Computerpraktikum

Block I

Der symmetrische verschränkte Modul

Matthias Künzer

Universität Stuttgart

8. Dezember 2017

Inhalt

Vorwort

Eine Gruppe bettet ein in die symmetrische Gruppe ihrer unterliegenden Menge, dank eines Lemmas von Cayley [**1**].

Eine Gruppe entspricht einem topologischen Raum mit nur Homotopiegruppe π_1 .

Ein verschränkter Modul entspricht einem topologischen Raum mit nur Homotopiegruppen π_1 und π_2 . Unter dem englischen Begriff eines Crossed modules wurden solche Objekte zu diesem Zweck von J.H.C. Whitehead eingeführt [**4**].

Ein verschränkter Modul bettet ein in den symmetrischen verschränkten Modul seiner unterliegenden Kategorie, dank eines Lemmas von Truong [**3**].

In diesem Block des Computerpraktikums soll diese Einbettung untersucht werden.

Dieser Begleittext wird während des Semesters bei Bedarf ergänzt oder geändert.

Vorausgesetzt wird der Begriff einer Gruppe, wie er etwa in der Linearen Algebra vermittelt wird.

Ein Dank geht an Sema Bahadir, Sonja Eisenreich und Heiko Mögerle für die Korrektur von Fehlern. Ein Dank geht an Monika Truong für Erklärungen zu verschränkten Moduln. Ein Dank geht an Sebastian Thomas für die zugrundeliegende Idee.

Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Stuttgart, Herbst 2017

Matthias Künzer

Konventionen

- Für $a,\, b \in \mathbf{Z}$ sei $[a,b] := \{\, z \in \mathbf{Z} \,:\, a \leqslant z \leqslant b \,\}$.

- Wir schreiben Abbildungen rechts. ([1]) Das soll folgendes bedeuten.

  Seien X, Y, Z Mengen. Seien $X \xrightarrow{f} Y \xrightarrow{g} Z$ Abbildungen.

  Ist $x \in X$, so schreiben wir $xf \in Y$ für das Bild von x unter f.

  Wir schreiben $X \xrightarrow{f \blacktriangle g} Z$ oder kurz $X \xrightarrow{fg} Z$ für das Kompositum von f und g.

  I.e. $x(fg) := (xf)g$ für $x \in X$.

[1] Auch Magma arbeitet so.

- Seien X, X', Y, Y' Mengen. Sei $f\colon X \to Y$ eine Abbildung mit $X'f \subseteq Y'$. Wir schreiben $f|_{X'}^{Y'}\colon X' \to Y'$ für die Einschränkung von f im Definitionsbereich auf X', im Zielbereich auf Y'. I.e. $x'(f|_{X'}^{Y'}) = x'f$ für $x' \in X'$.

  Ist $Y' = Y$, so schreiben wir auch $f_{X'} := f|_{X'}^{Y'}$.

  Ist $X' = X$, so schreiben wir auch $f^{Y'} := f|_{X'}^{Y'}$.

- Eine Gruppe $G = (G, \cdot)$ ist eine Menge G zusammen mit einer Multiplikationsabbildung $(\cdot) : G \times G \to G$, welche assoziativ ist, für welche ein beidseitig neutrales Element $1 = 1_G$ existiert und für welche zu jedem Element $g \in G$ ein beidseitiges Inverses g^- existiert. Oft schreiben wir $xy := x \cdot y$ für $x,\, y \,\in\, G$.

- Sei G eine Gruppe. Seien $x,\, g \,\in\, G$. Sei $g^x := x^- gx$ das Resultat der Konjugation von g mit x.

- Sei G eine Gruppe.

  Eine Teilmenge U von G heißt Untergruppe, falls $1_G \in U$ und falls für $u,\, v \,\in\, U$ auch $uv^- \in U$ ist. Wir schreiben diesenfalls $U \leqslant G$.

  Eine Untergruppe N von G heißt Normalteiler von G, falls für $n \in N$ und $x \in G$ auch $n^x \in N$ ist. Wir schreiben diesenfalls $N \trianglelefteqslant G$.

  Ist $N \trianglelefteqslant G$, dann ist $G/N := \{\, gN \,:\, g \in G \,\}$ mittels $gN \cdot \tilde{g}N := g\tilde{g}N$ für $g,\, \tilde{g} \,\in\, G$ eine Gruppe, die Faktorgruppe von G modulo N.

- Sei G eine Gruppe. Sei $X \subseteq G$ eine Teilmenge. Sei $\langle X \rangle$ der Schnitt aller Untergruppen von G, die X enthalten. Es heißt $\langle X \rangle$ das Untergruppenerzeugnis von X in G. Es ist $\langle X \rangle$ in jeder Untergruppe von G enthalten, die X enthält. Es besteht $\langle X \rangle$ aus allen Produkten von Elementen von X und ihrer Inversen. Als Beispiel, sind $x_1,\, x_2,\, x_3 \,\in X$, dann ist e.g. $x_2^- x_3 x_1^3 x_2^{-2} x_1^{-7} \in \langle X \rangle$.

- Seien G und H Gruppen. Ein Gruppenmorphismus von G nach H ist eine Abbildung $G \xrightarrow{f} H$, für welche $(xy)f = (xf)(yf)$ gilt für $x,\, y \,\in\, G$. Insbesondere ist dann $1f = 1$ und $(x^-)f = (xf)^-$ für $x \in G$.

- Eine Gruppe G heißt abelsch, falls $xy = yx$ ist für $x,\, y \,\in\, G$.

- Sei G eine endliche Gruppe. Es bezeichnet $|G|$ die Ordnung von G, i.e. die Anzahl der Elemente von G.

- Sei $n \geqslant 1$. Es bezeichnet S_n die symmetrische Gruppe auf der Menge $[1, n] = \{1, 2, \ldots, n\}$. I.e. S_n besteht aus den bijektiven Abbildungen von $[1, n]$ nach $[1, n]$. Die Multiplikation ist gegeben durch Komposition. Es ist $1_{\mathrm{S}_n} = \mathrm{id}_{[1,n]} =: \mathrm{id}$.

  Ein Element $\sigma \in \mathrm{S}_n$ wird in Zykelschreibweise geschrieben:

$$\sigma \;=\; (a_{1,1},\, a_{1,2},\, \ldots,\, a_{1,\ell_1})(a_{2,1},\, a_{2,2},\, \ldots,\, a_{2,\ell_2}) \ldots (a_{k,1},\, a_{k,2},\, \ldots,\, a_{k,\ell_k})$$

bedeute, daß sich für $i \in [1, k]$ zum einen $a_{i,j}\sigma = a_{i,j+1}$ ergibt für $j \in [1, \ell_i - 1]$, zum anderen $a_{i,\ell_i}\sigma = a_{i,1}$ ist.

In dieser Schreibweise werden Zykel der Länge $\ell_i = 1$ in der Regel nicht hingeschrieben.

So ist e.g. $\sigma := (1, 4, 2)(3, 8, 5, 7) \in \mathrm{S}_8$ die Abbildung $\sigma : [1, 8] \to [1, 8]$ mit $1\sigma = 4$, $4\sigma = 2$, $2\sigma = 1$, $3\sigma = 8$, $8\sigma = 5$, $5\sigma = 7$, $7\sigma = 5$ und $6\sigma = 6$.

Ferner ist e.g. $\mathrm{S}_3 = \{\mathrm{id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$. Da $(1, 2)(2, 3) = (1, 3, 2)$, aber $(2, 3)(1, 2) = (1, 2, 3)$, ist S_3 eine nichtabelsche Gruppe.

- Sei X eine Menge. Es bezeichnet S_X die symmetrische Gruppe auf X. I.e. S_X besteht aus den bijektiven Abbildungen von X nach X. Die Multiplikation ist gegeben durch Komposition. Es ist $1_{\mathrm{S}_X} = \mathrm{id}_X =: \mathrm{id}$.

  Für $n \geqslant 1$ ist also $\mathrm{S}_{[1,n]} = \mathrm{S}_n$.

1 Magma

Wir verwenden das Computeralgebra-System Magma.

Das Handbuch findet sich unter `magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`.

Ein Magma-Online-Rechner findet sich unter `magma.maths.usyd.edu.au/calc/`.

Am Rechner wird Magma in einer Shell mittels `magma` aufgerufen. Darin wird die Hilfe e.g. für den Begriff “Integers” mit `?Integers` aufgerufen.

2 Verschränkte Moduln

2.1 Automorphismengruppen

Definition 1 Sei M eine Gruppe. Die *Automorphismengruppe* $\mathrm{Aut}(M)$ besteht aus den bijektiven Gruppenmorphismen von M nach M. Die Multiplikation auf $\mathrm{Aut}(M)$ ist gegeben durch Komposition. Ferner ist $1_{\mathrm{Aut}(M)} = \mathrm{id}_M$.

Definition 2 (und Beispiel) Sei M eine Gruppe. Sei $x \in M$.

Es ist $\kappa_x^M : M \to M : m \mapsto m^x$ ein Automorphismus, die *Konjugation* mit x auf M.

Kurz, es ist $\kappa_x^M \in \mathrm{Aut}(M)$.

Wir schreiben oft $\kappa_x := \kappa_x^M$, wenn M aus dem Kontext hervorgeht.

Rechnen wir nach, daß κ_x ein Automorphismus von M ist. Es ist $\kappa_{xy} = \kappa_x\kappa_y$ für $x,\ y \in M$, da $m^{(xy)} = y^- x^- mxy = (m^x)^y$ ist für $m \in M$. Insbesondere ist $\kappa_x\kappa_{x^-} = \kappa_{xx^-} = \kappa_1 = \mathrm{id}_M$

und $\kappa_{x^-}\kappa_x = \kappa_{x^-x} = \kappa_1 = \mathrm{id}_M$. Also ist κ_x bijektiv. Ferner ist $(m\kappa_x)(n) = x^-mxx^-nx = x^-mnx = (mn)\kappa_x$ für $m,\, n \in M$. Also ist κ_x ein Gruppenmorphismus.

Beispiel 3 Sei $c := (1, 2, 3) \in \mathrm{S}_3 =: G$. Wir betrachten $M := \langle c\rangle = \{1, c, c^2\} \trianglelefteqslant G$.

Es ist $\kappa^G_{(1,2)} \in \mathrm{Aut}(G)$.

Es ist $\sigma := \kappa^G_{(1,2)}|^M_M \in \mathrm{Aut}(M)$.

Es wird $1\sigma = 1$, $c\sigma = (1, 2, 3)^{(1,2)} = (1, 3, 2) = c^2$ und also $c^2\sigma = c^4 = c$.

Da M abelsch ist, ist somit σ nicht von der Form κ^M_x für ein $x \in M$.

Diese Situation können wir mittels Magma untersuchen.

```
G := SymmetricGroup(3);
print G;
print Order(G);
print G!(1,2) * G!(2,3);
c := G!(1,2,3);
M := sub<G | c>;
A := AutomorphismGroup(M);
print A;
print Order(A);
AFP,phi := FPGroup(A);
AP,psi := PermutationGroup(AFP);
list := [x@@psi@phi : x in AP];
print c@list[1];
print c@list[2];
```

Um die Elemente von `A` $=$ Aut(M) auflisten zu können, wird man von Magma zu einer Pirouette gezwungen: man muß `A` umwandeln in eine endlich präsentierte Gruppe (finitely presented) und dann in eine Permutationsgruppe; diese darf man dann auflisten. Rückwärts ist dann mittels `@@` ein Urbild zu nehmen, mittels `@` ein Bild. Alternativ hätte man auch `x@(psi^-1*phi)` verwenden können.

Diese Liste der Elemente von Aut(M) heißt nun `list`. Darin ist `list[1]` $= \mathrm{id}_M$ und `list[2]` $= \gamma$. Da Aut(M) nur ein Element von Ordnung 2 hat, könnte man nach Erhalt von `AP` auch wie folgt vorgehen:

```
sigma := [x@@psi@phi : x in AP | Order(x) eq 2][1];
print c@sigma;
```

Notation 4 Seien G und M Gruppen. Sei $G \xrightarrow{\alpha} \mathrm{Aut}(M)$ ein Gruppenmorphismus.

Wir schreiben mißbräuchlicherweise oft $m^g := m(g\alpha)$ für $m \in M$ und $g \in G$, wenn α aus dem Kontext hervorgeht.

Dann ist $m^1 = m(1\alpha) = m1_{\mathrm{Aut}(M)} = m\,\mathrm{id}_M = m$ für $m \in M$.

Ferner ist $m^{(gh)} = m((gh)\alpha) = m(g\alpha)(h\alpha) = (m^g)^h$ für $m \in M$ und $g,\, h\, \in\, G$.

Schließlich ist $(m\tilde{m})^g = (m\tilde{m})(g\alpha) = m(g\alpha) \cdot \tilde{m}(g\alpha) = m^g \cdot \tilde{m}^g$ für $m \in M$ und $g \in G$.

2.2 Der Begriff des verschränkten Moduls

Definition 5 Ein *verschränkter Modul* $V = (G, M, f, \alpha)$ besteht aus

- einer Gruppe M,
- einer Gruppe G,
- einem Gruppenmorphismus $G \xrightarrow{\alpha} \mathrm{Aut}(M)$
- und einem Gruppenmorphismus $M \xrightarrow{f} G$

derart, daß die Eigenschaften (VM 1) und (VM 2) gelten.

(VM 1) Es ist $(m(g\alpha))f = (mf)^g$ für $m \in M$ und $g \in G$.

(VM 2) Es ist $m^n = m(nf\alpha)$ für $m \in M$ und $n \in M$.

Unter Verwendung von Notation 4 kann man dies auch wie folgt schreiben.

(VM 1) Es ist $(m^g)f = (mf)^g$ für $m \in M$ und $g \in G$.

(VM 2) Es ist $m^n = m^{nf}$ für $m \in M$ und $n \in M$.

Ist $V = (M, G, \alpha, f)$ ein verschränkter Modul, dann schreiben wir auch

- $V^{\mathrm{Modul}} := M$ für den *Modul von* V,
- $V^{\mathrm{Gruppe}} := G$ für die *Gruppe von* V,
- $\boldsymbol{\alpha}_V := \alpha$ für die *Operation von* V,
- $\mathrm{f}_V := f$ für das *Differential von* V.

Aus (VM 1) folgt $Mf \trianglelefteq G$.

Beispiel 6

(1) Sei $M = 1$. Sei G eine beliebige Gruppe. Dann liegen f und α eindeutig fest und es ist $(1, G, \alpha, f)$ ein verschränkter Modul.

