FORMALIZED MATHEMATICS
Vol. **27**, No. **4**, Pages 321–335, **2019**
DOI: 10.2478/forma-2019-0027

sciendo
https://www.sciendo.com/

AIM Loops and the AIM Conjecture[1]

Chad E. Brown
Český Institut Informatiky Robotiky a Kybernetiky
Zikova 4, 166 36 Praha 6,
Czech Republic

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. In this article, we prove, using the Mizar [2] formalism, a number of properties that correspond to the AIM Conjecture. In the first section, we define division operations on loops, inner mappings T, L and R, commutators and associators and basic attributes of interest. We also consider subloops and homomorphisms. Particular subloops are the nucleus and center of a loop and kernels of homomorphisms. Then in Section 2, we define a set Mlt Q of multiplicative mappings of Q and cosets (mostly following Albert 1943 for cosets [1]). Next, in Section 3 we define the notion of a normal subloop and construct quotients by normal subloops. In the last section we define the set InnAut of inner mappings of Q, define the notion of an AIM loop and relate this to the conditions on T, L, and R defined by satisfies TT, etc. We prove in Theorem (67) that the nucleus of an AIM loop is normal and finally in Theorem (68) that the AIM Conjecture follows from knowing every AIM loop satisfies aa1, aa2, aa3, Ka, aK1, aK2 and aK3.

The formalization follows M.K. Kinyon, R. Veroff, P. Vojtechovsky [4] (in [3]) as well as Veroff's Prover9 files.

MSC: 20N05 68T99 03B35

Keywords: loops; Abelian inner mapping; groups

MML identifier: `AIMLOOP`, version: `8.1.09 5.59.1363`

[1]This work has been supported by the European Research Council (ERC) Consolidator grant nr. 649043 *AI4REASON* and the Polish National Science Centre granted by decision no. DEC-2015/19/D/ST6/01473.

ISSN 1426–2630(Print), 1898-9934(Online)

1. Loops – Introduction

From now on Q, Q_1, Q_2 denote multiplicative loops and x, y, z, w, u, v denote elements of Q. Let X be a 1-sorted structure.

A permutation of X is a permutation of the carrier of X. Let Y be a 1-sorted structure. The functor Y^X yielding a set is defined by the term

(Def. 1) (the carrier of Y)$^{\alpha}$, where α is the carrier of X.

Let X, Y be 1-sorted structures. Let us observe that Y^X is functional.

Let Q be an invertible, left mult-cancelable, non empty multiplicative loop structure and x, y be elements of Q. The functor $x \setminus y$ yielding an element of Q is defined by

(Def. 2) $x \cdot it = y$.

Let Q be an invertible, right mult-cancelable, non empty multiplicative loop structure. The functor x/y yielding an element of Q is defined by

(Def. 3) $it \cdot y = x$.

Let us consider Q, x, and y. Note that $x \setminus (x \cdot y)$ reduces to y and $x \cdot (x \setminus y)$ reduces to y and $x \cdot y/y$ reduces to x and $(x/y) \cdot y$ reduces to x.

Let Q be an invertible, left mult-cancelable, non empty multiplicative loop structure and u, x be elements of Q. The functor $\mathtt{T}(u, x)$ yielding an element of Q is defined by the term

(Def. 4) $x \setminus (u \cdot x)$.

Let u, x, y be elements of Q. The functor $\mathtt{L}(u, x, y)$ yielding an element of Q is defined by the term

(Def. 5) $y \cdot x \setminus (y \cdot (x \cdot u))$.

Let Q be an invertible, right mult-cancelable, non empty multiplicative loop structure. The functor $\mathtt{R}(u, x, y)$ yielding an element of Q is defined by the term

(Def. 6) $u \cdot x \cdot y/(x \cdot y)$.

Let us consider Q. We say that Q satisfies TT if and only if

(Def. 7) for every elements u, x, y of Q, $\mathtt{T}(\mathtt{T}(u, x), y) = \mathtt{T}(\mathtt{T}(u, y), x)$.

We say that Q satisfies TL if and only if

(Def. 8) for every elements u, x, y, z of Q, $\mathtt{T}(\mathtt{L}(u, x, y), z) = \mathtt{L}(\mathtt{T}(u, z), x, y)$.

We say that Q satisfies TR if and only if

(Def. 9) for every elements u, x, y, z of Q, $\mathtt{T}(\mathtt{R}(u, x, y), z) = \mathtt{R}(\mathtt{T}(u, z), x, y)$.

We say that Q satisfies LR if and only if

(Def. 10) for every elements u, x, y, z, w of Q, $\mathtt{L}(\mathtt{R}(u, x, y), z, w) = \mathtt{R}(\mathtt{L}(u, z, w), x, y)$.

We say that Q satisfies LL if and only if

(Def. 11) for every elements u, x, y, z, w of Q, $\mathtt{L}(\mathtt{L}(u, x, y), z, w) = \mathtt{L}(\mathtt{L}(u, z, w), x, y)$.

We say that Q satisfies RR if and only if

(Def. 12) for every elements u, x, y, z, w of Q, $\mathtt{R}(\mathtt{R}(u,x,y),z,w) = \mathtt{R}(\mathtt{R}(u,z,w),x,y)$.

Let us consider x and y. The functor $\mathtt{K}(x,y)$ yielding an element of Q is defined by the term

(Def. 13) $y \cdot x \setminus (x \cdot y)$.

Let us consider z. The functor $\mathtt{a}(x,y,z)$ yielding an element of Q is defined by the term

(Def. 14) $x \cdot (y \cdot z) \setminus (x \cdot y \cdot z)$.

Let Q be a multiplicative loop. We say that Q satisfies aa1 if and only if

(Def. 15) for every elements x, y, z, u, w of Q, $\mathtt{a}(\mathtt{a}(x,y,z),u,w) = 1_Q$.

