $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ Untergruppe von $(\mathbb{Z}, +)$.

Bem 6.2

Die Vereinigung von Untergruppen einer Gruppe $(G, \circ)$ ist nicht notwendig wieder Untergruppe von $(G, \circ)$.
Zum Beispiel ist $2\mathbb{Z} \cup 3\mathbb{Z}$ (Menge aller ganzen Zahlen, die Vielfaches von 2 oder Vielfaches von 3 sind) keine Untergruppe von $(\mathbb{Z}, +)$; es gilt z.B. $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, aber $2 + 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Bem 6.3 (Untergruppenkriterium)

Es sei $(G, \circ)$ eine Gruppe und $U \subseteq G$, U nicht leer.

Dann gilt:

$$U \text{ Untergruppe von } (G, \circ) \iff \left(a, b \in U \Rightarrow a \circ b^{-1} \in U\right)$$

Beweis

$\Rightarrow$: trivial

$\Leftarrow$: Nach Voraussetzung existiert ein $u \in U$, da U nicht leer ist.
Nach Voraussetzung ist dann $u \circ u^{-1} = e \in U$.
Sei $a \in U$ beliebig. Nach Voraussetzung folgt $e \circ a^{-1} \in U$, also $a^{-1} \in U$.
Seien $a, b \in U$. Dann ist auch $b^{-1} \in U$ (s.o.) und nach Voraussetzung $a \circ (b^{-1})^{-1} \in U$. Nach Bem 3.3 (V) ist $(b^{-1})^{-1} = b$. Es folgt $a \cdot b \in U$.
Damit ist die Behauptung bewiesen.

Def. 6.2 (Nebenklassen)

Es sei $(G,\circ)$ eine Gruppe, $g \in G$ und U Untergruppe von $(G,\circ)$.

Dann heißt die Menge

$g \circ U := \{g \circ u \mid u \in U\}$ (die von g erzeugte) Linksnebenklasse von U.
↑ Man beachte: Dies ist keine Verknüpfung, sondern nur eine Schreibweise.

und die Menge

$U \circ g := \{u \circ g \mid u \in U\}$ (die von g erzeugte) Rechtsnebenklasse von U.

(Man beachte: $g \circ U$ und $U \circ g$ sind Teilmengen von G)

g heißt Repräsentant der Nebenklasse $g \circ U$ bzw. $U \circ g$.

Bem 6.4

Es sei $(G,\circ)$ eine Gruppe mit dem neutralen Element e und U eine Untergruppe von G.

(i) Dann ist offenbar $e \circ U = U$.

(ii) Für $g \in G$ gilt stets $g \in g \circ U$ und $g \in U \circ g$ (da $e \in U$) (Bem 6.1(i))

(iii) $\{e\}$ ist eine Untergruppe von $(G,\circ)$, die von g erzeugte Linksnebenklasse von $\{e\}$ ist $\{g\}$; natürlich besitzt G in G als einzige Nebenklasse.

Bem 6.5

Es sei U Untergruppe der Gruppe $(G,\circ)$. Dann gilt:

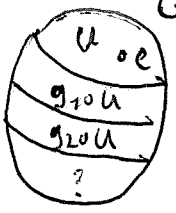
(i) Zwei Linksnebenklassen von U sind gleich oder elementefremd; d.h. für $g_1, g_2 \in G$ gilt stets

$$g_1 \circ U = g_2 \circ U \quad \text{oder} \quad (g_1 \circ U) \cap (g_2 \circ U) = \emptyset \text{ (Leere Menge)}.$$

(ii) Die Linksnebenklassen von U bilden eine Partion von G

(Die Aussagen gelten analog für Rechtsnebenklassen)

anschauliche Darstellung:



Linksnebenklassen von U.

Beweis

(i) Annahme: $(g_1 \circ U) \cap (g_2 \circ U) \neq \emptyset$; etwa $c \in g_1 \circ U$ und $c \in g_2 \circ U$.

Dann ist zu zeigen: $g_1 \circ U = g_2 \circ U$.

Wir zeigen $g_1 \circ U \subseteq g_2 \circ U$ (analog folgt $g_2 \circ U \subseteq g_1 \circ U$).

Wir betrachten ein beliebiges Element aus $g_1 \circ U$,

dieses besitzt die Form $g_1 \circ u$ mit einem $u \in U$. Zu zeigen: $g_1 \circ u \in g_2 \circ U$.

Das Element c läßt sich darstellen in der Form

$c = g_1 \circ u_1 = g_2 \circ u_2$ mit $u_1, u_2 \in U$; hieraus folgt $g_1 = g_2 \circ u_2 \circ u_1^{-1}$.

Weiter folgt $g_1 \circ u = g_2 \circ \underbrace{u_2 \circ u_1^{-1} \circ u}_{\in U} \in g_2 \circ U$.

(ii) ist klar wegen (i) und Bem 6.4 (ii).

Bem 6.6

Sei U Untergruppe der Gruppe $(G, \circ)$; $g_1, g_2 \in G$.

Dann gilt: $g_1 \circ U = g_2 \circ U$ gdw $g_1 \in g_2 \circ U$

Bew: klar nach Bem 6.5 (i).

Bem 6.7

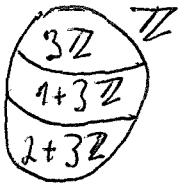
Sei U Untergruppe der Gruppe $(G, \circ)$.

Die von U verschiedenen Linksnebenklassen von U sind keine Untergruppen von $(G, \circ)$; nach Bem 6.5 enthalten sie e nicht als Element.

Bem 6.8 Ist die Gruppe $(G, \circ)$ kommutativ, U Untergruppe und $g \in G$, so gilt $g \circ U = U \circ g$.

Bsp 6.2

(i) $3\mathbb{Z}$ ist eine Untergruppe der Gruppe $(\mathbb{Z}, +)$.
Die Linksnebenklassen von $3\mathbb{Z}$ in $\mathbb{Z}$ sind
$3\mathbb{Z}$, $1+3\mathbb{Z}$ $(=\{1+3z \mid z\in\mathbb{Z}\})$, $2+3\mathbb{Z}$.
$1+3\mathbb{Z}$ enthält alle ganzen Zahlen, die bei Division durch 3 den Rest 1 haben.
$2+3\mathbb{Z}$ enthält alle ganzen Zahlen, die bei Division durch 3 den Rest 2 haben.



Die drei Nebenklassen bilden eine Partition von $\mathbb{Z}$

(ii) Sei $n\in\mathbb{N}$. Analog zu (i) erhält man:
$n\mathbb{Z}$ ist eine Untergruppe von $(\mathbb{Z}, +)$,
die Nebenklassen von $n\mathbb{Z}$ sind
$n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$.

Es gilt
$i+n\mathbb{Z} = j+n\mathbb{Z}$
$\overset{\text{Bem 6.6.}}{\Leftrightarrow}$ $i\in j+n\mathbb{Z}$
$\Leftrightarrow$ i hat die Form $j+nz$ für ein $z\in\mathbb{Z}$.
$\Leftrightarrow$ $(i-j)$ ist Vielfaches von n in $\mathbb{Z}$.

Zum Beispiel gilt $3+5\mathbb{Z} = 8+5\mathbb{Z} = -2+5\mathbb{Z} \neq 4+5\mathbb{Z}$.

§7 Untergruppen endlicher Gruppen

Bem 7.1

Es sei $(G,\circ)$ eine endliche Gruppe und U Untergruppe von $(G,\circ)$, $g \in G$.

Sei gU die von g erzeugte Linksnebenklasse von U.

Dann besitzen gU und U gleich viele Elemente, es gilt also

$|gU| = |U|$ (analog gilt dies auch für Rechtsnebenklassen).

Bew

Zwei endliche Mengen M_1 und M_2 besitzen gleich viel Elemente, wenn es eine bijektive Abb $\varphi: M_1 \to M_2$ gibt.

Es genügt also zu zeigen:

Die Abbildung $\varphi: U \to gU$ definiert durch $\varphi(u) = gou$ für alle $u \in U$ ist bijektiv.

φ ist surjektiv, denn ein Element $gou \in gU = \{gou \mid u \in U\}$ hat u als Urbild.

Ferner ist φ injektiv:

Annahme: $\varphi(u_1) = gou_1 = gou_2 = \varphi(u_2)$.

Durch Kürzen (Multiplikation mit g^{-1} von links) folgt $u_1 = u_2$.

Also ist φ injektiv.

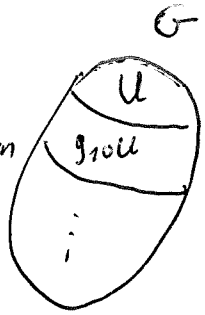
Satz 7.1 (Lagrange)

Es sei $(G,\circ)$ eine endliche Gruppe und U eine Untergruppe.
Es bezeichne $[G:U]$ die Anzahl der Linksnebenklassen von U in G (Index von U in G).

Dann gilt:

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

Speziell ist $|U|$ Teiler von $|G|$.
(Analog gilt dies für die Rechtsnebenklassen)



Beweis

Nach Bem 6.5 bilden die Linksnebenklassen von U eine Partition von G.

Jede Linksnebenklasse besitzt nach Bem 7.1 genau so viele Elemente wie U.

Daraus folgt die Behauptung.

Bem 7.2

Es sei $(G,\circ)$ eine endliche Gruppe, $g \in G$.

Setze $g^0 := e$ (neutrales Element von G).

Seien $e, g, \dots, g^{m-1}$ paarweise verschieden,
$e, g, \dots, g^{m-1}, g^m$ nicht paarweise verschieden.

Dann ist $g^m = e$ ($g^m = g^i$ für $0 < i < m$ ist nicht möglich, denn hieraus folgt durch Kürzen in der Gruppe $g^{m-i} = e$ und $e, g, \dots g^{m-1}$ wären nicht paarweise verschieden).

Dann ist $\{e, g, \dots, g^{m-1}\}$ eine Untergruppe von $(G,\circ)$;

es gilt $g^m = e = g^i \circ g^{m-i}$,

zu g^i ist also g^{m-i} invers.

Ferner gilt offenbar $g^i = g^j \Leftrightarrow (i-j)$ ist Vielfaches von m. (*)

$\{e, g, \dots, g^{m-1}\}$ heißt die von g erzeugte Untergruppe von $(G,\circ)$.

m wird als Ordnung von g bezeichnet.

Nach Satz 7.1 (Lagrange) folgt:

m ist Teiler von $|G|$.

Die Ordnung eines Elementes g aus G ist also stets Teiler der Gruppenordnung und gleich der Ordnung der von g erzeugten Untergruppe. Speziell folgt $g^{|G|} = e$ für jedes $g \in G$ (nach (*)).

Bem 7.3

Es sei $(G,\circ)$ eine endliche Gruppe, die Gruppenordnung $|G|$ sei eine Primzahl p.

Sei $g \in G$ nicht das neutrale Element von $(G,\circ)$.

Dann ist die Ordnung von g größer 1 und Teiler von p (nach Bem 7.2); die Ordnung von g ist also gleich $|G|$ $(= p)$ (da p Primzahl ist).

Es folgt

$$G = \{e, g, \dots, g^{p-1}\}$$

Jede Gruppe der Ordnung p läßt sich so darstellen.

Eine solche Gruppe heißt zyklische Gruppe.

Bsp 7.1

Es sei $(S_3, \circ)$ die symmetrische Gruppe vom Index 3.

S_3 enthält genau $3!$ $(=6)$ Elemente,

nämlich alle Permutationen der Menge $\{1, 2, 3\}$. (s. Bem 5.2. und Bem 5.3)

Dann ist $U := \{id, (1,2)\}$ die von $(1,2)$ erzeugte Untergruppe

der Gruppe $(S_3, \circ)$ (Man beachte: $(1,2) \circ (1,2) = (1,2)^2 = id$).

Nach Lagrange besitzt U in $(S_3, \circ)$ 3 Linksnebenklassen, neben U

noch 2 weitere, analog 3 Rechtsnebenklassen.

Es gilt $U \circ (2,3) = \{(2,3), (1,2) \circ (2,3)\} = \{(2,3), (1,2,3)\}$,

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

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

Die 3 Rechtsnebenklassen von U sind also U, $U \circ (2,3)$, $U \circ (1,3,2)$.

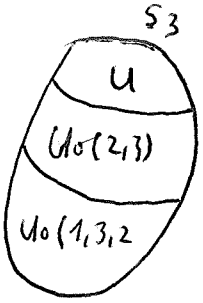
Es gilt $U \circ (2,3) \neq (2,3) \circ U$, $U \circ (1,2,3) \neq (2,3) \circ U$, $U \neq (2,3) \circ U$.

Also tritt ~~$U \circ (2,3) = (2,3) \circ U$~~ nicht als Rechtsnebenklasse auf.

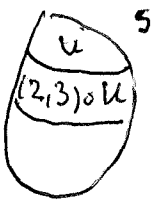
Die Linksnebenklassen von U liefern also eine andere Partition

von S_3 wie die Rechtsnebenklassen von U.

Rechtsnebenklassen von U:



Linksnebenklassen von U:



Die dritte Linksnebenklasse von U wird erzeugt von jedem Element aus S_3, das nicht in $U \circ (2,3) \circ U$ liegt.

§8 Normalteiler und Faktorgruppen

Wir betrachten Untergruppen, bei denen die Linksnebenklassen übereinstimmen mit den Rechtsnebenklassen; Bsp 7.1 zeigt, daß dies nicht immer der Fall ist.

Def 8.1 (Normalteiler)
Es sei N eine Untergruppe der Gruppe $(G,\circ)$.
Dann wird definiert:
N Normalteiler von $(G,\circ) :\Leftrightarrow g\circ N = N\circ g$ f.a. $g\in G$.

Bem 8.1
Sei $(G,\circ)$ eine kommutative Gruppe.
Dann ist jede Untergruppe Normalteiler (s. Bem. 6.8).

Bem 8.2 (triviale Normalteiler)
Sei $(G,\circ)$ eine Gruppe mit dem neutralen Element e.
Dann ist die Untergruppe $\{e\}$ von $(G,\circ)$ Normalteiler von $(G,\circ)$, und die Untergruppe G von $(G,\circ)$ ist ebenfalls Normalteiler von $(G,\circ)$ (s. Bem 6.4).
Diese beiden Untergruppen heißen triviale Normalteiler von $(G,\circ)$.

Bem 8.3
Sei N Normalteiler der Gruppe $(G,\circ)$ und $g\in G, n\in N$.
Dann läßt sich $g\circ n$ darstellen in der Form $n'\circ g$ mit einem geeigneten Element $n'\in N$. (analog für $n\circ g$)

Beweis Es gilt $g\circ n \in g\circ N = N\circ g = \{m\circ g \mid m\in N\}$.
($g\circ n \in g\circ N$: Def. der Linksnebenklasse; $g\circ N = N\circ g$: da N Normalteiler ist)

Bem 8.4 (Normalteilerkriterium)

Sei $(G,\circ)$ eine Gruppe und U Untergruppe von $(G,\circ)$.
Dann gilt:
U Normalteiler von $(G,\circ) \Leftrightarrow (g \in G, u \in U \Rightarrow g \circ u \circ \bar{g}^1 \in U)$

Beweis
$\Rightarrow$: Sei $g \in G, u \in U$.
Dann ist $g \circ u = u' \circ g$ für ein $u' \in U$ nach Bem 8.3.
Es folgt $g \circ u \circ \bar{g}^1 = u' \in U$
$\Leftarrow$: Gegeben sei eine beliebige Linksnebenklasse $g \circ U$ von U.
Dann ist zu zeigen: $g \circ U = U \circ g$.
Wir zeigen: $g \circ U \subseteq U \circ g$ (analog folgt $U \circ g \subseteq g \circ U$).
Sei ein beliebiges Element aus $g \circ U$ gegeben, dieses hat die Form $g \circ u$ mit $u \in U$.
Nach Voraussetzung folgt dann $g \circ u \circ \bar{g}^{-1} =: u' \in U$.
Es folgt $g \circ u = u' \circ g \in U \circ g$.

Das Normalteilerkriterium wird häufig verwendet, um von einer Untergruppe nachzuweisen, daß es sich um einen Normalteiler handelt. In der Regel ist dies einfacher als die Verwendung der Definition.

Die Bedeutung der Normalteiler besteht darin, daß man mit ihrer Hilfe neue Gruppen bilden kann, nämlich sogenannte Faktorgruppen.

Satz 8.1 (Faktorgruppe)

Es sei $(G,\circ)$ eine Gruppe und N Normalteiler von $(G,\circ)$.

Es bezeichne $G/N := \{a\circ N \mid a \in G\}$ die Menge der Linksnebenklassen (oder gleichwertig Rechtsnebenklassen) von N in $(G,\circ)$.

Dann gilt:

(i) Durch $(a\circ N)\bullet(b\circ N) := (a\circ b)\circ N$ wird auf G/N eine Verknüpfung $\bullet$ definiert; d.h. das Verknüpfungsergebnis der beiden Nebenklassen $a\circ N$ und $b\circ N$ ist diejenige Nebenklasse von N, die von $a\circ b$ erzeugt wird. (Häufig wird $\bullet$ auch wieder mit $\circ$ bezeichnet).

(ii) $(G/N, \bullet)$ ist eine Gruppe (Faktorgruppe von N in $(G,\circ)$);
Die Nebenklasse N $(= e\circ N)$ ist das neutrale Element der Faktorgruppe.
Zur Nebenklasse $a\circ N$ ist die Nebenklasse $\bar{a}^{-1}\circ N$ invers.

Beweis

(i) Man beachte: Eine Nebenklasse $a\circ N$ besitzt verschiedene Repräsentanten; es gilt $a\circ N = a'\circ N$ gdw $a' \in a\circ N$ ist (s. Bem. 6.6). Die Definition der Verknüpfung $\bullet$ in (i) ist natürlich nur sinnvoll, wenn das Verknüpfungsergebnis eindeutig bestimmt ist, also unabhängig von der Wahl der Repräsentanten der Nebenklassen ist (man sagt dann: $\bullet$ ist wohldefiniert).

Zu zeigen ist also:

Gegeben seien die beiden Nebenklassen $a \circ N = a' \circ N$ und $b \circ N = b' \circ N$ durch jeweils zwei verschiedene Repräsentanten.

Dann gilt $(a \circ b) \circ N = (a' \circ b') \circ N$.

Dies ergibt sich wie folgt:

$a \circ N = a' \circ N$, also hat a die Form $a = a' \circ n_1$ mit einem $n_1 \in N$,
$b \circ N = b' \circ N$, also hat b die Form $b = b' \circ n_2$ mit einem $n_2 \in N$.

Dann folgt (man beachte: Da N Normalteiler ist, hat $n_1 \circ b'$ die Form $b' \circ n_1'$ mit einem $n_1' \in N$ nach Bem 8.3)

$$a \circ b = a' \circ n_1 \circ b' \circ n_2 = a' \circ b' \circ \underbrace{n_1' \circ n_2}_{\in N} \in (a' \circ b') \circ N.$$

Nun ist $a \circ b \in (a \circ b) \circ N$ und $a \circ b \in (a' \circ b') \circ N$.
Zwei Nebenklassen sind gleich oder elementefremd, also folgt $(a \circ b) \circ N = (a' \circ b') \circ N$.

(ii) $e \circ N$ ist neutrales Element von $\cdot$, denn es gilt $(e \circ N) \cdot (g \circ N) = (e \circ g) \circ N = g \circ N$
und analog $(g \circ N) \cdot (e \circ N) = (g \circ e) \circ N = g \circ N$.
$a^{-1} \circ N$ ist zu $a \circ N$ invers, denn es gilt $(a \circ N) \cdot (a^{-1} \circ N) = (a \circ a^{-1}) \circ N = e \circ N = N$,
und analog $(a^{-1} \circ N) \cdot (a \circ N) = (a^{-1} \circ a) \circ N = e \circ N = N$.
Ferner ist $\cdot$ assoziativ, denn es gilt
$((a \circ N) \cdot (b \circ N)) \cdot (c \circ N) = ((a \circ b) \circ N) \cdot (c \circ N) = (a \circ b \circ c) \circ N$,
$(a \circ N) \cdot ((b \circ N) \cdot (c \circ N)) = a \circ b \circ c \circ N$.
Das Assoziativgesetz in $(G, \circ)$ wird also auf die Faktorgruppe übertragen.

Bem 8.4

(i) Sei $(G, \circ)$ eine Gruppe und N Normalteiler von $(G, \circ)$.
Die Elemente der Faktorgruppe $(G/N, \cdot)$ sind Teilmengen von G, nämlich Nebenklassen von N.

(ii) Ist $(G, \circ)$ eine endliche Gruppe und N ein Normalteiler, so läßt sich die Ordnung der Faktorgruppe von G nach N mit Hilfe des Satzes von Lagrange ermitteln.

(iii) Sei $(G, \circ)$ eine Gruppe. Die Faktorgruppe $(G/G, \cdot)$ besitzt nur ein Element, nämlich G.

Bsp 8.1

Sei $n \in \mathbb{N}$ gegeben.

