Mathematik I für Studierende der Informatik und Wirtschaftsinformatik (Diskrete Mathematik) im Wintersemester 2017/2018

11. Januar 2018

Gruppen

Erinnerung: Eine Gruppe ist eine algebraische Struktur $(G, *)$ mit einer zweistelligen Verknüpfung $*$ so dass gilt:

1. Die Verknüpfung $*$ erfüllt das Assoziativgesetz:
   $\forall a, b, c \in G((a * b) * c = a * (b * c))$
2. Es gibt ein neutrales Element $e \in G$:
   $\forall a \in G(a * e = a = e * a)$
3. Jedes Element von G hat ein Inverses:
   $\forall a \in G \exists b \in G(a * b = e = b * a)$

Das neutrale Element einer Gruppe ist eindeutig bestimmt.
Zu jedem Gruppenelement a gibt es genau ein Inverses, das wir mit a^{-1} bezeichnen.
Das Zeichen $*$ lassen wir oft weg, wie den Malpunkt der Multiplikation auf den reellen Zahlen (ab anstelle von $a * b$).

Untergruppen und Nebenklassen

Definition 7.27

Sei $(G, *)$ eine Gruppe. Dann heißt $U \subseteq G$ eine *Untergruppe*, von G, falls U zusammen mit der Einschränkung der Operation $*$ auf $U \times U$ wieder eine Gruppe ist.

Satz 7.29

Sei G eine Gruppe und $U \subseteq G$.

a) U ist genau dann eine Untergruppe von G, wenn für alle $a, b \in U$ gilt: $e, a^{-1}, ab \in U$

b) U ist genau dann eine Untergruppe von G, falls U nicht leer ist und für alle $a, b \in U$ gilt: $ab^{-1} \in U$

c) Ist U endlich, so ist U bereits dann eine Untergruppe von G, falls U nicht leer ist und für alle $a, b \in U$ gilt: $ab \in U$

Definition 7.30

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe.
Für $a \in G$ schreiben wir aU für die Menge $\{ag : g \in U\}$ sowie Ua für die Menge $\{ga : g \in U\}$.
Wir nennen die Mengen der Form aU *Linksnebenklassen* von U und die Mengen der Form Ua *Rechtsnebenklassen*.

Beispiel 7.31

a) Sei $G = (\mathbb{Z}, +)$, und $U = 6\mathbb{Z}$.
Dann ist die Rechtsnebenklasse von 4 von U die Menge
$6\mathbb{Z} + 4 = \{\ldots, -2, 4, 10, \ldots\} = [4]_6$.
Hierbei beachte man, dass die Operation die Gruppe G die Addition ist, auch wenn wir die Operation auf einer Gruppe im Allgemeinen multiplikativ schreiben.
Die Linksnebenklasse von 4 von U ist die Menge $4 + 6\mathbb{Z}$, die aber mit $6\mathbb{Z} + 4$ übereinstimmt, da $+$ das Kommutativgesetz erfüllt.

b) Wir betrachten die Gruppe $G_\triangle$ und die Untergruppe $U = \{i, y\}$. Dann gilt $iU = \{i, y\}$, $xU = \{x, r\}$, $yU = \{y, i\}$, $zU = \{z, s\}$, $rU = \{r, x\}$ und $sU = \{s, z\}$, wie man leicht an der Gruppentafel von $G_\triangle$ abliest.
Die verschiedenen Linksnebenklassen von U in $G_\triangle$ sind also die Mengen $iU = yU = U = \{i, y\}$, $xU = rU = \{r, x\}$ und $zU = sU = \{z, s\}$.

Die entsprechende Rechnung liefert die Rechtsnebenklassen $Ui = Uy = U = \{i, y\}$, $Ux = Us = \{x, s\}$ und $Uz = Ur = \{z, r\}$.

Satz 7.32

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe.

a) Für jedes $a \in G$ ist $a \in aU$ und $a \in Ua$.

b) Für alle $c \in U$ ist $cU = U = Uc$.

c) Für $a, b \in G$ mit $b \in aU$ gilt $aU = bU$.
Für $a, b \in G$ mit $b \in Ua$ gilt $Ua = Ub$.

d) Für $a, b \in G$ sind die Linksnebenklassen aU und bU entweder disjunkt oder gleich.
Auch die Rechtsnebenklassen Ua und Ub sind entweder disjunkt oder gleich.

e) Für alle $a \in G$ sind aU, U und Ua gleichmächtig.

