2.7 Semidirekte Produkte

In diesem Abschnitt findet sich eine einfache, aber wirkungsvolle Technik zur Konstruktion von Gruppen aus schon bekannten kleineren Gruppen: Gegeben zwei Gruppen H und T und eine Operation (im Sinne von Abschnitt 2.3) von H auf T durch Gruppenautomorphismen, so kann man das semidirekte Produkt $G = T \rtimes H$ von T und H (relativ zu dieser Operation) definieren. Dieses enthält T und H als Untergruppen und verallgemeinert die Konstruktion des direkten (kartesischen) Produktes $T \times H$. Viele wichtige Gruppen wie die affine Gruppe, die Symmetriegruppe des Hyperwürfels oder auch 13 der 17 hier nicht behandelten „Ornamentgruppen” (kristallographischen Gruppen der Ebene) besitzen eine Struktur als semidirektes Produkt. Für endliche Gruppen mit gewissen Ordnungen ergibt es sich aus den Sylowsätzen, dass eine Gruppe dieser Ordnung die Voraussetzungen eines semidirekten Produktes erfüllt.

Durch die Unterscheidung zwischen dem internen und dem externen semidirekten Produkt stellen wir die nötigen Begriffe einerseits zur Analyse gegebener Gruppen, andererseits zur Konstruktion neuer Gruppen in präziser Form zur Verfügung.

Wir benutzen in diesem Abschnitt wieder Erzeugendensysteme für Gruppen und geben eine Beschreibung der Diedergruppen als eine von zwei Elementen erzeugte Gruppe, die von der früher gegebenen konkreten Definition als Permutations- bzw. Matrizengruppen abstrahiert. Diedergruppen sind weitere einfache Beispiele für semidirekte Produkte.

Grundthema ist die „Zerlegung“ von Gruppen in kleinere Gruppen, bzw. der Konstruktion einer Gruppe aus kleineren Gruppen. Das folgende bekannte Resultat ist eins der einfachsten Beispiele hierfür.

Beispiel 2.7.1 Es sei G eine Gruppe der Ordnung $|G| = 6$. Dann gilt $G \cong Z_6$ (zyklische Gruppe) oder $G \cong S_3$ (symmetrische Gruppe).

Beweis: Wir geben hier einen elementaren Beweis: er benutzt nur Ordnungen von Elementen, den Satz von Lagrange und das Lemma von Cauchy 2.5.8.

Falls G ein Element der Ordnung 6 enthält, ist G zyklisch; dieser Fall muss nicht weiter betrachtet werden.

Nach dem Lemma von Cauchy 2.5.8 gibt es in G auf jeden Fall ein Element x der Ordnung 3 und ein Element y der Ordnung 2. Es folgt weiter

$$G = \{e, x, x^2, y, xy, x^2y\},$$

denn die angegebenen Elemente sind alle verschieden voneinander. (Diese Aussage ergibt sich auch aus dem folgenden Lemma 2.3.1.)

Man betrachtet nun das Konjugierte $x' := yxy^{-1} = yxy$. Dieses ist wieder von der Ordnung 3, muss also gleich x oder x^2 sein. (Wenn es weitere Elemente der Ordnung 3 gäbe, dann gäbe es zwei verschiedene Untergruppen der Ordnung 3, und G hätte insgesamt mindestens 9 Elemente.) Aus der Information $yx = x'y = xy$ bzw. $= x^2y$ kann man nun die gesamte Verknüpfungstafel hinschreiben, d.h. G ist bis auf Isomorphie bestimmt. Im ersten Fall ist G kommutativ, und das Element xy hat die Ordnung 6, also ist G sogar zyklisch. Im zweiten Fall muss G isomorph zur symmetrischen Gruppe S_3 sein, denn diese nicht-kommutative Gruppe mit 6 Elementen ist bereits bekannt. (Man sieht auch sofort, dass für einen beliebigen Dreierzykel x und eine beliebige Transpositionen y in S_3 die Gleichung $yxy = x^2$ gilt: $(ij)(ijk)(ij) = (ikj)$.) □

Wir erinnern an dieser Stelle an Lemma 2.3.1 und dem Begriff des (internen) direkten Produktes 2.3.2. Man sieht sofort, dass in einem direkten Produkt $G = AB$ die beiden Untergruppen A und B normal sind. Das folgende Lemma besagt, dass unter Voraussetzung von (DP1) und (DP2) die Normalität schon ausreichend ist für das Vorliegen eines direkten Produktes.