We say that Q satisfies aa2 if and only if

(Def. 16) for every elements x, y, z, u, w of Q, $\mathtt{a}(x,\mathtt{a}(y,z,u),w) = 1_Q$.

We say that Q satisfies aa3 if and only if

(Def. 17) for every elements x, y, z, u, w of Q, $\mathtt{a}(x,y,\mathtt{a}(z,u,w)) = 1_Q$.

We say that Q satisfies Ka if and only if

(Def. 18) for every elements x, y, z, u of Q, $\mathtt{K}(\mathtt{a}(x,y,z),u) = 1_Q$.

We say that Q satisfies aK1 if and only if

(Def. 19) for every elements x, y, z, u of Q, $\mathtt{a}(\mathtt{K}(x,y),z,u) = 1_Q$.

We say that Q satisfies aK2 if and only if

(Def. 20) for every elements x, y, z, u of Q, $\mathtt{a}(x,\mathtt{K}(y,z),u) = 1_Q$.

We say that Q satisfies aK3 if and only if

(Def. 21) for every elements x, y, z, u of Q, $\mathtt{a}(x,y,\mathtt{K}(z,u)) = 1_Q$.

Let us observe that there exists a multiplicative loop which is strict and satisfies TT, TL, TR, LR, LL, RR, aa1, aa2, aa3, Ka, aK1, aK2, and aK3.

Now we state the propositions:

(1) If $x \cdot y = u$ and $x \cdot z = u$, then $y = z$.

(2) If $y \cdot x = u$ and $z \cdot x = u$, then $y = z$.

(3) If $x \cdot y = x \cdot z$, then $y = z$.

(4) If $y \cdot x = z \cdot x$, then $y = z$.

Let us consider Q and x. Let us observe that $1_Q \setminus x$ reduces to x and $x/(1_Q)$ reduces to x. Let us consider y. Observe that $y/(x \setminus y)$ reduces to x and $(y/x) \setminus y$ reduces to x. Now we state the propositions:

(5) $x \setminus x = 1_Q$.

(6) $x/x = 1_Q$.

(7) If $x \setminus y = 1_Q$, then $x = y$.

(8) If $x/y = 1_Q$, then $x = y$.

(9) If $\mathtt{a}(x, y, z) = 1_Q$, then $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(10) If $\mathtt{K}(x, y) = 1_Q$, then $x \cdot y = y \cdot x$.

(11) If $\mathtt{a}(x, y, z) = 1_Q$, then $\mathtt{L}(z, y, x) = z$. The theorem is a consequence of (9).

Let us consider Q. The functors: $\mathrm{Nucl_l}(Q)$, $\mathrm{Nucl_m}(Q)$, $\mathrm{Nucl_r}(Q)$, and $\mathrm{Comm}(Q)$ yielding subsets of Q are defined by conditions

(Def. 22) $x \in \mathrm{Nucl_l}(Q)$ iff for every y and z, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(Def. 23) $y \in \mathrm{Nucl_m}(Q)$ iff for every x and z, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(Def. 24) $z \in \mathrm{Nucl_r}(Q)$ iff for every x and y, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(Def. 25) $x \in \mathrm{Comm}(Q)$ iff for every y, $x \cdot y = y \cdot x$,

respectively. The functor $\mathrm{Nucl}(Q)$ yielding a subset of Q is defined by the term

(Def. 26) $(\mathrm{Nucl_l}(Q) \cap \mathrm{Nucl_m}(Q)) \cap \mathrm{Nucl_r}(Q)$.

Now we state the proposition:

(12) $x \in \mathrm{Nucl}(Q)$ if and only if $x \in \mathrm{Nucl_l}(Q)$ and $x \in \mathrm{Nucl_m}(Q)$ and $x \in \mathrm{Nucl_r}(Q)$.

Let us consider Q. The functor $\mathrm{Cent}(Q)$ yielding a subset of Q is defined by the term

(Def. 27) $\mathrm{Comm}(Q) \cap \mathrm{Nucl}(Q)$.

Let Q_1, Q_2 be multiplicative loops and f be a function from Q_1 into Q_2. We say that f is unity-preserving if and only if

(Def. 28) $f(1_{Q_1}) = 1_{Q_2}$.

We say that f is quasi-homomorphic if and only if

(Def. 29) for every elements x, y of Q_1, $f(x \cdot y) = f(x) \cdot f(y)$.

We say that f is homomorphic if and only if

(Def. 30) f is unity-preserving and quasi-homomorphic.

Observe that every function from Q_1 into Q_2 which is unity-preserving and quasi-homomorphic is also homomorphic and every function from Q_1 into Q_2 which is homomorphic is also unity-preserving and quasi-homomorphic and $\Omega_{Q_1} \longmapsto 1_{Q_2}$ is homomorphic as a function from Q_1 into Q_2 and there exists a function from Q_1 into Q_2 which is homomorphic.

Let us consider Q and Q_2. Let f be a homomorphic function from Q into Q_2. The functor $\mathrm{Ker}\, f$ yielding a subset of Q is defined by

(Def. 31) $x \in it$ iff $f(x) = 1_{Q_2}$.

Let us consider a homomorphic function f from Q_1 into Q_2 and elements x, y of Q_1. Now we state the propositions:

(13) $f(x \setminus y) = f(x) \setminus f(y)$.

(14) $f(x/y) = f(x)/f(y)$.

(15) Let us consider a homomorphic function f from Q_1 into Q_2. Suppose for every element y of Q_2, there exists an element x of Q_1 such that $f(x) = y$ and for every elements x, y, z of Q_1, $\mathtt{a}(x, y, z) \in \operatorname{Ker} f$. Then Q_2 is associative. The theorem is a consequence of (13) and (9).

