1.2.2 Untergruppen

Wie für jede wichtige mathematische Struktur, gibt es auch für Gruppen eine eigenständige *Theorie*, das heißt eine systematische Sammlung von Begriffen und Ergebnissen deren Sinn darin besteht, die wichtigsten Eigenschaften von Gruppen und ihre Beziehungen zueinander zu erfassen. Ein Ziel dieser Theorie ist die Formulierung eines Verfahrens, mit dem man einerseits alle endlichen Gruppen mit einer vorgegebenen Elementezahl $n \in \mathbb{N}$ bestimmen kann, und das außerdem eine Einsicht in die »Bauprinzipien« endlicher Gruppen liefert. Oder als Analogon: Man möchte nicht nur ein gothische Kathedrale nach den Plänen eines Baumeisters errichten können, sondern auch verstehen welche Gesetze der Statik dabei zum tragen kommen.

Was das erste der beiden Teilziele angeht, so kommt es nicht darauf an, ob die Elemente der gesuchten Gruppen Zahlen, Vektoren, Matrizen oder andere mathematische Objekte sind. Es kommt einzig auf die Art und Weise an, in der die einzelnen Elemente miteinander verknüpft werden. So wird man etwa die Gruppe $G_1 := (\{-1, +1\}, \cdot)$ bestehend aus den Zahlen -1 und $+1$ versehen mit der Multiplikation von ganzen Zahlen als innerer Verknüpfung nicht von der Gruppe $G_2 := (\{a, b\}, \cdot)$ unterscheiden, in der die innere Verknüpfung durch die Gleichungen $a \cdot b = b \cdot a = b$, $b^2 = a$, $a^2 = a$ definiert ist. Das Element $+1$ spielt in G_1 dieselbe Rolle wie a in G_2. Das Element b spielt in G_2 dieselbe Rolle wie -1 in G_1. Um alle endlichen Gruppen mit n Elementen zu bestimmen, genügt es also eine Menge $G = \{g_1, \ldots, g_n\}$ mit n Elementen zu fixieren, und alle Verknüpfungstafeln für G zu erstellen, die zu einer assoziativen inneren Verknüpfung mit einem neutralen Element und Inversen führen. Da es genau n^n verschiedene Verknüpfungstafeln gibt, gibt es höchstens n^n endliche Gruppen mit n Elementen; in Wahrheit gibt es sehr viel weniger. Das Problem ist in jedem Fall mit einem Computer und selbst mit einem einfachen Algorithmus in endlicher Zeit lösbar. Allerdings gewinnt man auf diese Weise keinen Einblick in die oben angeführten »Bauprinzipien«.

Was dieses zweite Teilziel angeht, so ist es naheliegend anzunehmen, dass sich Gruppen mit n Elementen aus solchen mit kleinerer Elementezahl als Bausteinen aufbauen lassen. Man wird also dazu geführt nach Teilmengen einer Gruppe $(G, \cdot)$ zu suchen, die selbst Gruppen mit der vorgegebenen Verknüpfung $\cdot$ sind, und zu untersuchen wie sich $(G, \cdot)$ aus diesen »Untergruppen« aufbaut. Auch in einer Kathedrale liegt ja nicht einfach Stein auf Stein, sondern diese sind häufig untereinander in verschiedener Weise verzahnt. Der

zentrale Schlussstein in einer Kuppel kann zum Beispiel die gesamte Kuppel stabil halten.

Die Idee des Aufbaus einer Gruppe aus Untergruppen lässt sich zwar mit großem Erfolg umsetzen, löst das Problem allgemeiner »Bauprinzipien« endlicher Gruppen aber nicht vollständig, ein Sachverhalt auf den im Rahmen dieser Vorlesung nicht tiefer eingegangen werden kann.

Nach diesem Vorwort ist klar, dass zuerst präzise definiert werden muss, was eine Untergruppe ist:

DEFINITION 37: *Es sei $(H, \cdot)$ eine Halbgruppe. Eine Teilmenge $U \subseteq H$ heißt Unterhalbgruppe von $(H, \cdot)$, wenn sie folgende Eigenschaft besitzt:*

$$\forall u_1, u_2 \in U \quad u_1 \cdot u_2 \in U.$$

Ist $(H, \cdot)$ ein Monoid, so nennt man eine Teilmenge $U \subseteq H$ ein Untermonoid von $(H, \cdot)$, falls U eine Unterhalbgruppe von $(H, \cdot)$ ist und zusätzlich

$$1 \in U$$

gilt.

