Groups in Allegories

Kawahara, Yasuo
Department of Informatics, Kyushu University

出版情報：DOI Technical Report. 197, 2001-08. 九州大学大学院システム情報科学研究院情報理学部門
バージョン：
権利関係：

Groups in Allegories

Yasuo KAWAHARA

Department of Informatics, Kyushu University 33, Fukuoka 812-8581, Japan

{**kawahara@i.kyushu-u.ac.jp**}

Abstract. Groups are one of the most fundamental notions in mathematics. This paper provides a foundation of group theory in allegories. Almost all results in the paper can be applied to theory of fuzzy groups.

1 Introduction

The motivation of the paper arose from the following three fundamental exercises in group theory:

(a) Let $G = (G, \cdot)$ be a semigroup, that is, a binary operation $\cdot : G \times G \to G$ is associative. Show that if $\forall x \in G : xe = x$ and $\forall x \in G \exists y \in G : xy = e$ for some element $e \in G$, then $\forall x \in G : ex = x$ and $\forall x \in G \exists y \in G : yx = e$.
(b) Let H be a subgroup of a group $G = (G, \cdot, e, \cdot^{-1})$. Prove that the (binary) relation $x \equiv y$ on G, defined by $x^{-1}y \in H$, is an equivalence relation.
(c) Show that the set of all normal subgroups of a group G forms a modular lattice. In other words, the following modular law holds for three normal subgroups S, T and U of G:

$$S \subseteq U \implies ST \cap U \subseteq S(T \cap U).$$

To define group objects in categories [7] is not new, but it is difficult to directly treat algebraic relations, such as residual relations (b) induced by subgroups, in the ordinary category theory. Allegories [2], as a kind of relation categories, give a natural and suitable setting for manipulating algebraic binary relations in group theory, lattice theory [6] and so on. This paper provides a foundation of group theory in allegories, and solves the above three questions (a), (b) and (c).

The paper is organised as follows: In section 2 we recall the definition of allegories [2] and remark some fundamentals on relational products in allegories. In section 3 we review a simple sharpness property [3, 8, 4] on relational products of relations, which was initiated by Schmidt and will play an important rôle in the proof of the main results. In section 4 we explore some fundamental properties of relational binary operations and show a suitable formalisation (Theorem 2) of the associative law, as well as the commutative law, using with relational global elements. The inverse law and the absorption laws (in lattice theory) are of course not the case. In section 5 we mention unitary and inverse operations for binary operations in allegories. We also give a relational version (Theorem 4) for the first question (a). In section 6 we define notions of (functional) groups and subgroups, and prove an elementary fact (b) that the residual relation induced by a subgroup is an equivalence relation. In section 7 we describe a notion of normal subgroups in allegories, and answer the final question (c) that the set of all normal subgroups of a group forms a modular lattice.

2 Allegories

In this section we recall the fundamentals on relation categories, called allegories [2].

Throughout this paper, a morphism α from an object X into an object Y in an allegory (which will be defined below) will be denoted by a half arrow $\alpha : X \rightharpoonup Y$, and the composite of a morphism $\alpha : X \rightharpoonup Y$ followed by a morphism $\beta : Y \rightharpoonup Z$ will be written as $\alpha\beta : X \rightharpoonup Z$. Also we will denote the identity morphism on X as id_X.

Definition 1. An allegory $\mathcal{A}$ is a category satisfying the following:
D1. [Meet Semi-Lattice] For all pairs of objects X and Y the hom-set $\mathcal{A}(X,Y)$ consisting of all morphisms of X into Y is a meet semi-lattice with the greatest morphism ∇_{XY}. Its semi-lattice structure will be denoted by

$$\mathcal{A}(X,Y) = (\mathcal{A}(X,Y), \sqsubseteq, \sqcap, \nabla_{XY}).$$

D2. [Converse] There is given a converse operation $^\sharp : \mathcal{A}(X,Y) \to \mathcal{A}(Y,X)$. That is, for all morphisms $\alpha, \alpha' : X \rightharpoonup Y$, $\beta : Y \rightharpoonup Z$, the following converse laws hold:
(a) $(\alpha\beta)^\sharp = \beta^\sharp\alpha^\sharp$, (b) $(\alpha^\sharp)^\sharp = \alpha$, (c) If $\alpha \sqsubseteq \alpha'$, then $\alpha^\sharp \sqsubseteq \alpha'^\sharp$
for all morphisms $\alpha, \alpha' : X \rightharpoonup Y$ and $\beta : Y \rightharpoonup Z$.
D3. [Dedekind Formula] For all morphisms $\alpha : X \rightharpoonup Y$, $\beta : Y \rightharpoonup Z$ and $\gamma : X \rightharpoonup Z$ the Dedekind formula $\alpha\beta \sqcap \gamma \sqsubseteq \alpha(\beta \sqcap \alpha^\sharp\gamma)$ holds.
D4. [Sub-Distributivity] The composition preserves order: If $\alpha \sqsubseteq \alpha'$ and $\beta \sqsubseteq \beta'$, then $\alpha\beta \sqsubseteq \alpha'\beta'$. □

The fundamental properties of relational categories is referred to [1, 2, 9, 5]. The following is a basic property of allegories.

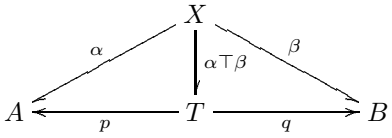
Proposition 1. *Let $\alpha, \alpha' : X \rightharpoonup Y$, $\beta, \beta' : Y \rightharpoonup Z$ and $\gamma : Y \rightharpoonup X$ be morphisms in an allegory $\mathcal{A}$. If $\alpha\gamma = \mathrm{id}_X$ and $\gamma\alpha = \mathrm{id}_Y$, then $\alpha = \gamma^\sharp$.* □

A morphism $\alpha : X \rightharpoonup Y$ is *total* if $\mathrm{id}_X \sqsubseteq \alpha\alpha^\sharp$ (or equivalently, $\alpha\nabla_{YX} = \nabla_{XX}$). A morphism $f : X \rightharpoonup Y$ such that $f^\sharp f \sqsubseteq \mathrm{id}_Y$ (*univalent*) is called a *function* and may be introduced as $f : X \to Y$. In what follows the word *relation* is used as synonym for morphisms in allegories.

Definition 2. A pair (A, B) of objects in an allegory $\mathcal{A}$ *has a relational product* if there exists a pair $(p : T \to A, q : T \to B)$ of total functions such that $p^\sharp q = \nabla_{AB}$ and $pp^\sharp \sqcap qq^\sharp = \mathrm{id}_T$. The pair $(p : T \to A, q : T \to B)$ is called a pair of projections for (A, B). An allegory $\mathcal{A}$ *has a relational product* if every pair of objects in $\mathcal{A}$ has a relational product. □

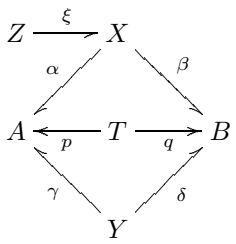
Throughout the rest of the paper we assume that $\mathcal{A}$ is a fixed allegory with relational products.

Let $(p : T \to A, q : T \to B)$ be a pair of projections for a pair (A, B) of objects. For each pair of relations $\alpha : X \rightharpoonup A$ and $\beta : X \rightharpoonup B$, we define a relation $\alpha\top\beta : X \rightharpoonup T$ by $\alpha\top\beta = \alpha p^\sharp \sqcap \beta q^\sharp$. It is trivial that $p\top q = \mathrm{id}_T$.



The following is a list of elementary properties of relational products in allegories. The proof is trivial and so omitted.