(2) Sei M eine abelsche Gruppe. Sei $G = 1$. Dann liegen f und α eindeutig fest und es ist $(M, 1, \alpha, f)$ ein verschränkter Modul. Insbesondere ist (VM 2) erfüllt, da $m^n = m = m^{nf}$ ist wegen M abelsch.

Definition 7 (und Beispiel) Sei G eine Gruppe. Sei $M \trianglelefteqslant G$.

Sei $M \xrightarrow{f} G$ der Einbettungsmorphismus, i.e. $f = \mathrm{id}_G|_M$, i.e. $f\colon M \to G\colon m \mapsto m$.

Sei $\alpha\colon G \to \mathrm{Aut}(M)\colon g \mapsto \kappa_g^G|_M^M$; cf. Definition 2. Es ist α ein Gruppenmorphismus.

Beachte, daß dann für $m \in M$ und $g \in G$ sich $m(g\alpha) = m\kappa_g^G = m^g$ ergibt, was die in Notation 4 angesprochene mißbräuchliche Notation rechtfertigt.

Es ist $\mathrm{V}_{M \trianglelefteqslant G} := (M, G, \alpha, f)$ ein verschränkter Modul.

Beispiel 8 Wir setzen Beispiel 3 fort, in welchem $c = (1,2,3)$ und $M = \langle c \rangle \trianglelefteqslant \mathrm{S}_3 = G$ war.

Es ist $\mathrm{V}_{M \trianglelefteqslant G}$ ein verschränkter Modul.

Für $c = (1,2,3) \in M$ und $g := (1,2) \in G$ ist also e.g.

$$c(g\alpha) \;=\; c\kappa_g^G \;=\; c^g \;=\; (1,2,3)^{(1,2)} \;=\; (2,1,3) \;=\; (1,3,2)\,.$$

In Magma kann dies wie folgt eingegeben werden.

```
G := SymmetricGroup(3);
M := sub<G | G!(1,2,3)>;
f := hom<M -> G | x :-> x>;
alpha := hom<G -> AutomorphismGroup(M) | x :-> hom<M -> M | m :-> m^x> >;
// Test:
print [(m@(g@alpha))@f : g in G, m in M];  // Linke Seite von (VM 1)
print [ (m@f)^g  : g in G, m in M];        // Rechte Seite von (VM 1)
print &and[(m@(g@alpha))@f eq (m@f)^g  : g in G, m in M]; // Test von (VM 1)
print [m^n : m in M, n in M];              // Linke Seite von (VM 2)
print [m@(n@f@alpha) : m in M, n in M];    // Rechte Seite von (VM 2)
print &and[m^n eq m@(n@f@alpha)  : m in M, n in M]; // Test von (VM 2)
```

Definition 9 (und Beispiel) Sei M eine Gruppe. Sei $G := \mathrm{Aut}(M)$.

Sei $f\colon M \to G\colon x \mapsto \kappa_x^M$. I.e. für $x \in M$ ist $xf \in \mathrm{Aut}(M)$ der Automorphismus von M, welcher $m \in M$ auf $m(xf) = m^x = x^- mx$ abbildet.

Sei $\alpha\colon G \to \mathrm{Aut}(M)\colon \sigma \mapsto \sigma$ die Identität auf $\mathrm{Aut}(M)$.

Dann ist $\mathrm{V}_{M \to \mathrm{Aut}(M)} := (M, G, \alpha, f) = (M, \mathrm{Aut}(M), \mathrm{id}_{\mathrm{Aut}(M)}, f)$ ein verschränkter Modul.

Beispiel 10 Wir suchen mittels Magma eine nichtabelsche Gruppe der Ordnung 8.

```
print SmallGroups(8);
print [IsAbelian(H) : H in SmallGroups(8)];
M := PermutationGroup(FPGroup(SmallGroups(8)[3]));
print [Order(x) : x in M];
print [x : x in M];
print sub< M |M!(1,2,3,4), M!(1,3)> eq M;
```

Sei also $M = \mathrm{D}_8 := \langle (1,2,3,4),(1,3)\rangle \leqslant \mathrm{S}_4$. Wir wollen $\mathrm{V}_{M\to\mathrm{Aut}(M)}$ via Magma betrachten.

```
T := SymmetricGroup(4);
M := sub<T | T!(1,2,3,4), T!(1,3)>;
GA := AutomorphismGroup(M);
GFP,phi := FPGroup(GA);
G,psi := PermutationGroup(GFP);
alpha := psi^-1 * phi; // von G nach GA = Aut(M)
f0 := hom< M -> AutomorphismGroup(M) | x :-> hom<M->M | m :-> m^x > >;
f := hom<M -> G | m :-> [x : x in G | m@f0 eq x@alpha][1] > ;
// Test:
print [<x,x@f> : x in M];
print [(m@(g@alpha))@f : g in G, m in M]; // Linke Seite von (VM 1)
print [ (m@f)^g  : g in G, m in M];       // Rechte Seite von (VM 1)
print &and[(m@(g@alpha))@f eq (m@f)^g  : g in G, m in M]; // Test von (VM 1)
print [m^n : m in M, n in M];             // Linke Seite von (VM 2)
print [m@(n@f@alpha) : m in M, n in M];   // Rechte Seite von (VM 2)
print &and[m^n eq m@(n@f@alpha)  : m in M, n in M]; // Test von (VM 2)
```

Definition 11 Seien $V = (M,G,\alpha,f)$ und $V' = (M',G',\alpha',f')$ verschränkte Moduln.

Ein *Morphismus von verschränkten Moduln* (γ,μ) von V nach V' besteht aus

- einem Gruppenmorphismus $G \xrightarrow{\gamma} G'$
- und einem Gruppenmorphismus $M \xrightarrow{\mu} M'$

derart, daß die Eigenschaften (MVM 1) und (MVM 2) gelten.

(MVM 1) Es ist $m\mu f' = mf\gamma$ für $m \in M$.

(MVM 2) Es ist $m(g\alpha)\mu = (m\mu)(g\gamma\alpha')$ für $m \in M$ und $g \in G$.

Die Eigenschaft (MVM 1) bedeutet die Kommutativität des Vierecks

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\mu"'] & G \arrow[d, "\gamma"] \\ M' \arrow[r, "f'"] & G' \end{tikzcd}$$

Unter Verwendung von Notation 4 können wir umschreiben:

(MVM 2) Es ist $(m^g)\mu = (m\mu)^{g\gamma}$ für $m \in M$ und $g \in G$.

E.g. ist $V \xrightarrow{(\mathrm{id},\mathrm{id})} V$ ein Morphismus verschränkter Moduln.

Sind V, V', V'' verschränkte Moduln und sind $V \xrightarrow{(\gamma,\mu)} V' \xrightarrow{(\gamma',\mu')} V''$ Morphismen verschränkter Moduln, dann auch ist auch ihr Kompositum

$$V \xrightarrow{(\gamma,\mu)\,\blacktriangle\,(\gamma',\mu') := (\gamma\gamma',\mu\mu')} V''$$

ein Morphismus verschränkter Moduln.

Sei $V \xrightarrow{(\gamma,\mu)} V'$ ein Morphismus verschränkter Moduln. Sind γ und μ bijektiv, dann ist auch $V \xleftarrow{(\gamma^-,\mu^-)} V'$ ein Morphismus verschränkter Moduln. Diesenfalls heißt (γ,μ) ein *Isomorphismus* verschränkter Moduln.

Existiert ein Isomorphismus verschränkter Moduln von V nach V', so heißen V und V' *isomorph*, geschrieben $V \simeq V'$.

Bemerkung 12 *Sei $M \trianglelefteqslant G$. Sei $M' \trianglelefteqslant G'$.*

Sei $G \xrightarrow{\gamma} G'$ ein Gruppenmorphismus mit $M\gamma \leqslant M'$.

Schreibe $\mu := \gamma|_M^{M'}$. Dann ist

$$\mathrm{V}_{M \trianglelefteqslant G} \xrightarrow{(\gamma,\mu)} \mathrm{V}_{M' \trianglelefteqslant G'}$$

ein Morphismus verschränkter Moduln.

Beweis. Zum einen erzwingt (MVM 1) die Definition von μ. Zum anderen können wir (MVM 2) wie folgt nachrechnen: für $m \in M$ und $g \in G$ wird

$$(m^g)\mu \;=\; (m^g)\gamma \;=\; (m\gamma)^{g\gamma} \;=\; (m\mu)^{g\gamma}\,.$$

□

Bemerkung 13 *Sei $V = (M, G, \alpha, f)$ ein verschränkter Modul.*

Ist f injektiv, dann ist V isomorph zu $\mathrm{V}_{Mf \trianglelefteqslant G}$.

Beweis. Wir haben einen Gruppenisomorphismus $M \xrightarrow{\bar f} Mf : m \mapsto mf$. Wir behaupten, daß $(\bar f, \mathrm{id}_G)$ ein Isomorphismus verschränkter Moduln von V nach $\mathrm{V}_{Mf \trianglelefteqslant G}$ ist.

Schreibe $\iota\colon Mf \to G : x \to x$ für dis Inklusionsabbildung.

Ad (MVM 1). Für $m \in M$ ist $m\bar f\iota = mf = mf\,\mathrm{id}_G$.

Ad (MVM 2). Für $m \in M$ und $g \in G$ ist $(m^g)\bar f = (m^g)f = (mf)^g = (mf)^{g\,\mathrm{id}_G}$. □

3 Konstruktion von Gruppen

3.1 Semidirekte Produkte

Sei G eine Gruppe. Sei M eine Gruppe. Sei $\alpha\colon G \to M$ ein Gruppenmorphismus.

Wir erinnern an die Schreibweise $m(g\alpha) = m^g$ für $m \in M$ und $g \in G$.

Definition 14 Wir betrachten die Menge $G \times M$.

Sei auf $G \times M$ eine Multiplikation erklärt durch

$$(g,m)(g',m') \;=\; (g,m) \underset{\alpha}{\cdot} (g',m') \;:=\; (gg', m^{g'}m')\ .$$

für (g,m), $(g',m') \in G \times M$.

(Merkregel: "das Element g' muß an m vorbei, das kostet eine Operation.")

Diese Multiplikation hat das neutrale Element $(1,1)$. Sie ist assoziativ, da bei Multiplikation der Elemente (g,m), (g',m'), $(g'',m'') \in G \times M$ sich

$$((g,m)(g',m'))(g'',m'') \;=\; (gg'g'', m^{g'g''}m'^{g''}m'') \;=\; (g,m)((g',m')(g'',m''))$$

ergibt. Für $(g,m) \in G \times M$ erhalten wir

$$(g,m)(g^-, (m^-)^{g^-}) \;=\; (1,1) \;=\; (g^-, (m^-)^{g^-})(g,m)$$

was die Existenz eines Inversen $(g,m)^- = (g^-, (m^-)^{g^-})$ sichert.

Folglich ist $(G \times M, \underset{\alpha}{\cdot})$ eine Gruppe, das *semidirekte Produkt* von G und M mittels α.

Diese Gruppe wird $G \underset{\alpha}{\ltimes} M$ geschrieben, oder kurz $G \ltimes M$, wenn kein Mißverständnis zu erwarten ist.

Der Normalteiler $\{\, (1,m) \,:\, m \in M \,\}$ von $G \ltimes M$ wird mit M via $m \mapsto (1,m)$ identifiziert.

Beispiel 15 Wir setzen Beispiel 8 fort. Dort war $c := (1,2,3)$ und $M = \langle c \rangle \trianglelefteq \mathrm{S}_3 = G$.

Der dortige Gruppenmorphismus $\alpha\colon G \to \mathrm{Aut}(M)$ schickte $x \in G$ auf die Konjugation mit x, eingeschränkt auf M.

Sei $d := (1,2)$. Sei $H := \langle d \rangle = \{\mathrm{id}, d\}$.

Sei $\beta := \alpha|_H\colon H \to \mathrm{Aut}(M)$. Wir wollen mittels Magma nachrechnen, daß

$$H \underset{\beta}{\ltimes} M \;\;\simeq\;\; \mathrm{S}_3$$

ist.

```
G := SymmetricGroup(3);
c := G!(1,2,3);
d := G!(1,2);
M := sub<G | c>;
H := sub<G | d>;
sigma := hom<M->M | c -> c^2 >;
beta := hom< H -> AutomorphismGroup(M) | d -> sigma >;
print Order(Image(beta));
SP := SemidirectProduct(M,H,beta);
print IsIsomorphic(SP,G);
```

Es ist hier sogar `SQ` gleich `G`, aber das liegt nur an der Art, wie Magma intern ein semidirektes Produkt konstruiert.

3.2 Kranzprodukte

Definition 16 Sei $t \geqslant 1$. Sei $H \leqslant \mathrm{S}_t$. Sei K eine Gruppe.

Sei $K^{\times t} := \{\, (k_i)_{i\in[1,t]} \;:\; k_i \in K \text{ für } i \in [1,t] \,\}$.

Oft schreiben wir dabei kurz $(k_i)_i := (k_i)_{i\in[1,t]}$.

Es ist $K^{\times t}$ eine Gruppe mit eintragsweiser Multiplikation, i.e. $(k_i)_i \cdot (\tilde{k}_i)_i := (k_i\tilde{k}_i)_i$ für $(k_i)_i\,,\, (\tilde{k}_i)_i \,\in\, K^{\times t}$.

Wir haben einen Gruppenmorphismus

$$\begin{array}{rcl} H & \xrightarrow{\alpha} & \mathrm{Aut}(K^{\times t}) \\ h & \mapsto & ((k_i)_i \mapsto (k_{ih^-})_i) \end{array}$$

Mit anderen Worten, es ist $((k_i)_i)^h = (k_{ih^-})_i$ für $(k_i)_i \in K^{[1,t]}$ und $h \in H$.

