Comment.Math.Univ.Carolin. 51,2 (2010) 279–286

Quasigroup automorphisms and symmetric group characters

Brent Kerby, Jonathan D.H. Smith

Abstract. The automorphisms of a quasigroup or Latin square are permutations of the set of entries of the square, and thus belong to conjugacy classes in symmetric groups. These conjugacy classes may be recognized as being annihilated by symmetric group class functions that belong to a λ-ideal of the special λ-ring of symmetric group class functions.

Keywords: Latin square, quasigroup, automorphism, λ-ring

Classification: 05B15, 19A22, 20N05

1. Introduction

For a given $n \geq 0$, the set of automorphisms of n-element quasigroups or Latin squares is a union of conjugacy classes in the symmetric group S_n. The main result of this note (Theorem 4.5) shows that the class functions annihilating these automorphisms form a λ-ideal AK_n in the special λ-ring $R(S_n)$ of class functions on S_n. Further study of this structure may prove to be of assistance in working towards a fuller specification of quasigroup automorphisms.

A preliminary section lists some known facts about quasigroup automorphisms, while Section 3 recalls the definition of a λ-ring. Section 4 then presents annihilators of automorphisms, and the way they fit in to the λ-ring structure of $R(S_n)$. For concepts and conventions that are not otherwise explained here, see [8], [9].

2. Quasigroup automorphisms

This section assembles some well-known and elementary observations about automorphisms of quasigroups or Latin squares. Readers are also referred to [2], [4], [5], [7] for further discussion (which may involve general quasigroup autotopies, and not just automorphisms).

Lemma 2.1. *Let $k \geq 0$. If θ is an automorphism of a quasigroup Q, then so is the power θ^k.*

A class $\mathcal{C}$ of quasigroups is said to be *abstract* if each quasigroup isomorphic to a member of $\mathcal{C}$ also lies in $\mathcal{C}$.

Lemma 2.2. *Let $\mathcal{C}$ be an abstract class of quasigroups. Let $n \geq 0$. Suppose that a permutation θ is an automorphism of an n-element quasigroup $(Q, \cdot)$ from the class $\mathcal{C}$. Then for each element π of the symmetric group S_n, the conjugate $\pi^{-1}\theta\pi$ is also an automorphism of an n-element $\mathcal{C}$-quasigroup.*

Proof: Define a product $\circ$ on Q by

$$x \circ y = (x\pi^{-1} \cdot y\pi^{-1})\pi \tag{2.1}$$

for $x, y \in Q$. Since $\pi : Q \to Q$ is bijective, it follows that $(Q, \circ)$ is a quasigroup. Indeed, (2.1) shows that $\pi : (Q, \cdot) \to (Q, \circ)$ is a quasigroup isomorphism. Thus the composite $\pi^{-1}\theta\pi : (Q, \circ) \to (Q, \circ)$ is an automorphism. Moreover, since $(Q, \circ)$ is isomorphic (via π) to the $\mathcal{C}$-quasigroup $(Q, \cdot)$, it itself lies in $\mathcal{C}$. □

Lemma 2.3. *For $i \in \{1, 2\}$, suppose that θ_i is an automorphism of a quasigroup Q_i. Then*

$$\theta_1 \times \theta_2 : Q_1 \times Q_2 \to Q_1 \times Q_2; (x_1, x_2) \mapsto (x_1\theta_1, x_2\theta_2)$$

is an automorphism of $Q_1 \times Q_2$.

Lemma 2.4 (Fixpoint Condition)**.** *A nontrivial automorphism of a finite quasigroup Q cannot fix more than $|Q|/2$ elements of Q.*

Proof: The set of fixed points of an automorphism of Q forms a subquasigroup of Q. No proper subquasigroup of Q can have more than $|Q|/2$ elements. □

Lemma 2.5. *Let q be a prime power. Then there is a quasigroup automorphism of cycle type $(q-1)^1 1^1$.*

Proof: Let e be a primitive element of the field $\mathrm{GF}(q)$. Then right multiplication by e in $\mathrm{GF}(q)$ gives an automorphism of the group $(\mathrm{GF}(q), +)$. □

Remark 2.6. The hypothesis that q be a prime power may be dropped. See [10, Theorem 6], or [2, Theorem 2.3, $f = 1$].

