Vorkurs
Formale Methoden der Informatik

Bettina Esser und Michael Kaibel

2. September bis 13. September 2024, Universität Bonn

Informatik V

Ein Hauch von Gruppentheorie

Motivation: Symmetrien

Um Gruppen zu verstehen, muss man erst Symmetrien verstehen. Sie sind das zugrundeliegende Konzept, später wird die Anschauung wegabstrahiert und nur noch „trockene Algebra" betrieben.

Motivation: Symmetrien

Um Gruppen zu verstehen, muss man erst Symmetrien verstehen. Sie sind das zugrundeliegende Konzept, später wird die Anschauung wegabstrahiert und nur noch „trockene Algebra" betrieben.

- Eine Symmetrie ist eine Aktion, die man auf ein Objekt anwenden kann, ohne dass sich die grundlegende Struktur des Objektes groß ändert.

Motivation: Symmetrien

Um Gruppen zu verstehen, muss man erst Symmetrien verstehen. Sie sind das zugrundeliegende Konzept, später wird die Anschauung wegabstrahiert und nur noch „trockene Algebra" betrieben.

- Eine Symmetrie ist eine Aktion, die man auf ein Objekt anwenden kann, ohne dass sich die grundlegende Struktur des Objektes groß ändert.
- Ein Quadrat kann man z.B. entlang einer der Diagonalen spiegeln und hat von außen betrachtet immernoch das gleiche Quadrat. Zwei Eckpunkte bleiben, wo sie waren, die zwei anderen tauschen die Position.

Motivation: Symmetrien

Um Gruppen zu verstehen, muss man erst Symmetrien verstehen. Sie sind das zugrundeliegende Konzept, später wird die Anschauung wegabstrahiert und nur noch „trockene Algebra" betrieben.

- Eine Symmetrie ist eine Aktion, die man auf ein Objekt anwenden kann, ohne dass sich die grundlegende Struktur des Objektes groß ändert.
- Ein Quadrat kann man z.B. entlang einer der Diagonalen spiegeln und hat von außen betrachtet immernoch das gleiche Quadrat. Zwei Eckpunkte bleiben, wo sie waren, die zwei anderen tauschen die Position.
- Ein Quadrat könnte man auch um 90 Grad drehen, dadurch würde jeder Eckpunkt „eins weiter wandern".

Motivation: Symmetrien

Um Gruppen zu verstehen, muss man erst Symmetrien verstehen. Sie sind das zugrundeliegende Konzept, später wird die Anschauung wegabstrahiert und nur noch „trockene Algebra" betrieben.

- Eine Symmetrie ist eine Aktion, die man auf ein Objekt anwenden kann, ohne dass sich die grundlegende Struktur des Objektes groß ändert.
- Ein Quadrat kann man z.B. entlang einer der Diagonalen spiegeln und hat von außen betrachtet immernoch das gleiche Quadrat. Zwei Eckpunkte bleiben, wo sie waren, die zwei anderen tauschen die Position.
- Ein Quadrat könnte man auch um 90 Grad drehen, dadurch würde jeder Eckpunkt „eins weiter wandern".
- Symmetrieaktionen kann man augenscheinlich hintereinander ausführen und erhält immernoch eine Symmetrieaktion.

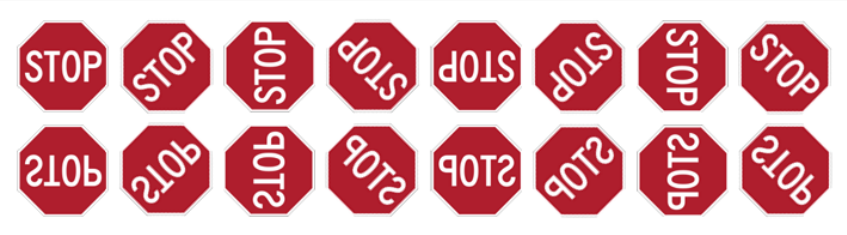
Motivation: Symmetrien

Um Gruppen zu verstehen, muss man erst Symmetrien verstehen. Sie sind das zugrundeliegende Konzept, später wird die Anschauung wegabstrahiert und nur noch „trockene Algebra" betrieben.

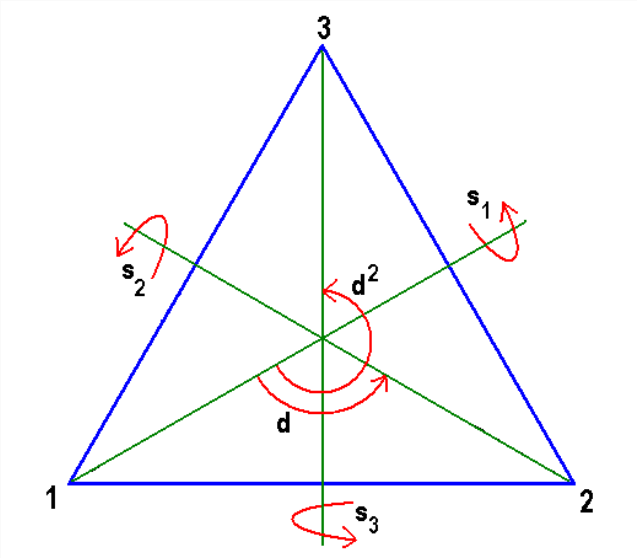
- Eine Symmetrie ist eine Aktion, die man auf ein Objekt anwenden kann, ohne dass sich die grundlegende Struktur des Objektes groß ändert.
- Ein Quadrat kann man z.B. entlang einer der Diagonalen spiegeln und hat von außen betrachtet immernoch das gleiche Quadrat. Zwei Eckpunkte bleiben, wo sie waren, die zwei anderen tauschen die Position.
- Ein Quadrat könnte man auch um 90 Grad drehen, dadurch würde jeder Eckpunkt „eins weiter wandern".
- Symmetrieaktionen kann man augenscheinlich hintereinander ausführen und erhält immernoch eine Symmetrieaktion.
- Nichtstun ist auch eine Symmetrieaktion!