Für $h \in H$ ist in der Tat $h\alpha$ bijektiv, da beidseitig invertiert von $(h^-)\alpha$. Es ist $h\alpha$ ein Gruppenmorphismus wegen $((k_i)_i \cdot (\tilde{k}_i)_i)^h = ((k_i\tilde{k}_i)_i)^h = (k_{ih^-}\tilde{k}_{ih^-})_i = (k_{ih^-})_i \cdot \tilde{k}_{ih^-})_i = ((k_i)_i)^h \cdot ((\tilde{k}_i)_i)^h$ für $(k_i)_i\,,\, (\tilde{k}_i)_i \,\in\, K^{\times[1,t]}$. Schließlich ist α ein Gruppenmorphismus wegen $((k_i)_i)^{h\tilde{h}} = (k_{i(h\tilde{h})^-})_i = (k_{i\tilde{h}^-h^-})_i = ((k_{ih^-})_i)^{\tilde{h}} = (((k_i)_i)^h)^{\tilde{h}}$ für $(k_i)_i \in K^{\times[1,t]}$, i.e. $(h\tilde{h})\alpha = (h\alpha) \blacktriangle (\tilde{h}\alpha)$, wobei $h,\, \tilde{h} \,\in\, H$.

Sei nun

$$H \wr K \;:=\; H \underset{\alpha}{\ltimes} K^{\times[1,t]}$$

das *Kranzprodukt* von H mit K.

Es werden Elemente $(h,(k_i)_i),\, (\tilde{h},(\tilde{k}_i)_i) \,\in\, H \wr K$ also wie folgt multipliziert.

$$(h,(k_i)_i) \cdot (\tilde{h},(\tilde{k}_i)_i) \;=\; (h\tilde{h},(k_{i\tilde{h}^-}\tilde{k}_i)_i)\ .$$

Beispiel 17 Sei einmal $t = 2$ und $H := \mathrm{S}_2 \leqslant \mathrm{S}_2$. Sei $K := \mathrm{S}_3$.

```
H := SymmetricGroup(2);
K := SymmetricGroup(3);
W,a,b,c := WreathProduct(K,H);
print W;
print a;
print b;
print c;
```

Nun ist `W` die Gruppe $H \wr K = H \ltimes (K \times K)$, welche Ordnung $|H| \cdot |K|^2 = 2 \cdot 6^2 = 72$ hat.

Es beinhaltet `a` die beiden Gruppenmorphismen von K in den jeweiligen direkten Faktor des direkten Produkts $K \times K$, was wiederum ein Normalteiler von $H \wr K$ ist.

Es ist b der Gruppenmorphismus von H in den ersten Faktor des semidirekten Produkts, was Untergruppe von $H \wr K$ ist.

Es ist `c` der Projektionsmorphismus von $H \wr K$ nach H.

4 Die Kategorie zu einem verschränkten Modul

4.1 Kategorien

Definition 18 Eine *Kategorie* $\mathcal{C}$ besteht aus ([2])

- einer Menge von *Objekten* $\mathrm{Ob}(\mathcal{C})$,
- einer Menge von *Morphismen* $\mathrm{Mor}(\mathcal{C})$,
- einer Abbildung $\mathrm{i}_{\mathcal{C}} \colon \mathrm{Ob}(\mathcal{C}) \to \mathrm{Mor}(\mathcal{C})$,
- zwei Abbildungen $\mathrm{s}_{\mathcal{C}}, \mathrm{t}_{\mathcal{C}} : \mathrm{Mor}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C})$ und einer
- *Kompositionsabbildung*.

Hierbei schreiben wir für $X \in \mathrm{Ob}(\mathcal{C})$ auch $\mathrm{id} = \mathrm{id}_X := X\mathrm{i}_{\mathcal{C}}$ (identity).

Ferner schreiben wir für $f \in \mathrm{Mor}(\mathcal{C})$ auch $X \xrightarrow{f} Y$, falls $X = f\mathrm{s}_{\mathcal{C}}$ und $Y = f\mathrm{t}_{\mathcal{C}}$ gelten (source und target, also Start- und Zielobjekt).

Die genannte Kompositionsabbildung ordnet jedem Paar von Morphismen der Form $X \xrightarrow{f} Y \xrightarrow{g} Z$ sein *Kompositum* $X \xrightarrow{f \blacktriangle g} Z$ zu.

Dieses Kompositum wird oft auch kurz $X \xrightarrow{fg} Z$ geschrieben.

Die Eigenschaften (Cat 1–3) sollen gelten.

[2] Mengentheoretische Probleme werden nun außen vorgelassen und bei Bedarf mittels Universen wegdiskutiert.

(Cat 1) Es ist $X\mathrm{i}_{\mathcal{C}}\mathrm{s}_{\mathcal{C}} = X$ und $X\mathrm{i}_{\mathcal{C}}\mathrm{t}_{\mathcal{C}} = X$ für $X \in \mathrm{Ob}(\mathcal{C})$.

I.e. es ist $X \xrightarrow{\mathrm{id}_X} X$ für $X \in \mathrm{Ob}(\mathcal{C})$.

(Cat 2) Für $X \overset{f}{\to} Y$ ist $\mathrm{id}_X \blacktriangle f = f = f \blacktriangle \mathrm{id}_Y$.

(Cat 3) Für $X \overset{f}{\to} Y \overset{g}{\to} Z \overset{h}{\to} W$ ist $(f \blacktriangle g) \blacktriangle h = f \blacktriangle (g \blacktriangle h)$.

Ein Morphismus $X \overset{f}{\to} Y$ heißt *Isomorphismus*, falls es einen Morphismus $X \overset{g}{\leftarrow} Y$ mit $f \blacktriangle g = \mathrm{id}_X$ und mit $g \blacktriangle f = \mathrm{id}_Y$ gibt.

Beispiel 19

(1) Die Kategorie der Mengen und Abbildungen.

(2) Die Kategorie der Gruppen und Gruppenmorphismen.

(3) Die Kategorie der **R**-Vektorräume und **R**-linearen Abbildungen.

(4) Die Kategorie der topologischen Räume und stetigen Abbildungen.

(5) Die Kategorie der verschränkten Moduln und Morphismen verschränkter Moduln.

4.2 Konstruktion einer Kategorie zu einem verschränkten Modul

Definition 20 Sei $V = (M, G, \alpha, f)$ ein verschränkter Modul.

Sei die Kategorie $V\mathrm{Cat}$ definiert durch

- $\mathrm{Ob}(V\mathrm{Cat}) := G$,
- $\mathrm{Mor}(V\mathrm{Cat}) := G \underset{\alpha}{\ltimes} M$,
- $g\,\mathrm{i}_{V\mathrm{Cat}} = (g, 1)$ für $g \in G$, i.e. $\mathrm{id}_g = (g, 1)$,
- $(g, m)\mathrm{s}_{V\mathrm{Cat}} := g$ und $(g, m)\mathrm{t}_{V\mathrm{Cat}} := g(mf)$ für $(g, m) \in \mathrm{Mor}(V\mathrm{Cat})$, i.e. es verläuft $g \xrightarrow{(g,m)} g(mf)$,
- und die Komposition, die

$$g \xrightarrow{(g,m)} g(mf) \xrightarrow{(g(mf),m')} g((mm')f)$$

zu

$$g \xrightarrow{(g,m)\,\blacktriangle\,(g(mf),m') := (g,mm')} g((mm')f)$$

komponiert.

Da nun Elemente von $\operatorname{Mor}(V\mathrm{Cat}) = G \underset{\alpha}{\ltimes} M$ sowohl komponiert als auch multipliziert werden können, empfiehlt sich hier, die Kompositionsoperation konsequent mit $(\blacktriangle)$ zu kennzeichnen.

Bemerkung 21 Sei G eine Gruppe. Sei $M \trianglelefteq G$. Wir erinnern an $\operatorname{Ob}(\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}) = G$ und $\operatorname{Mor}(\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}) = G \rtimes M$.

Seien $g,\, g' \in G$.

Ist $g' \notin gM$, dann gibt es keinen Morphismus von g nach g' in $\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}$.

Ist $g' \in gM$, dann ist der einzige Morphismus von g nach g' gegeben durch $g \xrightarrow{(g, g^{-} g')} g'$ in $\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}$.

Da genau dann $g' \in gM$ liegt, wenn $g \in g'M$ liegt, ist jeder Morphismus in $\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}$ ein Isomorphismus.

Beispiel 22 Wir setzen Beispiel 15 fort, in welchem $c = (1,2,3)$ und $M = \langle c \rangle \trianglelefteq \mathrm{S}_3 = G$ war.

Der dortige Gruppenmorphismus $\alpha\colon G \to \operatorname{Aut}(M)$ schickte $x \in G$ auf die Konjugation mit x, eingeschränkt auf M.

Es hat $\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}$ zum einen $\operatorname{Ob}(\mathrm{V}_{M \trianglelefteq G}) = G$, zum anderen $\operatorname{Mor}(\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}) = G \underset{\alpha}{\ltimes} M$.

Es handelt sich also um eine Kategorie mit 6 Objekten und 18 Morphismen.

Es werden e.g.

$$(1,2) \xrightarrow{((1,2),(1,2,3))} (1,3) \xrightarrow{((1,3),(1,2,3))} (2,3)$$

komponiert zu

$$(1,2) \xrightarrow{((1,2),(1,2,3))\,\blacktriangle\,((1,3),(1,2,3))\,=\,((1,2),(1,3,2))} (2,3)\ .$$

Folgendes Diagramm enthält die Objekte und die nichtidentischen Morphismen von $\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}$.

$$\begin{tikzcd}
 & \mathrm{id} \arrow[dl, shift left] \arrow[dr, shift left] & \\
(1,2,3) \arrow[ur, shift left] \arrow[rr, shift left] & & (1,3,2) \arrow[ul, shift left] \arrow[ll, shift left]
\end{tikzcd}
\qquad
\begin{tikzcd}
 & (1,2) \arrow[dl, shift left] \arrow[dr, shift left] & \\
(1,3) \arrow[ur, shift left] \arrow[rr, shift left] & & (2,3) \arrow[ul, shift left] \arrow[ll, shift left]
\end{tikzcd}$$

Beispiel 23 Wir setzen Beispiel 10 fort, in welchem $M = \mathrm{D}_8 = \langle (1,2,3,4), (1,3) \rangle \leqslant \mathrm{S}_4$ und $G = \operatorname{Aut}(M)$ war, wobei α die Identität war und f ein Element x auf κ_x^M schickt, also auf die Konjugation mit x.

Wir schreiben $a := (1,2,3,4)$ und $b := (1,3)$. Es ist $M = \langle a, b \rangle$.

Wir schreiben $c := (1,3,2,4)$ und $d := (3,4)$. Im genannten Beispiel wurde G von Magma isomorph ersetzt durch die Gruppe $\langle c, d\rangle \leqslant \mathrm{S}_4$, die wieder G genannt werden soll. Nach isomorpher Ersetzung ist $af = c^2$ und $bf = d$. Der Kern von f ist erzeugt von a^2. Ferner ist $a^c = a$ und $b^c = a^3 b$. Schließlich ist $a^d = a^{-1}$ und $b^d = b$. Dies alles erhalten wir wie folgt aus Magma.

```
a := M!(1,2,3,4);
b := M!(1,3);
c := G!(1,3,2,4);
d := G!(3,4);
print a@f, b@f;
print c^2, d;
print Kernel(f);
print a@(c@alpha), b@(c@alpha);
print a, a^-1*b;
print a@(d@alpha), b@(d@alpha);
print a^-1, b;
```

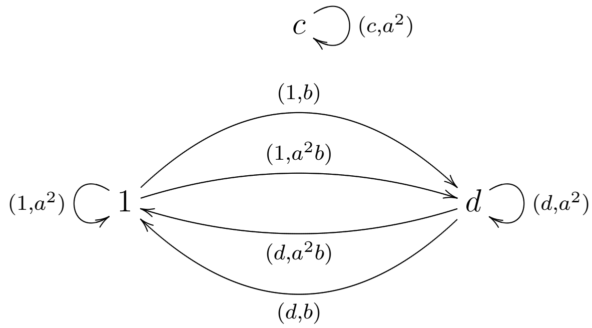
Wir wollen einen Ausschnitt der Kategorie $V := \mathrm{V}_{M\to\mathrm{Aut}(M)} = (M, G, f, \alpha)$ graphisch darstellen, eine sogenannte volle Teilkategorie, auf den Objekten 1, c, $d \in G = \mathrm{Ob}(V\mathrm{Cat})$.

Die Identitäten auf 1, c und d werden nicht dargestellt.

Es gibt keine Morphismen von 1 nach c und keine Morphismen von c nach 1. Es gibt keine Morphismen von d nach c und keine Morphismen von c nach d.

Es sind $(1, b)$ und $(1, a^2 b)$ Morphismen von 1 nach d. Es sind (d, b) und $(d, a^2 b)$ Morphismen von d nach 1.

Es ist $(1, a^2)$ ein nichtidentischer Morphismus von 1 nach 1. Es ist (d, a^2) ein nichtidentischer Morphismus von d nach d. Es ist (c, a^2) ein nichtidentischer Morphismus von c nach c.



Zum Beispiel wird $(1, b) \blacktriangle (d, a^2 b) = (1, b \cdot a^2 b) = (1, a^2)$.

Das Bild ist nun natürlich unvollständig: es fehlen die Objekte c^2, c^3, cd, $c^2 d$, $c^3 d$ sowie die Morphismen, die ein solches Objekt als Start- oder Zielobjekt haben.

5 Der symmetrische verschränkte Modul zu einer Kategorie

5.1 Funktoren

Definition 24 Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien.

Ein *Funktor* $\mathcal{C} \xrightarrow{F} \mathcal{D}$ besteht aus Abbildungen

- $\mathrm{Ob}(\mathcal{C}) \xrightarrow{\mathrm{Ob}(F)} \mathrm{Ob}(\mathcal{D})$
- und $\mathrm{Mor}(\mathcal{C}) \xrightarrow{\mathrm{Mor}(F)} \mathrm{Mor}(\mathcal{D})$.

Die Eigenschaften (Fu 1–3) sollen gelten.

(Fu 1) Es ist $\mathrm{id}_X \,\mathrm{Mor}(F) = \mathrm{id}_{X\,\mathrm{Ob}(F)}$ für $X \in \mathrm{Ob}(\mathcal{C})$.

(Fu 2) Sei $X \xrightarrow{u} Y$ ein Morphismus in $\mathcal{C}$. Dann ist $X\,\mathrm{Ob}(F) \xrightarrow{u\,\mathrm{Mor}(F)} Y\,\mathrm{Ob}(F)$ in $\mathcal{D}$.

(Fu 3) Für $X \xrightarrow{u} Y \xrightarrow{v} Z$ in $\mathcal{C}$ ist $(u \blacktriangle v)\,\mathrm{Mor}(F) = (u\,\mathrm{Mor}(F)) \blacktriangle (v\,\mathrm{Mor}(F))$.

