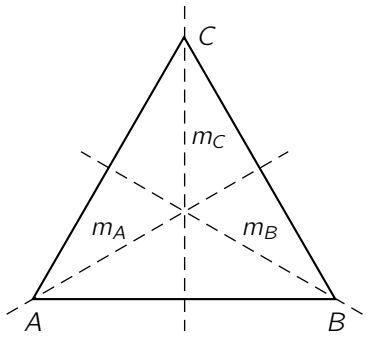
3 Gruppen

Wir betrachten ein *reguläres* Dreieck ABC und seine Symmetrien:



Welche Abbildungen/Symmetrieoperationen bilden das Dreieck auf sich selber ab?

- $\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} =$ „3“
- $\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} =$ „m_C“
- $\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} =$ „3^{-1}“
- $\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} =$ „m_A“
- $\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} =$ „1“
- $\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} =$ „m_B“

Abbildungen kann man hintereinander ausführen oder „zusammensetzen“. Man verwendet für diese Operation oft das Symbol $\circ$. Beachten Sie, dass die Abbildungen *von rechts nach links* zur Anwendung kommen:

$$(3 \circ m_A)(A) = 3(m_A(A)) = 3(A) = B$$

Die Abbildung $3 \circ m_A$ bildet also die Ecke A auf B ab. Weiter:

$$(3 \circ m_A)(B) = 3(m_A(B)) = 3(C) = A$$
$$(3 \circ m_A)(C) = 3(m_A(C)) = 3(B) = C$$

Die „Zusammensetzung“ $3 \circ m_A$ entspricht also der Abbildung

$$3 \circ m_A = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = m_C$$

Die Menge $D_3 = \{\, 1,\, 3,\, 3^{-1},\, m_A,\, m_B,\, m_C \,\}$ besitzt also mit $\circ$ eine interne Rechenoperation, zu welcher wir eine Tabelle aufstellen können, ähnlich wie die Additions- und Multiplikationstafeln bei den kleinen Zahlkörpern.

Wir berechnen noch zwei „Produkte“ und geben dann die ganze Tabelle an:

- $m_A \circ 3 = m_B$, denn
$$\begin{aligned} A &\longrightarrow B \longrightarrow C \\ B &\longrightarrow C \longrightarrow B \\ C &\longrightarrow A \longrightarrow A \end{aligned}$$

- $m_B \circ m_A = 3^{-1}$, denn
$$\begin{aligned} A &\longrightarrow A \longrightarrow C \\ B &\longrightarrow C \longrightarrow A \\ C &\longrightarrow B \longrightarrow B \end{aligned}$$

a \ b	1	3	3^{-1}	m_A	m_B	m_C
1	1	3	3^{-1}	m_A	m_B	m_C
3	3	3^{-1}	1	m_C	m_A	m_B
3^{-1}	3^{-1}	1	3	m_B	m_C	m_A
m_A	m_A	m_B	m_C	1	3	3^{-1}
m_B	m_B	m_C	m_A	3^{-1}	1	3
m_C	m_C	m_A	m_B	3	3^{-1}	1

Hier steht jeweils $a \circ b$ (also zuerst b, dann a anwenden!!)

Meditieren wir über dieser *Gruppentafel*, so stellen wir fest:

1. $a \circ b$ ist für alle Elemente definiert und liefert wieder ein Element der Menge (es liegt also eine *interne Operation* vor)
2. Es existiert ein Neutralelement, nämlich die 1
3. In jeder Zeile und in jeder Spalte steht jedes Element der Menge genau ein mal
4. Da 1 in jeder Zeile und in jeder Spalte steht, besitzt jedes Element ein Inverses bezüglich dieser Operation
5. Die Operation genügt dem Assoziativgesetz, da die Zusammensetzung von Abbildungen ganz allgemein assoziativ ist
6. Das Kommutativgesetz ist nicht erfüllt, es ist z. B. $m_A \circ 3 = m_B$, aber $3 \circ m_A = m_C$

Definition 3.1. Eine Menge M, in welcher eine Rechenoperation definiert ist (sei es $+$, $\cdot$, $\circ$, ...) heisst eine *Gruppe*, wenn für diese Operation die Axiome i) bis iii) erfüllt sind:

i) $[\forall\, a, b, c \in M]\,[\, a \circ (b \circ c) = (a \circ b) \circ c\,]$

ii) $[\exists\, 1 \in M]\,[\forall\, a \in M]\,[\, 1 \circ a = a \text{ und } a \circ 1 = a\,]$

iii) $[\forall\, a \in M]\,[\exists\, b \in M]\,[\, a \circ b = 1\,]$

Die Operation muss also assoziativ sein, es muss ein Neutralelement geben und jedes Element muss ein Inverses besitzen.

