Quasigroups and quandles

Jonathan D.H. Smith
Department of Mathematics, Iowa State University, Ames, IA 50011, USA

Received March 1990
Revised 1 March 1991

Dedicated to Prof. Gert Sabidussi on the occasion of his sixtieth birthdav.

Abstract

Smith, J.D.H., Quasigroups and quandles, Discrete Mathematics 109 (1992) 277–282.

Two connexions between quasigroups and quandles are established. In one direction, Joyce's homogeneous quandle construction is shown to yield a quasigroup isotopic to the loop constructed by Scimemi on the set of ϕ-commutators of a group automorphism ϕ. In the other direction, the universal multiplication group construction of quasigroup theory is extended to quandles. The group of a knot becomes the universal right multiplication group of the knot quandle.

0. Introduction

A *quasigroup* $(Q, \cdot)$ is a set Q equipped with a binary multiplication $\cdot$ such that. in the equation

$$x \cdot y = z, \tag{0.1}$$

knowledge of any two of x, y, z specifies the third uniquely. It follows that for each element x of Q, the *right multiplication*

$$R(x): Q \to Q;\ y \mapsto y \cdot x \tag{0.2}$$

and *left multiplication*

$$L(x): Q \to Q;\ y \mapsto x \cdot y \tag{0.3}$$

are permutations of Q. From the standpoint of universal algebra, the definition (0.1) is rather awkward, since it (implicitly) involves quantifiers. An equivalent [8, p. 117] definition of a quasigroup $(Q, \cdot, /, \backslash)$ may be given as a set Q equipped with three binary operations, namely *multiplication*, *right division*, and *left division* respectively, such that the identities

$$\begin{aligned} &(ER)\colon\ (x/y) \cdot y = x, \\ &(UR)\colon\ (x \cdot y)/y = x \end{aligned} \tag{0.4}$$

and

$$\begin{aligned}(EL)&: x \cdot (x\backslash y) = y,\\ (UL)&: x\backslash(x \cdot y) = y\end{aligned} \tag{0.5}$$

are satisfied. Note that identity (ER) expresses the surjectivity of the right multiplication $R(y): Q \to Q$, while (UR) expresses its injectivity.

A *right quasigroup* $(Q, \cdot, /)$ is a set Q equipped with two binary operations, namely multiplication and right division, such that the identities (0.4) are satisfied. Thus each right multiplication (0.2) is a permutation of Q. If each right multiplication is also an automorphism of the algebra $(Q, \cdot, /)$, then the right quasigroup $(Q, \cdot, /)$ is said to be *right distributive*. Note that automorphisms of $(Q, \cdot)$ are automatically automorphisms of $(Q, /)$.

A right quasigroup is said to be *idempotent* if each singleton in Q is a subalgebra of $(Q, \cdot)$, and hence also a subalgebra of $(Q, \cdot, /)$. In [3], idempotent right distributive right quasigroups were defined directly and studied under the name *quandles*. The purpose of the current paper is to emphasize the point of view that quandles are right quasigroups. The connections and analogies betwen quasigroups and quandles are used in two directions.

In the first part, Joyce's representation of quandles as coset classes [3, §7] is used to shed new light on a construction of Scimemi [6] which in turn arose from Glauberman's work [2] on the solubility of certain loops of odd order and Lazard's relationship [5] between Lie rings and nilpotent groups. In the second part, a standard construction from quasigroup theory, the universal multiplication group [8, Section 2.4], is carried over to quandle theory in order to give a concrete interpretation to a group that Joyce defined abstractly [3, §6] in terms of generators and relations. This interpretation tightens the relationship between knot groups and knot quandles that was part of the original motivation for studying quandles.

1. Commutators of automorphisms

Let φ be an automorphism of a group G. For an element x in G, the commutator $[\varphi, x]$ denotes the element $\varphi(x^{-1})x$ of G. (The notation corresponds to the usual group commutator of φ and x in the holomorph of G.) Set $[\varphi, G] = \{[\varphi, x] \mid x \in G\}$. If G is of prime power order coprime to the order of φ [6, Theorem 1], or if is an involution and square roots may be extracted in G [6, §3], Scimemi defines a loop $([\varphi, G], \circ)$ by

$$xy \in C_G(\varphi)(x \circ y). \tag{1.1}$$

Here $C_G(\varphi)$ is the fixed point set of φ. Recall that a loop is a quasigroup with an *identity element* e such that $R(e) = L(e) = 1$. Scimemi's construction is one of the basic components of an extremely interesting programme examining relationships between the Feit–Thompson Theorem, the Burnside Problem, and Baker–Campbell–Hausdorff formulae.