Häufig schreibt man kurz $F := \mathrm{Ob}(F)$ und $F := \mathrm{Mor}(F)$. Dann werden (Fu 1–3) zu:

(Fu 1) Es ist $\mathrm{id}_X F = \mathrm{id}_{XF}$ für $X \in \mathrm{Ob}(\mathcal{C})$.

(Fu 2) Es wird $X \xrightarrow{u} Y$ in $\mathcal{C}$ auf $XF \xrightarrow{uF} YF$ in $\mathcal{D}$ abgebildet.

(Fu 3) Für $X \xrightarrow{u} Y \xrightarrow{v} Z$ in $\mathcal{C}$ ist $(u \blacktriangle v)F = (uF) \blacktriangle (vF)$.

Sind $\mathcal{C}$, $\mathcal{D}$ und $\mathcal{E}$ Kategorien und sind $\mathcal{C} \xrightarrow{F} \mathcal{D} \xrightarrow{F'} \mathcal{E}$ Funktoren, dann ist auch ihr Kompositum $\mathcal{C} \xrightarrow{F \blacktriangle F'} \mathcal{E}$ ein Funktor, für welches $\mathrm{Ob}(F \blacktriangle F') := \mathrm{Ob}(F) \blacktriangle \mathrm{Ob}(F')$ und $\mathrm{Ob}(F \blacktriangle F') := \mathrm{Ob}(F) \blacktriangle \mathrm{Ob}(F')$ gesetzt wird.

Ein Funktor F heißt *Autofunktor von* $\mathcal{C}$, wenn er von $\mathcal{C}$ nach $\mathcal{C}$ verläuft und $\mathrm{Ob}(F)$ und $\mathrm{Mor}(F)$ bijektiv sind. ([3])

E.g. ist $\mathrm{id}_{\mathcal{C}}$ mit $\mathrm{Ob}(\mathrm{id}_{\mathcal{C}}) := \mathrm{id}_{\mathrm{Ob}(\mathcal{C})}$ und $\mathrm{Mor}(\mathrm{id}_{\mathcal{C}}) := \mathrm{id}_{\mathrm{Mor}(\mathcal{C})}$ ein Autofunktor von $\mathcal{C}$.

Ist F ein Autofunktor, dann auch F^-, bestehend aus $\mathrm{Ob}(F^-) := \mathrm{Ob}(F)^-$ und $\mathrm{Mor}(F^-) := \mathrm{Mor}(F)^-$.

Insgesamt bildet die Menge

$$\mathrm{Aut}(\mathcal{C})$$

der Autofunktoren von $\mathcal{C}$ zusammen mit der Komposition als Multiplikation und $\mathrm{id}_{\mathcal{C}}$ als neutralem Element eine Gruppe.

[3] An dieser Stelle sollte man auch die Eigenschaften “voll” und “treu” erwähnen, wenn man größere Allgemeinheit anstrebt.

Beispiel 25 Sei Grp die Kategorie aus Gruppen und Gruppenmorphismen.

Für eine Gruppe G sei ihre *Kommutatoruntergruppe* durch

$$G^{(1)} \;:=\; \langle x^- y^- xy \colon x,\, y \,\in\, G\rangle \trianglelefteqslant G$$

gegeben. Sei $G^{\mathrm{ab}} := G/G^{(1)}$.

Es ist G^{ab} abelsch, da für $x,\, y \,\in\, G$ sich

$$(xG^{(1)})(yG^{(1)}) \;=\; xyG^{(1)} \;=\; yxG^{(1)} \;=\; (yG^{(1)})(xG^{(1)})$$

ergibt, weil $(yx)^- xy \in G^{(1)}$ liegt.

Für einen Gruppenmorphismus $G \xrightarrow{f} H$ sei

$$\begin{array}{rcl} G^{\mathrm{ab}} & \xrightarrow{f^{\mathrm{ab}}} & H^{\mathrm{ab}} \\ xG^{(1)} & \mapsto & xfH^{(1)}\ . \end{array}$$

Wegen $G^{(1)}f \leqslant H^{(1)}$ ist das ein wohldefinierter Gruppenmorphismus.

Es ist

$$\begin{array}{rcl} \mathrm{Grp} & \xrightarrow{(-)^{\mathrm{ab}}} & \mathrm{Grp} \\ (G \xrightarrow{f} H) & \mapsto & (G^{\mathrm{ab}} \xrightarrow{f^{\mathrm{ab}}} H^{\mathrm{ab}}) \end{array}$$

ein Funktor von Grp nach Grp.

Wir wollen mittels Magma nachrechnen, daß $(-)^{\mathrm{ab}}$ kein Autofunktor ist. Genauer, wir wollen nachrechnen, daß dieser Funktor auf den Morphismen nicht injektiv ist.

```
G := SymmetricGroup(3);
c := G!(1,2,3);
d := G!(1,2);
sigma := hom< G->G | x :-> x^c >;
id_G  := hom< G->G | x :-> x   >;
print d eq d@sigma;
print id_G eq sigma;
N := CommutatorSubgroup(G);
Gab,rho := quo<G | N>;
print rho;
id_Gab := hom< Gab->Gab | x :-> x >;
print sigma * rho eq rho * id_Gab;
print id_G  * rho eq rho * id_Gab;
```

Natürlich hätte man auch argumentieren können, daß $(-)^{\mathrm{ab}}$ auf Objekten nicht surjektiv ist, da S_3 als nichtabelsche Gruppe nicht im Bild liegt.

Lemma 26 *Sei G eine endliche Gruppe. Sei $M \trianglelefteqslant G$. Schreibe $t := |G|/|M| = |G/M|$.*

Wähle $g_i \in G$ für $i \in [1,t]$ mit $G = \bigsqcup_{i\in[1,t]} g_i M$.

Wir betrachten die symmetrischen Gruppen $H := \mathrm{S}_t \leqslant \mathrm{S}_t$ und $K := \mathrm{S}_M$.

Wir bilden das Kranzprodukt $H \wr K = \mathrm{S}_t \wr \mathrm{S}_M$; cf. Definition 16.

Dieses hat Ordnung $|\mathrm{S}_t \wr \mathrm{S}_M| = t! \cdot |M|!^{\,t}$.

Darin ist $(\psi, (\varphi_i)_i) \cdot (\tilde{\psi}, (\tilde{\varphi}_i)_i) = (\psi \blacktriangle \tilde{\psi}, (\varphi_{i\psi^-} \blacktriangle \tilde{\varphi}_i)_i)$ für $(\psi, (\varphi_i)_i),\ (\tilde{\psi}, (\tilde{\varphi}_i)_i) \in \mathrm{S}_t \wr \mathrm{S}_M$.

Die Elemente von $\mathrm{S}_t \wr \mathrm{S}_M$ sind von der Form $(\psi, (\varphi_i)_i)$, mit $\psi \in \mathrm{S}_t$ und $\varphi_i \in \mathrm{S}_M$ für $i \in [1,t]$. Es ist also φ_i eine bijektive Abbildung von M nach M.

Wir haben den Gruppenisomorphismus

$$
\begin{array}{rcl}
\mathrm{S}_t \wr \mathrm{S}_M & \overset{\xi}{\underset{\sim}{\to}} & \mathrm{Aut}(\mathrm{V}_{M\trianglelefteqslant G}\,\mathrm{Cat}) \\
(\psi, (\varphi_i)_i) & \mapsto & \left(\begin{array}{ccc} g_j\, m & & g_{j\psi}(m\varphi_j) \\ {\scriptstyle (g_j\, m,\, m^- m')}\big\downarrow & \mapsto & \big\downarrow{\scriptstyle (g_{j\psi}(m\varphi_{j\psi}),\, (m\varphi_{j\psi})^-(m'\varphi_{j\psi}))} \\ g_j\, m' & & g_{j\psi}\,(m'\varphi_{j\psi}) \end{array} \right) .
\end{array}
$$

Hierbei sind $j \in [1,t]$ und $m,\ m' \in M$.

Insbesondere ist auch $|\,\mathrm{Aut}(\mathrm{V}_{M\trianglelefteqslant G}\,\mathrm{Cat})| = t! \cdot |M|!^{\,t}$.

Beweis.

Zeigen wir, daß das behauptete Bild ein Funktor ist.

Sei $j \in [1,t]$. Sei $m \in M$. Die Identität auf $g_j\, m$ ist $(g_j m, 1)$ und wird auf $(g_{j\psi}(m\varphi_{j\psi}),\ (m\varphi_{j\psi})^-(m\varphi_{j\psi})) = (g_{j\psi}(m\varphi_{j\psi}),\ 1)$ geschickt, also auf die Identität auf $g_{j\psi}(m\varphi_{j\psi})$.

Sei $j \in [1,t]$. Seien $m,\ m',\ m'' \in M$. Wir betrachten die Morphismen

$$g_j\, m \xrightarrow{(g_j\, m,\, m^- m')} g_j\, m' \xrightarrow{(g_j\, m',\, m'^- m'')} g_j\, m'' \ .$$

Das Bild ihres Kompositums

$$(g_j\, m,\ m^- m') \blacktriangle (g_j\, m',\ m'^- m'') \ = \ (g_j\, m,\ m^- m'')$$

ist $(g_{j\psi}(m\varphi_{j\psi}),\ (m\varphi_{j\psi})^-(m''\varphi_{j\psi}))$.

Auf der anderen Seite berechnet sich das Kompositum ihrer Bilder zu

$$
\begin{array}{rl}
& (g_{j\psi}(m\varphi_{j\psi}),\ (m\varphi_{j\psi})^-(m'\varphi_{j\psi})) \blacktriangle (g_{j\psi}(m'\varphi_{j\psi}),\ (m'\varphi_{j\psi})^-(m''\varphi_{j\psi})) \\
= & (g_{j\psi}(m\varphi_{j\psi}),\ (m\varphi_{j\psi})^-(m''\varphi_{j\psi})) \ .
\end{array}
$$

Die Resultate stimmen überein.

Zeigen wir, daß das behauptete Bild ein Autofunktor ist.

Zeigen wir die Bijektivität auf der Objektmenge G. Da diese endlich ist, genügt es, die Injektivität zu zeigen. Seien $j,\ \tilde{j} \in [1,t]$. Seien $m,\ \tilde{m} \in M$. Seien $j,\ \tilde{j} \in [1,t]$ und $m,\ \tilde{m} \in M$ mit übereinstimmenden Bildern von $g_j\, m$ und $g_{\tilde{j}}\, \tilde{m}$ gegeben, i.e. sei $g_{j\psi}(m\varphi_{j\psi}) = g_{\tilde{j}\psi}(\tilde{m}\varphi_{\tilde{j}\psi})$. Dann ist $g_{j\psi}M = g_{\tilde{j}\psi}M$ und also $j\psi = \tilde{j}\psi$. Da ψ injektiv ist, folgt $j = \tilde{j}$. Aus $g_{j\psi}(m\varphi_{j\psi}) = g_{j\psi}(\tilde{m}\varphi_{j\psi})$ folgt nun $m\varphi_{j\psi} = \tilde{m}\varphi_{j\psi}$, wegen $\varphi_{j\psi}$ injektiv also $m = \tilde{m}$.

Zwei Morphismen, die auf denselben Morphismus abgebildet werden, haben demnach dasselbe Start- und dasselbe Zielobjekt, sind also dank Bemerkung 21 gleich. Somit ist die Abbildung auch auf der Morphismenmenge $G \ltimes M$ injektiv. Da diese Menge endlich ist, zeigt dies die Bijektivität der Abbildung auf der Morphismenmenge.

Zeigen wir, daß ξ ein Gruppenmorphismus ist.

Seien $(\psi, (\varphi_i)_i),\ (\tilde{\psi}, (\tilde{\varphi}_i)_i) \in \mathrm{S}_t \wr \mathrm{S}_M$ gegeben. Es genügt zu zeigen, daß das Bild ihres Produktes auf Objekten genauso operiert wie das Produkt ihrer Bilder, denn die Operation auf den Objekten legt hier die Operation auf den Morphismen fest; cf. Bemerkung 21.

Sei $j \in [1,t]$ und $m \in M$ gegeben.

Das Produkt der Bilder dieser beiden Elemente aus $\mathrm{S}_t \wr \mathrm{S}_M$, i.e. ihr Kompositum, schickt das Objekt $g_j\, m$ in einem ersten Schritt auf $g_{j\psi}(m\varphi_{j\psi})$, und dieses schließlich auf $g_{(j\psi)\tilde{\psi}}((m\varphi_{j\psi})\tilde{\varphi}_{(j\psi)\tilde{\psi}})$.

Das Bild des Produktes $(\psi, (\varphi_i)_i) \cdot (\tilde{\psi}, (\tilde{\varphi}_i)_i) = (\psi \blacktriangle \tilde{\psi}, (\varphi_{i\tilde{\psi}^-} \blacktriangle \tilde{\varphi}_i)_i)$ dieser beiden Elemente schickt das Objekt $g_j\, m$ auf

$$g_{j(\psi \blacktriangle \tilde{\psi})}\,(m(\varphi_{(j(\psi \blacktriangle \tilde{\psi}))\tilde{\psi}^-} \blacktriangle \tilde{\varphi}_{j(\psi \blacktriangle \tilde{\psi})})) \;=\; g_{(j\psi)\tilde{\psi}}\,((m\varphi_{j\psi})\tilde{\varphi}_{(j\psi)\tilde{\psi}})\ .$$

Die Resultate stimmen überein.

Zeigen wir, daß ξ injektiv ist. Hierzu sollten wir nachweisen, daß der Kern von ξ nur aus dem neutralen Element besteht.

Sei also $(\psi, (\varphi_i)_i) \in \mathrm{S}_t \wr \mathrm{S}_M$ derart gegeben, daß sein Bild der identische Funktor ist. Für $j \in [1,t]$ und $m \in M$ wird also $g_j\, m$ auf $g_{j\psi}(m\varphi_{j\psi}) = g_j\, m$ geschickt. Da also stets $g_{j\psi}M = g_jM$ ist, ist $\psi = \mathrm{id}_{[1,t]}$. Da nun stets $g_j(m\varphi_j) = g_j\, m$ ist, ist $\varphi_j = \mathrm{id}_M$ für $j \in [1,t]$. Folglich ist $(\psi, (\varphi_i)_i) = (\mathrm{id}_{[1,t]}\, , (\mathrm{id}_M)_i)$ das neutrale Element in $\mathrm{S}_t \wr \mathrm{S}_M$.

Zeigen wir, daß ξ surjektiv ist.