Definition 3.2. Eine Gruppe $(M, \circ)$, in welcher auch noch das Axiom iv) gilt, heisst eine *kommutative Gruppe* oder auch eine *Abelsche Gruppe*.

iv) $[\forall\, a, b \in M]\,[\, a \circ b = b \circ a\,]$

Wir hätten unseren Kurs auch mit dieser Definition starten können! Dann hätten wir später einen Körper folgendermassen definiert:

Ein Körper ist eine Menge k mit zwei Operationen $+$ und $\cdot$, für die gilt

- $(\, k, +)$ ist eine Abelsche Gruppe
- $(\, k \setminus \{\, 0\,\}, \cdot)$ ist eine Abelsche Gruppe
- die Operationen $+$ und $\cdot$ sind durch das Distributivgesetz miteinander verknüpft

Das heisst auch, dass wir schon ganz viele Gruppen kennen:

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{Q} \setminus \{\, 0\,\}, \cdot)$
- $(\mathbb{Z}_n, +)$
- $(\mathbb{Z}_n \times \mathbb{Z}_m\,, +)$
- $(\mathbb{M}^{n \times m}, +)$ über k
- $(\mathbb{R}, +)$
- $(\mathbb{R} \setminus \{\, 0\,\}, \cdot)$
- $(\mathbb{Z}_p \setminus \{\, 0\,\}, \cdot)$ p prim

Dazu kommen schnell noch viele weitere Beispiele:

- D_n, die Menge aller Symmetrien eines regulären n-Ecks 
- C_n, die Menge aller Drehsymmetrien eines regulären n-Ecks 
- S_n, die Menge aller Permutationen (Vertauschungen) in einer Menge mit n Elementen
- Zu jedem geometrischen Körper die Menge seiner Symmetrien (Quader, Tetraeder, Würfel, Prismen, Pyramiden usw.)

Aufgaben:

1. Wieviele Elemente haben die Gruppen C_n, D_n und S_n?
2. Die folgenden drei Gruppen enthalten alle 4 Elemente: C_4, die Drehsymmetrien eines Quadrates; D_2, alle Symmetrien eines Rechtecks sowie $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$, die multiplikative Gruppe im Zahlkörper $\mathbb{Z}_5$. Stellen Sie die drei Gruppentafeln auf. Welche dieser drei Gruppen sind ‚gleich'? Wann wird man zwei Gruppen ‚gleich' nennen?
3. Unser einführendes Beispiel war die Gruppe D_3. Jedes Element von D_3 bewirkt eine Permutation der drei Ecken. Gehört zu jeder Permutation von (A, B, C) auch eine Dreieckssymmetrie? Sind die Gruppen D_3 und S_3 also ‚gleich'?
4. Wieviele Elemente enthält die Tetraeder-Gruppe? Liefert *jede* Vertauschung der 4 Ecken eines Tetraders eine Tetraedersymmetrie? Wenn ja: Welche andere Gruppe wäre dann ‚gleich' wie die Tetraedergruppe?
5. Wie gross ist die Symmetriegruppe eines **Quaders**? Stellen Sie die Gruppentafel auf. Fangen Sie dabei mit der Identität und den Drehungen um 180ř an. Werfen Sie am Schluss einen Blick auf die Hauptdiagonale der Gruppentafel!
6. Zählt man die identische Abbildung 1 mit, so gibt es 24 Drehungen, die einen Würfel auf sich selber abbilden. Warum *muss* dann ein Würfel insgesamt 48 Symmetrien aufweisen, wenn man die Spiegelungen auch hinzunimmt?