(16) Let us consider multiplicative loop Q_1 satisfying aa1, aa2, aa3, aK1, aK2, and aK3, a multiplicative loop Q_2, and a homomorphic function f from Q_1 into Q_2. Suppose for every element y of Q_2, there exists an element x of Q_1 such that $f(x) = y$ and $\operatorname{Nucl}(Q_1) \subseteq \operatorname{Ker} f$. Then Q_2 is a commutative multiplicative group. The theorem is a consequence of (9), (12), (13), (10), and (15).

(17) Let us consider multiplicative loop Q_1 satisfying aa1, aa2, aa3, and Ka, a multiplicative loop Q_2, and a homomorphic function f from Q_1 into Q_2. Suppose for every element y of Q_2, there exists an element x of Q_1 such that $f(x) = y$ and $\operatorname{Cent}(Q_1) \subseteq \operatorname{Ker} f$. Then Q_2 is a multiplicative group. The theorem is a consequence of (10), (9), (12), and (15).

Let Q be a non empty multiplicative loop structure. A sub-loop structure of Q is a non empty multiplicative loop structure defined by

(Def. 32) the carrier of $it \subseteq$ the carrier of Q and the multiplication of $it =$ (the multiplication of Q) $\restriction$ (the carrier of it) and the one of $it =$ the one of Q.

Let Q be a multiplicative loop. Let us note that there exists a sub-loop structure of Q which is well unital, invertible, cancelable, non empty, and strict.

A sub-loop of Q is a well unital, invertible, cancelable sub-loop structure of Q. Let Q be a non empty multiplicative loop structure, H be a sub-loop structure of Q, and A be a subset of H. The functor ${}^{@}A$ yielding a subset of Q is defined by the term

(Def. 33) A.

Let us consider Q. Let H_1, H_2 be subsets of Q. The functor $\operatorname{LoopClose1}(H_1, H_2)$ yielding a subset of Q is defined by

(Def. 34) $x \in it$ iff $x \in H_1$ or $x = 1_Q$ or there exists y and there exists z such that y, $z \in H_2$ and ($x = y \cdot z$ or $x = y \setminus z$ or $x = y/z$).

Let H be a subset of Q. The functor $\operatorname{lp}(H)$ yielding a strict sub-loop of Q is defined by

(Def. 35) $H \subseteq \Omega_{it}$ and for every sub-loop H_2 of Q such that $H \subseteq \Omega_{H_2}$ holds $\Omega_{it} \subseteq \Omega_{H_2}$.

Now we state the propositions:

(18) Let us consider a subset H of Q. Suppose $1_Q \in H$ and for every x and y such that x, $y \in H$ holds $x \cdot y \in H$ and for every x and y such that x,

$y \in H$ holds $x \setminus y \in H$ and for every x and y such that x, $y \in H$ holds $x/y \in H$. Then $\Omega_{\mathrm{lp}(H)} = H$.

PROOF: Reconsider $O = 1_Q$ as an element of H.

Set $m_2 =$ (the multiplication of Q) $\restriction H$. Set $L_4 = \langle H, m_2, O\rangle$ by [5, (1)]. L_4 is a sub-loop of Q. □

(19) Let us consider a homomorphic function f from Q into Q_2. Then $\Omega_{\mathrm{lp}(\mathrm{Ker}\, f)} = \mathrm{Ker}\, f$. The theorem is a consequence of (13), (14), and (18).

(20) $1_Q \in \mathrm{Nucl}_{\mathrm{l}}(Q)$.

(21) $1_Q \in \mathrm{Nucl}_{\mathrm{m}}(Q)$.

(22) $1_Q \in \mathrm{Nucl}_{\mathrm{r}}(Q)$.

(23) $1_Q \in \mathrm{Nucl}(Q)$. The theorem is a consequence of (20), (21), (12), and (22).

Let us consider Q. Note that $\mathrm{Nucl}_{\mathrm{l}}(Q)$ is non empty and $\mathrm{Nucl}_{\mathrm{m}}(Q)$ is non empty and $\mathrm{Nucl}_{\mathrm{r}}(Q)$ is non empty and $\mathrm{Nucl}(Q)$ is non empty.

(24) If x, $y \in \mathrm{Nucl}(Q)$, then $x \cdot y \in \mathrm{Nucl}(Q)$. The theorem is a consequence of (12).

(25) If x, $y \in \mathrm{Nucl}(Q)$, then $x \setminus y \in \mathrm{Nucl}(Q)$. The theorem is a consequence of (12) and (1).

(26) If x, $y \in \mathrm{Nucl}(Q)$, then $x/y \in \mathrm{Nucl}(Q)$. The theorem is a consequence of (12) and (2).

(27) $\Omega_{\mathrm{lp}(\mathrm{Nucl}(Q))} = \mathrm{Nucl}(Q)$. The theorem is a consequence of (23), (24), (25), (26), and (18).

(28) $\Omega_{\mathrm{lp}(\mathrm{Cent}(Q))} = \mathrm{Cent}(Q)$. The theorem is a consequence of (23), (12), (24), (25), (26), and (18).

2. Multiplicative Mappings and Cosets

Let X be a functional set. We say that X is composition-closed if and only if

(Def. 36) for every elements f, g of X such that f, $g \in X$ holds $f \cdot g \in X$.

We say that X is inverse-closed if and only if

(Def. 37) for every element f of X such that $f \in X$ holds $f^{-1} \in X$.

Let A be a set. One can verify that $\{\mathrm{id}_A\}$ is composition-closed and inverse-closed and there exists a functional set which is composition-closed, inverse-closed, and non empty.

Let Q be a multiplicative loop structure. Let us note that there exists a subset of Q^Q which is composition-closed, inverse-closed, and non empty.

Let Q be a non empty multiplicative loop structure, H be a subset of Q, and S be a subset of Q^Q. We say that H is left-right-mult-closed w.r.t. S if and only if

(Def. 38) for every element u of Q such that $u \in H$ holds (curry(the multiplication of Q))(u), (curry$'$(the multiplication of Q))$(u) \in S$.