Beispiel I

Beispiel II


STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP
STOP

Beispiel III



Warum machen wir so abstrakte Sachen wie Gruppen

- Wir studieren Strukturen sehr allgemein um möglichst weitreichede Aussagen treffen zu können

Warum machen wir so abstrakte Sachen wie Gruppen

- Wir studieren Strukturen sehr allgemein um möglichst weitreichede Aussagen treffen zu können
- Wenn wir viele Aussagen für Gruppen im allgemeinen beweisen können, reicht es zu zeigen, dass etwas eine Gruppe ist, um all diese Theoreme nutzen zu können

Warum machen wir so abstrakte Sachen wie Gruppen

- Wir studieren Strukturen sehr allgemein um möglichst weitreichede Aussagen treffen zu können
- Wenn wir viele Aussagen für Gruppen im allgemeinen beweisen können, reicht es zu zeigen, dass etwas eine Gruppe ist, um all diese Theoreme nutzen zu können
- Gruppentheorie hilft auch unserem Verständnis komplexerer algebraischer Strukturen

Warum machen wir so abstrakte Sachen wie Gruppen

- Wir studieren Strukturen sehr allgemein um möglichst weitreichede Aussagen treffen zu können
- Wenn wir viele Aussagen für Gruppen im allgemeinen beweisen können, reicht es zu zeigen, dass etwas eine Gruppe ist, um all diese Theoreme nutzen zu können
- Gruppentheorie hilft auch unserem Verständnis komplexerer algebraischer Strukturen
  - Insbesondere Vektorräume und Matritzen haben sehr viele Anwendungen in der Informatik

Gruppen: Definition

Definition

Sei $(G, \circ)$ ein Tupel, wobei G eine Menge ist und $\circ : G \times G \to G$ eine Abbildung. Wir nennen $(G, \circ)$ oder bei klarem Kontext einfach nur G ein **Magma**. Anstelle $\circ(g, g')$ schreiben wir $g \circ g'$. Man nennt $\circ$ eine auf G **abgeschlossene Verknüpfung**, da die Verknüpfung $g \circ g'$ für $g, g' \in G$ wieder in G liegt.

Gruppen: Definition

Definition

Sei $(G, \circ)$ ein Tupel, wobei G eine Menge ist und $\circ : G \times G \to G$ eine Abbildung. Wir nennen $(G, \circ)$ oder bei klarem Kontext einfach nur G ein **Magma**. Anstelle $\circ(g, g')$ schreiben wir $g \circ g'$. Man nennt $\circ$ eine auf G **abgeschlossene Verknüpfung**, da die Verknüpfung $g \circ g'$ für $g, g' \in G$ wieder in G liegt.

Eine Gruppe ist ein Magma $(G, \circ)$, sodass folgende drei Gesetze gelten:

Gruppen: Definition

Definition

Sei $(G, \circ)$ ein Tupel, wobei G eine Menge ist und $\circ : G \times G \to G$ eine Abbildung. Wir nennen $(G, \circ)$ oder bei klarem Kontext einfach nur G ein **Magma**. Anstelle $\circ(g, g')$ schreiben wir $g \circ g'$. Man nennt $\circ$ eine auf G **abgeschlossene Verknüpfung**, da die Verknüpfung $g \circ g'$ für $g, g' \in G$ wieder in G liegt.

Eine Gruppe ist ein Magma $(G, \circ)$, sodass folgende drei Gesetze gelten:

1. Assoziativgesetz: $\forall g, g', g'' \in G : g \circ (g' \circ g'') = (g \circ g') \circ g''$.

Gruppen: Definition

Definition

Sei $(G, \circ)$ ein Tupel, wobei G eine Menge ist und $\circ : G \times G \to G$ eine Abbildung. Wir nennen $(G, \circ)$ oder bei klarem Kontext einfach nur G ein **Magma**. Anstelle $\circ(g, g')$ schreiben wir $g \circ g'$. Man nennt $\circ$ eine auf G **abgeschlossene Verknüpfung**, da die Verknüpfung $g \circ g'$ für $g, g' \in G$ wieder in G liegt.

Eine Gruppe ist ein Magma $(G, \circ)$, sodass folgende drei Gesetze gelten:

1. Assoziativgesetz: $\forall g, g', g'' \in G : g \circ (g' \circ g'') = (g \circ g') \circ g''$.
2. Existenz eines neutralen Elementes: $\exists e \in G \forall g \in G : e \circ g = g \circ e = g$.

Gruppen: Definition

Definition

Sei $(G, \circ)$ ein Tupel, wobei G eine Menge ist und $\circ : G \times G \to G$ eine Abbildung. Wir nennen $(G, \circ)$ oder bei klarem Kontext einfach nur G ein **Magma**. Anstelle $\circ(g, g')$ schreiben wir $g \circ g'$. Man nennt $\circ$ eine auf G **abgeschlossene Verknüpfung**, da die Verknüpfung $g \circ g'$ für $g, g' \in G$ wieder in G liegt.

Eine Gruppe ist ein Magma $(G, \circ)$, sodass folgende drei Gesetze gelten:

1. Assoziativgesetz: $\forall g, g', g'' \in G : g \circ (g' \circ g'') = (g \circ g') \circ g''$.
2. Existenz eines neutralen Elementes: $\exists e \in G \forall g \in G : e \circ g = g \circ e = g$.
3. Existenz von Inversen: $\forall x \in G \exists y \in G : x \circ y = y \circ x = e$. Man schreibt für das (eindeutige!) Inverse y von g auch g^{-1}.

Gruppen: Definition

Definition

Sei $(G, \circ)$ ein Tupel, wobei G eine Menge ist und $\circ : G \times G \to G$ eine Abbildung. Wir nennen $(G, \circ)$ oder bei klarem Kontext einfach nur G ein **Magma**. Anstelle $\circ(g, g')$ schreiben wir $g \circ g'$. Man nennt $\circ$ eine auf G **abgeschlossene Verknüpfung**, da die Verknüpfung $g \circ g'$ für $g, g' \in G$ wieder in G liegt.

