Isomorphiesatz

Thm: Ist $f: G \to H$ ein Homomorphismus, so ist $h: G/\ker(f) \to \text{im}(f)$, $x\ker(f) \mapsto f(x)$ ein Isomorphismus.

Bew: Wegen $f(xn) = f(x)$ für alle $n \in \ker(f)$ ist h wohldefiniert. Außerdem ist es auch surjektiv. Wegen $x\ker(f) \cdot y\ker(f) = (xy)\ker(f)$ ergibt sich $h(x)h(y) = h(xy)$, also ist h ein Homomorphismus. Ferner folgt aus $h(x\ker(f)) = f(x) = 1_H$, daß $x \in \ker(f)$ ist, also $x\ker(f) = \ker(f)$. Daher ist h auch injektiv. $\square$

Direktes Produkt

Seien G und H Gruppen. Dann in $G \times H$ koordinatenweise die Gruppengesetze definieren: $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$.
Einheitselement $(1_G, 1_H)$.

Damit wird $G \times H$ zur Gruppe.

Einbettung $G \to G \times H$, $x \mapsto (x, 1_H)$ von G ist Monomorphismus.
Projektion $G \times H \to G$, $(x, y) \mapsto x$ auf G ist Epimorphismus.

Kern der Projektion auf G ist Untergruppe $\{1_G\} \times H$ von $G \times H$.

Erzeuger

Seien $g_1, \dots, g_r \in G$. Die von den g_i erzeugte Untergruppe U von G besteht aus allen Elementen von G, die durch Verknüpfung und Inversion aus den g_i erhalten werden können.
Schreibweise $U = \langle g_1, \dots, g_r \rangle$.

Äquivalent kann U als der Schnitt aller Untergruppen von G definiert werden, welche die g_i enthalten.

Ist die von den g_i erzeugte Untergruppe gleich G, so heißen die g_i ein Erzeugendensystem von G.

Gilt $G = \langle g_1, \dots, g_r \rangle$ mit $r < \infty$, so heißt G endlich erzeugt.
Gilt $G = \langle g \rangle$, so heißt G zyklisch.

Homomorphismen sind bereits durch ihre Bildwerte auf Erzeugern definiert.

Ordnungen

Sei G eine Gruppe und $a \in G$. Dann heißt $\#\langle a \rangle$ die Ordnung von a.
Es gilt $a^{\#\langle a \rangle} = e$ und $\#\langle a \rangle \mid \#G$ nach Lagrange.

Thm (Fermat): Ist G endlich, so gilt $a^{\#G} = e$ für $a \in G$.
Bew: Es gilt $a^{\#G} = (a^{\#\langle a \rangle})^{\#G/\#\langle a \rangle} = e^{\#G/\#\langle a \rangle} = e$. $\square$

Thm: Ist $\#G$ prim, so ist G zyklisch.
Bew: Für $a \in G \backslash \{e\}$ folgt $\#\langle a \rangle > 1$ und $\#\langle a \rangle \mid \#G$, also $\#\langle a \rangle = \#G$.

Thm: Sind U, V Untergruppen von G mit teilerfremden Ordnungen, so gilt $U \cap V = \{e\}$.
Bew: $\#(U \cap V) \mid \gcd\{\#U, \#V\} = 1$. $\square$

Endlich erzeugte abelsche Gruppen

Sei G eine endlich erzeugte abelsche Gruppe.

Thm (Version 1): Es gibt ein eindeutig bestimmtes n und eindeutig bestimmte $c_i \in \mathbb{Z}^{\geq 0}$ mit $c_i \mid c_{i+1}$ für $1 \leq i \leq n-1$, so daß gilt:

$$G \cong \prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}.$$

Thm (Version 2): Es gibt Primzahlen p_i und Exponenten $e_i \geq 1$, so daß

$$G \cong \prod_{i=1}^{m} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

gilt. Die Paare (p_i, e_i) sind bis auf die Reihenfolge eindeutig bestimmt.

Bemerkung: Die Äquivalenz von Version 1 und 2 beruht auf dem chinesischen Restsatz.