Lemma 2.7.2 (Produktzerlegung)
Es sei G eine Gruppe und $A, B \subseteq G$ Untergruppen mit den folgenden Eigenschaften:

(DP1) $G = AB$
(DP2) $A \cap B = \{e\}$
(DP4) A, B sind beide Normalteiler.

Dann ist G das direkte Produkt von A und B, also isomorph zu $A \times B$.

BEWEIS: Zu zeigen ist die Eigenschaft (DP3). Für $a \in A,\ b \in B$ liegt der Kommutator $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1}$ wegen der vorausgesetzten Normalität sowohl in A als auch in B, ist also gleich e. □

Aus 2.3.1, 2.7.2 und 2.3.2 ergibt sich nun folgendes einfache hinreichende Kriterium für eine Produktzerlegung:

Korollar 2.7.3 *Sei G endliche Gruppe, ihre Ordnung zerlegt als $|G| = \ell m$, wobei $\mathrm{ggT}(\ell, m) = 1$. Es seien A, B Normalteiler in G mit $|A| = \ell,\ |B| = m$. Dann ist G das direkte Produkt von A und B.*

Im allgemeinen werden Normalteiler mit den gewünschten Ordnungen nicht existieren und deshalb das letzte Korollar nicht anwendbar sein. Eine Ausnahme von dieser Regel haben wir im vergleichsweise trivialen Fall der abelschen Gruppen. Hier ist erstens Normalität keine Bedingung, und zweitens existieren zu jeder teilerfremden Zerlegung der Gruppenordnung entsprechende Untergruppen. Dieses Ergebnis ist uns aus dem Satz 2.3.6 bereits bekannt. Es muss betont werden, dass der Beweis dieses Satzes nicht auf dem vorigen Resultat 2.7.3 beruht. Wenn man nämlich zeigt, dass die dortigen Untergruppen G_i die richtige Ordnung haben, kann man gleich die komplette Aussage über das direkte Produkt beweisen.

Für den Fall allgemeiner, nicht als abelsch vorausgesetzter Gruppen können wir versuchen, das Korollar 2.7.3 anzuwenden, wenn ℓ und m Potenzen von Primzahlen sind. Dann existieren nach dem Satz von Sylow Untergruppen A und B

mit den gesuchten Ordnungen. Die Normalität etwa von A liegt genau dann vor, wenn G nur eine p-Sylowgruppe ($\ell = p^k$) besitzt, worüber wieder die Sylowsätze eine Aussage machen. So erhält man z.B. das folgende Standardresultat:

Satz 2.7.4 *Es sei G ein Gruppe der Ordnung pq, wobei p und q Primzahlen sind mit $p < q$. Weiter sei $q \not\equiv 1 \pmod p$ vorausgesetzt. Dann gilt $G \cong Z_p \times Z_q \cong Z_{pq}$, wobei Z_m die zyklische Gruppe der Ordnung m bezeichnet.*

Unter den genannten Voraussetzungen ist also die Gruppe G durch ihre Ordnung bis auf Isomorphie eindeutig bestimmt. Sie ist direktes Produkt von zyklischen Gruppen von Primzahlordnung, und auch selbst zyklisch, insbesondere abelsch.

Zum Beweis ist nur noch festzustellen, dass die q-Sylowgruppe auf jeden Fall normal ist, denn die Anzahl s_q aller q-Sylowgruppen ist ein Teiler von p und kongruent zu 1 modulo q, wofür wegen $p < q$ nur die Möglichkeit $s_q = 1$ bleibt. Aus der zusätzlichen Voraussetzung ergibt sich, das auch $s_p = 1$ ist, womit alle Voraussetzungen von 2.7.3 erfüllt sind. □

Die Voraussetzung $q \not\equiv 1 \pmod p$ in diesem Satz ist essentiell. Sie liefert, dass die p-Sylowgruppe normal ist. Wenn $q \equiv 1 \pmod p$ ist, kann man tatsächlich eine Gruppe konstruieren, die q p-Sylowgruppen enthält; diese Gruppe ist insbesondere nicht abelsch. Wir kommen unten darauf zurück.

Für $p = 2$ ist der Satz nie anwendbar, weil dann für jede weitere Primzahl q gilt $q \equiv 1 \pmod p$. Die angekündigte nicht-abelsche Gruppe der Ordnung $2q$ mit q 2-Sylowgruppen ist dann die aus Beispiel 1.3.12 (6) bekannte Diedergruppe Di_q; siehe auch deren vertiefte Behandlung unten unter 2.7.8.