Definition 3.3. Es seien $(M, \cdot)$ und $(G, \circ)$ zwei Gruppen. Diese heissen *isomorph*, wenn es eine bijektive Abbildung

$f : M \longrightarrow G$ gibt mit $[\forall\, a, b \in M]\,[\, f(a \cdot b) = f(a) \circ f(b)\,]$

Bemerkungen:

- M und G müssen gleich viele Elemente haben, wenn sie isomorph sind (sonst gibt es keine Bijektion von M auf G)
- f bildet 1_M zwingend auf 1_G ab: $f(a) = f(1_M \cdot a) = f(1_M) \circ f(a) \implies f(1_M) = 1_G$
- Es gilt $f(a^{-1}) = [f(a)]^{-1}$ wegen $f(a) \circ f(a^{-1}) = f(a \cdot a^{-1}) = f(1_M) = 1_G = f(a) \circ [f(a)]^{-1}$

Ein Gruppenisomorphismus f transportiert also die ganze Gruppenstruktur von M auf G hinüber; und f^{-1} macht dasselbe in der Gegenrichtung. Sind zwei Gruppen isomorph, so unterscheiden sie sich in ihrer Struktur nicht. Was bedeuten die Komponenten „iso" und „morph" in anderen Ihnen bereits bekannten Begriffen?!

Weitere wichtige Beispiele von Gruppen erhalten wir, wenn wir den folgenden Satz bewiesen haben:

Satz 3.4. Es sei $(M, +, \cdot)$ ein Ring. M^* sei die Menge derjenigen Elemente von M, die ein multiplikatives Inverses besitzen. Dann bildet $(M^*, \cdot)$ eine Gruppe.

Bevor wir den Satz beweisen, wollen wir am Beispiel $(\mathbb{Z}_{10}, +, \cdot)$ schauen, was damit genau gemeint ist:

$$\mathbb{Z}_{10}^* = \{\, \not{0}, 1, \not{2}, 3, \not{4}, \not{5}, \not{6}, 7, \not{8}, 9 \,\} = \{\, 1, 3, 7, 9 \,\}$$

Wir betrachten nun die Multiplikationstafel in $\mathbb{Z}_{10}^*$:

$\mathbb{Z}_{10}^*$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Es liegt tatsächlich eine interne Operation in der Menge $\mathbb{Z}_{10}^*$ vor!

Beweis von Satz 3.4

- Es ist $1_M \in M^*$ wegen $1 \cdot 1 = 1$.
- Jedes Element in M^* hat ein Inverses gemäss Definition.
- Sind a, $b \in M^*$, dann auch $a \cdot b$ und $b \cdot a$, da $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ (wie in Lemma 2.14). Die Multiplikation ist also eine interne Operation in M^*.
- Die Multiplikation ist assoziativ, weil sie es in M ja schon ist.

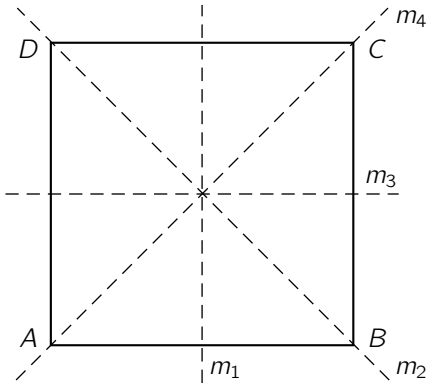
□

Ist der Ring $(M, +, \cdot)$ kommutatitiv wie im Falle von $\mathbb{Z}_n$, dann ist auch die Gruppe $(M^*, \cdot)$ kommutativ.

Aufgaben:

1. Studieren Sie $\mathbb{Z}_4^*$, $\mathbb{Z}_6^*$, $\mathbb{Z}_8^*$, $\mathbb{Z}_9^*$ und $\mathbb{Z}_{10}^*$
2. Können Sie isomorphe Gruppen finden zu den Gruppen der Aufgabe 1, wenn Sie an C_n, D_n oder S_n denken?
3. Beweisen Sie die folgende Behauptung:

   $[\forall\, a \in \mathbb{Z}_n\,]\,[\,a \in \mathbb{Z}_n^* \iff \mathrm{ggT}(a, n) = 1\,]$
4. Wieviele Elemente haben die Gruppen $\mathbb{Z}_{15}^*$, $\mathbb{Z}_{16}^*$, $\mathbb{Z}_{20}^*$ und $\mathbb{Z}_{24}^*$? Welche von diesen Gruppen sind isomorph zueinander?
   Ein Tip: Betrachten Sie die Menge der Quadrate in diesen vier Gruppen! Können Sie einen Gegenstand basteln oder zeichnen, dessen Symmetriegruppe isomorph ist zu $\mathbb{Z}_{15}^*$?