Sei $F \in \mathrm{Aut}(\mathrm{V}_{M \trianglelefteq G}\, \mathrm{Cat})$.

Sei $\psi \in \mathrm{S}_t$ definiert durch $(g_jF)M =: g_{j\psi}M$ für $j \in [1,t]$. Um zu zeigen, daß ψ bijektiv ist, genügt es zu zeigen, daß ψ injektiv ist. Seien $j,\ \tilde{j} \in [1,t]$ gegeben mit $(g_jF)M = (g_{\tilde{j}}F)M$. Dann gibt es ein $m \in M$ mit $(g_jF)m = g_{\tilde{j}}F$. Also gibt es einen Morphismus (g_jF, m) von g_jF nach $g_{\tilde{j}}F$. Das Bild unter F^- von diesem Morphismus geht also von g_j nach $g_{\tilde{j}}$. Somit gibt es auch ein $m' \in M$ mit $g_j\, m' = g_{\tilde{j}}$. Also ist $g_jM = g_{\tilde{j}}M$. Somit ist $j = \tilde{j}$.

Für $j \in [1,t]$ sei nun $\varphi_{j\psi}$ definiert durch $m\varphi_{j\psi} := g_{j\psi}^- \cdot ((g_j\, m)F)$. Da $(g_jF)M = g_{j\psi}M$, liegt $m\varphi_{j\psi}$ tatsächlich in M. Um zu zeigen, daß $\varphi_{j\psi}$ bijektiv ist, genügt es zu zeigen, daß

$\varphi_{j\psi}$ injektiv ist. Seien $m, \tilde{m} \in M$ gegeben mit $g_{j\psi}^{-} \cdot ((g_j\, m)F) = g_{j\psi}^{-} \cdot ((g_j\, \tilde{m})F)$. Dann ist $(g_j\, m)F = (g_j\, \tilde{m})F$. Da F auf der Objektmenge bijektiv ist, folgt $g_j\, m = g_j\, \tilde{m}$ und schließlich $m = \tilde{m}$.

Also ist $(\psi, (\varphi_i)_i) \in \mathrm{S}_t \wr \mathrm{S}_M$.

Wir haben noch zu zeigen, daß $(\psi, (\varphi_i)_i)$ tatsächlich auf F abgebildet wird. Da die Operation eines Autofunktors gemäß Bemerkung 21 durch seine Operation auf den Objekten bestimmt ist, genügt es, die Operation auf den Objekten von F und vom Bild dieses Elements zu vergleichen. Sei $j \in [1, t]$. Sei $m \in M$. Das Bild von $(\psi, (\varphi_i)_i)$ schickt $g_j\, m$ in der Tat nach

$$g_{j\psi}(m\varphi_{j\psi}) \;=\; g_{j\psi} \cdot g_{j\psi}^{-} \cdot ((g_j\, m)F) \;=\; (g_j\, m)F \;.$$

□

5.2 Transformationen

Definition 27 Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien.

Seien $\mathcal{C} \xrightarrow{F} \mathcal{D}$ und $\mathcal{C} \xrightarrow{F'} \mathcal{D}$ Funktoren.

Eine *Transformation* a von F nach F' ist ein Tupel von Morphismen

$$(XF \xrightarrow{Xa} XF')_{X \in \mathrm{Ob}(\mathcal{C})} ,$$

für welches

$$Xa \blacktriangle uF' \;=\; uF \blacktriangle Ya$$

gilt für alle Morphismen $X \xrightarrow{u} Y$ von $\mathcal{C}$.

$$\begin{tikzcd} XF \arrow[r, "Xa"] \arrow[d, "uF"'] & XF' \arrow[d, "uF'"] \\ YF \arrow[r, "Ya"] & YF' \end{tikzcd}$$

Diese Eigenschaft heiße auch die *Natürlichkeit* des Tupels $(Xa)_{X \in \mathrm{Ob}\,\mathcal{C}}$.

Oft wird eine Transformation a von F nach F' wie folgt veranschaulicht.

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left, "F"] \arrow[r, bend right, "F'"'] \arrow[r, phantom, "a\Downarrow"] & \mathcal{D} \end{tikzcd}$$

Sind Funktoren und Transformationen

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left=60, "F"] \arrow[r, "F'" near end] \arrow[r, bend right=60, "F''"'] \arrow[r, phantom, bend left=30, "a\Downarrow"] \arrow[r, phantom, bend right=30, "a'\Downarrow"] & \mathcal{D} \end{tikzcd}$$

gegeben, so definieren wir die *vertikale Komposition*

$$a \blacktriangle a' \;=\; (Xa)_{X \in \operatorname{Ob} \mathcal{C}} \blacktriangle (Xa')_{X \in \operatorname{Ob} \mathcal{C}} \;:=\; (Xa \blacktriangle Xa')_{X \in \operatorname{Ob} \mathcal{C}} \;,$$

i.e. $X(a \blacktriangle a') = Xa \blacktriangle Xa'$ für $X \in \operatorname{Ob} \mathcal{C}$.

Ferner sei $\mathrm{id}_F := (\mathrm{id}_{XF})_{X \in \operatorname{Ob} \mathcal{C}}$.

Eine Transformation a von F nach F' heiße *Isotransformation*, wenn Xa ein Isomorphismus ist für alle $X \in \operatorname{Ob} \mathcal{C}$. Diesenfalls ist $a^- := ((Xa)^-)_{X \in \operatorname{Ob} \mathcal{C}}$ eine Isotransformation von F' nach F. Es ist $a \blacktriangle a^- = \mathrm{id}_F$ und $a^- \blacktriangle a = \mathrm{id}_{F'}$.

Beispiel 28 Wir setzen Beispiel 25 fort.

Wir definieren eine Transformation von $\mathrm{id}_{\mathrm{Grp}}$ nach $(-)^{\mathrm{ab}}$.

Für eine Gruppe G sei $Ga : G \to G^{\mathrm{ab}} = G/G^{(1)}$, $g \mapsto gG^{(1)}$.

Das Tupel $(Ga)_{G \in \operatorname{Ob} \mathrm{Grp}}$ ist natürlich und damit eine Transformation, da für jeden Gruppenmorphismus $G \xrightarrow{u} H$ sich

$$Ga \blacktriangle u^{\mathrm{ab}} \;=\; u \blacktriangle Ha$$

ergibt, denn für $g \in G$ ist zum einen $g(Ga \blacktriangle u^{\mathrm{ab}}) = (gG^{(1)})u^{\mathrm{ab}} = guH^{(1)}$, zum anderen $g(u \blacktriangle Ha) = (gu)(Ha) = guH^{(1)}$.

Es ist a keine Isotransformation, wie wir mit Magma verifizieren wollen.

```
G := SymmetricGroup(3);
N := CommutatorSubgroup(G);
Gab,rho := quo<G | N>;
print Kernel(rho);
```

Bemerkung 29 (und Definition) Seien $\mathcal{C}$, $\mathcal{D}$ und $\mathcal{E}$ Kategorien. Seien Funktoren und Transformationen

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left, "F"] \arrow[r, bend right, "F'"'] \arrow[r, phantom, "a\Downarrow"] & \mathcal{D} \arrow[r, bend left, "G"] \arrow[r, bend right, "G'"'] \arrow[r, phantom, "b\Downarrow"] & \mathcal{E} \end{tikzcd}$$

gegeben.

Es ist also a eine Transformation von F nach F'. Dann ist $aG := (XaG)_{X \in \operatorname{Ob} \mathcal{C}}$ eine Transformation von FG nach $F'G$.

Es ist also b eine Transformation von G nach G'. Dann ist $Fb := (XFb)_{X \in \operatorname{Ob} \mathcal{C}}$ eine Transformation von FG nach FG'.

Wir setzen das *horizontale Kompositum* zu

$$a * b \;:=\; aG \blacktriangle F'b \;=\; Fb \blacktriangle aG'$$

Es ist also $a * b$ eine Transformation von FG nach $F'G'$.

Die darin behauptete Gleichheit gilt, da sich für $X \in \mathrm{Ob}(\mathcal{C})$

$$\begin{array}{rcl} X(aG \blacktriangle F'b) & = & (Xa)G \blacktriangle (XF')b \\ & = & (XF)b \blacktriangle (Xa)G' \\ & = & X(Fb \blacktriangle aG') \end{array}$$

ergibt wegen der Natürlichkeit von b.

Lemma 30 Seien $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ und $\mathcal{F}$ Kategorien.

(1) Seien Funktoren und Transformationen

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left=50, "F"] \arrow[r, "F'" description] \arrow[r, bend right=50, "F''" description] \arrow[r, bend right=90, "F'''"'] & \mathcal{D} \end{tikzcd}$$

$$a \Downarrow,\quad a' \Downarrow,\quad a'' \Downarrow$$

Dann ist $a \blacktriangle (a' \blacktriangle a'') = (a \blacktriangle a') \blacktriangle a''$.

(2) Seien Funktoren und Transformationen

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left, "F"{name=F}] \arrow[r, bend right, "F'"'{name=Fp}] \arrow[from=F, to=Fp, Rightarrow, "a"'] & \mathcal{D} \arrow[r, bend left, "G"{name=G}] \arrow[r, bend right, "G'"'{name=Gp}] \arrow[from=G, to=Gp, Rightarrow, "b"'] & \mathcal{E} \arrow[r, bend left, "H"{name=H}] \arrow[r, bend right, "H'"'{name=Hp}] \arrow[from=H, to=Hp, Rightarrow, "c"'] & \mathcal{E} \end{tikzcd}$$

gegeben. Dann ist $a * (b * c) = (a * b) * c$.

(3) Seien Funktoren und eine Transformation

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left, "F"{name=F}] \arrow[r, bend right, "F'"'{name=Fp}] \arrow[from=F, to=Fp, Rightarrow, "a"'] & \mathcal{D} \end{tikzcd}$$

gegeben. Dann ist $\mathrm{id}_{\mathrm{id}_\mathcal{C}} * a = a$ und $a * \mathrm{id}_{\mathrm{id}_\mathcal{D}} = a$.

(4) Seien Funktoren und Transformationen

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left=50, "F"{name=F}] \arrow[r, "F'" description, ""{name=Fp}] \arrow[r, bend right=50, "F''"'{name=Fpp}] \arrow[from=F, to=Fp, Rightarrow, "a"'] \arrow[from=Fp, to=Fpp, Rightarrow, "a'"'] & \mathcal{D} \arrow[r, bend left=50, "G"{name=G}] \arrow[r, "G'" description, ""{name=Gp}] \arrow[r, bend right=50, "G''"'{name=Gpp}] \arrow[from=G, to=Gp, Rightarrow, "b"'] \arrow[from=Gp, to=Gpp, Rightarrow, "b'"'] & \mathcal{E} \end{tikzcd}$$

gegeben. Dann ist $(a * b) \blacktriangle (a' * b') = (a \blacktriangle a') * (b \blacktriangle b')$.

Beweis.

Ad (1). Für $X \in \mathrm{Ob}\,\mathcal{C}$ ist

$$\begin{array}{rclcl} X(a \blacktriangle (a' \blacktriangle a'')) & = & Xa \blacktriangle X(a' \blacktriangle a'') & = & Xa \blacktriangle (Xa' \blacktriangle Xa'') \\ & = & (Xa \blacktriangle Xa') \blacktriangle Xa'' & = & X(a \blacktriangle a') \blacktriangle Xa'' \\ & = & X((a \blacktriangle a') \blacktriangle a'') \; . & & \end{array}$$

Ad (2). Für $X \in \mathrm{Ob}\,\mathcal{C}$ ist

$$\begin{array}{rclcl} X(a * (b * c)) & = & XaGH \blacktriangle XF'(b * c) & = & XaGH \blacktriangle XF'bH \blacktriangle XF'G'c \\ & = & X(a * b)H \blacktriangle XF'G'c & = & X((a * b) * c) \; . \end{array}$$

Ad (3). Für $X \in \mathrm{Ob}\,\mathcal{C}$ ist

$$X(\mathrm{id}_{\mathrm{id}_{\mathcal{C}}} * a) \;=\; X\,\mathrm{id}_{\mathrm{id}_{\mathcal{C}}} F \blacktriangle X\,\mathrm{id}_{\mathcal{C}}\, a \;=\; \mathrm{id}_X F \blacktriangle Xa \;=\; \mathrm{id}_{XF} \blacktriangle Xa \;=\; Xa$$

und

$$X(a * \mathrm{id}_{\mathrm{id}_{\mathcal{D}}}) \;=\; Xa\,\mathrm{id}_{\mathcal{D}} \blacktriangle XF'\,\mathrm{id}_{\mathrm{id}_{\mathcal{D}}} \;=\; Xa \blacktriangle \mathrm{id}_{XF'\,\mathrm{id}_{\mathcal{D}}} \;=\; Xa \; .$$

Ad (4). Für $X \in \mathrm{Ob}\,\mathcal{C}$ ist

$$\begin{array}{rclcl} X((a * b) \blacktriangle (a' * b')) & = & X(a * b) \blacktriangle X(a' * b') & = & X(a * b) \blacktriangle X(a' * b') \\ & = & XaG \blacktriangle XF'b \blacktriangle Xa'G' \blacktriangle XF''b' & \overset{b \text{ nat.}}{=} & XaG \blacktriangle Xa'G \blacktriangle XF''b \blacktriangle XF''b' \\ & = & (Xa \blacktriangle Xa')G \blacktriangle (XF''b \blacktriangle XF''b') & = & X(a \blacktriangle a')G \blacktriangle XF''(b \blacktriangle b') \\ & = & X(a \blacktriangle a') * (b \blacktriangle b') \; . & & \end{array}$$

□

Lemma 31 *Sei $\mathcal{C}$ eine Kategorie. Dann ist*

$$\{\, \mathrm{id}_{\mathcal{C}} \xrightarrow{a} F \;:\; \textit{es ist } F \in \mathrm{Aut}(\mathcal{C}) \textit{ und } a \textit{ eine Isotransformation} \,\}$$

eine Gruppe, mit der horizontalen Komposition $(*)$ als Multiplikation.

Für a und a' aus dieser Menge ist $\mathrm{id}_{\mathcal{C}} \xrightarrow{a * a'} FF'$.