Eine Teilmenge $U \subseteq H$ eines Monoids $(H, \cdot)$ heißt Untergruppe von $(H, \cdot)$, falls U ein Untermonoid von $(H, \cdot)$ ist und zusätzlich

$$U \subseteq H^\times \text{ und } \forall u \in U \; u^{-1} \in U$$

gilt.

Knapper kann man sagen: Eine Teilmenge U einer Halbgruppe (eines Monoids, einer Gruppe) $(H, \cdot)$ ist eine Unterhalbgruppe (ein Untermonoid, eine Untergruppe), falls U versehen mit der Verknüpfung $\cdot$ zu einer Halbgruppe (einem Monoid, eine Gruppe) wird.

Als erstes Beispiel erhält man aus Feststellung 17:

FESTSTELLUNG 38: *Für jedes Monoid $(H, \cdot)$ ist $H^\times$ eine Untergruppe.*

Für die weiteren Beispiele ist es relevant die folgende einfache Transitivitätsaussage im Auge zu behalten: *Ist $(U, \cdot)$ Unterhalbgruppe der Halbgruppe $(H, \cdot)$ und $(H, \cdot)$ Unterhalbgruppe der Halbgruppe $(H', \cdot)$, so ist $(U, \cdot)$ auch Unterhalbgruppe von $(H', \cdot)$.* Eine analoge Aussage gilt auch für Untermonoide und Untergruppen.

Beispiel 39 (Zahlbereiche (Forts.)): Die Menge $2\mathbb{N} := \{2n : n \in \mathbb{N}\}$ ist eine Unterhalbgruppe der Halbgruppe $(\mathbb{N}, +)$, denn für beliebige $k, \ell \in \mathbb{N}$ gilt $2k + 2\ell = 2(k + \ell)$.

Die Menge $2\mathbb{Z} := \{2z : z \in \mathbb{Z}\}$ dagegen ist eine Untergruppe der Gruppe $(\mathbb{Z}, +)$: Mit demselben Argument wie für $2\mathbb{N}$ ist die Addition eine innere Verknüpfung. Weiter gilt $0 \in 2\mathbb{Z}$ und mit $2k$ ist auch stets das Inverse $-2k$ in $2\mathbb{Z}$.

Die Menge $2\mathbb{N}_0 + 1 := \{2n + 1 : n \in \mathbb{N} \cup \{0\}\}$ aller ungeraden natürlichen Zahlen ist ein Untermonoid des Monoids $(\mathbb{N}, \cdot)$, denn es gilt für alle $k, \ell \in \mathbb{N} \cup \{0\}$:

$$(2k + 1)(2\ell + 1) = 2(2k\ell + k + \ell) + 1,$$

sowie $1 \in 2\mathbb{N}_0 + 1$.

Auch die folgenden Fakten lassen sich ähnlich einfach nachprüfen:

- $(\mathbb{Z}, +)$ ist ein Untergruppe der Gruppe $(\mathbb{Q}, +)$,
- $(\mathbb{Q}, +)$ ist ein Untergruppe der Gruppe $(\mathbb{R}, +)$,
- $(\mathbb{R}, +)$ ist ein Untergruppe der Gruppe $(\mathbb{C}, +)$,
- $(\mathbb{N}, \cdot)$ ist ein Untermonoid der Gruppe $(\mathbb{Q}^\times, \cdot)$,
- $(\mathbb{Q}^\times, \cdot)$ ist eine Untergruppe der Gruppe $(\mathbb{R}^\times, \cdot)$,
- $(\mathbb{Q}^{>0}, \cdot)$ ist eine Untergruppe der Gruppe $(\mathbb{R}^{>0}, \cdot)$,
- $(\mathbb{R}^\times, \cdot)$ ist eine Untergruppe der Gruppe $(\mathbb{C}^\times, \cdot)$.

Beispiel 40 (Vektoraddition (Forts.)): Die folgenden Fakten lassen sich leicht auf die entsprechenden Aussagen über Zahlbereiche zurückführen:

- $(\mathbb{Z}^n, +)$ ist eine Untergruppe von $(\mathbb{Q}^n, +)$,
- $(\mathbb{Q}^n, +)$ ist eine Untergruppe von $(\mathbb{R}^n, +)$,
- $(\mathbb{R}^n, +)$ ist eine Untergruppe von $(\mathbb{C}^n, +)$.