Eine Gruppe ist ein Magma $(G, \circ)$, sodass folgende drei Gesetze gelten:

1. Assoziativgesetz: $\forall g, g', g'' \in G : g \circ (g' \circ g'') = (g \circ g') \circ g''$.
2. Existenz eines neutralen Elementes: $\exists e \in G \forall g \in G : e \circ g = g \circ e = g$.
3. Existenz von Inversen: $\forall x \in G \exists y \in G : x \circ y = y \circ x = e$. Man schreibt für das (eindeutige!) Inverse y von g auch g^{-1}.

Gilt dazu noch das Kommutativgesetz für $\circ$, so nennen wir G kommutativ oder abelsch.

Definition verstehen

Einige Überlegungen sind vielleicht wichtig:

- Gibt es nur ein neutrales Element?

Definition verstehen

Einige Überlegungen sind vielleicht wichtig:

- Gibt es nur ein neutrales Element?
- Gibt es nur ein Inverses zu jedem $g \in G$?

Definition verstehen

Einige Überlegungen sind vielleicht wichtig:

- Gibt es nur ein neutrales Element?
- Gibt es nur ein Inverses zu jedem $g \in G$?
- Ist es wichtig, dass neutrale Elemente und Inverse beidseitig sind?

Definition verstehen

Einige Überlegungen sind vielleicht wichtig:

- Gibt es nur ein neutrales Element?
- Gibt es nur ein Inverses zu jedem $g \in G$?
- Ist es wichtig, dass neutrale Elemente und Inverse beidseitig sind?
- Wieso braucht man das Assoziativgesetz?

Definition verstehen

Einige Überlegungen sind vielleicht wichtig:

- Gibt es nur ein neutrales Element?
- Gibt es nur ein Inverses zu jedem $g \in G$?
- Ist es wichtig, dass neutrale Elemente und Inverse beidseitig sind?
- Wieso braucht man das Assoziativgesetz?
- Was ist eine Verknüpfungstafel?

Definition verstehen

Einige Überlegungen sind vielleicht wichtig:

- Gibt es nur ein neutrales Element?
- Gibt es nur ein Inverses zu jedem $g \in G$?
- Ist es wichtig, dass neutrale Elemente und Inverse beidseitig sind?
- Wieso braucht man das Assoziativgesetz?
- Was ist eine Verknüpfungstafel?
- Was ist eine Untergruppe?

Beispiele für Gruppen (algebraischer Blickwinkel)

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind abelsche Gruppen.

Beispiele für Gruppen (algebraischer Blickwinkel)

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind abelsche Gruppen.
- $(\mathbb{R}, \cdot)$ ist keine Gruppe, aber $(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.

Beispiele für Gruppen (algebraischer Blickwinkel)

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind abelsche Gruppen.
- $(\mathbb{R}, \cdot)$ ist keine Gruppe, aber $(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.
- Die zyklischen Gruppen $C_n = \{0, \ldots, n-1\}$ (mit Verknüpfung Addition mod n) sind zentrale Gruppen in allen Bereichen.

Beispiele für Gruppen (algebraischer Blickwinkel)

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind abelsche Gruppen.
- $(\mathbb{R}, \cdot)$ ist keine Gruppe, aber $(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.
- Die zyklischen Gruppen $C_n = \{0, \ldots, n-1\}$ (mit Verknüpfung Addition mod n) sind zentrale Gruppen in allen Bereichen.
- Die triviale Gruppe ist $G = \{e\}$ (mit der Verknüpfung $e \circ e = e$).

Beispiele für Gruppen (algebraischer Blickwinkel)

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind abelsche Gruppen.
- $(\mathbb{R}, \cdot)$ ist keine Gruppe, aber $(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.
- Die zyklischen Gruppen $C_n = \{0, \ldots, n-1\}$ (mit Verknüpfung Addition mod n) sind zentrale Gruppen in allen Bereichen.
- Die triviale Gruppe ist $G = \{e\}$ (mit der Verknüpfung $e \circ e = e$).
- $GL_n(\mathbb{R})$, die Menge aller $n \times n$–Matrizen mit reellen Koeffizienten und Determinante ungleich 0 ist eine Gruppe (mit Matrizenmultiplikation als Verknüpfung).

Beispiele für Gruppen (algebraischer Blickwinkel)

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind abelsche Gruppen.
- $(\mathbb{R}, \cdot)$ ist keine Gruppe, aber $(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.
- Die zyklischen Gruppen $C_n = \{0, \ldots, n-1\}$ (mit Verknüpfung Addition mod n) sind zentrale Gruppen in allen Bereichen.
- Die triviale Gruppe ist $G = \{e\}$ (mit der Verknüpfung $e \circ e = e$).
- $GL_n(\mathbb{R})$, die Menge aller $n \times n$–Matrizen mit reellen Koeffizienten und Determinante ungleich 0 ist eine Gruppe (mit Matrizenmultiplikation als Verknüpfung).
- Die Gruppe $SO(3)$ spielt in der theoretischen Physik eine große Rolle. Sie ist die Gruppe aller Rotationen des Dreidimensionalen Raums um den Ursprung, die die Rechte-Hand-Regel erhalten.