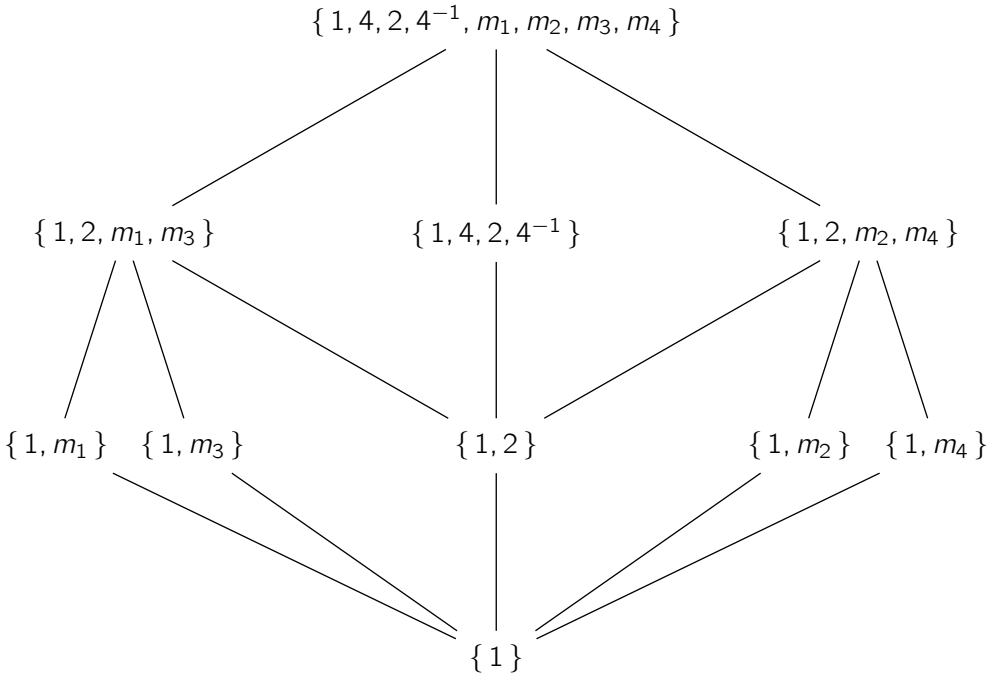


Betrachten wir nun D_4, die Gruppe aller Symmetrien eines Quadrates.

C_4, die Menge der Drehsymmetrien, ist eine Teilmenge von D_4 und selber auch eine Gruppe.

In C_4 finden wir noch die Teilmenge $C_2 = \{1, 2\}$, welche ebenfalls eine Gruppe ist, und in dieser Gruppe steckt noch die ‚triviale' Gruppe $C_1 = \{1\}$, welche nur aus der identischen Abbildung besteht.

D_4 enthält aber noch weitere *Untergruppen*: $\{1, m_i\}$ ist für jede der 4 Achsenspiegelungen eine Gruppe vom Typ $D_1 \cong C_2$. Zudem sind $\{1, 2, m_1, m_3\}$ und $\{1, 2, m_2, m_4\}$ Untergruppen vom Typ D_2. Das folgende Diagramm stellt alle diese Untergruppenbeziehungen dar:



Solche Betrachtungen führen zu der folgenden Definition:

Definition 3.5. Es sei $(G, \cdot)$ eine Gruppe, und es sei H eine nicht-leere Teilmenge von G. Ist für alle $a, b \in H$ auch $a \cdot b \in H$, und ist für alle $a \in H$ auch $a^{-1} \in H$, so ist $(H, \cdot)$ ebenfalls eine Gruppe. Man nennt dann H eine *Untergruppe* von G.

Bemerkungen:

- Man braucht $1 \in H$ nicht zu verlangen: H enthält ja mindestens ein Element a und damit auch a^{-1} und $a \cdot a^{-1} = 1$.
- Bezeichnet man mit $\text{ord}(H)$ die Anzahl Elemente der Menge H, so gilt also immer
$$1 \leq \text{ord}(H) \leq \text{ord}(G),$$
wenn H eine Untergruppe ist von G.
- $\{1\}$ und G selber sind Untergruppen von G, und eine Gruppe braucht keine andern Untergruppen zu haben, wie das Beispiel $(\mathbb{Z}_5, +)$ zeigt.

Lemma 3.6. Es seien H und K zwei Untergruppen von $(G, \cdot)$. Dann ist auch $H \cap K$ eine Untergruppe von G.

