Algebra

Inhaltsverzeichnis

1 Zyklische Gruppen

1.1 Restklassen

Das Zifferblatt einer Uhr geht von eins bis zwölf. Dreht sich der Uhrzeiger von zwölf aus um eine Stunde weiter, so landet er wieder bei der Zahl eins. Die Stunde zwölf können wir auch als Stunde null bezeichnen. Die Menge der Zahlen ist dann

$$Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

Dreht sich der Uhrzeiger bei der Zahl elf um eine Stunde weiter, so landet er bei der Zahl null. D.h. $11 + 1 = 0$. Da das etwas seltsam aussieht, schreiben wir $11 + 1 \equiv 0$ und sagen $11 + 1$ ist kongruent zu null.

Wir machen nun die grundlegende Beobachtung, dass sich die Zahl nicht ändert, wenn wir 12 hinzu addieren. Die Zahl wird sich auch nicht ändern, wenn wir 12 subtrahieren. Wenn wir die Zahl als h bezeichnen, dann ist also

$$h \equiv h + 12 \equiv h + 24 \equiv h - 12 \quad \text{usw.}$$

Die Zahl 12 nennen wir den Modul.

Wie überprüft man, ob zwei Zahlen kongruent sind? Man kann doch solange 12 subtrahieren oder addieren, bis man bei einer Zahl in der Menge Z_{12} landet. Z.B. sind 86 und 182 kongruent, denn es ist

$$86 = 2 + 7 \times 12,$$
$$182 = 2 + 15 \times 12.$$

Das ist natürlich eine etwas unpraktische Methode. Ich will nicht bis zum Abend 12 subtrahieren, wenn die Zahlen sehr groß sind. Wenn man aber die Differenz $182 - 86$ betrachtet, so erkennt man

$$182 - 86 = (2 + 15 \times 12) - (2 + 7 \times 12)$$
$$= (15 - 7) \times 12.$$

Die Differenz ist ein Vielfaches von 12 und daher durch 12 teilbar. Das geht auch im Allgemeinen. Sind a_1, a_2 zwei kongruente Zahlen, so ist

$$a_2 - a_1 = (r + 12q_2) - (r + 12q_1)$$
$$= 12(q_2 - q_1).$$

Wenn a_1, a_2 nicht kongruent sind, dann ist $a_1 = r_1 + 12q_1$ und $a_2 = r_2 + 12q_2$ mit $r_1 \neq r_2$. Wir können ohne Beschränkung der Allgmeinheit $r_1 < r_2$ annehmen. Dann ist

$$a_2 - a_1 = (r_2 + 12q_2) - (r_1 + 12q_1)$$
$$= (r_2 - r_1) + 12(q_2 - q_1).$$

Die Differenz lässt bei Division den Rest $r_2 - r_1$ und ist daher nicht durch 12 teilbar. Zwei Zahlen sind also genau dann kongruent modulo 12, wenn die Differenz durch 12 teilbar ist. Offenbar ist diese Aussage auch für andere Moduln als 12 gültig. Wir wollen den Modul allgemein mit dem Buchstaben m bezeichnen. Man erhält den

Satz. Zwei Zahlen sind genau dann kongruent modulo m, wenn ihre Differenz durch m teilbar ist.

Wenn man sagt a ist kongruent zu b modulo m, dann schreibt man

$$a \equiv b \pmod{m} \quad \text{oder kurz} \quad a \equiv b \quad (m).$$

Jede Zahl können wir ja in der Form $a = r + 12q$ mit $0 \leq r \leq 11$ darstellen. Dabei haben r und q eine besondere Bedeutung. Es handelt sich bei r um den Rest bei der Division durch 12 und q ist der Quotient.

Es ist $-10 \equiv 2 \equiv 14 \equiv 26$ usw. modulo 12. Alle diese Zahlen sind kongruent und lassen sich in der Form $a = 2 + 12k$ mit $k \in \mathbb{Z}$ schreiben. Die Menge M dieser Zahlen wollen wir daher als Restklasse zum Rest zwei bezeichnen und schreiben kurz $M = 2 + 12\mathbb{Z}$ in Anlehnung daran, dass sich ein Element dieser Menge als $a = 2 + 12k$ schreiben lässt.

Jeder Zahl r aus Z_{12} kann man genau eine Restklasse zuordnen. Wir ordnen r einfach mal $r + 12\mathbb{Z}$ zu. Diese Zuordnung ist bijektiv. Zwei Restklassen kann man nun addieren, indem man die entsprechenden Zahlen aus Z_{12} addiert und die Summe per Konruenz wieder in Z_{12} hineinbringt.