Beispiel

$G = \mathbb{Z}$, $H = \mathbb{Z}/25\mathbb{Z}$, $f : \mathbb{Z} \to \mathbb{Z}/25\mathbb{Z}$ Restklassenhomomorphismus.
Isomorphiesatz $\mathbb{Z}/\ker(f) \cong \mathbb{Z}/25\mathbb{Z}$. Ist hier klar.

Ein direktes Produkt $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z} \times 5\mathbb{Z}$.
Erzeuger: $(1+3\mathbb{Z}, 0, 0), (0+3\mathbb{Z}, 1, 0), (0+3\mathbb{Z}, 0, 5)$.
Ist nicht zyklisch.

$\mathbb{Z}/5\mathbb{Z}$ hat Erzeuger $1+5\mathbb{Z}$. Ist zyklisch.

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ist auch zyklisch (!):
Erzeuger $(1+2\mathbb{Z}, 1+3\mathbb{Z})$.

Als Gruppen sind $\mathbb{Z}$ und $5\mathbb{Z}$ unter $x \mapsto 5x$ isomorph.

Für einen endlichen Körper $\mathbb{F}_q$ gilt $\mathbb{F}_q^{\times} \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

Exponentiation in Gruppen

Wie g^n effizient ausrechnen? Z.B. für $n = 27354268183173165356$.

Schreibe $n = \sum_{i=0}^{k} r_i 2^i$, $r_i \in \{0,1\}$. Dann $g^n = \prod_{r_i \neq 0} g^{2^i} = g^{(\cdots(r_k 2 + r_{k-1})2+\cdots)2+r_0}$.

Eingabe: g und $n \geq 0$.
Ausgabe: g^n.

1. Wenn $n = 0$ dann Ausgabe von 1.
2. Berechne rekursiv $b \leftarrow g^{n \text{ div } 2}$. Berechne $b \leftarrow b^2$.
3. Wenn n ungerade, dann $b \leftarrow bg$.
4. Ausgabe von b.

Aufwand $\leq 2\log_2(n) + 2$ Operationen (Quadrieren und Multiplizieren).
Von diesem Verfahren gibt es einige Varianten (mit vorberechneter Tabelle, links-rechts, rechts-links, sliding windows, ...).

Ringe

Sei R eine Menge, $+ : R \times R \to R$, $\cdot : R \times R \to R$. Es gebe $0, 1 \in R$ mit

- $(R,+)$ ist eine abelsche Gruppe mit neutralem Element 0.
- $(R\backslash\{0\}, \cdot)$ ist eine Halbgruppe mit neutralem Element 1.
- Distributivgesetz: $(a+b)c = ac+bc$ und $c(a+b) = ca+cb$ für alle $a, b, c \in R$.

Dann heißt R ein Ring mit Nullelement 0 und Einselement 1.

In einem Ring gilt:

1. $0x = x0 = 0$, denn wegen $0+0 = 0$ folgt $0x = (0+0)x = 0x+0x$ und damit $0x = 0$ durch Kürzen. Analog geht man für $x0$ vor.
2. $(-x)y = x(-y) = -(xy)$, denn $xy + (-x)y = (x-x)y = 0y = 0$, und analog mit $x(-y)$.
3. $(-x)(-y) = xy$, denn $(-x)(-y) = -(-x)y = -(-(xy)) = xy$.

Ringe, Körper

Ist $(R\backslash\{0\},\cdot)$ abelsch, so heißt R kommutativ. Wir betrachten ab jetzt nur kommutative Ringe.

Die Elemente von $R\backslash\{0\}$, die in $(R\backslash\{0\},\cdot)$ invertierbar sind, heißen Einheiten von R und bilden eine Gruppe, die mit $R^\times$ bezeichnet wird.

Sind $a,b \in R\backslash\{0\}$ und $c = ab$, so nennen wir a, b Teiler von c und schreiben $a \mid c$ und $b \mid c$. Gilt $c = 0$, so heißen a und b Nullteiler.

Ist R kommutativ und hat keine Nullteiler, so heißt R ein Integritätsring.

