Mem. Fac. Lit. & Sci., Shimane Univ., Nat. Sci., 7, pp. 29–35, March 10, 1974

On some Quasigroups of Algebraic Models of Symmetric Spaces II

Michihiko KIKKAWA

(Received September 12, 1973)

In the previous paper [3], we introduced a concept of symmetric loop and showed that it is obtained, interchangeably, from a quasigroup of reflection with a base point. The latter is an algebraic model of symmetric space ([4], [5]). In this paper, we shall investigate further properties of symmetric loop G about di-associativity (§1) and show that the left inner mapping group is a subgroup of **Aut**G (§2). In §3, we shall give an embedding of G into a group **Aut**G_*, the automorphism group of the quasigroup of reflection of G. The method of embedding was suggested, essentially, by Professor Kiyosi Yamaguti in his recent letter to the author.

1. Di-associativity of symmetric loops.

We recall a definition of symmetric loop given in [3].

DEFINITION. A loop G is called a *symmetric loop* if it satisfies the following conditions ;

(1. 1) G is left di-associative (in the weak sense), i. e., G is power associative and both of equations $x(xy) = (xx)y$, $x^{-1}(xy) = y$ hold for all $x, y \in G$,

(1. 2) $x(yyz) = (xy)(xy)(x^{-1}z)$ holds for all $x, y, z \in G$,

(1. 3) the quadratic mapping $Q: G \longrightarrow G$ defined by $Q(x) = x^2$ is bijective.

PROPOSITION 1. *Let G be a symmetric loop. Then,*

i) $(xy)^{-1} = x^{-1}y^{-1}$,

ii) *G is left di-associative in the strong sense*, i. e.,

(1. 4) $f_{(x^p)} \circ f_{(x^q)} = f_{(x^{p+q})}$

holds for any integers p and q, where f_x denotes a left translation of G by an element x of G.

Proof. i) is easily obtained by putting $z = y^{-1}$ in (1. 2). For the proof of ii), we shall prove a formula $f_{(x^n)} = (f_x)^n$ for positive integer n by induction. Then the formula (1. 4) will be shown for any positive integers p and q, and its validity for any integers will be found by noting the property $(f_x)^{-1} = f_{(x^{-1})}$.

Now, assume that the formula $f_{(x^n)} = (f_x)^n$ holds for all positive integers $n \leqq m$. If m is odd, set $m = 2k-1$. Then the left di-associativity of G and the assumption of the induction imply that $f_{(x^{m+1})} = f_{x^k x^k} = f_{(x^k)} \circ f_{(x^k)} = (f_x)^k \circ (f_x)^k = (f_x)^{m+1}$. If m is even, set $m = 2k$. Then $f_{(x^{2k+1})} = (f_x)^{2k+1}$ holds. In fact, since G is power associative and the quadratic mapping Q has an inverse, we have $x^{2k+1} = (\bar{x})^{2(2k+1)} = (x^k\bar{x})(x^k\bar{x})$, where $\bar{x} = Q^{-1}(x)$. Applying the formula $f_x \circ f_y \circ f_x = f_{(x\bar{y})(x\bar{y})}$, obtained from (1. 2) (Theorem 4 in [3]), and taking into account of the assumption of the induction, we have $f_{(x^k\bar{x})(x^k\bar{x})} = (f_x)^k \circ f_x \circ (f_x)^k = (f_x)^{2k+1}$. The induction is thus completed.

DEFINITION. A loop G is called a *Moufang loop* if the equation

(1. 5) $x(y(xz)) = ((xy)x)z$

holds for all x, y, z of G.

It is well known that the above equation is equivalent to one of the following equations;

$$x(y(zy)) = ((xy)z)y,$$
$$(xy)(zx) = (x(yz))x,$$

and that every Moufang loop is di-associative (Moufang's Theorem). For the details, see [2].

The following results about commutative Moufang loops will be used later. For the proofs we refer to [1] (Theorem 7C).