Beispiel:

$$8 + 9 = 17 \equiv 5 \quad (12)$$

Man kann es auch so schreiben:

$$8 + 12\mathbb{Z} + 9 + 12\mathbb{Z} = (8 + 9) + 12\mathbb{Z}$$
$$= 17 + 12\mathbb{Z} = 5 + 12 + 12\mathbb{Z} = 5 + 12\mathbb{Z}$$

In dieser Notation kann $12\mathbb{Z}$ die Zahl 12 verschlucken und ausspucken.

Die Summe liegt per Kongruenz immer wieder in Z_{12}. Außerdem ist null das neutrale Element. Zu jeder Zahl a in Z_{12} gibt es eine inverse Zahl a', so dass $a + a' \equiv 0$ (12) ist.

Ich will zeigen, wie man eine Zahl invertiert. Die inverse Zahl zu 2 ist z.B. -2. Per Kongruenz addiert man noch 12 und erhält 10. Es ist also

$$a' = -a + 12 = 12 - a.$$

Die Menge Z_{12} zusammen mit der Addition besitzt damit die Struktur einer Gruppe. Man bezeichnet diese Gruppe als Gruppe der Restklassen zum Modul 12 oder kurz als Restklassengruppe modulo 12.

Mit Z_m wird allgmein die Restklassengruppe modulo m bezeichnet. Eine alternative Schreibweise dafür ist Z/mZ.

1.2 Erzeuger

Aus Z_{12} kann man ein Element a nehmen und es wiederholt zu sich selbst addieren. Das inverse Element von a soll man auch addieren dürfen. Summen sind z.B. $a + a = 2a$, $a + a + a = 3a$ oder $a + a' = 0a$.

Mit $\langle a \rangle$ bezeichnet man die Hülle von a. Das ist die Menge aller Summen, welche per Kongruenz wieder auf Z_{12} eingeschränkt werden. Es ist

$$\langle a \rangle := \{g |\ g = ka,\ k \in \mathbb{Z}\} \quad \text{modulo}\, 12.$$

Ein Element a mit der Eigenschaft $\langle a \rangle = Z_{12}$ heißt Erzeuger von Z_{12}. Z.B. ist drei kein Erzeuger von Z_{12}, denn es ist

$$\langle 3 \rangle = \{0, 3, 6, 9\}.$$

Bei fünf handelt es sich um einen Erzeuger, denn es ist

$$\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}.$$

Warum ist fünf ein Erzeuger und drei nicht? Wir überprüfen alle Zahlen in Z_{12}, um einen Überblick darüber zu bekommen, welche der Zahlen Erzeuger sind. Die Erzeuger sind $1, 5, 7, 11$. Das sind Primzahlen. Aber zwei und drei sind keine Erzeuger, obwohl sie auch Primzahlen sind. Wir machen nun die grundlegende Beobachtung, dass zwei und drei in der Primfaktorzerlegung von 12 vorkommen, die Zahlen $1, 5, 7, 11$ jedoch nicht.

Wir sehen uns Z_{35} an. Dort sind unter anderem 1,2,3,4,6,8,9 Erzeuger. Unsere Vermutung scheint sich zu bestätigen. Eine Zahl ist Erzeuger der Gruppe Z_m, wenn sie teilerfremd zum Modul m ist.

Satz. $\langle a \rangle = Z_m$ gdw. $\text{ggT}(a, m) = 1$.

Beweis der Implikation. Bei den Produkten ka soll für k gelten $1 \leq k \leq m - 1$. Alle diese Produkte müssen (für ein festes a) ungleich einem Vielfachen von m sein, damit es überhaupt möglich ist, genügend unterschiedliche Elemente zu erzeugen. Wenn a aber Primfaktoren von m enthält, so kann man immer ein k finden, sodass das Produkt ka ein Vielfaches von m ist. Daher muss a teilerfremd zu m sein. qed.

Beweis der Gegenimplikation. Alle Produkte müssen (für ein festes a) inkongruent sein. Sei ohne Beschränkung der Allgemeinheit $k_1 < k_2$. Es darf $k_2 a - k_1 a = (k_2 - k_1)a$ kein Vielfaches von m sein. Die Differenz $k = k_2 - k_1$ ist wieder ein k mit $1 \leq k \leq m - 1$. Dass ka kein Vielfaches von m ist, ist aber durch die Voraussetzung $\text{ggT}(a, m) = 1$ abgesichert. qed.

Mit $\text{ord}(a)$ wird die Ordnung eines Elements von Z_m bezeichnet. Das ist die kleinste natürliche Zahl k für die $ka \equiv 0$ ist.

Mit $\text{ord}(G) = |G|$ wird die Ordnung der Gruppe G bezeichnet. Das ist die Anzahl der Elemente von G. Z.B. ist $|Z_m| = m$.