On the other hand, if φ is again an automorphism of a group G, then Joyce [3, §7] defines a quandle $(G, \cdot, /)$ by

$$\begin{aligned} x \cdot y &= \varphi(x)[\varphi, y], \\ x/y &= \varphi^{-1}(x)[\varphi^{-1}, y]. \end{aligned} \tag{1.2}$$

If H is a subgroup of $C_G(\varphi)$, then $x \mapsto Hx$ induces a quandle structure on the set $H\backslash G$ of right cosets of H in G. This quandle $(H\backslash G; \varphi)$ is *homogeneous*, in the sense that its automorphism group is transitive. Each homogeneous quandle is constructed in this way [3, Theorem 7.1].

The main result of this section, Theorem 1, gives a general condition on a group automorphism under which Scimemi's construction works. In the same context Joyce's construction builds a quandle which is actually a quasigroup. Then Scimemi's loop and Joyce's quasigroup are principally isotopic. Recall that a *principal isotopy* $(\alpha, \beta):(A, \cdot)\rightarrow(A, \circ)$ between two binary multiplication structures $(A, \cdot)$ and $(A, \circ)$ on a set A is a pair (α, β) of bijections of A such that

$$\alpha(x)\circ\beta(y)=x\cdot y \tag{1.3}$$

for all x, y in A.

Theorem 1. *Let φ be an automorphism of a group G such that $C_G(\varphi)$ is finite and has $[\varphi, G]$ as a right transversal. Then*

$$xy \in C_G(\varphi)(x\circ y) \tag{1.4}$$

defines a loop $([\varphi, G], \circ)$, while

$$\varphi(x)[\varphi, y] \in C_G(\varphi)(x\cdot y) \tag{1.5}$$

defines a right distributive quasigroup $([\varphi, G], \cdot)$ principally isotopic to the loop $([\varphi, G], \circ)$.

Proof. The bijection $[\varphi, G]\rightarrow C_G(\varphi)\backslash G$; $x\mapsto C_G(\varphi)x$ yields an isomorphism of $([\varphi, G], \cdot)$ with the homogeneous quandle $(C_G(\varphi)\backslash G; \varphi)$. Since $[\varphi, G]$ is a right transversal to $C_G(\varphi)$, it follows that the left multiplication $L(1):C_G(\varphi)\rightarrow C_G(\varphi)$; $y\mapsto[\varphi, y]$ is injective, and thus bijective by the finiteness of $C_G(\varphi)$.

Since the quandle is homogeneous, all its left multiplications (0.3) then have to be invertible, and the quandle becomes a quasigroup $([\varphi, G], \cdot)$. By (1.4) and (1.5), one has $\varphi(x)\circ[\varphi, y]=x\cdot y$. Thus $(\varphi, L(1)):([\varphi, G], \cdot)\rightarrow([\varphi, G], \circ)$ is a principal isotopy. As a principal isotope of the quasigroup $([\varphi, G], \cdot)$, the binary multiplication $([\varphi, G], \circ)$ itself becomes a quasigroup, and indeed a loop with 1 as identity element. □

Remark 1.1. A notable instance of Theorem 1 is obtained on taking G to be the multiplication group (as below) of a finite commutative Moufang loop of exponent 3, and φ to be conjugation (within the permutation group of the underlying set of the commutative Moufang loop) by the inversion mapping $x \mapsto x^{-1}$ of the commutative Moufang loop. Then (1.4) recovers the commutative Moufang loop, while (1.5) yields the totally symmetric distributive quasigroup associated with a Hall triple system. See [1] and [7].