Proposition 2. *Let $(p : T \to A, q : T \to B)$ be a pair of projections for (A, B) and let $\alpha, \alpha' : X \rightharpoonup A$, $\beta, \beta' : X \rightharpoonup B$, $\gamma : Y \rightharpoonup A$, $\delta : Y \rightharpoonup B$ and $\xi : Z \rightharpoonup X$ be relations.*



Then the following hold:

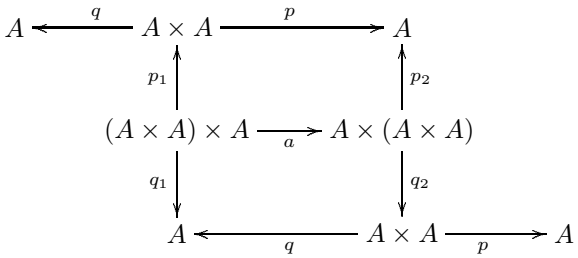
(a) *If $\alpha \sqsubseteq \alpha'$ and $\beta \sqsubseteq \beta'$, then $\alpha\top\beta \sqsubseteq \alpha'\top\beta'$,*
(b) *$\xi(\alpha\top\beta) \sqsubseteq \xi\alpha\top\xi\beta$,*

(c) $\xi(\alpha\top\nabla_{XY}\delta) = \xi\alpha\top\nabla_{ZY}\delta$,
(d) $\xi(\nabla_{XY}\gamma\top\beta) = \nabla_{ZY}\gamma\top\xi\beta$,
(e) *If* $\xi : Z \rightharpoonup X$ *is a function, then* $\xi(\alpha\top\beta) = \xi\alpha\top\xi\beta$.
(f) *If* α *and* β *are total functions, then* $\alpha\top\beta$ *is a unique total function such that* $(\alpha\top\beta)p = \alpha$ *and* $(\alpha\top\beta)q = \beta$,
(g) $(\alpha \sqcap \alpha')\top\beta = (\alpha\top\beta) \sqcap (\alpha'\top\beta)$ *and* $\alpha\top(\beta \sqcap \beta') = (\alpha\top\beta) \sqcap (\alpha\top\beta')$. □

As in ordinary category theory, the common domain T of projections $p : T \to A$ and $q : T \to B$ is uniquely determined up to isomorphism by the virtue of the last Proposition 2(f). This enables us to write the object T as $A \times B$.

Let $(p : A \times A \to A, q : A \times A \to A)$ be a pair of projections for (A, A). The twisting function $t : A \times A \to A \times A$ is defined by $t = q\top p$ $(= qp^\sharp \sqcap pq^\sharp)$. That is, t is a unique total function such that $tp = q$ and $tq = p$. Then $tt = t(q\top p) = tq\top tp = p\top q = \mathrm{id}_{A\times A}$. The diagonal function $d_A : A \to A \times A$ is defined by $d_A = \mathrm{id}_A\top\mathrm{id}_A = p^\sharp \sqcap q^\sharp$. That is, d_A is a unique total function such that $d_A p = \mathrm{id}_A$ and $d_A q = \mathrm{id}_A$.

In addition we assume that $(p_1 : (A \times A) \times A \to A \times A, q_1 : (A \times A) \times A \to A)$ is a pair of projections for $(A \times A, A)$, and $(p_2 : A \times (A \times A) \to A, q_2 : A \times (A \times A) \to A \times A)$ a pair of projections for $(A, A \times A)$.



The associative function $a : (A \times A) \times A \to A \times (A \times A)$ is defined by

$$a = p_1 p\top(p_1 q\top q_1).$$

That is, a is a unique total function such that

$$ap_2 = p_1 p, \qquad aq_2 p = p_1 q, \qquad aq_2 q = q_1.$$

Another associative function $b : A \times (A \times A) \to (A \times A) \times A$ is defined by

$$b = (p_2\top q_2 p)\top q_2 q.$$

That is, b is a unique total function such that

$$bp_1 p = p_2, \qquad bp_1 q = q_2 p, \qquad bq_1 = q_2 q.$$

It is trivial that a and b are mutually inverse, that is, $ab = \mathrm{id}_{(A\times A)\times A}$ and $ba = \mathrm{id}_{A\times(A\times A)}$. For

$$\begin{aligned}
ab &= a\{(p_2\top q_2 p)\top q_2 q\} \\
&= (ap_2\top aq_2 p)\top aq_2 q && \{\text{ Proposition 2(e) }\} \\
&= (p_1 p\top p_1 q)\top q_1 && \{\ ap_2 = p_1 p,\ aq_2 p = p_1 q,\ aq_2 q = q_1\ \} \\
&= p_1(p\top q)\top q_1 && \{\text{ Proposition 2(e) }\} \\
&= p_1\top q_1 && \{\ p\top q = \mathrm{id}_{A\times A}\ \} \\
&= \mathrm{id}_{(A\times A)\times A},
\end{aligned}$$

and

$$\begin{aligned}
ba &= b\{p_1 p\top(p_1 q\top q_1)\} \\
&= bp_1 p\top(bp_1 q\top bq_1) && \{\text{ Proposition 2(e) }\} \\
&= p_2\top(q_2 p\top q_2 q) && \{\ bp_1 p = p_2,\ bp_1 q = q_2 p,\ bq_1 = q_2 q\ \} \\
&= p_2\top q_2(p\top q) && \{\text{ Proposition 2(e) }\} \\
&= p_2\top q_2 && \{\ p\top q = \mathrm{id}_{A\times A}\ \} \\
&= \mathrm{id}_{A\times(A\times A)}.
\end{aligned}$$

Proposition 3. *Let $\alpha, \beta, \gamma : X \rightharpoonup A$ be relations. Then the following hold:*

(a) $\{(\alpha\top\beta)\top\gamma\}a = \alpha\top(\beta\top\gamma)$,
(b) $\{\alpha\top(\beta\top\gamma)\}b = (\alpha\top\beta)\top\gamma$.

Proof. As $ab = \mathrm{id}_{(A\times A)\times A}$ and $ba = \mathrm{id}_{A\times(A\times A)}$ we have $a = b^\sharp$ and $b = a^\sharp$ using Proposition 1.
(a)

$$\begin{aligned}
\{(\alpha\top\beta)\top\gamma\}a &= \{(\alpha p^\sharp \sqcap \beta q^\sharp)p_1^\sharp \sqcap \gamma q_1^\sharp\}b^\sharp && \{\ a = b^\sharp\ \}\\
&= \alpha p^\sharp p_1^\sharp b^\sharp \sqcap \beta q^\sharp p_1^\sharp b^\sharp \sqcap \gamma q_1^\sharp b^\sharp\\
&= \alpha p_2^\sharp \sqcap \beta p^\sharp q_2^\sharp \sqcap \gamma q^\sharp q_2^\sharp && \{\ bp_1p = p_2,\ bp_1q = q_2p,\ bq_1 = q_2q\ \}\\
&= \alpha p_2^\sharp \sqcap (\beta p^\sharp \sqcap \gamma q^\sharp)q_2^\sharp\\
&= \alpha\top(\beta\top\gamma)
\end{aligned}$$

(b)

$$\begin{aligned}
\{\alpha\top(\beta\top\gamma)\}b &= \{(\alpha\top\beta)\top\gamma\}ab && \{\ \text{(a)}\ \}\\
&= (\alpha\top\beta)\top\gamma && \{\ ab = \mathrm{id}_{(A\times A)\times A}\ \}
\end{aligned}$$

□

Let $\xi : A \rightharpoonup X$ and $\eta : B \rightharpoonup Y$ be a pair of relations. We define a relation $\xi \times \eta : A \times B \rightharpoonup X \times Y$ by $\xi\times\eta = p\xi\top q\eta = p\xi p_0^\sharp \top q\eta q_0^\sharp$. If $f : A \to X$ and $g : B \to Y$ are total functions, then $f \times g$ is a unique function such that $(f \times g)p_0 = pf$ and $(f \times g)q_0 = qg$.

$$\begin{array}{ccccc}
A & \xleftarrow{p} & A\times B & \xrightarrow{q} & B\\
{\scriptstyle\xi}\downarrow & & \downarrow{\scriptstyle\xi\times\eta} & & \downarrow{\scriptstyle\eta}\\
X & \xleftarrow[p_0]{} & X\times Y & \xrightarrow[q_0]{} & Y
\end{array}$$

Remark that an equality $(f \times g)(f' \times g') = ff' \times gg'$ always holds for total functions f, f', g and g'.