Wir beobachten nun, dass die Ordnung eines Erzeugers von Z_m mit der Ordnung von Z_m übereinstimmt. Weiterhin beobachten wir

$$\text{ord}(a) = \text{ord}(\langle a \rangle).$$

Tatsächlich bildet $\langle a \rangle$ wieder eine Gruppe, auch wenn a kein Erzeuger von Z_m ist. Die Gruppe $\langle a \rangle$ ist immer eine Untergruppe von Z_m.

1.3 Untergruppen

Eine Teilmenge von Z_m, die wieder eine Gruppe ist, wird Untergruppe von Z_m genannt. Z.B. ist $A = \{0, 3, 6, 9\}$ eine Untergruppe von Z_{12}. Jedoch ist $B = \{0, 4\}$ keine Untergruppe von Z_{12}, weil z.B. $4 + 4 = 8$ ist. Die Summe muss aber per Kongruenz modulo 12 wieder in der gleichen Menge liegen. Das Axiom der Abgeschlossenheit trifft nicht zu, und so kann B keine Gruppe sein.

Wenn H eine Untergruppe von G ist, dann schreibt man $H \leq G$ in Anlehnung an $H \subseteq G$. Wenn H eine echte Untergruppe von G ist, dann schreibt man $H < G$.

Ein Isomorphismus ist eine bijektive Funktion φ zwischen zwei Gruppen, die die Eigenschaft der Verträglichkeit hat. Die Eigenschaft der Verträglichkeit ist

$$\varphi(a + b) = \varphi(a) + \varphi(b).$$

Wenn man für zwei Gruppen G, H einen Isomorphimus finden kann, dann sind diese beiden Gruppen isomorph und man schreibt $G \simeq H$. Zwei isomorphe Gruppen haben die gleiche Struktur. Zwei isomorphe Gruppen sind in Wirklichkeit ein und die selbe Gruppe, bloß in einer anderen Gestalt.

Z.B. ist $Z_4 \simeq \{0, 3, 6, 9\}$. Durch die folgende Wertetabelle ist ein Isomorphismus gegeben.

g	0	1	2	3
$\varphi(g)$	0	3	6	9

Mit φ^{-1} soll die Umkehrfunktion von φ bezeichnet werden. Um $a + b$ zu berechnen kann man doch auch

$$a + b = \varphi(\varphi^{-1}(a + b)) = \varphi(\varphi^{-1}(b) + \varphi^{-1}(a))$$
$$= \varphi(\varphi^{-1}(a) + \varphi^{-1}(b))$$

rechnen. Z.B. ist

$$3 + 6 = \varphi(1 + 2) = \varphi(3) = 9.$$

Man muss aber beachten, dass man modulo vier rechnet, wenn man sich in Z_4 befindet. Nach Anwendung des Isomorphismus befindet man sich in $\{0, 3, 6, 9\}$, und dort muss man wieder modulo 12 rechnen.

Die Untergruppen von Z_{12} sind alle wieder zyklisch, d.h. man kann für jede Untergruppe einen Erzeuger finden. Tatsächlich gilt diese Aussage auch allgemein für die Gruppen Z_m. Alle Untergruppen einer zyklischen Gruppe sind auch wieder zyklisch.

1.4 Produkte von Gruppen

Wenn man zwei Gruppen G, H hat, dann kann man das kartesische Produkt $G \times H$ von den Mengen G, H bilden, das aus allen Tupeln (g, h) mit $g \in G$ und $h \in H$ besteht. Mit

$$(g_1, h_1) + (g_2, h_2) := (g_1 + g_2, h_1 + h_2)$$

wird das Produkt wieder zu einer Gruppe, die direktes Produkt (oder einfach Produkt) der Gruppen G und H genannt wird.

Natürlich ist es unproblematisch das direkte Produkt aus mehr als zwei Gruppen zu bilden. Wenn das direkte Produkt n Faktoren hat, so hat man halt Tupel mit n Komponenten.

Die Produkte von zyklischen Gruppen können in bestimmten Fällen selbst wieder zyklisch sein. Es gilt der

Satz. Das Produkt von $Z_m \times Z_n$ ist genau dann zyklisch, wenn $\mathrm{ggT}(m, n) = 1$ ist. Wenn das Produkt zyklisch ist, dann ist $Z_m \times Z_n \simeq Z_{mn}$.

Das ist ein sehr interessanter Satz. Nach diesem Satz ist z.B.

$$Z_{12} \simeq Z_4 \times Z_3 = Z[2^2] \times Z[3].$$

Was Gruppen jetzt von Zahlen unterscheidet ist z.B.

$$(Z_2)^2 = Z_2 \times Z_2 \not\simeq Z_4 = Z[2^2].$$

Über die Gruppe $Z_2^2 = (Z_2)^2$ wissen wir mit dem Satz über Produkte von zyklischen Gruppen, dass sie nicht zyklisch sein kann. Diese Gruppe ist isomorph zur kleinschen Vierergruppe. Drei Elemente dieser Gruppe erzeugen Untergruppen, die jeweils isomorph zu Z_2 sind. Das vierte Element ist das neutrale Element.