LEMMA. *If G is a commutative Moufang loop, then*;

i) *the subset F of G consisting of all elements of finite order is a normal subloop of G,*

ii) *the quotient loop G/F is an Abelian group.*

PROPOSITION 2. *A loop G with a surjective quadratic mapping Q has the following properties if and only if G is a commutative Moufang loop*;

i) *G is left and right di-associative in the weak sense,*

ii) *the equation* (1. 2) *holds.*

Proof. Suppose that G is a loop with surjective mapping Q and that it satisfies i) and ii). Then, in the equation (1. 2), substituting z by an identity e of G, we have

(1. 6) $x(yy) = (xy)(xy)x^{-1}$.

Since the left hand side of this equation can be replaced by $(xy)y$, we can see that G is commutative. On the other hand, from (1. 2), we have

$$x(y(xz)) = (x\bar{y})(x\bar{y})z,$$

where $\bar{y} \in Q^{-1}(y)$. The right hand side of this equation is equal to $((xy)x)z$, for (1. 6) implies $(x(\bar{y}\bar{y}))x = (x\bar{y})(x\bar{y})$. Thus we can conclude that G satisfies the Moufang axiom (1. 5).

Conversely, let G be a commutative Moufang loop with a surjective quadratic mapping. Since G is di-associative, it is, of course, left and right di-associative. We are only to prove the formula (1. 2). Since G is commutative, the Moufang axiom (1. 5) is equivalent to

$$x(y(xz)) = (xxy)z.$$

In this equation, if y and xz are substituted by y^2 and z, respectively, it holds ;

$$x(yyz) = ((xx)(yy))(x^{-1}z),$$

which shows (1. 2), for $(xx)(yy) = (xy)(xy)$ is valid in G.

THEOREM 1. *Let G be a loop. A necessary and sufficient condition that G should be a di-associative symmetric loop is that G be a commutative Moufang loop with a bijective quadratic mapping* $Q(x) = x^2$.

In this case, the quotient loop G/F is an Abelian group, where F is a subloop of G consisting of all elements of finite order.

Proof. This is an immediate consequence of Proposition 2 and the preceding Lemma.

2. Left inner automorphisms.

DEFINITION. Let G be a loop. For x, y of G, a mapping $L_{x,y} = f_{xy}^{-1} \circ f_x \circ f_y$ of G onto itself is called a *left inner mapping* of G, where f_x denotes a left translation by $x \in G$. A group $\mathbf{L}(G)$ of transformations of G generated by the set of all left inner mappings is called the *left inner mapping group* of G.

THEOREM 2. *Let G be a symmetric loop. Then the left inner mapping group* $\mathbf{L}(G)$ *is a subgroup of automorphisms group of G.*

Proof. It is sufficient to show that every left inner mapping is a homomorphism of G. We shall prove it by means of the results obtained in the previous paper [3]. Let $(G, *)$ be a *quasigroup of reflection* associated with the symmetric loop G (Theorem 2 in [3]). Then every left translation of G is a homomorphism of $(G, *)$ (Lemma 8 in [3]). That is, the equation

$$x(y_*z) = (xy)_*(xz)$$

holds for all $x, y, z \in G$, where $y_*z = yyz^{-1}$ by definition.

Hence every left inner mapping $L_{x,y}$ is also a homomorphism of $(G, *)$. Now, let x, y, u and v be elements of G. The multiplication in the symmetric loop can be expressed by that of $(G, *)$ as follows ;

(2. 1) $uv = \bar{u}_*(e_*v)$,

where e is an identity of the loop and $\bar{u} = Q^{-1}(u)$. (Theorem 2, [3]).

Thus we have

(2. 2) $(L_{x,y}u)(L_{x,y}v)=(\overline{L_{x,y}u})_*(e_*(L_{x,y}v))=(\overline{L_{x,y}u})_*(L_{x,y}(e_*v))$.

On the other hand, an equation

(2. 3) $\overline{L_{x,y}u}=L_{x,y}\bar{u}$

holds, because $\overline{L_{x,y}u}_*e=L_{x,y}u=L_{x,y}(\bar{u}_*e)=(L_{x,y}\bar{u})_*e$. Therefore from (2. 1), (2. 2) and (2. 3), it follows that the left inner mapping $L_{x,y}$ is an automorphism of G.