Beweis. Sind $F,\, F' \in \mathrm{Aut}(\mathcal{C})$ und sind $\mathrm{id}_{\mathcal{C}} \xrightarrow{a} F$ und $\mathrm{id}_{\mathcal{C}} \xrightarrow{a'} F'$ Isotransformationen, dann ist $\mathrm{id}_{\mathcal{C}} \xrightarrow{a * a'} FF'$ mit $FF' \in \mathrm{Aut}(\mathcal{C})$. Ferner ist mit a' auch Fa' eine Isotransformation. Somit ist auch $a * a' = a \blacktriangle Fa'$ eine Isotransformation.

Dank Lemma 30.(2, 3) ist die Multiplikation assoziativ und hat ein neutrales Element $\mathrm{id}_{\mathcal{C}} \xrightarrow{\mathrm{id}_{\mathrm{id}_{\mathcal{C}}}} \mathrm{id}_{\mathcal{C}}$.

Bleibt zu zeigen, daß zu einer Isotransformation $\mathrm{id}_{\mathcal{C}} \xrightarrow{a} F$ mit $F \in \mathrm{Aut}(\mathcal{C})$ ein Inverses bezüglich $(*)$ existiert. Schreibe $a^{*,-} := F^- a^- : \mathrm{id}_{\mathcal{C}} \to F^-$. Es wird

$$a * a^{*,-} \;=\; a \blacktriangle Fa^{*,-} \;=\; a \blacktriangle FF^- a^- \;=\; a \blacktriangle a^- \;=\; \mathrm{id}_{\mathrm{id}_{\mathcal{C}}}$$

und

$$a^{*,-} * a \;=\; a^{*,-} \blacktriangle F^- a \;=\; F^- a^- \blacktriangle F^- a \;=\; F^-(a^- \blacktriangle a) \;=\; F^-\,\mathrm{id}_F \;=\; \mathrm{id}_{\mathrm{id}_{\mathcal{C}}} \; .$$

□

5.3 Konstruktion des symmetrischen verschränkte Moduls

Definition 32 (und Behauptung) Sei $\mathcal{C}$ eine Kategorie. Sei $\mathrm{S}_\mathcal{C}$ der verschränkte Modul aus folgenden Bestandteilen.

Sei $(\mathrm{S}_\mathcal{C})^{\mathrm{Gruppe}} := \mathrm{Aut}(\mathcal{C})$, mit der Komposition von Autofunktoren als Multiplikation.

Sei $(\mathrm{S}_\mathcal{C})^{\mathrm{Modul}} := \{\, \mathrm{id}_\mathcal{C} \xrightarrow{a} F \;:\; \text{es ist } F \in \mathrm{Aut}(\mathcal{C}) \text{ und } a \text{ eine Isotransformation} \,\}$, mit der Multiplikation $(*)$; cf. Lemma 31.

Sei das Differential von $\mathrm{S}_\mathcal{C}$ erklärt durch

$$\begin{array}{rcl} (\mathrm{S}_\mathcal{C})^{\mathrm{Modul}} & \xrightarrow{\mathrm{f}_{\mathrm{S}_\mathcal{C}}} & (\mathrm{S}_\mathcal{C})^{\mathrm{Gruppe}} \\ (\mathrm{id}_\mathcal{C} \xrightarrow{a} F) & \mapsto & F \end{array}$$

Sei die Operation von $(\mathrm{S}_\mathcal{C})^{\mathrm{Gruppe}}$ auf $(\mathrm{S}_\mathcal{C})^{\mathrm{Modul}}$ gegeben durch

$$\begin{array}{rcl} (\mathrm{S}_\mathcal{C})^{\mathrm{Gruppe}} & \xrightarrow{\alpha_{\mathrm{S}_\mathcal{C}}} & \mathrm{Aut}((\mathrm{S}_\mathcal{C})^{\mathrm{Modul}}) \\ H & \mapsto & (a \mapsto H^- a H =: a^H)\ . \end{array}$$

Wir behaupten, daß dies in der Tat einen verschränkten Modul $\mathrm{S}_\mathcal{C}$ definiert.

Es heißt $\mathrm{S}_\mathcal{C}$ der *symmetrische verschränkte Modul* auf der Kategorie $\mathcal{C}$.

Der symmetrische verschränkte Modul auf einer Kategorie spielt dieselbe Rolle wie die symmetrische Gruppe auf einer Menge; cf. [**3**]. Den folgenden Beweis kenne ich aus [**3**].

Beweis. Dank 31 ist $\mathrm{f}_{\mathrm{S}_\mathcal{C}}$ ein Gruppenmorphismus.

Für $H \in (\mathrm{S}_\mathcal{C})^{\mathrm{Gruppe}}$ gibt $a \mapsto H^- a H$ einen Gruppenmorphismus von $(\mathrm{S}_\mathcal{C})^{\mathrm{Modul}}$ nach $(\mathrm{S}_\mathcal{C})^{\mathrm{Modul}}$, denn für $\mathrm{id}_\mathcal{C} \xrightarrow{a} F$ und $\mathrm{id}_\mathcal{C} \xrightarrow{a'} F'$ in $(\mathrm{S}_\mathcal{C})^{\mathrm{Modul}}$ wird

$$\begin{array}{rcl} H^-(a * a')H & = & H^-(a \blacktriangle Fa')H \;=\; H^- aH \blacktriangle H^- Fa'H \\ & = & (H^- aH)\blacktriangle(H^- FH)(H^- a'H) \;=\; (H^- aH) * (H^- a'H)\ . \end{array}$$

Dieser Gruppenmorphismus ist bijektiv, da er von $a \mapsto HaH^-$ beidseitig invertiert wird. Also ist $a \mapsto H^- aH$ in $\mathrm{Aut}((\mathrm{S}_\mathcal{C})^{\mathrm{Modul}})$.

Für $H,\ H' \in (\mathrm{S}_\mathcal{C})^{\mathrm{Gruppe}}$ erhalten wir das Kompositum $a \mapsto H^- aH \mapsto H'^- H^- aHH'$, und dies ist auch das Bild von HH'. Also ist $\alpha_{\mathrm{S}_\mathcal{C}}$ ein Gruppenmorphismus.

Ad (VM 1). Sei $\mathrm{id}_\mathcal{C} \xrightarrow{a} F$ in $(\mathrm{S}_\mathcal{C})^{\mathrm{Modul}}$. Sei $H \in (\mathrm{S}_\mathcal{C})^{\mathrm{Gruppe}}$. Es wird

$$(\mathrm{id}_\mathcal{C} \xrightarrow{a^H} H^- FH)\mathrm{f}_{\mathrm{S}_\mathcal{C}} \;=\; H^- FH \;=\; F^H \;=\; ((\mathrm{id}_\mathcal{C} \xrightarrow{a} F)\mathrm{f}_{\mathrm{S}_\mathcal{C}})^H\ .$$

Ad (VM 2). Seien $\mathrm{id}_\mathcal{C} \xrightarrow{a} F$ und $\mathrm{id}_\mathcal{C} \xrightarrow{b} G$ in $(\mathrm{S}_\mathcal{C})^{\mathrm{Modul}}$. Zum einen wird

$$\begin{array}{rcl} a^b & = & b^{*,-} * a * b \;=\; G^- b^- * a * b \;=\; G^- b^- \blacktriangle G^-(a * b) \\ & = & G^- b^- \blacktriangle\, G^-(b \blacktriangle aG) \;=\; G^- b^- \blacktriangle G^- b \blacktriangle G^- aG \;=\; G^- aG\ , \end{array}$$

zum anderen wird

$$a^{b\,\mathrm{fs}_{\mathcal{C}}} \;=\; a^G \;=\; G^- a G\;,$$

was dasselbe ist. ▫

Lemma 33 *Sei G eine endliche Gruppe. Sei $M \trianglelefteq G$. Schreibe $t := |G|/|M| = |G/M|$.*

Wähle $g_i \in G$ für $i \in [1,t]$ mit $G = \bigsqcup_{i\in[1,t]} g_i M$.

Wir betrachten die symmetrischen Gruppen $H := \mathrm{S}_t \leqslant \mathrm{S}_t$ und $K := \mathrm{S}_M$.

Wir bilden das Kranzprodukt $H \wr K = \mathrm{S}_t \wr \mathrm{S}_M$; cf. Definition 16.

Dieses hat den Normalteiler $\mathrm{S}_M^{\times t}$.

Dann ist der verschränkte Modul

$$\mathrm{S}_{\mathrm{V}_{M \trianglelefteq G}\,\mathrm{Cat}}$$

isomorph zum verschränkten Modul

$$\mathrm{V}_{\mathrm{S}_M^{\times t} \trianglelefteq \mathrm{S}_t \wr \mathrm{S}_M}\;.$$

> In diesem Sinne kann eine Untersuchung von $\mathrm{S}_{\mathrm{V}_{M\trianglelefteq G}\,\mathrm{Cat}}$, i.e. eine Untersuchung des symmetrischen verschränkten Moduls der Kategorie, die zu einem verschränkten Modul der Form $\mathrm{V}_{M\trianglelefteq G}$ gehört, nichts Neues zutagefördern. Nichtsdestoweniger basiert die Grundidee des Programms `SymmetricCrossedModule` des nächsten Abschnitts §5.4 auf diesem einfachen Fall.

Beweis. Dank Lemma 26 und Bemerkung 13 genügt es zu zeigen, daß das Differential von $\mathrm{S}_{\mathrm{V}_{M\trianglelefteq G}\,\mathrm{Cat}}$ injektiv ist und als Bild den Normalteiler $(\mathrm{S}_M^{\times t})\xi$ von $(\mathrm{S}_t \wr \mathrm{S}_M)\xi$ hat.

Schreibe $\mathcal{C} := \mathrm{V}_{M\trianglelefteq G}\,\mathrm{Cat}$.

Zeigen wir die Injektivität des Differentials von $\mathrm{S}_{\mathcal{C}}$. Sei $F \in \mathrm{Aut}(\mathcal{C})$. Seien $\mathrm{id}_{\mathcal{C}} \xrightarrow{a} F$ und $\mathrm{id}_{\mathcal{C}} \xrightarrow{\tilde a} F$ Isotransformationen. Wir haben $a \overset{!}{=} \tilde a$ zu zeigen. Sei $g \in \mathrm{Ob}(\mathcal{C}) = G$. Wir haben $ga \overset{!}{=} g\tilde a$ zu zeigen. Nun sind aber ga und $g\tilde a$ beides Morphismen von $g\,\mathrm{id}_{\mathcal{C}} = g$ nach gF. Dank Bemerkung 21 ist also $ga = g\tilde a$.

Zeigen wir, daß das Differential von $\mathrm{S}_{\mathcal{C}}$ als Bild den Normalteiler $(\mathrm{S}_M^{\times t})\xi$ von $(\mathrm{S}_t \wr \mathrm{S}_M)\xi$ hat.

Sei zum einen $F \in \mathrm{Aut}(\mathcal{C})$ und sei $\mathrm{id}_{\mathcal{C}} \xrightarrow{a} F$ eine Isotransformationen. Wir haben zu zeigen, daß F in $(\mathrm{S}_M^{\times t})\xi$ liegt. I.e. wir haben zu zeigen, daß $(g_j m)F \overset{!}{\in} g_j M$ liegt für $j \in [1,t]$ und $m \in M$; cf. Lemma 26, Bemerkung 13. Nun verläuft der Morphismus $(g_j m)a$ von $(g_j m)\,\mathrm{id}_{\mathcal{C}} = g_j m$ nach $(g_j m)F$. Also ist $(g_j m)M = (g_j m)FM$, i.e. $(g_j m)F \in g_j M$; cf. Bemerkung 13.

Sei zum anderen $(\varphi_i)_i \in \mathrm{S}_M^{\times t}$. Wir haben zu zeigen, daß $F := (\mathrm{id}, (\varphi_i)_i)\xi$ im Bild des Differentials von $\mathrm{S}_{\mathcal{C}}$ liegt. Es ist nun $(g_j m)F \in g_j M = (g_j m)M$ für $j \in [1,t]$ und $m \in M$, sodaß wir das Tupel

$$\big(g \to gF\big)_{g\in \mathrm{Ob}(\mathcal{C}) = G}$$

von Isomorphismen betrachten können; cf. Bemerkung 13. Die Natürlichkeit dieses Tupels folgt daraus, daß es in $\mathcal{C}$ zwischen zwei Objekten höchstens einen Morphismus gibt; cf. Bemerkung 13.

Folglich liegt eine Isotransformation von $\mathrm{id}_{\mathcal{C}}$ nach F vor, die unter dem Differential auf F abgebildet wird. ▫

5.4 Ein etwas zu großes Programm

Algorithmus 34

Folgendes Programm berechnet den symmetrischen verschränkten Modul auf der zu einem verschränkten Modul $V = (M, G, \alpha, f)$ gehörigen Kategorie V Cat.