Beispiele für Gruppen (algebraischer Blickwinkel)

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind abelsche Gruppen.
- $(\mathbb{R}, \cdot)$ ist keine Gruppe, aber $(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.
- Die zyklischen Gruppen $C_n = \{0, \ldots, n-1\}$ (mit Verknüpfung Addition mod n) sind zentrale Gruppen in allen Bereichen.
- Die triviale Gruppe ist $G = \{e\}$ (mit der Verknüpfung $e \circ e = e$).
- $GL_n(\mathbb{R})$, die Menge aller $n \times n$–Matrizen mit reellen Koeffizienten und Determinante ungleich 0 ist eine Gruppe (mit Matrizenmultiplikation als Verknüpfung).
- Die Gruppe $SO(3)$ spielt in der theoretischen Physik eine große Rolle. Sie ist die Gruppe aller Rotationen des Dreidimensionalen Raums um den Ursprung, die die Rechte-Hand-Regel erhalten.
- $\mathrm{Aut}(\hat{\mathbb{C}}) = \{f \colon \mathbb{C} \to \mathbb{C} | f(z) = \frac{az+b}{cz+d}, ad - bc \neq 0\}$ (mit Funktionsverkettung als Verknüpfung) nennt sich die Möbiusgruppe und ist auch in der Physik von zentraler Rolle.

Beispiele für Gruppen (algebraischer Blickwinkel)

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind abelsche Gruppen.
- $(\mathbb{R}, \cdot)$ ist keine Gruppe, aber $(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.
- Die zyklischen Gruppen $C_n = \{0, \ldots, n-1\}$ (mit Verknüpfung Addition mod n) sind zentrale Gruppen in allen Bereichen.
- Die triviale Gruppe ist $G = \{e\}$ (mit der Verknüpfung $e \circ e = e$).
- $GL_n(\mathbb{R})$, die Menge aller $n \times n$–Matrizen mit reellen Koeffizienten und Determinante ungleich 0 ist eine Gruppe (mit Matrizenmultiplikation als Verknüpfung).
- Die Gruppe $SO(3)$ spielt in der theoretischen Physik eine große Rolle. Sie ist die Gruppe aller Rotationen des Dreidimensionalen Raums um den Ursprung, die die Rechte-Hand-Regel erhalten.
- $\mathrm{Aut}(\hat{\mathbb{C}}) = \{f \colon \mathbb{C} \to \mathbb{C} | f(z) = \frac{az+b}{cz+d}, ad - bc \neq 0\}$ (mit Funktionsverkettung als Verknüpfung) nennt sich die Möbiusgruppe und ist auch in der Physik von zentraler Rolle.

Beispiele für Gruppen (symmetrischer Blickwinkel)

- Karthesisches Produkt $G \times H$ von zwei Gruppen G, H ist wieder eine Gruppe. Es werden intuitiv zwei unabhängige Symmetrieaktionen unabhängig voneinander ausgeführt.

Beispiele für Gruppen (symmetrischer Blickwinkel)

- Karthesisches Produkt $G \times H$ von zwei Gruppen G, H ist wieder eine Gruppe. Es werden intuitiv zwei unabhängige Symmetrieaktionen unabhängig voneinander ausgeführt.
- Kleinsche Vierergruppe: Gruppe der Symmetrien eines Rechtecks, das kein Quadrat ist.

Beispiele für Gruppen (symmetrischer Blickwinkel)

- Karthesisches Produkt $G \times H$ von zwei Gruppen G, H ist wieder eine Gruppe. Es werden intuitiv zwei unabhängige Symmetrieaktionen unabhängig voneinander ausgeführt.
- Kleinsche Vierergruppe: Gruppe der Symmetrien eines Rechtecks, das kein Quadrat ist.
- Die Diedergruppen D_{2n}: Die Rotationen und Spiegelungen eines regelmäßigen n-Ecks.

Beispiele für Gruppen (symmetrischer Blickwinkel)

- Karthesisches Produkt $G \times H$ von zwei Gruppen G, H ist wieder eine Gruppe. Es werden intuitiv zwei unabhängige Symmetrieaktionen unabhängig voneinander ausgeführt.
- Kleinsche Vierergruppe: Gruppe der Symmetrien eines Rechtecks, das kein Quadrat ist.
- Die Diedergruppen D_{2n}: Die Rotationen und Spiegelungen eines regelmäßigen n-Ecks.
- Die symmetrischen Gruppen S_n: Alle Permutationen der Menge $\{1, \ldots, n\}$, Hintereinanderausführung als Verknüpfung.

Beispiele für Gruppen (symmetrischer Blickwinkel)

- Karthesisches Produkt $G \times H$ von zwei Gruppen G, H ist wieder eine Gruppe. Es werden intuitiv zwei unabhängige Symmetrieaktionen unabhängig voneinander ausgeführt.
- Kleinsche Vierergruppe: Gruppe der Symmetrien eines Rechtecks, das kein Quadrat ist.
- Die Diedergruppen D_{2n}: Die Rotationen und Spiegelungen eines regelmäßigen n-Ecks.
- Die symmetrischen Gruppen S_n: Alle Permutationen der Menge $\{1, \ldots, n\}$, Hintereinanderausführung als Verknüpfung.
- Auf gewisse Weise ist jede endliche Gruppe „Untergruppe" einer symmetrischen Gruppe.

Homomorphismen

Wenn man Gruppen studiert, muss man sich auch mit Abbildungen befassen. Wir erlauben allerdings nicht alle, sondern nur solche, die strukturerhaltend sind.

Homomorphismen

Wenn man Gruppen studiert, muss man sich auch mit Abbildungen befassen. Wir erlauben allerdings nicht alle, sondern nur solche, die strukturerhaltend sind.

Definition

Seien $(G, \circ_G), (H, \circ_H)$ Gruppen. Wir nennen eine Funktion $f : G \to H$ **strukturerhaltend** oder **Homomorphismus**, wenn für alle $g, g' \in G : f(g \circ_G g') = f(g) \circ_H f(g')$.

Homomorphismen

Wenn man Gruppen studiert, muss man sich auch mit Abbildungen befassen. Wir erlauben allerdings nicht alle, sondern nur solche, die strukturerhaltend sind.

Definition

Seien $(G, \circ_G), (H, \circ_H)$ Gruppen. Wir nennen eine Funktion $f : G \to H$ **strukturerhaltend** oder **Homomorphismus**, wenn für alle $g, g' \in G : f(g \circ_G g') = f(g) \circ_H f(g')$.

- Ist f injektiv, nennen wir f Einbettung oder Monomorphismus.