Beispiel 41 (Matrixoperationen (Forts.)): Entsprechend den Inklusionen $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ von Zahlbereichen ist $\mathrm{GL}(n, \mathbb{Q})$ Untergruppe von $\mathrm{GL}(n, \mathbb{R})$ und letztere Untergruppe von $\mathrm{GL}(n, \mathbb{C})$. Man bedenke hierbei, dass es auf den ersten Blick nicht selbstverständlich ist, dass zum Beispiel

die Inverse A^{-1} einer Matrix mit rationalen Koeffizienten wiederum rationale Koeffizienten besitzt. Dies wird klar, wenn man berücksichtigt, dass die Inverse mittels elementarer Zeilen- und Spaltenumformungen aus A berechnet werden kann, das heißt mittels Grundrechenarten, die nicht aus dem Zahlbereich $\mathbb{Q}$ herausführen.

Beispiel 42 (Punktweise Operationen (Forts.)): In der Analysis wird gezeigt, dass die punktweise Summe $f + g$ und das punktweise Produkt $f \cdot g$ zweier stetiger Funktionen $f, g \in \mathrm{Fun}([a, b], \mathbb{R})$ wiederum stetig sind. Jede konstante Funktion ist stetig, und mit einer Funktion f ist auch die Funktion $-f$ stetig. Die analogen Aussagen gelten auch, wenn man die Eigenschaft der Stetigkeit durch die Eigenschaft der Differenzierbarkeit ersetzt. Berücksichtigt man noch, dass differenzierbare Funktionen stetig sind, so folgt:

- Die Menge $\mathrm{C}([a, b], \mathbb{R})$ aller stetigen Funktionen $f : [a, b] \to \mathbb{R}$ ist eine Untergruppe von $(\mathrm{Fun}([a, b], \mathbb{R}), +)$,
- Die Menge $\mathrm{D}([a, b], \mathbb{R})$ aller differenzierbaren Funktionen $f : [a, b] \to \mathbb{R}$ ist eine Untergruppe von $(\mathrm{C}([a, b], \mathbb{R}), +)$,
- Die Menge $\mathrm{C}([a, b], \mathbb{R})$ ist ein Untermonoid von $(\mathrm{Fun}([a, b], \mathbb{R}), \cdot)$,
- Die Menge $\mathrm{D}([a, b], \mathbb{R})$ ist ein Untermonoid von $(\mathrm{C}([a, b], \mathbb{R}), \cdot)$.

Anstelle der stetigen Funktionen kann man auch für jedes $n \in \mathbb{N}$ die Menge der n-mal (stetig) differenzierbaren Funktionen betrachten um weitere Untergruppen und Untermonoide zu erhalten.

Wir werden ab jetzt nur noch den Fall von Untergruppen einer Gruppe diskutieren, da dieser für Anwendungen der Gruppentheorie am interessantesten ist. Das folgende einfache Kriterium für den »Untergruppentest« erweist sich oft als nützlich:

Feststellung 43: *Es sei $(G, \cdot)$ eine Gruppe. Eine nicht leere Teilmenge $U \subseteq G$ ist genau dann eine Untergruppe von G, wenn für beliebige Elemente $u_1, u_2 \in U$ auch $u_1 \cdot u_2^{-1}$ ein Element von U ist.*

Beweis: Es sei U eine Untergruppe. Dann ist nach Definition $1 \in U$ und für jedes $u_2 \in U$ auch $u_2^{-1} \in U$, und folglich gilt für $u_1, u_2 \in U$ auch $u_1 \cdot u_2^{-1} \in U$.

Für die Teilmenge $U \subseteq G$ gelte andererseits, dass aus $u_1, u_2 \in U$ stets $u_1 \cdot u_2^{-1} \in U$ folgt. Nach Voraussetzung existiert ein $u \in U$ und daher ist $1 = u \cdot u^{-1}$ in U – setze $u_1 = u_2 = u$. Damit ist zu jedem $u \in U$ auch $u^{-1} = 1 \cdot u^{-1} \in U$ – setze $u_1 = 1$ und $u_2 = u$. Folglich ist U eine Untergruppe. □

Untergruppen der Diedergruppen D_3 und D_6

Im Hinblick auf das Verständnis der »Bauprinzipien« von Gruppen ist es nützlich, sich einen Überblick über alle Untergruppen einer gegebenen Gruppe G zu machen, und über ihre gegenseitige »Lage« innerhalb von G. Da unendliche Gruppen in der Regel auch unendlich viele Untergruppen besitzen, ist ein solches Vorgehen nur im Fall endlicher Gruppen wirklich gangbar. Beispielhaft soll es anhand der Diedergruppen D_3 und D_6 durchgeführt werden.