Wir kommen nun zum Hauptthema dieses Abschnittes, den semidirekten Produkten. Wir schwächen die Voraussetzungen eines direkten Produktes ab und betrachten Produkte von zwei Untergruppen, von denen nur eine als Normalteiler vorausgesetzt ist. Hierzu zunächst ein kleines Lemma:

Lemma 2.7.5 Es sei G eine Gruppe und $T, H \subseteq G$ zwei Untergruppen derart, dass T von H normalisiert wird: $hth^{-1} \in T$ für alle $h \in H$, $t \in T$. Dann ist TH eine Untergruppe von G.

Beweis: Offenbar ist $e \in TH$. Die Abgeschlossenheit unter der Verknüpfung und unter Inversenbildung ergibt sich aus den folgenden beiden Formeln:

(M) $th\,t'h' = t(ht'h^{-1})(hh')$

(I) $(th)^{-1} = h^{-1}t^{-1} = (h^{-1}t^{-1}h)h^{-1}$ □

Die Voraussetzung kann auch so ausgedrückt werden: H ist im Normalisator $N_G(T)$ enthalten. Das ist natürlich erfüllt, wenn T ein Normalteiler in G ist. In jedem Fall ist unter der Voraussetzung des Lemmas T normal in TH. Wegen $ht = (tht^{-1})t$ gilt unter den Voraussetzungen des Lemmas $TH = HT$, d.h. auf die Reihenfolge der Faktoren in einem semidirekten Produkt kommt es nicht an. (Auf die Reihenfolge der Gruppen nicht, auf die der Elemente schon.)

In der folgenden Definition wird der Situation des Lemmas 2.7.5 noch die bekannte Bedingung hinzugefügt, dass die beiden Untergruppen trivialen Schnitt haben.

Definition 2.7.6 Eine Gruppe G heißt *(internes) semidirektes Produkt* von zwei Untergruppen T und H, falls gilt
(SD1) $G = TH$
(SD2) $T \cap H = \{e\}$
(SD3) $T \trianglelefteq G$.

Beispiele 2.7.7 (Semidirekte Produkte I)

(1) Die Würfelgruppe $\mathbb{W} = \mathbb{W}_3$ (aufgefasst als Untergruppe der orthogonalen 3×3-Matrizen) ist das semidirekte Produkt der Untergruppe T der Diagonalmatrizen in $\mathbb{W}$ mit der Gruppe H der Permutationsmatrizen; das ensprechende gilt für die Symmetriegruppe $\mathbb{W}_n$ des n-dimensionalen Hyperwürfels (vergl. Übungen).

(2) Die *affine Gruppe* $\mathrm{AGL}(V)$ eines Vektorraumes V ist das semidirekte Produkt der Translationsgruppe $\mathrm{T}(V)$ mit der Gruppe der Vektorraumautomorphismen $\mathrm{GL}(V)$. Hier ist $\mathrm{T}(V) = \{\tau_v \mid v \in V\}$, und τ_v bezeichnet die Translation $V \to V,\ x \mapsto v + x$.

(3) Die *Isometriegruppe* $\mathrm{Iso}(E)$ eines euklidischen Vektorraumes E ist das semidirekte Produkt der Translationsgruppe $\mathrm{T}(V)$ mit der orthogonalen Gruppe $\mathrm{O}(E)$. Dabei ist $\mathrm{Iso}(E)$ definitionsgemäß die Gruppe der abstandserhaltenden bijektiven Abbildungen von E auf sich. Man zeigt, dass jede solche Abbildung eine affine Abbildung ist. In der klassischen Geometrie werden diese Abbildungen übrigens oft *Bewegungen* genannt, und $\mathrm{Iso}(E)$ heißt *Bewegungsgruppe* von E.