The functor MltClos1(H, S) yielding a subset of Q^Q is defined by

(Def. 39) for every object f, $f \in it$ iff there exists an element u of Q such that $u \in H$ and $f =$ (curry$'$(the multiplication of Q))(u) or there exists an element u of Q such that $u \in H$ and $f =$ (curry(the multiplication of Q))(u) or there exist permutations g, h of Q such that g, $h \in S$ and $f = g \cdot h$ or there exists a permutation g of Q such that $g \in S$ and $f = g^{-1}$.

Now we state the propositions:

(29) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q}. Suppose for every subset X of Q^Q, $\varphi(X) =$ MltClos1(H, X). Then φ is $\subseteq$-monotone.

(30) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q}. Suppose for every subset X of Q^Q, $\varphi(X) =$ MltClos1(H, X). Let us consider a subset Y of Q^Q. Suppose $\varphi(Y) \subseteq Y$. Then

(i) for every element u of Q such that $u \in H$ holds (curry(the multiplication of Q))$(u) \in Y$, and

(ii) for every element u of Q such that $u \in H$ holds (curry$'$(the multiplication of Q))$(u) \in Y$.

(31) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q}. Suppose for every subset X of Q^Q, $\varphi(X) =$ MltClos1(H, X). Let us consider a subset Y of Q^Q. Suppose for every subset S of Q^Q such that $\varphi(S) \subseteq S$ holds $Y \subseteq S$. Let us consider an element f of Q^Q. If $f \in Y$, then f is a permutation of Q.

PROOF: Set $S_3 =$ the set of all f where f is a permutation of Q. $S_3 \subseteq Q^Q$. $\varphi(S_3) \subseteq S_3$. $\square$

(32) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q}. Suppose for every subset X of Q^Q, $\varphi(X) =$ MltClos1(H, X). Let us consider a subset Y of Q^Q. Suppose Y is a fixpoint of φ and for every subset S of Q^Q such that $\varphi(S) \subseteq S$ holds $Y \subseteq S$. Then Y is composition-closed and inverse-closed. The theorem is a consequence of (31).

(33) (curry(the multiplication of Q))(u) is a permutation of Q.

PROOF: Set $f =$ (curry(the multiplication of Q))(u). Define $\mathcal{G}$(element of Q) $= u \setminus \$_1$. Consider g being a function from Q into Q such that for

every element x of Q, $g(x) = \mathcal{G}(x)$. For every element x of Q, $(g \cdot f)(x) = (\mathrm{id}_Q)(x)$. For every element x of Q, $(f \cdot g)(x) = (\mathrm{id}_Q)(x)$. $\square$

(34) (curry′(the multiplication of Q))(u) is a permutation of the carrier of Q.
PROOF: Set $f =$ (curry′(the multiplication of Q))(u). Define $\mathcal{G}$(element of Q) $= \$_1/u$. Consider g being a function from Q into Q such that for every element x of Q, $g(x) = \mathcal{G}(x)$. For every element x of Q, $(g \cdot f)(x) = (\mathrm{id}_Q)(x)$. For every element x of Q, $(f \cdot g)(x) = (\mathrm{id}_Q)(x)$. $\square$

Let us consider Q. Let H be a subset of Q. The functor $\mathrm{Mlt}(H)$ yielding a composition-closed, inverse-closed subset of Q^Q is defined by

(Def. 40) H is left-right-mult-closed w.r.t. it and for every composition-closed, inverse-closed subset X of Q^Q such that H is left-right-mult-closed w.r.t. X holds $it \subseteq X$.

Let us consider a subset H of Q and an element u of Q. Now we state the propositions:

(35) If $u \in H$, then (curry(the multiplication of Q))$(u) \in \mathrm{Mlt}(H)$.

(36) If $u \in H$, then (curry′(the multiplication of Q))$(u) \in \mathrm{Mlt}(H)$.

(37) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q}. Suppose for every subset X of Q^Q, $\varphi(X) = \mathrm{MltClos1}(H, X)$. Then

(i) $\mathrm{Mlt}(H)$ is a fixpoint of φ, and

(ii) for every subset S of Q^Q such that $\varphi(S) \subseteq S$ holds $\mathrm{Mlt}(H) \subseteq S$.

The theorem is a consequence of (36), (35), (33), (34), and (31).

(38) Let us consider a subset H of Q, and an element f of Q^Q. If $f \in \mathrm{Mlt}(H)$, then f is a permutation of Q.
PROOF: Define $\mathcal{M}$(subset of Q^Q) $= \mathrm{MltClos1}(H, \$_1)$. Consider φ being a function from 2^{Q^Q} into 2^{Q^Q} such that for every subset X of Q^Q, $\varphi(X) = \mathcal{M}(X)$. For every subset S of Q^Q such that $\varphi(S) \subseteq S$ holds $\mathrm{Mlt}(H) \subseteq S$. $\square$

Let us consider Q. Let H be a subset of Q and x be an element of Q. The functor $x \cdot H$ yielding a subset of Q is defined by

(Def. 41) $y \in it$ iff there exists a permutation h of Q such that $h \in \mathrm{Mlt}(H)$ and $y = h(x)$.

Let H be a sub-loop of Q. The functor $x \cdot H$ yielding a subset of Q is defined by the term

(Def. 42) $x \cdot ({}^{@}\Omega_H)$.

Let N be a sub-loop of Q. The functor $\mathrm{Cosets}(N)$ yielding a family of subsets of Q is defined by

(Def. 43) for every subset H of Q, $H \in it$ iff there exists x such that $H = x \cdot N$.

Let us note that Cosets(N) is non empty.