Beweis

- $H \cap K$ ist nicht leer, da $1 \in H$ und $1 \in K$
- $a \in H \cap K \implies a \in H$ und $a \in K \implies a^{-1} \in H$ und $a^{-1} \in K$
$\implies a^{-1} \in H \cap K$
- $a, b \in H \cap K \implies a, b \in H$ und $a, b \in K \implies a \cdot b \in H$ und $a \cdot b \in K$
$\implies a \cdot b \in H \cap K$

□

Lemma 3.7. Es seien H und K zwei Untergruppen von $(G, \cdot)$. Dann gibt es eine eindeutig bestimmte kleinste Untergruppe $L \subset G$ mit $H \subset L$ und $K \subset L$.

Beweis

- Es gibt solche Untergruppen L von G mit $H \subset L$ und $K \subset L$, nämlich mindestens G selber.
- Gibt es mehrere solche Untergruppen L, dann bilde den Durchschnitt über all diese Untergruppen. Dieser bildet das kleinstmögliche L.
- Gäbe es zwei verschiedene solcher minimalen L's, dann wäre ihr Durchnitt eine noch kleinere Lösung, im Widerspruch dazu, dass die L's schon minimal waren.

□

Bemerkung: L ist sozusagen die minimale *Obergruppe* von H und K in G. Dieser Ausdruck wird allerdings nicht verwendet.

Lemma 3.8. Die Menge aller Untergruppen einer Gruppe bildet einen *Verband*, so wie die Menge aller Teiler einer natürlichen Zahl einen Verband bildet. Hier der Durchschnitt zweier Untergruppen, dort der ggT zweier Teiler. Hier die kleinste Obergruppe, dort das kgV.

Dieses Lemma können wir nicht beweisen, da wir nicht exakt gesagt haben, was ein *Verband* sein soll. Zeichnen Sie aber die Teilerverbände der Zahlen 48 und 60 auf!

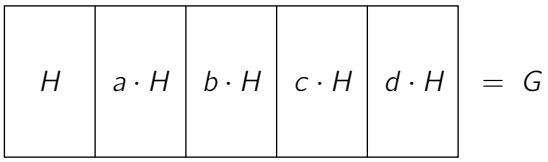
In einem Verband gibt es immer ein kleinstes und ein grösstes Element. Im Teilerverband einer Zahl n sind das die 1 und n selber. Wer hat diese Rollen im Verband der Untergruppen von G?

Was unterscheidet diese ‚Grössenrelation'in einem Verband von der Grössenrelation in den reellen Zahlen?

Die Beziehungen zwischen Teilerverbänden und Verbänden von Untergruppen gehen tiefer, wie der nächste Satz zeigt:

Satz 3.9. Sei H eine Untergruppe von G. Dann ist ord(H) ein Teiler von ord(G).

Beweis: Wir zeigen, dass die Mengen $a \cdot H = \{ a \cdot b \mid b \in H \}$ eine *Partition* der Gruppe G bilden, wobei jede der Teilmengen genau ord(H) Elemente enthält. Wenn das stimmt, folgt daraus sofort die Behauptung.



- Für alle $h \in H$ gilt $h \cdot H = H$:

  Ist $k \in H$, so auch $h \cdot k$, und ist $l \in H$, dann gibt es auch ein $k \in H$ mit $h \cdot k = l$, nämlich $h^{-1} \cdot l$.

- Sei jetzt $b \in G$ mit $b \notin H$. Dann sind alle Produkte $b \cdot h$ mit $h \in H$ verschieden, und es gilt somit ord($b \cdot H$) = ord(H). Aus $b \cdot h = b \cdot k$ mit $h, k \in H$ folgt nämlich:

  $b \cdot h \cdot k^{-1} = b \cdot k \cdot k^{-1} = b \cdot 1 = b$. Somit gilt $h \cdot k^{-1} = 1$, also $h = k$.

- Nun seien $a, b \in G$. Dann gilt $a \cdot H = b \cdot H$ oder $a \cdot H \cap b \cdot H = \emptyset$. Wir zeigen $a \cdot H = b \cdot H$, falls der Durchschnitt von $a \cdot H$ und $b \cdot H$ nicht leer ist:

  Es sei also $c \in a \cdot H \cap b \cdot H$. Es gibt also $h, k \in H$ mit $c = a \cdot h$ und $c = b \cdot k$. Dann ist $a \cdot h = b \cdot k$, $a \cdot h \cdot k^{-1} = b \cdot k \cdot k^{-1} = b \cdot 1 = b$ und $b^{-1} \cdot a \cdot h \cdot k^{-1} = b^{-1} \cdot b = 1$.

  $b^{-1} \cdot a$ ist also das Inverse von $h \cdot k^{-1}$, somit $b^{-1} \cdot a \in H$.