Homomorphismen

Wenn man Gruppen studiert, muss man sich auch mit Abbildungen befassen. Wir erlauben allerdings nicht alle, sondern nur solche, die strukturerhaltend sind.

Definition

Seien $(G, \circ_G), (H, \circ_H)$ Gruppen. Wir nennen eine Funktion $f : G \to H$ **strukturerhaltend** oder **Homomorphismus**, wenn für alle $g, g' \in G : f(g \circ_G g') = f(g) \circ_H f(g')$.

- Ist f injektiv, nennen wir f Einbettung oder Monomorphismus.
- Ist f surjektiv, nennen wir f Quotient oder Epimorphismus.

Homomorphismen

Wenn man Gruppen studiert, muss man sich auch mit Abbildungen befassen. Wir erlauben allerdings nicht alle, sondern nur solche, die strukturerhaltend sind.

Definition

Seien $(G, \circ_G), (H, \circ_H)$ Gruppen. Wir nennen eine Funktion $f : G \to H$ **strukturerhaltend** oder **Homomorphismus**, wenn für alle $g, g' \in G : f(g \circ_G g') = f(g) \circ_H f(g')$.

- Ist f injektiv, nennen wir f Einbettung oder Monomorphismus.
- Ist f surjektiv, nennen wir f Quotient oder Epimorphismus.
- Ist f bijektiv, nennen wir f Isomorphismus, wir nennen G und H isomorph und schreiben $G \cong H$.

Homomorphismen

Wenn man Gruppen studiert, muss man sich auch mit Abbildungen befassen. Wir erlauben allerdings nicht alle, sondern nur solche, die strukturerhaltend sind.

Definition

Seien $(G, \circ_G), (H, \circ_H)$ Gruppen. Wir nennen eine Funktion $f : G \to H$ **strukturerhaltend** oder **Homomorphismus**, wenn für alle $g, g' \in G : f(g \circ_G g') = f(g) \circ_H f(g')$.

- Ist f injektiv, nennen wir f Einbettung oder Monomorphismus.
- Ist f surjektiv, nennen wir f Quotient oder Epimorphismus.
- Ist f bijektiv, nennen wir f Isomorphismus, wir nennen G und H isomorph und schreiben $G \cong H$.

Das allerwichtigste dieser drei Zusatzbegriffe ist der **Isomorphismus**. Isomorphie ist eine Äquivalenzrelation, und besagt quasi, dass zwei Gruppen bis auf Umbenennung der Elemente (von Isomorphismus vorgegeben) die absolut gleiche Struktur haben, konzeptuell also „die gleiche Gruppe sind".

Untergruppen

Definition (Untergruppe)

Seien $G = (G, \circ)$ und $H = (H, \circ)$ Gruppen mit $H \subseteq G$, dann nennen wir H eine Untergruppe von G.

Untergruppen

Definition (Untergruppe)

Seien $G = (G, \circ)$ und $H = (H, \circ)$ Gruppen mit $H \subseteq G$, dann nennen wir H eine Untergruppe von G.

Beide verwenden dieselbe Verknüpfung, wobei wir bei der Verknüpfung für H die Eingabe- und Ausgabemenge auf H einschrenken müssen.

Untergruppen

Definition (Untergruppe)

Seien $G = (G, \circ)$ und $H = (H, \circ)$ Gruppen mit $H \subseteq G$, dann nennen wir H eine Untergruppe von G.
Beide verwenden dieselbe Verknüpfung, wobei wir bei der Verknüpfung für H die Eingabe- und Ausgabemenge auf H einschrenken müssen.

- Für jede Gruppe G sind G und die triviale Gruppe $(\{e\}, \circ)$ Untergruppen

Untergruppen

Definition (Untergruppe)

Seien $G = (G, \circ)$ und $H = (H, \circ)$ Gruppen mit $H \subseteq G$, dann nennen wir H eine Untergruppe von G.
Beide verwenden dieselbe Verknüpfung, wobei wir bei der Verknüpfung für H die Eingabe- und Ausgabemenge auf H einschrenken müssen.

- Für jede Gruppe G sind G und die triviale Gruppe $(\{e\}, \circ)$ Untergruppen
  - Wir nennen diese die trivialen Untergruppen

Untergruppen

Definition (Untergruppe)

Seien $G = (G, \circ)$ und $H = (H, \circ)$ Gruppen mit $H \subseteq G$, dann nennen wir H eine Untergruppe von G.
Beide verwenden dieselbe Verknüpfung, wobei wir bei der Verknüpfung für H die Eingabe- und Ausgabemenge auf H einschrenken müssen.

- Für jede Gruppe G sind G und die triviale Gruppe $(\{e\}, \circ)$ Untergruppen
  - Wir nennen diese die trivialen Untergruppen
- Das Studieren von Untergruppen hat große Bedeutung für Algebra

Untergruppen

Definition (Untergruppe)

Seien $G = (G, \circ)$ und $H = (H, \circ)$ Gruppen mit $H \subseteq G$, dann nennen wir H eine Untergruppe von G.
Beide verwenden dieselbe Verknüpfung, wobei wir bei der Verknüpfung für H die Eingabe- und Ausgabemenge auf H einschrenken müssen.

- Für jede Gruppe G sind G und die triviale Gruppe $(\{e\}, \circ)$ Untergruppen
  - Wir nennen diese die trivialen Untergruppen
- Das Studieren von Untergruppen hat große Bedeutung für Algebra
- In Informatik treten sie seltener auf, haben aber etwas Bedeutung in der (leicht esoterischen) Studie von Graphstrukturen

Permutationsgruppen im Detail

- Die Permutationsgruppe $(S_n, \circ)$ ist die Gruppe gegeben durch $S_n = \{f : A \to A \mid f \text{ ist bijektiv}\}$ wobei A eine Menge mit n Elementen ist.