3. Normal Subloop

Let Q be a multiplicative loop structure and H_1, H_2 be subsets of Q. The functors: $H_1 \cdot H_2$ and $H_1 \setminus H_2$ yielding subsets of Q are defined by conditions

(Def. 44) for every element x of Q, $x \in H_1 \cdot H_2$ iff there exist elements y, z of Q such that $y \in H_1$ and $z \in H_2$ and $x = y \cdot z$,

(Def. 45) for every element x of Q, $x \in H_1 \setminus H_2$ iff there exist elements y, z of Q such that $y \in H_1$ and $z \in H_2$ and $x = y \setminus z$,

respectively. Let Q be a multiplicative loop and H be a sub-loop of Q. We say that H is normal if and only if

(Def. 46) for every elements x, y of Q, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$ and for every element z of Q, if $(x \cdot H) \cdot (y \cdot H) = x \cdot H \cdot (z \cdot H)$, then $y \cdot H = z \cdot H$ and if $(y \cdot H) \cdot (x \cdot H) = z \cdot H \cdot (x \cdot H)$, then $y \cdot H = z \cdot H$.

Let us consider Q. One can verify that there exists a sub-loop of Q which is normal.

Let N be a normal sub-loop of Q. The functor SubLoopAsCoset(N) yielding an element of Cosets(N) is defined by the term

(Def. 47) $1_Q \cdot N$.

The functor CosetLoopOp(N) yielding a binary operation on Cosets(N) is defined by

(Def. 48) for every elements H_1, H_2 of Cosets(N), $it(H_1, H_2) = H_1 \cdot H_2$.

The functor $Q \,/\, N$ yielding a strict multiplicative loop structure is defined by the term

(Def. 49) $\langle \text{Cosets}(N), \text{CosetLoopOp}(N), \text{SubLoopAsCoset}(N) \rangle$.

One can check that $Q \,/\, N$ is non empty and $Q \,/\, N$ is well unital, invertible, and cancelable.

The functor QuotientHom(Q, N) yielding a function from Q into $Q \,/\, N$ is defined by

(Def. 50) for every x, $it(x) = x \cdot N$.

Let us observe that QuotientHom(Q, N) is homomorphic.

Now we state the propositions:

(39) Let us consider a sub-loop H of Q, x, y, and elements x_1, y_1 of H. If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

(40) Let us consider a sub-loop H of Q, x, and y. Suppose x, $y \in$ the carrier of H. Then $x \cdot y \in$ the carrier of H. The theorem is a consequence of (39).

(41) Let us consider a sub-loop H of Q, x, y, and elements x_1, y_1 of H. If $x = x_1$ and $y = y_1$, then $x \setminus y = x_1 \setminus y_1$. The theorem is a consequence of (39).

(42) Let us consider a sub-loop H of Q, x, and y. Suppose x, $y \in$ the carrier of H. Then $x \setminus y \in$ the carrier of H. The theorem is a consequence of (41).

(43) Let us consider a sub-loop H of Q, x, y, and elements x_1, y_1 of H. If $x = x_1$ and $y = y_1$, then $x/y = x_1/y_1$. The theorem is a consequence of (39).

(44) Let us consider a sub-loop H of Q, x, and y. Suppose x, $y \in$ the carrier of H. Then $x/y \in$ the carrier of H. The theorem is a consequence of (43).

The scheme *MltInd* deals with a multiplicative loop $\mathcal{Q}$ and a subset $\mathcal{H}$ of $\mathcal{Q}$ and a unary predicate $\mathcal{P}$ and states that

(Sch. 1) For every function f from $\mathcal{Q}$ into $\mathcal{Q}$ such that $f \in \mathrm{Mlt}(\mathcal{H})$ holds $\mathcal{P}[f]$ provided

- for every element u of $\mathcal{Q}$ such that $u \in \mathcal{H}$ for every function f from $\mathcal{Q}$ into $\mathcal{Q}$ such that for every element x of $\mathcal{Q}$, $f(x) = x \cdot u$ holds $\mathcal{P}[f]$ and
- for every element u of $\mathcal{Q}$ such that $u \in \mathcal{H}$ for every function f from $\mathcal{Q}$ into $\mathcal{Q}$ such that for every element x of $\mathcal{Q}$, $f(x) = u \cdot x$ holds $\mathcal{P}[f]$ and
- for every permutations g, h of $\mathcal{Q}$ such that $\mathcal{P}[g]$ and $\mathcal{P}[h]$ holds $\mathcal{P}[g \cdot h]$ and
- for every permutation g of $\mathcal{Q}$ such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$.

Now we state the proposition:

(45) Let us consider a sub-loop N of Q, and a function f from Q into Q. Suppose $f \in \mathrm{Mlt}({}^{@}\Omega_N)$. $x \in {}^{@}\Omega_N$ if and only if $f(x) \in {}^{@}\Omega_N$.
PROOF: Reconsider $H = {}^{@}\Omega_N$ as a subset of Q. Define $\mathcal{P}$[function from Q into Q] $\equiv$ for every x, $x \in H$ iff $\$_1(x) \in H$. For every element u of Q such that $u \in H$ for every function f from Q into Q such that for every element x of Q, $f(x) = x \cdot u$ holds $\mathcal{P}[f]$. For every element u of Q such that $u \in H$ for every function f from Q into Q such that for every element x of Q, $f(x) = u \cdot x$ holds $\mathcal{P}[f]$. For every permutations g, h of Q such that $\mathcal{P}[g]$ and $\mathcal{P}[h]$ holds $\mathcal{P}[g \cdot h]$. For every permutation g of Q such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$. For every function f from Q into Q such that $f \in \mathrm{Mlt}(H)$ holds $\mathcal{P}[f]$. □

Let us consider a normal sub-loop N of Q. Now we state the propositions:

(46) The carrier of $N = 1_Q \cdot N$.
PROOF: The carrier of $N \subseteq 1_Q \cdot N$. □