Auf jeden Fall gilt aber immer

$$|G \times H| = |G|\,|H|.$$

Diese Formel hilft, die Ordnung einer Gruppe zu bestimmen, wenn eine Zerlegung in einfachere Gruppen bekannt ist. Z.B. ist die Ordnung der kleinschen Vierergruppe

$$|Z_2 \times Z_2| = |Z_2|\,|Z_2| = 2 \times 2 = 4.$$

1.5 Gruppentafeln

Die Gruppentafel dient zur Veranschaulichung kleiner endlicher Gruppen, sie enthält alle Ergebnisse $a + b$. Dabei steht a in der Eingangsspalte und b in der Kopfzeile. Das Ergebnis $a + b$ steht in der Zelle, die durch Zeilennummer und Spaltennummer bestimmt wird. Für die zyklische Gruppe Z_4 lautet die Gruppentafel z.B.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

An der Gruppentafel kann man bestimmte Dinge ablesen. Wenn eine Gruppe kommutativ ist, dann ist die Gruppentafel bezüglich der Diagonalen symmetrisch. Das neutrale Element hat eine Kopie der Kopfzeile als Zeile. Um ein inverses Element bezüglich eines Elements zu suchen, geht man in der Zeile bis zum neutralen Element, und dann nach oben.

1.6 Prime Restklassengruppen

Die Elemente von Z_{12} kann man ja auch multiplizieren. Nicht jede Zahl aus Z_{12} hat auch eine inverse Zahl. Wir suchen eine Zahl a', sodass $aa' \equiv 1$ ist. Z.B. ist $5 \times 5 \equiv 1$. D.h. fünf ist zu sich selbst invers. Zu vier kann man allerdings keine inverse Zahl finden.

Eine Zahl a aus Z_m hat nur dann eine inverse Zahl, wenn $\mathrm{ggT}(a, m) = 1$ ist. Die Menge der multiplikativ invertierbaren Zahlen aus Z_m bildet mit der Multiplikation eine Gruppe. Diese Gruppe wird Gruppe der primen Restklassen oder kurz prime Restklassengruppe genannt. Für die prime Restklassengruppe von Z_m verwendet man die Notation Z_m^*. Z.B. ist

$$Z_{12}^* = \{1, 5, 7, 11\}.$$

Diese Gruppe ist nicht zyklisch. Die Gruppe ist isomorph zur kleinschen Vierergruppe. Die Gruppe

$$Z_{10}^* = \{1, 3, 7, 9\}$$

ist jedoch zyklisch und isomorph zu Z_4. Beachte, dass man in Z_{10}^* multipliziert und modulo 10 rechnet. In Z_4 addiert man jedoch und rechnet modulo vier.

Bei der folgenden Funktion handelt es sich nicht um einen Isomorphismus. Die Funktion wird nur zufällig mit dem gleichen Buchstaben φ bezeichnet, der auch für Isomorphismen gewählt wurde. Mit φ wird die eulersche Phi-Funktion bezeichnet. Wenn m und n teilerfremd sind, dann ist $\varphi(mn) = \varphi(m)\varphi(n)$. Wenn p eine Primzahl ist, dann ist $\varphi(p^k) = p^{k-1}(p-1)$. Hat man eine Primfaktorzerlegung von einer Zahl a, so kann man also auch leicht $\varphi(a)$ ausrechnen.

Der Zusammenhang zwischen der Phi-Funktion und primen Restklassengruppen ist die Gleichung

$$\mathrm{ord}(Z_m^*) = \varphi(m).$$

Wir kennen ja schon $\mathrm{ord}(Z_{12}^*) = 4$ und $\mathrm{ord}(Z_{10}^*) = 4$. Das müsste man auch mit der Phi-Funktion erhalten.

Wir rechnen nach.

$$\varphi(12) = \varphi(2^2 \times 3) = \varphi(2^2)\varphi(3)$$
$$= 2(2-1)(3-1) = 4$$
$$\varphi(10) = \varphi(2 \times 5) = \varphi(2)\varphi(5)$$
$$= (2-1)(5-1) = 4$$

Die Erzeuger einer zyklischen primen Restklassengruppe werden auch Primitivwurzeln genannt.