Beweis.

a) Wegen $e \in U$ gilt $a = ae \in aU$ und $a = ea \in Ua$.

b) Sei $c \in U$. Es ist klar, dass $cU, Uc \subseteq U$ gilt. Sei nun $d \in U$. Dann ist $c^{-1}d \in U$. Also ist $d = cc^{-1}d \in cU$. Das zeigt $U \subseteq cU$. Auf ähnliche Weise sieht man $cU \subseteq U$, $U \subseteq Uc$ und $Uc \subseteq U$. Also ist $U = cU = Uc$

c) Ist $b \in aU$, so existiert $c \in U$ mit $b = ac$. Es gilt $bU = acU = aU$.
Auf ähnliche Weise sieht man $U = Ub$, falls $b \in Ua$ gilt.

d) Falls $aU \cap bU$ nicht leer ist, so existiert $c \in aU \cap bU$. Nach c) gilt $aU = cU = bU$.
Auf ähnliche Weise sieht man, dass Ua und Ub entweder gleich oder disjunkt sind.

e) Wir zeigen nur, dass U und aU gleichmächtig sind, indem wir eine Bijektion zwischen beiden Mengen angeben.
Die Gleichmächtigkeit von U und Ua kann auf ähnliche Weise nachgerechnet werden.
Sei $f : U \to aU; b \mapsto ab$. Aus der Definition von aU folgt sofort, dass f surjektiv ist. Seien nun $b, c \in U$ mit
$ab = f(b) = f(c) = ac$. Durch Multiplikation von links mit a^{-1} folgt daraus $b = c$. Damit ist f injektiv. Also sind U und aU in der Tat gleichmächtig. Das beendet den Beweis des Satzes.

Für eine Gruppe G nennen wir $|G|$ die *Ordnung* der Gruppe.

Beispiel 7.33

Sei G eine Gruppe und $a \in G$.
Dann ist $U = \{a^n : n \in \mathbb{Z}\}$ eine Untergruppe von G, die von a *erzeugte Untergruppe* von G.
Die Ordnung von U ist genau die Ordnung von a.
Wir schreiben $\langle a \rangle$ für die von a erzeugte Untergruppe.

Korollar 7.34 (Satz von Lagrange)

Ist G eine endliche Gruppe und U eine Untergruppe von G, so ist die Ordnung von U ein Teiler der Ordnung von G.
Insbesondere ist die Ordnung von jedem Element von G ein Teiler von $|G|$.

Definition 7.35

Sei G eine Gruppe und G eine Untergruppe von G.
Die Zahl der Rechtsnebenklassen von U in G (die identisch ist mit der Zahl der Linksnebenklassen) nennt man den *Index* von U in G.
Man schreibt $[G : U]$ für den Index von U in G.

Der Beweis des Satzes von Lagrange zeigt also für jede endliche Gruppe G und jede Untergruppe U die Gleichung

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

was auch die Notation $[G : U]$ erklärt.

Beispiel 7.36

Wir betrachten wieder die Dreiecksgruppe $G_\triangle$.
Die Gruppe hat 6 Elemente.
Also sind die möglichen Ordnungen von Untergruppen von G die Zahlen 1, 2, 3 und 6.
Die einzige Untergruppe der Ordnung 1 ist $\{i\}$. Diese Untergruppe hat den Index 6.

Ist $U \subseteq G_\triangle$ eine Untergruppe der Ordnung 2, so enthält U das Element i und ein weiteres Element, dass die Ordnung 2 haben muss.
Damit sind die Untergruppen der Ordnung 2 genau $\{i, x\}$, $\{i, y\}$ und $\{i, z\}$. Diese Untergruppen haben den Index 3.

Sei nun U eine Untergruppe von G der Ordnung 3.
Nach Korollar 7.34 hat jedes Element von U eine Ordnung, die die Zahl 3 teilt.
Also hat U nur Elemente der Ordnung 1 und 3.
Damit ist $U = \{i, r, s\}$. Diese Untergruppe hat den Index 2.