  Daraus folgt nach Punkt 1 $b \cdot H = b \cdot (b^{-1} \cdot a \cdot H) = b \cdot b^{-1} \cdot (a \cdot H) = a \cdot H$.

Die *Nebenklassen* $a \cdot H$ der Untergruppe H bilden also tatsächlich eine Partition von G, und alle Nebenklassen haben gleich viele Elemente.

□

Aber nicht nur die Untergruppen einer Gruppe G, sondern auch deren Elemente stehen in einer Beziehung zu den Teilern von $\mathrm{ord}(G)$. Dazu brauchen wir

Definition 3.10. Sei G eine beliebige Gruppe. Wir definieren

i) $[\forall\, g \in G\,]\,[\,g^0 := 1\,]$

ii) $[\forall\, g \in G\,]\,[\forall\, n \in \mathbb{N} \setminus \{0\}\,]\,[\,g^n := g \cdot g^{n-1}\,]$

iii) $[\forall\, g \in G\,]\,[\,g^{-1} := k \text{ wo } g \cdot k = 1\,]$

iv) $[\forall\, g \in G\,]\,[\forall\, n \in \mathbb{N} \setminus \{0\}\,]\,[\,g^{-n} := k^n \text{ wo } g \cdot k = 1\,]$

Damit ist für jedes Element g einer beliebigen Gruppe G und für jede Zahl $z \in \mathbb{Z}$ der Term g^z definiert. Es gelten dabei erwartungsgemäss die folgenden Regeln für Potenzen:

Lemma 3.11. In jeder Gruppe gelten die folgenden Potenzgesetze für ganzzahlige Exponenten:

i) $[\forall\, g \in G\,]\,[\forall\, m, n \in \mathbb{Z}\,]\,[\,g^m \cdot g^n = g^{m+n}\,]$

ii) $[\forall\, g \in G\,]\,[\forall\, n \in \mathbb{Z}\,]\,[\,g^{-n} = (g^n)^{-1}\,]$

iii) $[\forall\, g \in G\,]\,[\forall\, m, n \in \mathbb{Z}\,]\,[\,(g^m)^n = g^{m \cdot n}\,]$

Die Beweise sind nicht schwierig und sind dem Leser als Übung überlassen. Beachten Sie dass ein viertes Potenz-Rechengesetz nur gilt, wenn die Gruppe G kommutativ ist:

iv) $[\forall\, g, h \in G\,]\,[\forall\, n \in \mathbb{Z}\,]\,[\,g^n \cdot h^n = (g \cdot h)^n\,]$

In $(\mathbb{Z}_n^*, \cdot)$ ist das aber immer der Fall.

Lemma 3.12. Es sei G eine endliche Gruppe der Ordnung n. Zudem sei $a \in G$. Dann gibt es ein $k \in \mathbb{N}$ mit $1 \leq k \leq n$ sodass gilt $a^k = 1$.

Beweis: Betrachte die n (nicht unbedingt verschiedenen) Elemente $a, a^2, a^3, \ldots, a^n$ in G. Sind sie alle verschieden, dann muss eines schon 1 sein, da ja G nur n Elemente enthält. Andernfalls gilt $a^k = a^l$ mit $1 \leq k < l \leq n$. Wir setzen $p := l - k$, somit $1 \leq p < l \leq n$.

Es ist $a^k \cdot a^p = a^k \cdot a^{l-k} = a^{k+(l-k)} = a^l$. Wegen $a^k = a^l$ folgt daraus $a^p = 1$. □

Lemma 3.13. Es sei G eine endliche Gruppe der Ordnung n, zudem sei $a \in G$. Weiter sei k die **kleinste** Zahl in $\mathbb{N}$ mit $a^k = 1$.

Dann sind die Elemente $a, a^2, a^3, \ldots, a^k$ alle verschieden, und sie bilden eine kommutative Untergruppe A in G der Ordnung k.

Bemerkung: k heisst dann auch die *Ordnung des Elements* a, und A ist die *von* a *erzeugte Untergruppe* von G.

Beweis: Die Menge $\{ a, a^2, a^3, \ldots, a^k \}$ ist abgeschlossen in bezug auf die Multiplikation:

$$a^i \cdot a^j = a^{i+j} = a^{(i+j) \bmod k} \text{ mit } a^0 = 1$$

Die Menge enthält auch genau k Elemente, denn wären nicht alle a^i verschieden, dann könnten wir wie im Beweis von Lemma 3.12 folgern, dass es ein $p < k$ gäbe mit $a^p = 1$ im Widerspruch dazu, dass k die kleinste Zahl sein soll mit $a^k = 1$. □

Aufgabe: Bestimmen Sie die Ordnungen der Elemente in $\mathbb{Z}_7^*$, $\mathbb{Z}_8^*$, $\mathbb{Z}_9^*$ und $\mathbb{Z}_{10}^*$.