(47) $\operatorname{Ker}\operatorname{QuotientHom}(Q, N) = {}^{@}\Omega_N$.
PROOF: Set $f = \operatorname{QuotientHom}(Q, N)$. For every x, $x \in \operatorname{Ker} f$ iff $x \in {}^{@}\Omega_N$. □

(48) Let us consider a multiplicative loop Q_2, a homomorphic function f from Q into Q_2, and a function h from Q into Q. If $h \in \operatorname{Mlt}(\operatorname{Ker} f)$, then $f \cdot h = f$.
PROOF: Set $H = \operatorname{Ker} f$. Define $\mathcal{P}$[function from Q into Q] $\equiv f \cdot \$_1 = f$. For every element u of Q such that $u \in H$ for every function h from Q into Q such that for every element x of Q, $h(x) = x \cdot u$ holds $\mathcal{P}[h]$. For every element u of Q such that $u \in H$ for every function h from Q into Q such that for every element x of Q, $h(x) = u \cdot x$ holds $\mathcal{P}[h]$. For every permutation g of Q such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$. For every function f from Q into Q such that $f \in \operatorname{Mlt}(H)$ holds $\mathcal{P}[f]$. □

Let us consider a multiplicative loop Q_2, a homomorphic function f from Q into Q_2, x, and y. Now we state the propositions:

(49) $y \in x \cdot (\operatorname{Ker} f)$ if and only if $f(x) = f(y)$.
PROOF: If $y \in x \cdot (\operatorname{Ker} f)$, then $f(x) = f(y)$. There exists a permutation h of Q such that $h \in \operatorname{Mlt}(\operatorname{Ker} f)$ and $y = h(x)$. □

(50) $y \in x \cdot (\operatorname{lp}(\operatorname{Ker} f))$ if and only if $f(x) = f(y)$. The theorem is a consequence of (19) and (49).

(51) $x \cdot (\operatorname{lp}(\operatorname{Ker} f)) = y \cdot (\operatorname{lp}(\operatorname{Ker} f))$ if and only if $f(x) = f(y)$. The theorem is a consequence of (50).

(52) Let us consider a multiplicative loop Q_2, and a homomorphic function f from Q into Q_2. Then $\operatorname{lp}(\operatorname{Ker} f)$ is normal.
PROOF: Set $H = \operatorname{lp}(\operatorname{Ker} f)$. For every x and y, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$. For every x and y, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$ and for every z, if $(x \cdot H) \cdot (y \cdot H) = x \cdot H \cdot (z \cdot H)$, then $y \cdot H = z \cdot H$ and if $(y \cdot H) \cdot (x \cdot H) = z \cdot H \cdot (x \cdot H)$, then $y \cdot H = z \cdot H$. □

(53) (i) $1_Q \in \Omega_{\operatorname{lp}(\operatorname{Cent}(Q))}$, and
(ii) $1_Q \in \operatorname{Cent}(Q)$.
The theorem is a consequence of (28).

(54) Let us consider a function f from Q into Q. Suppose $f \in \operatorname{Mlt}(\operatorname{Cent}(Q))$. Then there exists z such that
(i) $z \in \operatorname{Cent}(Q)$, and
(ii) for every x, $f(x) = x \cdot z$.
PROOF: Set $H = \operatorname{Cent}(Q)$. Define $\mathcal{P}$[function from Q into Q] $\equiv$ there exists z such that $z \in H$ and for every x, $\$_1(x) = x \cdot z$. For every element u of Q such that $u \in H$ for every function f from Q into Q such that for

every element x of Q, $f(x) = u \cdot x$ holds $\mathcal{P}[f]$. For every permutations g, h of Q such that $\mathcal{P}[g]$ and $\mathcal{P}[h]$ holds $\mathcal{P}[g \cdot h]$. For every permutation g of Q such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$. For every function f from Q into Q such that $f \in \mathrm{Mlt}(H)$ holds $\mathcal{P}[f]$. □

(55) $y \in x \cdot (\mathrm{lp}(\mathrm{Cent}(Q)))$ if and only if there exists z such that $z \in \mathrm{Cent}(Q)$ and $y = x \cdot z$.

PROOF: If $y \in x \cdot (\mathrm{lp}(\mathrm{Cent}(Q)))$, then there exists z such that $z \in \mathrm{Cent}(Q)$ and $y = x \cdot z$. Reconsider $h = (\mathrm{curry}'(\text{the multiplication of } Q))(z)$ as a permutation of Q. There exists a permutation h of Q such that $h \in \mathrm{Mlt}(\mathrm{Cent}(Q))$ and $h(x) = y$. □

(56) $x \cdot (\mathrm{lp}(\mathrm{Cent}(Q))) = y \cdot (\mathrm{lp}(\mathrm{Cent}(Q)))$ if and only if there exists z such that $z \in \mathrm{Cent}(Q)$ and $y = x \cdot z$.

PROOF: If $x \cdot (\mathrm{lp}(\mathrm{Cent}(Q))) = y \cdot (\mathrm{lp}(\mathrm{Cent}(Q)))$, then there exists z such that $z \in \mathrm{Cent}(Q)$ and $y = x \cdot z$. If there exists z such that $z \in \mathrm{Cent}(Q)$ and $y = x \cdot z$, then $x \cdot (\mathrm{lp}(\mathrm{Cent}(Q))) = y \cdot (\mathrm{lp}(\mathrm{Cent}(Q)))$. □

(57) $\mathrm{lp}(\mathrm{Cent}(Q))$ is normal.