Permutationsgruppen im Detail

- Die Permutationsgruppe $(S_n, \circ)$ ist die Gruppe gegeben durch $S_n = \{f : A \to A \mid f \text{ ist bijektiv}\}$ wobei A eine Menge mit n Elementen ist.
  - Wir nennen diese Permutationen

Permutationsgruppen im Detail

- Die Permutationsgruppe $(S_n, \circ)$ ist die Gruppe gegeben durch $S_n = \{f : A \to A \mid f \text{ ist bijektiv}\}$ wobei A eine Menge mit n Elementen ist.
  - Wir nennen diese Permutationen
- Ihre Verknüpfung ist $\circ$ die Verknüpfung von Funktionen

Permutationsgruppen im Detail

- Die Permutationsgruppe $(S_n, \circ)$ ist die Gruppe gegeben durch $S_n = \{f : A \to A \mid f \text{ ist bijektiv}\}$ wobei A eine Menge mit n Elementen ist.
  - Wir nennen diese Permutationen
- Ihre Verknüpfung ist $\circ$ die Verknüpfung von Funktionen
- Das neutrale Element ist die Identitätsfunktion Id mit $Id(x) = x$

Permutationsgruppen im Detail

- Die Permutationsgruppe $(S_n, \circ)$ ist die Gruppe gegeben durch $S_n = \{f : A \to A \mid f \text{ ist bijektiv}\}$ wobei A eine Menge mit n Elementen ist.
  - Wir nennen diese Permutationen
- Ihre Verknüpfung ist $\circ$ die Verknüpfung von Funktionen
- Das neutrale Element ist die Identitätsfunktion Id mit $Id(x) = x$
- Das inverse Element einer Permutation f ist ihre inverse Funktion

Man kann den Permutationsgruppen nicht entkommen

Theorem

Sein $G = (G, *)$ eine endliche Gruppe, d.h. $|G| = n$ für ein $n \in \mathbb{N}$. Dann ist G isomorph zu einer Untergruppe der Permutationsgruppe S_n.

Man kann den Permutationsgruppen nicht entkommen

Theorem

Sein $G = (G, *)$ eine endliche Gruppe, d.h. $|G| = n$ für ein $n \in \mathbb{N}$. Dann ist G isomorph zu einer Untergruppe der Permutationsgruppe S_n.

Beweis: Wir wollen jedes Element $g \in G$ eins zu eins mit einer Permutation assoziieren. Am leichtesten ist es, g mit einer Permutation auf G zu assoziieren. Sei $\pi(G)$ die Menge aller bijektiven Funktionen von G auf G.
Wir definieren dazu die Funktion $f\colon G \to \pi(G)$ mit $f(g) = p_g$ wobei wir p_g definieren als

$$p_g(x) = g * x$$

Man kann den Permutationsgruppen nicht entkommen

Theorem

Sein $G = (G, *)$ eine endliche Gruppe, d.h. $|G| = n$ für ein $n \in \mathbb{N}$. Dann ist G isomorph zu einer Untergruppe der Permutationsgruppe S_n.

Beweis: Wir wollen jedes Element $g \in G$ eins zu eins mit einer Permutation assoziieren. Am leichtesten ist es, g mit einer Permutation auf G zu assoziieren. Sei $\pi(G)$ die Menge aller bijektiven Funktionen von G auf G.
Wir definieren dazu die Funktion $f\colon G \to \pi(G)$ mit $f(g) = p_g$ wobei wir p_g definieren als

$$p_g(x) = g * x$$

$\pi(G)$ alleine ist natürlich keine Gruppe, da wir noch keine Verknüpfung definiert haben. Wir wählen als Verknüpfung die Verknüpfung $\circ$ von Funktionen. Damit bildet $(\pi(G), \circ)$ eine Permutationsgruppe auf n Elementen.

Man kann den Permutationsgruppen nicht entkommen

Theorem

Sein $G = (G, *)$ eine endliche Gruppe, d.h. $|G| = n$ für ein $n \in \mathbb{N}$. Dann ist G isomorph zu einer Untergruppe der Permutationsgruppe S_n.

Beweis: Wir wollen jedes Element $g \in G$ eins zu eins mit einer Permutation assoziieren. Am leichtesten ist es, g mit einer Permutation auf G zu assoziieren. Sei $\pi(G)$ die Menge aller bijektiven Funktionen von G auf G.
Wir definieren dazu die Funktion $f\colon G \to \pi(G)$ mit $f(g) = p_g$ wobei wir p_g definieren als

$$p_g(x) = g * x$$

$\pi(G)$ alleine ist natürlich keine Gruppe, da wir noch keine Verknüpfung definiert haben. Wir wählen als Verknüpfung die Verknüpfung $\circ$ von Funktionen. Damit bildet $(\pi(G), \circ)$ eine Permutationsgruppe auf n Elementen. Wir schreiben im Beweis weiterhin $(\pi(G), \circ)$ um den Bezug auf G zu verdeutlichen.

Beweis, dass f in $\pi(G)$ abbildet

Um zu beweisen, dass f in $\pi(G)$ abbildet, müssen wir zeigen, dass für jedes $g \in G$ die Funktion p_g auf G bijektiv ist.

Beweis, dass f in $\pi(G)$ abbildet

Um zu beweisen, dass f in $\pi(G)$ abbildet, müssen wir zeigen, dass für jedes $g \in G$ die Funktion p_g auf G bijektiv ist.

Injektivität: Seien $x, x' \in G$ beliebig mit $p_g(x) = p_g(x')$. Dann gilt

$$
\begin{aligned}
& p_g(x) = p_g(x') && \text{Definition von } p_g \\
\Leftrightarrow \quad & g * x = g * x' && \text{von links } g^{-1} \text{ anknüpfen} \\
\Leftrightarrow \quad & g^{-1} * g * x = g{-}1 * g * x' && \text{Definition von Inversen} \\
\Leftrightarrow \quad & x = e * x = e * x' = x'
\end{aligned}
$$

Beweis, dass f in $\pi(G)$ abbildet

Um zu beweisen, dass f in $\pi(G)$ abbildet, müssen wir zeigen, dass für jedes $g \in G$ die Funktion p_g auf G bijektiv ist.