Ist R kommutativ und jedes Element ungleich Null invertierbar - also $R^\times = R\backslash\{0\}$, so heißt R ein Körper. Ein Körper ist auch ein Integritätsring (wegen $a = (ab)b^{-1} = 0$ für $ab = 0$).

Ringe, Körper

Beispiel $\mathbb{Z}$:
- $\mathbb{Z}^\times = \{-1,1\}$.
- Keine Nullteiler.

Beispiel $\mathbb{Z}/6\mathbb{Z}$:
- Nullteiler $(2+6\mathbb{Z})\cdot(3+6\mathbb{Z}) = 0+6\mathbb{Z}$.

Beispiel: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für p prim.

Homomorphismen

Seien R,S Ringe und $f : R \to S$. Gilt $f(a+b) = f(a)+f(b)$ und $f(ab) = f(a)f(b)$ und $f(1_R) = 1_S$ für alle $a,b \in R$, so heißt f ein Homomorphismus.

Epimorphismus = surjektiv.
Monomorphismus = injektiv.
Isomorphismus = bijektiv.
Endomorphismus = $S = R$.
Automorphismus = $S = R$ und bijektiv.

Es gilt wie eben:
- $f(0_R) = 0_S$, $f(1_R) = 1_S$.
- $f(-a) = -f(a)$, $f(a^{-1}) = f(a)^{-1}$, wenn a^{-1} existiert.

Unterringe, Ideale, Kern, Bild

Sei R ein Ring und $U \subseteq R$ ein Ring. Stimmen Addition und Multiplikation von U mit der R überein und gilt $1_U = 1_R$, so heißt U ein Unterring von R.

Sei $I \subseteq R$. Wir schreiben $RI = \sum_{a\in I} Ra = \{\sum_{i=0}^n r_i a_i \mid r_i \in R, a_i \in I, n \in \mathbb{Z}^{\geq 0}\}$. Gilt $RI = I$, so heißt I ein Ideal von R.

Für einen Homomorphismus $f : R \to S$ definieren wir $\ker(f) = f^{-1}(\{0_S\})$. Dies ist ein Ideal von R.
- Sind $a_i \in \ker(f)$ und $r_i \in R$, so gilt $f(\sum_i r_i a_i) = \sum_i f(r_i) f(a_i) = 0$, also $\sum_i r_i a_i \in \ker(f)$ und $R\ker(f) = \ker(f)$.

Ähnlich ist $\mathrm{im}(f) = f(R)$ ein Unterring von S.

Faktorring

Sei R ein Ring und I ein Ideal von R.
Bezeichne R/I zunächst die Faktorgruppe der additiven Gruppen R und I.

Für $a+I$ und $b+I$ definieren wir $(a+I)\cdot(b+I) = ab+I$.
Dies ist wohldefiniert:

- Für $a'+I = a+I$ und $b'+I = b+I$ gibt es $i_1, i_2 \in I$ mit $a' = a+i_1$ und $b' = b+i_2$. Dann gilt $a'b' = ab+ai_2+bi_1+i_1i_2 \in ab+I$ aufgrund der Idealeigenschaft, also $a'b'+I = ab+I$.

Einselement ist 1_R+I.

Damit wird R/I zu einem Ring und $f: R \to R/I$, $x \mapsto x+I$ zu einem Epimorphismus (Restklassenhomomorphismus).

Beispiel: $R = \mathbb{Z}$ und $I = 5\mathbb{Z}$. I ist ein Ideal, und $R/I = \mathbb{F}_5$ der Faktorring.

Isomorphiesatz

Thm: Ist $f: R \to S$ ein Homomorphismus, so ist $h: R/\ker(f) \cong \mathrm{im}(f)$, $x+\ker(f) \mapsto f(x)$ ein Isomorphismus.

Bew: Fassen wir R und S nur als additive abelsche Gruppen auf, ist der Satz bereits bewiesen. Wir müssen daher nur noch die Multiplikativität von h überprüfen. Wegen $(x+\ker(f))(y+\ker(f)) = (xy+\ker(f))$ folgt diese direkt aus der Multiplikativität von f. $\square$

Direktes Produkt

Sind R, S Ringe, so können wir $R \times S$ durch $(a_1,a_2)+(b_1,b_2) = (a_1+b_1, a_2+b_2)$ und $(a_1,a_2)(b_1,b_2) = (a_1b_1, a_2b_2)$ zu einem Ring machen.

