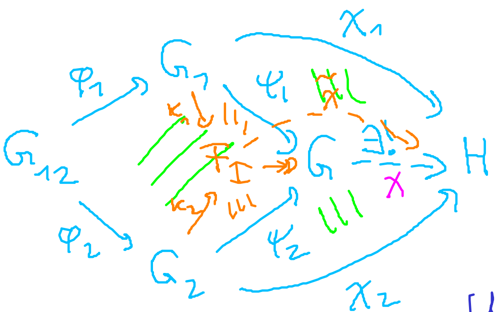
1.15.4 Definition: Betrachte Gruppen und Homomorphismen $G_1 \xleftarrow{\varphi_1} G_{12} \xrightarrow{\varphi_2} G_2$. Eine Gruppe G zusammen mit Homomorphismen $G_1 \xrightarrow{\psi_1} G \xleftarrow{\psi_2} G_2$ heisst ein *Pushout* oder *amalgamiertes Produkt von G_1 und G_2 über G_{12}*, wenn $\psi_1 \circ \varphi_1 = \psi_2 \circ \varphi_2$ gilt und für jede Gruppe H und je zwei Homomorphismen $G_1 \xrightarrow{\chi_1} H \xleftarrow{\chi_2} G_2$ mit $\chi_1 \circ \varphi_1 = \chi_2 \circ \varphi_2$ genau ein Homomorphismus $\chi \colon G \to H$ existiert mit $\chi \circ \psi_1 = \chi_1$ und $\chi \circ \psi_2 = \chi_2$.

1.15.5 Proposition: Ein amalgamiertes Produkt existiert und ist eindeutig bis auf eindeutige Isomorphie.

wie sonst.



Beweis:

Existenz: OBdA $G_1 \cap G_2 = \emptyset$. Setze $I := G_1 \cup G_2$.

Will $G := F_I / N_J$ für $J := \{\kappa_1(g) \cdot \kappa_1(g') \cdot \kappa_1(gg')^{-1} \mid g, g' \in G_1\}$
$\cup \{\kappa_2(g) \cdot \kappa_2(g') \cdot \kappa_2(gg')^{-1} \mid g, g' \in G_2\}$
$\cup \{\kappa_1\varphi_1(g) \cdot \kappa_2\varphi_2(g)^{-1} \mid g \in G_{12}\}$

UE: H, χ_1, χ_2 gegeben
$\Rightarrow \exists! \tilde{\chi} \colon F_I \to H$ Homo mit $\forall g \in G_i$: $\tilde{\chi}(\kappa_i(g)) = \chi_i(g)$, d.h.: $\chi_1 = \tilde{\chi} \circ \kappa_1$ und $\chi_2 = \tilde{\chi} \circ \kappa_2$.
χ_i Homo $\wedge$ $\chi_1\varphi_1 = \chi_2 \circ \varphi_2$ $\Rightarrow J \subset \ker(\tilde{\chi}) \Rightarrow \exists!$ Homo $\chi \colon G \to H$ wie gewünscht.

1.15.6 Definition: Das amalgamierte Produkt von G_1 und G_2 über G_{12} wird bezeichnet mit $G_1 *_{G_{12}} G_2$. Im Fall $G_{12} = 1$ heisst es auch das *freie Produkt von G_1 und G_2* und wird bezeichnet mit $G_1 * G_2$.

qed

1.15.7 Beispiel: Für disjunkte Mengen I und J ist $F_I * F_J \cong F_{I \sqcup J}$.

1.15.8 Beispiel: Für alle $m, n \geqslant 0$ ist $F_m * F_n \cong F_{m+n}$.

1.15.9 Beispiel: Für die Einbettungen der zyklischen Gruppen $C_6 \hookleftarrow C_2 \hookrightarrow C_4$ gilt

$$\mathrm{SL}_2(\mathbb{Z}) \;\cong\; C_6 *_{C_2} C_4 \;\cong\; \langle R, S \mid R^3 = S^2,\ S^4 = 1 \rangle.$$

$R^6 = 1$

$$\begin{tikzcd}
 & \langle S \mid S^4 = 1 \rangle \arrow[d, phantom, "\shortparallel"] & \\
 & S^2 \in C_4 \arrow[dr] & \\
C_2 \arrow[ur] \arrow[dr] & & C_4 *_{C_2} C_6 \\
 & R^3 \in C_6 \arrow[ur] \arrow[d, phantom, "\shortparallel"] & \\
 & \langle R \mid R^6 = 1 \rangle &
\end{tikzcd}$$

(Vergleiche `https://en.wikipedia.org/wiki/Modular_group`)

<u>Variante</u>: $PSl_2(\mathbb{Z}) := Sl_2(\mathbb{Z}) / \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = C_3 * C_2$

2 Ringe

Kommutative unitäre Ringe sowie Moduln über solchen sind Gegenstand des Gebiets der *Kommutativen Algebra*. Wir behandeln einige Grundlagen daraus.