3 Sharpness

Schmidt initially suggested that the so-called sharpness property

$$(\xi \times \eta)(\xi' \times \eta') = \xi\xi' \times \eta\eta'$$

does not hold for relations ξ, ξ', η and η' (Cf. [8, 4]) in general. In this section we review a simple sharpness property [3] needed in the later disscusion.

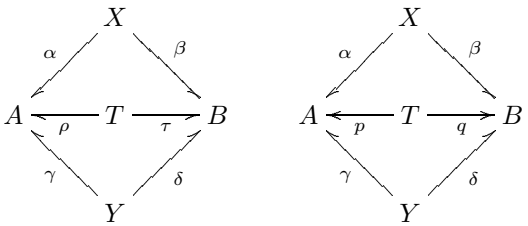
Theorem 1 (Sharpness).

(a) *If two conditions* (1) $\alpha^\sharp\beta \sqcap \gamma^\sharp\delta \sqsubseteq \rho^\sharp\tau$ *and* (2) $\alpha\alpha^\sharp\beta \sqsubseteq \beta$ *hold, then*

$$\alpha\gamma^\sharp \sqcap \beta\delta^\sharp \sqsubseteq (\alpha\rho^\sharp \sqcap \beta\tau^\sharp)(\rho\gamma^\sharp \sqcap \tau\delta^\sharp).$$

(b) *If $p : T \to A$ and $q : T \to B$ is a pair of total functions and two conditions* (i) $p^\sharp q = \nabla_{AB}$ *and* (ii) $\beta\beta^\sharp\beta \sqsubseteq \beta$ *hold, then*

$$\alpha\gamma^\sharp \sqcap \beta\delta^\sharp = (\alpha p^\sharp \sqcap \beta q^\sharp)(p\gamma^\sharp \sqcap q\delta^\sharp).$$



Proof. (a)

$$\begin{aligned}
\alpha\gamma^\sharp \sqcap \beta\delta^\sharp &\sqsubseteq \alpha(\gamma^\sharp \sqcap \alpha^\sharp\beta\delta^\sharp) && \{ \text{ Dedekind Formula } \}\\
&= \alpha\{\gamma^\sharp \sqcap (\gamma^\sharp\delta \sqcap \alpha^\sharp\beta)\delta^\sharp\} && \{ \text{ DF } \}\\
&\sqsubseteq \alpha\{\gamma^\sharp \sqcap (\rho^\sharp\tau \sqcap \alpha^\sharp\beta)\delta^\sharp\} && \{ (1) \}\\
&\sqsubseteq \alpha\{\gamma^\sharp \sqcap (\rho^\sharp \sqcap \alpha^\sharp\beta\tau^\sharp)\tau\delta^\sharp\} && \{ \text{ DF } \}\\
&\sqsubseteq \alpha(\rho^\sharp \sqcap \alpha^\sharp\beta\tau^\sharp)\{(\rho \sqcap \tau\beta^\sharp\alpha)\gamma^\sharp \sqcap \tau\delta^\sharp\} && \{ \text{ DF } \}\\
&\sqsubseteq (\alpha\rho^\sharp \sqcap \alpha\alpha^\sharp\beta\tau^\sharp)(\rho\gamma^\sharp \sqcap \tau\delta^\sharp) && \{ \text{ Sub-distributive } \}\\
&\sqsubseteq (\alpha\rho^\sharp \sqcap \beta\tau^\sharp)(\rho\gamma^\sharp \sqcap \tau\delta^\sharp). && \{ (2) \}
\end{aligned}$$

(b) An inclusion $(\alpha p^\sharp \sqcap \beta q^\sharp)(p\gamma^\sharp \sqcap q\delta^\sharp) \sqsubseteq \alpha\gamma^\sharp \sqcap \beta\delta^\sharp$ is trivial from the univalency $p^\sharp p \sqsubseteq \mathrm{id}_T$ and $q^\sharp q \sqsubseteq \mathrm{id}_T$. Note that $\rho = pp^\sharp$, $\tau = q$, $\hat{\alpha} = \alpha p^\sharp \sqcap \beta q^\sharp$, $\hat{\gamma} = \gamma p^\sharp$, β and δ satisfy the conditions (1) and (2) of (a). (1) $\nabla_{TB} \sqsubseteq pp^\sharp\nabla_{TB} \sqsubseteq p\nabla_{AB} = pp^\sharp q = \rho^\sharp q$ by (i). (2) $\hat{\alpha}\hat{\alpha}^\sharp\beta \sqsubseteq \beta q^\sharp q\beta^\sharp\beta \sqsubseteq \beta\beta^\sharp\beta \sqsubseteq \beta$ by (ii). Also it is easy to see that (*) $\hat{\alpha}\rho^\sharp \sqsubseteq \alpha p^\sharp pp^\sharp = \alpha p^\sharp$ and $\rho\hat{\gamma}^\sharp = pp^\sharp p\gamma^\sharp = p\gamma^\sharp$. Therefore

$$\begin{aligned}
\alpha\gamma^\sharp \sqcap \beta\delta^\sharp &\sqsubseteq (\alpha \sqcap \beta\delta^\sharp\gamma)\gamma^\sharp \sqcap \beta\delta^\sharp && \{ \text{ DF } \}\\
&\sqsubseteq (\alpha \sqcap \beta q^\sharp p)\gamma^\sharp \sqcap \beta\delta^\sharp && \{ p^\sharp q = \nabla_{AB} \ \}\\
&\sqsubseteq (\alpha p^\sharp \sqcap \beta q^\sharp)p\gamma^\sharp \sqcap \beta\delta^\sharp && \{ \text{ DF } \}\\
&= \hat{\alpha}\hat{\gamma}^\sharp \sqcap \beta\delta^\sharp\\
&\sqsubseteq (\hat{\alpha}\rho^\sharp \sqcap \beta q^\sharp)(\rho\hat{\gamma}^\sharp \sqcap q\delta^\sharp) && \{ \text{ (a) } \}\\
&\sqsubseteq (\alpha p^\sharp \sqcap \beta q^\sharp)(p\gamma^\sharp \sqcap q\delta^\sharp). && \{ \text{ (*) } \}
\end{aligned}$$

□

A relation γ is called *difunctional* if it satisfies the condition $\gamma\gamma^\sharp\gamma \sqsubseteq \gamma$. It is obvious that functions are difunctional.