Es sei zunächst U eine Untergruppe von D_3. Folgende Fälle können eintreten:

- U enthält nur das neutrale Element id. Diese Untergruppe von D_3 bezeichnet man oft mit E.

- U besitzt genau zwei Elemente. Das von id verschiedene Element $\tau \in U$ muss dann die Eigenschaft $\tau^2 = \mathrm{id}$ haben, also eine Spiegelung sein. Folglich gibt es drei verschiedene Untergruppen U_1, U_2, U_3 dieser Art, nämlich $U_i := \{\mathrm{id}, \tau_i\}$.

- U besitzt genau drei Elemente. Liegt in U eine Drehung σ, so liegt auch die Drehung σ^2 in U. Folglich ist dann $U = \{\mathrm{id}, \sigma_1, \sigma_2\} =: U_4$.

  Liegen in U zwei verschiedene Spiegelungen τ, τ', so zeigt die Verknüpfungstafel der D_3 (siehe Abschnitt 1.2.1), dass dann $\tau \circ \tau' \in U$ eine Drehung ist, woraus sich zusammen mit obiger Überlegung ein Widerspruch zur angenommenen Elementezahl ergibt. Dieser Fall tritt also nicht auf.

- Enthält U mehr als drei Elemente, so liegt in U mindestens eine Drehung und eine Spiegelung. Die Verknüpfungstafel zeigt, dass dann $U = D_3$ gilt.

Insgesamt besitzt D_3 also fünf Untergruppen. Ihre gegenseitige Lage stellt man üblicherweise in einem *Untergruppendiagramm* dar. Dabei handelt es

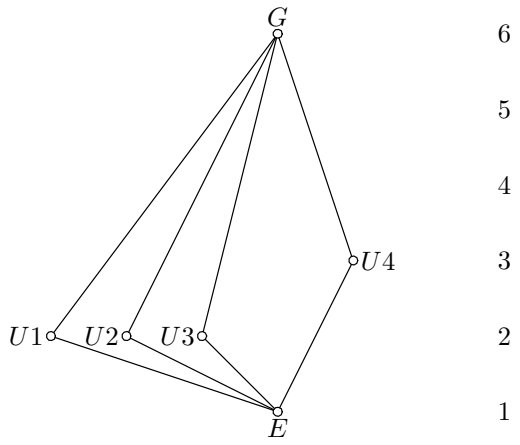

Abbildung 6: Untergruppen der Diedergruppe D_3

sich um einen Graphen, in dem die Untergruppen entsprechend zunehmender Elementezahl von unten nach oben angeordnet erscheinen. Zwei Untergruppen werden mit einer Linie verbunden, wenn die tiefer stehende Untergruppe in der höher stehenden enthalten ist. Die Abbildung 6 zeigt das Untergruppendiagramm der D_3. Die Skala auf der rechten Seite gibt die Elementezahlen der Untergruppen auf der jeweiligen Horizontalen an.

Um die Idee allgemeiner Bauprinzipien endlicher Gruppen weiter zu illustrieren, geht man zur Betrachtung der Diedergruppe D_6 des regelmäßigen 6-Ecks über. An dieser kann man die engen Beziehungen zwischen den Symmetrien des 6-Ecks und der Gruppenstruktur, insbesondere der Anzahl und Art vorhandener Untergruppen, gut darstellen.

In Abbildung 7 ist zu sehen, dass einem regelmäßigen 6-Eck H verschiedene Dreiecke und Rechtecke einbeschrieben sind. Im Folgenden werden diese durch Angabe ihrer Eckpunkte aufgelistet:

- Vier Dreiecke: $\Delta_1 = (E_1, E_3, E_5)$, $\Delta_2 = (M_1, M_3, M_5)$, $\Delta_3 = (E_2, E_4, E_6)$, $\Delta_4 = (M_2, M_4, M_6)$.

- Sechs Rechtecke: $R_1 = (M_1, M_3, M_4, M_6)$, $R_2 = (E_1, E_2, E_4, E_5)$, $R_3 = (M_1, M_2, M_4, M_5)$, $R_4 = (E_2, E_3, E_5, E_6)$, $R_5 = (M_2, M_3, M_5, M_6)$, $R_6 = (E_3, E_4, E_6, E_1)$.