Auch die Diedergruppe (beliebiger Ordnung $2n$) ist ein semidirektes Produkt; in der geometrischen Interpretation ist dabei T die Untergruppe aller Drehungen in Di_n. Bevor wir dieses Resultat in zitierfähiger Form festhalten, wollen wir die Diedergruppen Di_n etwas ausführlicher behandeln. Wir hatten sie in den Beispielen 1.3.12 (5) und (6) geometrisch eingeführt. Insbesondere die Gruppe Di_4 der Ordnung 8 war verschiedentlich wieder aufgetaucht. Es gibt verschiedene Realisierungen dieser Gruppe; selbst wenn man nur auf die geometrische Bedeutung schaut (wir werden noch andere kennenlernen), hat man (mindestens) zwei Möglichkeiten: durch Permutationen, also als Untergruppe der S_n, oder durch 2×2-Matrizen bzw. durch orthogonale Abbildungen der Ebene, also als Untergruppe von $\mathrm{O}_2(\mathbb{R})$. Es ist also nicht unbedingt sinnvoll, sich für einen Vertreter in der Isomorphieklasse aller Diedergruppen (gegebener Ordnung) entscheiden zu wollen, wenn man von „der” Diedergruppe spricht. Vielmehr wollen wir jetzt „die” Diedergruppe, genauer ihre Isomorphieklasse, durch möglichst wenige Bedingungen kennzeichnen. Jedenfalls kann die Diedergruppe von zwei Elementen erzeugt werden im Sinne der Definition 2.6.14. Es gibt auch eine unendliche Diedergruppe, die wir bei dieser Gelegenheit einführen wollen.

Satz 2.7.8 (Kennzeichnung der Diedergruppen) *Es sei* $n \in \mathbb{N} \cup \{\infty\}$*. Dann gibt es bis auf Isomorphie genau eine Gruppe* G *mit den folgenden Eigenschaften:* $G = \langle x, y\rangle$ *für zwei Elemente* $x, y \in G$ *für die gilt*

(Di1) $x \neq y,\ \operatorname{ord} x = n, \operatorname{ord} y = 2$

(Di2) $yxy^{-1} = x^{-1}$.

Diese Gruppe hat die Ordnung $|G| = 2n$*; sie heißt die* Diedergruppe *der Ordnung* $2n$*, Bezeichnung* Di_n *oder* D_n*.*

Beweis(skizze): zur Existenz: Es reicht, in irgendeiner Gruppe G zwei Elemente x und y mit den gewünschten Eigenschaften anzugeben. Für $n < \infty$ betrachten wir in der symmetrischen Gruppe die Elemente $x = (1, 2, 3, \ldots, n)$ und $y = (1, n)(2, n-1)\cdots(n/2, n/2+1)$ für gerades n, ähnlich für ungerades n. Die gewünschte Gleichung $xyx^{-1} = y^{-1}$ ergibt sich unmittelbar aus der bekannten Formel für Konjugation in S_n (Proposition 2.2.10). Für $n = \infty$ betrachten wir zwei bijektive (affine) Abbildungen $\mathbb{R} \to \mathbb{R}$, nämlich $x(t) = t + 1,\ y(t) = -t$. Dann ist $x \circ y \circ x^{-1} = x \circ y \circ x$ die Abbildung $t \mapsto t - 1$, also gleich x^{-1}, wie gewünscht. Wir haben also Di_∞ als Untergruppe der affinen Gruppe $\mathrm{AGL}(\mathbb{R})$ eines eindimensionalen Raumes realisiert; siehe auch Beispiel 2.7.7 (2).

zur Eindeutigkeit: Wenn x, y Elemente in irgendeiner Gruppe G sind, die (Di1) und (Di2) erfüllen, dann rechnet man nach, dass $\langle x\rangle \cup \langle x\rangle y$ eine Untergruppe ist, also gleich ganz G, wenn $\langle x, y\rangle = G$, und dass jede weitere solche Gruppe $G' = \langle x', y'\rangle$ durch $x^i y^j \mapsto x'^i y'^j,\ i = 0, \ldots, n-1, j = 0, 1$ zu G isomorph ist. □

In der Diedergruppe ist die zyklische Untergruppe $\langle x\rangle$ ein Normalteiler, wie sofort aus (Di2) folgt: es reicht, dass die Untergruppe von den beiden Erzeugern x und y normalisiert wird. (Man kann auch benutzen, dass $\langle x\rangle$ den Index 2 in Di_n hat, aber dieses Argument trifft weniger gut den Kern der Sache.) Die ersten beiden Bedingungen eines semidirekten Produktes sind ohnehin offensichtlich. Also gilt wie angekündigt:

Proposition 2.7.9 Die Diedergruppe $\mathrm{Di}_n = \langle x, y\rangle$ ist semidirektes Produkt des Normalteilers $\langle x\rangle$ mit der Untergruppe $\langle y\rangle$, also semidirektes Produkt einer zyklischen Gruppe der Ordnung n mit einer Gruppe der Ordnung 2.