Die einzige Untergruppe von $G_\triangle$ mit 6 Elementen ist $G_\triangle$ selbst.
Diese Untergruppe hat den Index 1.

Wir bestimmen die Nebenklassen der Untergruppen von $G_\triangle$.
Für jede Untergruppe U ist $U = iU = Ui$ sowohl eine Rechts- als auch Linksnebenklasse.
$U = G_\triangle$ hat nur die Nebenklasse U, und hierbei ist es egal, ob wir Rechts- oder Linksnebenklassen betrachten.

$U = \{i, r, s\}$ hat die Rechts und Linksnebenklasse U.
Da die Nebenklassen alle dieselbe Mächtigkeit haben wie U und eine Partition von $G_\triangle$ bilden, gibt es genau eine weitere Nebenklasse, nämlich $\{x, y, z\}$.
Diese Menge ist wieder sowohl Rechts- als auch Linksnebenklasse.

Nun betrachten wir eine Untergruppe der Ordnung 2, zum Beispiel $U = \{i, x\}$.
Es gibt insgesamt 3 Rechts- und 3 Linksnebenklassen.
Eine Nebenklasse, die sowohl Rechts- als auch Linksnebenklasse ist, ist U selbst.
Es gilt $yU = \{y, s\}$, wie wir der Gruppentafel von $G_\triangle$ entnehmen.
$\{y, s\}$ ist also eine Linksnebenklasse von U.
Da die Linksnebenklassen von U eine Partition von $G_\triangle$ bilden und alle dieselbe Mächtigkeit haben, hat U noch eine dritte Linksnebenklasse, nämlich $\{z, r\}$.

Auf dieselbe Weise rechnet man nach, dass die Rechtsnebenklassen von U genau die Mengen U, $Uy = \{y, r\}$ und $\{z, s\}$ sind.
Insbesondere sind die Linksnebenklassen von U in $G_\triangle$ nicht identisch mit den Rechtsnebenklassen.

Die Nebenklassen von $U = \{i\}$ sind die Einermengen $U = \{i\}$, $\{x\}$, $\{y\}$, $\{z\}$, $\{r\}$ und $\{s\}$.
Hierbei stimmen wieder die Links- und Rechtsnebenklassen überein, auch wenn $G_\triangle$ nicht abelsch ist.

Beispiel 7.37

Auch wenn die Gruppe G und ihre Untergruppe U unendlich sind, kann es sein, dass der Index von U in G endlich ist.
Für jedes $m \in \mathbb{N}$ ist $m\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ und es gilt

$$[\mathbb{Z} : m\mathbb{Z}] = m,$$

da die Mengen $[0]_m, \ldots, [m-1]_m$ genau die verschiedenen Nebenklassen von $m\mathbb{Z}$ in $\mathbb{Z}$ sind.
In $\mathbb{Z}$ ist es nicht nötig, zwischen Links- und Rechtsnebenklassen zu unterscheiden, da die Gruppe abelsch ist.

Beispiel 7.38

Aus dem Satz von Lagrange (Korollar 7.34) können wir sehr einfach den Satz von Fermat und Euler (Satz 6.14) folgern.
Sei $m \geq 2$ und $n \in \mathbb{Z}$ zu m teilerfremd. Dann ist $[n]_m \in E(\mathbb{Z}_m)$ und $E(\mathbb{Z}_m)$ hat die Ordnung $\varphi(m)$.
Nach dem Satz von Lagrange ist die Ordnung von $[n]_m$ in $E(\mathbb{Z}_m)$ ein Teiler der Ordnung $\varphi(m)$ von $E(\mathbb{Z}_m)$.
Damit gilt aber $([n]_m)^{\varphi(m)} = [1]_m$, also $n^{\varphi(m)} \equiv 1 \pmod{m}$.

Satz 7.39

Sei G eine zyklische Gruppe. Ist U eine Untergruppe von G, so ist auch U zyklisch.

Beweis. Sei a das erzeugende Element von G, also $G = \{a^n : n \in \mathbb{Z}\}$. Ist $U = \{e\}$, so ist U zyklisch. Wir können also annehmen, dass U ein von e verschiedenes Element enthält. Also gibt es ein $n \in \mathbb{Z}$ mit $n \neq 0$ und $a^n \in U$. Mit a^n ist auch $a^{-n} = (a^n)^{-1}$ in U. Damit existiert ein $n > 0$ mit $a^n \in U$.