Genauer gesagt, es würde ihn berechnen, wenn die Rechnerkapazitäten ausreichen würden für die Art, wie es programmiert wurde.

```
SymmetricCrossedModule := function(M,G,alpha,f);
 Ob  := Set(G);
 Gseq := [x : x in G];
 Mor := CartesianProduct(Set(G),Set(M));
 invert := map< Mor -> Mor | x :-> <x[1] * (x[2]@f) , x[2]^-1> >;
 MFP,xi := FPGroup(M);
 numb0 := map<{-1,0,1} -> {1,2} | [<-1,1>,<0,2>,<1,2>]>;
 numb := map< Integers() -> {1,2} | z :-> Sign(z)@numb0 >;
 m_seq := function(m)
  return ElementToSequence(m@@xi);
 end function;
 nog := NumberOfGenerators(MFP);
 M_gen := [(MFP.i)@xi : i in [1..nog]];
 Mor_gen := CartesianProduct(Set(G),{1..nog});
 Mf := Image(f);
 Kf := Kernel(f);
 Tr0 := Transversal(G,Mf);
 Tr := [x^-1 : x in Tr0]; // Linksnebenklassenreprsentanten
 TrRep := map<G -> Tr | g :-> [x : x in Tr | g^-1 * x in Mf][1]>;
 MfRep := map<G -> Mf | g :-> Mf!((g@TrRep)^-1 * g)>;
 sect := map<Mf -> M | n :-> [m : m in M | m@f eq n][1]>;
 STr := SymmetricGroup(Set(Tr));
 phi := Action(GSet(STr));
 SMf := SymmetricGroup(Set(Mf));
 psi := Action(GSet(SMf));
 DPSMf := CartesianProduct([SMf : i in [1..#Tr]]);
 SKf := SymmetricGroup(Set(Kf));
 eta := Action(GSet(SKf));
 DPSKf_inner := CartesianProduct([SKf : i in [1..nog]]);
 DPSKf_outer := CartesianProduct([DPSKf_inner : i in [1..#G]]);
 DPKf := CartesianProduct([Kf : i in [1..#G]]);
 counter := 0; // spy
 ListOfAutofunctors := [];
```

```
ListOfIsotrafos := [];
for s in STr do
 for smftup in DPSMf do
  F_Ob := map<Ob -> Ob | g :->  <g@TrRep,s>@phi * <g@MfRep,smftup[Index(Tr,g@TrRep)]>@psi > ;
  SetOfAttempts := {};
  for skftup in DPSKf_outer do
   counter +:= 1; // spy
   sk := map< Mor_gen -> SKf | x :-> skftup[Index(Gseq,x[1])][x[2]] >;
   F_Mor_gen_plus
      := map< Mor_gen -> Mor | x :-> <x[1]@F_Ob, ( (x[1]@F_Ob)^-1 * (x[1] * M_gen[x[2]]@f)@F_Ob )@sect
                                     * < Kf!((M_gen[x[2]]@f@sect)^-1 * M_gen[x[2]]), x@sk >@eta > >;
   F_Mor_gen_plus_list := {<x,x@F_Mor_gen_plus> : x in Mor_gen};
   if not F_Mor_gen_plus_list in SetOfAttempts then
    SetOfAttempts join:= { F_Mor_gen_plus_list };
    F_Mor_gen_minus
      := map< Mor_gen -> Mor | x :-> < x[1] * (M_gen[x[2]]@f)^-1 , x[2] >@F_Mor_gen_plus@invert >;
    F_Mor_gen := [F_Mor_gen_minus,F_Mor_gen_plus];
    F_Mor := map< Mor -> Mor | x :-> < x[1]@F_Ob ,
             &*([Id(M)] cat [(< x[1] * &*([Id(M)] cat [ M_gen[Abs(i)]^Sign(i)
             where i is (x[2]@m_seq)[j] : j in [1..l-1]])@f ,
             Abs((x[2]@m_seq)[l]) >@F_Mor_gen[(x[2]@m_seq)[l]@numb])[2] :
             l in [1..#(x[2]@m_seq)]]) > >;
    is_functor := true;
    for y in CartesianProduct([G,M,M]) do
     if not (<y[1], y[2] * y[3]>@F_Mor)[2]
         eq (<y[1],y[2]>@F_Mor)[2] * (<y[1] * y[2]@f, y[3]>@F_Mor)[2] then
      is_functor := false;
      // print "spy nein", counter;
      break y;
     end if;
    end for;
    if is_functor and #[x@F_Mor : x in Mor] eq #{x@F_Mor : x in Mor} then
     //print "spy", &and[w[1]*(w[2]@f) eq (z[1]*(z[2]@f))@F_Ob where w is z@F_Mor : z in Mor]; // Probe
     print "spy autofunctor", counter;
     ListOfAutofunctors cat:= [<F_Ob,F_Mor>];
     if s eq Id(STr) then
      // nun untersuchen wir Isotransformationen
      for k_tup in DPKf do
       candidate_trafo
         := map<Ob -> Mor | g :-> < g, (Mf!(g^-1 * g@F_Ob))@sect * k_tup[Index(Gseq,g)]> >;
       is_trafo := true;
       for z in Mor do
        if not (z[1]@candidate_trafo)[2] * (z@F_Mor)[2]
            eq z[2] * ((z[1]*(z[2]@f))@candidate_trafo)[2] then
         is_trafo := false;
         break z;
        end if;
       end for;
       if is_trafo then
        print "spy isotrafo", counter;
        ListOfIsotrafos cat:= [<candidate_trafo,<F_Ob,F_Mor>>];
       end if;
      end for;
```

```
      end if;
     end if;
    end if;
   end for;
  end for;
 end for;
 return <ListOfAutofunctors, ListOfIsotrafos>;
end function;
```

Beispiel 35 Werde zu Testzwecken der verschränkte Modul $\mathrm{V}_{M\to\mathrm{Aut}(M)}$ aus Beispiel 10 nochmal herangezogen.

```
T := SymmetricGroup(4);
M := sub<T | T!(1,2,3,4), T!(1,3)>;
GA := AutomorphismGroup(M);
GFP,phi := FPGroup(GA);
G,psi := PermutationGroup(GFP);
alpha := psi^-1 * phi; // von G nach GA
f0 := hom< M -> AutomorphismGroup(M) | x :-> hom<M->M | m :-> m^x > >;
f := hom<M -> G | m :-> [x : x in G | m@f0 eq x@alpha][1] > ;
```

Das Programm aus Algorithmus 34 kann mittels

```
SCM := SymmetricCrossedModule(M,G,alpha,f);
```

getestet werden. Auf den momentan verfügbaren Maschinen führt es aus Größen- und Zeitgründen für diesen verschränkten Modul nicht zum Ziel.

Wir versuchen nun trotzdem, Einzelresultate herauszuholen; einzelne Autofunktoren, einzelne Isotransformationen.

```
Ob  := Set(G);
Gseq := [x : x in G];
Mor := CartesianProduct(Set(G),Set(M));
invert := map< Mor -> Mor | x :-> <x[1] * (x[2]@f) , x[2]^-1> >;
MFP,xi := FPGroup(M);
numb0 := map<{-1,0,1} -> {1,2} | [<-1,1>,<0,2>,<1,2>]>;
numb := map< Integers() -> {1,2} | z :-> Sign(z)@numb0 >;
m_seq := function(m)
 return ElementToSequence(m@@xi);
end function;
nog := NumberOfGenerators(MFP);
M_gen := [(MFP.i)@xi : i in [1..nog]];
Mor_gen := CartesianProduct(Set(G),{1..nog});
Mf := Image(f);
Kf := Kernel(f);
Tr0 := Transversal(G,Mf);
Tr := [x^-1 : x in Tr0]; // Linksnebenklassenreprsentanten
TrRep := map<G -> Tr | g :-> [x : x in Tr | g^-1 * x in Mf][1]>;
```

```
MfRep := map<G -> Mf | g :-> Mf!((g@TrRep)^-1 * g)>;
sect := map<Mf -> M | n :-> [m : m in M | m@f eq n][1]>;
STr := SymmetricGroup(Set(Tr));
phi := Action(GSet(STr));
SMf := SymmetricGroup(Set(Mf));
psi := Action(GSet(SMf));
DPSMf := CartesianProduct([SMf : i in [1..#Tr]]);
SKf := SymmetricGroup(Set(Kf));
eta := Action(GSet(SKf));
DPSKf_inner := CartesianProduct([SKf : i in [1..nog]]);
DPSKf_outer := CartesianProduct([DPSKf_inner : i in [1..#G]]);
DPKf := CartesianProduct([Kf : i in [1..#G]]);

STr_list := [x : x in STr];
DPSMf_list := [x : x in DPSMf];
DPSKf_outer_list := [x : x in DPSKf_outer];

STr_length := #STr_list;
DPSMf_length := #DPSMf_list;
DPSKf_outer_length := #DPSKf_outer_list;

i := 1; // in [1..STr_length]
j := 1; // in [1..DPSMf_length]
k_start := 1; k_end := 300; // Intervall in [1..DPSKf_outer_length]

s := STr_list[i];
smftup := DPSMf_list[j];

SymmetricCrossedModule_stepwise := function(M,G,alpha,f,s,smftup,DPSKf_outer_list,k_start,k_end);
 Ob := Set(G);
 ListOfAutofunctors := [];
 ListOfIsotrafos := [];
 F_Ob := map<Ob -> Ob | g :-> <g@TrRep,s>@phi * <g@MfRep,smftup[Index(Tr,g@TrRep)]>@psi> ;
 SetOfAttempts := {};
 for k in [k_start..k_end] do
  print "spy k =", k;
  skftup := DPSKf_outer_list[k];
  sk := map< Mor_gen -> SKf | x :-> skftup[Index(Gseq,x[1])][x[2]] >;
  F_Mor_gen_plus
    := map< Mor_gen -> Mor | x :-> <x[1]@F_Ob, ( (x[1]@F_Ob)^-1 * (x[1] * M_gen[x[2]]@f)@F_Ob )@sect
                                   * < Kf!((M_gen[x[2]]@f@sect)^-1 * M_gen[x[2]]), x@sk >@eta > >;
  F_Mor_gen_plus_list := {<x,x@F_Mor_gen_plus> : x in Mor_gen};
  if not F_Mor_gen_plus_list in SetOfAttempts then
   SetOfAttempts join:= { F_Mor_gen_plus_list };
   F_Mor_gen_minus
     := map< Mor_gen -> Mor | x :-> < x[1] * (M_gen[x[2]]@f)^-1 , x[2] >@F_Mor_gen_plus@invert >;
   F_Mor_gen := [F_Mor_gen_minus,F_Mor_gen_plus];
   F_Mor := map< Mor -> Mor | x :-> < x[1]@F_Ob , &*([Id(M)] cat [(< x[1] * &*([Id(M)]
                      cat [ M_gen[Abs(i)]^Sign(i) where i is (x[2]@m_seq)[j] : j in [1..l-1]])@f ,
        Abs((x[2]@m_seq)[l]) >@F_Mor_gen[(x[2]@m_seq)[l]@numb])[2] : l in [1..#(x[2]@m_seq)]]) > >;
   is_functor := true;
   for y in CartesianProduct([G,M,M]) do
    if not (<y[1], y[2] * y[3]>@F_Mor)[2]
```

```
        eq (<y[1],y[2]>@F_Mor)[2] * (<y[1] * y[2]@f, y[3]>@F_Mor)[2] then
     is_functor := false;
     break y;
    end if;
   end for;
   if is_functor and #[x@F_Mor : x in Mor] eq #{x@F_Mor : x in Mor} then
    print "spy autofunctor";
    ListOfAutofunctors cat:= [<F_Ob,F_Mor>];
    if s eq Id(STr) then
     for k_tup in DPKf do
      candidate_trafo
         := map<Ob -> Mor | g :-> < g, (Mf!(g^-1 * g@F_Ob))@sect * k_tup[Index(Gseq,g)]> >;
      is_trafo := true;
      for z in Mor do
       if not (z[1]@candidate_trafo)[2] * (z@F_Mor)[2]
           eq z[2] * ((z[1]*(z[2]@f))@candidate_trafo)[2] then
        is_trafo := false;
        break z;
       end if;
      end for;
      if is_trafo then
       print "spy isotrafo";
       ListOfIsotrafos cat:= [<candidate_trafo,<F_Ob,F_Mor>>];
      end if;
     end for;
    end if;
   end if;
  end if;
 end for;
 return <ListOfAutofunctors, ListOfIsotrafos>;
end function;
```

Dieser kann nun wie folgt aufgerufen werden.

```
SCM_stepwise
:= SymmetricCrossedModule_stepwise(M,G,alpha,f,s,smftup,DPSKf_outer_list,k_start,k_end);
```

Mit den oben gewählten Einstellungen liefert das Programm nun den identischen Autofunktor für `k` $= 1$ und einen weiteren Autofunktor für `k` $= 271$.

Wir überprüfen ersteres.

```
Id := SCM_stepwise[1][1];
print &and[g@Id[1] eq g : g in Ob];
print &and[x@Id[2] eq x : x in Mor];
```

Der zweite gefundene Autofunktor hat Ordnung 2.

```
F271 := SCM_stepwise[1][2];
```

```
print &and[g@F271[1] eq g : g in Ob];
print &and[x@F271[2] eq x : x in Mor];
print &and[g@(F271[1]*F271[1]) eq g : g in Ob];
print &and[x@(F271[2]*F271[2]) eq x : x in Mor];
```

Wir haben ferner einige Isotrafos gefunden.

```
IdId_1   := SCM_stepwise[2][1];
IdId_2   := SCM_stepwise[2][2];
IdId_3   := SCM_stepwise[2][3];
IdId_4   := SCM_stepwise[2][4];
IdF271_1 := SCM_stepwise[2][5];
IdF271_2 := SCM_stepwise[2][6];
IdF271_3 := SCM_stepwise[2][7];
IdF271_4 := SCM_stepwise[2][8];
```

Die Variablen `s`, `smftup` und das Intervall `k_start,k_end` können nun wie oben beschrieben variiert werden.

Zum Abspeichern einzelner Objekte brauchen wir folgende Prozedur.

```
PFM := procedure(Datei, Bezeichnung, X)
 PrintFile(Datei, Bezeichnung);
 PrintFile(Datei, ":=");
 PrintFileMagma(Datei, X);
 PrintFile(Datei, ";\n");
end procedure;
```

Wir speichern `Id`, `F271` und, sagen wir, `IdF271_3` noch im File `experiment` im selben Verzeichnis, in welchem wir Magma aufgerufen haben.

```
F271_Ob := [<g,g@F271[1]> : g in Ob];
F271_Mor := [<x,x@F271[2]> : x in Mor];
IdF271_3_OM := [<g,g@IdF271_3[1]> : g in Ob];
ex := "experiment"; // Dateiname
PFM(ex, "Ob", Ob);
PFM(ex, "Mor", Mor);
PFM(ex, "F271_Ob", F271_Ob);
PFM(ex, "F271_Mor", F271_Mor);
PFM(ex, "IdF271_3_OM", IdF271_3_OM);
```

Mittels

```
load "experiment";
F271 := <map<Ob -> Ob | F271_Ob>, map<Mor -> Mor | F271_Mor>>;
IdF271_3 := <map<Ob -> Mor | IdF271_3_OM>, F271>;
```

können die Daten wieder hergestellt werden. Falls man diese Daten weiter verarbeiten möchte, sollte man oft auch den verschränkten Modul (M, G, α, f) wie oben an Magma übermitteln.