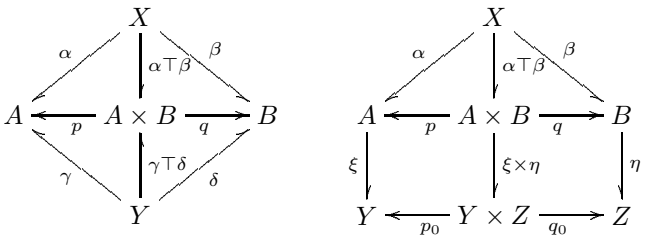
Corollary 1. *Let $(p : A \times B \to A, q : A \times B \to B)$ and $(p_0 : Y \times Z \to Y, q_0 : Y \times Z \to Z)$ be pairs of projections for (A, B) and (Y, Z), respectively.*

(a) *If at least one of four relations $\alpha, \beta, \gamma, \delta$ is difunctional, then*

$$\alpha\gamma^\sharp \sqcap \beta\delta^\sharp = (\alpha\top\beta)(\gamma\top\delta)^\sharp.$$

(b) *If at least one of four relations α, β, ξ, η is difunctional, then*

$$\alpha\xi\top\beta\eta = (\alpha\top\beta)(\xi \times \eta).$$



Proof. It is a direct corollary of Theorem 1(b). □

4 Binary Operations

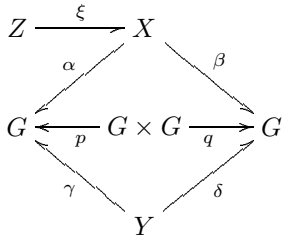
In this section we will study fundamental properties of binary operations in allegories.

Throughout of the rest of the paper we assume that G is an object in an allegory $\mathcal{A}$ and $(p : G \times G \to G, q : G \times G \to G)$ is a pair of projections for (G, G).

Definition 3. A binary operation on G is a relation $\mu : G \times G \rightharpoonup G$ in $\mathcal{A}$. □

Let $\mu : G \times G \rightharpoonup G$ be a binary operation. Then we define $\alpha \odot \beta = (\alpha \top \beta)\mu$ for a pair of relations $\alpha, \beta : X \rightharpoonup G$. Remark that $p \odot q = \mu$.

Lemma 1. *Assume $\mu : G \times G \rightharpoonup G$ is a binary operation on G. Let $\alpha, \alpha', \beta, \beta' : X \rightharpoonup G$, $\gamma, \delta : Y \rightharpoonup G$ and $\xi : Z \rightharpoonup X$ be relations.*



Then the following hold:

(a) *If $\alpha \sqsubseteq \alpha'$ and $\beta \sqsubseteq \beta'$, then $\alpha \odot \beta \sqsubseteq \alpha' \odot \beta'$,*
(b) $\xi(\alpha \odot \beta) \sqsubseteq \xi\alpha \odot \xi\beta$,
(c) $\xi(\alpha \odot \nabla_{XY}\delta) = \xi\alpha \odot \nabla_{ZY}\delta$,
(d) $\xi(\nabla_{XY}\gamma \odot \beta) = \nabla_{ZY}\gamma \odot \xi\beta$,
(e) *If $\xi : Z \rightharpoonup X$ is a function, then $\xi(\alpha \odot \beta) = \xi\alpha \odot \xi\beta$,*
(f) $(\alpha \sqcap \alpha') \odot \beta \sqsubseteq (\alpha \odot \beta) \sqcap (\alpha' \odot \beta)$ *and* $\alpha \odot (\beta \sqcap \beta') \sqsubseteq (\alpha \odot \beta) \sqcap (\alpha \odot \beta')$,

Proof. It is just a corollary of Proposition 2. □

The next proposition is a simple result from the sharpness Corollary 1, but it will play an important rôle in the proof of Theorem 5 and 6.

Proposition 4. *Assume that a binary operation $\mu : G \times G \rightharpoonup G$ is total. If at least one of four relations $\alpha, \beta : X \rightharpoonup G$ and $\gamma, \delta : Y \rightharpoonup G$ is difunctional, then*

$$\alpha\gamma^\sharp \sqcap \beta\delta^\sharp \sqsubseteq (\alpha \odot \beta)(\gamma \odot \delta)^\sharp.$$

Proof. It is immediate from Corollary 1 (sharpness):

$$\begin{aligned} \alpha\gamma^\sharp \sqcap \beta\delta^\sharp &= (\alpha \top \beta)(\gamma \top \delta)^\sharp && \{ \text{ Corollary 1(a) } \} \\ &\sqsubseteq (\alpha \top \beta)\mu\mu^\sharp(\gamma \top \delta)^\sharp && \{ \text{ } \mathrm{id}_{G\times G} \sqsubseteq \mu\mu^\sharp \text{ } (\mu : \text{total}) \text{ } \} \\ &= (\alpha \odot \beta)(\gamma \odot \delta)^\sharp. \end{aligned}$$

□

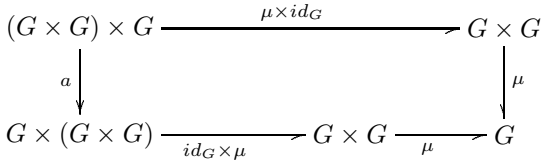
Definition 4. A (relational) semigroup $G = (G, \mu)$ in an allegory $\mathcal{A}$ is a pair of an object G in $\mathcal{A}$ and a binary operation $\mu : G \times G \rightharpoonup G$ in $\mathcal{A}$, satisfying the associative law $(\mu \times \mathrm{id}_G)\mu = a(\mathrm{id}_G \times \mu)\mu$, where $a = a_{GGG} : (G \times G) \times G \to G \times (G \times G)$ is the associative function. □

The associative law is an indispensable property on binary operations to simplify iterations of operations. There are often difficulties when one manipulates the associative law in terms of morphisms. So it is convenient to use the traditional form of the associative law

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

The following theorem guarantees that the associative law in terms of morphisms and the traditional form of the associative law using global elements are equivalent.

Theorem 2. *A binary operation $\mu : G \times G \rightharpoonup G$ satisfies the associative law $(\mu \times \mathrm{id}_G)\mu = a(\mathrm{id}_G \times \mu)\mu$ if and only if $(\alpha \odot \beta) \odot \gamma = \alpha \odot (\beta \odot \gamma)$ for all relations $\alpha, \beta, \gamma : X \rightharpoonup G$.*



Proof. ($\Rightarrow$)

$$\begin{aligned}
(\alpha \odot \beta) \odot \gamma &= \{(\alpha \top \beta)\mu \top \gamma\}\mu \\
&= \{(\alpha \top \beta) \top \gamma\}(\mu \times \mathrm{id}_G)\mu && \{ \text{ Corollary 1(b) (sharpness) } \} \\
&= \{(\alpha \top \beta) \top \gamma\} a(\mathrm{id}_G \times \mu)\mu && \{ \text{ associative law } \} \\
&= \{\alpha \top (\beta \top \gamma)\}(\mathrm{id}_G \times \mu)\mu && \{ \text{ Proposition 3(a) } \} \\
&= \{\alpha \top (\beta \top \gamma)\mu\}\mu && \{ \text{ Corollary 1(b) (sharpness) } \} \\
&= \alpha \odot (\beta \odot \gamma)
\end{aligned}$$

($\Leftarrow$)

$$\begin{aligned}
(\mu \times \mathrm{id}_G)\mu &= (p_1\mu \top q_1)\mu && \{ \mu \times \mathrm{id}_G = p_1\mu \top q_1 \} \\
&= p_1(p \odot q) \odot q_1 && \{ \mu = p \odot q \} \\
&= (p_1 p \odot p_1 q) \odot q_1 && \{ \text{ Lemma 1(e) } \} \\
&= p_1 p \odot (p_1 q \odot q_1) && \{ \text{ (associative law) } \} \\
&= a p_2 \odot (a q_2 p \odot a q_2 q) && \{ a p_2 = p_1 p, a q_2 p = p_1 q, a q_2 q = q_1 \} \\
&= a(p_2 \top q_2 \mu)\mu && \{ \text{ Lemma 1(e), } \mu = p \odot q \} \\
&= a(\mathrm{id}_G \times \mu)\mu && \{ \mathrm{id}_G \times \mu = p_2 \top q_2 \mu \}
\end{aligned}$$

□

Remark. It is trivial that a binary operation $\mu : G \times G \rightharpoonup G$ satisfies the commutative law $t\mu = \mu$ (where $t : G \times G \to G \times G$ is the twisting function defined by $t = q \top p$) if and only if $\alpha \odot \beta = \beta \odot \alpha$ for all relations $\alpha, \beta : X \rightharpoonup G$.