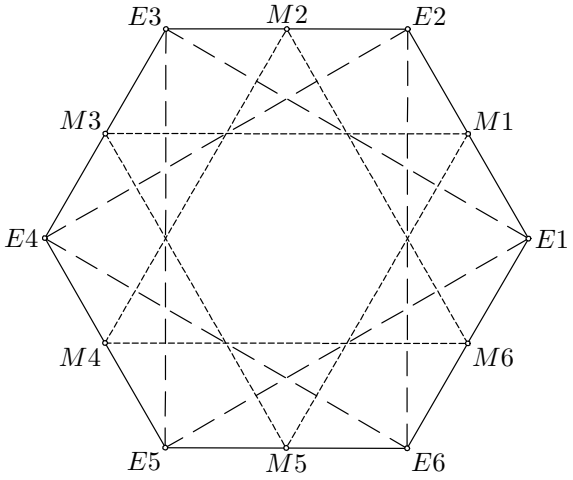

Abbildung 7: Beziehungen zwischen D_3 und D_6

Es ist nun naheliegend diejenigen $s \in D_6$ zu betrachten, die eine bestimmte der einbeschriebenen Figuren $F \subset H$ in sich abbilden:

$$U_F := \{s \in D_6 : s(F) = F\}$$

FESTSTELLUNG 44: *Die Teilmenge $U_F \subseteq D_6$ ist eine Untergruppe.*

BEWEIS: Ist $s \in U_F$ und E eine Ecke von F, so gibt es genau eine Ecke E' von F mit $s(E') = E$, da s die Ecken von F permutiert. Es folgt $E = s^{-1}(E')$. Da E beliebig war, permutiert s^{-1} also die Ecken von F, womit $s^{-1} \in U_F$ gilt.

Sei nun zusätzlich $t \in U_F$. Dann gilt für jede Ecke von F:

$$(t \circ s^{-1})(E) = t(s^{-1}(E)) = t(E') = E'',$$

wobei E' und E'' Ecken von F sind. Es folgt $t \circ s^{-1} \in U_F$; aus dem Untergruppenkriterium 43 kann man nun folgern, dass U_F eine Untergruppe von D_6 ist. □

Mit Hilfe der Feststellung 44 kann man nun eine Reihe von Untergruppen der D_6 angeben, wobei für die Elemente von D_6 die Bezeichnungen aus Abschnitt 1.2.1 verwendet werden:

- $V_1 := U_{\Delta_1} = U_{\Delta_3} = \{\mathrm{id}\,, \sigma_1^2, \sigma_1^4, \tau_1, \tau_3, \tau_5\}$,
- $V_2 := U_{\Delta_2} = U_{\Delta_4} = \{\mathrm{id}\,, \sigma_1^2, \sigma_1^4, \tau_2, \tau_4, \tau_6\}$,
- $W_1 := U_{R_1} = U_{R_4} = \{\mathrm{id}\,, \sigma_1^3, \tau_1, \tau_4\}$,
- $W_2 := U_{R_2} = U_{R_5} = \{\mathrm{id}\,, \sigma_1^3, \tau_2, \tau_5\}$,
- $W_3 := U_{R_3} = U_{R_6} = \{\mathrm{id}\,, \sigma_1^3, \tau_3, \tau_6\}$.

Aufällig an diesen Ergebnissen ist, dass sich zwei verschiedene der Untergruppen W_k stets in der Menge

$$Z_1 := \{\mathrm{id}\,, \sigma_1^3\}$$

schneiden. Man erkennt unmittelbar, dass es sich bei Z_1 um eine Untergruppe handelt. Auch die Untergruppen V_k zeigen ein solches Verhalten: Je zwei verschiedene schneiden sich in der Menge

$$Z_2 := \{\mathrm{id}\,, \sigma_1^2, \sigma_1^4\},$$

und auch diese Menge lässt sich leicht als Untergruppe von D_6 identifizieren.

Ein Mathematiker wird hinter diesen beiden Beobachtungen eine Gesetzmäßigkeit vermuten. Diese ist tatsächlich vorhanden:

Satz 45: *Es seien $U_1, \ldots, U_r$ Untergruppen der Gruppe G. Dann ist die Schnittmenge*

$$U := U_1 \cap \ldots \cap U_r$$

ebenfalls eine Untergruppe von G.

Beweis: Der Beweis wird durch vollständige Induktion nach r geführt.