2. Knot groups and quandles

For a quasigroup Q, the subgroup $\langle R(x), L(x) \mid x \in Q \rangle$ of the permutation group $Q!$ of the set Q generated by all the right and left multiplications (0.2), (0.3) is called the *(combinatorial) multiplication group* $G = \operatorname{Mlt} Q$ of Q [8, Section 2.1]. If Q is a subquasigroup of a quasigroup P, then the subgroup $\langle R_P(x), L_P(x) \mid x \in Q \rangle$ of the permutation group $P!$ of the set P generated by all the *relative* right and left multiplications $R_P(x): P \to P$; $y \mapsto yx$ and $L_P(x): P \to P$; $y \mapsto xy$ for x restricted to Q is called the *relative multiplication group* $\operatorname{Mlt}_P Q$ *of Q in P*. Finally, if Q lies in a variety V of quasigroups, Q may be identified with its image in the coproduct $Q[X]$ of Q with the free V-quasigroup $\langle X \rangle$ on a singleton 'indeterminate' X. Then the *universal multiplication group* $\tilde{G} = U(Q; V)$ of Q in V is defined to be the relative multiplication group of Q in $Q[X]$ [8, Section 2.3].

One usually writes $\tilde{R}(x)$ for $R_{Q[X]}(x)$, and similarly $\tilde{L}(x)$. The universal multiplication group plays an important role in the representation theory of quasigroups [8, Chapter 3]. Moreover, the assignment of universal multiplication groups gives a functor from the category V of V-quasigroups and homomorphisms to the category of groups, whereas the assignment of combinatorial multiplication groups does not. The mappings $\tilde{R}(x) \mapsto R_P(x)$ and $\tilde{L}(x) \mapsto L_P(x)$ induce a homomorphism from $\tilde{G}$ onto any relative multiplication group of Q in a V-quasigroup P, in particular onto the combinatorial multiplication group G. Thus the composite homomorphism $\tilde{G} \to G \to Q!$ gives a natural permutation representation of $\tilde{G}$ on Q.

For a quandle Q, the right multiplications are permutations, so one may analogously define the *right multiplication group* $G = R \operatorname{Mlt} Q$ of Q to be the subgroup $\langle R(x) \mid x \in Q \rangle$ of $Q!$. Joyce [3, §5] called this group the 'inner automorphism group' of A. Extending the analogy, one may define a *relative right multiplication group* $R \operatorname{Mlt}_P Q$ for Q a subquandle of P, and then a universal right multiplication group $\tilde{G} = RU(Q; W)$ for a quandle Q in a variety W of quandles. The argument of [8, Section 2.3] carries over to show that Q embeds in the corresponding coproduct $Q[X]$. Let K denote the variety of all quandles ('Kwandles'). The main result of this section, Theorem 2 below, identifies $RU(Q; K)$ as being a group that Joyce [3, §6] defined abstractly in terms of generators and relations. Joyce called this group 'Adconj Q', while Winker [9, Definition 5.1.1] called it 'Conj Q'.

Theorem 2. *Let Q be a quandle. Let A be the group generated by the set $\{\bar q \mid q \in Q\}$ subject to the relations*

$$\overline{q\cdot r} = \bar r^{-1}\bar q\bar r \tag{2.1}$$

for q, r in Q. Then the mappings $\bar q \mapsto \tilde R(q)$ induce an isomorphism of A with $RU(Q;\boldsymbol{K})$.

Proof. For x in $Q[X]$, one has $(x\cdot r)\tilde R(q\cdot r) = (x\cdot r)\cdot(q\cdot r) = (x\cdot q)\cdot r = (x\cdot r)\tilde R(r)^{-1}\tilde R(q)\tilde R(r)$. Thus $RU(Q;\boldsymbol{K})$ is an image of the group A via the mappings $\bar q \mapsto \tilde R(q)$. Conversely, it will be shown that the group A in turn is a homomorphic image of $RU(Q;\boldsymbol{K})$ under $\tilde R(q)\mapsto \bar q$, showing that the groups are in fact isomorphic as claimed.