REMARK. If G is a left di-associative loop, an inverse of a left inner mapping $L_{x,y}$ is also a left inner mapping. Hence the left inner mapping group $\mathbf{L}(G)$ consists of all finite products of left inner mappings of G.

PROPOSITION 3. *Let G be a left di-assoeiative loop (in the weak sense), in which all left inner mappings are automorphisms. Then the equation*

(2. 4) $(xy)^{-1}=x(y(y^{-1}x^{-1})^2)$

holds for all $x, y\in G$.

Proof. Since a left inner mapping $L_{y,z}=f_{yz}^{-1}\circ f_y\circ f_z$ is a homomorphism of G, we have

$$L_{y,z}z=(L_{y,z}z^{-1})^{-1}=((yz)^{-1}y)^{-1}.$$

In this equation, if we set $x=(yz)^{-1}$ and substitute z with $y^{-1}x^{-1}$, we have the required formula.

REMARK. Suppose that the loop G in the above Proposition is also right di-associative (even if in the weak sense). Then we have $(xy)^{-1}=y^{-1}x^{-1}$, that is, in this case, a transformation $x\longrightarrow x^{-1}$ of G is an anti-automorphism of G. The converse is valid more generally.

PROPOSITION 4. *Under the assumption in* Proposition 3, *the following three equations are equivalent ;*

i) $(xy)^{-1}=x^{-1}y^{-1}$,

ii) $x(yyz^{-1})=(xy)(xz)^{-1}$,

iii) $x(yyz)=(xy)(xy)(x^{-1}z)$.

Proof. i) implies ii). In fact, in the formula (2. 4), if x is substituted with x^{-1}, it holds

(2. 5) $xxy^{-1}=y(y^{-1}x)^2$,

and also

(2. 6) $z(xxy^{-1})=z(y(y^{-1}x)^2)$.

Moreover, if x and y in (2. 5) are substituted with zx and zy, respectively, it follows

(2. 7) $(zx)(zx)(zy)^{-1}=(zy)((zy)^{-1}(zx))^2$.

On the other hand, an equation $L_{z,y}(y^{-1}x)^2=(L_{z,y}(y^{-1}x))^2$ implies

(2. 8) $(zy)^{-1}(z(y(y^{-1}x)^2)) = ((zy)^{-1}(zx))^2$.

Comparing the right hand sides of (2. 6), (2. 7) and (2. 8), we have an equation

$$z(xxy^{-1}) = (zx)(zx)(zy)^{-1},$$

which is the same as ii). Also, iii) follows from ii) under the assumption i).

Conversely, i) is obtained by setting $y = x^{-1}$ in ii) or $z = y^{-1}$ in iii).

THEOREM 3. *A left di-associative loop G is a symmetric loop if and only if it satisfies the following conditions* ;

i) *the left inner mapping group* $\mathbf{I}_l(G)$ *is a subgroup of the automorphism group of G,*

ii) *the quadratic mapping is bijective,*

iii) $(xy)^{-1} = x^{-1}y^{-1}$.

Proof. By the definition of symmetric loop and by Proposition 1 and Theorem 2, it is seen that a symmetric loop has the properties i), ii) and iii). Conversely, if G is a left di-associative loop whose left inner mappings are automorphisms of G and if it satisfies iii), then Proposition 4 shows that G satisfies the axiom (1. 2) of symmetric loop. Therefore, G is a symmetric loop if it satisfies ii) additionally.

3. Embedding of symmetric loop into a group.

Let G be a symmetric loop. An associated quasigroup of reflection, G_*, of G is a quasigroup with the same underlying set as G and with a multiplication defined by

(3. 1) $x_*y = xxy^{-1}$.

The multiplication of the loop G is expressed, reciprocally, by

(3. 2) $xy = \bar{x}_*(e_*y)$.

For the details, see [3]. The axiom (1. 2) of symmetric loop implies that any left translation f_x of G is an automorphism of G_*.

Denote $\mathbf{Aut}\,G$ and $\mathbf{Aut}\,G_*$ the automorphism groups of G and G_* respectively.

