KAPITEL 1

Einleitung

Als Einstieg in die Vorlesung möchte ich zunächst zeigen, dass aus den Grundvorlesungen schon eine ganze Fülle von Beispielen algebraischer Strukturen bekannt sind. Von diesen Beispielen ausgehend möchte ich dann versuchen, die wichtigsten Ideen des heute üblichen Zugangs zur Algebra zu skizzieren und dabei insbesondere die Rolle der Abstraktion zu klären.

Zum Verständnis dieses Kapitels wird es für die Studierenden hilfreich sein, einige Konzepte aus den Grundvorlesungen, insbesondere über lineare Algebra und Geometrie, zu wiederholen.

Aus den Grundvorlesungen bekannte Beispiele algebraischer Strukturen

Die Algebra ist einer der Grundpfeiler der modernen Mathematik und kann grob gesagt als das Studium verschiedener Arten von "Rechenoperationen" angesehen werden. Die ersten Beispiele von algebraischen Strukturen kommen daher aus den schon aus der Schule bekannten Zahlbereichen.

1.1. Zahlbereiche. Wir betrachten hier die üblichen Zahlbereiche $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ mit den üblichen Operationen Addition und Multiplikation. Betrachten wir zunächst die Addition auf den verschiedenen Zahlbereichen, dann ist diese assoziativ (d.h. es gilt $(a+b)+c = a+(b+c)$ für beliebige Elemente a, b, c des jeweiligen Bereichs) und kommutativ (d.h. es gilt $a + b = b + a$ für beliebige Elements a und b). Außerdem gibt es in jedem der Bereiche ein neutrales Element 0 für die Addition, d.h. es gilt $0 + a = a$ für alle Elements a. (Wir werden immer die Konvention verwenden, dass $0 \in \mathbb{N}$ gilt.) Spricht man über Gruppen, dann wird das neutrale Element oft auch als "Einselement" bezeichnet, weil in allgemeinen Gruppen die Operation meist wie eine Multiplikation geschrieben wird. Man darf sich also nicht davon verwirren lassen, dass die Zahl Null das Einselement in der additiven Gruppen ist.

In $\mathbb{Z}$ und in den größeren Zahlbereichen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ gibt es für die Addition inverse Elemente. Das bedeutet, dass es zu jedem Element a ein Element b gibt, sodass $a+b = 0$ gilt. Da dieses Element durch a eindeutig bestimmt ist, wird es üblicherweise mit $-a$ bezeichnet.

Formal ausgedrückt bedeuten die bisherigen Beobachtungen, dass $(\mathbb{N}, +)$ eine *kommutative Halbgruppe mit Einselement* oder kurz ein *kommutatives Monoid* ist, während $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ *kommutative Gruppen* sind. Tatsächlich kann man den Übergang von $\mathbb{N}$ zu $\mathbb{Z}$ so verstehen, dass man zu den Elementen von $\mathbb{N}$ additiv inverse Elemente hinzufügt, bzw. dass man das Monoid $(\mathbb{N}, +)$ zu einer kommutativen Gruppe "vervollständigt". Die Erweiterungsprozesse, die zu den größeren Zahlbereichen führen sind dann alle so gestaltet, dass die schönen Eigenschaften der Addition erhalten bleiben.

Nun kann man analog die Operation der Multiplikation auf den Zahlbereichen betrachten. Diese ist ebenfalls immer assoziativ und kommutativ und hat ein neutrales

Element (diesmal wirklich die Eins). Damit macht die Multiplikation alle angeführten Zahlbereiche zu kommutativen Halbgruppen mit Einselement. Sobald man aber beginnt, über multiplikativ inverse Elemente nachzudenken, muss man die Null ausschließen. Will man die Multiplikation als Operation auf den Elementen ungleich Null betrachten, dann muss man zunächst bemerken, dass ein Produkt von Zahlen ungleich Null ist, wenn beide Faktoren ungleich Null sind.

In dieser Sichtweise sind dann $(\mathbb{N}\setminus\{0\},\cdot)$ und $(\mathbb{Z}\setminus\{0\},\cdot)$ wieder kommutative Halbgruppen mit Einselement. In den Zahlbereichen ab $\mathbb{Q}$ gibt es für jedes Element $a\neq 0$ ein multiplikativ inverses Element, nämlich $1/a$. Daher sind $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ und $(\mathbb{C}\setminus\{0\},\cdot)$ kommutative Gruppen.