Injektivität: Seien $x, x' \in G$ beliebig mit $p_g(x) = p_g(x')$. Dann gilt

$$
\begin{aligned}
& p_g(x) = p_g(x') && \text{Definition von } p_g \\
\Leftrightarrow \quad & g * x = g * x' && \text{von links } g^{-1} \text{ anknüpfen} \\
\Leftrightarrow \quad & g^{-1} * g * x = g{-}1 * g * x' && \text{Definition von Inversen} \\
\Leftrightarrow \quad & x = e * x = e * x' = x'
\end{aligned}
$$

Surjektivität: Sei $y \in G$ beiliebig. Wir suchen $x \in G$ mit $p_g(x) = y$.

$$
\begin{aligned}
& p_g(x) = y && \text{Definition von } p_g \text{ einsetzen} \\
\Leftrightarrow \quad & g * x = y && \text{von links } g^{-1} \text{ anknüpfen} \\
\Leftrightarrow \quad & g^{-1} * g * x = g^{-1} * y && \text{Definition von Inversen} \\
\Leftrightarrow \quad & x = g^{-1} * y
\end{aligned}
$$

Beweis, dass f in $\pi(G)$ abbildet

Um zu beweisen, dass f in $\pi(G)$ abbildet, müssen wir zeigen, dass für jedes $g \in G$ die Funktion p_g auf G bijektiv ist.

Injektivität: Seien $x, x' \in G$ beliebig mit $p_g(x) = p_g(x')$. Dann gilt

$$
\begin{aligned}
& p_g(x) = p_g(x') && \text{Definition von } p_g \\
\Leftrightarrow \quad & g * x = g * x' && \text{von links } g^{-1} \text{ anknüpfen} \\
\Leftrightarrow \quad & g^{-1} * g * x = g{-}1 * g * x' && \text{Definition von Inversen} \\
\Leftrightarrow \quad & x = e * x = e * x' = x'
\end{aligned}
$$

Surjektivität: Sei $y \in G$ beiliebig. Wir suchen $x \in G$ mit $p_g(x) = y$.

$$
\begin{aligned}
& p_g(x) = y && \text{Definition von } p_g \text{ einsetzen} \\
\Leftrightarrow \quad & g * x = y && \text{von links } g^{-1} \text{ anknüpfen} \\
\Leftrightarrow \quad & g^{-1} * g * x = g^{-1} * y && \text{Definition von Inversen} \\
\Leftrightarrow \quad & x = g^{-1} * y
\end{aligned}
$$

f ist als Funktion also wohldefiniert.

Beweis, dass f ein Homomorphismus ist

Seien $g, h \in G$ beliebig. Wir zeigen als erstes das $p_g \circ p_h = p_{g \circ h}$.

Beweis, dass f ein Homomorphismus ist

Seien $g, h \in G$ beliebig. Wir zeigen als erstes das $p_g \circ p_h = p_{g \circ h}$. Um die Gleichheit der Funktionen zu zeigen, zeigen wir, dass sie für jede Eingabe dieselbe Ausgabe haben. Sei $x \in G$ beliebig

Beweis, dass f ein Homomorphismus ist

Seien $g, h \in G$ beliebig. Wir zeigen als erstes das $p_g \circ p_h = p_{g \circ h}$. Um die Gleichheit der Funktionen zu zeigen, zeigen wir, dass sie für jede Eingabe dieselbe Ausgabe haben. Sei $x \in G$ beliebig

$$\begin{aligned}(p_g \circ p_h)(x) &= p_g(p_h(x)) \\ &= p_g(h * x) \\ &= g * h * x \\ &= (g * h) * x \\ &= p_{(g*h)}(x)\end{aligned}$$

Beweis, dass f ein Homomorphismus ist

Seien $g, h \in G$ beliebig. Wir zeigen als erstes das $p_g \circ p_h = p_{g \circ h}$. Um die Gleichheit der Funktionen zu zeigen, zeigen wir, dass sie für jede Eingabe dieselbe Ausgabe haben. Sei $x \in G$ beliebig

$$\begin{aligned}(p_g \circ p_h)(x) &= p_g(p_h(x)) \\ &= p_g(h * x) \\ &= g * h * x \\ &= (g * h) * x \\ &= p_{(g*h)}(x)\end{aligned}$$

Damit können wir nun zeigen, dass f ein Homomprphismus ist.

$$\begin{aligned}f(g * h) &= p_{(g*h)} \\ &= p_g \circ p_h \\ &= f(g) \circ f(h)\end{aligned}$$

Beweis, dass f injektiv ist

Wir haben nun einen Homomprohismus von G in $\pi(G)$. Wir zeigen nun, dass dieser injektiv ist und schränken uns dann auf das Bild von f als die Gruppe ein, zu der G isomorph ist.

Beweis, dass f injektiv ist

Wir haben nun einen Homomprohismus von G in $\pi(G)$. Wir zeigen nun, dass dieser injektiv ist und schränken uns dann auf das Bild von f als die Gruppe ein, zu der G isomorph ist.

Injektivität von f Seien $x, x' \in G$ mit $f(x) = f(x')$

Beweis, dass f injektiv ist

Wir haben nun einen Homomprohismus von G in $\pi(G)$. Wir zeigen nun, dass dieser injektiv ist und schränken uns dann auf das Bild von f als die Gruppe ein, zu der G isomorph ist.

Injektivität von f Seien $x, x' \in G$ mit $f(x) = f(x')$

$$f(x) = f(x') \qquad \text{Definition von } f \text{ einsetzen}$$

$$\Leftrightarrow \quad p_x = p_{x'}$$

Beweis, dass f injektiv ist

Wir haben nun einen Homomprohismus von G in $\pi(G)$. Wir zeigen nun, dass dieser injektiv ist und schränken uns dann auf das Bild von f als die Gruppe ein, zu der G isomorph ist.