Wir kehren zur Analyse allgemeiner semidirekter Produkte zurück. Wir stellen den Zusammenhang zu Gruppenoperationen her und kommen dadurch schnell zu einem Konstruktionsprizip. Wenn $G = TH$ ein semidirektes Produkt wie in 2.7.5

ist, dann operiert H auf T durch (von G auf T eingeschränkte) innere Automorphismen (die Abbildung $H \times T \to T,\ (h,t) \mapsto hth^{-1}$ ist eine Gruppenoperation). Nach den im Beweis von 2.7.5 angegebenen Formeln ist die Verknüpfung in G bekannt, wenn die beiden Verknüpfungen in T und H bekannt sind und ferner die genannte Operation. Mit anderen Worten, die Struktur eines semidirekten Produktes ergibt sich aus der Struktur der beiden beteiligten einzelnen Gruppen zusammen mit einer Operation der einen Gruppe auf der anderen. Wenn wir noch beachten, dass nach 2.4.18 eine Operation einer Gruppe H auf einer Menge T (hier: ebenfalls einer Gruppe) im wesentlichen dasselbe ist wie ein Homomorphismus von H in die Permutationsgruppe $\mathrm{Per}(T)$ (hier $\mathrm{Aut}(T)$), so kommt man auf den folgenden Satz.

Satz und Definition 2.7.10 (Semidirektes Produkt)

a) *Es seien T und H Gruppen und $\alpha : H \to \mathrm{Aut}(T),\ g \mapsto \alpha_g$ eine Operation von H auf T durch Gruppenautomorphismen von T. Dann ist die Produktmenge $T \times H$ mit der Verknüpfung*

$$(x,g)(y,h) := (x\,\alpha_g(y),\ gh),\ x,y \in T,\ g,h \in H$$

eine Gruppe. Diese wird mit $T \rtimes H$, genauer $T \rtimes_\alpha H$ bezeichnet und heißt (externes) semidirektes Produkt (mittels α) *von T und H.*

b) *Wenn $G = TH$ semidirektes Produkt zweier Untergruppen mit normalem T ist und $\alpha : H \to \mathrm{Aut}(T)$ durch $\alpha_h(t) = hth^{-1}$ definiert wird, dann ist die Abbildung $T \rtimes_\alpha H \to G,\ (t,h) \mapsto th$ ein Gruppenisomorphismus.*

Der Teil b) gibt nur wieder, was wir uns als Hinführung zur Definition des externen semidirekten Produktes überlegt hatten: die Abbildung $(t,h) \mapsto th$ ist verknüpfungstreu, wenn man auf $T \times H$ die Verknüpfung wie unter a) angegeben definiert. Das wesentliche an Teil a) dieses Satzes ist, dass unter alleiniger Voraussetzung der Gruppen T und H und des Homomorphismus α die angegebene Verknüpfung eine Gruppenstruktur definiert. Nachdem diese Behauptung steht, ergibt sich der Beweis des Assoziativgesetzes durch einfaches Nachrechnen, und aus obiger Formel (I) liest man ab, dass das Inverse von (t,h) gleich $(\alpha_{h^{-1}}(t), h^{-1})$ sein sollte, was dann ebenfalls durch einfaches Nachrechnen verifiziert wird. Wenn man (wie beim direkten Produkt) T bzw. H mit den entsprechenden Teilmengen von $T \rtimes_\alpha H$ identiziert, ist die Verknüpfung hierauf die ursprünglich gegebene, und $T \rtimes_\alpha H$ ist das (interne) semidirekte Produkt dieser zwei Untergruppen. D.h. wie bei direkten Produkten sind interne und externe semidirekte Produkte bis auf Isomorphie die gleichen Gruppen. Wir halten das zur Abrundung noch explizit als Zusatz zum letzten Satz fest:

Zusatz 2.7.11 Die Teilmengen $\widetilde{T} = T \times \{e\}$ und $\widetilde{H} = \{e\} \times H$ sind Untergruppen von $T \rtimes_\alpha H$ und $T \cong \widetilde{T},\ H \cong \widetilde{H}$; weiter ist $\widetilde{T}$ ein Normalteiler in $T \rtimes H$. Die

Gruppe $T \rtimes_\alpha H$ ist das (interne) semidirekte Produkt dieser Untergruppen. Die Operation von $\widetilde{H}$ auf $\widetilde{T}$ durch Konjugation entspricht der gegebenen Operation α von H auf T.