Die Tatsache, dass bei der Betrachtung der Multiplikation auf den Zahlbereichen das neutrale Element der Addition eine besondere Rolle spielt zeigt schon, dass der "richtige" Standpunkt ist, die Zahlbereiche als Mengen mit zwei Operationen zu betrachten. Dazu muss man noch bemerken, dass die Multiplikation *distributiv* bezüglich der Addition ist, also $a\cdot(b+c)=a\cdot b+a\cdot c$ für alle a,b,c gilt. Zusammen mit den oben aufgelisteten Eigenschaften der Addition und Multiplikation bedeutet das, dass $(\mathbb{Z},+,\cdot)$ ein *kommutativer Ring mit Einselement* ist, während $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$ *Körper* sind. Es gibt auch für die oben bemerkten Eigenschaften von $(\mathbb{N},+,\cdot)$ einen allgemeinen Begriff ("kommutativer Halbring mit Einselement") der aber nicht so wichtig ist, wie die anderen genannten Begriffe.

Wie oben beschrieben, kann man von $(\mathbb{N},+)$ zu $(\mathbb{Z},+)$ übergehen, indem man additiv inverse Elemente "dazu gibt". In diesem Prozess kann die Multiplikationsoperation auf $\mathbb{N}$ eindeutig auf $\mathbb{Z}$ ausgedehnt werden, indem man verlangt, dass das Distributivgesetz weiterhin gilt. Tatsachen wie "Minus mal Minus ist Plus" sind also keine Konvention, sondern ergeben sich zwingend aus den Verträglichkeitsbedingungen der Rechenoperationen (siehe Übungen).

Analog kann man den Übergang von $(\mathbb{Z},+,\cdot)$ zu $(\mathbb{Q},+,\cdot)$ allgemein so verstehen, dass man einen kommutativen Ring (mit gewissen zusätzlichen Eigenschaften) zu einem Körper "vervollständigen" kann, indem man multiplikativ inverse Elemente (für Elemente ungleich Null) hinzufügt. Es ist nicht möglich, zu allen Elementen multiplikativ inverse Elemente zu haben (siehe Übungen).

Der Übergang von $(\mathbb{Q},+,\cdot)$ zu $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+\cdot)$ ist **nicht** von algebraischer Natur. Es handelt sich dabei um eine Vervollständigung im technischen Sinn. Hier kann Vollständigkeit entweder über die natürliche Ordnungsrelation definiert werden ("jede nichtleere nach oben beschränkte Teilmenge besitzt ein Supremum") oder über metrisch–topologische Eigenschaften ("jede Cauchyfolge konvergiert"). Zwar haben $\mathbb{R}$ und $\mathbb{C}$ auch algebraisch "bessere" Eigenschaften als $\mathbb{Q}$, insbesondere was die Existenz von Lösungen von Polynomgleichungen betrifft, aber diese Eigenschaften sind "Nebeneffekte" der Vollständigkeit.

Will man etwas sehen, dass die Gleichung $x^2=2$ (die in $\mathbb{Q}$ nicht lösbar ist) eine Lösung in $\mathbb{R}$ besitzt, dann kann man entweder argumentieren (siehe Übungen), dass das Supremum der Menge $\{x\in\mathbb{R}: x^2<2\}$, die offensichtlich nicht leer und nach oben beschränkt ist, eine Lösung sein muss. Alternativ kann man beobachten, dass $f(x)=x^2-2$ eine stetige Funktion $f:\mathbb{R}\to\mathbb{R}$ definiert, und die Existenz einer Nullstelle aus dem Zwischenwertsatz folgern. Man beachte, dass beide Methoden nur die Existenz der Lösung beweisen. Um genauere Informationen zu bekommen, wie diese Lösung aussieht, sind zusätzliche Überlegungen nötig.

In enger Beziehung zu den Zahlbereiche stehen die Mengen von Restklassen, die ebenfalls aus den Grundvorlesungen bzw. aus der Zahlentheorie bekannt sind. Für eine fixe Zahl $p \in \mathbb{N}$, $p > 1$ betrachtet man $m, n \in \mathbb{Z}$ als äquivalent, falls $m - n$ ein ganzzahliges Vielfaches von p ist. Die Menge der Äquivalenzklassen wird mit $\mathbb{Z}_p$ bezeichnet und für $n \in \mathbb{Z}$ schreibt man $\bar{n}$ für die Äquivalenzklasse von n. Es gibt für diese Relation genau p Äquivalenzklassen und $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$. Man verifiziert dann, dass $\bar{m}+\bar{n} = \overline{m+n}$ und $\bar{m}\cdot\bar{n} = \overline{m \cdot n}$ eine wohldefinierte Addition und Multiplikation auf $\mathbb{Z}_p$ Liefern. Die Eigenschaften der Operationen auf $\mathbb{Z}$ lassen sich leicht auf $\mathbb{Z}_p$ übertragen, sodass $(\mathbb{Z}_p, +, \cdot)$ für jedes p ein kommutativer Ring mit Einselement ist.