Dann ist $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ eine Untergruppe von $(\mathbb{Z}, +)$;

da $(\mathbb{Z}, +)$ kommutative Gruppe ist, ist $n\mathbb{Z}$ auch Normalteiler (nach Bem 8.1)

Die Nebenklassen von $n\mathbb{Z}$ sind $n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}$ (s. Bsp 6.2 ii)

Betrachte die Faktorgruppe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$.

Dann ist $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}\}$.

und $(i+n\mathbb{Z}) + (j+n\mathbb{Z}) = (i+j)+n\mathbb{Z}$.

$1\mathbb{Z}$ $(= 0+n\mathbb{Z})$ ist das neutrale Element (die Null)

Zu $i+n\mathbb{Z}$ ist $(n-i)+n\mathbb{Z}$ invers.

Man beachte (s. Bsp 6.6 (ii))

$$i+n\mathbb{Z} = j+n\mathbb{Z} \iff i \text{ hat die Form } i = j+nz \text{ für ein } z \in \mathbb{Z}$$
$$\iff (i-j) \text{ ist Vielfaches von } n.$$

Z.B. gilt

$$(3+5\mathbb{Z}) + (8+5\mathbb{Z}) = 11+5\mathbb{Z} = 1+5\mathbb{Z}$$

$$(3+5\mathbb{Z}) + (2+5\mathbb{Z}) = 5+5\mathbb{Z} = 5\mathbb{Z}, \text{ also } -(3+5\mathbb{Z}) = 2+5\mathbb{Z}.$$

Bem 8.5 Für die Nebenklasse $i+n\mathbb{Z}$ schreibt man auch $i \pmod n$.
Wir werden später darauf zurückkommen.

§9 Gruppen-Homomorphismen

Def. 9.1

Es seien $(G,\circ)$ und $(H,\cdot)$ Gruppen und $\varphi: G \to H$ eine Abbildung.

$\varphi: G \to H$ heißt (Gruppen-) Homomorphismus, wenn φ relationstreu bzgl. $\circ$ ist, d.h. wenn gilt

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

Ein bijektiver (Gruppen-) Homomorphismus heißt (Gruppen-) Isomorphismus.

$(G,\circ)$ und $(H,\cdot)$ heißen isomorph, wenn es einen Isomorphismus $\varphi: G \to H$ gibt. Schreibweise: $G \cong H$.

Bem 9.1

Isomorphe Gruppen gehen durch Umbezeichnung der Elemente auseinander hervor, und Umbezeichnung der Verknüpfung.

Bsp 9.1

Betrachte die Gruppe $(G,\circ)$ mit $G = \{e,a\}$ und der Verknüpfungstafel

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

und die Gruppe $(Z_2,+)$ mit $Z_2 = \{0,1\}$ und der Verknüpfungstafel

$+$	0	1
0	0	1
1	1	0.

(S. Bsp 4.1 und Bem 4.3)

Sei $\varphi: G \to Z_2$ definiert durch $\varphi(e) := 0$, $\varphi(a) := 1$.

Dann ist φ ein Gruppen-Isomorphismus, da gilt $\varphi(a \circ a) = \varphi(e) = 0$;

$\varphi(a) + \varphi(a) = 1 + 1 = 0$; also $\varphi(a \circ a) = \varphi(a) \cdot \varphi(a)$.

Beide Gruppen sind bis "auf die Schreibweise gleich".

Bsp 9.2

Betrachte die Gruppen $(\mathbb{Z},+)$ und $(3\mathbb{Z},+)$.

Dann ist $\varphi : \mathbb{Z} \to 3\mathbb{Z}$ definiert durch $\varphi(z) := 3z$ für alle $z \in \mathbb{Z}$ ein Gruppen-Homomorphismus, denn es gilt

$$\varphi(z_1+z_2) = 3(z_1+z_2) = 3z_1+3z_2 = \varphi(z_1)+\varphi(z_2) \text{ für alle } z_1,z_2 \in \mathbb{Z}.$$

Da φ bijektiv ist, ist φ auch Gruppen-Isomorphismus.
(Es erscheint etwas überraschend, daß die echte Untergruppe $3\mathbb{Z}$ von $(\mathbb{Z},+)$ isomorph zu $(\mathbb{Z},+)$ ist).

Bsp 9.3

Es sei $(G,\circ)$ eine Gruppe mit dem neutralen Element e.

(i) Sei $\varphi : G \to G$ definiert durch $\varphi(g) := e$ für alle $g \in G$.
Dann ist φ ein Homomorphismus.

(ii) Sei $f : G \to G$ definiert durch $f(g) := g$ für alle $g \in G$.
Dann ist φ ein Isomorphismus.

Bem 9.2 (Eigenschaften von Gruppenhomomorphismen)

Es seien $(G,\circ)$ und $(H,\circ)$ Gruppen,
$\varphi : G \to H$ ein Gruppen-Homomorphismus,
e das neutrale Element der Gruppe $(G,\circ)$,
e' das neutrale Element der Gruppe $(H,\circ)$.
Dann gilt:

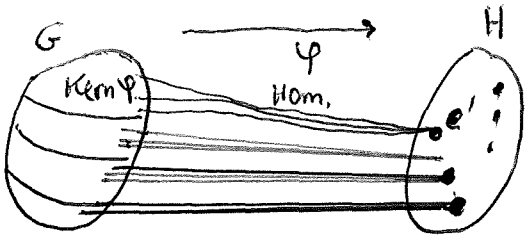
(i) $\varphi(e) = e'$

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$ für alle $g \in G$

(iii) Sei U Untergruppe von $(G,\circ)$.
Dann ist das Bild $\varphi(U) := \{\varphi(u) \mid u \in U\}$ Untergruppe von $(H,\circ)$

(iv) Sei $\operatorname{Kern}\varphi := \{g \in G \mid \varphi(g) = e'\}$. ($\operatorname{Kern}$ von φ).
Dann ist $\operatorname{Kern}\varphi$ ein Normalteiler von $(G,\circ)$.

(v) Es gilt
$$\varphi(a) = \varphi(b) \iff a \circ \operatorname{Kern}\varphi = b \circ \operatorname{Kern}\varphi.$$
Zwei Elemente besitzen also dasselbe Bild gdw sie in derselben Nebenklasse des Kerns von φ liegen.



Beweis

(i) $\varphi(e \circ e) = \varphi(e) = \varphi(e) \circ \varphi(e)$ Multiplikation mit $\varphi(e)^{-1}$ in H
↑ e ist neutrales Element. ↑ φ ist Hom. liefert $e' = \varphi(e)$.

(ii) $\varphi(\underbrace{g \circ g^{-1}}_{=e}) = \varphi(g) \circ \varphi(g^{-1})$ ↑ φ ist Hom. also ist $\varphi(g^{-1})$ zu $\varphi(g)$ invers.
$=e'$ nach (i)

(iii) Es gilt nach (i) $\varphi(e) = e'$, also ist $e' \in \varphi(U)$.
Seien $\varphi(a), \varphi(b) \in \varphi(U)$. Dann folgt $\varphi(a) \circ \varphi(b) = \varphi(\underbrace{a \circ b}_{\in U}) \in \varphi(U)$.
Ist $\varphi(a) \in \varphi(U)$, so folgt $\varphi(a)^{-1} \overset{(ii)}{=} \varphi(\underbrace{a^{-1}}_{\in U}) \in \varphi(U)$.

(iv) Es läßt sich leicht nachrechnen, daß $\operatorname{Kern}\varphi$ eine Untergruppe von $(G, \circ)$ ist.
Wir wenden das Normalteilerkriterium (Bem 8.4) an.
Sei $g \in G$, $u \in \operatorname{Kern}\varphi$. Dann folgt
$\varphi(g \circ u \circ g^{-1}) = \varphi(g) \circ \underbrace{\varphi(u)}_{=e' \text{ nach Def. des Kerns}} \circ \varphi(g^{-1}) \overset{(ii)}{=} \varphi(g) \circ \varphi(g)^{-1} = e'$,
also $g \circ u \circ g^{-1} \in \operatorname{Kern}\varphi$.

(v) Es gilt
$\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a) \circ \underbrace{\varphi(b)^{-1}}_{= \varphi(b^{-1}) \text{ nach (ii)}} = e' \Leftrightarrow a \circ b^{-1} \in \operatorname{Kern}\varphi$
$= \varphi(a \circ b^{-1})$

$\Leftrightarrow a \in \operatorname{Kern}\varphi \circ b \Leftrightarrow \operatorname{Kern}\varphi \circ a = \operatorname{Kern}\varphi \circ b$
↑ 2 Nebenklassen sind gleich, wenn sie ein gemeinsames Element besitzen (s. Bem 6.5)

$\Leftrightarrow a \circ \operatorname{Kern}\varphi = b \circ \operatorname{Kern}\varphi$.
↑ $\operatorname{Kern}\varphi$ ist nach (iv) Normalteiler.

§10 Der Homomorphiesatz für Gruppen

Ein wichtiges Hilfsmittel in der Gruppentheorie ist der Homomorphiesatz für Gruppen.

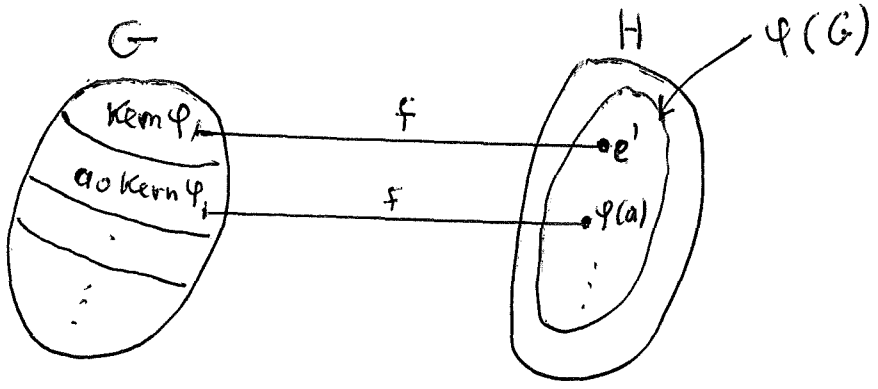
Satz 10.1 (Homomorphiesatz für Gruppen)

Es seien $(G,\circ)$ und $(H,\cdot)$ zwei Gruppen. Sei e' das neutrale Element von $(H,\cdot)$.
Ferner sei $\varphi: G \to H$ ein Gruppen-Homomorphismus.
Nach Bem 9.2(iii) ist $\varphi(G) := \{\varphi(g) \mid g \in G\}$ eine Untergruppe von $(H,\cdot)$.
Nach Bem 9.2(iv) ist der Kern $\operatorname{Kern}\varphi := \{g \mid g \in G,\ \varphi(G) = e'\}$
ein Normalteiler von $(G,\circ)$; also ist auch die Faktorgruppe $G/\operatorname{Kern}\varphi$ definiert.

Dann gilt:

$$f: G/\operatorname{Kern}\varphi \longrightarrow \varphi(G), \quad a\circ\operatorname{Kern}\varphi \overset{f}{\longmapsto} \varphi(a)$$

ist ein Gruppen-Isomorphismus.



Also ist $G/\operatorname{Kern}\varphi \cong \varphi(G)$.

Beweis

f ist wohldefiniert; d.h. die Zuordnungsvorschrift ist unabhängig von der Wahl des Repräsentanten der Nebenklasse des Kerns (nach Bem 9.2 (V 1)).

f ist injektiv (Verschiedene Nebenklassen haben verschiedene Bilder) nach Bem 9.2 (V).

f ist surjektiv, denn ein Element aus $\varphi(G)$ hat die Form $\varphi(g)$ mit $g \in G$ und $\varphi(g)$ besitzt bezüglich f offenbar g als Urbild.

f ist relationstreu, denn es gilt

$$f((a \circ \operatorname{Kern}\varphi) \circ (b \circ \operatorname{Kern}\varphi)) = \varphi(a \circ b) = \varphi(a) \cdot \varphi(b) =$$

(↑ Def. von f; ↑ φ ist Hom)

$= (a \circ b) \circ \operatorname{Kern}\varphi$ (Verknüpfung in der Faktorgruppe $(G/\operatorname{Kern}\varphi, \circ)$)

$= f(a \circ \operatorname{Kern}\varphi) \circ f(b \circ \operatorname{Kern}\varphi)$,

↑ Def. von f

Bsp 10.1

Es sei $G = \{e, g, \dots, g^{n-1}\}$ eine zyklische Gruppe der Ordnung n; also $g^n = e$ (neutrales Element) (S. Bem. 7.2)

Dann gilt: $g^i = e \Leftrightarrow n \mid i$ (*) (nach Bem 7.2)

Betrachte die Gruppe $(\mathbb{Z}, +)$.

Sei $\varphi: \mathbb{Z} \to G$ definiert durch $\varphi(z) = g^z$ f.a. $z \in \mathbb{Z}$.

Dann ist φ ein Gruppen-Homomorphismus, denn es gilt

$\varphi(z_1 + z_2) = g^{z_1+z_2} = g^{z_1} \circ g^{z_2} = \varphi(z_1) \circ \varphi(z_2)$ für alle $z_1, z_2 \in \mathbb{Z}$.

Offenbar ist φ surjektiv. Der Kern von φ ist $n\mathbb{Z}$, wegen (*).

Nach dem Homomorphiesatz für Gruppen folgt: $\mathbb{Z}/n\mathbb{Z} \cong G$.

In Beispiel 8.1 ist die Faktorgruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ genauer beschrieben.

Bsp 10.2

Wir betrachten die Faktorgruppe

$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}\} = \{0 \pmod n, \dots, (n-1) \bmod n\}$
↑ s. Bem d. 5

für $n = 15$:

Sei $\varphi : \mathbb{Z}_{15} \to \mathbb{Z}_{15}$ definiert durch $\varphi(a \pmod{15}) := 3a \pmod{15}$.

Dann ist φ ein Gruppenhomomorphismus, denn es gilt

$$\varphi(\underbrace{a \pmod{15} + b \pmod{15}}_{= (a+b) \pmod{15} \text{ (Addition in } \mathbb{Z}_{15})}) \overset{\text{↑ Def. von } \varphi}{=} 3(a+b) \pmod{15} = 3a \pmod{15} + 3b \pmod{15}$$
↑ Addition in $\mathbb{Z}_{15}$

$$= \varphi(a \pmod{15}) + \varphi(b \pmod{15})$$
↑ Def. von φ.

Es ist $\ker \varphi = \{0 \pmod{15}, 5 \pmod{15}, 10 \pmod{15}\}$.

Das Bild von φ ist $\varphi(\mathbb{Z}_{15}) = \{0 \pmod{15}, 3 \pmod{15}, 6 \bmod 15, 9 \pmod{15}, 12 \pmod{15}\}$.

Nach dem Homomorphiesatz für Gruppen folgt

$$\mathbb{Z}_{15}/\ker\varphi \cong \varphi(\mathbb{Z}_{15}).$$

Kap. 2 Ringe

§11 Ringe und Körper

Def. 11.1 (Ringe)

(i) Auf der Menge R seien zwei Verknüpfungen definiert, die üblicherweise mit $+$ und $\cdot$ bezeichnet werden.

Dann heißt $(R, +, \cdot)$ Ring, wenn gilt:

(i) $(R,+)$ ist eine kommutative Gruppe

(ii) $(R, \cdot)$ ist eine Halbgruppe (d.h. $\cdot$ ist assoziativ)

(iii) Es gelten die Distributivgesetze

$$a \cdot (b+c) = a \cdot b + a \cdot c,$$
$$(a+b) \cdot c = a \cdot c + b \cdot c$$

(wie üblich soll Punkt- vor Strichrechnung gehen, auf der ~~linken~~ rechten Seite der beiden Gleichungen kann also auf Klammern verzichtet werden)

Der Ring $(R, +, \cdot)$ heißt kommutativ, wenn $\cdot$ kommutativ ist.

0 bezeichne stets das neutrale Element der Gruppe $(R, +)$ (auch Null).

Besitzt der Ring $(R, +, \cdot)$ ein neutrales Element bzgl. $\cdot$, so wird dies i.a. mit 1 (Eins) bezeichnet (dann gilt also: $1 \cdot r = r \cdot 1 = r$ für alle $r \in R$).

(Anmerkung: Ein Ring hat höchstens eine Eins: $1 \cdot 1' = 1 = 1'$)

(ii) Sei $S \subseteq R$, $(R, +, \cdot)$ ein Ring.

Ist S bzgl. $+, \cdot$ ebenfalls ein Ring, so heißt S Unterring von $(R, +, \cdot)$ (analog wie bei Gruppen).

Bsp 11.1

(i) $(\mathbb{Z},+,\cdot)$ ist ein Ring mit Eins; kommutativ;

$(2\mathbb{Z},+,\cdot)$ ist ein Ring ohne Eins; kommutativ.

(ii) Sei $R:=\{0\}$; $0+0=0$; $0\cdot 0=0$. Dann ist $(R,+,\cdot)$ ein Ring (Nullring)

(iii) Sei $n\in\mathbb{N}$ und M_n die Menge aller $n\times n$-Matrizen mit Einträgen aus $\mathbb{R}$ (oder $\mathbb{Q}$).

Dann ist $(M_n,+,\cdot)$ ein Ring, der für $n>1$ nicht kommutativ ist.

Dabei bezeichne $+$ bzw. $\cdot$ die übliche Matrizenaddition bzw. Matrizenmultiplikation.

(iv) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ sind kommutative Ringe

(v) $(\mathbb{N},+,\cdot)$ ist kein Ring.

(vi) Sei $\mathbb{Z}[\sqrt{2}]:=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$.

Dann ist $(\mathbb{Z}[\sqrt{2}],+,\cdot)$ ein Ring mit der üblichen Verknüpfung reeller Zahlen.

Bem 11.1

Es sei $(R,+,\cdot)$ ein Ring. Dann gilt:

(i) $a\cdot 0=0\cdot a=0$ für alle $a\in R$

(ii) In $(R,+,\cdot)$ gelten die Vorzeichenrechenregeln

(a) $(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$; (b) $(-a)\cdot(-b)=a\cdot b$.

Beweis

(i) $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$

Dies ist eine Gleichung in der Gruppe $(R,+)$; addiert man $-(a\cdot 0)$, so folgt $0=a\cdot 0$. Analog ist $0\cdot a=0$.

(ii) (a) $(-a)\cdot b+a\cdot b=(-a+a)\cdot b=0\cdot b\overset{(i)}{=}0$, also $(-a)\cdot b$ ist zu ab invers.

(b) $(-a)(-b)=-a(-b)=-(-a\cdot b)=a\cdot b$

(a) wegen (a); $\overset{\text{s. Bem 3.3 (v)}}{=}$

Def. 11.2 (Einheiten)

Es sei $(R,+,\cdot)$ ein Ring mit $1 \in R$ und $\varepsilon \in R$. Dann:

ε Einheit von R :$\Leftrightarrow$ Existiert ein $\varepsilon' \in R$ mit $\varepsilon' \cdot \varepsilon = \varepsilon \cdot \varepsilon' = 1$.

(d.h. ε besitzt ein multiplikativer Inverses).

Bsp 11.2:

(i) Die Einheiten des Ringes $(\mathbb{Z},+,\cdot)$ sind ± 1.

(ii) Die Einheiten des Ringes $(\mathbb{Q},+,\cdot)$ sind alle $q \in \mathbb{Q}$ mit $q \neq 0$.

Bem 11.2 (Einheitengruppe)

Es sei $(R,+,\cdot)$ ein Ring mit $1 \in R$.

Dann bilden die Einheiten von R bzgl. $\cdot$ eine Gruppe.

Beweis

Sei E die Menge der Einheiten von R.

Offenbar ist $1 \in E$.

Ist $\varepsilon \in E$, so existiert ein $\varepsilon' \in R$ mit $\varepsilon \cdot \varepsilon' = \varepsilon' \cdot \varepsilon = 1$.

Dann ist ε zu ε' multiplikativ invers, und es folgt $\varepsilon' \in E$.

Offenbar ist dann $\varepsilon' = \varepsilon^{-1}$.

Seien $\varepsilon_1, \varepsilon_2 \in E$. Dann ist auch $\varepsilon_1 \cdot \varepsilon_2 \in E$, denn es gilt

$\varepsilon_1 \cdot \varepsilon_2 \cdot (\varepsilon_2^{-1} \cdot \varepsilon_1^{-1}) = 1$, [illegible] $\in E$.

Def 11.3 (Körper)

Es sei $(R,+,\cdot)$ Ring, $R \neq \{0\}$. Dann wird definiert:

$(R,+,\cdot)$ Körper :$\Leftrightarrow$ $(R \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe.

Bem 11.3

Die Einheitengruppe eines Körpers $(K,+,\cdot)$ ist $K \setminus \{0\}$.

(klar nach Def. 11.3)

Bem 11.4

Es sei $(K,+,\cdot)$ ein Körper; $a,b \in K$ mit $a \cdot b = 0$.

Dann ist $a = 0$ oder $b = 0$.

Gleichwertig: Ist $a \neq 0$ und $b \neq 0$, so ist auch $a \cdot b \neq 0$.