2 Gruppen allgemein

2.1 Äquivalenzklassen

Man denke sich eine Schule mit Schülern. Zwei Schüler a, b sind äquivalent, wenn sie in die gleiche Klasse gehen. Man schreibt dann $a \sim b$. Eine Relation heißt Äquivalenzrelation, wenn sie reflexiv, symmetrisch und transitiv ist. Das heißt es ist

$$a \sim a,$$
$$a \sim b \Rightarrow b \sim a,$$
$$a \sim b \wedge b \sim c \Rightarrow a \sim c.$$

Wenn a ein Schüler ist, dann ist $[a]$ die Äquivalenzklasse von a. Das ist die Menge aller Schüler, die zu a äquivalent sind. Mit M soll die Menge aller Schüler der Schule bezeichnet werden. Die Menge der Schüler kann in disjunkte Äquivalenzklassen zerlegt werden. Damit ist gemeint, dass kein Schüler der Schule gleichzeitig in zwei unterschiedlichen Klassen sein kann. Ein Schüler einer bestimmten Klasse wird Repräsentant dieser Klasse genannt.

Was haben wir jetzt davon? Angenommen man hat zwei Mengen A, B mit sehr vielen Elementen und will überprüfen, ob diese beiden Mengen gleich sind. Dann müsste man jedes Element aus A nehmen und überprüfen, ob es auch in B vorhanden ist und jedes Element aus B nehmen und überprüfen, ob es in A vorhanden ist. Wenn diese beiden Mengen A, B aber Äquivalenzklassen sind, so braucht man sich nur zwei Repräsentanten $a \in A$ und $b \in B$ auszusuchen und überprüft, ob sie Äquivalent sind.

Man kann z.B. alle Geraden im $\mathbf{R}^2$ betrachten, die durch den Koordinatenursprung gehen. Man will jetzt überprüfen, ob zwei Geraden g_1, g_2 gleich sind. Dann müsste man zu jedem Punkt (x, y) auf g_1 schauen, ob dieser Punkt auch in der Menge g_2 liegt. Für g_2 müsste man das selbe tun.

Die Menge g_1 hat unendlich viele Punkte, so dass man sie nicht einmal auf ein Blatt Papier schreiben kann. Die Lösung ist jetzt, die Geraden als Äquivalenzklassen anzusehen, wenn wir uns den Koordinatenursprung einmal wegdenken. Wir suchen uns nun Repräsentanten $(x_1, y_1) \in g_1$ und $(x_2, y_2) \in g_2$ aus. Welche das sind, das ist unerheblich. Man darf jedoch nicht den Koordinatenursprung wählen. Die Äquivalenzrelation lautet nun

$$(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow \exists r\colon (rx_1, ry_1) = (x_2, y_2).$$

Die Menge aller Äquivalenzklassen wird auch als Faktormenge oder Quotientenmenge bezeichnet. Wenn M eine Menge ist, dann ist mit $M/\sim$ die Faktormenge bezüglich der Äquivalenzrelation $\sim$ gemeint.

Mit $\mathbf{R}^2/\sim$ ist also die Menge aller Ursprungsgeraden gemeint. Diese Menge ist von der Ebene $\mathbf{R}^2$ zu unterscheiden.

2.2 Präsentation einer Gruppe

Für die Operation, bezüglich der die Menge G eine Gruppe bildet, wurde bisher immer ein Pluszeichen verwendet. Man kann auch ein Malzeichen benutzen. Anstelle von $a + b$ schreibt man also ab. Anstelle von ka schreibt man dann a^k. Das neutrale Element ist dann nicht null, sondern eins.

Es gibt eine erweiterte Notation für die Hülle $\langle g \rangle$. Man schreibt hinter das Element g noch einen senkrechten Strich. Hinter den Strich kommen Bedingungen, die erfüllt sind. Die von g erzeugte zyklische Gruppe ist z.B.

$$Z_m = \langle g |\, g^m = 1 \rangle.$$

Diese Notation heißt Präsentation einer Gruppe. Alternativ kann man auch die additative Schreibweise verwenden. Dann schreibt man

$$Z_m = \langle g |\, mg = 0 \rangle.$$

Im Allgemeinen hat man

$$\langle g_1, \dots g_n |\, R_1, \dots R_p \rangle.$$

Man bildet beliebige Worte aus den Symbolen $g_1, \dots, g_n$, wobei die inversen Elemente auch als Symbole zugelassen sind. Dann wendet man die Relationen $R_1, \dots, R_p$ an, um die Menge der Worte zu reduzieren. Allgemeine Eigenschaften wie $g^{-1}g = 1$ oder $(ab)^{-1} = b^{-1}a^{-1}$ dürfen natürlich auch verwendet werden.