For a group H, let $HJ = (H, \cdot, /)$ denote the quandle on H with $x\cdot y = y^{-1}xy$ and $x/y = yxy^{-1}$. (Joyce [3, Definition 1.2] writes 'Conj H' for HJ.) The mappings $q \mapsto \bar q$ for q in Q induce a quandle homomorphism $\eta : Q \to AJ$ [3, §6]. Applying the universal right multiplication group functor yields a group homomorphism

$$RU(\eta;\boldsymbol{K}) : RU(Q;\boldsymbol{K}) \to RU(AJ;\boldsymbol{K}) \tag{2.2}$$

mapping $\tilde R(q)$ to $\tilde R(\bar q)$ for q in Q. Now let C denote the free product (or coproduct in the category of groups and homomorphisms) of A with the free group $\mathbb{Z}X$ on the singleton $\{X\}$. The group A embeds into C, so the quandle AJ embeds into CJ. The relative right multiplication group $M\,\mathrm{Mlt}_{CJ}\,AJ$ is a quotient of $RU(AJ;\boldsymbol{K})$ via $\tilde R(a) \mapsto R_{CJ}(a)$ for a in A. Since $R_{CJ}(ab) = R_{CJ}(a)R_{CJ}(b)$ for a, b in A, the group $R\,\mathrm{Mlt}_{CJ}\,AJ$ is generated by $\{R_{CJ}(\bar q) \mid q \in Q\}$. Thus $R\,\mathrm{Mlt}_{CJ}\,AJ$ is a quotient of $U(Q;\boldsymbol{K})$ via the composite of $RU(\eta;\boldsymbol{K})$ with $RU(AJ;\boldsymbol{K}) \to R\,\mathrm{Mlt}_{CJ}\,AJ$. It remains to be shown that A is isomorphic to $R\,\mathrm{Mlt}_{CJ}\,AJ$, via the surjective group homomorphism

$$R_{CJ} : A \to R\,\mathrm{Mlt}_{CJ}\,AJ;\ a \mapsto R_{CJ}(a). \tag{2.3}$$

But if $R_{CJ}(a) = 1$ for a in A, then $a^{-1}Xa = XR_{CJ}(a) = X \in \mathbb{Z}X \cap a^{-1}\mathbb{Z}Xa$. By the structure of free products of groups [4, Corollary 4.1.5 and Lemma 4.1] it follows that $a \in A \cap \mathbb{Z}X = \{1\}$. Thus (2.3) is an isomorphism. The composite $RU(Q;\boldsymbol{K}) \to RU(AJ;\boldsymbol{K}) \to R\,\mathrm{Mlt}_{CJ}\,AJ \to A$ maps $\tilde R(q) \mapsto \tilde R(\bar q) \mapsto R_{CJ}(\bar q) \mapsto \bar q$, as required. □

Joyce [3, §14] associates a quandle $Q(K)$ to a knot K. It is a complete invariant for tame knots [3, Corollary 16.3].

Corollary 2.1. *For a knot K embedded tamely in the 3-sphere S^3, the knot group $\pi_1(S^3 - K)$ is isomorphic to the universal right multiplication group $RU(Q(K);\boldsymbol{K})$ of the knot quandle.*

Proof. For $Q = Q(K)$ in Theorem 2, the knot group is isomorphic to A [3, §15]. □

References

[1] M. Deza and G. Sabidussi, Combinatorial structures arising from commutative Moufang loops, in: O. Chein, H. Pflugfelder and J.D.H. Smith, eds., Quasigroups and Loops: Theory and Applications (Heldermann, Berlin, 1990).

[2] G. Glauberman, On loops of odd order, J. Algebra 1 (1964) 374–396.

[3] D. Joyce, A classifying invariant of knots, the knot quandle, J. Pure Appl. Algebra 23 (1982) 37–65.

[4] A. Karras, W. Magnus and D. Solitar, Combinatorial Group Theory (Wiley, New York, 1966).

[5] M. Lazard, Sur les groups nilpotents et les anneaux de Lie, Ann. Sci. École Norm. Sup. 71 (1954) 101–190.

[6] B. Scimemi, Cappi di Bruck e loro generalizzazioni, Rend. Sem. Mat. Univ. Padova 60 (1978) 141–149.

[7] J.D.H. Smith, On the nilpotence class of commutative Moufang loops, Math. Proc. Cambridge Philos. Soc. 84 (1978) 387–404.

[8] J.D.H. Smith, Representation Theory of Infinite Groups and Finite Quasigroups (Presses Univ. Montréal, Montréal, 1986).

[9] S.K. Winker, Quandles, knot invariants, and the n-fold branched cover, Ph.D. Thesis, University of Illinois at Chicago Circle, Chicago, 1984.