Sprechweise: Der Körper $(K,+,\cdot)$ ist nullteilerfrei.

Beweis Annn: $a \neq 0$. Dann gilt:

$$a \cdot b = 0 \Rightarrow \underbrace{a^{-1} \cdot a \cdot b}_{=b} = a^{-1} \cdot 0 = 0 \quad \text{, also } b = 0.$$

↑ Bem 11.1 ii).

Bsp 11.3

(i) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ sind Körper;
$(\mathbb{Z},+,\cdot)$, $(2\mathbb{Z},+,\cdot)$ keine Körper.

(ii) Sei $\mathbb{Z}_2 := \{0,1\}$.
Seien auf $\mathbb{Z}_2$ zwei Verknüpfungen $+$ und $\cdot$ definiert durch:

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

Dann läßt sich leicht nachrechnen:
$(\mathbb{Z}_2,+,\cdot)$ ist ein Körper.
(Nach Bsp. 4.1 ist $(\mathbb{Z}_2,+)$ eine Gruppe)

Bem 11.5

In einem Körper $(K, +, \cdot)$ gelten die bekannten Bruchrechenregeln.

Für $a \cdot b^{-1}$ schreibt man auch $\frac{a}{b}$ oder $a : b$, falls $b \neq 0$ ist.

Es gilt

$$\frac{a}{b} = \frac{a \cdot c}{b \cdot c} \quad ; \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} \; ;$$

$$\frac{a}{b} : \frac{c}{d} = \frac{a \cdot d}{b \cdot c} \quad ; \quad \frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm cb}{b \cdot d} \; .$$

Man beachte: Nach Bem 11.4 ist $b \cdot d \neq 0$, falls $b \neq 0$ und $b \neq 0$ ist.

Beweis:

Zum Beispiel gilt

$$\frac{a}{b} + \frac{c}{d} = a \cdot b^{-1} + c \cdot d^{-1} = ad\, b^{-1} d^{-1} + cb\, b^{-1} d^{-1}$$

↑ beachte: $\cdot$ ist kommutativ

$$= (ad + bc)\, b^{-1} d^{-1} = (ad + bc)\,(bd)^{-1} = \frac{ad + cb}{b \cdot d}$$

↑ Distributivgesetz

↑ Inversenbildung von Produkten in eine Gruppe, Bem 3.3 (iv); $\cdot$ ist kommutativ

Anmerkung: Die Bruchrechenregeln gelten nicht in sog. Schiefkörpern, bei denen auf die Kommutativität von $\cdot$ verzichtet wird.

§12 Ideale und Restklassenringe

In der Gruppentheorie wurden Normalteiler und Faktorgruppen eingeführt. In der Ringtheorie werden analoge Betrachtungen durchgeführt. Dabei werden Normalteiler ersetzt durch Ideale und die Bildung von Faktorgruppen durch die Bildung von Restklassenringen.

Def. 12.1 (Ideale)

Es sei $(R,+,\cdot)$ ein Ring und $\mathfrak{a} \subseteq R$. Dann wird definiert:

$\mathfrak{a}$ Ideal von $R :\Leftrightarrow$ (i) $\mathfrak{a}$ ist Untergruppe von $(R,+)$

(ii) $r \in R,\ a \in \mathfrak{a} \Rightarrow (r \cdot a \in \mathfrak{a}$ und $a \cdot r \in \mathfrak{a})$

(Idealeigenschaft)

(In kommutativen Ringen kann die Bedingung $a \cdot r \in \mathfrak{a}$ auch weggelassen werden)

Bsp 12.1

(i) Jeder Ring $(R,+,\cdot)$ besitzt die Ideale $\{0\}$ und R (triviale Ideale).

(ii) Sei $n \in \mathbb{N}$. Offenbar ist dann $n\mathbb{Z}$ Ideal von $(\mathbb{Z},+,\cdot)$

(iii) Es sei $(R,+,\cdot)$ ein kommutativer Ring, $r \in R$ und

$(r) := \{s \cdot r \mid s \in R\}$

Dann ist (r) ein Ideal von R (das von r erzeugte Hauptideal)

Für $(R,+,\cdot) = (\mathbb{Z},+,\cdot)$ erhält man als Spezialfall (ii').

Anmerkung (ohne Bew.): $(\mathbb{Z},+,\cdot)$ besitzt nur Hauptideale.

Def. 12.2 (Restklassenringe)

Es sei $(R,+,\cdot)$ ein kommutativer Ring und $\mathfrak{a}$ Ideal von R.
Dann ist $\mathfrak{a}$ Untergruppe der kommutativen Gruppe $(R,+)$;
also ist $\mathfrak{a}$ auch Normalteiler von $(R,+)$.
Dann ist auch die Faktorgruppe $(R/\mathfrak{a},+)$ definiert (s. §8).
Dabei ist $R/\mathfrak{a} := \{r+\mathfrak{a} \mid r\in R\}$ die Menge der (Links-)
Nebenklassen von $\mathfrak{a}$ in R.
Die Verknüpfung $+$ auf $R/\mathfrak{a}$ ist definiert durch

$$(r+\mathfrak{a}) + (r'+\mathfrak{a}) := (r+r') + \mathfrak{a} \quad \text{für alle } r,r'\in R.$$

($+$: neu definierte Verknüpfung auf $R/\mathfrak{a}$; $+$: Addition in R)

Beachte: Nach §8 ist das Verknüpfungsergebnis unabhängig von der Wahl der Repräsentanten der Nebenklassen.
Nun wird auf $R/\mathfrak{a}$ eine Multiplikation $\cdot$ definiert durch

$$(r+\mathfrak{a})\cdot(r'+\mathfrak{a}) := r\cdot r' + \mathfrak{a} \quad \text{für alle } r,r'\in R.$$

($\cdot$: neu definierte Verknüpfung auf $R/\mathfrak{a}$; $\cdot$: Multiplikation in R.)

Es gilt:

(i) Die Multiplikation $\cdot$ auf $R/\mathfrak{a}$ ist wohldefiniert;
d.h. das Verknüpfungsergebnis ist unabhängig von der Wahl der Repräsentanten (Sprechweise: wohldefiniert),

(ii) $(R/\mathfrak{a},+,\cdot)$ ist ein kommutativer Ring (Restklassenring von R nach $\mathfrak{a}$).

Beweis

(i) (Das Beweisschema ist ähnlich wie das von Satz 8.1 (i')).

Zu zeigen ist:

$$\left.\begin{aligned} r_1 + \mathfrak{a} &= r_1' + \mathfrak{a} \\ r_2 + \mathfrak{a} &= r_2' + \mathfrak{a} \end{aligned}\right\} \Rightarrow r_1 \cdot r_2 + \mathfrak{a} = r_1' \cdot r_2' + \mathfrak{a}.$$

Aus der linken Seite folgt:

$r_1' = r_1 + a_1$ für ein $a_1 \in \mathfrak{a}$,
$r_2' = r_2 + a_2$ für ein $a_2 \in \mathfrak{a}$

Es folgt weiter

$$r_1' \cdot r_2' = r_1 \cdot r_2 + \underbrace{\underbrace{r_1 a_2}_{\in \mathfrak{a}} + \underbrace{r_2 a_1}_{\in \mathfrak{a}} + \underbrace{a_1 \cdot a_1}_{\in \mathfrak{a}}}_{\in \mathfrak{a} \quad ((R,+) \text{ ist Gruppe})} \in r_1 \cdot r_2 + \mathfrak{a}.$$

(Ideal (Normalteiler)eigenschaft)

Da zwei Nebenklassen von $\mathfrak{a}$ gleich oder elementefremd sind und $r_1' \cdot r_2' \in r_1' r_2' + \mathfrak{a}$, $r_1' \cdot r_2' \in r_1 r_2 + \mathfrak{a}$ ist, folgt $r_1 \cdot r_2 + \mathfrak{a} = r_1' \cdot r_2' + \mathfrak{a}$.

(ii) Die Ringeigenschaften von $(R, +, \cdot)$ übertragen sich auf $(R/\mathfrak{a}, +', \cdot')$;
ZB ist $0 + \mathfrak{a}$ die Null in $(R/\mathfrak{a}, +', \cdot')$

$-(a + \mathfrak{a}) = (-a) + \mathfrak{a}$, da $(-a + \mathfrak{a}) + (a + \mathfrak{a}) = (-a + a) + \mathfrak{a} = 0 + \mathfrak{a}$
↑ Add. in $R/\mathfrak{a}$.

§ 13 Der Restklassenring $\mathbb{Z}/n\mathbb{Z}$

Es sei $n \in \mathbb{N}$ gegeben.

Dann ist $n\mathbb{Z}$ Ideal des Ringes $(\mathbb{Z}, +, \cdot)$ (s. Bsp 12.1 (iii))

Die Menge der Nebenklassen von $n\mathbb{Z}$ in $\mathbb{Z}$ ist

$\mathbb{Z}_n := \frac{\mathbb{Z}}{n\mathbb{Z}} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$ (s. Bsp. 8.1)

Dabei gilt: $a+n\mathbb{Z} = b+n\mathbb{Z} \Leftrightarrow n \mid (a-1) \Leftrightarrow Ex.\, \gamma \in \mathbb{Z}$ mit $b = a+\gamma n$.

Addition im Restklassenring $(\mathbb{Z}_n, +, \cdot)$:

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) := (a+b) + n\mathbb{Z}.$$

Multiplikation im Restklassenring $(\mathbb{Z}_n, +, \cdot)$:

$$(a+n\mathbb{Z}) \cdot (b+n\mathbb{Z}) := a \cdot b + n\mathbb{Z}.$$

Für $a+n\mathbb{Z}$ schreibt man auch $a \pmod n$.

Nullelement von $(\mathbb{Z}_n, +, \cdot)$: $0+n\mathbb{Z}$ $(= n\mathbb{Z})$.

Einselement von $(\mathbb{Z}_n, +, \cdot)$: $1+n\mathbb{Z}$.

$-(a+n\mathbb{Z}) = -a+n\mathbb{Z} = (n-a)+n\mathbb{Z}$.

<u>Bsp 13.1</u> In $\mathbb{Z}_6$ gilt $\underbrace{(2+6\mathbb{Z})}_{\neq \text{Null}} \cdot \underbrace{(3+6\mathbb{Z})}_{\neq \text{Null}} = 6+6\mathbb{Z} = 6\mathbb{Z} = \text{Null}$

Sprechweise: $\mathbb{Z}_6$ ist nicht nullteilerfrei

(Allgemein heißt ein Ring $(R, +, \cdot)$ nullteilerfrei, wenn gilt:
$a \neq 0, b \neq 0 \Rightarrow a \cdot b \neq 0$).

Bem 13.1

(i) Sei $n \in \mathbb{N}$ keine Primzahl, etwa $n = n_1 \cdot n_2$ mit $1 < n_1, n_2 < n$.

Dann gilt in $\mathbb{Z}_n$: $\underbrace{(n_1 + n\mathbb{Z})}_{\neq \text{Null}} \underbrace{(n_2 + n\mathbb{Z})}_{\neq \text{Null}} = n_1 \cdot n_2 + n\mathbb{Z} = \text{Null}$.

$\mathbb{Z}_n$ ist also nicht nullteilerfrei.

(ii) Ist p Primzahl, so ist $\mathbb{Z}_p$ nullteilerfrei.

Def 13.1

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

Bem 13.2

(i) $(\mathbb{Z}_n, +, \cdot)$ Integritätsbereich $\Leftrightarrow$ n Primzahl (nach Bem 13.1)

(ii) Jeder Körper ist nullteilerfrei, also auch Integritätsbereich (s. Bem 11.4.)

Bsp. 13.2

(i) $(\mathbb{Z}_3, +, \cdot)$ ist ein Körper; $2 \pmod 3$ ist zu sich selbst multiplikativ invers (denn es gilt $(2 \pmod 3)(2 \pmod 3) = 4 \pmod 3 = 1 \pmod 3$).

(ii) $(\mathbb{Z}_5, +, \cdot)$ ist ein Körper; $(4 \pmod 5)^{-1} = 4 \pmod 5$

$2 \pmod 5$ und $3 \pmod 5$ sind zueinander invers

(iii) Ist n keine Primzahl, so ist $(\mathbb{Z}_n, +, \cdot)$ kein Körper (nach Bem 13.2).
In §18 wird gezeigt: Ist p Primzahl, so ist $(\mathbb{Z}_p, +, \cdot)$ ein Körper

Bsp 13.3 In $(\mathbb{Z}_n, +, \cdot)$ gilt: $\underbrace{(1 + n\mathbb{Z}) + \ldots + (1 + n\mathbb{Z})}_{n\text{-mal}} = n + n\mathbb{Z} = \text{Null}$.

Ist in einem kommutativen Ring mit Eins $m \in \mathbb{N}$ minimal mit $\underbrace{1 + \ldots + 1}_{m\text{-mal}} = 0$, so heißt m die Charakteristik von R

Die Charakteristik von $(\mathbb{Z}_n, +, \cdot)$ ist also n.
Ex. ein solches m nicht, so wird die Charakteristik des Ringes als 0 definiert.

§14 Ring-Homomorphismen und der Homomorphiesatz für Ringe

Def. 14.1 (Ring-Homomorphismus)

Es seien $(R_1, +, \cdot)$ und $(R_2, +, \cdot)$ Ringe.
Eine Abbildung $\varphi: R_1 \to R_2$ heißt (Ring-) Homomorphismus, wenn gilt:

$\varphi(a+b) = \varphi(a) + \varphi(b)$ für alle $a, b \in R_1$ (d.h. φ ist relationstreu bzgl. $+$);
$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ für alle $a, b \in R_1$ (d.h. φ ist relationstreu bzgl. $\cdot$).

Ein bijektiver Ring-Homomorphismus heißt Ring-Isomorphismus.
Existiert ein Ring-Isomorphismus $\varphi: R_1 \to R_2$, so heißen $(R_1, +, \cdot)$ und $(R_2, +, \cdot)$ isomorph (in Zeichen: $R_1 \cong R_2$).

Bem 14.1

Jeder Ring-Homomorphismus $\varphi: R_1 \to R_2$ ist bzgl. $+$ ein Gruppenhomomorphismus.

Bsp 14.1

(1) Es sei $(R, +, \cdot)$ ein Ring.
Dann ist die Abbildung $\varphi: R \to R$ definiert durch $\varphi(r) = 0$ für alle $r \in R$ ein Ring-Homomorphismus.
Ferner ist die Abbildung $f: R \to R$ def. durch $f(r) = r$ für alle $r \in R$ ein Ring-Homomorphismus.

(ii) Betrachte den Ring $\mathbb{Z}[\sqrt{2}] := \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$

Sei $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ definiert durch

$\varphi(a+b\sqrt{2}) := a-b\sqrt{2}$ für alle $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

Dann ist φ ein Ring-Homomorphismus, denn es gilt:

$\varphi((a+b\sqrt{2})+(c+d\sqrt{2})) = \varphi((a+c)+(b+d)\sqrt{2}) = (a+c)-(b+d)\sqrt{2}$

(($\varphi(a+b\sqrt{2}) + \varphi(c+d\sqrt{2}) = (a-b\sqrt{2}) + (c-d\sqrt{2})$

und

$\varphi((a+b\sqrt{2})\cdot(c+d\sqrt{2})) = \varphi((ac+2bd)+(ad+bc)\sqrt{2}) = (ac+2bd)-(ad+bc)\sqrt{2}$

(($\varphi(a+b\sqrt{2})\cdot\varphi(c+d\sqrt{2}) = (a-b\sqrt{2})(c-d\sqrt{2}) = (ac+2bd)-(ad+bc)\sqrt{2}$.

Offenbar ist φ bijektiv; also ist φ auch Ring-Isomorphismus.

(iii) Sei $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ definiert durch $\varphi(z) := 2z$ für alle $z \in \mathbb{Z}$.

Dann ist φ kein Ring-Homomorphismus, denn es gilt

$\varphi(z_1 \cdot z_2) = 2z_1 z_2$, $\varphi(z_1)\cdot\varphi(z_2) = 2z_1 \cdot 2 \cdot z_2$.

Im Fall $z_1 \neq 0$ und $z_2 \neq 0$ ist also $\varphi(z_1 \cdot z_2) \neq \varphi(z_1)\cdot\varphi(z_2)$.

Beachte: φ ist bzgl. $+$ ein Gruppen-Homomorphismus (analog zu Bsp. 9.2).

Bem 14.2

Es sei $\varphi : R_1 \to R_2$ ein Ring-Homomorphismus.

Sei $\operatorname{Kern}\varphi := \{r_1 \in R_1 \mid \varphi(r_1) = 0\}$ (Kern von φ).

(i) Dann ist $\operatorname{Kern}\varphi$ Ideal von R_1

(ii) Das Bild $\varphi(R_1)$ ist Unterring von $(R_2, +, \cdot)$.

Beweis

(i) Da φ bzgl. $+$ ein Gruppen-Homomorphismus ist, ist
$\operatorname{Kern}\varphi$ Normalteiler von $(R_1, +, \cdot)$ (s. Bem 9.2 (iv))
$\operatorname{Kern}\varphi$ erfüllt die Idealeigenschaft, denn es gilt:
Sei $r_1 \in R_1$, $a \in \operatorname{Kern}\varphi$. Dann folgt
$\varphi(r_1 \cdot a) = \varphi(r_1) \cdot \underbrace{\varphi(a)}_{=0} = 0$ (also $r_1 \cdot a \in \operatorname{Kern}\varphi$; analog $a \cdot r_1 \in \operatorname{Kern}\varphi$.
$\uparrow$ Bem 11.1 (i)

(ii) Nach Bem. 9.2 (iii) ist $\varphi(R_1)$ Untergruppe von $(R_2, +, \cdot)$.
Es ist leicht zu zeigen, daß $\varphi(R_1)$ auch Unterring von $(R_2, +, \cdot)$ ist.

Satz 14.1 (Homomorphiesatz für Ringe)
Es seien $(R_1, +, \cdot)$ und $(R_2, +, \cdot)$ Ringe;
Sei $\varphi: R_1 \to R_2$ ein Ring-Homomorphismus.
Dann ist $\operatorname{Kern}\varphi := \{ r_1 \in R_1 \mid \varphi(r_1) = 0 \}$ ein Ideal von R_1 (nach Bem 14.2);
$\varphi(R_1) := \{ \varphi(r_1) \mid r_1 \in R_1 \}$ ein Unterring von $(R_2, +, \cdot)$ (nach Bem 14.2).
Bzgl. $+$ ist φ ein Gruppen-Homomorphismus.
Nach dem Homomorphie-Satz für Gruppen (Satz 10.1) gilt:

$$f: \frac{R_1}{\operatorname{Kern}\varphi} \longrightarrow \varphi(R_1)$$
$$r_1 + \operatorname{Kern}\varphi \overset{f}{\longmapsto} \varphi(r_1)$$

ist ein Gruppen-Isomorphismus.

Darüber hinaus gilt: (Homomorphie-Satz für Ringe)
f ist ein Ring-Isomorphismus.
Also ist $\frac{R_1}{\operatorname{Kern}\varphi} \cong \varphi(R_1)$. (Ring-Isomorphie).

Beweis

Es ist nur zu zeigen: f ist relationstreu bzgl. $\circ$.

Es gilt

$$f\Big(\underbrace{r_1 + \operatorname{Kern}\varphi) \circ (r_1' + \operatorname{Kern}\varphi)}_{= r_1 \circ r_1' + \operatorname{Kern}\varphi \text{ (Multiplikation im Restklassenring } R_1/\operatorname{Kern}\varphi)}\Big) = \varphi(r_1 \circ r_1') =$$

$\uparrow$ Definition von f

$$= \varphi(r_1) \circ \varphi(r_1') = f(r_1 + \operatorname{Kern}\varphi) \circ f(r_1' + \operatorname{Kern}\varphi)$$

$\uparrow$ φ ist ein Ring-Homomorphismus; $\uparrow$ Def. von f

$\square$

Kap. 3 Ganzzahlige Kongruenzen

§15 Ganzzahlige Kongruenzen

Def. 15.1 (Ganzzahlige Kongruenz)

Es sei $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann wird definiert:

$$a \equiv b \pmod{n} :\Leftrightarrow n \mid (a-b) \text{ in } \mathbb{Z}$$

Bem 15.1

Nach §13 gilt:

$$a \equiv b \pmod{n} \Leftrightarrow a \pmod{n} = b \pmod{n}.$$

Jeder ganzzahligen Kongruenz $a \equiv b \pmod{n}$ entspricht also eine Gleichung im Restklassenring $(\mathbb{Z}_n, +, \cdot)$.

Bem 15.2 (Kongruenzen)

Es sei $(R, +, \cdot)$ ein kommutativer Ring; α Ideal von R und $a, b \in R$.

Dann wird definiert:

$$a \equiv b \pmod{\alpha} :\Leftrightarrow a + \alpha = b + \alpha.$$

Im Fall $(R, +, \cdot) = (\mathbb{Z}, +, \cdot)$ und $\alpha = n\mathbb{Z}$ erhält man als Spezialfall Def. 15.1.