5 Unitary and Inverse Operations

A *unit* I is an object in an allegory $\mathcal{A}$ such that $\mathrm{id}_I = \nabla_{II}$. In what follows we assume that $\mathcal{A}$ has a unit I. A total function $x : I \to X$ is called an *I-point* of an object X. A relation $\rho : I \rightharpoonup X$ is *nonempty* if there is some I-point $x : I \to X$ such that $x \sqsubseteq \rho$.

In this section we assume $G = (G, \mu)$ is a semigroup in an allegory $\mathcal{A}$.

Proposition 5. *Let $\varepsilon, \varepsilon' : I \rightharpoonup G$ be relations. Then*

(a) $\mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$ *iff* $\alpha \odot \nabla_{XI}\varepsilon = \alpha$ *for all relations* $\alpha : X \rightharpoonup G$.
(b) $\nabla_{GI}\varepsilon \odot \mathrm{id}_G = \mathrm{id}_G$ *iff* $\nabla_{XI}\varepsilon \odot \alpha = \alpha$ *for all relations* $\alpha : X \rightharpoonup G$,
(c) *If* $\mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$ *and* $\nabla_{GI}\varepsilon' \odot \mathrm{id}_G = \mathrm{id}_G$, *then* $\varepsilon = \varepsilon'$.
(d) *If* $\mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$ *or* $\nabla_{GI}\varepsilon \odot \mathrm{id}_G = \mathrm{id}_G$, *then* $\mu^\sharp$ *is total.*

Proof. (a) ($\Rightarrow$)

$$\begin{aligned}
\alpha &= \alpha\,\mathrm{id}_G \\
&= \alpha(\mathrm{id}_G \odot \nabla_{GI}\varepsilon) && \{ \mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G \} \\
&= \alpha\,\mathrm{id}_G \odot \nabla_{XI}\varepsilon \\
&= \alpha \odot \nabla_{XI}\varepsilon && \{ \text{ Lemma 1(c) } \}
\end{aligned}$$

($\Leftarrow$) Set $\alpha = \mathrm{id}_G$. Then $\mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$ simply follows from $\alpha = \alpha \odot \nabla_{XI}\varepsilon$.
(b) It is similar to (a).
(c)

$$\begin{aligned}
\varepsilon' &= \varepsilon' \odot \nabla_{II}\varepsilon && \{ \text{ (a) : } \mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G \} \\
&= \varepsilon' \odot \varepsilon && \{ \nabla_{II} = \mathrm{id}_I \} \\
&= \nabla_{II}\varepsilon' \odot \varepsilon && \{ \mathrm{id}_I = \nabla_{II} \} \\
&= \varepsilon && \{ \text{ (b) : } \nabla_{GI}\varepsilon' \odot \mathrm{id}_G = \mathrm{id}_G \}
\end{aligned}$$

(d) Assume $\mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$. Then $\nabla_{GG} = \nabla_{GG}(\mathrm{id}_G \top \nabla_{GI}\varepsilon)\mu \sqsubseteq \nabla_{GG \times G}\mu$ and so $\nabla_{GG \times G}\mu = \nabla_{GG}$, which is equivalent to $\mathrm{id}_G \sqsubseteq \mu^\sharp\mu$. □

A relation $\varepsilon : I \rightharpoonup G$ is called a *unitary* operation for μ if it satisfies two conditions $\mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$ and $\nabla_{GI}\varepsilon \odot \mathrm{id}_G = \mathrm{id}_G$. As in the ordinary group theory a unitary operation for a binary operation is unique by Proposition 5(c).

Corollary 2. *Let $\varepsilon : I \rightharpoonup G$ a unitary operation for μ, and let $\alpha, \beta, \gamma : X \rightharpoonup G$ be relations. If $\alpha \odot \beta = \beta \odot \gamma = \nabla_{XI}\varepsilon$, then $\alpha = \gamma$.*

Proof.

$$\begin{array}{ll} \alpha = \alpha \odot \nabla_{XI}\varepsilon & \{ \text{ Proposition 5(a) : } \mathrm{id}_G = \mathrm{id}_G \odot \nabla_{GI}\varepsilon \ \} \\ = \alpha \odot (\beta \odot \gamma) & \{ \ \beta \odot \gamma = \nabla_{XI}\varepsilon \ \} \\ = (\alpha \odot \beta) \odot \gamma & \{ \text{ (associative) } \} \\ = \nabla_{XI}\varepsilon \odot \gamma & \{ \ \alpha \odot \beta = \nabla_{XI}\varepsilon \ \} \\ = \gamma. & \{ \text{ Proposition 5(b) : } \mathrm{id}_G = \nabla_{GI}\varepsilon \odot \mathrm{id}_G \ \} \end{array}$$

□

The following states that a nonempty unitary operation for a total binary operation is an I-point.

Theorem 3. *Let $\varepsilon : I \rightharpoonup G$ be a unitary operation for μ. If μ is total and ε is nonempty, then ε is an I-point.*

Proof. As ε is nonempty there is an I-point $e : I \to G$ such that $e \sqsubseteq \varepsilon$. Then $\mathrm{id}_G \odot \nabla_{GI}e = (\mathrm{id}_G \top \nabla_{GI}e)\mu$ is total (since μ is total by the assumtion) and $\mathrm{id}_G \odot \nabla_{GI}e \sqsubseteq \mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$. Hence $\mathrm{id}_G \odot \nabla_{GI}e = \mathrm{id}_G$ (remarking that $\mathrm{id}_G \odot \nabla_{GI}e$ is total and id_G is a function), and so $\varepsilon = e$ by Proposition 5(c). □

Remark. Every total relation $\varepsilon : I \rightharpoonup G$ is nonempty under the *relational axiom of choice* : For all relations $\alpha : A \rightharpoonup B$ there exists a function $f : A \to B$ such that $f \sqsubseteq \alpha$ and $f\nabla_{BA} = \alpha\nabla_{BA}$. □

The notion of inverse operations of course depends on unitary operations. Here we only mention a few general properties on inverse-like relations.

Corollary 3. *Let $\varepsilon : I \rightharpoonup G$ be a unitary operation for μ. If two relations $\iota, \iota' : G \rightharpoonup G$ satisfy $\mathrm{id}_G \odot \iota = \iota' \odot \mathrm{id}_G = \nabla_{GI}\varepsilon$, then $\iota = \iota'$.*

Proof. It directly follows from Corollary 2. □

Recall a fundamental excercise in the ordinary group theory: If $\forall x \in G : xe = x$ and $\forall x \in G \exists y \in G : xy = e$ for some element $e \in G$, then $\forall x \in G : ex = x$ and $\forall x \in G \exists y \in G : yx = e$. (Answer. Assume $xy = e$ and $yz = e$. Then $yx = (yx)e = (yx)(yz) = (y(xy))z = (ye)z = yz = e$ and $ex = (xy)x = x(yx) = xe = x$.)