2.1 Grundbegriffe

Sei R eine Menge mit Abbildungen

$$\begin{aligned} + :\quad & R \times R \to R, \quad (x,y) \mapsto x + y, \\ \cdot :\quad & R \times R \to R, \quad (x,y) \mapsto x \cdot y = xy, \end{aligned}$$

und ausgezeichneten Elementen $0 = 0_R$ sowie $1 = 1_R \in R$. Betrachte die Axiome:

(1)	$\forall x, y, z \in R$:	$x + (y + z) = (x + y) + z$	Assoziativität der Addition
(2)	$\forall x, y \in R$:	$x + y = y + x$	Kommutativität der Addition
(3)	$\forall x \in R$:	$0 + x = x$	Neutrales Element der Addition
(4)	$\forall x \in R\ \exists x' \in R$:	$x + x' = 0$	Inverses Element der Addition
(5)	$\forall x, y, z \in R$:	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	Assoziativität der Multiplikation
(6)	$\forall x, y, z \in R$:	$\left\{\begin{array}{l} x \cdot (y + z) = x \cdot y + x \cdot z \\ (y + z) \cdot x = y \cdot x + z \cdot x \end{array}\right\}$	Distributivität
(7)	$\forall x, y \in R$:	$x \cdot y = y \cdot x$	Kommutativität der Multiplikation
(8)	$\forall x \in R$:	$1 \cdot x = x = x \cdot 1$	Neutrales Element der Multiplikation
(9)		$1 \neq 0$	Nichttrivialität
(10)	$\forall x \in R \setminus \{0\}\ \exists x' \in R$:	$x' \cdot x = 1 = x \cdot x'$	Inverses Element der Multiplikation

2.1.1 Definition: Ein Tupel $(R, +, \cdot, 0, 1)$ mit ...

(a) den Axiomen (1) bis (8) heisst ein *kommutativer unitärer Ring* oder *kommutativer Ring mit Eins*.

(b) den Axiomen (1) bis (10) heisst ein *Körper*.

2.1.2 Konvention: Einen kommutativen unitären Ring nennen wir in diesem Abschnitt nur kurz *Ring*. (Aber Vorsicht: Gewisse weitere Begriffe werden beim Fehlen eines Einselementes anders definiert.) Wie üblich schreiben wir nur kurz R anstelle des ganzen Tupels und sehen die Zusatzdaten als implizit mitgegeben an.

Sei also R ein Ring.

2.1.3 Bemerkung: Die Axiome (1) bis (4) besagen, dass $(R, +, 0)$ eine abelsche Gruppe ist, genannt die *additive Gruppe von R.* Insbesondere ist das inverse Element $-x$ von x bezüglich der Addition eindeutig bestimmt. Für $x+(-y)$ schreibt man auch kürzer $x-y$. Für jede ganze Zahl n ist das *n-te Vielfache von x* definiert durch

$$n \cdot x \;:=\; \begin{cases} \quad x + \ldots + x \;\; \text{mit } n \text{ Summanden} & \text{falls } n > 0, \\ \quad 0 & \text{falls } n = 0, \\ -(x + \ldots + x) \;\; \text{mit } |n| \text{ Summanden} & \text{falls } n < 0. \end{cases}$$

2.1.4 Rechenregeln: Für alle $x, y \in R$ und alle $m, n \in \mathbb{Z}$ gilt:

$$\begin{aligned} (\pm n) \cdot x &= \pm(n \cdot x) \\ (m \pm n) \cdot x &= m \cdot x \pm n \cdot x \\ m \cdot (x \pm y) &= m \cdot x \pm m \cdot y \\ (m \cdot n) \cdot x &= m \cdot (n \cdot x) \\ m \cdot (x \cdot y) &= (m \cdot x) \cdot y \end{aligned}$$

2.1.5 Bemerkung: Für jede ganze Zahl $n \geqslant 0$ ist die *n-te Potenz von x* definiert durch

$$x^n \;:=\; \begin{cases} x\cdots x \;\; \text{mit } n \text{ Faktoren} & \text{falls } n > 0, \\ 1 & \text{falls } n = 0. \end{cases}$$

2.1.6 Rechenregeln: Für alle $x, y \in R$ und alle $m, n \geqslant 0$ gilt:

$$\begin{aligned} x^{m+n} &= x^m \cdot x^n \\ (x \cdot y)^m &= x^m \cdot y^m \\ x^{m\cdot n} &= (x^m)^n \end{aligned}$$

2.1.7 Bemerkung: Für Summen $\sum_{i\in I} x_i$ und Produkte $\prod_{i\in I} x_i$ in einem Ring gelten die gleichen Konventionen und Grundregeln wie in einem Körper.