In diesem Kapitel 3 betrachten wir nur ganzzahlige Kongruenzen und nennen sie einfach Kongruenzen.

Bem 15.3

(i) Stets gilt $a \equiv a \pmod n$, und $\left(a \equiv b \pmod n \Rightarrow b \equiv a \pmod n\right)$

(ii) Kongruenzen dürfen addiert und multipliziert werden, und mit einer Konstanten multipliziert werden.

$$\left.\begin{aligned} a_1 &\equiv a_2 \pmod n \\ b_1 &\equiv b_2 \pmod n \end{aligned}\right\} \Rightarrow \begin{cases} a_1 + b_1 \equiv a_2 + b_2 \pmod n \\ a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod n, \end{cases}$$

und $a_1 \cdot c \equiv a_2 \cdot c \pmod n$ für ein $c \in \mathbb{Z}$.

(iii) In einer Kongruenz darf ein Summand oder Faktor ersetzt werden durch ein dazu kongruentes Element.

ZB gilt: $\left.\begin{aligned} 5 \cdot 3 &\equiv 7 \pmod 8 \\ 11 &\equiv 3 \pmod 8 \end{aligned}\right\} \Rightarrow 5 \cdot 11 \equiv 7 \pmod 8$

Beweis

(i) trivial nach Def 15.1 (Def. der ganzzahligen Kongruenz)

(ii) und (iii): Nach Bem 15.1 können Kongruenzen durch Gleichungen im Restklassenring ersetzt werden. Die Behauptung folgt dann aus der Wohldefiniertheit der Verknüpfungen im Restklassenring (s. Def. 12.2).

Bem 15.4

In jeder Restklasse mod n gibt es genau einen Repräsentanten i mit $0 \leq i \leq n-1$.

In einer Kongruenz mod n kann also jede Zahl ersetzt werden durch eine Zahl i mit $0 \leq i \leq n-1$.

Bsp 15.1

(i) $2 \equiv 9 \pmod 7$
$-1 \equiv 41 \pmod 7$
$-2 \equiv 9 \cdot 41 \pmod 7$ (Multiplikation)
$1 \equiv 50 \pmod 7$ (Addition)

(ii) $5 \cdot 2 \equiv 2 \cdot 2 \pmod 6$ (in dieser Kongruenz darf nicht gekürzt werden)
$5 \not\equiv 2 \pmod 6$

(iii) $x^2 \equiv 2 \pmod 5$ ist nicht lösbar (d.h. es gibt kein $x_0 \in \mathbb{Z}$ mit $x_0^2 \equiv 2 \pmod 5$)

Durch Einsetzen ergibt sich, daß 0, 1, 2, 3, 4 keine Lösungen sind.
Die Behauptung folgt dann nach Bem 15.4.

(iv) $x^2 \equiv a \pmod 4$ ist lösbar gdw $a \equiv 0 \pmod 4$ oder $a \equiv 1 \pmod 4$
Es gilt $0^2 \equiv 0 \pmod 4$, $1^2 \equiv 1 \pmod 4$, $2^2 \equiv 0 \pmod 4$, $3^2 \equiv 1 \pmod 4$. i.V.

(v) Eine ganze Zahl der Form $3+4n$ $(n \in \mathbb{Z})$ ist nicht Summe zweier ganzzahliger Quadrate.

Beweis: Annahme $3+4n = a^2+b^2$.
Dann folgt: $3 \equiv a^2+b^2 \pmod 4$.
Nach (iv) kann aber a^2+b^2 nur kongruent $0, 1, 2 \pmod 4$ sein.

(vi) $10 \equiv 1 \pmod 3$, also auch $10^r \equiv 1 \pmod 3$ (Multiplikation von Kongruenzen)
und $a \cdot 10^r \equiv a \pmod 3$

Analog gilt $10 \equiv 1 \pmod 9$, also auch $a \cdot 10^r \equiv a \pmod 9$
Ferner ist $10 \equiv -1 \pmod{11}$, r-fache Multiplikation liefert
$10^r \equiv 1 \pmod{11}$, falls r gerade
$10^r \equiv -1 \pmod{11}$, falls r ungerade

§16 Rechenproben

Bem 16.1 (Dreierprobe)

Sei $n \in \mathbb{N}$, $a = a_0 + a_1 \cdot 10 + \dots + a_r \cdot 10^r$ mit $0 \le a_i < 9$ für $i = 0, \dots, r$ und $a_r \neq 0$.

Dann sind die a_i die Ziffern von n im Dezimalsystem.

Es bezeichne $q(n) := a_0 + \dots + a_r$ die Quersumme von n.

Aus Bsp 15.1 (vi) folgt:

(i) $n \equiv q(n) \pmod 3$

Aus (i) folgt

(ii) $3 \mid n \iff 3 \mid q(n)$ (einfache Dreierprobe)

(iii) $n = n_1 + n_2 \Rightarrow q(n) \equiv q(n_1) + q(n_2) \pmod 3$.

$n = n_1 \cdot n_2 \Rightarrow q(n) \equiv q(n_1) \cdot q(n_2) \pmod 3$.

Dreierprobe: Ist $q(n) \equiv q(n_1) + q(n_2) \pmod 3$ falsch, so ist auch $n = n_1 + n_2$ falsch.

Ist $q(n) \equiv q(n_1) \cdot q(n_2) \pmod 3$ falsch, so ist auch $n = n_1 \cdot n_2$ falsch.

Ist $q(n) \equiv q(n_1) \pm q(n_2) \pmod 3$ richtig, so läßt sich keine Aussage über die Gültigkeit der Gleichung $n = n_1 \pm n_2$ treffen; klar ist dann nur, daß die Differenz $n - (n_1 \pm n_2)$ Vielfaches von 3 ist.

Bsp 16.1

Die Dreierprobe liefert, daß die Gleichung $71 \cdot 82 = 5824$ falsch ist, denn es gilt: $(7+1) \cdot (8+2) \equiv 2 \cdot 1 \not\equiv \underbrace{5+8+2+4}_{\equiv 1 \pmod 3} \pmod 3$

usw. (Ergänzung: Es gilt $71 \cdot 82 = 5822$, also ist $71 \cdot 82 - 5824 (= -2)$ nicht Vielfaches von 3.

Bem 16.2 (Neunerprobe)

Analog zu Bem 16.1 gilt:

Ist $q(n)$ die Quersumme von n, so folgt wegen $10 \equiv 1 \pmod 9$:

(i) $n \equiv q(n) \pmod 9$

und weiter

(ii) $9 \mid n \Leftrightarrow 9 \mid q(n)$ (einfache Neunerprobe)

(iii) $n = n_1 + n_2 \Rightarrow q(n) \equiv q(n_1) + q(n_2) \pmod 9$

$n = n_1 \cdot n_2 \Rightarrow q(n) \equiv q(n_1) \cdot q(n_2) \pmod 9$

Neunerprobe: Ist $q(n) \equiv q(n_1) \pm q(n_2) \pmod 9$ falsch, so ist auch $n = n_1 \pm n_2$ falsch.

Ist $q(n) \equiv q(n_1) \pm q(n_2) \pmod 9$ richtig, so läßt sich keine Aussage über die Gültigkeit der Gleichung $n = n_1 \pm n_2$ treffen; klar ist nur, daß $n - (n_1 \pm n_2)$ Vielfaches von 9 ist.

Läßt sich mit der Dreierprobe nachweisen, daß eine Gleichung falsch ist, so auch mit der Neunerprobe.

Bsp 16.2

Die Neunerprobe liefert, daß die Gleichung $71 \cdot 82 = 5828$ falsch ist, denn es gilt $\underbrace{(7+1)}_{\equiv 8} \cdot \underbrace{(8+2)}_{\equiv 1} \not\equiv \underbrace{5+8+2+8}_{\equiv 5} \pmod 9$.

Mit Hilfe der Dreierprobe läßt sich nicht entscheiden, ob $71 \cdot 82 = 5828$ richtig ist, denn es gilt

$$\underbrace{(7+1)}_{\equiv 2}\underbrace{(8+2)}_{\equiv 1} \equiv \underbrace{(5+8+2+8)}_{\equiv 2} \pmod 3.$$

Bem 16.3 (11-er Probe)

Sei $n \in \mathbb{N}$, $a = a_0 + a_1 \cdot 10 + \dots + a_r \cdot 10^r$ mit $0 \le a_i \le 9$ für $i = 0, \dots, r$; $a_r \neq 0$.

Es bezeichne $\bar{q}(n) = a_0 - a_1 + a_2 - \dots (-1)^{r+1} \cdot a_r$

die alternierende Quersumme von n,

Aus Beispiel 15.1 (VII) folgt: $10^r \equiv (-1)^r \pmod{11}$, also

(i) $n \equiv \bar{q}(n) \pmod{11}$.

Hieraus folgt weiter

(ii) $11 \mid n \iff 11 \mid \bar{q}(n)$ (einfache 11-er Probe)

(iii) $n = n_1 \pm n_2 \Rightarrow \bar{q}(n) \equiv \bar{q}(n_1) \pm \bar{q}(n_2) \pmod{11}$.

11-er Probe: Ist $\bar{q}(n) \equiv \bar{q}(n_1) \pm \bar{q}(n_2) \pmod{11}$ falsch,

so ist auch $n = n_1 \pm n_2$ falsch.

Ist $\bar{q}(n) = \bar{q}(n_1) \pm \bar{q}(n_2)$ richtig, so läßt sich keine

Aussage über die Gültigkeit der Gleichung $n = n_1 \pm n_2$

treffen; Klar ist nur, daß $n - (n_1 \pm n_2)$ Vielfaches von 11 ist.

Bsp 16.3 $71 \cdot 82 = 5824$ ist falsch, denn es gilt

$$\underbrace{(1-7)}_{\equiv 4} \cdot \underbrace{(2-8)}_{\equiv 7} \not\equiv \underbrace{(4-2+8-5)}_{\equiv 5} \pmod{11}$$

Bem 16.4 Wird eine Gleichung mit Hilfe der Neuner- und 11-er Probe überprüft, so wird ein Fehler erkannt mit der Wahrscheinlichkeit $\frac{98}{99}$ (der Fehler ist nicht Vielfaches von $9 \cdot 11 = 99$).

Bsp 16.4 Die Gleichung $71 \cdot 82 = 5821$ ist falsch.

Zum Nachweis kann die Dreier-, Neuner- oder 11-er Probe verwendet werden.

Man kann aber auch mod 2 rechnen oder mod 5 oder mod 10.

§17 Lineare Kongruenzen

Bem 17.1

Sei $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann gilt:

(i) $a \cdot X \equiv 1 \pmod n$ lösbar $\Leftrightarrow ggT(a,n) = 1$.

Sind x_1, x_2 zwei Lösungen, so gilt $x_1 \equiv x_2 \pmod n$

(d.h. die Lösung ist mod n eindeutig bestimmt.)

(ii) $aX \equiv b \pmod n$ lösbar $\Leftrightarrow$ $ggT(a,n) \mid b$.

Beweis

(i)

$\Rightarrow$: Sei X_0 Lösung von $a \cdot X \equiv 1 \pmod n$, also $a \cdot X_0 \equiv 1 \pmod n$

Nach Def. der Kongruenz existiert ein $\gamma \in \mathbb{Z}$ mit

$\underbrace{a \cdot X_0 - \gamma n}_{\text{ist Vielfaches von } ggT(a,n)} = 1$; also folgt $ggT(a,n) = 1$.

$\Leftarrow$: (Beachte: Der Beweis ist konstruktiv, ererlaubt also die Bestimmung einer Lösung)

Man verwende den Euklidischen Algorithmus.

Da $ggT(a,n) = 1$ ist, existieren $\gamma, \mu \in \mathbb{Z}$ mit

$$\gamma a + \mu n = 1.$$

Es folgt $\gamma \cdot a \equiv 1 \pmod n$,

also ist γ Lösung von $aX \equiv 1 \pmod n$.

Eindeutigkeit: Sind X_1 und X_2 Lösungen von $aX \equiv 1 \pmod n$, so ist $aX_1 - aX_2 \equiv a(X_1 - X_2) \equiv 0 \pmod n$. Wegen $ggT(a,n) = 1$ folgt $n \mid (X_1 - X_2)$.

(Beachte: γ läßt sich mit Hilfe des Euklidischen Algorithmus schnell berechnen)

(ii) $\Rightarrow$: Der Beweis erfolgt analog zu dem in (i).

$\Leftarrow$: Analog zu (i) existiert ein $x_0 \in \mathbb{Z}$ mit

$$a \cdot x_0 \equiv ggT(a,n) \pmod{n}.$$

Wegen $ggT(a,n) \mid b$ existiert ein $\mu \in \mathbb{Z}$ mit $b = \mu \cdot ggT(a,n)$.

Dann gilt: $x_0 \cdot \mu$ ist Lösung von $a \cdot x \equiv b \pmod{n}$.

Bsp 17.1

(i) $3x \equiv 1 \pmod{11}$ ist lösbar, da $ggT(3,11) = 1$. (Bem 17.1(ii))

Durch Probieren findet man eine Lösung: $x = \not{0}, \not{1}, \not{2}, \not{3}, 4$.

Zu probieren sind nur die Zahlen $0, 1, \dots, 10$.

Ist der Modul groß, so ist das im Beweis von Bem 17.1 (i) beschriebene Verfahren mit Hilfe des Euklidischen Algorithmus (wesentlich) schneller.

In diesem Fall erhält man:

$$\boxed{11} = 3 \cdot \boxed{3} + \underline{2} \quad \text{I}$$

$$\boxed{3} = 1 \cdot \boxed{2} + \underline{1} \quad \text{II}$$

$$2 = 2 \cdot \boxed{1} + 0 \quad \text{III}$$

beachte: Der Letzte von 0 verschiedene Rest, also 1, ist der $ggT(11,3)$.

Dies liefert $1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (11 - 3 \cdot 3) =$

($1 = 3 - 1 \cdot 2$: Gleichung II; 2 ersetzen; $= 3 - 1 \cdot (11 - 3 \cdot 3)$: Gleichung I)

$$= \underbrace{4 \cdot 3 - 1 \cdot 11}$$

Linearkombination von 3 und 11

Modulo 11 erhält man: $4 \cdot 3 \equiv 1 \pmod{11}$; also 4 als Lösung.

Die Gesamtheit aller Lösungen ist $\{4 + 11 \cdot z \mid z \in \mathbb{Z}\}$.

(ii) $3X \equiv 5 \pmod{11}$ ist lösbar nach Bem 17.1 (ii).

Nach (i) ist 4 Lösung von $3 \cdot X \equiv 1 \pmod{11}$, also

$$3 \cdot 4 \equiv 1 \pmod{11}.$$

Multiplikation mit 5 liefert

$$3 \cdot (4 \cdot 5) \equiv 5 \pmod{11},$$

also ist $4 \cdot 5$ ($\equiv 7$) Lösung von $3X \equiv 5 \pmod{11}$.

Bsp 17.2

$7 \cdot X \equiv 1 \pmod{11}$ ist lösbar, da $ggT(7,11) = 1$.

Durch Probieren erhält man 8 als Lösung.

Mit Hilfe des Euklidischen Algorithmus ergibt sich:

$11 = 1 \cdot 7 + 4$	I	Der Divisionsrest in III, also 1
$7 = 1 \cdot 4 + 3$	II	ist der $ggT(11,7)$.
$4 = 1 \cdot 3 + 1$	III	
$3 = 3 \cdot 1 + 0$		

Stelle 1 dar als Linearkombination von 7 und 4; verwende dabei die Gleichungen III, II, I: Es gilt

$1 = 4 - 1 \cdot 3$ (Gleichung III)

$= 4 - 1 \cdot (7 - 4)$ (ersetze 3 mit Hilfe von Gleichung II)

$= (11 - 7) - 1(7 - (11 - 7))$ (ersetze 4 mit Hilfe von Gleichung I)

$= 2 \cdot 11 - 3 \cdot 7$ (dies ist die gesuchte Linearkombination von 7 und 11.

Also folgt $7 \cdot (-3) \equiv 1 \pmod{11}$, also ist -3 eine Lösung (beachte: $8 \equiv -3 \pmod{11}$).

Achtung: In der obigen Rechnung sollte man Summen oder Produkte nicht vorzeitig ausrechnen (z.B. $7 - 4$ nicht durch 3 ersetzen), weil sonst nicht mehr klar wird, welche Zahl mit Hilfe welche Gleichung ersetzt wird.

§18 Kongruenzen und Restklassenringe

Nach Bem 15.1 gilt

$$a \equiv b \pmod n \iff a \pmod n = b \pmod n.$$

Jeder ganzzahligen Kongruenz $a \equiv b \pmod n$ entspricht also eine Gleichung im Restklassenring $(\mathbb{Z}_n, +, \cdot)$.

Aussagen über Kongruenzen können also in Aussagen über Restklassen umformuliert werden und umgekehrt.

Bem 18.1 (Einheiten im Restklassenring)

Die Restklasse $a \pmod n$ ist Einheit im Restklassenring $(\mathbb{Z}_n, +, \cdot)$ gdw $ggT(a,n) = 1$ ist.

Erinnerung: Nach Def. 11.2 heißt $a \pmod n$ Einheit von $(\mathbb{Z}_n, +, \cdot)$, wenn $a \pmod n$ ein Inverses bzgl. der Multiplikation besitzt. Die Einheiten von $(\mathbb{Z}_n, +, \cdot)$ bilden eine multiplikative Gruppe (Einheitengruppe) nach Bem 11.2.

Beweis

$a \cdot x_0 \equiv 1 \pmod n$ ist gleichwertig mit

$$a \cdot x_0 \pmod n = a \pmod n \cdot x_0 \pmod n = 1 \pmod n$$
$$\uparrow \text{ Multiplikation im Restklassenring}$$

Ferner ist $a \cdot x \equiv 1 \pmod n$ lösbar gdw $ggT(a,n) = 1$ ist (Bem 17.1 (i)).

Zusammen folgt die Behauptung.

Bem 18.2 (siehe auch Bsp 13.2.(iii.1))

$(\mathbb{Z}_n, +, \cdot)$ Körper $\Leftrightarrow$ n Primzahl.

Beweis

Nach Def. ist $(\mathbb{Z}_n, +, \cdot)$ Körper gdw jedes Element $a \pmod n \neq$ Null ein multiplikatives Inverses besitzt.

Also folgt die Behauptung aus Bem. 18.1

Bsp 18.1

In $(\mathbb{Z}_7, +, \cdot)$ sind $1 \pmod 7$, $1 \pmod 7$;
$-1 \pmod 7$, $-1 \pmod 7$; (bzw. $6 \pmod 7$, $6 \pmod 7$))
$2 \pmod 7$, $4 \pmod 7$;
$3 \pmod 7$, $5 \pmod 7$.

jeweils zueinander invers.

Bem 18.3 (prime Restklassen)

(i) Sei $a \in \mathbb{Z}$ und $n \in \mathbb{N}$.

$a \pmod n$ heißt prime Restklasse mod n, falls $ggT(a, n) = 1$ ist.

(Anmerkung: Die Definition ist sinnvoll, denn es gilt:

$$a \equiv b \pmod n \Rightarrow ggT(a, n) = ggT(b, n)$$ [Leicht nachzurechnen])

Nach Bem 18.1 sind die primen Restklassen mod n genau die Einheiten von $(\mathbb{Z}_n, \cdot)$.

Die Einheitengruppe von $(\mathbb{Z}_n, \cdot)$ heißt auch prime Restklassengruppe mod n.

(ii) Die Abbildung $\varphi: \mathbb{N} \to \mathbb{N}$ definiert durch

$\varphi(n) :=$ Anzahl aller natürlichen Zahlen $\leq n$, die zu n teilerfremd sind

heißt Eulersche φ-Funktion.

Nach (i) ist also $\varphi(n)$ die Anzahl der Einheiten von $(\mathbb{Z}_n, \cdot)$.

Bem 18.4 (Eulersche φ-Funktion)

Sei p Primzahl. Dann gilt:

(i) $\varphi(p) = p-1$ (Jede der Zahl $1, \dots, p-1$ ist zu p teilerfremd)

(ii) $\varphi(p^k) = p^{k-1}(p-1)$

(iii) $\varphi(n_1 \cdot n_2) = \varphi(n_1) \cdot \varphi(n_2)$, falls $\operatorname{ggT}(n_1, n_2) = 1$ ist.

Also: Ist die Primfaktorzerlegung von n bekannt, so läßt sich $\varphi(n)$ mit Hilfe von (i), (ii), (iii) leicht ausrechnen.

Beweis

(i) ist ein Spezialfall von (ii)

(ii): Betrachte die Zahlen

$$1 \quad 2 \quad 3 \quad \cdots \quad p \quad \cdots \quad 2 \cdot p \quad \cdots \quad p^{k-1} \cdot p.$$

Unter diesen Zahlen sind p^{k-1} Zahlen Vielfaches von p; die übrigen sind zu p teilerfremd.