Die kleinsche Vierergruppe hat z.B. die Präsentation

$$Z_2^2 = \langle a, b |\, a^2 = 1, b^2 = 1, ab = ba \rangle.$$

Wir können z.B. das Wort $a^5b^{-2}a^3a^2b^2$ bilden. Aber das kann auf folgende Weise reduziert werden.

$$a^5b^{-1}a^3a^2b^2 = a^5b^{-1}a^3 = aa^2a^2b^{-1}aa^2$$
$$= ab^{-1}a = ab^{-1}bba$$
$$= aba = aab = b$$

Da die Multiplikation durch $ab = ba$ kommutativ wird, kann man die Potenzen auch einfach zusammenfassen und macht folgende einfachere Rechnung.

$$a^5b^{-1}a^3a^2b^2 = a^{10}b$$
$$= (a^2)^5b = 1^5b = b$$

Egal welches Wort man nimmt, es lässt sich immer auf ein Element aus

$$Z_2^2 = \{1, a, b, ab\}$$

reduzieren. Eine etwas interessantere Gruppe ist die Diedergruppe D_4. Die Diedergruppe D_4 hat z.B. die Präsentation

$$D_4 = \langle a, b |\, a^2 = b^2 = (ab)^4 = 1 \rangle.$$

Die Gruppe ist nicht kommutativ und hat die Elemente

$$D_4 = \{1, a, b, aba, bab, ab, ba, (ab)^2\}.$$

Jedes andere Wort lässt sich wieder auf eines in dieser Menge reduzieren. Z.B. ist

$$\begin{aligned}(ab)^3 &= (ab)^{-1}(ab)^4 = (ab)^{-1} \\ &= b^{-1}a^{-1} = b^{-1}bba^{-1}aa = ba.\end{aligned}$$

Woher ich weiß, dass es keine weiteren Elemente gibt? Nun ja, D_4 hat vier Elemente, die jeweils das neutrale Element als Quadrat haben. Das sind im Einzelnen

$$a^2 = b^2 = (aba)^2 = (bab)^2 = 1.$$

Hinzu kommt noch ein Zyklus der Länge vier. Der Zyklus ist

$$1, ab, (ab)^2, (ab)^3.$$

Man braucht sich bloß den Zykelgraph von D_4 ansehen.

Bei der Diedergruppe D_4 handelt es sich um die Symmetriegruppe des Quadrats. Es gibt vier Spiegelungen, drei Drehungen und die identische Operation. Man sieht, dass D_4 die Symmetrie des Quadrats kodiert.

Was ist mit dem gleichseitigen Dreieck? Die Diedergruppe D_3 kodiert die Symmetrie des gleichseitigen Dreiecks. Es sind drei Spiegelungen, zwei Drehungen und die identische Operation. Ob es zwei oder drei Drehungen gibt, ist Ansichtssache, denn die Drehung um 360° ist auch immer die identische Operation.

Wir stellen jetzt natürlich die Frage, was Gruppen mit Symmetrien zu tun haben. Bei D_3 und D_4 besteht die Gruppe anscheinend aus den Symmetrieabbildungen. Verfolgt man diese Überlegung weiter, so erkennt man, dass es sich bei der Multiplikation von Elementen um die Komposition der entsprechenden Symmetrieabbildungen handelt.

Von der Präsentation von D_4 wissen wir jetzt auch, dass man mit zwei Spiegelungen alle anderen Symmetrieabbildungen erzeugen kann.

2.3 Permutationen

Was ist eine Permutation? Man nehme das Tupel $(1, 2, 3, 4)$. Die Komponenten des Tupels kann man vertauschen. Z.B. zu $(3, 2, 4, 1)$. Das Vertauschen bezeichnet man als Permutation des Tupels.

Sei $M = \{1, \ldots, n\}$. Eine Permutation wird definiert als bijektive Funktion p mit M als Definitionsbereich und Bildmenge.

Beim Tupel ordnet die Permutation einem Komponentenindex einen anderen Komponentenindex zu. Schreiben wir das Tupel kurz als

$$(a_k) = (a_1, \ldots, a_n).$$

Durch die Permutation p erhält man das Tupel

$$(a_{p(k)}) = (a_{p(1)}, \ldots, a_{p(n)}).$$

Eine Permutation kann durch eine Wertetablle angegeben werden. Z.B.

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ p(1) & p(2) & p(3) & p(4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

Eine Transposition ist eine spezielle Permutation, die zwei Komponenten vertauscht. Jede Permutation lässt sich als Komposition von Transpositionen zusammensetzen.

Die Menge aller Permutationen der Menge M bildet zusammen mit der Komposition von Permutationen eine Gruppe, die als symmetrische Gruppe S_n bezeichnet wird. Die Untergruppen der symmetrischen Gruppe bezeichnet man als Permutationsgruppen. Von grundlegender Bedeutung ist nun der

Satz von Cayley. Jede Gruppe ist zu einer Permutationsgruppe isomorph.