PROPOSITION 5. $\mathbf{Aut}\,G$ *is a subgroup of* $\mathbf{Aut}\,G_*$ *consisting of all elements* α *of* $\mathbf{Aut}\,G_*$ *such that* $\alpha(e) = e$.

Proof. Suppose α be an element of $\mathbf{Aut}\,G$. Then $\alpha(e) = e$ and $\alpha(x_*y) = \alpha(xxy^{-1}) = \alpha(x)\alpha(x)\alpha(y)^{-1} = \alpha(x)_*\alpha(y)$. On the other hand, if $\alpha \in \mathbf{Aut}\,G_*$ satisfies $\alpha(e) = e$, then, by (3. 2), we have $\alpha(xy) = \alpha(\bar{x}_*(e_*y)) = \alpha(\bar{x})_*(e_*\alpha(y))$. Since $\bar{x}_*e = x$, it follows that $\alpha(x) = \alpha(\bar{x}_*e) = \alpha(\bar{x})_*e$, which shows $\overline{\alpha(x)} = \alpha(\bar{x})$. Thus we have $\alpha(xy) = \overline{\alpha(x)}_*(e_*\alpha(y)) = \alpha(x)\alpha(y)$.

THEOREM 4. *Let G be a symmetric loop. Then* :

i) *A mapping* $j : G \longrightarrow \mathbf{Aut}\, G_*$ *defined by* $j(x) = f_{x^2}$ *is injective.*

ii) *The image* $j(G) = \mathbf{S}$ *is an* $\mathbf{Aut}\, G$*-invariant subset of* $\mathbf{Aut}\, G_*$.

iii) $\mathbf{S} \cap \mathbf{Aut}\, G = \{\mathrm{id}\}$.

iv) *A mapping* $k : G \longrightarrow \mathbf{Aut}\, G_*/\mathbf{Aut}\, G$ (quotient space) *defined by* $k(x) = [f_x]$ *is bijective, where* $[f_x]$ *denotes a coset with a representative* f_x.

v) $\mathbf{Aut}\, G_*/\mathbf{Aut}\, G$ *is a symmetric loop with a multiplication defined by* $[f_x]\,[f_y] = [f_x \circ f_y]$, *and* k *is an isomorphism of the symmetric loops.*

Proof. i) Since any left translation of G is an automorphism of G_*, j is well defined, and i) follows from the fact that the quadratic mapping Q of G is bijective. ii) Suppose $f_{x^2} \in \mathbf{S}$ and $\alpha \in \mathbf{Aut} G$. Then $\alpha \circ f_{x^2} \circ \alpha^{-1}$ is also an element of $\mathbf{S}$. Indeed, $\alpha \circ f_{x^2}(z) = \alpha(xxz) = \alpha(x)\alpha(x)\alpha(z) = f_{\alpha(x)\alpha(x)} \circ \alpha(z)$, for any element $z \in G$. Thus $\alpha \circ j(x) = j(\alpha(x)) \circ \alpha$ holds. iii) If $\alpha \in \mathbf{S} \cap \mathbf{Aut} G$, then $\alpha = f_{x^2}$ for some $x \in G$ and $\alpha(e) = e$. Hence, we have $x^2 e = e$, which shows $x = e$ since the quadratic mapping is injective. Therefore, α must be the identity mapping. iv) If $f_x^{-1} \circ f_y$ belongs to $\mathbf{Aut}\, G$, then $f_x^{-1} \circ f_y(e) = e$, and we have $x^{-1} y = e$. Hence the mapping k is injective. On the other hand, let α be any element of $\mathbf{Aut} G_*$. Then, $\alpha^{-1} \circ f_{\alpha(e)}(e) = \alpha^{-1}(\alpha(e)e) = e$. Therefore, it follows by Proposition 5 that $\alpha^{-1} \circ f_{\alpha(e)} \in \mathbf{Aut} G$, i. e., $[\alpha] = [f_{\alpha(e)}]$. The mapping k is thus surjective. v) In Theorem 2, we proved that any left inner mapping $f_{xy}^{-1} \circ f_x \circ f_y$ of G is an automorphism of G. Hence, the coset $[f_{xy}]$ coincides with $[f_x \circ f_y]$. Since each coset of $\mathbf{Aut} G_*/\mathbf{Aut} G$ has a unique representative of left translation of G, the coset $[f_{xy}]$ is determined uniquely by the cosets $[f_x]$ and $[f_y]$. Thus the multiplication in $\mathbf{Aut} G_*/\mathbf{Aut} G$ is well defined and k is an isomorphism of the loops.