The above fact reflects the following theorem on our framework:

Theorem 4. *Let $\varepsilon : I \rightharpoonup G$ and $\iota : G \rightharpoonup G$ be relations satisfying $\mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$ and $\mathrm{id}_G \odot \iota = \nabla_{GI}\varepsilon$. Then the following four conditions are equivalent:*

(a) *ι is a total function,*
(b) *$\iota \odot \iota^2 = \nabla_{GI}\varepsilon$,*
(c) *$\nabla_{GI}\varepsilon \odot \iota^2 = \mathrm{id}_G$ and $\nabla_{GI}\varepsilon \odot \mathrm{id}_G = \mathrm{id}_G$,*
(d) *$\iota^2 = \mathrm{id}_G$.*

Proof. (a)⇒(b)

$$\begin{array}{ll} \iota \odot \iota^2 = \iota(\mathrm{id}_G \odot \iota) & \{ \text{ Lemma 1(e) } \iota : \text{function } \} \\ = \iota\nabla_{GI}\varepsilon & \{ \ \mathrm{id}_G \odot \iota = \nabla_{GI}\varepsilon \ \} \\ = \nabla_{GI}\varepsilon. & \{ \ \iota : \text{total } \} \end{array}$$

(b)⇒(c) (i)

$$\begin{array}{ll} \nabla_{GI}\varepsilon \odot \iota^2 = (\mathrm{id}_G \odot \iota) \odot \iota^2 & \{ \ \mathrm{id}_G \odot \iota = \nabla_{GI}\varepsilon \ \} \\ = \mathrm{id}_G \odot (\iota \odot \iota^2) & \{ \text{ (associative) } \} \\ = \mathrm{id}_G \odot \nabla_{GI}\varepsilon & \{ \text{ (b) } \} \\ = \mathrm{id}_G, & \{ \ \mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G \ \} \end{array}$$

(ii)

$$\begin{aligned}\iota \odot \mathrm{id}_G &= \iota \odot (\nabla_{GI}\varepsilon \odot \iota^2) && \{\text{ (i) }\}\\ &= (\iota \odot \nabla_{GI}\varepsilon) \odot \iota^2 && \{\text{ (associative) }\}\\ &= \iota \odot \iota^2 && \{\ \mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G\ \}\\ &= \nabla_{GI}\varepsilon, && \{\text{ (b }\}\end{aligned}$$

(iii)

$$\begin{aligned}\nabla_{GI}\varepsilon \odot \mathrm{id}_G &= (\mathrm{id}_G \odot \iota) \odot \mathrm{id}_G && \{\ \mathrm{id}_G \odot \iota = \nabla_{GI}\varepsilon\ \}\\ &= \mathrm{id}_G \odot (\iota \odot \mathrm{id}_G) && \{\text{ (associative) }\}\\ &= \mathrm{id}_G \odot \nabla_{GI}\varepsilon && \{\text{ (ii) }\}\\ &= \mathrm{id}_G. && \{\ \mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G\ \}\end{aligned}$$

(c)⇒(d)

$$\begin{aligned}\iota^2 &= \iota^2(\nabla_{GI}\varepsilon \odot \mathrm{id}_G) && \{\text{ (c) }\}\\ &= \nabla_{GI}\varepsilon \odot \iota^2 && \{\text{ Lemma 1(d) }\}\\ &= \mathrm{id}_G. && \{\text{ (c) }\}\end{aligned}$$

(d)⇒(a) It is trivial by Proposition 1. □

Remark. Supposed the relational axiom of choice. If $\mathrm{id}_G \odot \nabla_{GI}\varepsilon = \mathrm{id}_G$ and $\mathrm{id}_G \odot \iota = \nabla_{GI}\varepsilon$, and if $\mu : G\times G \rightharpoonup G$ and $\iota : G \rightharpoonup G$ are total and $\varepsilon : I \rightharpoonup G$ is a function, then ι is a (unique) total function. (By the relational axiom of choice there exists a total function $i : G \to G$ such that $i \sqsubseteq \iota$. Then $\mathrm{id}_G \odot i \sqsubseteq \mathrm{id}_G \odot \iota = \nabla_{GI}\varepsilon$ and so $\mathrm{id}_G \odot i = \nabla_{GI}\varepsilon$, since $\mathrm{id}_G \odot i$ is total and $\nabla_{GI}\varepsilon$ is a function. Hence, by the virtue of the last Theorem 4, i is a right and left inverse, and finally we have $\iota = i$ by Corollary 3.)

6 Groups

In this section we define the notion of subgroups and residual relations induced by subgroups, and show a fundamental fact that the residual relations are equivalence relations in allegories. However we limit all the operations of group structures to be total functions for the sake of simplicity.

Definition 5. A group $G = (G, m, e, i)$ in an allegory $\mathcal{A}$ is a quartet of an object G and three total functions $m : G \times G \to G$, $e : I \to G$ and $i : G \to G$ satisfying the following conditions:
(Associative Law) $(m \times \mathrm{id}_G)m = a(\mathrm{id}_G \times m)m$,
(Right Unitary) $(\mathrm{id}_G \top \nabla_{GI}e)m = \mathrm{id}_G$,
(Right Inverse) $(\mathrm{id}_G \top i)m = \nabla_{GI}e$.

□

The following proposition is trivial from the arguments in the previous sections:

Proposition 6. *Let $G = (G, m, e, i)$ be a group and $\alpha, \beta, \gamma : X \rightharpoonup G$ relations in an allegory $\mathcal{A}$. Then the following hold:*

(a) $(\alpha \odot \beta) \odot \gamma = \alpha \odot (\beta \odot \gamma)$ (associative),
(b) $\alpha \odot \nabla_{XI}e = \nabla_{XI}e \odot \alpha = \alpha$ (unitary),
(c) $\mathrm{id}_G \odot i = i \odot \mathrm{id}_G = \nabla_{GI}e$, (inverse),
(d) $i^2 = \mathrm{id}_G$,
(e) $ei = e$ *and* $e \odot e = e$,
(f) $mi = qi \odot pi$.

Proof. The statement (a) has already been seen in Theorem 2. The statements (b), (c) and (d) follow from Proposition 5 and Theorem 4.
(e) An identity $e \odot e = e$ is trivial by (b) and it is easily seen that $ei = ei \odot e = e(i \odot \mathrm{id}_G) = e\nabla_{GI}e = e$.
(f) It follows from Corollary 2, since we have $mi \odot m = (qi \odot pi) \odot m = \nabla_{G\times GI}e$ as follows:

$$\begin{aligned}mi \odot m &= m(i \odot \mathrm{id}_G) && \{\text{ Lemma 1(e) }\}\\ &= m\nabla_{GI}e && \{\ i \odot \mathrm{id}_G = \nabla_{GI}\ \}\\ &= \nabla_{G\times GI}e && \{\ m : \text{total }\}\end{aligned}$$

and

$$\begin{aligned}
m \odot (qi \odot pi) &= (p \odot q) \odot (qi \odot pi) && \{\ m = p \odot q\ \} \\
&= \{p \odot (q \odot qi)\} \odot pi && \{\ \text{(associative)}\ \} \\
&= \{p \odot q(\mathrm{id}_G \odot i)\} \odot pi && \{\ \text{Lemma 1(e)}\ \} \\
&= (p \odot q\nabla_{GI} e) \odot pi \\
&= (p \odot \nabla_{G\times GI} e) \odot pi && \{\ q : \text{total}\ \} \\
&= p \odot pi \\
&= p(\mathrm{id}_G \odot i) && \{\ 1\text{(e)}\ \} \\
&= p\nabla_{GI} e \\
&= \nabla_{G\times GI} e. && \{\ p : \text{total}\ \}
\end{aligned}$$

Note that $qi \odot pi = t(i \times i)m$ where $t = q \top p : G \times G \to G \times G$ is the twisting function. □

In what follows we assume $G = (G, m, e, i)$ is a group in an allegory $\mathcal{A}$. In relational calculus there are a few different ways how to specify subobjects. For example, Schmidt and Ströhlein [9] made use of "vectors", to represent subobjects in relation algebras. We are going to use relations from a unit I into some object G; these do in fact satisfy the vector equation $\nabla_{II}\rho = \rho$.