2.4 Nebenklassen

Sei H eine Untergruppe von G. Man kann nun ein $g \in G$ nehmen, und es von links auf jedes $h \in H$ anwenden. Die Menge, welche dabei entsteht, wird Linksnebenklasse von H genannt und mit gH bezeichnet. Es ist also

$$gH := \{gh |\, h \in H\}.$$

In additativer Schreibweise ist

$$g + H := \{g + h |\, h \in H\}.$$

Nehmen wir die Gruppe Z_{12} und die Untergruppe $H = \{0, 3, 6, 9\}$. Es ergibt sich z.B.

$$2 + H = 2 + \{0, 3, 6, 9\} = \{2, 5, 8, 11\}.$$

Mit G/H wird die Menge aller Linksnebenklassen von H bezeichnet. Die Anzahl der Elemente von G/H wird mit $|G/H|$ bezeichnet. Von grundlegender Bedeutung ist der

Satz von Lagrange. $|G| = |H|\,|G/H|$.

Dieser Satz sagt aus, dass der Quotient $|G|/|H|$ eine natürliche Zahl ist, dass die Ordnung einer Untergruppe also ein Teiler der Gruppenordnung ist. Eine Untergruppe kann also garnicht jede beliebige Ordnung haben.

Die Gruppe Z_{12} kann z.B. nur Untergruppen mit der Ordnung $1, 2, 3, 4, 6, 12$ haben. Die Gruppe Z_{11} kann nur $\{1\}$ und sich selbst als Untergruppe haben. Mit dem Satz von Lagrange kann man also Gruppen als Untergruppen sofort ausschließen.

Die Diedergruppe D_4 hat die Ordnung acht. Für Untergruppen sind also nur die Ordnungen $1, 2, 4, 8$ erlaubt. Tatsächlich sind die nichttrivialen Untergruppen Z_2 und Z_4.

2.5 Gruppenaktionen

Sei G eine Gruppe und X eine Menge. Eine Funktion $f: G \times X \to X$ heißt Gruppenaktion, wenn sie die folgenden Eigenschaften erfüllt:

$$f(g_1 g_2, x) = f(g_1, f(g_2, x)),$$
$$f(e, x) = x.$$

Dabei sollen $g_1, g_2 \in G$ sein. Mit e ist das neutrale Element von G gemeint. Anstelle von $f(g, x)$ schreibt man auch kürzer gx. Wenn man additative Schreibweise verwendet, dann schreibt man wieder $g_1 + g_2$ anstelle von $g_1 g_2$.

Nehmen wir z.B. ein Quadrat und nummerieren die Ecken mit A, B, C, D durch. Die Gruppe Z_4 kann man nun auf der Menge $X = \{A, B, C, D\}$ agieren lassen. Wir definieren die Gruppenaktion durch

$$f(1, A) = B, \quad f(1, B) = C,$$
$$f(1, C) = D, \quad f(1, D) = A.$$

Z.B. ist

$$f(3, B) = f(1 + 1 + 1, B) = f(1, f(1, f(1, B)))$$
$$= f(1, f(1, C)) = f(1, D) = A.$$

Die Bahn bzw. der Orbit von x ist definiert als

$$Gx := \{gx |\, g \in G\}.$$

Z.B. berechnet man den Orbit von A zu

$$f(Z_4, A) = \{f(0, A),\ f(1, A),\ f(2, A),\ f(3, A)\}$$
$$= \{A, B, C, D\}.$$

Bei {0,2} handelt es sich um eine Untergruppe von Z_4. Man erhält den Orbit

$$f(\{0, 2\}, A) = \{f(0, A),\ f(2, A)\} = \{A, C\}.$$

Was das soll? Wir sind hier beim zentralen Werkzeug angelangt, was die Untersuchung von Symmetrien angeht. Nehmen wir z.B. das Quadrat und legen die Mitte auf den Koordinatenursprung. Der Rand des Quadrats ist eine Menge X aus Punkten (x, y). Die Gruppenaktion definieren wir durch

$$f(1, (x, y)) = (y, -x).$$

Eine Objekt ist nur dann symmetrisch, wenn die Anwendung von Gruppenaktionen nicht aus der Menge X herausführt.

Außerdem haben wir jetzt die Möglichkeit, ein kompliziertes Objekt aus einem Keim heraus zu erzeugen. Das Quadrat ist z.B. der Orbit einer der Kanten. Wir gehen einen Schritt weiter und bilden Figuren nach dem Motto

symmetrische Figur = Orbit von Tintenklecks.

Mit dem bilden des Orbits GM von einer Figur M wird diese Figur vervollständigt, so dass sie symmetrisch bezüglich der Gruppenaktion gx wird. Eigentlich haben wir nur Orbits von Punkten definiert und nicht von Mengen. Intuitiv kann man aber für jeden Punkt aus M den Orbit bilden. Der Orbit von M soll dann einfach die Vereinigungsmenge aller Orbits sein.

Die Punkte eines Orbits sind äquivalent. Eine symmetrische Figur kann daher in disjunkte Orbits zerlegt werden.