PROOF: Set $H = \mathrm{lp}(\mathrm{Cent}(Q))$. For every x and y, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$. For every x and y, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$ and for every z, if $(x \cdot H) \cdot (y \cdot H) = x \cdot H \cdot (z \cdot H)$, then $y \cdot H = z \cdot H$ and if $(y \cdot H) \cdot (x \cdot H) = z \cdot H \cdot (x \cdot H)$, then $y \cdot H = z \cdot H$. □

4. AIM Conjecture

Let Q be a multiplicative loop. The functor $\mathrm{InnAut}(Q)$ yielding a subset of Q^Q is defined by

(Def. 51) for every object f, $f \in it$ iff there exists a function g from Q into Q such that $f = g$ and $g \in \mathrm{Mlt}(\Omega_Q)$ and $g(1_Q) = 1_Q$.

Observe that $\mathrm{InnAut}(Q)$ is non empty, composition-closed, and inverse-closed.

Now we state the proposition:

(58) Let us consider a function f from Q into Q. Then $f \in \mathrm{InnAut}(Q)$ if and only if $f \in \mathrm{Mlt}(\Omega_Q)$ and $f(1_Q) = 1_Q$.

Let Q be a multiplicative loop. We say that Q is an AIM if and only if

(Def. 52) for every functions f, g from Q into Q such that f, $g \in \mathrm{InnAut}(Q)$ holds $f \cdot g = g \cdot f$.

Let us consider Q and x. The functor $\mathtt{T}(x)$ yielding a function from Q into Q is defined by

(Def. 53) for every u, $it(u) = \mathtt{T}(u, x)$.

Now we state the proposition:

(59) $\mathtt{T}(x) \in \mathrm{InnAut}(Q)$.

PROOF: Set $f = \mathtt{T}(x)$. Reconsider $g = (\mathrm{curry}(\text{the multiplication of } Q))(x)$ as a permutation of the carrier of Q.

Reconsider $h = (\mathrm{curry}'(\text{the multiplication of } Q))(x)$ as a permutation of the carrier of Q. $f = g^{-1} \cdot h$. $g \in \mathrm{Mlt}(\Omega_Q)$. $h \in \mathrm{Mlt}(\Omega_Q)$. □

Let us consider Q, x, and y. The functor $\mathtt{L}(x, y)$ yielding a function from Q into Q is defined by

(Def. 54) for every u, $it(u) = \mathtt{L}(u, x, y)$.

Now we state the proposition:

(60) $\mathtt{L}(x, y) \in \mathrm{InnAut}(Q)$.

PROOF: Set $f = \mathtt{L}(x, y)$. Reconsider $g = (\mathrm{curry}(\text{the multiplication of } Q))(y \cdot x)$ as a permutation of the carrier of Q.

Reconsider $h = (\mathrm{curry}(\text{the multiplication of } Q))(x)$ as a permutation of the carrier of Q.

Reconsider $k = (\mathrm{curry}(\text{the multiplication of } Q))(y)$ as a permutation of the carrier of Q. $f = g^{-1} \cdot (k \cdot h)$. $g \in \mathrm{Mlt}(\Omega_Q)$. h, $k \in \mathrm{Mlt}(\Omega_Q)$. □

Let us consider Q, x, and y. The functor $\mathtt{R}(x, y)$ yielding a function from Q into Q is defined by

(Def. 55) for every u, $it(u) = \mathtt{R}(u, x, y)$.

Now we state the proposition:

(61) $\mathtt{R}(x, y) \in \mathrm{InnAut}(Q)$.

PROOF: Set $f = \mathtt{R}(x, y)$. Reconsider $g = (\mathrm{curry}'(\text{the multiplication of } Q))(x \cdot y)$ as a permutation of the carrier of Q.

Reconsider $h = (\mathrm{curry}'(\text{the multiplication of } Q))(x)$ as a permutation of the carrier of Q.

Reconsider $k = (\mathrm{curry}'(\text{the multiplication of } Q))(y)$ as a permutation of the carrier of Q. $f = g^{-1} \cdot (k \cdot h)$. $g \in \mathrm{Mlt}(\Omega_Q)$. h, $k \in \mathrm{Mlt}(\Omega_Q)$. □

Observe that Trivial-multLoopStr is an AIM and there exists a multiplicative loop which is non empty, strict, and AIM and every AIM multiplicative loop satisfies TT, TL, TR, LR, LL, and RR.

Now we state the propositions:

(62) Let us consider a function f from Q into Q. Suppose $f \in \mathrm{Mlt}(\mathrm{Nucl}(Q))$. Then there exists u and there exists v such that u, $v \in \mathrm{Nucl}(Q)$ and for every x, $f(x) = u \cdot (x \cdot v)$.

PROOF: Set $H = \mathrm{Nucl}(Q)$. Define $\mathcal{P}$[function from Q into Q] ≡ there exists u and there exists v such that u, $v \in \mathrm{Nucl}(Q)$ and for every x, $\$_1(x) = u \cdot (x \cdot v)$. For every element u of Q such that $u \in H$ for every

function f from Q into Q such that for every element x of Q, $f(x) = x \cdot u$ holds $\mathcal{P}[f]$. For every element u of Q such that $u \in H$ for every function f from Q into Q such that for every element x of Q, $f(x) = u \cdot x$ holds $\mathcal{P}[f]$. For every permutations g, h of the carrier of Q such that $\mathcal{P}[g]$ and $\mathcal{P}[h]$ holds $\mathcal{P}[g \cdot h]$. For every permutation g of Q such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$. For every function f from Q into Q such that $f \in \mathrm{Mlt}(H)$ holds $\mathcal{P}[f]$. □

(63) $y \in x \cdot (\mathrm{lp}(\mathrm{Nucl}(Q)))$ if and only if there exists u and there exists v such that u, $v \in \mathrm{Nucl}(Q)$ and $y = u \cdot (x \cdot v)$.
PROOF: If $y \in x \cdot (\mathrm{lp}(\mathrm{Nucl}(Q)))$, then there exists u and there exists v such that u, $v \in \mathrm{Nucl}(Q)$ and $y = u \cdot (x \cdot v)$. There exists a permutation h of the carrier of Q such that $h \in \mathrm{Mlt}(\mathrm{Nucl}(Q))$ and $h(x) = y$. □

(64) $x \cdot (\mathrm{lp}(\mathrm{Nucl}(Q))) = y \cdot (\mathrm{lp}(\mathrm{Nucl}(Q)))$ if and only if there exists u and there exists v such that u, $v \in \mathrm{Nucl}(Q)$ and $y = u \cdot (x \cdot v)$. The theorem is a consequence of (23), (63), (12), (27), (44), (42), and (40).