Das Nullelement und Einselement sind hier $(0,0)$ bzw. $(1,1)$.

Die Einheiten von $R \times S$ sind genau die Paare, welche an der ersten und zweiten Koordinate eine Einheit zu stehen haben. Als Formel gilt also $(R \times S)^\times = R^\times \times S^\times$.

Euklidische Ringe

Sei R ein Integritätsring. Man nennt R einen euklidischen Ring, wenn es eine Gradfunktion $d: R\backslash\{0\} \to \mathbb{Z}^{\geq 0}$ mit der folgenden Eigenschaft gibt: Zu $a, b \in R$ und $b \neq 0$ gibt es $s, r \in R$ mit $a = sb+r$ und $r = 0$ oder $d(r) < d(b)$ (Division mit Rest).

Beispiele:

- $\mathbb{Z}$ mit der Gradfunktion $|\cdot|$.
- $k[x]$ mit der Gradfunktion $\deg$.
- Jeder Körper mit der konstanten Gradfunktion 1.

Euklidische Ringe

Sei R ein euklidischer Ring mit Gradfunktion d.

Thm: Für jedes Ideal I von R gibt es ein $b \in R$ mit $I = Rb$ (das heißt I ist ein Hauptideal).

Bew: Ein Element $b \in I$ mit dem kleinsten d-Wert ist ein Erzeuger, da es jedes weitere Element $a \in I$ teilt. Sonst hätte $r = a - sb \in I$ nämlich einen kleineren d-Wert. $\square$

Sind $a_1, a_2 \in R$, so gibt es daher ein $c \in R$ mit $Rc = Ra_1 + Ra_2$. Es gibt also $\lambda_1, \lambda_2 \in R$ mit $c = \lambda_1 a_1 + \lambda_2 a_2$ und $c \mid a_1$, $c \mid a_2$. Die Elemente λ_i können mit dem euklidischen Algorithmus ausgerechnet werden.

Die Verallgemeinerung auf n Elemente a_i ist induktiv möglich.

Euklidischer Algorithmus

Eingabe: a_1 und a_2 aus R.
Ausgabe: $c, \lambda_1, \lambda_2 \in R$ mit $c = \lambda_1 a_1 + \lambda_2 a_2$ und $c \mid a_1$, $c \mid a_2$.

1. $(u_1, u_2) \leftarrow (a_1, a_2)$, $M \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Im folgenden zusätzlich $d(0) = -\infty$.
2. Wenn $d(u_1) > d(u_2)$, dann vertausche u_1, u_2 und die Spalten von M.
3. Wenn $u_1 = 0$, dann schreibe $M = \begin{pmatrix} * & \lambda_1 \\ * & \lambda_2 \end{pmatrix}$. Ausgabe von u_2, λ_1, λ_2.
4. Schreibe $u_2 = su_1 + r$. Setze $u_2 \leftarrow r$ und subtrahiere das s-fache der ersten Spalte von M von der zweiten Spalte.
5. Gehe zu 2.

Euklidischer Algorithmus

Es gilt stets $(u_1, u_2) = (a_1, a_2)M$ und M ist invertierbar in $R^{2\times 2}$, da jede einzelne Transformation im Algorithmus invertierbar ist. Daher gilt stets $(a_1, a_2) = (u_1, u_2)M^{-1}$ mit $M^{-1} \in R^{2\times 2}$ und $Ru_1 + Ru_2 = Ra_1 + Ra_2$.

Der Algorithmus terminiert, da in Schritt 4 der Wert $d(r)$ echt kleiner ist als der Wert $d(u_2)$, außer wenn $u_1 = 0$.

Für $u_1 = 0$ folgt $Ru_2 = Ra_1 + Ra_2$, und folglich ist u_2 von der Form $u_2 = \lambda_1 a_1 + \lambda_2 a_2$ mit $u_2 \mid a_1$ und $u_2 \mid a_2$.