Definition 6. A nonempty relation $\rho : I \rightharpoonup G$ is a *subgroup* of G if $\rho i \sqsubseteq \rho$ and $\rho \odot \rho \sqsubseteq \rho$. □

Note that every subgroup $\rho : I \rightharpoonup G$ contains the unitary operation $e : I \to G$, that is, $e \sqsubseteq \rho$: Assume $x \sqsubseteq \rho$ for some I-point $x : I \to G$. Then $e = x\nabla_{GI} e = x(i \odot \mathrm{id}_G) = xi \odot x \sqsubseteq \rho i \odot \rho \sqsubseteq \rho \odot \rho \sqsubseteq \rho$. Thus a relation $\rho : I \rightharpoonup G$ is a subgroup of G iff $e \sqsubseteq \rho$, $\rho i = \rho$ and $\rho \odot \rho = \rho$. The unitary operation e and the universal relation ∇_{IG} are trivial subgroups of G.

Proposition 7. *If $\rho, \rho' : I \rightharpoonup G$ are two subgroups of G, then so is $\rho \sqcap \rho'$.*

Proof. It is trivial. □

Now let us go back to an exercise (that is, the second question (b) in the introduction) in classical group theory: Let S be a subgroup of a group G. Prove that the right residual relation $x \equiv y$ on G, defined by $x^{-1}y \in S$, is an equivalence relation. (Answer. The reflexive law: $x^{-1}x = e \in S$, the symmetric law: If $x^{-1}y \in S$, then $y^{-1}x = (x^{-1}y)^{-1} \in S$, and the transitive law: If $x^{-1}y \in S$ and $y^{-1}z \in S$, then $x^{-1}z = (x^{-1}y)(y^{-1}z) \in S$.)

The following theorem is a generalization of this fundamental fact.

Theorem 5. *If $\rho : I \rightharpoonup G$ is a subgroup, then $\theta = \mathrm{id}_G \odot \nabla_{GI}\rho$ is an equivalence relation on G.*

Proof. Reflexivity $\mathrm{id}_G \sqsubseteq \theta$ is direct from $\mathrm{id}_G = \mathrm{id}_G \odot \nabla_{GI} e \sqsubseteq \mathrm{id}_G \odot \nabla_{GI}\rho = \theta$. Next we can show transitivity $\theta\theta \sqsubseteq \theta$ by the following computation:

$$\begin{aligned}
\theta\theta &= \theta(\mathrm{id}_G \odot \nabla_{GI}\rho) \\
&\sqsubseteq \theta \odot \theta\nabla_{GI}\rho && \{\ \text{Lemma 1(b)}\ \} \\
&\sqsubseteq \theta \odot \nabla_{GI}\rho && \{\ \theta\nabla_{GI} \sqsubseteq \nabla_{GI}\ \} \\
&= (\mathrm{id}_G \odot \nabla_{GI}\rho) \odot \nabla_{GI}\rho \\
&= \mathrm{id}_G \odot (\nabla_{GI}\rho \odot \nabla_{GI}\rho) && \{\ \text{(associative)}\ \} \\
&= \mathrm{id}_G \odot \nabla_{GI}(\rho \odot \rho) && \{\ \nabla_{GI} : \text{total function, Lemma 1(e)}\ \} \\
&\sqsubseteq \mathrm{id}_G \odot \nabla_{GI}\rho && \{\ \rho \odot \rho \sqsubseteq \rho\ \} \\
&= \theta.
\end{aligned}$$

Finally we will see symmetry $\theta^\sharp \sqsubseteq \theta$. The proof is somewhat complicated as follows:

$$\begin{aligned}
\theta &= (p^\sharp \sqcap \nabla_{GI}\rho q^\sharp)m \\
&= \{p^\sharp \sqcap \nabla_{GI}\rho(q^\sharp \sqcap \rho^\sharp \nabla_{IG\times G})\}m && \{\ \rho q^\sharp = \rho(q^\sharp \sqcap \rho^\sharp \nabla_{IG\times G}) : \mathrm{DF}\ \} \\
&= \{p^\sharp \sqcap \nabla_{GI}\rho(q^\sharp \sqcap i\rho^\sharp \nabla_{IG\times G})\}m && \{\ \rho i = \rho,\ i^\sharp = i\ \} \\
&\sqsubseteq \{p^\sharp \sqcap \nabla_{GI}\rho(\mathrm{id}_G \odot i)(q \odot \nabla_{G\times GI}\rho)^\sharp\}m && \{\ \text{Proposition 4}\ \} \\
&= \{p^\sharp \sqcap \nabla_{GI}\rho\nabla_{GI}e(q \odot \nabla_{G\times GI}\rho)^\sharp\}m && \{\ \mathrm{id}_G \odot i = \nabla_{GI}e\ \} \\
&= \{p^\sharp \sqcap \nabla_{GI}e(q \odot \nabla_{G\times GI}\rho)^\sharp\}m && \{\ \rho\nabla_{GI} = \mathrm{id}_I\ \} \\
&\sqsubseteq (\mathrm{id}_G \odot \nabla_{GI}e)\{p \odot (q \odot \nabla_{G\times GI}\rho)\}^\sharp m && \{\ \text{Proposition 4}\ \} \\
&= \{(p \odot q) \odot \nabla_{G\times GI}\rho\}^\sharp m && \{\ \mathrm{id}_G \odot \nabla_{GI}e = \mathrm{id}_G\ \} \\
&= (m \odot \nabla_{G\times GI}\rho)^\sharp m && \{\ p \odot q = m\ \} \\
&= \{m(\mathrm{id}_G \odot \nabla_{GI}\rho)\}^\sharp m && \{\ \text{Lemma 1(c)}\ \} \\
&= \theta^\sharp m^\sharp m \\
&\sqsubseteq \theta^\sharp. && \{\ m : \text{function}\ \}
\end{aligned}$$

□

7 Normal Subgroups

In the final section we define normal subgroups of groups in allegories and show the main result that normal subgroups of a group form a modular lattice.

In classical group theory a subgroup of a group is normal iff the right and the left residual relations coincide. We adopt this property to define normal subgroups in our framework:

Definition 7. A subgroup $\rho : I \rightharpoonup G$ of G is called *normal* if $\mathrm{id}_G \odot \nabla_{GI}\rho = \nabla_{GI}\rho \odot \mathrm{id}_G$. □

It is trivial that a subgroup $\rho : I \rightharpoonup G$ is normal iff $\alpha \odot \nabla_{XI}\rho = \nabla_{XI}\rho \odot \alpha$ for all relations $\alpha : X \rightharpoonup G$.

The following is also an analogy from the classical case:

Proposition 8. *If $\rho, \sigma : I \rightharpoonup G$ are normal subgroups of G, then so is $\rho \odot \sigma$.*

Proof. It is easy to see that $\rho \odot \sigma$ is a subgroup of G. We only show the normality:

$$\begin{aligned}
\mathrm{id}_G \odot \nabla_{GI}(\rho \odot \sigma) &= \mathrm{id}_G \odot (\nabla_{GI}\rho \odot \nabla_{GI}\sigma) && \{\ \text{Lemma 1(e)}\ \} \\
&= (\mathrm{id}_G \odot \nabla_{GI}\rho) \odot \nabla_{GI}\sigma \\
&= (\nabla_{GI}\rho \odot \mathrm{id}_G) \odot \nabla_{GI}\sigma && \{\ \rho : \text{normal}\ \} \\
&= \nabla_{GI}\rho \odot (\mathrm{id}_G \odot \nabla_{GI}\sigma) \\
&= \nabla_{GI}\rho \odot (\nabla_{GI}\sigma \odot \mathrm{id}_G) && \{\ \sigma : \text{normal}\ \} \\
&= (\nabla_{GI}\rho \odot \nabla_{GI}\sigma) \odot \mathrm{id}_G \\
&= \nabla_{GI}(\rho \odot \sigma) \odot \mathrm{id}_G. && \{\ \text{Lemma 1(e)}\ \}
\end{aligned}$$

□

Let $\rho, \sigma : I \rightharpoonup G$ be normal subgroups of G. Then it is obvious that the normal subgroup $\rho \odot \sigma$ is the supremum (or, join) of ρ and σ with respect to the relational inclusion $\sqsubseteq$ of normal subgroups.