Beispiele 2.7.12 (Semidirekte Produkte II)

(1) Für jede abelsche Gruppe A ist die Inversenbildung $x \mapsto x^{-1}$ ein Automorphismus von A; dieser hat die Ordnung 2. Anders interpretiert haben wir also eine Operation der Gruppe $\{\pm 1\} \cong Z_2$ auf A, die durch $(\varepsilon, x) \mapsto x^\varepsilon$ gegegeben ist. Das zugehörige semidirekte Produkt $A \rtimes \{\pm 1\}$ hat also die Verknüpfung

$$(\varepsilon, x)(\delta, y) = (xy^\varepsilon, \varepsilon\delta), \quad \varepsilon, \delta \in \{\pm 1\},\ x, y \in A.$$

Speziell für eine zyklische Gruppe $A = Z_m$ erhalten wir hier eine neue, direkte Konstruktion der Diedergruppe.

(2) Für jeden Vektorraum V operiert die allgemeine lineare Gruppe $\mathrm{GL}(V)$ in natürlicher Weise auf V. Das entsprechende semidirekte Produkt $V \rtimes \mathrm{GL}(V)$ mit Verknüpfung $(v, f) \cdot (w, g) = (v + f(w), f \circ g)$ ist durch $(v, f) \mapsto \tau_v \circ f$ isomorph zur affinen Gruppe $\mathrm{AGL}(V)$. Vergleiche 2.7.7(2).

(3) Für einen euklidischen Vektorraum E und seine orthogonale Gruppe $\mathrm{O}(E)$ hat man entsprechend einen kanonischen Isomorphismus $E \rtimes \mathrm{O}(E) \cong \mathrm{Iso}(E)$. Vergleiche 2.7.7(3).

(4) Wir betrachten die euklidische Ebene $E = \mathbb{R}^2$ und hierin das „Gitter" $\mathbb{Z}^2$ aller ganzzahligen Punkte. Mit p4m bezeichnet man die (Unter-)Gruppe aller $\varphi \in \mathrm{Iso}(\mathbb{R}^2)$, die $\mathbb{Z}^2$ in sich abbilden, das ist also die Symmetriegruppe von $\mathbb{Z}^2$ (vergl. 2.4.4 (9)). Man kann hier die diskrete Punktmenge $\mathbb{Z}^2$ durch das „quadratische Gitter" ersetzen, das ist die Vereinigung aller Geraden durch ganzzahlige Punkte und parallel zur x-Achse der y-Achse (in der folgenden Zeichnung das Gitter aus den fetten Linien). Die Symmetriegruppe bleibt hierbei die gleiche.