Korollar 3.14. Sei G eine endliche Gruppe der Ordnung n, und A sei die von $a \in G$ erzeugte Untergruppe der Ordnung k. Dann ist k ein Teiler von n, und es gilt immer $a^n = 1$.

Beweis: Satz 3.9 sagt uns, dass k ein Teiler ist von n, also $k \cdot p = n$ für ein $p \in \mathbb{N}$. Somit gilt $a^n = a^{k \cdot p} = (a^k)^p = 1^p = 1$. □

Da $a \in G$ im Korollar 3.14 beliebig gewählt ist, können wir auch sagen: Die Ordnung eines Elements einer endlichen Gruppe ist immer ein Teiler der Gruppenordnung, und für alle Elemente a gilt $a^{\text{ord}(G)} = 1$. Diesen Satz werden wir im nächsten Dokument „RSA und PGP“ massiv benützen.

Gratis erhalten wir noch das folgende

Korollar 3.15. Jede Gruppe von Primzahlordnung ist zyklisch und damit auch kommutativ. Jedes Element ausser 1 ist in einer solchen Gruppe erzeugend.

Beweis: Jedes Element a erzeugt eine zyklische Untergruppe $A = \{ a, a^2, a^3, \ldots, a^k \}$. Da $\text{ord}(A)$ ein Teiler sein muss von $\text{ord}(G)$, $\text{ord}(G)$ aber eine Primzahl ist, folgt schon $k = p$ und daraus $A = G$. □

Einfache Beispiele für Korollar 3.15 sind die additiven Gruppen $(\mathbb{Z}_p, +)$, wo p eine Primzahl ist. Korollar 3.15 sagt uns, dass alle Gruppen mit $\text{ord}(G) = p$ isomorph sind zu $(\mathbb{Z}_p, +)$.

Ebenfalls gratis können wir den *kleinen Satz von Fermat* ernten:

Korollar 3.16. Es sei p eine Primzahl. Dann gilt $a^p = a$ modulo p.

Beweis: Die Gruppe $(\mathbb{Z}_p^*, \cdot)$ enthält $p - 1$ Elemente. Es ist somit $\text{ord}(\mathbb{Z}_p^*) = p - 1$ und damit nach Korollar 3.14 $a^{p-1} = 1$ modulo p. Multipliziert man die Gleichung beidseits mit a, erhält man die Behauptung. □

Aufgaben:

1. Wir betrachten die Gruppe $(\mathbb{Z}_{17}^*, \cdot)$. Bilden Sie für $k = 1, 2, 3, 4$ die Mengen $\{ a^k \mid a \in \mathbb{Z}_{17}^* \}$.

2. Es sei $f : G \longrightarrow H$ ein Gruppenhomomorphismus (f genüge also den Forderungen von Definition 3.3, nur dass f nicht notwendigerweise bijektiv sein muss). Beweisen Sie:

a) Der Kern von f, also $\{ a \in G \mid f(a) = 1_H \}$, ist eine Untergruppe von G.

b) Das Bild von f, also $\{ b \in H \mid [\exists\, a \in G][\, b = f(a)\,] \}$, ist eine Untergruppe von H.

3. Zeigen Sie, dass für jeden Gruppenhomomorphismus $f : G \longrightarrow H$ gilt:

$$\text{ord}(\text{Kern von } f) \cdot \text{ord}(\text{Bild von } f) = \text{ord}(G)$$

4. Zeigen Sie: Für eine Abelsche Gruppe $(G, \cdot)$ ist die Abbildung $f : G \longrightarrow G$, $f(a) = a^k$ für jedes $k \in \mathbb{N}$ ein Gruppenhomomorphismus.

5. Es sei G eine Abelsche Gruppe von gerader Ordnung. Zeigen Sie, dass der Kern der Quadratfunktion $f : G \longrightarrow G$, $f(a) = a^2$ nicht nur aus 1_G besteht. Tipp: Zeigen Sie zuerst, dass eine solche Gruppe auch ein Element von gerader Ordnung enthalten muss!