Interessant ist aber, dass die algebraische Struktur auf $\mathbb{Z}_p$ bessere Eigenschaften haben kann als die Struktur auf $\mathbb{Z}$ von der sie induziert wird. Ist nämlich p eine Primzahl, dann kann man relativ leicht zeigen, dass $\mathbb{Z}_p$ ein Körper ist, es also für Elemente $\neq \bar{0}$ immer ein multiplikativ inverses Element in $\mathbb{Z}_p$ gibt. Man kann also durch Quotientenbildung Strukturen konstruieren, die schönere Eigenschaften haben, als die Strukturen von denen man ausgegangen ist.

1.2. Andere Beispiele. Eine fundamentale Quelle von Beispielen von Gruppen ist mit dem Konzept der Symmetrie verbunden, dass eine zentrale Rolle in vielen Bereichen der Mathematik spielt. Der Hintergrund dieser Beispiele ist, dass die Komposition von Funktionen zwischen Mengen automatisch assoziativ ist. Betrachtet man nun Funktionen von einer Menge auf sich selbst, dann hat man neben der Assoziativität der Komposition auch automatisch ein neutrales Element für die Komposition, nämlich die Identitätsabbildung $id_X : X \to X$. Für eine bijektive Funktion $f : X \to X$ gibt es die inverse Funktion $f^{-1} : X \to X$, die nach Definition $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$ erfüllt, also ein zu f inverses Element bezüglich der Komposition bildet. Allerdings gibt es keinen Grund, warum das Resultat einer Komposition unabhängig von der Reihenfolge der Faktoren sein sollte. Die Komposition ist daher nur in Ausnahmefällen kommutativ. Für invertierbare Funktionen f und g sieht man aber sofort, dass die Funktion $f^{-1} \circ g^{-1}$ invers zu $g \circ f$ ist. Somit ist $g \circ f$ bijektiv und $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Aus diesen Beobachtungen folgt insbesondere, dass die Komposition für jede Menge X eine Gruppenstruktur auf der Menge $\mathrm{Bij}(X)$ aller bijektiven Funktionen $f : X \to X$ definiert. Falls X mindestens 3 Elemente hat, ist diese Gruppe nicht kommutativ (siehe Übungen). Setzt man $X = \{1, \dots, n\}$ für eine natürliche Zahl n, dann erhält man so die aus den Grundvorlesungen bekannte Permutationsgruppe $\mathfrak{S}_n$.

Man kann dieses Prinzip aber ganz allgemein anwenden, und muss oft nicht einmal wissen, wie die betrachteten Funktionen konkret aussehen. Ein Beispiel mit fundamentaler Bedeutung für die Geometrie ist folgendes. Betrachten wir $\mathbb{R}^n$ mit der üblichen Euklidischen Distanz $d(x, y) := \sqrt{\langle y - x, y - x\rangle}$. Eine *Isometrie* von $\mathbb{R}^n$ ist eine bijektive Funktion $f : \mathbb{R}^n \to \mathbb{R}^n$, sodass $d(f(x), f(y)) = d(x, y)$ für alle $x, y \in \mathbb{R}^n$ gilt. Ist nun f eine Isometrie und f^{-1} die inverse Funktion zu f, dann rechnen wir für $x, y \in \mathbb{R}^n$:

$$d(f^{-1}(x), f^{-1}(y)) = d(f(f^{-1}(x)), f(f^{-1}(y))) = d(x, y).$$

Somit ist auch f^{-1} eine Isometrie. Analog gilt für eine weitere Isometrie g natürlich

$$d(g(f(x)), g(f(y))) = d(f(x), f(y)) = d(x, y),$$

also ist auch $g \circ f$ eine Isometrie. Somit schließen wir aus den obigen Beobachtungen, dass die Komposition die Menge der Isometrien von $\mathbb{R}^n$ zu einer Gruppe macht.

Auf diese Weise erhält man eine Vielzahl von Beispielen, von denen einige schon in den Grundvorlesungen aufgetaucht sind. Ist etwa V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{K}$, dann kann man die Menge aller bijektiven *linearen*

Abbildung $f : V \to V$ betrachten. Nachdem die inverse Funktion zu einer bijektiven linearen Abbildung sowie die Komposition zweier linearer Abbildungen wieder linear ist, folgt wie oben, dass die bijektiven linearen Abbildungen $f : V \to V$ eine Gruppe unter der Komposition bilden. Spezialisiert man auf $V = \mathbb{K}^n$, dann kann man analog invertierbare $n \times n$–Matrizen über $\mathbb{K}$ betrachten und feststellen, dass diese eine Gruppe bezüglich der Matrizenmultiplikation bilden.