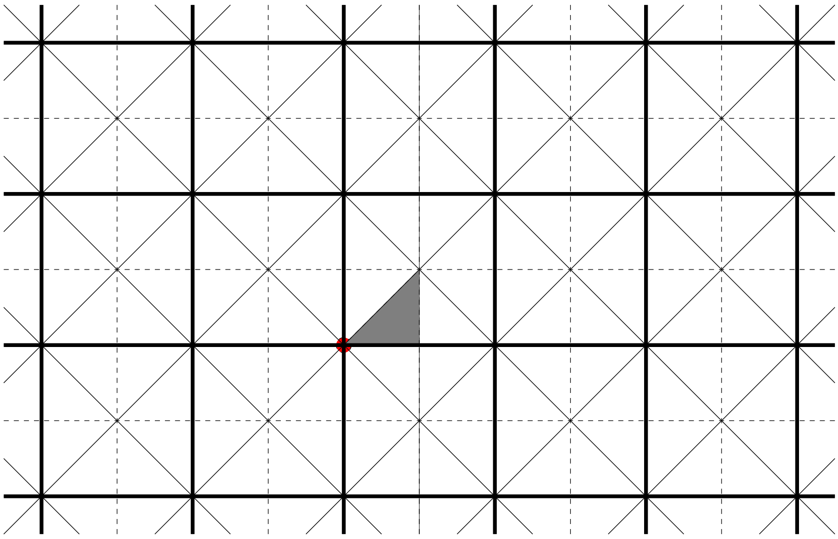

Abb. 2.5.1: Die Symmetrien des Quadrate-Gitters

Diese Gruppe ist ein Beispiel einer zweidimensionalen kristallographischen Gruppe (Ornamentgruppe), aus dieser Theorie kommt auch der Name p4m. Sie hat zwei offensichtliche Untergruppen: zum einen die Translationsgruppe mit ganzzahligen Verschiebungsvektoren $\mathrm{T}(\mathbb{Z}^2) = \{\tau_v \mid v \in \mathbb{Z}^2\}$, zum anderen den Stabilisator eines Punktes $x \in \mathbb{Z}^2$. Da alle diese Stabilisatoren konjugiert sind (siehe 2.4.14), reicht es $x = 0$ zu betrachten. Der Stabilisator von 0 in p4m besteht aus 4 Spiegelungen (an der x-Achse, y-Achse und den beiden durch $y = \pm x$ gegebenen Geraden), sowie den 4 Drehungen um Vielfache von 90°. Dieses ist genau die Diedergruppe Di_4, wie wir sie als Symmetriegruppe eines Quadrates mit Mittelpunkt im Nullpunkt kennen. Anders gesehen, entspricht diese Gruppe denjenigen 8 orthogonalen Matrizen, die gleichzeitig ganzzahlig sind: $\mathrm{Di}_4 \cong \mathrm{O}(\mathbb{Z}^2)$. Man überlegt sich nun leicht, dass p4m das Produkt der Untergruppen $\mathrm{T}(\mathbb{Z}^2)$ und $\mathrm{O}(\mathbb{Z}^2)$ ist; dieses ist ein semidirektes Produkt, weil $\mathrm{T}(\mathbb{Z}^2)$ normal ist. Ferner operiert $\mathrm{O}(\mathbb{Z}^2)$ auf $\mathbb{Z}^2$, und das externe semidirekte Produkt $\mathbb{Z}^2 \rtimes \mathrm{O}(\mathbb{Z}^2)$ ist wie unter (2) und (3) isomorph zu p4m.

Die Beispiele unter 2.7.12 waren überwiegend geometrischer Natur. Es gibt auch andere Situationen, in denen semidirekte Produkte mehr oder weniger zwangsläufig ins Spiel kommen, z.B. für Gruppen der Ordnung $p^k q^l$ für zwei Primzahlen p und q. Eine solche Gruppe ist immer das Produkt ihrer beiden Sylowgruppen, sobald eine von diesen normal ist, hat man ein semidirektes Produkt. Wir wissen aus dem Beweis von 2.5.14 c) (Gruppen der Ordnung < 60), dass dieses häufig vorkommt, z.B. immer für Gruppen der Ordnung pq oder pq^2. Um semidirekte Produkte mit Normalteiler T zu konstruieren, muss man naturgemäß die Automorphismengruppe von T kennen. Wir klären deren Gestalt im einfachen Fall einer zyklischen Gruppe.

Satz 2.7.13 *Die Automorphismengruppe einer zyklischen Gruppe Z der Ordnung $m < \infty$ ist kanonisch isomorph zu $(\mathbb{Z}/m\mathbb{Z})^*$. Der Isomorphismus ist gegeben durch*

$$(\mathbb{Z}/m\mathbb{Z})^* \to \operatorname{Aut} Z, \quad [k]_m \mapsto \alpha_k, \text{ wobei } \alpha_k(x) = x^k.$$

Wir erinnern daran, dass $(\mathbb{Z}/m\mathbb{Z})^*$ die Einheitengruppe des Rings $\mathbb{Z}/m\mathbb{Z}$ bezeichnet, das ist die Gruppe der Restklassen $[k]_m = k + m\mathbb{Z}$ mit zu m teilerfremden k und der Multiplikation als Verknüpfung. Wir weisen besonders darauf hin, dass der angegebene Isomorphismus nicht von der Wahl eines erzeugenden Elementes von Z, oder einer Identifikation von Z mit $(\mathbb{Z}/m\mathbb{Z}, +)$ abhängt; deshalb spricht man von einem „kanonischen" Isomorphismus.

Nun können wir die Klassifikation der Gruppen der Ordnung pq abschließend klären:

Satz 2.7.14 *Es seien p und q Primzahlen mit $q \equiv 1 \pmod p$. Dann gibt es eine nicht-abelsche Gruppe G der Ordnung pq. Sie ist semidirektes Produkt zweier zyklischer Gruppen, $G \cong Z_q \rtimes Z_p$, und bis auf Isomorphie eindeutig bestimmt.*