Let us consider AIM multiplicative loop Q and elements x, u of Q. Now we state the propositions:

(65) If $u \in \mathrm{Nucl}(Q)$, then $\mathtt{T}(u, x) \in \mathrm{Nucl}(Q)$.
PROOF: $u \in \mathrm{Nucl}_{\mathrm{l}}(Q)$ and $u \in \mathrm{Nucl}_{\mathrm{m}}(Q)$ and $u \in \mathrm{Nucl}_{\mathrm{r}}(Q)$. For every elements y, z of Q, $(\mathtt{T}(u, x) \cdot y) \cdot z = \mathtt{T}(u, x) \cdot (y \cdot z)$. For every elements y, z of Q, $(y \cdot z) \cdot \mathtt{T}(u, x) = y \cdot (z \cdot \mathtt{T}(u, x))$. For every elements y, z of Q, $(y \cdot \mathtt{T}(u, x)) \cdot z = y \cdot (\mathtt{T}(u, x) \cdot z)$. □

(66) If $u \in \mathrm{Nucl}(Q)$, then $x \cdot u/x \in \mathrm{Nucl}(Q)$.
PROOF: $u \in \mathrm{Nucl}_{\mathrm{l}}(Q)$ and $u \in \mathrm{Nucl}_{\mathrm{m}}(Q)$ and $u \in \mathrm{Nucl}_{\mathrm{r}}(Q)$. Define $\mathcal{T}(\text{element of } Q) = x \cdot \$_1/x$. Consider t being a function from Q into Q such that for every element v of Q, $t(v) = \mathcal{T}(v)$. $t \in \mathrm{InnAut}(Q)$. For every elements y, z of Q, $(\mathcal{T}(u) \cdot y) \cdot z = \mathcal{T}(u) \cdot (y \cdot z)$. For every elements y, z of Q, $(y \cdot z) \cdot \mathcal{T}(u) = y \cdot (z \cdot \mathcal{T}(u))$. For every elements y, z of Q, $(y \cdot \mathcal{T}(u)) \cdot z = y \cdot (\mathcal{T}(u) \cdot z)$. □

Now we state the proposition:

(67) If Q is an AIM, then $\mathrm{lp}(\mathrm{Nucl}(Q))$ is normal.
PROOF: Set $H = \mathrm{lp}(\mathrm{Nucl}(Q))$. For every elements x, y of Q, there exists an element v of Q such that $v \in \mathrm{Nucl}(Q)$ and $y = x \cdot v$ iff there exist elements u, v of Q such that u, $v \in \mathrm{Nucl}(Q)$ and $y = u \cdot (x \cdot v)$. For every elements x, y of Q, $y \in x \cdot H$ iff there exists an element v of Q such that $v \in \mathrm{Nucl}(Q)$ and $y = x \cdot v$. For every elements x, y of Q, $x \cdot H = y \cdot H$ iff there exists an element v of Q such that $v \in \mathrm{Nucl}(Q)$ and $y = x \cdot v$. For every x and y, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$. For every x and y, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$ and for every z, if $(x \cdot H) \cdot (y \cdot H) = x \cdot H \cdot (z \cdot H)$, then $y \cdot H = z \cdot H$ and if $(y \cdot H) \cdot (x \cdot H) = z \cdot H \cdot (x \cdot H)$, then $y \cdot H = z \cdot H$. □

Let Q be AIM multiplicative loop. Let us observe that $\mathrm{lp}(\mathrm{Nucl}(Q))$ is normal.
Let Q be a multiplicative loop. One can check that $\mathrm{lp}(\mathrm{Cent}(Q))$ is normal.
Now we state the proposition:

(68) **Main Theorem**: THE AIM CONJECTURE
The AIM Conjecture follows from knowing every AIM loop satisfies aa1, aa2, aa3, Ka, aK1, aK2 and aK3. This theorem justifies using first-order theorem provers to try to prove the AIM Conjecture:
Suppose for every multiplicative loop Q such that Q satisfies TT, TL, TR, LR, LL, and RR holds Q satisfies aa1, aa2, aa3, Ka, aK1, aK2, and aK3. Let us consider AIM multiplicative loop Q. Then

(i) $Q \,/\, \mathrm{lp}(\mathrm{Nucl}(Q))$ is a commutative multiplicative group, and

(ii) $Q \,/\, \mathrm{lp}(\mathrm{Cent}(Q))$ is a multiplicative group.

The theorem is a consequence of (47), (27), (16), (28), and (17).

REFERENCES

[1] A. A. Albert. Quasigroups. I. *Transactions of the American Mathematical Society*, 54(3): 507–519, 1943.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Maria Paola Bonacina and Mark E. Stickel, editors. *Automated Reasoning and Mathematics – Essays in Memory of William W. McCune*, volume 7788 of *Lecture Notes in Computer Science*, 2013. Springer.

[4] Michael K. Kinyon, Robert Veroff, and Petr Vojtěchovský. Loops with abelian inner mapping groups: An application of automated deduction. In Bonacina and Stickel [3], pages 151–164.

[5] Christoph Schwarzweller and Artur Korniłowicz. Characteristic of rings. Prime fields. *Formalized Mathematics*, 23(**4**):333–349, 2015. doi:10.1515/forma-2015-0027.

Accepted August 29, 2019