Beispiel 36 Werde wieder der verschränkte Modul $V := \mathrm{V}_{M \to \mathrm{Aut}(M)}$ aus Beispiel 10 betrachtet.

```
T := SymmetricGroup(4);
M := sub<T | T!(1,2,3,4), T!(1,3)>;
GA := AutomorphismGroup(M);
GFP,phi := FPGroup(GA);
G,psi := PermutationGroup(GFP);
alpha := psi^-1 * phi; // von G nach GA
f0 := hom< M -> AutomorphismGroup(M) | x :-> hom<M->M | m :-> m^x > >;
f := hom<M -> G | m :-> [x : x in G | m@f0 eq x@alpha][1] > ;
Ob  := Set(G);
Mor := CartesianProduct(Set(G),Set(M));
load "experiment";
F271 := <map<Ob -> Ob | F271_Ob>, map<Mor -> Mor | F271_Mor>>;
IdF271_3 := <map<Ob -> Mor | IdF271_3_OM>, F271>;
```

Zur Probe schauen wir uns die Operation von `F271` auf einem kommutativen Dreieck in $V\,\mathrm{Cat}$ an. Wir kürzen wie ab in Beispiel 23.

```
a := M!(1,2,3,4);
b := M!(1,3);
c := G!(1,3,2,4);
d := G!(3,4);
```

Die Rechnung

```
print c*((a*b)@f);
print c^3*d;
print c^3*d*(a@f);
print c*d;
print c*(b@f);
```

liefert das kommutative Dreieck

$$\begin{tikzcd}
 & c^3d \arrow[dr, "{(c^3d,a)}"] & \\
c \arrow[ur, "{(c,ab)}"] \arrow[rr, "{(c,b)}"'] & & cd\,.
\end{tikzcd}$$

I.e. es ist der horizontale Morphismus das Kompositum der anderen beiden. Magma gibt die Operation von `F271` darauf wie folgt.

```
print &and[x eq x@F271[1] : x in Ob];
print <c,a*b>@F271[2];
print <c^3*d,a>@F271[2];
print <c,b>@F271[2];
print a^3*b, a^3;
```

Es resultiert in der Tat das kommutative Dreieck

$$\begin{tikzcd}
 & c^3d \arrow[dr, "{(c^3d,a^3)}"] & \\
c \arrow[ur, "{(c,a^3b)}"] \arrow[rr, "{(c,b)}"'] & & cd\ .
\end{tikzcd}$$

Ferner können wir zur Illustration ein kommutatives Viereck aus der Isotransformation `IdF271_3` gewinnen. Vertikal links steht der Morphismus (c, ab), gesehen als sein eigenes Bild unter dem identischen Funktor. Vertikal rechts steht das Bild von dieses Morphismus unter `F271`, zu erhalten als `<c,a>@F271[2]`. Horizontal stehen die Einträge der Isotransformation `IdF271_3`, oben der Eintrag am oberen linken Objekt, geliefert von `c@IdF271_3[1]`, unten der Eintrag am unteren linken Objekt, geliefert von `(c^3*d)@IdF271_3[1]`.

$$\begin{tikzcd}
c \arrow[r, "{(c,1)}"] \arrow[d, "{(c,ab)}"'] & c \arrow[d, "{(c,a^3b)}"] \\
c^3d \arrow[r, "{(c^3d,a^2)}"'] & c^3d
\end{tikzcd}$$

In der Tat ist dieses Viereck kommutativ, da in M sich $ab \cdot a^2 = 1 \cdot a^3b$ ergibt.

Algorithmus 37

Folgendes Programm berechnet die Ordnung eines Autofunktors.

```
OrderAutofunctor := function(F) // F: Autofunktor
 t := 1;
 while not (&and[g@(F[1]^t) eq g : g in Ob]
        and &and[x@(F[2]^t) eq x : x in Mor]) do
  t +:= 1;
 end while;
 return t;
end function;
```

Folgendes Programm berechnet das Produkt zweier Isotrafos aus einem symmetrischen verschränkten Modul.

```
MultiplyIsotrafos := function(a,b)
 return
  < map< Ob -> Mor | [<g, <g,(g@(a[1]))[2] * ( g@(a[2][1])@(b[1]) )[2]> > : g in Ob] >,
                                              <a[2][1] * b[2][1], a[2][2] * b[2][2]> >;
end function;
```

Folgendes Programm berechnet die Ordnung einer Isotransformation aus einem symmetrischen verschränkten Modul.

```
OrderIsotrafo := function(a)
 k := 1;
 aprod := a;
 while not &and[(g@(aprod[1]))[2] eq M!1 : g in Ob] do
  k +:= 1;
  aprod := MultiplyIsotrafos(a,aprod);
 end while;
 return k;
end function;
```

Beispiel 38

Wir setzen Beispiel 35 unter Verwendung der Programme aus Algorithmus 37 fort.

Es liefert

`OrderAutofunctor(F271);`

die Ordnung 2 des Autofunktors `F271`, wie bereits in loc. cit. bestimmt.

Ferner liefert

`OrderIsotrafo(IdF271_3);`

die Ordnung 2 der Isotransformation `IdF271_3`.

6 Die Einbettung von Cayley-Truong via Magma

Das folgende Analogon des Lemmas von Cayley [**1**] kenne ich von Truong [**3**].

Lemma 39 (Cayley-Truong) *Sei $V = (M, G, \alpha, f)$ ein verschränkter Modul.*

Für $x \in G$ erhalten wir einen Autofunktor

$$\begin{array}{ccc} V\,\mathrm{Cat} & \xrightarrow{x\gamma} & V\,\mathrm{Cat} \\ \left(\begin{array}{c} g \\ {\scriptstyle (g,m)}\big\downarrow \\ g(mf) \end{array}\right) & \mapsto & \left(\begin{array}{c} gx \\ \big\downarrow{\scriptstyle (gx,m^x)} \\ g(mf)x \end{array}\right) \end{array} .$$

So wird $\gamma\colon G \to (\mathrm{S}_{V\,\mathrm{Cat}})^{\mathrm{Gruppe}}$ *ein injektiver Gruppenmorphismus.*

Für $y \in M$ *erhalten wir die Isotransformation*

$$y\mu \;:=\; (g \xrightarrow{(g,y)} g(yf))_{g\in G}$$

von $\mathrm{id}_{V\,\mathrm{Cat}}$ *nach* $(yf)\gamma$*.*

So wird $\mu\colon M \to (\mathrm{S}_{V\,\mathrm{Cat}})^{\mathrm{Modul}}$ *ein injektiver Gruppenmorphismus.*

Insgesamt wird (γ,μ) *ein Morphismus verschränkter Moduln von* V *nach* $\mathrm{S}_{V\,\mathrm{Cat}}$*, der aus zwei injektiven Gruppenmorphismen besteht.*

Beweis. Zunächst sehen wir, daß γ ein injektiver Gruppenmorphismus ist.

Es ist für $y \in M$ das Tupel $(g \xrightarrow{(g,y)} g(yf))_{g\in G}$ eine Isotransformation von $\mathrm{id}_{V\,\mathrm{Cat}}$ nach $(yf)\gamma$, da für einen Morphismus (g,m) das Viereck

$$\begin{tikzcd}
g \arrow[r, "{(g,y)}"] \arrow[d, "{(g,m)}"'] & g(yf) \arrow[d, "{(g(yf),m^{yf})}"] \\
g(mf) \arrow[r, "{(g(mf),y)}"'] & g(mf)(yf)
\end{tikzcd}$$

kommutiert, unter Verwendung von $m^{yf} = m^y$.

Es ist μ ein injektiver Gruppenmorphismus, da für $y,\ y' \in M$ sich bei $g \in G$ die Gleichheit

$$\begin{array}{rcl}
g((y\mu) * (y'\mu)) & = & g((y\mu) \blacktriangle ((yf)\gamma)(y'\mu)) \\
& = & (g,y) \blacktriangle g((yf)\gamma)(y'\mu) \\
& = & (g,y) \blacktriangle (g(yf))(y'\mu) \\
& = & (g,y) \blacktriangle (g(yf),y') \\
& = & (g,yy') \\
& = & g((yy')\mu)
\end{array}$$

ergibt, was $(y\mu) * (y'\mu) = (yy')\mu$ nach sich zieht.

Um zu zeigen, daß (γ,μ) ein Morphismus verschränkter Moduln ist, verifizieren wir die Eigenschaften aus Definition 11.

Ad (MVM 1). Für $y \in M$ ist $(y\mu)\mathrm{f}_{\mathrm{S}_{V\,\mathrm{Cat}}} = (yf)\gamma$, da $y\mu$ Ziel $(yf)\gamma$ hat.

Ad (MVM 2). Für $y \in M$ und $x \in G$ ist bei $g \in G$ zum einen

$$g((y^x)\mu) \;=\; (g,y^x)\;,$$

zum anderen

$$g((y\mu)^{(x\gamma)}) \;=\; g(x\gamma)^-(y\mu)(x\gamma) \;=\; (gx^-)(y\mu)(x\gamma) \;=\; (gx^-,y)(x\gamma) \;=\; (gx^-x,y^x) \;=\; (g,y^x)\;,$$

was dasselbe ist. $\square$

Algorithmus 40

```
gamma := function(x,M,G,alpha,f) // x in G
 Ob  := Set(G);
 Mor := CartesianProduct(Set(G),Set(M));
 F_Ob := map<Ob -> Ob | g :-> g*x >;
 F_Mor := map<Mor -> Mor | u :-> <u[1]*x,u[2]@(x@alpha)> >;
 if not &and[(<y[1], y[2] * y[3]>@F_Mor)[2] eq
      (<y[1],y[2]>@F_Mor)[2] * (<y[1] * y[2]@f, y[3]>@F_Mor)[2] :
      y in CartesianProduct([G,M,M])] then
  print "Kein Funktor";
 end if;// Probe
 return <F_Ob,F_Mor>;
end function;
```

Man könnte `Ob` und `Mor` auch als globale Variablen verwenden und der Funktion nicht in Form eines verschränkten Moduls mit übergeben. Das setzt dann voraus, daß man den Überblick über die bereits global definierten Variablen hat.

```
mu := function(y,M,G,alpha,f) // y in M
 Ob  := Set(G);
 Mor := CartesianProduct(Set(G),Set(M));
 F := gamma(y@f,M,G,alpha,f);
 trafo := map<Ob -> Mor | g :-> <g,y> >;
 if not &and[(z[1]@trafo)[2] * (z@F[2])[2]
         eq z[2] * ((z[1]*(z[2]@f))@trafo)[2] : z in Mor] then
   print "Keine Transformation";
 end if; // Probe
 return <trafo, F>;
end function;
```

Beispiel 41

Wir verwenden wieder unseren verschränkten Modul $\mathrm{V}_{M \to \mathrm{Aut}(M)}$ aus Beispiel 10.

```
T := SymmetricGroup(4);
M := sub<T | T!(1,2,3,4), T!(1,3)>;
GA := AutomorphismGroup(M);
GFP,phi := FPGroup(GA);
G,psi := PermutationGroup(GFP);
alpha := psi^-1 * phi; // von G nach GA
f0 := hom< M -> AutomorphismGroup(M) | x :-> hom<M->M | m :-> m^x > >;
f := hom<M -> G | m :-> [x : x in G | m@f0 eq x@alpha][1] > ;
```

Wir laden Daten aus Beispiel 35 wieder ein.

```
load "experiment";
F271 := <map<Ob -> Ob | F271_Ob>, map<Mor -> Mor | F271_Mor>>;
IdF271_3 := <map<Ob -> Mor | IdF271_3_OM>, F271>;
```

Das Bild von `gamma` wird von

```
image_gamma := [gamma(x,M,G,alpha,f) : x in G];
```

geliefert. Wir wollen abgleichen, ob bestimmte Autofunktoren auf dieser Liste stehen.

```
IsEqualAutofunctor := function(F1,F2,M,G,alpha,f)
 Ob  := Set(G);
 Mor := CartesianProduct(Set(G),Set(M));
 return &and[g@F1[1] eq g@F2[1] : g in Ob] and &and[x@F1[2] eq x@F2[2] : x in Mor];
end function;
```

Ob nun `F271` auf dieser Liste steht, entscheiden wir mit folgendem Befehl.

```
&or[IsEqualAutofunctor(F271,image_gamma[i],M,G,alpha,f) : i in [1..Order(G)]];
```

Er steht nicht auf der Liste, liegt also nicht im Bild von `gamma`.

Das Bild von `mu` wird von

```
image_mu := [mu(y,M,G,alpha,f) : y in M];
```

geliefert. Wir wollen abgleichen, ob bestimmte Autofunktoren auf dieser Liste stehen.

```
IsEqualIsotrafo := function(IdF1,IdF2,M,G,alpha,f)
 Ob  := Set(G);
 Mor := CartesianProduct(Set(G),Set(M));
 return IsEqualAutofunctor(IdF1[2],IdF2[2],M,G,alpha,f)
        and &and[g@IdF1[1] eq g@IdF2[1] : g in Ob];
end function;
```

Ob nun `IdF271_3` auf dieser Liste steht, entscheiden wir mit folgendem Befehl.

```
&or[IsEqualIsotrafo(IdF271_3,image_mu[i],M,G,alpha,f) : i in [1..Order(M)]];
```

Sie steht nicht auf der Liste, liegt also nicht im Bild von `mu`.

7 Aufgabenstellung

Für einen verschränkten Modul $V := (M, G, \alpha, f)$ sollen Autofunktoren von $V\mathrm{Cat}$ und Isotransformationen von $\mathrm{id}_{V\mathrm{Cat}}$ in Autofunktoren gefunden werden.

Mit anderen Worten, es sollten Elemente der Gruppe $(\mathrm{S}_{V\mathrm{Cat}})^{\mathrm{Gruppe}}$, also Autofunktoren von $V\mathrm{Cat}$, und Elemente der Gruppe $(\mathrm{S}_{V\mathrm{Cat}})^{\mathrm{Modul}}$, also Isotransformationen von $\mathrm{id}_{V\mathrm{Cat}}$ in Autofunktoren, gefunden werden.

Die Ordnungen dieser Elemente sollen betrachtet werden.

Es soll untersucht werden, ob die gefundenen Elemente im Bild von Cayley-Truong liegen.

Eine graphische Darstellung eines Teils der Kategorie $V\mathrm{Cat}$ kann helfen.

Der Fall $M = \mathrm{D}_8$ und $V = \mathrm{V}_{M \to \mathrm{Aut}(M)}$ wird in den grün markierten Beispielen durchgeführt. Diese Beispiele eignen sich zur Nachahmung.

Literatur

[1] Cayley, A., *On the theory of groups, as depending on the symbolic equation* $\vartheta^n = 1$, Philos. Mag. 7 (4), p. 40–47, 1854.

[2] Bosma, W.; Cannon, J.J.; Fieker, C.; Steel, A. (eds.), *Handbook of Magma functions,* Edition 2.16, 2010; cf. magma.maths.usyd.edu.au, magma.maths.usyd.edu.au/calc.

[3] Truong, M., Masterarbeit, im Entstehen begriffen.

[4] Whitehead, J.H.C., *Combinatorial Homotopy II*, Bull. Am. Math. Soc. 55 (5), p. 453–496, 1949.