2.1.8 Proposition: Es ist $1 = 0$ genau dann, wenn der Ring der Nullring ist.

Beweis: $1_R = 0_R \Rightarrow \forall x \in R: \; x = 1_R \cdot x = 0_R \cdot x = (0_R + 0_R) \cdot x = 0_R \cdot x + 0_R \cdot x$

$\Rightarrow 0_R \cdot x = 0_R$.

$R = \{0_R\} \Rightarrow 1_R = 0_R$.

qed.

Beispiel: Die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$, die komplexen Zahlen $\mathbb{C}$, jeweils mit den üblichen Rechenoperationen und den üblichen neutralen Elementen.

Beispiel: Der Ring $\mathbb{Z}$ der ganzen Zahlen mit den üblichen $+$, $\cdot$, 0, 1.

Beispiel: Der Ring $\mathbb{Z}/n\mathbb{Z}$ der ganzen Zahlen modulo n für jede ganze Zahl $n \geqslant 1$.

Beispiel: Der Körper $\mathbb{F}_p$ der ganzen Zahlen modulo p für jede Primzahl p. Insbesondere für $p = 2$ der Körper der binären Zahlen $\mathbb{F}_2 = \{0, 1\}$ mit den Operationen:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Beispiel: Ring von Funktionen auf einer Menge

Beispiel: Ringe stetiger, differenzierbarer, holomorpher Funktionen

2.2 Einheiten

2.2.1 Definition: Ein Element $x \in R$ mit der Eigenschaft

$$\exists x' \in R\colon\ \ x' \cdot x = 1$$

heisst *invertierbar* oder eine *Einheit von R.* Die Menge aller Einheiten von R bezeichnen wir mit $R^\times$ (sprich „R Kreuz“) oder auch R^*.

2.2.2 Proposition: Die Menge $R^\times$ ist bezüglich Multiplikation eine abelsche Gruppe, genannt die *Einheitengruppe von R.*

Bew.: $\forall x, y \in R^\times \Rightarrow$ Seien $x', y' \in R$ mit $x'x = y'y = 1$. Dann ist $(x'y')(xy) = (x'x)(y'y) = 1 \cdot 1 = 1$
$\rightsquigarrow xy \in R^\times$. und $xx' = 1 \Rightarrow x' \in R^\times$.
assoz.; komm.: $1 \in R^\times$ neutrales Element; x' inverses Element. qed.

Insbesondere ist das inverse Element x' jeder Einheit x eindeutig bestimmt. Es wird bezeichnet mit x^{-1} oder $\frac{1}{x}$. Für $\frac{1}{x} \cdot y$ schreibt man auch $\frac{y}{x}$. Weiter ist jedes Produkt und jeder Quotient von Einheiten eine Einheit, und das Einselement 1 ist eine Einheit. Für jede Einheit x und jede natürliche Zahl n definieren wir $x^{-n} := (x^{-1})^n$, mit denselben Rechenregeln wie oben.

2.2.3 Beispiel: Für jeden Körper K ist $K^\times = K \setminus \{0\}$.

2.2.4 Beispiel: Es ist $\mathbb{Z}^\times = \{\pm 1\}$.

2.3 Homomorphismen

Betrachte zwei Ringe R und S.

2.3.1 Definition: Ein *(Ring)-Homomorphismus* $\varphi\colon R \to S$ ist eine Abbildung mit

(a) $\varphi(1_R) = 1_S$.

(b) $\forall x, y \in R\colon\ \varphi(x+y) = \varphi(x) + \varphi(y)$.

(c) $\forall x, y \in R\colon\ \varphi(xy) = \varphi(x)\varphi(y)$.

Bsp.: $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}$, $n \mapsto 0$ kein Ringhomo.

2.3.2 Proposition: Für jeden Homomorphismus $\varphi\colon R \to S$ gilt:

(a) $\varphi(0_R) = 0_S$.

(b) $\forall x \in R\ \forall n \in \mathbb{Z}\colon\ \varphi(nx) = n\varphi(x)$.

(c) $\forall x \in R\ \forall n \in \mathbb{Z}^{\geqslant 0}\colon\ \varphi(x^n) = \varphi(x)^n$.