Also ist $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

(iii) Seien P_1, P_2, P die primen Restklassengruppen von $(\mathbb{Z}_{n_1}, \cdot)$, $(\mathbb{Z}_{n_2}, \cdot)$, $(\mathbb{Z}_{n_1 \cdot n_2}, \cdot)$.

Dann ist $|P_1| = \varphi(n_1)$, $|P_2| = \varphi(n_2)$, $|P| = \varphi(n_1 \cdot n_2)$.

Es bezeichne $P_1 \times P_2 := \{(a \pmod{n_1}, b \pmod{n_2}) \mid a \pmod{n_1} \in P_1, b \pmod{n_2} \in P_2\}$ das Cartesische Produkt von P_1 und P_2.

Dann ist $|P_1 \times P_2| = \varphi(n_1)\cdot\varphi(n_2)$.

Zu zeigen ist also: $|P| = |P_1 \times P_2|$

Die Abbildung $f : P \to P_1 \times P_2$ sei definiert durch

$$f(a \pmod{n_1 n_2}) := (a \pmod{n_1},\ b \pmod{n_2}).$$

Dann folgt die Behauptung, wenn f bijektiv ist.
Leicht nachzurechnen ist, daß f injektiv ist.
Nach dem chinesischen Restsatz ist f auch surjektiv (s. § 20).

Bsp 18.2

(i) $\varphi(4) = 2$ (↑ Bem 18.4(ii)), $\varphi(5) = 4$ (↑ Bem 18.4(i)), $\varphi(20) = \varphi(2^2 \cdot 5) = \varphi(2^2)\cdot\varphi(5) = 8$ (↑ Bem 18.4(iii)).

(ii) $\varphi(8 \cdot 49) = \varphi(8)\cdot\varphi(49) = 4 \cdot 7 - 6$.

(iii) $\varphi(56) = \varphi(8)\cdot\varphi(7) = 4 \cdot 6 = 24$;

$\varphi(4) = 2,\ \varphi(14) = \varphi(2)\cdot\varphi(7) = 1 \cdot 6$;

also $\varphi(4)\cdot\varphi(14) = 12$ ≠ $\varphi(\underbrace{4 \cdot 14}_{=56}) = 24$ (beachte: $ggT(4,14) \neq 1$)

(iv) $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\cdot\varphi(5^2) = (2-1)\cdot(5\cdot 4) = 40$

Natürlich kann man $\varphi(100)$ auch direkt bestimmen, in dem man die Anzahl aller natürlichen < 100, die zu 100 teilerfremd sind, bestimmt:

1, ~~2~~, 3, ~~4~~, ~~5~~, ~~6~~, 7, ~~8~~, 9, ~~10~~, 11, ~~12~~, 13, ... , ~~96~~, 97, ~~98~~, 99.

Man erhält 40 Zahlen.

§19 Die Sätze von Euler und Fermat

Satz 19.1

Es bezeichne φ die Eulersche φ-Funktion (s. Bem 18.3 (iii))

(i) (Euler):

Sei $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $ggT(a,n) = 1$. Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

(ii) (Fermat)

Sei p eine Primzahl, $a \in \mathbb{Z}$, $p \nmid a$. Dann gilt

$$a^{p-1} \equiv 1 \pmod{p}.$$

Beweis

(ii) ist ein Spezialfall von (i)

(i): Die Kongruenz läßt sich zu einer Gleichung im Restklassenring umschreiben:

$$a^{\varphi(n)} \pmod{n} = \big(a \pmod{n}\big)^{\varphi(n)} = 1 \pmod{n}$$

↑ Multiplikation im Restklassenring $(\mathbb{Z}_n, +, \cdot)$.

Wegen $ggT(a,n) = 1$ ist dies eine Gleichung in der Einheitengruppe von $(\mathbb{Z}_n, +, \cdot)$, diese besitzt die Ordnung $\varphi(n)$ (s. Bem 18.3).

Nun folgt die Behauptung aus der folgenden allgemeinen Aussage:

Sei $(G, \circ)$ eine Gruppe der Ordnung n; e das neutrale Element und $g \in G$. Dann folgt: $g^n = e$ (s. Bem 7.2).

Bsp 19.1

(i) Nach Euler gilt $23^{42} \equiv 1 \pmod{49}$, beachte $\varphi(49) = \varphi(7^2) = 7 \cdot 6 = 42$.

(ii) $27^{29} \equiv 27 \cdot \underbrace{27^{28}}_{\equiv 1 \text{ (Fermat)}} \equiv 27 \pmod{29}$ (beachte: 29 ist Primzahl)

(iii) Es gilt $\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$;

$$7^{34} \equiv \underbrace{(7^8)^4}_{\equiv 1 \text{ (Euler)}} \cdot 7^2 \equiv 49 \equiv 4 \pmod{15}.$$

Bem 19.1

Sei p eine Primzahl, $a \in \mathbb{Z}$, [illegible]. Dann folgt

$$a^p \equiv a \pmod{p}$$

Im Fall $a \equiv 0 \pmod{p}$ ist dies unmittelbar klar; im Fall $a \not\equiv 0 \pmod{p}$ folgt die Behauptung aus dem Satz von Fermat.

§20 Primitivwurzeln und der Chinesische Restsatz

Bem 20.1 (Primitivwurzeln) (ohne Beweis)

Es sei p eine Primzahl.

Dann existiert im Restklassenring $(\mathbb{Z}_p, +, \cdot)$ ein Element $g \pmod p$ der Ordnung $p-1$; d.h.

$1 \pmod p, g \pmod p, \ldots, g^{p-2} \pmod p$ sind die $p-1$ von Null verschiedenen Elemente von $\mathbb{Z}_p$. (beachte: Nach Satz 19.1(ii) (Fermat) gilt: $g^{p-1} \pmod p = 1 \pmod p$)

Die Einheitengruppe von $(\mathbb{Z}_p, +, \cdot)$ ist also zyklisch, sie enthält genau die Potenzen von $g \pmod p$; ~~die Einheitengruppe ist also zyklisch~~.

Man beachte: $g \pmod p$ ist nicht eindeutig bestimmt.

g heißt Primitivwurzel mod p.

Bsp 20.1

(i) 2 ist keine Primitivwurzel mod 7; es gilt

$2 \not\equiv 1 \pmod 7$, $2^2 \not\equiv 1 \pmod 7$, $2^3 \equiv 1 \pmod 7$.

Die Ordnung von $2 \pmod 7$ in $\mathbb{Z}_7$ ist also 3 (und nicht 6).

3 ist Primitivwurzel mod 7 ; es gilt

$3 \not\equiv 1 \pmod 7$, $3^2 \equiv 2 \not\equiv 1 \pmod 7$, $3^3 \equiv 2\cdot 3 \equiv 6 \not\equiv 1 \pmod 7$,

$3^4 \equiv 3\cdot 6 \equiv 4 \pmod 7$, $3^5 \equiv 4\cdot 3 \equiv 5 \not\equiv 1 \pmod 7$;

nach Fermat $3^6 \equiv 1 \pmod 7$.

Analog erhält man:

5 ist Primitivwurzel mod 7 ;

4 ist nicht Primitivwurzel mod 7.

(ii) 2 ist Primitivwurzel mod 11 ; es gilt

$2 \not\equiv 1 \pmod{11}$, $2^2 \equiv 4 \not\equiv 1 \pmod{11}$, $2^3 \equiv 8 \not\equiv 1 \pmod{11}$, $2^4 \equiv 2\cdot 8 \equiv 5 \not\equiv 1 \pmod{11}$

$2^5 \equiv 2\cdot 5 \equiv 10 \not\equiv 1 \pmod{11}$, ... An dieser Stelle kann man schon abbrechen:

Die Ordnung von $2 \pmod{11}$ in der Einheitengruppe von $(\mathbb{Z}_{11}, +, \cdot)$ ist also > 5 ; andererseits Teiler der Ordnung der Einheitengruppe (Satz 7.1, Lagrange). Die Einheitengruppe besitzt die Ordnung $\varphi(11) = 10$.

Also hat $2 \pmod{11}$ die Ordnung 10 und 2 ist Primitivwurzel mod 11.

Bem 20.2 (ohne Beweis)

(i) Analog zu Bem 20.1 gilt:

Ist $p \neq 2$ Primzahl, so besitzt die Einheitengruppe von $(\mathbb{Z}_{p^a}, \cdot, \cdot)$ ein erzeugendes Element (also ein Element der Ordnung $\varphi(p^a)$) $g \pmod{p^a}$.

Dann heißt g Primitivwurzel mod p^a.

(ii) Man kann leicht überprüfen:

$(\mathbb{Z}_8, \cdot, \cdot)$ besitzt keine Primitivwurzel.

Bem 20.3 (Der Chinesische Restsatz)

Es seien $n_1, \dots, n_r \in \mathbb{N}$ paarweise teilerfremd.

Es seien $a_1, \dots, a_r \in \mathbb{Z}$ beliebig.

(i) Dann existiert ein $a \in \mathbb{Z}$ mit

$$a \equiv a_i \pmod{n_i} \text{ für } i = 1, \dots, r.$$

(ii) a ist modulo $n_1 \cdots n_r$ eindeutig bestimmt.

Beweis

(i) Im Fall $r = 1$ ist die Behauptung trivial.

Sei $r = 2$.

Wegen $\operatorname{ggT}(n_1, n_2) = 1$ lassen sich $x_1, x_2 \in \mathbb{Z}$ bestimmen, so daß gilt:

$$n_1 \cdot x_1 \equiv 1 \pmod{n_2} \text{ und } n_2 x_2 \equiv 1 \pmod{n_1}.$$

Setze $a := a_1 n_2 x_2 + a_2 n_1 x_1$. Dann folgt

$$a \equiv a_1 \pmod{n_1} \text{ und } a \equiv a_2 \pmod{n_2}.$$

Beweis durch vollständige Induktion nach r:

$r = 1$ s.o.

Schluß von $(r-1)$ auf r: Verwende den Fall $r = 2$.

(ii) Ist $a \equiv a_i \pmod{n_i}$ und $b \equiv a_i \pmod{n_i}$ für $i = 1, \dots, r$;

so ist $a - b \equiv 0 \pmod{n_i}$ für $i = 1, \dots, r$.

Also ist $a - b$ Vielfaches von $n_1, \dots, n_r$.

Da $n_1, \dots, n_r$ paarweise teilerfremd sind, ist $a - b$ dann auch Vielfaches von $n_1 \cdots n_r$.

Bsp 20.2

Bestimme ein $a \in \mathbb{Z}$ mit

$$a \equiv 3 \pmod 5 \quad \text{und} \quad a \equiv 2 \pmod 7.$$

Also ist $n_1 = 5$, $a_1 = 3$ und $n_2 = 7$, $a_2 = 2$.

$5 \cdot x_1 \equiv 1 \pmod 7$ besitzt als Lösung $x_1 = 3$,

$7 \cdot x_2 \equiv 1 \pmod 5$ besitzt als Lösung $x_2 = 3$.

Setze $a = a_1 n_2 x_2 + a_2 n_1 x_1 = 3 \cdot 7 \cdot 3 + 2 \cdot 5 \cdot 3 = 93$.

Dann gilt $a \equiv 3 \pmod 5$ und $a \equiv 2 \pmod 7$.

a ist mod $5 \cdot 7$ eindeutig bestimmt.

Für $a' = 23$ gilt ebenfalls $a' \equiv 3 \pmod 5$, $a' \equiv 2 \pmod 7$.

Für kleine Moduln kann man a auch durch Probieren schnell finden. Betrachte die Elemente aus der Restklasse $2 \pmod 7$ (diese erfüllen stets die Kongruenz $a \equiv 2 \pmod 7$):

$2, \; 2+7, \; 2+14, \; 2+21, \; \ldots$

Teste so lange bis ein Element $\equiv 3 \pmod 5$ auftritt:

~~2~~, ~~$2+7$~~, ~~$2+14$~~, $2+21$, $\ldots$.

(Nach spätestens 5 Schritten ist man am Ziel).

Kap. 4 Polynome

§21 Polynome

Def 21.1 (Polynome)

Sei $(R, +, \cdot)$ Ring,

sei $a_0, a_1, a_2, \ldots$ eine Folge von Elementen aus R,

die Folgenelemente seien von einer Stelle ab 0,

etwa $a_0, a_1, \ldots, a_n, 0, 0, \ldots$

Schreibweise für die Folge:

$$f(X) := \underbrace{a_0}_{\text{oder } a_0 \cdot X^0} + a_1 X + \ldots + a_n X^n,$$

$f(X)$ heißt Polynom mit Koeffizienten aus R; Schreibweise: $f(X) \in R[X]$.

a_i heißt Koeffizient von X^i.

X heißt Unbestimmte von $f(X)$; X ist nur ein formales Hilfssymbol, das auch mit einem anderen Symbol bezeichnet werden kann.

Die Reihenfolge der "Summanden" von $f(X)$ ist beliebig, der Koeffizient von X^i ist das Folgenelement a_i.

Ist $a_n \neq 0$, so heißt n Grad von $f(X)$; in Zeichen: $\operatorname{grad} f(X)$.

Ist $a_n = 1$, so heißt $f(X)$ normiertes Polynom.

Ist $a_i = 0$, so wird der "Summand" von $f(X)$ oft auch nicht mit aufgeführt.

Sind alle $a_i = 0$, so heißt $f(X)$ Nullpolynom,

dem Nullpolynom ist kein Grad zugeordnet.

Ein Koeffizient 1 wird häufig nicht mitgeschrieben.

Ist $f(X) = a_0$, so heißt $f(X)$ Konstantes Polynom.

Def. 21.2

Es bezeichne $R[X]$ die Menge aller Polynome mit Koeffizienten aus R.

Auf $R[X]$ werden 2 Verknüpfungen $+$ und $\cdot$ definiert "wie üblich"; d.h.:

$+$ durch "komponentenweise" Addition,

$\cdot$ durch übliches Ausmultiplizieren nach dem Distributivgesetz.

Für $f(x) \cdot g(x)$ schreibt man auch $(f \cdot g)(x)$;
für $f(x) + g(x)$ schreibt man auch $(f+g)(x)$.

Bem 21.1

Sei $f(x) \in R[X]$, $f(x) = a_n X^n + \dots + a_1 X + a_0$.

Dann läßt sich $+$ auch interpretieren als Summe zweier Polynome der Form $a_i X^i + a_j X^j$ und $a_i \cdot X^i$ als Produkt der Polynome a_i (konstantes Polynom) mit X^i.

Bem 21.2 (Polynomringe)

(i) $(R[X], +, \cdot)$ ist ein Ring (Polynomring über R)
(leicht nachzurechnen)

(ii) R ist ein Unterring von $(R[X], +, \cdot)$ (Unterring der konstanten Polynome).
(Beweis ist klar)

Bsp: 21.1

(i) $X = 1 \cdot X \in \mathbb{Z}[X]$; $X \notin 2\mathbb{Z}[X]$ (beachte: $1 \notin 2\mathbb{Z}$).

(ii) In $\mathbb{Z}[X]$ gilt: $(3X^3 + X)(2X^2 - 1) = 6X^5 - 3X^3 + 2X^3 - X$
$= 6X^5 - X^3 - X \in \mathbb{Z}[X]$.

Bem 21,3

Es sei $(\mathbb{Z}_n, +, \cdot)$ der Restklassenring mod n und

$f(X) := \overline{a_n} X^n + \dots + \overline{a_1} X + \overline{a_0} \in \mathbb{Z}_n[X]$.

Dann ist $\overline{a_i}$ die Restklasse $a_i \pmod n$.

Häufig wird einfach geschrieben: $f(X) = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}_n[X]$

Bsp 21,2

In $\mathbb{Z}_6[X]$ gilt:

$(3x^3 + x)(2x^2 - 1) = 6x^5 - x^3 - x = -x^3 - x \in \mathbb{Z}_6[x]$,

hier ist 6 die Null in $\mathbb{Z}_6$.

Bem 21,4

Der Ring $(R, +, \cdot)$ sei nullteilerfrei (s. Bsp 13,1) (d.h.: $a \neq 0, b \neq 0 \Rightarrow a \cdot b \neq 0$).

Dann gilt offenbar:

$$\operatorname{grad}(g(x) \cdot f(x)) = \operatorname{grad} g(x) + \operatorname{grad} f(x).$$

Def. 21,3 (Polynomabbildung)

Sei $f(x) \in R[X]$, $f(x) = a_n X^n + \dots + a_1 X + a_0$.

Die Abbildung $\tilde{f} : R \to R$ sei definiert durch

$$\tilde{f}(r) = a_n r^n + \dots + a_1 r + a_0 \quad \text{für alle } r \in R.$$

$\tilde{f}$ heißt Polynomabbildung von f.

Häufig wird $\tilde{f}$ auch mit f bezeichnet.

Bsp. 21.3

Sei $f(x) := x^2 - x \in \mathbb{Z}_2[X]$; $f(x)$ ist also nicht das Nullpolynom.

Es gilt $\tilde{f}(0) = 0$, $\tilde{f}(1) = 0$; $\tilde{f}: \mathbb{Z}_2 \to \mathbb{Z}_2$ ist also die Nullabbildung.

Bem 21.5 (Einsetzungshomomorphismus)

Es sei $(R, +, \cdot)$ ein kommutativer Ring (d.h. $\cdot$ ist kommutativ).

Sei $r \in R$ gegeben.

Sei $\varphi_r : R[X] \to R$ definiert durch

$$\varphi_r(f(x)) = \tilde{f}(r) \quad \text{(auch mit } f(r) \text{ bezeichnet).}$$

(Das Bild des Polynoms $f(x)$ erhält man, in dem für X das Element r eingesetzt wird).

Dann ist φ_r ein Ring-Homomorphismus; d.h. es gilt für alle $r \in R$

(i) $(f \cdot g)(r) = f(r) \cdot g(r)$

(ii) $(f + g)(r) = f(r) + g(r)$

} (leicht nachzurechnen)

φ_r heißt Einsetzungshomomorphismus.

Beachte: Zum Beweis von (i) benötigt man die Kommutativität von $\cdot$ in R;

zB gilt: $X(a \cdot X) = aX^2$ (in $R[X]$);

einsetzen von $r \in R$ liefert $r(a \cdot r) = a \cdot r^2$

und dies muß nicht richtig sein, falls der Ring nicht kommutativ ist

Bem 21.6 (Polynomdivision mit Rest).

Es sei $(K,+,\cdot)$ ein Körper ; $f(x)\in K[x]$, $g(x)\in K[x]$;
$g(x) \neq$ Nullpolynom.

Dann existieren $q(x), r(x) \in K[x]$ mit

$$f(x) = q(x)\cdot g(x) + r(x),$$

wobei gilt: $\operatorname{grad} r(x) < \operatorname{grad} g(x)$ oder $r(x) =$ Nullpolynom.

Die Behauptung und die Bestimmung von $q(x)$ und $r(x)$ ergeben sich aus der bekannten Division für Polynome (aus $\mathbb{R}[x]$).

Bsp 21.4

Seien $f(x) := x^3+x+1 \in \mathbb{Q}[x]$ und $g(x) := 2x^2+4 \in \mathbb{Q}[x]$.

Der Divisionsalgorithmus für Polynome liefert:

$$\begin{array}{l} x^3+x+1 \;:\; 2x^2+4 \;=\; \frac{1}{2}x \\ \underline{-(x^3+2x)} \\ \quad -x+1 \quad \text{(Rest)}. \end{array}$$

Man erhält die Gleichung

$$\underbrace{(x^3+x+1)}_{f(x)} = \underbrace{\frac{1}{2}x}_{q(x)}\underbrace{(2x^2+4)}_{g(x)} + \underbrace{(-x+1)}_{r(x)}.$$

Man beachte: Die Division in $\mathbb{Z}[x]$ ist hier nicht möglich, da eine Division durch den höchsten Koeffizienten 2 von $g(x)$ erforderlich ist.

Bem 22.7 Sei $(R,+,\cdot)$ ein Ring mit $1 \in R$; $f(x), g(x) \in R[x]$; $g(x)$ normiert.
Dann läßt sich $f(x)$ durch $g(x)$ mit Rest in $R[x]$ dividieren analog zu Bem 21.6. (denn in diesem Fall sind nur Divisionen durch 1 erforderlich).

§22 Nullstellen von Polynomen

Bem 22.1

Es sei $(R,+,\cdot)$ ein kommutativer Ring;

$f(x) \in R[X]$, $\alpha \in R$.

Ist $f(\alpha)=0$, so heißt α Nullstelle von $f(x)$.

Sei $1 \in R$. Dann gilt:

Ist α Nullstelle von $f(x) \in R[X]$, so läßt sich $f(x)$ in $R[x]$ darstellen in der Form

$$f(x) = (x-\alpha) \cdot q(x) \text{ mit einem } q(x) \in R[X].$$

Beweis (konstruktiv für die Berechnung von $q(x) \in R[x]$)

Dividiere $f(x)$ durch $x-\alpha$ mit Rest (vergleiche Bem. 22.7).

Dies liefert eine Gleichung der Form

$$f(x) = q(x)(x-\alpha) + r(x) \in R[X],$$

wobei $\operatorname{grad} r(x) < \operatorname{grad}(x-\alpha)$ ist oder $r(x) =$ Nullpolynom.