Injektivität von f Seien $x, x' \in G$ mit $f(x) = f(x')$

$$
\begin{aligned}
& f(x) = f(x') && \text{Definition von } f \text{ einsetzen} \\
\Leftrightarrow \quad & p_x = p_{x'} &&
\end{aligned}
$$

Sei $g \in G$ beliebig. Dann gilt

$$
\begin{aligned}
& p_x(g) = p_{x'}(g) && \text{Definition von } p_\cdot \text{ einsetzen} \\
\Leftrightarrow \quad & x * g = x' * g && \text{von rechts } g^{-1} \text{ anhängen} \\
\Leftrightarrow \quad & x * g * g^{-1} = x' * g * g^{-1} && \text{Definition von Inversen} \\
\Leftrightarrow \quad & x = x' &&
\end{aligned}
$$

Abschluss des Beweis

Wir schränken nun den Zielbereich von f auf die Menge $\alpha(G) = \{p_g \mid g \in G\}$ ein. Wir nennen diese eingeschränkte Funktion $f' : G \to \alpha(G)$ mit $f'(x) = f(x)$. Da f' injektiv ist und jedes p_g von g per Definition von f' getroffen wird ist f' bijektiv.

Abschluss des Beweis

Wir schränken nun den Zielbereich von f auf die Menge $\alpha(G) = \{p_g \mid g \in G\}$ ein. Wir nennen diese eingeschränkte Funktion $f' : G \to \alpha(G)$ mit $f'(x) = f(x)$. Da f' injektiv ist und jedes p_g von g per Definition von f' getroffen wird ist f' bijektiv.
f' ist wie Bewiesen auch ein Homomorphismus. Somit ist f' ein Isomorphismus.

Abschluss des Beweis

Wir schränken nun den Zielbereich von f auf die Menge $\alpha(G) = \{p_g \mid g \in G\}$ ein. Wir nennen diese eingeschränkte Funktion $f' : G \to \alpha(G)$ mit $f'(x) = f(x)$. Da f' injektiv ist und jedes p_g von g per Definition von f' getroffen wird ist f' bijektiv.
f' ist wie Bewiesen auch ein Homomorphismus. Somit ist f' ein Isomorphismus.
Es gilt also $G \cong (\alpha(G), \circ)$ und $(\alpha(G), \circ)$ ist ein Untergruppe der Permutationsgruppe $(\pi(G), \circ)$.

Abschluss des Beweis

Wir schränken nun den Zielbereich von f auf die Menge $\alpha(G) = \{p_g \mid g \in G\}$ ein. Wir nennen diese eingeschränkte Funktion $f' : G \to \alpha(G)$ mit $f'(x) = f(x)$. Da f' injektiv ist und jedes p_g von g per Definition von f' getroffen wird ist f' bijektiv.
f' ist wie Bewiesen auch ein Homomorphismus. Somit ist f' ein Isomorphismus.
Es gilt also $G \cong (\alpha(G), \circ)$ und $(\alpha(G), \circ)$ ist ein Untergruppe der Permutationsgruppe $(\pi(G), \circ)$.
Damit ist der Beweis abgeschlossen.

Und was bringt uns das?

- Permutationen können leicht im Computer gespeichert und verknüpft werden

Und was bringt uns das?

- Permutationen können leicht im Computer gespeichert und verknüpft werden

$\Rightarrow$ gibt uns einen allgemeinen Weg, um mit endlichen Gruppen im Computer zu rechnen

Und was bringt uns das?

- Permutationen können leicht im Computer gespeichert und verknüpft werden

$\Rightarrow$ gibt uns einen allgemeinen Weg, um mit endlichen Gruppen im Computer zu rechnen

- Leider recht ineffizient, wenn Gruppe groß ist

Und was bringt uns das?

- Permutationen können leicht im Computer gespeichert und verknüpft werden

$\Rightarrow$ gibt uns einen allgemeinen Weg, um mit endlichen Gruppen im Computer zu rechnen

- Leider recht ineffizient, wenn Gruppe groß ist
  - Has G n Elemente, so brauchen wir $\sim n^2$ Speicher um alle dazugehörigen Permutationen zu speichern

Und was bringt uns das?

- Permutationen können leicht im Computer gespeichert und verknüpft werden

$\Rightarrow$ gibt uns einen allgemeinen Weg, um mit endlichen Gruppen im Computer zu rechnen

- Leider recht ineffizient, wenn Gruppe groß ist
  - Has G n Elemente, so brauchen wir $\sim n^2$ Speicher um alle dazugehörigen Permutationen zu speichern
  - Viele Interessante Gruppen sind riesig grop und wir wollen sie nicht explizit speichern müssen

Und was bringt uns das?

- Permutationen können leicht im Computer gespeichert und verknüpft werden

$\Rightarrow$ gibt uns einen allgemeinen Weg, um mit endlichen Gruppen im Computer zu rechnen

- Leider recht ineffizient, wenn Gruppe groß ist
  - Has G n Elemente, so brauchen wir $\sim n^2$ Speicher um alle dazugehörigen Permutationen zu speichern
  - Viele Interessante Gruppen sind riesig grop und wir wollen sie nicht explizit speichern müssen
    - Permutationsgruppe auf nur 20 Elementen hat über 10^{18} Elemente

Und was bringt uns das?

- Permutationen können leicht im Computer gespeichert und verknüpft werden

$\Rightarrow$ gibt uns einen allgemeinen Weg, um mit endlichen Gruppen im Computer zu rechnen

- Leider recht ineffizient, wenn Gruppe groß ist
  - Has G n Elemente, so brauchen wir $\sim n^2$ Speicher um alle dazugehörigen Permutationen zu speichern
  - Viele Interessante Gruppen sind riesig grop und wir wollen sie nicht explizit speichern müssen
    - Permutationsgruppe auf nur 20 Elementen hat über 10^{18} Elemente
- Suche nach effizienteren Speicherungsmethoden ist offenes Forschungsgebiet