Induktionsanfang ($r = 2$): Man wendet das Untergruppenkriterium 43 an. Dazu seien $u, v \in U_1 \cap U_2$. Da die U_i Untergruppen sind, gilt dann für das Inverse v^{-1} von v in G: $v^{-1} \in U_1$ und $v^{-1} \in U_2$, also $v^{-1} \in U_1 \cap U_2$. Entsprechend folgt $u \cdot v^{-1} \in U_1$ und $u \cdot v^{-1} \in U_2$, also $u \cdot v^{-1} \in U_1 \cap U_2$.

Induktionsschritt: Sind $U_1, \ldots, U_{r+1}$, $r \geq 2$, Untergruppen von G, so ist nach Induktionsannahme

$$U' := U_1 \cap \ldots \cap U_r$$

eine Untergruppe von G. Damit ist auch

$$U = U' \cap U_{r+1}$$

durch erneute Anwendung der Induktionsannahme eine Untergruppe von G. □

Die Untergruppen Z_1 und Z_2 bestehen ausschließlich aus Drehungen. Es drängt sich die Frage auf, ob es weitere solche nur aus Drehungen bestehende Untergruppen der D_6 gibt. Tatsächlich findet man eine weitere, und kann hierzu ein allgemein gültiges Resultat über Diedergruppen D_n formulieren:

FESTSTELLUNG 46: *Die Menge* $U := \{\mathrm{id}\,, \sigma_1, \sigma_1^2, \ldots, \sigma_1^{n-1}\}$ *aller Drehungen in der Diedergruppe* D_n *bildet eine zyklische Untergruppe von* D_n.

BEWEIS: Man wendet wieder das Untergruppenkriterium 43 an. Sind $u_1 := \sigma_1^k$ und $u_2 := \sigma_1^\ell$ zwei Elemente von U, so gilt

$$u_2^{-1} = \sigma_1^{n-\ell} \in U.$$

Es folgt

$$u_1 \circ u_2^{-1} = \sigma_1^k \circ \sigma_1^{n-\ell} = \sigma_1^{n-k+\ell} \in U.$$

Die Untergruppe U ist zyklisch, weil σ_1 die Gruppe erzeugt. □

Im Fall der Diedergruppe D_6 erhält man also eine weitere Untergruppe, nämlich

$$Z_3 = \{\mathrm{id}\,, \sigma_1, \sigma_1^2, \sigma_1^3, \sigma_1^4, \sigma_1^5\}.$$

Schließlich liefert jede der sechs Spiegelungen τ_k eine Untergruppe, nämlich

$$U_k := \{\mathrm{id}\,, \tau_k\}.$$

Die bisherige Diskussion der D_6 hat insgesamt 14 von E und D_6 verschiedene Untergruppen zutage gefördert, deren gegenseitige Lage im Untergruppendiagramm 8 dargestellt ist. Man erkennt deutlich, dass etwa die Untergruppe V_1 diesselbe Struktur wie die Diedergruppe D_3 besitzt, denn V_1 besteht nach Definition genau aus den Symmetrieoperationen des Dreiecks $\Delta_1 \subset H$. Dasselbe gilt für die Untergruppe V_2. Auffällig ist auch, dass es keine Untergruppen mit Elementezahlen zwischen 7 und 11, sowie der Elementezahl 5 zu geben scheint. Es ist natürlich nicht auszuschließen, dass die oben geführte Diskussion solche Untergruppen einfach nicht erfasst hat.