Also ist $r(x)$ ein konstantes Polynom.

Der Einsetzungshomomorphismus liefert (s. Bem 21.5; beachte: $(R,+,\cdot)$ ist kommutativ)

$$\underbrace{f(\alpha)}_{=0} = q(\alpha)\underbrace{(\alpha-\alpha)}_{=0} + r(x).$$

$$=0$$

Das konstante Polynom $r(x)$ ist also das Nullpolynom.

Damit ist die Behauptung bewiesen.

Bem 22.2 (Nullstellen von Polynomen mit Koeffizienten aus einem Körper)

Es sei $(K,+,\cdot)$ ein Körper; $f(X)\in K[X]$, $f(X)\neq$ Nullpolynom.

Dann läßt sich $f(X)$ (bis auf die Reihenfolge der Faktoren eindeutig) darstellen in der Form

$$f(X)=(X-\alpha_1)^{a_1}\cdots(X-\alpha_r)^{a_r}\cdot q(X) \text{ mit } \alpha_1,\dots,\alpha_r\in K;\ a_1,\dots,a_r\in\mathbb{N}$$

und $q(X)\in K[X]$, wobei $q(X)$ in K keine Nullstelle besitzt.

Dann heißt α_i a_i-fache Nullstelle von $f(X)\in K[X]$.

Speziell folgt (nach Bem 21.4 und Bem 11.4):

$$\operatorname{grad} f(X)=a_1+\dots+a_r+\operatorname{grad} q(X)\ ;\ \text{also auch}$$

$$a_i\leq \operatorname{grad} f(X),$$

$$r\leq \operatorname{grad} f(X).$$

Beweis

Die Existenz einer solchen Darstellung für $f(X)$ ergibt sich durch wiederholte Anwendung von Bem 22.1

Die Eindeutigkeit ergibt sich aus den Ausführungen in §23 (Bem 23.1)

Bsp. 22.1

(i) $x^3 - x \in \mathbb{Z}_5[x]$ hat in $\mathbb{Z}_5$ die Nullstellen $0, 1, -1 (=4)$
(beachte: $a \pmod 5$ ist dabei mit a bezeichnet) (s. Bem 21.3)

Nach Bem 22.2 folgt:

$$x^3 - x = x(-1)(x+1) \in \mathbb{Z}_5[x].$$

Die Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.
Beachte: $\mathbb{Z}_5$ ist ein Körper.

(ii) $x^2 + x \in \mathbb{Z}_6[x]$ hat in $\mathbb{Z}_6$ die vier Nullstellen $0, -1 (=5), 2, 3$.

Es gilt $x^2 + x = x(x+1) = (x-2)(x-3)$ in $\mathbb{Z}_6[x]$.

Beachte: $\mathbb{Z}_6$ ist kein Körper, Bem. 22.2 ist also nicht anwendbar.

(iii) Es sei p eine Primzahl,
$a \in \mathbb{Z}_p$, $a \neq$ Null.
Dann gilt nach Fermat: $a^{p-1} = 1$ in $\mathbb{Z}_p$.
Also: $a^p \equiv a$ in $\mathbb{Z}_p$ für alle $a \in \mathbb{Z}_p$.
Also: $x^p - x \in \mathbb{Z}_p[x]$ hat jedes Element aus $\mathbb{Z}_p$ als Nullstelle.

Es gilt:

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)) \in \mathbb{Z}_p[x].$$

Mit Hilfe der folgenden Bemerkung ist es leicht, alle rationalen Nullstellen eines Polynoms $f(x) \in \mathbb{Z}[x]$ zu bestimmen.
Eine für Anwendungen sehr wichtige Methode.

Bem 22.3

Es sei $f(x) := a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[x]$; $a_n \neq 0$, $a_0 \neq 0$.

Sei $\alpha \in \mathbb{Q}$ eine rationale Nullstelle von $f(x)$;

dann hat α die Form $\alpha = \frac{a}{b}$; $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $ggT(a,b) = 1$.

Dann gilt: $a \mid a_0$, $b \mid a_n$ in $\mathbb{Z}$.

(Für a und b kommen also nur endlich viele Elemente in Frage).

Anmerkung: Bem. 22.3 ist auch anwendbar für Polynome $g(x) \in \mathbb{Q}[x]$.
Hierfür multipliziere man $g(x)$ mit dem kgV der Nenner, die Nullstellen ändern sich dabei nicht.

Beweis

Setzt man α in $f(x)$ ein, so erhält man

$$a_n \frac{a^n}{b^n} + \dots + a_1 \frac{a}{b} + a_0 = 0$$

Multiplikation mit b^n liefert

$$a_n \cdot a^n + \underbrace{b\, a_{n-1} a^{n-1} + \dots + b^{n-1} a_1 \cdot a + b^n \cdot a_0}_{\text{ist Vielfaches von } b} = 0$$

also ist $b \mid a_n \cdot a^n$ und wegen $ggT(b,a) = 1$ folgt $b \mid a_n$.

$a_n a^n + b a_{n-1} a^{n-1} + \dots + b^{n-1} a_1 \cdot a$ ist Vielfaches von a,

also ist $a \mid b^n \cdot a_0$ und wegen $ggT(a,b) = 1$ folgt $a \mid a_0$.

Bsp. 22.2

(i) Bestimme alle rationalen Zahlen, die Nullstelle von

$f(x) := 2x^3+x+1 \in \mathbb{Z}[x]$ sind.

Sei $\alpha = \frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $ggT(a,b)=1$ Nullstelle von $f(x)$.

Nach Bem 22.3 ist dann

$$a \mid 1 \quad (a \in \mathbb{Z}) \quad \text{und} \quad b \mid 2 \quad (b \in \mathbb{N}).$$

Mögliche Werte für a: $1, -1$

Mögliche Werte für b: $1, 2$.

Als mögliche Nullstellen kommen für α also in Frage

$$1, \; -1, \; \frac{1}{2}, \; -\frac{1}{2}.$$

Durch Einsetzen in $f(x)$ erhält man, daß keine der vier Zahlen Nullstelle von $f(x)$ ist.

Also besitzt $f(x)$ in $\mathbb{Q}$ keine Nullstelle.

(ii) $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1 \in \mathbb{Z}[x]$.

Mögliche rationale Nullstellen sind ± 1.

-1 ist keine Nullstelle; 1 ist Nullstelle.

Wir untersuchen, ob 1 mehrfache Nullstelle ist.

Dividiert man $f(x)$ durch $(x-1)$, so erhält man

$$f(x) = (x-1)\cdot(x^3 - x^2 + x - 1).$$

Mögliche rationale Nullstellen von $x^3 - x^2 + x - 1$ sind 1 und -1.

-1 ist keine Nullstelle; 1 ist Nullstelle.

Division von $x^3 - x^2 + x - 1$ durch $(x-1)$ liefert $x^3 - x^2 + x - 1 = (x-1)(x^2+1)$.

Es folgt $f(x) = (x-1)^2(x^2+1)$. x^2+1 hat keine rationale Nullstelle;

also ist 1 2-fache Nullstelle von $f(x)$.

§23 Der Euklidische Algorithmus für Polynome

Bem 23.1

Bekanntlich läßt sich jede natürliche Zahl bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen darstellen. Zum Beweis benötigt man wesentlich die bekannte Möglichkeit der Division mit Rest in $\mathbb{Z}$.

Es sei $(K,+,\cdot)$ ein Körper. Dann gibt es im Polynomring $K[x]$ ebenfalls eine Möglichkeit der Division mit Rest (Polynomdivision, s. Bem 21.6). Diese kann verwendet werden zum Beweis der folgenden Aussage, die in einer gewissen Analogie zur Aussage über die eindeutige Primfaktorzerlegung natürlicher Zahlen steht.

Es gilt:

Es sei $(K,+,\cdot)$ ein Körper, $f(x) \in K[x]$, $f(x) \neq$ Nullpolynom.

(i) Dann läßt sich $f(x)$ darstellen in der Form

$$f(x) = a \cdot f_1(x) \cdots f_r(x) \text{ mit } a \in K;\ f_i(x) \in K[x] \text{ normiert}$$

und $f_i(x) \in K[x]$ irreduzibel für $i = 1, \dots, r$.

Die $f_1(x), \dots, f_r(x)$ müssen nicht paarweise verschieden sein. Dabei heißt $f_i(x) \in K[x]$ irreduzibel, wenn sich $f_i(x)$ in $K[x]$ nicht darstellen läßt als Produkt zweier nichtkonstanter Polynome aus $K[x]$ (s. § 24). (Def. 24.1)

(ii) Die Darstellung von $f(x)$ in (i) ist bis auf die Reihenfolge der Faktoren eindeutig.

Die irreduziblen Polynome aus $K[X]$ spielen dabei eine analoge Rolle wie die Primzahlen in $\mathbb{Z}$.

Die Aussage (i) ist leicht zu beweisen, da sich bei jeder Abspaltung eines nicht konstanten Polynoms von $f(x)$ die Grade der Polynome verkleinern.

Zum Beweis von (ii) wird die Polynomdivision verwendet.

Man beachte: Ist $(K,+,\cdot)$ kein Körper, so ist die Polynomdivision nicht möglich und die Aussage (ii) stimmt nicht mehr (s. Bsp. 22.1 (ii))

Bem 23.2 (Der Euklidische Algorithmus für Polynome)

Es sei $(K,+,\cdot)$ ein Körper; $f_1(x), f_2(x) \in K[X]$; $f_2(x) \neq$ Nullpolynom.

Man bilde die folgenden Divisionen in $K[X]$ (in Analogie zur Division in $\mathbb{Z}$):

$$f_1(x) = q_1(x) \cdot f_2(x) + f_3(x) \; ; \; \operatorname{grad} f_3(x) < \operatorname{grad} f_2(x)$$

$$f_2(x) = q_2(x) \cdot f_3(x) + f_4(x) \; ; \; \operatorname{grad} f_4(x) < \operatorname{grad} f_3(x)$$

$$\vdots$$

$$f_{n-2}(x) = q_{n-2}(x) \cdot f_{n-1}(x) + f_n(x) \; ; \; \operatorname{grad} f_n(x) < \operatorname{grad} f_{n-1}(x),$$

$$f_{n-1}(x) = q_{n-1}(x) f_n(x) + \text{Nullpolynom}.$$

Da sich der Grad des Restpolynoms bei jedem Schritt verkleinert, so hält man nach endlich vielen Schritten das Nullpolynom als Rest.

Dann gilt (analog zum Euklidischen Algorithmus in $\mathbb{Z}$):

(i) $f_n(x)$ ist ein ggT von $f_1(x)$ und $f_2(x)$; d.h.:

$f_n(x)$ ist ein Polynom maximalen Grades mit

$f_n(x) \mid f_1(x)$ und $f_n(x) \mid f_2(x)$ in $K[X]$.

Achtung: Der ggT ist (nur) bis auf einen konstanten Faktor aus K eindeutig bestimmt (dies ergibt sich aus Bem. 23.1).

(ii) Es existieren $g_1(x), g_2(x) \in K[X]$ mit

$$g_1(x) \cdot f_1(x) + g_2(x) \cdot f_2(x) = f_n(x).$$

Bsp. 23.1

Es sei $f_1(x) := x^4 - 1 \in \mathbb{Q}[X]$, $f_2(x) := 3x^3 - 3x^2 + 6x - 6 \in \mathbb{Q}[X]$

(i) Es gilt $f_1(x) = (x-1)(x+1)(x^2+1) \in \mathbb{Q}[X]$;

dies ist die Darstellung von $f_1(x)$ als Produkt irreduzibler Polynome aus $\mathbb{Q}[X]$ ($x-1, x+1$ sind trivialerweise irreduzibel; $x^2+1 \in \mathbb{Q}[X]$ ist irreduzibel, weil das Polynom in $\mathbb{Q}$ keine Nullstelle besitzt).

Es gilt $f_2(x) = 3x^3 - 3x^2 + 6x - 6 = 3 \cdot (x-1)(x^2+2) \in \mathbb{Q}[X]$;

dies ist die Darstellung von $f_2(x)$ als Produkt irreduzibler Polynome aus $\mathbb{Q}[X]$.

(ii) Aus (i) und Bem 23.1 folgt:

$(X-1)$ ist ggT von $f_1(X)$ und $f_2(X)$;

natürlich auch $c\cdot(X-1)$ für $c\in\mathbb{Q}$.
(Analog kann man den ggT zweier natürlicher Zahlen bestimmen mit Hilfe deren Primfaktorzerlegung)

(iii) Bestimmung des ggT von $f_1(X)$ und $f_2(X)$

mit Hilfe des Euklidischen Algorithmus:

$$\underbrace{X^4-1}_{f_1(X)} = \underbrace{\left(\tfrac{1}{3}X+\tfrac{1}{3}\right)}_{q_1(X)}\cdot\underbrace{(3X^3-3X^2+6X-6)}_{f_2(X)} + \underbrace{(-X^2+1)}_{f_3(X)}$$

$$\underbrace{3X^3-3X^2+6X-6}_{f_2(X)} = \underbrace{(-3X+3)}_{q_2(X)}\cdot\underbrace{(-X^2+1)}_{f_3(X)} + \underbrace{(9X-9)}_{f_4(X)}$$

$$\underbrace{(-X^2+1)}_{f_3(X)} = \underbrace{\left(-\tfrac{1}{9}X-\tfrac{1}{9}\right)}_{q_3(X)}\cdot\underbrace{(9X-9)}_{f_4(X)} + \text{Nullpolynom}$$

Also: $9X-9$ ist ggT von $f_1(X)$ und $f_2(X)$.

(iv) Suche $\gamma_1(X), \gamma_2(X)\in\mathbb{Q}[X]$ mit

$$\gamma_1(X)\cdot f_1(X) + \gamma_2(X)\cdot f_2(X) = \underbrace{9X-9}_{f_4(X)}.$$

(Verwende dabei die Divisionsgleichungen von "unten" nach "oben"; analog zu (ii))
Es gilt

$$f_4(X) = f_2(X) - q_2(X)\cdot\underbrace{f_3(X)}_{=f_1(X)-q_1(X)f_2(X)} = (-q_2(X))\,f_1(X) + (1+q_1(X)\cdot q_2(X))\cdot f_2(X)$$

$$= \underbrace{(3X-3)}_{\gamma_1(X)}\cdot f_1(X) + \underbrace{(-X^2+2)}_{\gamma_2(X)} f_2(X).$$

§24 Irreduzible Polynome

Def 24.1 (irreduzible Polynome)

Es sei $(R,+,\cdot)$ ein Integritätsbereich

(also ein kommutativer, nullteilerfreier Ring mit $R \neq \{0\}$, (s. Def 13.1)).

Sei $f(x) \in R[x]$ nicht konstant. Dann wird definiert:

$f(x) \in R[x]$ irreduzibel $:\Leftrightarrow$

$f(x)$ ist in $R[x]$ nicht darstellbar als Produkt zweier nichtkonstanter Polynome aus $R[x]$.

(Beachte: Nach Bem 12.2 ist jeder Körper ein Integritätsbereich und der Restklassenring $\mathbb{Z}_p$, falls p Primzahl ist, und auch $\mathbb{Z}$).

Bem 24.1 (Irreduzibilitätskriterien)

(i) Jedes lineare Polynom $aX+b \in R[x]$ ist irreduzibel.

(ii) Sei $(K,+,\cdot)$ ein Körper, $f(x) \in K[x]$, $\operatorname{grad} f(x) \geq 2$.

Besitzt $f(x)$ in K eine Nullstelle, so ist $f(x) \in K[x]$ nicht irreduzibel (denn f besitzt einen Linearfaktor) (s. Bem 22.1)

(iii) Sei $(K,+,\cdot)$ ein Körper, $f(x) \in K[x]$.

Sei $\operatorname{grad} f(x) = 2$ oder $\operatorname{grad} f(x) = 3$.

Besitzt $f(x)$ in K keine Nullstelle, so ist $f(x) \in K[x]$ irreduzibel (anderenfalls hätte $f(x)$ in $K[x]$ einen Linearfaktor)

(iv) Sei $(R,+,\cdot)$ ein Integritätsbereich, $f(x) \in R[x]$, $a \in R$. Dann:

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

Beweis: Es gilt $f(x) = f_1(x) \cdot f_2(x) \Leftrightarrow f(x+a) = f_1(x+a) \cdot f_2(x+a)$.

Bem 24.2 (Lemma von Gauß)

Es gilt:

$f(x) \in \mathbb{Z}[x]$ irreduzibel $\Leftrightarrow$ $f(x) \in \mathbb{Q}[x]$ irreduzibel

Beweis

Eine Zerlegung von $f(x)$ in $\mathbb{Z}[x]$ ist auch eine Zerlegung in $\mathbb{Q}[x]$.

Gegeben sei eine Zerlegung von $f(x)$ in $\mathbb{Q}[x]$; also

$$f(x) = f_1(x) \cdot f_2(x) \; ; \; f_1(x), f_2(x) \in \mathbb{Q}[x]; \quad \operatorname{grad} f_1(x) \geq 1, \; \operatorname{grad} f_2(x) \geq 1.$$

Dann ist zu zeigen: $f(x)$ besitzt auch eine Zerlegung in $\mathbb{Z}[x]$.

Multipliziert man das Produkt der Nenner der Koeffizienten von $f_1(x)$ mit $f_1(x)$, so erhält man ein Polynom aus $\mathbb{Z}[x]$; dividiert man nun dieses Polynom durch den ggT seiner Koeffizienten, so erhält man für $f_1(x)$ eine Darstellung der Form

$$f_1(x) = \frac{a_1}{b_1} \cdot f_1^*(x) \quad \text{mit} \quad \frac{a_1}{b_1} \in \mathbb{Q}, \; f_1^*(x) \in \mathbb{Z}[x],$$

der ggT der Koeffizienten von $f_1^*(x)$ ist 1.

Eine analoge Darstellung erhält man für $f_2(x)$. Für $f(x)$ ergibt sich dann eine Darstellung der Form

$$f(x) = \frac{a}{b} \, f_1^*(x) \cdot f_2^*(x), \quad ggT(a,b) = 1.$$

Ist $\frac{a}{b} \in \mathbb{Z}$, so ist die Behauptung bewiesen.

Andernfalls betrachten wir

$$b \cdot f(x) = a \cdot f_1^*(x) \cdot f_2^*(x) \qquad (*)$$

und einen Primteiler p von b. Dann ist $p \nmid a$, da $\operatorname{ggT}(a,b)=1$.

Der ggT der Koeffizienten von $f_1^*(x)$ ist 1, also kann p nicht Teiler aller Koeffizienten von $f_1^*(x)$ sein;

analog gilt dies für $f_2^*(x)$.

Gelte $f_1^*(x) = a_0 + a_1 x + \dots + a_n x^n$; $p \mid a_0, \dots, p \mid a_{i-1}, p \nmid a_i$.

Gelte $f_2^*(x) = b_0 + b_1 x + \dots + b_m x^m$; $p \mid b_0, \dots, p \mid b_{j-1}, p \nmid b_j$.

Der Koeffizient von x^{i+j} des Polynoms $a \cdot f_1^*(x) \cdot f_2^*(x)$ ist

$$a\,(\underbrace{a_i b_j}_{\substack{\text{nicht Vielfaches von } p \\ \text{nicht Vielfaches von } p}} + \underbrace{a_{i-1} \cdot b_{j+1} + a_{i-2} \cdot b_{j+2} + \dots}_{\text{Vielfaches von } p}) \text{, also nicht Vielfaches von } p.$$

Vielfaches von p

Alle Koeffizienten von $b \cdot f(x)$ sind wegen $p \mid b$ Vielfaches von p.

Zusammen ergibt sich ein Widerspruch zu $(*)$.

Der Fall $\frac{a}{b} \notin \mathbb{Z}$ kann also nicht eintreten.

Damit ist Bem 24.2 bewiesen.

Bem 24.3 (Eisensteinkriterium)

Es sei $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ nicht konstant.

Existiert eine Primzahl p mit

$$p \nmid a_n \,;\, p \mid a_{n-1}, \dots, p \mid a_0 \,;\, p^2 \nmid a_0,$$

so ist $f(x) \in \mathbb{Z}[x]$ irreduzibel.

Beweis

Annahme: $f(x)$ besitzt in $\mathbb{Z}[X]$ eine echte Zerlegung, etwa

$$f(x) = \underbrace{(c_r X^r + \dots + c_0)}_{=: f_1(x)} \underbrace{(b_s X^s + \dots + b_0)}_{=: f_2(x).} \quad ; \quad \begin{matrix} 1 \le r < n \\ 1 \le s < n. \end{matrix}$$

Dann ist $a_0 = b_0 \cdot c_0$ und nach Voraussetzung $p \mid c_0 \cdot b_0$, $p^2 \nmid c_0 \cdot b_0$.

Gelte oBdA $p \mid c_0$, $p \nmid b_0$.

Ferner ist $a_n = c_r \cdot b_s$ und wegen der Voraussetzung $p \nmid a_n$ folgt $p \nmid c_r$ und $p \nmid b_s$.