Sei nun m die kleinste natürliche Zahl mit $a^m \in U$. Wir zeigen, dass alle Elemente von U Potenzen von a^m sind.

Sei $a^n \in U$. Wir zeigen, dass n ein Vielfaches von m ist. Wieder können wir annehmen, dass $n > 0$ ist.

Seien $q, r \in \mathbb{Z}$ mit $n = qm + r$ und $0 \leq r < m$. Dann gilt $a^n a^{-qm} = a^r \in U$. Aus $r < m$ und der Wahl von m als kleinste natürliche Zahl mit $a^m \in U$ folgt $r = 0$. Damit ist $n = qm$ und $a^n = (a^m)^q$. Das zeigt, dass U zyklisch ist.

Beispiel 7.40

Wir betrachten die Untergruppen der Gruppe $\mathbb{Z}_{12}$.
Die möglichen Ordnungen sind 1, 2, 3, 4, 6 und 12 und alle Untergruppen sind zyklisch.

Für alle $m \in \{1, \ldots, 11\}$ die zu 12 teilerfremd sind, erzeugt $[m]_{12}$ die ganze Gruppe $\mathbb{Z}_{12}$.
$[2]_{12}$ und $[8]_{12}$ erzeugen jeweils die Untergruppe

$$\{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}.$$

$[3]_{12}$ und $[9]_{12}$ erzeugen jeweils die Untergruppe

$$\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}.$$

$[4]_{12}$ und $[8]_{12}$ erzeugen jeweils die Untergruppe $\{[0]_{12}, [4]_{12}, [8]_{12}\}$.
$[6]_{12}$ erzeugt die Untergruppe $\{[0]_{12}, [6]_{12}\}$.
Das sind alle Untergruppen von $\mathbb{Z}_{12}$.

Satz 7.41

Sei G eine Gruppe, deren Ordnung eine Primzahl p ist.
Dann ist G zyklisch und die einzige Untergruppen von G sind G und $\{e\}$.

Beweis.

Sei $a \in G$.
Nach dem Satz von Lagrange ist die Ordnung von a ein Teiler von p.
Damit hat a entweder die Ordnung 1 oder p.
Im ersten Fall gilt $a = e$.
Im zweiten Fall ist $G = \{a^n : n \in \mathbb{Z}\}$. □

Permutationen

Man kann zeigen, dass jede Gruppe zu einer Menge von Permutationen isomorph ist.
Daher ist das Studium von Permutationen in der Gruppentheorie von besonderem Interesse.

Zur Erinnerung: Eine Permutation einer Menge A ist eine Bijektion von A nach A.
Die Komposition $g \circ f$ zweier Permutationen einer Menge A ist wieder eine Permutation von A.
Die Menge aller Permutationen einer Menge A zusammen mit der Komposition $\circ$ ist eine Gruppe $S(A)$.
Das neutrale Element ist die Identität $\mathrm{id}_A : A \to A; x \mapsto x$.
Für jede Permutation $\pi \in S(A)$ ist die Umkehrfunktion π^{-1} das zu π inverse Element von $S(A)$.

Ist A endlich, also zum Beispiel $A = \{a_1, \ldots, a_n\}$, so können wir eine Permutation $\pi : A \to A$ als

$$\begin{pmatrix} a_1 & \ldots & a_n \\ \pi(a_1) & \ldots & \pi(a_n) \end{pmatrix}$$

aufschreiben.

Beispiel 7.42

Es gilt

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Die Permutation auf der rechten Seite der Gleichung ist $\mathrm{id}_{\{1,2,3,4,5\}}$. Damit sind die beiden Permutationen auf der linken Seite der Gleichung in $\mathcal{S}_5 = S(\{1, 2, 3, 4, 5\})$ invers zueinander.

Wir betrachten die Permutation $\pi := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ etwas eingehender.

Es gilt $\pi(2) = 2$.
Die 2 wird also durch π auf sich selbst abgebildet.