THEOREM 5. *Let* j *be the mapping of a symmetric loop* G *into the automorphism group* $\mathbf{Aut} G_*$ of G_*, *defined in* Theorem 4. *Then* :

i) $j(xy) = \overline{j(x)} \circ j(y) \circ \overline{j(x)}$, *where* $\overline{j(x)}$ *is a square root of* $j(x)$.

ii) *The subset* $\mathbf{S} = j(G)$ *of* $\mathbf{Aut} G_*$ *satisfies the followings* ;

(1) $\mathrm{id} \in \mathbf{S}$,

(2) $\mathbf{S}^{-1} = \mathbf{S}$,

(3) *if* $\alpha, \beta \in \mathbf{S}$, *then* $\alpha \circ \beta \circ \alpha \in \mathbf{S}$,

(4) *any element* $\alpha \in \mathbf{S}$ *has a unique square root* $\bar{\alpha}$ *in* $\mathbf{S}$.

Conversely, let $\mathbf{G}$ *be a group with multiplication denoted by* $\alpha \circ \beta$. *Then, any subset* $\mathbf{S}$ of $\mathbf{G}$ *satisfying* (1), (2), (3) *and* (4) *is a symmetric loop with a new multiplication defined by* $\alpha\beta = \bar{\alpha} \circ \beta \circ \bar{\alpha}$. *In this case, the identity, inverse element and any power of an element in the loop coincide with those in the group, respectively.*

Proof. i) is evident since $f_x \circ f_{y^2} \circ f_x = f_{(xy)^2}$ holds in G, and ii) is an immediate consequence of Theorem 4 in [3]. To prove the second part of the theorem, we note that any subset of a group closed under a binary operation $\alpha * \beta = \alpha \circ \beta^{-1} \circ \alpha$ is a reflection space (see [4], [5]), that is, it satisfies the axioms ; $\alpha * \alpha = \alpha$, $\alpha * (\alpha * \beta) = \beta$ and $\alpha * (\beta * \gamma) = (\alpha * \beta) * (\alpha * \gamma)$. Since any element of S has a unique square root in S, (S, $*$) itself is a quasigroup of reflection. Indeed, for any α, $\beta \in$ S, the equation $x * \alpha = \beta$ has a unique solution $x = \bar{\alpha} \circ (\overline{\bar{\alpha}^{-1} \circ \beta \circ \bar{\alpha}^{-1}}) \circ \bar{\alpha}$. Henceforth, there can be defined a symmetric loop on S with the identity element of G as that of the loop, as was studied in our previous paper [3]. (Theorem 1 in [3]). In this case, the loop multiplication $\alpha\beta$ on **S** is expressed, by definition, as (3. 2), which is equal to $\bar{\alpha} \circ \beta \circ \bar{\alpha}$. The last assertion of the theorem is clear from this expression of multiplication.

Department of Mathematics
Shimane University
Matsue, Japan

References

[1] BRUCK, R. H., *Contributions to the theory of loops*, Trans. Amer. Math. Soc., 60 (1946), 245-354.
[2] ———, *A survey of binary systems*, Springer, 1971.
[3] KIKKAWA, M., *On some quasigroups of algebraic models of symmetric spaces.*, Mem. Fac. Lit. Sci. Shimane Univ. (Nat. Sci.), 6 (1973). 9-13.
[4] LOOS, O., *Spiegelungsräume und homogene symmetrische Räume.*, Math. Zeitschr., 99 (1967), 141-170.
[5] ———, *Symmetric spaces I*, Benjamin, 1969.