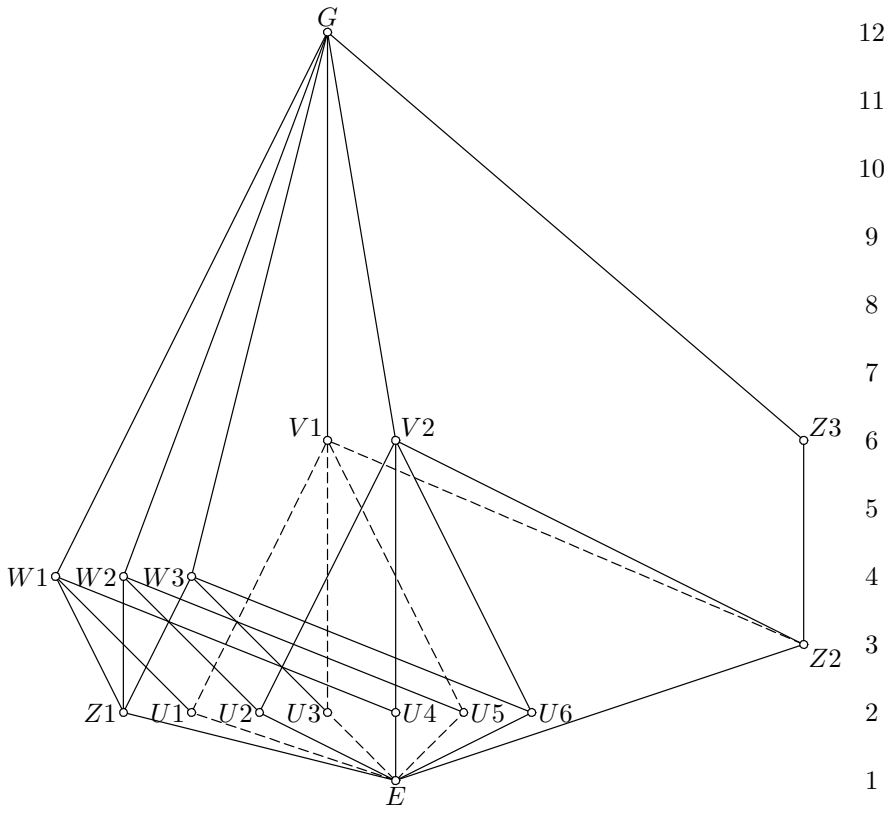

Abbildung 8: Untergruppen der D_6

Tatsächlich hat unsere Diskussion alle Untergruppen erfasst, wie eine etwas längliche aber elementare Argumentation zeigen würde, die hier allerdings nicht durchgeführt werden soll.

Wir wenden uns nun der Beobachtung zu, dass zu bestimmten Zahlen kleiner als $12 = |D_6|$ keine Untergruppen existieren, also der Frage, welche Größen Untergruppen einer endlichen Gruppe überhaupt haben können.

Der Satz von Lagrange

Um zu ermitteln in welcher Beziehung die Elementezahl $|U|$ einer Untergruppe einer endlichen Gruppe $(G, \cdot)$ zur Elementezahl $|G|$ steht, verfolgt man eine einfache Idee, die auf folgender nun schon öfter benutzten Tatsache

beruht: Ist $g \in G$, so ist die *Linksmultiplikation mit g*

$$\ell_g : \ G \to G, \ h \mapsto g \cdot h \tag{11}$$

eine bijektive Abbildung. Denn die Linksmultiplikation $\ell_{g^{-1}}$ mit dem Inversen zu g ist die Umkehrabbildung zu ℓ_g. Dies gilt auch für unendliche Gruppen.

Sind nun $1, u_1, \ldots, u_r$ die verschiedenen Elemente der Untergruppe U und ist $g \in G \setminus U$, so sind die Elemente $g, g \cdot u_1, \ldots, g \cdot u_r$ alle verschieden und keines liegt in U. Ersteres folgt aus der Injektivivität von ℓ_g und Letzteres aus folgender Überlegung: Wäre $g \cdot u_k = u$ für ein $u \in U$, so ergäbe sich der Widerspruch $g = u \cdot u_k^{-1} \in U$. Insgesamt hat man damit $2r$ verschiedene Elemente in G ermittelt. Dieses Verfahren lässt sich fortsetzen: Man wählt ein $h \in G \setminus U$ mit $h \notin \{g, g \cdot u_1, \ldots, g \cdot u_r\}$, falls ein solches Element existiert, das heißt $2r < |G|$ gilt. Damit gewinnt man r verschiedene Elemente $h, h \cdot u_1, \ldots, h \cdot u_r$, die nicht in U liegen. Mehr noch, keines der neuen Element $h \cdot u_i$ ist gleich einem $g \cdot u_j$, denn dies würde $h = g \cdot u_j \cdot u_i^{-1} = g \cdot u_k$ für ein bestimmtes k bedeuten.

Man erkennt, dass das Fortführen des obigen Verfahrens zu der Gleichung $|G| = s|U|$, $s \in \mathbb{N}$, führt. Dies ist der sogenannte Satzes von Lagrange, den wir jetzt etwas konzeptioneller darstellen wollen.