Die 1 wird durch π auf 3 abgebildet, die 3 auf die 5, die 5 auf die 4 und die 4 wieder auf die 1.
Iteriert man also die Anwendung von π auf 1 so landet man zunächst bei 3, dann bei 5, bei 4 und schließlich wieder bei 1.

Lemma 7.43

Ist A eine endliche Menge und $\pi \in S(A)$, so existiert für jedes $a \in A$ ein $n \in \mathbb{N}$ mit $\pi^n(a) = a$.

Beweis.

Da A endlich ist, gibt es $k, \ell \in \mathbb{N}$ mit $k < \ell$ und $\pi^k(a) = \pi^\ell(a)$.
Nun gilt $a = (\pi^{-k} \circ \pi^k)(a) = (\pi^{-k} \circ \pi^\ell(a) = \pi^{\ell-k}(a)$.
Setzt man $n := \ell - k$, so ergibt sich $\pi^n(a) = a$. □

Definition 7.44

Sei A eine Menge, $n \geq 2$ und $a_1, \ldots, a_n$ paarweise verschiedene Elemente von A.
Dann bezeichen wir mit $(a_1 a_2 \ldots a_n)$ die Permutation π von A, die wie folgt definiert ist:

$$\pi(a) = \begin{cases} a, \text{ falls } a \in A \setminus \{a_1, \ldots, a_n\}, \\ a_{i+1}, \text{ falls } a = a_i \text{ für ein } i \in \{1, \ldots, n-1\} \text{ und} \\ a_1, \text{ falls } a = a_n. \end{cases}$$

Die Permutation $(a_1 a_2 \ldots a_n)$ nennen wir einen *Zyklus* der Länge n.

Zwei Zyklen $(a_1, \ldots, a_n)$ und $(b_1, \ldots, b_m)$ heißen disjunkt, falls die Mengen $\{a_1, \ldots, a_n\}$ und $\{b_1, \ldots, b_m\}$ disjunkt sind.
Zyklen der Länge 2 heißen *Transpositionen*.

Satz 7.45

Sei A eine endliche Menge.

a) Jede Permutation π von A ist ein Produkt von paarweise disjunkten Zyklen.
Eine Darstellung von π als Produkt disjunkter Zyklen heißt Zyklenzerlegung *von π.*
Die Zyklenzerlegung von π ist bis auf die Reihenfolge eindeutig.

b) Jeder Zyklus ist ein Produkt von Transpositionen.

c) Jede Permutation von A ist ein Produkt von Transpositionen.

Beispiel 7.46

Sei $A = \{1, 2, 3, 4, 5, 6\}$ und

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

Dann gilt

$$\pi = (143) \circ (256).$$

Weiter gilt $(143) = (14) \circ (43)$ und $(256) = (25) \circ (56)$.
Damit ist

$$\pi = (14) \circ (43) \circ (25) \circ (56).$$

Satz 7.47

Sei π eine Permutation einer endlichen Menge A.
Ist π ein Produkt von gerade vielen Transpositionen, so hat jede Darstellung von π als Produkt von Transpositionen eine gerade Anzahl von Faktoren.
In diesem Falle nennen wir π eine gerade *Permutation.*
Permutationen, die nicht gerade sind, nennen wir ungerade*.*

Korollar 7.48

Sei A eine endliche Menge.
Die geraden Permutationen bilden eine Untergruppe der Gruppe aller Permutationen von A vom Index 2.

Beispiel 7.49

Die Gruppe $\mathcal{S}_3$ hat $3! = 6$ Elemente.
Damit gibt es 3 gerade Permutationen und 3 ungerade Permutationen.

Die die geraden Permutationen sind die Identität, $(123) = (12)(23)$ und $(321) = (32)(21)$.
Die ungeraden Permutationen sind (12), (13) und (23).

Man beachte, dass die Darstellungen von Permutationen als Produkt von Transpositionen nicht eindeutig ist.
Es gilt zum Beispiel

$$(123) = (12)(23) = (231) = (23)(31) = (312) = (31)(12).$$

Auch die Anzahl der Transpositionen ist nicht eindeutig:

$$(321) = (32)(21) = (123)^2 = (12)(23)(31)(12)$$

Was aber nach Satz 7.47 eindeutig ist, ist die Anzahl der Transpositionen modulo 2.