Die lineare Algebra bietet auch interessante Beispiele von Strukturen mit zwei Operationen. Betrachtet man etwa den Raum $L(V, V)$ aller linearen Abbildungen $f : V \to V$ für einen endlichdimensionalen Vektorraum V, dann kann man neben der bereits erwähnten Komposition auch die Addition betrachten, die punktweise, also durch $(f + g)(v) := f(v) + g(v)$ definiert ist. Auf der rechten Seite dieser Gleichung steht die Addition im Vektorraum V und aus den Eigenschaften dieser Addition folgt sofort, dass die punktweise Addition $L(V, V)$ zu einer kommutativen Gruppe macht. (In der linearen Algebra zeigt man ja sogar, das $L(V, V)$ selbst wieder ein Vektorraum ist.) Da man mit linearen Abbildungen arbeitet folgt, dass die Komposition distributiv bezüglich der punktweisen Addition macht (siehe Übungen). Außerdem bildet die Identitätsabbildung id_V natürlich ein neutrales Element bezüglich der Komposition. Damit ist $(L(V, V), +, \circ)$ ein (im Allgemeinen nicht kommutativer) Ring mit Einselement.

Betrachtet man das für den Spezialfall $V = \mathbb{K}^n$ dann kann man den Raum $L(V, V)$ mit dem Raum $M_n(\mathbb{K})$ aller $n \times n$–Matrizen über $\mathbb{K}$ identifizieren. In diesem Bild entspricht die punktweise Addition linearer Abbildungen der komponentenweisen Addition von Matrizen und die Komposition der Matrizenmultiplikation. Somit ist auch $(M_n(\mathbb{K}), +, \cdot)$ ein (im Allgemeinen nicht kommutativer) Ring mit Einselement.

Aus der linearen Algebra ist auch (zumindest in Ansätzen) der Raum $\mathbb{K}[x]$ aller Polynome (beliebigen Grades) über einem fixen Körper $\mathbb{K}$ bekannt. Solche Polynome werden am besten als formale Ausdrücke betrachtet. Alternativ kann man für unendliche Körper Polynome auch als spezielle Funktionen von $\mathbb{K}$ nach $\mathbb{K}$ betrachten. Im ersten Fall definiert man die Addition und Multiplikation einfach explizit über die Koeffizienten der Polynome. Diese Operationen entsprechen dann genau der punktweisen Addition und Multiplikation von Funktionen. Aus der letzten Betrachtungsweise folgt sofort, dass $\mathbb{K}[x]$ ein kommutativer Ring mit Einselement ist, im Bild der formalen Ausdrücke kann man das relativ leicht explizit verifizieren.

Einige allgemeine Prinzipien der Algebra

Einige Prinzipien der Algebra sind schon aus den Grundvorlesungen über lineare Algebra (je nach Vortragendem in mehr oder weniger expliziter Form) bekannt. Wir werden daher die Prinzipien oft mit Beispielen aus der linearen Algebra illustrieren.

1.3. Strukturen. Es hat sich in der Mathematik allgemein durchgesetzt, die Objekte, die man untersucht immer als Mengen mit gewissen zusätzlichen Strukturen zu beschrieben. In der Algebra sind diese Strukturen meist Operationen, die als Funktionen auf Produkten der beteiligten Mengen definiert werden. So ist etwa ein Vektorraum über einem Körper $\mathbb{K}$ definiert als eine Menge V zusammen mit zwei Operationen, der Addition $+ : V \times V \to V$ und der Multiplikation mit Skalaren $\cdot : \mathbb{K} \times V \to V$. Man verlangt dann, dass diese Operationen bestimmte Eigenschaften haben (Assoziativität, etc.) bzw. in gewisser Weise mit der Addition und der Multiplikation des Körpers $\mathbb{K}$ verträglich sind. (Ein Vektorraum über einem Körper ist vergleichsweise eine ziemlich komplizierte algebraische Struktur.)

Ein weiteres ganz allgemeines Prinzip der Mathematik ist, dass zu Objekten mit einer gewissen Struktur immer auch strukturerhaltende Abbildungen ("Morphismen") gehören, mit deren Hilfe man verschiedene Objekte in Beziehung setzen kann. Die Menge $\mathbb{R}$ zum Beispiel tritt in so vielen verschiedenen Rollen auf, dass man hauptsächlich an den betrachteten Funktionen (linear, stetig, differenzierbar, integrierbar, ...) erkennen kann, welche Struktur auf $\mathbb{R}$ im Moment gerade relevant ist. Im Fall der Vektorräume über einem Körper $\mathbb{K}$ sind die strukturerhaltenden Abbildungen natürlich die linearen Abbildungen.