Nun existiert ein i, so daß gilt

$$p \mid c_0, \dots, p \mid c_{i-1}, \quad p \nmid c_i, \quad \text{wobei } 1 \le i \le s < n \text{ ist.}$$

Wir betrachten das Produktpolynom $f_1(x) \cdot f_2(x)$ und dessen Koeffizienten bei X^i:

$$a_i = \underbrace{c_i \cdot b_0}_{\text{nicht Vielfaches von } p} + \underbrace{c_{i-1} b_1 + \dots}_{\text{Vielfaches von } p} \qquad (\text{ist nicht Vielfaches von } p).$$

Wegen $1 \le i < n$ ist aber $p \mid a_i$.

Dies ist ein Widerspruch.

Also kann $f(x)$ in $\mathbb{Z}[X]$ keine echte Zerlegung besitzen.

Damit ist Bem 243 bewiesen.

Bsp 24.4.

(i) $2X-1 \in \mathbb{Z}[X]$ ist irreduzibel (Bem 24.1 (i))

$2X-1 \in \mathbb{Q}[X]$ ist irreduzibel (Bem 24.1 (i))

(ii) $2X^3+X+1 \in \mathbb{Q}[X]$ ist irreduzibel nach Bem 24.1(iii).
Beachte: Nach Bsp 22.2 (i) besitzt das Polynom in $\mathbb{Q}$ keine Nullstelle.

(iii) $X^3-2 \in \mathbb{Z}[X]$ ist irreduzibel nach Bem 24.3 (Eisenstein); wähle $p=2$.
Man beachte $p \mid 0$ wegen $p \cdot 0 = 0$.
Die Koeffizienten von X^2 bzw. X sind 0, besitzen also p als Teiler.
Nach Bem 24.2 (Lemma von Gauß) ist auch
$X^3-2 \in \mathbb{Q}[X]$ irreduzibel.

$X^3-2 \in \mathbb{Q}[X]$ ist auch nach Bem 24.1 (iii) irreduzibel, denn das Polynom besitzt in $\mathbb{Q}$ keine Nullstelle; dies ergibt sich aus Bem 22.3.

(iv) $X^2-2 \in \mathbb{Z}_3[X]$ ist irreduzibel nach Bem 24.1(iii), denn das Polynom besitzt in $\mathbb{Z}_3$ keine Nullstelle (zum Nachweis setze man $0, 1, 2$ ein).

(v) $3X^5+10X^2+35 \in \mathbb{Q}[X]$ ist irreduzibel, denn es gilt:
$3X^5+10X^2+35 \in \mathbb{Z}[X]$ ist irreduzibel (nach Eisenstein, wähle $p=5$), nach dem Lemma von Gauß folgt die Behauptung.
Achtung: Das Polynom besitzt in $\mathbb{Q}$ keine Nullstelle (nach Bem 22.3); da der Grad des Polynoms > 3 ist, folgt daraus aber nicht die Irreduzibilität von $3X^5+10X^2+35 \in \mathbb{Q}[X]$ (beachte Bem 24.1(iii))

(vi) $f(x) := x^3 - \frac{3}{4} - \frac{1}{8} \in \mathbb{Q}[X]$ ist irreduzibel

Nach Bem 24.1 (iii) genügt es zu zeigen, daß das Polynom in $\mathbb{Q}$ keine Nullstelle besitzt.

$f(x)$ und $8 \cdot f(x) =: g(x) = 8x^3 - 6x - 1$ besitzen in $\mathbb{Q}$ dieselben Nullstellen.
Mit Hilfe von Bem 22.3 erhält man, daß $g(x)$ in $\mathbb{Q}$ keine Nullstelle besitzt.

Bem 24.4

$x^n - a \in \mathbb{Z}[X]$ ist irreduzibel, falls eine Primzahl p existiert mit $p \mid a$, $p^2 \nmid a$ (nach Bem 24.3, Eisensteinkriterium), also ist $x^n - a \in \mathbb{Q}[X]$ auch irreduzibel (nach dem Lemma von Gauß, Bem 24.2)
Im Fall $n > 1$ besitzt $x^n - a$ in $\mathbb{Q}$ dann auch keine Nullstelle (nach Bem 24.1 ii).
Also ist $\sqrt[n]{a}$ nicht rational; insbesondere ist $\sqrt{2} \notin \mathbb{Q}$.

Kap. 5 Körper

§25 Ringadjunktion und Körperadjunktion

Def. 25.1

(i) (Ringadjunktion)

Sei R_1 Unterring des Ringes $(R_2, +, \cdot)$ und $M \subseteq R_2$. Dann:

$R_1[M] :=$ Kleinster Unterring von $(R_2, +, \cdot)$, der R_1 und M enthält.
(= Durchschnitt aller Unterringe von R_2, die R_1 und M enthalten)

(ii) (Körperadjunktion)

Sei K_1 Unterkörper des Körpers $(K_2, +, \cdot)$ und $M \subseteq K_2$. Dann:

$K_1(M) :=$ Kleinster Unterkörper von $(K_2, +, \cdot)$, der K_1 und M enthält
(= Durchschnitt aller Unterkörper von K_2, die K_1 und M enthalten)

Bsp 25.1

Sei $(\mathbb{C}, +, \cdot)$ der Körper der komplexen Zahlen; $i \in \mathbb{C}$ mit $i^2 = -1$.
Also ist $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$.

(i) Dann ist $\mathbb{Z}$ ein Unterring von $(\mathbb{C}, +, \cdot)$.

Es gilt $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

Es ist leicht nachzurechnen, daß $\mathbb{Z}[i]$ ein Unterring ist;
mit a, b, i muß auch $a + b \cdot i$ in $\mathbb{Z}[i]$ liegen.

$\mathbb{Z}[i]$ heißt Gaußscher Zahlring.

(ii) Es gilt $\mathbb{Q}[i] = \{a+bi \mid a,b \in \mathbb{Q}\}$.

Im Fall $a+bi \neq 0$ gilt

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a}{a^2+b^2} + \frac{(-1)}{a^2+b^2} \cdot i \in \mathbb{Q}[i].$$

Also ist $\mathbb{Q}[i]$ ein Körper.

Es folgt $\mathbb{Q}[i] = \mathbb{Q}(i)$. (Hier ist Ring - gleich Körperadjunktion)
(s. auch Bem. 27.1)

(iii) Es gilt $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$.

Im Fall $a+b\sqrt{2} \neq 0$ gilt

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2+2b^2} = \frac{a}{a^2+2b^2} + \frac{(-1)}{a^2+2b^2} \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Also ist $\mathbb{Q}[\sqrt{2}]$ ein Körper.

Es folgt $\mathbb{Q}[i] = \mathbb{Q}(i)$.
(s. auch Bem 27.1)

Bem 25.1

Es sei $(K, +, \cdot)$ ein Körper. Dann gilt stets

$$K[M] \subseteq K(M),$$

da jeder Körper auch ein Ring ist.

Bem 25.2

Es sei $(K, +, \cdot)$ ein Körper.

Eine Ringadjunktion $K[\alpha]$ enthält genau alle endlichen Summen der Form

$$a_0 + a_1 \alpha + \dots + a_m \alpha^m \text{ mit } m \in \mathbb{N}, \text{ alle } a_i \in K.$$

Die Körperadjunktion $K(\alpha)$ enthält genau alle Quotienten von Elementen aus $K[\alpha]$ mit Nenner $\neq 0$.

Bew Es ist unmittelbar klar, daß die behaupteten Elemente in $K[\alpha]$ bzw. $K(\alpha)$ liegen müssen. Außerdem bildet die Menge der Elemente offenbar auch einen Ring bzw. Körper.

§26 Das Minimalpolynom

Def. 26.1 (algebraische Elemente)

Es sei K ein Unterkörper des Körpers $(E, +, \cdot)$. Dann:

α algebraisch über K :$\Leftrightarrow$ Es existiert ein Polynom $f(X) \in K[X]$, $f(X) \neq$ Nullpolynom mit $f(\alpha) = 0$.

Ist α nicht algebraisch über K, so heißt α transzendent über K.

Bsp. 26.1

(i) $\sqrt[3]{2}$ ist algebraisch über $\mathbb{Q}$, da $\sqrt[3]{2}$ Nullstelle von $x^3 - 2 \in \mathbb{Q}[X]$ ist

(ii) Sei $a \in \mathbb{Q}$. Dann ist $\sqrt[n]{a}$ algebraisch über $\mathbb{Q}$ ($\sqrt[n]{a}$ ist Nullstelle von $x^n - a \in \mathbb{Q}[X]$).

(iii) Jedes $a \in K$ ist algebraisch über K, da a Nullstelle von $x - a \in K[X]$ ist.

Bem 26.1 (ohne Beweis)

(i) Die Kreiszahl π ist nicht algebraisch über $\mathbb{Q}$.

(ii) Die Basis e des natürlichen Logarithmus ist nicht algebraisch über $\mathbb{Q}$.

Bem 26.2 (Minimalpolynom)

Es sei $\alpha \in E$ algebraisch über K.

Dann existiert ein Polynom kleinsten Grades aus $K[X]$ mit α als Nullstelle, oBdA sei das Polynom normiert und mit $p(x)$ bezeichnet.

Dann ist $p(x) \in K[X]$ eindeutig bestimmt (denn die Differenz zweier verschiedener Polynome mit dieser Eigenschaft wäre ein Polynom kleineren Grades mit α als Nullstelle).

Schreibweise für $p(x)$: $\mathrm{Irr}(\alpha, K)$ oder $\mathrm{Min}(\alpha, K)$.

$\mathrm{Irr}(\alpha, K)$ heißt Minimalpolynom von α über K.

Wegen der Minimalität des Polynomgrades ist $\mathrm{Irr}(\alpha, K) \in K[X]$ offenbar irreduzibel.

Bem 26.3

Sei $\alpha \in E$ algebraisch über K.

(i) Sei $f(x) \in K[X]$ mit $f(\alpha) = 0$.

Dann gilt: $\mathrm{Irr}(\alpha, K) \mid f(x)$ in $K[X]$.

(ii) Sei $f(x) \in K[X]$ mit $f(\alpha) \neq 0$.

Dann gilt: $\mathrm{Irr}(\alpha, K) \nmid f(x)$ in $K[X]$

Beweis

(i) Dividiere $f(x)$ durch $\mathrm{Mr}(\alpha,K)(x)$ mit Rest:

$$f(x) = q(x) \cdot \mathrm{Mr}(\alpha,K)(x) + r(x);$$ $\operatorname{grad} r(x) < \operatorname{grad} \mathrm{Mr}(\alpha,K)(x)$ oder $r(x) =$ Nullpolynom.

Der Einsetzungshomomorphismus für α liefert:

$$\underbrace{f(\alpha)}_{=0} = q(\alpha)\,\underbrace{\mathrm{Mr}(\alpha,K)(\alpha)}_{=0} + r(\alpha), \quad \text{also } r(\alpha)=0.$$

Wegen der Minimalität des Grades von $\mathrm{Mr}(\alpha,K)(x)$ folgt: $r(x) =$ Nullpolynom.

(ii) Ist klar, da $\mathrm{Mr}(\alpha,K)$ α als Nullstelle besitzt.

Bem 26.4

Sei $\alpha \in E$ algebraisch über K. Dann gilt:

$f(x) \in K[x]$ ist das Minimalpolynom von α über K $\Leftrightarrow$

$f(x) \in K[x]$ ist irreduzibel, normiert und es gilt $f(\alpha)=0$.

Beweis

$\Rightarrow$: s. Bem 26.2.

$\Leftarrow$: Nach Bem. 26.3 folgt: $\mathrm{Mr}(\alpha,K)(x) \mid f(x)$ in $K[x]$.

Da $f(x) \in K[x]$ irreduzibel ist und $\mathrm{Mr}(\alpha,K)(x)$ und $f(x)$ beide normiert sind, folgt $f(x) = \mathrm{Mr}(\alpha,K)(x)$.

Bsp 26.2

(i) $\mathrm{Irr}(\sqrt[n]{2}, \mathbb{Q})(x) = x^n - 2 \in \mathbb{Q}[x]$, denn es gilt:

$x^n - 2$ ist normiert,

$x^n - 2$ hat $\sqrt[n]{2}$ als Nullstelle

$x^n - 2 \in \mathbb{Q}[x]$ ist irreduzibel (s. Bem 24.4).

Man beachte:

Zum Beweis wird Bem 26.4 verwendet, da dann die Irreduzibilitätskriterien aus §24 verwendet werden können.

(iii) Sei $(E, +, \cdot)$ eine Körpererweiterung von $\mathbb{Z}_3$ (bzw. $\mathbb{Z}_3$ ist Unterkörper von $(E, +, \cdot)$).

Sei $\alpha \in E$ Nullstelle von $x^2 - 2 \in \mathbb{Z}_3[x]$.

Dann ist $\mathrm{Irr}(\alpha, \mathbb{Z}_3) = x^2 - 2 \in \mathbb{Z}_3[x]$

(beachte: Nach Bsp 24.1 ist $x^2 - 2 \in \mathbb{Z}_3[x]$ irreduzibel)

~~Bild Zeichnung~~

§27 Einfach algebraische Körpererweiterungen

Bem 27.1

Es sei K Unterkörper des Körpers $(E, +, \cdot)$.

Sprechweise: E ist eine Körpererweiterung von K

Schreibweise für die Körpererweiterung: $E : K$.

$$\begin{array}{c} E \\ | \\ K \end{array}$$

Sei $\alpha \in E$ algebraisch über K;

also ist das Minimalpolynom $\mathrm{Irr}(\alpha, K)(x) \in K[x]$ definiert.

Sei $\operatorname{grad} \mathrm{Irr}(\alpha, K)(x) =: n$.

Dann gilt:

(i) $K[\alpha] = K(\alpha)$

(d.h. die Ringadjunktion ist auch schon Körperadjunktion)

(ii) Jedes Element aus $K[\alpha]$ läßt sich eindeutig darstellen in der Form

$$a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1}, \text{ wobei } a_0, \dots, a_{n-1} \in K \text{ ist.}$$

$K(\alpha)$ heißt einfach algebraische Körpererweiterung.

Beweis

(i) Es ist nur zu zeigen:

Jedes Element $\neq 0$ aus $K[\alpha]$ besitzt in $K[\alpha]$ ein multiplikativ Inverses.

Der folgende Beweis ist konstruktiv:

Ein beliebiges Element aus $K[\alpha]$ hat nach Bem 27.1(ii) die Form

$$\beta := a_0 + a_1\alpha + \dots + a_m\alpha^m \; ; \; m \in \mathbb{N}; \; a_0, \dots, a_m \in K.$$

Sei $\beta \neq 0$.

Betrachte das Polynom

$$f(x) := a_0 + a_1 X + \dots + a_m X^m \in K[X] \; ;$$

dann ist $f(\alpha) = \beta \neq 0$.

Nach Bem 26.3 (ii) ist dann $f(x)$ nicht Vielfaches von $\mathrm{Irr}(\alpha, K)(x)$ in $K[X]$.

Da $\mathrm{Irr}(\alpha, K)(x) \in K[X]$ irreduzibel ist, folgt:

1 ist ggT von $f(x)$ und $\mathrm{Irr}(\alpha, K)(x)$.

Nach dem Euklidischen Algorithmus existieren Polynome $\gamma_1(x), \gamma_2(x) \in K[x]$ mit

$$\gamma_1(x) \cdot f(x) + \gamma_2(x) \cdot \mathrm{Irr}(\alpha, K)(x) = 1.$$

Der Einsetzungshomomorphismus liefert

$$\gamma_1(\alpha) \cdot \underbrace{f(\alpha)}_{=\beta} + \gamma_2(\alpha) \cdot \underbrace{\mathrm{Irr}(\alpha, K)(\alpha)}_{=0} = 1.$$

Also ist $\gamma_1(\alpha)$ zu $f(\alpha)$ $(= \beta)$ multiplikativ invers.

(ii)

Existenz der Darstellung:

Sei $\beta := a_0 + a_1\alpha + \dots + a_m\alpha^m \in K[\alpha]$ beliebig gegeben. (*)

Im Fall $m \leq n-1$ sind wir fertig.

Sei also $m \geq n$.

Betrachte $f(X) := a_0 + a_1 X + \dots + a_m X^m \in K[X]$.

Dann ist $f(\alpha) = \beta$.

Dividiere $f(X)$ durch $\mathrm{Irr}(\alpha, K)(X)$ in $K[X]$ mit Rest:

$f(X) = q(X) \cdot \mathrm{Irr}(\alpha, K)(X) + r(X)$, wobei $\operatorname{grad} r(X) < n$ ist oder $r(X) =$ Nullpolynom

Der Einsetzungshomomorphismus liefert

$$\beta = f(\alpha) = r(\alpha)$$

und $r(\alpha)$ besitzt die behauptete Form.

Ein zweiter Beweis für die Existenz:

Ist $\mathrm{Irr}(\alpha, K)(X) = b_0 + b_1 X + \dots + b_{n-1} X^{n-1} + X^n$,

so gilt

$$\alpha^n = -(b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}) \quad (**)$$

(sog. Nullstellengleichung für α)

Ersetze α^n in (*) mit Hilfe von (**).

Wiederholte Anwendung liefert die Behauptung.

Eindeutigkeit der Darstellung:

Annahme: $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = a_0' + a_1'\alpha + \dots + a_{n-1}'\alpha^{n-1}$.

Dann ist $(a_0 - a_0') + (a_1 - a_1')\alpha + \dots + (a_{n-1} - a_{n-1}')\alpha^{n-1} = 0$

Da $\mathrm{Irr}(\alpha, K)(X) \in K[X]$ ein Polynom kleinsten Grades mit α als Nullstelle ist, folgt $a_0 = a_0', \dots, a_{n-1} = a_{n-1}'$.

Def. 27.1 (Grad einer Körpererweiterung)

Es sei K Unterkörper des Körpers $(E, +, \cdot)$.

Dann läßt sich E auffassen als K-Vektorraum in dem folgenden Sinn:

$(E,+)$ ist die Gruppe der Vektoren,

der Körper $(K,+,\cdot)$ ist der Skalarbereich,

das Produkt $\underset{\in K}{\lambda} \cdot \underset{\in E}{a}$ von Skalar mit Vektor

ist definiert durch die Multiplikation in E.

Dann sind alle Vektorraumaxiome erfüllt.

Dann wird definiert:

$[E:K] := \dim$ des K-Vektorraums E.

$[E:K]$ heißt Grad der Körpererweiterung $E:K$.

Mit Hilfe von Def. 27.1 läßt sich Bem 27.1 umformulieren zu

Bem 27.2

Es sei $\alpha \in E$ algebraisch über K und $n := \operatorname{grad} \operatorname{Irr}(\alpha, K)(X)$.

Dann ist der Körpergrad $[K(\alpha):K] = n$ und

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

ist eine Basis des K-Vektorraums E.

Sprechweise: Basis von $K(\alpha):K$.

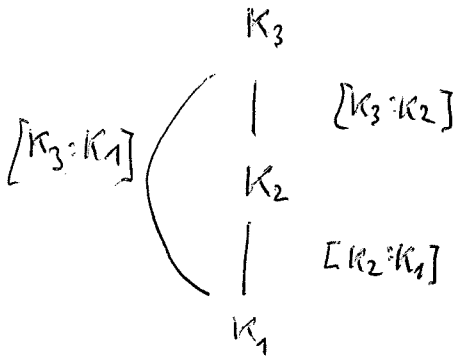
Bem. 27.3 (ohne Beweis)

Gegeben seien die Körper $K_1 \subseteq K_2 \subseteq K_3$.

Dann gilt:

$$[K_3 : K_1] = [K_3 : K_2] \cdot [K_2 : K_1]$$

(Ist $[K_3 : K_2] = \infty$ oder $[K_2 : K_1] = \infty$, so ist auch $[K_3 : K_1] = \infty$)



In diesem Sinne ist der Körpergrad multiplikativ.

Bsp 27.1

Sei $f(x) := x^3 + 10x + 5 \in \mathbb{Q}[X]$ und $\alpha \in \mathbb{R}$ Nullstelle von $f(x)$.

(1) Man gebe eine Basis von $\mathbb{Q}(\alpha) : \mathbb{Q}$ an.

Wir gehen nach Bem. 27.2 vor:

Zunächst ist das Minimalpolynom $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Q}[X]$ zu berechnen nach Bem 26.4:

$f(x) = x^3 + 10x + 5 \in \mathbb{Q}[X]$ ist irreduzibel

(nach Bem 24.3 (Eisenstein) (und Bem 24.2 (b)ff) oder man zeige, daß $f(x)$ in $\mathbb{Q}$ keine Nullstelle besitzt unter Verwendung von Bem 22.3 und wende dann Bem 24.1 an)

$f(x)$ ist normiert und besitzt α als Nullstelle.

Also folgt: $\mathrm{Irr}(\alpha, K)(x) = x^3 + 10x + 5 \in \mathbb{Q}[X]$.

Nach Bem. 27.2 folgt

$\{1, \alpha, \alpha^2\}$ ist eine Basis von $\Theta(\alpha) : \Theta$.