(d) φ induziert einen Gruppenhomomorphismus $R^\times \to S^\times$.

Bew. (a) $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R) \Rightarrow \varphi(0_R) = 0_S$.

(b) Induktion über n, $\varphi(-x) = -\varphi(x)$.

(c) " "

(d) $\forall x \in R^\times$: $\varphi(x^{-1}) \cdot \varphi(x) = \varphi(x^{-1}x) = \varphi(1_R) = 1_S \Rightarrow \varphi(x) \in S^\times$.

qed.

2.3.3 Proposition: Die Identität $\mathrm{id}_R\colon R \to R$ ist ein Homomorphismus. Die Komposition zweier Homomorphismen ist ein Homomorphismus.

2.3.4 Definition: Ein Homomorphismus $\varphi\colon R \to S$ mit einem beidseitigem Inversen φ^{-1} heisst ein *Isomorphismus*, und wir schreiben dann $\boxed{\varphi\colon R \xrightarrow{\sim} S}$. Existiert ein Isomorphismus $R \xrightarrow{\sim} S$, so heissen R und S *isomorph* und wir schreiben $R \cong S$.

2.3.5 Proposition: Ein Ringhomomorphismus ist ein Isomorphismus genau dann, wenn er bijektiv ist.

Beweis: Iso $\Rightarrow$ bijektiv.

bijektiv $\Rightarrow$ $1_R = \varphi^{-1}(1_S)$. ...

Wende φ^{-1} auf Axiome an. qed

2.3.6 Proposition: Die Komposition zweier Isomorphismen ist ein Isomorphismus. Das Inverse eines Isomorphismus ist eindeutig bestimmt und selbst ein Isomorphismus. Isomorphie von Ringen ist eine Äquivalenzrelation.

2.3.7 Definition: Ein Isomorphismus $R \xrightarrow{\sim} R$ heisst ein *Automorphismus von R*.

$\varphi : K \to L$

2.3.8 Proposition: Jeder Homomorphismus zwischen zwei Körpern ist injektiv.

Bew.: $2.3.2(d) \Rightarrow \varphi(K^\times) \subset L^\times$

$\Rightarrow \forall x \in K \setminus \{0\} : \varphi(x) \neq 0$

$\Rightarrow \ker(\varphi) = \{0\} \Rightarrow \varphi$ injektiv. qed.

2.3.9 Beispiel: Für jeden Ring R existiert genau ein Ringhomomorphismus $\mathbb{Z} \to R$, nämlich die Abbildung $n \mapsto n \cdot 1_R$.

z.B. $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$

$1 \longmapsto [1]$.

z.B. $\mathbb{Z} \hookrightarrow \mathbb{Q}$

2.4 Unterringe, Produkte

2.4.1 Definition: Ein *Unterring von R* ist eine Teilmenge $R' \subset R$ mit den Eigenschaften:

(a) $\forall x, y \in R' : \ x + y \in R'$. $0_R = 1_R + (-1_R) \in R'$.

(b) $\forall x, y \in R' : \ xy \in R'$.

(c) $\forall x \in R' : \ -x \in R'$.

(d) $1_R \in R'$.

Die Teilmenge R' bildet dann zusammen mit den Restriktion der Operationen von R selbst einen Ring, und die Inklusionsabbildung $R' \hookrightarrow R$ einen Ringhomomorphismus.

2.4.2 Beispiel: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

2.4.3 Proposition: Der Durchschnitt jeder nichtleeren Kollektion von Unterringen von R ist ein Unterring von R.

Bew.: $\bigcap_{i \in I} R_i$ ... qed.

Unterring.

2.4.4 Proposition: Für jeden Unterring $R' \subset R$ und jede Teilmenge $A \subset R$ existiert ein eindeutiger kleinster Unterring von R, welcher R' und A enthält. Dieser besteht aus den Elementen der Form

$$\boxed{\sum_{i_1,\ldots,i_n \geqslant 0}{}' x_{i_1,\ldots,i_n} a_1^{i_1} \cdots a_n^{i_n}}$$

für alle $n \geqslant 0$ und $a_1, \ldots, a_n \in A$ und $x_{i_1,\ldots,i_n} \in R'$, fast alle gleich 0.

Bem.: Durchschnitt aller Unterringe, die $R' \cup A$ enthalten. Tut's !!

2.4.5 Definition: Dieser Unterring heisst *der von A über R' erzeugte Unterring* und wird bezeichnet mit $R'[A]$. Für endlich viele Elemente $a_1, \ldots, a_n \in R$ schreiben wir auch $R'[a_1, \ldots, a_n] := R'[\{a_1, \ldots, a_n\}]$.