Definition 8. Let $m : X \times X \to X$ be a binary operation on X. A relation $\theta : X \rightharpoonup X$ is a *congruence* with respect to m if it is an equivalence relation such that $(\theta \times \theta)m \sqsubseteq m\theta$. □

Proposition 9. *If $\rho : I \rightharpoonup G$ is a normal subgroup of G, then $\theta = \mathrm{id}_G \odot \nabla_{GI}\rho$ is a congruence with respect to m.*

Proof.

$$\begin{aligned}
(\theta \times \theta)m &= (p\theta \top q\theta)m \\
&= p\theta \odot q\theta \\
&= p(\mathrm{id}_G \odot \nabla_{GI}\rho) \odot q(\mathrm{id}_G \odot \nabla_{GI}\rho) \\
&= (p \odot \nabla_{G\times GI}\rho) \odot (q \odot \nabla_{G\times GI}\rho) && \{\text{ Lemma 1(e) }\} \\
&= p \odot (\nabla_{G\times GI}\rho \odot q) \odot \nabla_{G\times GI}\rho && \{\text{ (associative) }\} \\
&= p \odot (q \odot \nabla_{G\times GI}\rho) \odot \nabla_{G\times GI}\rho && \{\text{ } \rho : \text{normal }\} \\
&= (p \odot q) \odot (\nabla_{G\times GI}\rho \odot \nabla_{G\times GI}\rho) && \{\text{ (associative) }\} \\
&= m \odot \nabla_{G\times GI}(\rho \odot \rho) && \{\text{ } m = p \odot q,\ \text{Lemma 1(e) }\} \\
&= m \odot \nabla_{G\times GI}\rho && \{\text{ } \rho : \text{subgroup }\} \\
&= m(\mathrm{id}_G \odot \nabla_{GI}\rho) && \{\text{ Lemma 1(c) }\} \\
&= m\theta
\end{aligned}$$

□

In the ordinary group theory it is well-known that the set of all normal subgroups of a group forms a modular lattice. In other words, for three normal subgroups S, T and U of a group G the following modular law holds:

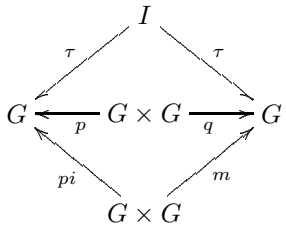
$$S \subseteq U \implies ST \cap U \subseteq S(T \cap U).$$

The proof of the fact is fundamental: Assume $S \subseteq U$ and $x \in ST \cap U$. Then $x \in U$ and $x \in ST$, so $x = st$ for some $s \in S$ and $t \in T$. Hence $t = s^{-1}x \in U$ holds since $x \in U$ and $s \in S \subseteq U$ and U is a subgroup. That is, $x = st$ with $s \in S$ and $t \in T \cap U$. Hence $x \in S(T \cap U)$.

To see the above fact in allegories we need the next lemma:

Lemma 2. *If $\tau : I \rightharpoonup G$ is a subgroup of G, then $\tau p^\sharp \sqcap \tau m^\sharp \sqsubseteq \tau q^\sharp$.*

Proof. First recall that $\tau = \tau i$. Applying Proposition 4



we have

$$\begin{aligned}
\tau p^\sharp \sqcap \tau m^\sharp &= \tau i^\sharp p^\sharp \sqcap \tau m^\sharp && \{\text{ } \tau = \tau i^\sharp \text{ }\} \\
&\sqsubseteq (\tau \odot \tau)(pi \odot m)^\sharp && \{\text{ Proposition 4 }\} \\
&\sqsubseteq \tau(pi \odot m)^\sharp. && \{\text{ } \tau \odot \tau \sqsubseteq \tau \text{ }\}
\end{aligned}$$

On the other hand we can see the identity $pi \odot m = q$ from

$$\begin{aligned}
pi \odot m &= pi \odot (p \odot q) && \{\text{ } m = p \odot q \text{ }\} \\
&= (pi \odot p) \odot q && \{\text{ (associative) }\} \\
&= p(i \odot \mathrm{id}_G) \odot q && \{\text{ Lemma 1(e) }\} \\
&= p\nabla_{GI}e \odot q && \{\text{ } i \odot \mathrm{id}_G = \nabla_{GI}e \text{ }\} \\
&= \nabla_{G\times GI}e \odot q && \{\text{ } p : \text{total }\} \\
&= q. && \{\text{ Proposition 6(b) }\}
\end{aligned}$$

□

Finally we prove a main result that the set of all normal subgroups in allegories forms a modular lattice, as in the classical case:

Theorem 6. *Let $\rho, \sigma, \tau : I \rightharpoonup G$ be normal subgroups of a group G. If $\rho \sqsubseteq \tau$, then $(\rho \odot \sigma) \sqcap \tau \sqsubseteq \rho \odot (\sigma \sqcap \tau)$.*

Proof. It follows from the simple computation:

$$\begin{aligned}
(\rho \odot \sigma) \sqcap \tau &= (\rho p^\sharp \sqcap \sigma q^\sharp) m \sqcap \tau \\
&\sqsubseteq (\rho p^\sharp \sqcap \sigma q^\sharp \sqcap \tau m^\sharp) m && \{ \text{ DF } \} \\
&= \{\rho p^\sharp \sqcap \sigma q^\sharp \sqcap (\tau p^\sharp \sqcap \tau m^\sharp)\} m && \{ \rho \sqsubseteq \tau \} \\
&\sqsubseteq (\rho p^\sharp \sqcap \sigma q^\sharp \sqcap \tau q^\sharp) m && \{ \text{ Lemma 2 : } \tau p^\sharp \sqcap \tau m^\sharp \sqsubseteq \tau q^\sharp \} \\
&= \{\rho p^\sharp \sqcap (\sigma \sqcap \tau) q^\sharp\} m \\
&= \rho \odot (\sigma \sqcap \tau).
\end{aligned}$$

□

References

1. C. Brink, W. Kahl and G. Schmidt (eds.), Relational methods in computer science. Advances in Computing Science, (Springer, Wien, New York, 1997).
2. P. Freyd and A. Scedrov, Categories, allegories (North-Holland, Amsterdam, 1990).
3. J. Desharnais, *Monomorphic characterization of n-ary direct products*, Information Sciences **119**(1999), 275–288.
4. W. Kahl and G. Schmidt, *Exploring (finite) relation algebras using tools written in Haskell*, Technical Report 2000-02, Fakultät für Informatik, Universität der Bundeswehr München, October 2000.
5. Y. Kawahara, *Relational set theory*, Lecture Notes in Computer Science, **953**(1995), 44–58.
6. Y. Kawahara, *Lattices in Dedekind categories*, In: Orlowska, E. and Szalas, A. (Eds), Relational Methods for Computer Science Applications, Physica-Verlag, 2001.
7. S. Mac Lane, *Categories for the working mathematician*, (Springer-Verlag, 1972).
8. R. Maddux, *On the derivation of identities invloving projection functions*, Logic Colloquium '92, ed. Csirmaz, Gabbay, de Rijke, Center for the Study of Language and Information Publications, Stanford, 1995, 145–163.
9. G. Schmidt and T. Ströhlein, Relations and graphs – Discrete Mathematics for Computer Science – (Springer-Verlag, 1993).
10. A. Rosenfeld, *Fuzzy groups*, J. Math. Anal. Appl. **35**(1971), 512–517.