(ii) Gilt in $\Theta(\alpha)$: $3\alpha^3 + \alpha + 1 = 2\alpha^2 + 5$?

α ist Nullstelle von $f(x)$, α erfüllt also die Nullstellengleichung

$\alpha^3 + 10\alpha + 5 = 0$ bzw. $\alpha^3 = -10\alpha - 5$.

Dies liefert

$$3\alpha^3 + \alpha + 1 = 3(-10\alpha - 5) + \alpha + 1 = -30\alpha - 15 + \alpha + 1$$

$$= 29\alpha - 14$$

Nach (i) ist $\{1, \alpha, \alpha^2\}$ eine Basis von $\Theta(\alpha) : \Theta$, jedes Element aus $\Theta(\alpha)$ läßt sich also darstellen in der Form

$$a_0 + a_1\alpha + a_2\alpha^2 \quad \text{mit } a_0, a_1, a_2 \in \Theta$$

und a_0, a_1, a_2 sind dabei eindeutig bestimmt.

Also folgt:

$$3\alpha^3 + \alpha + 1 \; (= 29\alpha - 14) \neq 2\alpha^2 + 5.$$

(iii) Man stelle $\alpha^3 + \alpha^2 + 10\alpha + 1$ dar als Linearkombination der Basiselemente $1, \alpha, \alpha^2$. Wir folgen dem zweiten Beweis von Bem. 27.1(ii). Verwendet man wieder die Nullstellengleichung von α, so erhält man

$$\alpha^3 + \alpha^2 + 10\alpha + 1 = 1\alpha^2 + 0\cdot\alpha + 4.$$

Man kann aber auch dem ersten Beweis von Bem 27.1(ii) folgen.

(iv) Ist α^2 zu $1+\alpha$ in $\mathbb{Q}(\alpha)$ multiplikativ invers?

Es gilt $\alpha^2(1+\alpha) = \alpha^3 + \alpha^2 \overset{\uparrow}{=} \alpha^2 - 10\alpha - 5$.

Nullstellengleichung von α

Da $\{1, \alpha, \alpha^2\}$ eine Basis von $\mathbb{Q}(\alpha) : \mathbb{Q}$ ist, gilt

$$\alpha^2 - 10\alpha - 5 \neq 0 \cdot \alpha^2 + 0 \cdot \alpha + 1 = 1.$$

Also ist α^2 nicht zu $1+\alpha$ invers.

(v) Bestimme das multiplikativ Inverse von $(1+\alpha)$ in $\mathbb{Q}(\alpha)$ als Linearkombination der Basiselemente $1, \alpha, \alpha^2$.

Wir folgen dem Beweis von Bem 27.1 (i).

Wir betrachten das Polynom

$$g(x) = x + 1 \in \mathbb{Q}[x],$$

das man erhält, wenn bei $(1+\alpha)$ die Zahl α durch x ersetzt wird. Dann ist $g(\alpha) = 1+\alpha$.

Wir wenden nun den Euklidischen Algorithmus an auf die beiden Polynome $f(x) = \mathrm{Irr}(\alpha, \mathbb{Q})(x)$ und $g(x)$:

$$x^3 + 10x + 5 = (x^2 - x + 11)(x+1) - 6$$

Die nächste Division liefert den Rest Nullpolynom.
Also müssen keine weiteren Divisionen durchgeführt werden.
Wir setzen α ein und erhalten

$$0 = \alpha^3 + 10\alpha + 5 = (\alpha^2 - \alpha + 11)(\alpha + 1) - 6,$$

also $$\frac{1}{1+\alpha} = \frac{\alpha^2 - \alpha + 11}{6} = \frac{11}{6} - \frac{1}{6}\alpha + \frac{1}{6}\alpha^2.$$

($\overline{\text{VI}}$) Man bestimme das multiplikativ Inverse von α^2+10 in $\mathbb{Q}(\alpha)$ als Linearkombination der Basiselemente $1, \alpha, \alpha^2$.

Man kann wieder verfahren analog zu ($\overline{\text{V}}$).

In diesem Fall geht es aber auch einfacher.

Die Nullstellengleichung von α lautet

$$\alpha^3 + 10\alpha + 5 = 0,$$

also $$\alpha(\alpha^2+10) = -5,$$

also $$\frac{1}{\alpha^2+10} = -\frac{1}{5}\cdot\alpha$$

Bsp 27.2

(i) Sei $f(x) = x^3+10x+5 \in \mathbb{Z}_7[X]$; d.h. die Koeffizienten werden als Restklassen mod 7 aufgefaßt. (s. Bem 21.3)
Das Polynom ist irreduzibel, da es in $\mathbb{Z}_7$ keine Nullstelle besitzt (Man setze $0, 1, -1, 2, -2, 3, -3$ ein).
Alle Ergebnisse aus Bsp 27.1 lassen sich nun direkt übertragen, wenn α Nullstelle von f (ist) in einer Körpererweiterung von $\mathbb{Z}_7$.

(ii) $f(x) := x^3+10x+5 \in \mathbb{Z}_3[X]$ ist nicht irreduzibel.
In diesem Fall läßt sich Bsp 27.1 natürlich nicht übertragen, da die Irreduzibilität wichtig ist (zur Bestimmung des Minimalpolynoms)

Bsp 27.3

Sei $\alpha \in E$ Nullstelle von $x^2-2 \in \mathbb{Z}_3[X]$.
Nach Bsp 26.2 (iii) ist $\mathrm{Irr}(\alpha, \mathbb{Z}_3) = x^2-2$.
Dann ist $\{1, \alpha\}$ eine Basis von $\mathbb{Z}_3(\alpha)$.
Die Elemente aus $\mathbb{Z}_3(\alpha)$ lassen sich also eindeutig darstellen in der Form

$$a_0 + a_1\alpha \text{ mit } a_0, a_1 \in \mathbb{Z}_3$$

Es gibt genau $3 \cdot 3 (= 9)$ solcher Linearkombinationen.
$\mathbb{Z}_3(\alpha)$ hat also genau 9 Elemente.

§28 Konstruktionen mit Zirkel und Lineal

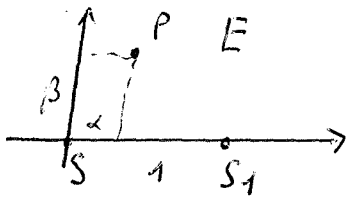
Zunächst muß präzisiert werden, was unter einer Konstruktion mit Zirkel und Lineal verstanden wird.

Bem 28.1

Gegeben sei eine Menge P_0 von Punkten in der Ebene E ($E = \mathbb{R} \times \mathbb{R}$), P_0 enthalte mindestens 2 Elemente.
Untersucht werden soll, welche Punkte der Ebene E sich daraus mit Zirkel und Lineal konstruieren lassen.

Zunächst wird in der Ebene ein Koordinaten-System fixiert. Dazu werden 2 nicht parallele Geraden fixiert, so daß gilt:
Der Schnittpunkt S der beiden Geraden gehört zu P_0, auf einer der beiden Geraden liegt noch ein weiterer Punkt S_1 aus P_0.
Es wird ein Längenmaß eingeführt, in dem die Strecke $\overline{SS_1}$ als Strecke der Länge 1 definiert wird.
Hierdurch werden den Punkten der Ebene eindeutig Koordinaten-Paare aus $\mathbb{R} \times \mathbb{R}$ zugeordnet:

$P \longleftrightarrow (\alpha, \beta)$. (α, β) heißen Koordinaten von P



Zwei Operationen sind möglich

Operation L (Lineal): Ziehe durch 2 Punkte aus P_0 eine Gerade.

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

Def. 28.1

(i) $P \in E$ ist aus P_0 im ersten Schritt Konstruierbar $:\Leftrightarrow$ Perhält man als Schnittpunkt zweier Kreise bzw. Geraden, die jeweils durch eine Operation L oder Z entstehen.

(ii) $P \in E$ ist aus P_0 Konstruierbar $:\Leftrightarrow$
Es existieren endlich viele Punkte $p_1, \dots, p_n = P$, so daß für alle i gilt:
P_{i+1} ist Konstruierbar aus $P_0 \cup \{p_1, \dots, p_i\}$ im 1. Schritt.

(iii) $\alpha \in \mathbb{R}$ heißt aus P_0 Konstruierbar, wenn der Punkt mit den Koordinaten $(\alpha, 0)$ aus P_0 Konstruierbar ist.

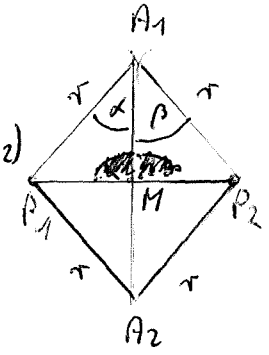
Bem 28.2 :

Da 1 nach Voraussetzung konstruierbar ist aus P_0, ist auch jedes $n \in \mathbb{N}$ aus P_0 konstruierbar.

Beweis: klar

Bem 28.3 : (Streckenhalbierung)

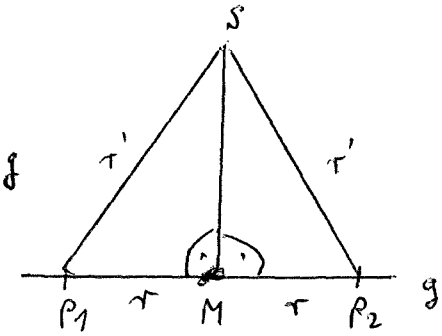
Es seien P_1 und P_2 gegebene Punkte der Ebene. Dann läßt sich der Mittelpunkt M der Strecke $\overline{P_1P_2}$ konstruieren



Beweis

Die Dreiecke $\Delta(A_1, P_1, A_2)$, $\Delta(A_1, P_2, A_2)$ sind kongruent (SSS), also ist $\alpha = \beta$.

Die Dreiecke $\Delta(A_1, P_1, M)$, $\Delta(A_1, P_2, M)$ sind kongruent. (SWS).
Also halbiert M die Strecke $\overline{P_1P_2}$



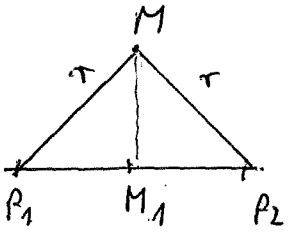
Bem 28.4 : (Rechter Winkel)

Trage im Punkt M an die Gerade g einen rechten Winkel an:

s. Skizze, beachte die Dreiecke $\Delta(M, P_1, S)$ und $\Delta(M, P_2, S)$ sind kongruent.

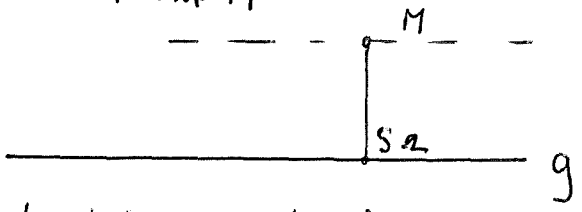
Bem 28.5 (Lot)

Fälle das Lot von einem Punkt M auf eine Gerade g.
Konstruiere P_1 und P_2 und halbiere die Strecke $\overline{P_1P_2}$ nach Bem 28.3



Bem 28.6 (Parallelen)

Zeichne zu einer Geraden g die Parallele durch einem Punkt M

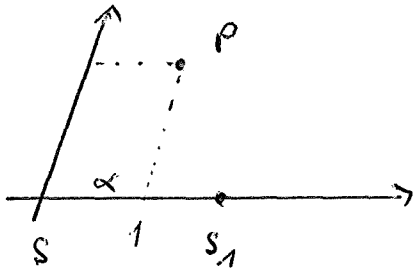


Fälle das Lot von M auf g.

Trage im Punkt M an $\overline{MS_2}$ einen rechten Winkel an.

Bem 28.7

Ein Punkt P läßt sich konstruieren gdw seine Koordinaten konstruierbar sind.



Beweis: Klar nach Bem 28.6.

Nach Bem 28.7 genügt es also zu untersuchen, welche reellen Zahlen konstruierbar sind. Dabei ist 1 stets gegeben (da die Einheitsstrecke zu Anfang fixiert wird).

Bem 28.8

Seien $1, a, b \in \mathbb{R}$ gegeben. Dann gilt:

(i) $a+b$ ist Konstruierbar

(ii) $a \cdot b$ ist Konstruierbar

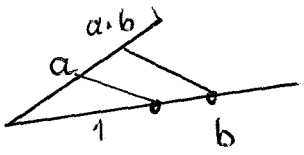
(iii) $\frac{a}{b}$ $(b \neq 0)$ ist Konstruierbar.

(iv) Alle Elemente aus Θ sind Konstruierbar.

Beweis

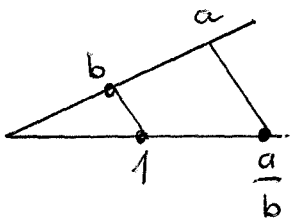
(i) klar

(ii) Man wende den Strahlensatz an:



Die Parallele durch b läßt sich Konstruieren nach Bem 28.6

(iii) Man wende den Strahlensatz an:



Die Parallele durch a läßt sich Konstruieren nach Bem 28.6.

(iv) folgt aus (i), (ii), (iii).

Bem 28.9

Sei $M \subseteq \mathbb{R}$ gegeben mit $1 \in M$.

Sei $\Theta(M)$ der kleinste Teilkörper von $\mathbb{R}$, der Θ und M enthält (Körperadjunktion).

Dann ist jedes Element aus $\Theta(M)$ aus M Konstruierbar.

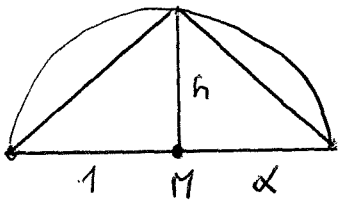
Bew: nach Bem 28.8 und beachte, daß sich die Elemente aus $\Theta(M)$ zusammensetzen aus Summen, Produkten, Quotienten von Elementen aus $\Theta \cup M$. Wende Bem 28.8 an.

Bem 28,10

Seien 1 und $\alpha \in \mathbb{R}$ gegeben,
Dann läßt sich daraus $\sqrt{\alpha}$ konstruieren.

Beweis

Man wende den Höhensatz an:



Es gilt
$1 \cdot \alpha = h^2$,
also $\sqrt{\alpha} = h$.

M ist der Mittelpunkt des Halbkreises,
M ist konstruierbar nach Bem 28.3

Bem 28,11

Sei $M \subseteq \mathbb{R}$ und $1 \in M$.
Sei α aus M konstruierbar.
Dann ist $\alpha \in \mathfrak{O}(M)$ oder es existiert ein $a \in M$,
so daß gilt $\alpha \in \mathfrak{O}(M)(\sqrt{a})$.

Beweis
Entsteht α durch den Schnittpunkt zweier Geraden,
so ist $\alpha \in \mathfrak{O}(M)$, andernfalls lassen sich die Koordinaten
des Schnittpunktes durch eine Wurzel $\sqrt{a}$ ausdrücken
(nach der (P,9) - Formel für quadratische Gleichungen),
damit folgt die Behauptung.

Satz 28.1

Sei $M \subseteq \mathbb{R}$, $1 \in M$. Dann gilt:

α ist aus M konstruierbar $\Leftrightarrow$

Es existiert eine Körperkette

$$\mathbb{Q}(M) \subseteq \mathbb{Q}(M)(\sqrt{a_1}) \subseteq \dots \subseteq \mathbb{Q}(M)(\sqrt{a_1}, \dots, \sqrt{a_r})$$

mit $\alpha \in \mathbb{Q}(M)(\sqrt{a_1}, \dots, \sqrt{a_r})$.

Beweis Ergibt sich aus Bem 28.9, Bem 28.10, Bem 28.11.

Satz 28.2

Sei $1 \in \mathbb{R}$ gegeben und $\alpha \in \mathbb{R}$ aus 1 konstruierbar.

Dann ist der Körpergrad $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ Potenz von 2.

Bew

Jede Erweiterung in der Körperkette aus Satz 28.1 ist eine Erweiterung vom Grad 1 oder Grad 2, da jeweils eine Quadratwurzel adjungiert wird.

Die Behauptung ergibt sich nun aus der Multiplikativität der Körpergrade (Bem 27.3).

Bsp 28.1 (Delisches Problem)

Gegeben sei die Kantenlänge eines Würfels mit dem Volumen 1. (also $1 \in \mathbb{R}$).
Läßt sich daraus die Kantenlänge eines Würfels mit dem Volumen 2 (also $\sqrt[3]{2}$) konstruieren?

Es gilt $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2 \in \mathbb{Q}[X]$ (Bsp 26.2) und

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \mathrm{grad}\ \mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = 3$ (nach Bem 27.2).
Nach Satz 28.2 ist also $\sqrt[3]{2}$ nicht lösbar.

Beispiel 28.2 (Dreiteilung eines Winkels)

Man kann sich leicht überlegen, wie die Winkelhalbierende eines Winkels mit Zirkel und Lineal konstruiert werden kann.

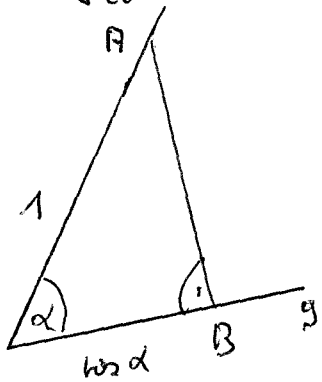
Wir betrachten hier die Dreiteilung eines Winkels, also das Problem: Läßt sich ein gegebener Winkel mit Zirkel und Lineal in drei gleich große Teilwinkel zerlegen? Es wird sich zeigen, daß dies für den Winkel $\alpha = 60°$ nicht möglich ist.

Zunächst eine Vorbemerkung:
Es sei die Einheitsstrecke, also $1 \in \mathbb{R}$ gegeben. Dann gilt:

Der Winkel α ist konstruierbar

gdw $\cos\alpha$ konstruierbar ist.

Ist der Winkel gegeben, so kann man das Lot von A auf g fällen (nach Bem 28.5).
Ist $\cos\alpha$ gegeben, so kann man an g im Punkt B einen rechten Winkel antragen (nach Bem 28.4)



Wir betrachten nun also keine Winkel, sondern den Cosinus.
Sei nun die Einheitsstrecke gegeben, also $1 \in \mathbb{R}$

und $\cos 3\alpha$,

zu untersuchen ist, ob daraus $\cos\alpha$ konstruiert werden

kann.

Hierzu verwenden wir die Formel von Moivre:

$$(\cos\alpha + i\sin\alpha)^n = \cos n\alpha + i\sin n\alpha$$

[Zur Erinnerung:

Allgemein gilt für zwei komplexe Zahlen:

$$r_1(\cos\alpha_1 + i\sin\alpha_1) \cdot r_2(\cos\alpha_2 + i\sin\alpha_2) = r_1 r_2(\cos(\alpha_1+\alpha_2) + i\sin(\alpha_1+\alpha_2))]$$

Für $n=3$ erhält man durch Ausmultiplizieren

der linken Seite

$$\cos^3\alpha + 3i\cos^2\alpha\sin\alpha + 3\underbrace{i^2}_{=-1}\cos\alpha\sin^2\alpha + \underbrace{i^3}_{=-i}\sin^3\alpha = \cos 3\alpha + i\sin 3\alpha.$$

Durch Vergleich der Realteile auf beiden Seiten ergibt sich

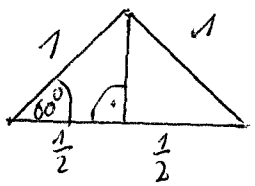
$$\cos^3\alpha - 3\cos\alpha\sin^2\alpha = \cos 3\alpha$$

und wegen $\cos^2\alpha + \sin^2\alpha = 1$

$$4\cos^3\alpha - 3\cos\alpha = \cos 3\alpha.$$

Wir betrachten nun den Fall $3\alpha = 60°$,

also $\cos 3\alpha = \cos 60° = \frac{1}{2}$. (s. Skizze).



Dann gilt

$$4\cos^3\alpha - 3\cos\alpha - \frac{1}{2} = 0.$$

$\cos\alpha$ ist also Nullstelle von $4X^3 - 3X - \frac{1}{2} \in \mathbb{Q}[X]$,

Nach Beispiel 21.6 (VI) ist $X^3 - \frac{3}{4}X - \frac{1}{8} \in \mathbb{Q}[X]$ irreduzibel.

Das Minimalpolynom von $\cos\alpha$ über $\mathbb{Q}$ ist also
$\mathrm{Irr}(\cos\alpha, \mathbb{Q}) = x^3 - \frac{3}{4}x - \frac{1}{8} \in \mathbb{Q}[x]$. (nach Bem 26.4)

Nach Bem 27.2 folgt

$$[\mathbb{Q}(\cos\alpha) : \mathbb{Q}] = \operatorname{grad} \mathrm{Irr}(\cos\alpha, \mathbb{Q}) = 3.$$

Nach Satz 28.2 ist also $\cos\alpha$ nicht konstruierbar.

Eine Dreiteilung eines Winkels $\alpha = 60°$ ist mit Zirkel und Lineal also nicht möglich.