Definition 47: *Es sei G eine Gruppe und U eine Untergruppe von G. Eine Linksnebenklasse von G modulo U ist eine Menge der Form*

$$g_0 \cdot G := \{g_0 \cdot u : u \in U\}, \ g_0 \in G.$$

Wir tragen die Eigenschaften von Linksnebenklassen zusammen:

Feststellung 48: *Für die Nebenklassen der Gruppe G modulo U gilt:*

1. $\forall g \in G \quad g \in g \cdot U$.
2. $g_1 \cdot U = g_2 \cdot U \ \Leftrightarrow \ g_2 = g_1 \cdot u$ *für ein* $u \in U$.
3. $(g_1 \cdot U \cap g_2 \cdot U \neq \emptyset) \Rightarrow (g_1 \cdot U = g_2 \cdot U)$.

Beweis: 1. $g = g \cdot 1$, wobei $1 \in U$.

2. Gilt $g_1 \cdot U = g_2 \cdot U$, so folgt $g_2 = g_1 \cdot u$ für ein $u \in U$. Ist andererseits $g_1 \cdot U$ eine beliebige Linksnebenklasse und $g_2 := g_1 \cdot u$ für ein beliebiges $u \in U$, so gilt für ein beliebiges $u' \in U$:

$$g_2 \cdot u' = g_1 \cdot (u \cdot u') \in g_1 \cdot U,$$

das heißt $g_1 \cdot U \subseteq g_2 \cdot U$. Genauso zeigt man: $g_2 \cdot U \subseteq g_1 \cdot U$. Insgesamt gilt also $g_1 \cdot U = g_2 \cdot U$.

3. Jedes Element $h \in g_1 \cdot U \cap g_2 \cdot U$ besitzt die Form $h = g_1 \cdot u_1 = g_2 \cdot u_2$ für gewisse $u_1, u_2 \in U$. Es folgt $g_2 = g_1 \cdot u_1 \cdot u_2^{-1}$. Punkt 2 liefert daher $g_1 \cdot U = g_2 \cdot U$. □

Im Weiteren sei

$$G/U := \{g \cdot U : g \in G\}$$

die Menge aller Linksnebenklassen von G modulo U.

Satz 49 (J. L. Lagrange (∗ 1736, † 1813), 1771): *Es sei G eine endliche Gruppe. Dann gilt für jede Untergruppe U von G die Formel*

$$|G| = |U|(G : U),$$

wobei das Symbol $(G : U)$ die Anzahl der Linksnebenklassen von G modulo U bezeichnet. Man nennt diese Zahl den Index von U in G.

Beweis: Für jedes $g \in G$ gilt $g \in g \cdot U$ und verschiedene Linksnebenklassen sind disjunkt. Also folgt

$$G = \bigcup_{g \cdot U \in G/U} g \cdot U.$$

Hieraus folgt die Behauptung nach Definition von $(G : U)$ und weil alle Linksnebenklassen $|U|$ Elemente besitzen. □

Auch wenn der Satz von Lagrange keine Aussage über die Anzahl von Untergruppen vorgegebener Elementezahl macht, so liefert er doch eine wichtige und stark einschränkende Bedingung für die möglichen Größen von Untergruppen. Die überraschenden Konsequenzen aus dem Satz machen das deutlich:

Korollar 50: *Ist die Ordnung einer endlichen Gruppe eine Primzahl, so besitzt sie keine Untergruppen $U \neq E$, $U \neq G$ und ist zyklisch.*

Beweis: Ist U eine Untergruppe von G, so kann nach dem Satz von Lagrange unter der Voraussetzung, dass $|G|$ eine Primzahl ist, nur $|U| = 1$ oder $|U| = |G|$ gelten.

Es sei $g \in G$, $g \neq 1$. Dann ist $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ eine zyklische Untergruppe von G und es gilt $\langle g \rangle \neq E$. Folglich muss nach dem bereits Bewiesenen $\langle g \rangle = G$ gelten. □

Die *Ordnung eines Elements* g einer Gruppe $(G, \cdot)$ ist die kleinste natürliche Zahl m, für die $g^m = 1$ gilt, sofern eine solche Zahl existiert. Man bezeichnet sie dann mit dem Symbol $\operatorname{ord}(g)$.

KOROLLAR 51: *In einer endlichen Gruppe G ist die Ordnung* $\operatorname{ord}(g)$ *jedes Elements g ein Teiler der Gruppenordnung $|G|$.*

BEWEIS: Die Aussage folgt aus dem letzten Korollar, wenn man sich in Erinnerung ruft, dass nach Satz 29 $\operatorname{ord}(g)$ die Elementzahl der zyklischen Untergruppe $\langle g \rangle$ von G ist. □