Die grundlegenden Definitionen einer algebraischen Struktur sind oft sehr allgemein und "abstrakt". Diese Abstraktion ist nicht Selbstzweck und soll auch nicht suggerieren, dass man sich unbedingt für die allgemeinsten Beispiele so einer Struktur interessieren soll oder muss. Der wesentliche Punkt ist, dass man versucht herauszuarbeiten, welche Eigenschaften einer Struktur man momentan tatsächlich benutzt, und welche momentan nicht relevant sind. Damit ist sichergestellt, dass bewiesene Resultate effizient (weil möglichst breit) anwendbar sind. Zugleich sinkt die Gefahr, dass man sich von zusätzlichen Eigenschaften, die Im diesem Moment gar nicht wirklich relevant sind, verwirren lässt. In tiefliegenderen Teilen der Algebra führt das oft zu einer ganzen Hierarchie von Eigenschaften einer algebraischen Struktur. Wir werden das in Ansätzen bei konkreten Strukturen kennen lernen.

An dieser Stelle ist noch ein wichtiger Punkt zu erwähnen: Wenn man sich Definitionen oder Begriffe in der Algebra (oder in anderen Teilen der Mathematik) ansieht, dann stellen sich oft Fragen wie "Warum sind gerade diese Eigenschaften so wichtig, dass man sie zur Definition erhebt?". Solche Fragen sind ganz natürlich und man darf sich nicht erhoffen, dass man die Antwort sofort (oder überhaupt) intuitiv erkennt. Gute und angemessene Begriffe zu finden ist schwierig und oft ein wichtiger Schritt in der Weiterentwicklung der Mathematik. In vielen Fällen haben sich die "richtigen" Begriffe erst in einer längeren Entwicklung herauskristallisiert. Eine verwandte Frage ist "Könnte man das nicht auch ein bisschen anders machen?". Hier ist die Antwort, dass die meisten alternativen Konzepte schon von irgend jemandem ausprobiert wurden und üblicherweise entweder zu äquivalenten Definitionen führen wie die üblichen Begriffe oder im Vergleich zu diesen Nachteile aufweisen.

1.4. Beispiele und Konstruktionen. Beispiele für algebraische Strukturen spielen in doppelter Hinsicht eine wichtige Rolle. Zum einen sind natürlich einfache und typische Beispiele für algebraische Strukturen wichtig. Diese können auch den Ausgangspunkt bilden, um mittels gewisser Konstruktionen kompliziertere Objekte aufzubauen. Im Fall der Vektorräume wären die einfachen Beispiele etwa die Räume $\mathbb{K}^n$ als Vektorräume über $\mathbb{K}$. Andererseits sind auch "exotische" Beispiele wichtig, um die Grenzen dessen, was man noch allgemein beweisen kann, abzustecken. Im Fall der Vektorräume sind etwa $\mathbb{R}$ als Vektorraum über $\mathbb{Q}$ und der Raum aller Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ als Vektorraum über $\mathbb{R}$ solche Beispiele.

Um kompliziertere Objekte aus einfacheren aufbauen zu können sind einerseits die Konzepte von Teilobjekten und von Quotientenobjekten notwendig. (Im Fall der Vektorräume über einem Körper sind das lineare Teilräume und Quotientenräume.) Die grundlegenden Idee eines Teilobjekts einer gegebenen algebraischen Struktur ist, dass man Teilmengen betrachtet, auf die man die Operationen so einschränken kann, dass man eine Struktur der gleichen Art erhält. Im Fall von Quotientenobjekten einer algebraischen Struktur sucht man Äquivalenzrelationen auf der Menge, auf der die Struktur

definiert ist, sodass die Operationen wohldefinierte Operationen auf der Menge aller Äquivalenzklassen liefern, die dann eine Struktur gleicher Art definieren.

Andererseits benötige man Konstruktionen wie Produkte oder die direkte Summe von Vektorräumen. Diese Konstruktionen können sowohl dazu dienen, Strukturen zu analysieren als auch dazu dienen komplizierte Objekte aus einfachen Bausteinen aufzubauen. Im Idealfall erhält man Klassifikationsresultate, kann also zeigen, dass alle Instanzen einer bestimmten Struktur durch solche Konstruktionen erhalten werden können.