Punkte x mit $gx = x$ heißen Fixpunkte der Gruppenaktion. Der Einzige Fixpunkt der Drehung mit Z_4 ist der Punkt $(0, 0)$.

Eine Symmetriegruppe besteht ja aus den Symmetrieabbildungen, wobei die Gruppenmultiplikation der Komposition von Abbildungen entspricht. Die Symmetrieabbildungen bilden auf natürliche Weise eine solche Gruppe, denn die Verkettung ist ja assoziativ und zu jeder Abbildung gibt es auch eine Umkehrabbildung.

Man fragt sich nun, warum man die Gruppenaktion braucht, wenn doch die Symmetrieabbildungen schon die Symmetriegruppe bilden. Der Vorteil ist der folgende. Bei der Symmetriegruppe ist die Menge festgelegt, auf der die Symmetrieabbildungen agieren. Bei der Gruppenaktion kann man ein und die selbe Gruppe jedoch für unterschiedliche Mengen verwenden. Z.B. haben die Ecken eines Quadrates die selbe Symmetrie, wie der Rand des Quadrates und wie die gesamte Quadratfläche. Mit der Gruppenaktion kann man diese drei Symmetriegruppen durch die gleiche Gruppe beschreiben.

Der Zusammenhang zwischen Gruppenaktion und Symmetrieabbildung ist der folgende. Wenn man bei der Gruppenaktion $f(g, x)$ das Gruppenelement g konstant hält, so erhält man die entsprechende Symmetrieabbildung $f(x) := f(g, x)$. Es kann aber sein, dass unterschiedliche Gruppenelemente die gleiche Symmetrieabbildung produzieren. Nehmen wir die Menge $X = \{a, b\}$ und $G = Z_4$. Die Gruppenaktion legen wir mit $f(1, a) = b$ und $f(1, b) = a$ fest. Damit ergibt sich $f(0, x) = f(2, x)$ und $f(1, x) = f(3, x)$. Die auf X agierende Gruppe Z_4 hat vier Elemente, die Symmetriegruppe jedoch nur zwei.

Man definiert daher den Begriff der treuen Gruppenaktion. Eine Gruppenaktion heißt treu, wenn zu zwei unterschiedlichen Gruppenelementen g, h auch immer die Gruppenaktionen unterschiedlich sind. Dafür muss jedes mal $f(g, x) \neq f(h, x)$ für mindestens ein x sein.

2.6 Kontinuierliche Gruppen

Die Rotationssymmetrie eines regelmäßigen Polygons mit n Ecken wird durch die Gruppe Z_n beschrieben. Ein Kreis hat jedoch eine Rotationssymmetrie, bei der man um einen beliebig kleinen Winkel drehen kann. Man benötigt eine kontinuierliche Gruppe. Diese Gruppe heißt spezielle orthogonale Gruppe der Drehungen in der Ebene und wird mit SO(2) abgekürzt. Eine Drehung kann durch die Drehmatrix

$$D(\varphi) = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}$$

beschrieben werden. Es gilt dann $D(\varphi_1)D(\varphi_2) = D(\varphi_1 + \varphi_2)$. Die Summe der Winkel berechnet man modulo 2π. Man hat also gewissermaßen immernoch eine Restklassengruppe, der Rest liegt jedoch im kontinuierlichen Intervall $0 \leq x < 2\pi$.

Ebenso gibt es eine Gruppe der Translationen T(2), welche aus allen Translationen der Ebene zusammengesetzt ist. Eine Translation t kann man durch $t(x) = x + v$ beschreiben. Dabei wird zum Punkt x der Verschiebungsvektor v addiert.

Diese Gruppen haben eine besondere Eigenschaft. Es handelt sich um Isometriegruppen. Eine Isometrieabbildung erhält Abstände. Das heißt

$$d(x_1, x_2) = d(f(x_1), f(x_2)),$$

wenn d die Abstandsfunktion und f die Isometrieabbildung ist. Eine Gruppe, die aus Isometrieabbildungen besteht, heißt Isometriegruppe. Die Gruppen SO(2), T(2) und alle ihre diskreten Untergruppen sind Isometriegruppen.

Alle Isometrieabbildungen des euklidischen Raumes bilden eine Gruppe. Diese Gruppe wird euklidische Gruppe E(2) genannt. Die Gruppen SO(2) und T(2) sind Untergruppen von E(2).

Isometrieabbildungen sind spezielle Symmetrieabbildungen. Es gibt auch Symmetrieabbildungen, die keine Isometrieabbildungen sind, z.B. die Skalierung $f(k, x) = 2^k x$ mit $k \in \mathbb{Z}$. Eine Bezüglich dieser Skalierung symmetrische Figur ist z.B. die Menge der Kreise mit Radius $r = 2^k$ und Mittelpunkt im Koordinatenursprung.