6. Folgern Sie aus **3.** und **5.**, dass es in der Gruppe $(\mathbb{Z}_p^*, \cdot)$ für $p \geq 3$ Elemente geben muss, die **keine** Quadrate sind.

7. Zeigen Sie in $(\mathbb{Z}_p^*, \cdot)$, $p \geq 3$, dass für alle Elemente $a \in \mathbb{Z}_p^*$ gilt $a^2 = (p - a)^2$ modulo p. Ziehen Sie daraus und aus **3.** ebenfalls den Schluss, dass $(\mathbb{Z}_p^*, \cdot)$ für $p \geq 3$ Element enthalten muss, die **keine** Quadrate sind.

8. Nach **6.** und **7.** gibt es also in $\mathbb{Z}_p^*$, $p \geq 3$ eine Zahl c, die nicht als Quadrat geschrieben werden kann. Wir setzen $i^2 = c$ und bilden die Menge $\mathbb{F}_{p^2} = \{ a + b \cdot i \mid a, b \in \mathbb{Z}_p \}$. Zeigen Sie, dass $\mathbb{F}_{p^2}$ ähnlich wie $\mathbb{C}$ aus $\mathbb{R}$ zu einem Körper gemacht werden kann.

Wo braucht man genau die Eigenschaft, dass c keine Quadratzahl ist?

9. Zeigen Sie, dass es auch zu $p = 2$ einen Körper mit $p^2 = 4$ Elementen gibt. Setzen Sie $\mathbb{F}_4 = \{ 0, 1, i, j \}$ und denken Sie daran, dass C_3 (bis auf Isomorphie) die einzige Gruppe mit drei Elementen ist, $\mathbb{F}_4^*$ also schon festgelegt ist.

10. Es sei $(k, +, \cdot)$ ein Körper. Zeigen Sie: Der Kern von $f : k^* \longrightarrow k^*$, $f(a) = a^n$ enthält höchstens n Elemente. Erinnern Sie sich an die Polynomdivision und das Abspalten von Nullstellen als lineare Faktoren ...

11. Folgern Sie aus **5.** und **10.**, dass in der multiplikativen Gruppe $\mathbb{Z}_p^*$ mit $p \geq 3$ genau die Hälfte aller Elemente Quadratzahlen sind.

12. Schon recht anspruchsvoll ist die Verallgemeinerung von **5.**: Es sei G eine Abelsche Gruppe der Ordnung n, und p sei ein Primfaktor von n. Zeigen Sie, dass dann ein Element $a \in G$ existiert mit $\text{ord}(a) = p$.

13. Zeigen Sie, dass aus **10.** und **12.** folgt: Ist die Primzahl q ein Teiler der Ordnung von $\mathbb{Z}_p^*$, also von $p - 1$, so gibt es in $\mathbb{Z}_p^*$ genau q Lösungen der Gleichung $x^q = 1$.

Bemerkungen:

- Man kann zeigen, dass es zu jeder Primzahl p und jeder natürlichen Zahl $k \geq 1$ bis auf Isomorphie genau einen Zahlkörper $\mathbb{F}_{p^k}$ gibt, der p^k Elemente enthält. Zudem kann man zeigen, dass diese Liste **alle** endlichen Körper enthält.
- Ist k ein Körper, so ist jede endliche Untergruppe von $(k^*, \cdot)$ zyklisch, d.h. es gibt ein Element $a \in k^*$, welches mit seinen Potenzen die ganze Untergruppe erzeugt.

  Denken Sie zum Beispiel an die $n$ten Einheitswurzeln in $\mathbb{C}$!
- Aus dem letzten Punkt folgt insbesondere, dass die multiplikativen Gruppen $\mathbb{Z}_p^*$ und alle ihre Untergruppen zyklisch sind. Es gibt aber keine schnelle Methode, ein erzeugendes Element für $\mathbb{Z}_p^*$ zu finden.
- Aus dem vorangehenden Punkt folgt wiederum, dass es zu jedem Teiler t von $n = \text{ord}(\mathbb{Z}_p^*)$ auch ein Element geben muss, welches diese Ordnung hat.
- Sehr allgemeine Resultate auch für nicht-abelsche Gruppen liegen in den **Sätzen von Sylow** vor ($\rightarrow$ wikipedia).

Version 2.0, vom Juli 2011

Ausgearbeitet von Martin Gubler, Kantonsschule Frauenfeld, anno 1999

Mit LaTeX in eine lesbare Form gebracht von Alfred Hepp im Juli 2011