Lemma 2.7. *Let n be a positive integer.*

(a) *If n is even, there is no quasigroup automorphism of cycle type n^1.*
(b) *If n is odd, there is a quasigroup automorphism of cycle type n^1.*

Proof: (a) Compare the discussion of [10, Theorem 6].

(b) For odd n, the translation $x \mapsto x + 1$ is an automorphism of the arithmetic mean quasigroup $x \circ y = (x + y)/2$ on the set of integers modulo n. □

For small values of n, Table 1 lists the cycle types of automorphisms of n-element quasigroups, determined by an exhaustive computer calculation (compare [4]). The results discussed in this section serve to specify many of these types, and eliminate types that do not appear. However, these results do not account for the absence of the cycle types 2^3 and $4^1 2^1$ from the list for $n = 6$, for example. This absence is addressed in Remark 4.6.

n	Cycle types of n-element quasigroup automorphisms
1	1^1
2	1^2
3	$1^3,\ 2^1 1^1,\ 3^1$
4	$1^4,\ 2^1 1^2,\ 2^2,\ 3^1 1^1$
5	$1^5,\ 2^2 1^1,\ 3^1 1^2,\ 4^1 1^1,\ 5^1$
6	$1^6,\ 2^2 1^2,\ 3^1 1^3,\ 3^2,\ 4^1 1^2,\ 5^1 1^1$
7	$1^7,\ 2^2 1^3,\ 2^3 1^1,\ 3^2 1^1,\ 4^1 1^3,\ 4^1 2^1 1^1,\ 5^1 1^2,\ 6^1 1^1,\ 7^1$
8	$1^8,\ 2^2 1^4,\ 2^3 1^2,\ 2^4,\ 3^2 1^2,\ 4^1 1^4,\ 4^1 2^1 1^2,\ 4^1 2^2,\ 4^2,\ 5^1 1^3,\ 6^1 1^2,\ 7^1 1^1$
9	$1^9,\ 2^3 1^3,\ 2^4 1^1,\ 3^2 1^3,\ 3^3,\ 4^2 1^1, 5^1 1^4, 6^1 1^3, 6^1 2^1 1^1, 6^1 3^1, 7^1 1^2, 8^1 1^1, 9^1$

Table 1. Cycle types of quasigroup automorphisms

3. λ-rings

A *λ-ring* A [1, §1], [3, §3.1] [1] is a commutative, unital ring equipped with unary *λ-operations* λ^n for each $n \geq 0$, such that the identities

$$\lambda^0(x) = 1, \qquad \lambda^1(x) = x,$$

and

$$\lambda^n(x+y) = \sum_{k=0}^{n} \lambda^k(x)\lambda^{n-k}(y) \tag{3.1}$$

are satisfied. Defining the generating function

$$\lambda_t(x) = \sum_{n=0}^{\infty} \lambda^n(x) t^n$$

for each element x of A, with indeterminate t, the identity (3.1) may be rewritten in the form $\lambda_t(x+y) = \lambda_t(x)\lambda_t(y)$.

Example 3.1. The ring $\mathbb{Z}$ of integers becomes a λ-ring with $\lambda_t(x) = (1+t)^x$, the identity $\lambda_t(x+y) = \lambda_t(x)\lambda_t(y)$ being clearly satisfied.

Definition 3.2. A subset I of a λ-ring A is said to be a λ-*ideal* if

(a) I is an ideal of A;

[1] Some authors say *pre-λ-ring*, reserving the term *λ-ring* for the special λ-rings of Definition 3.3 — compare [6, pp. 7, 13].

(b) for each element x of I, one has $\lambda^k(x) \in I$ for $k > 0$.

Now let $\xi_1, \dots, \xi_q$, $\eta_1, \dots, \eta_r$ be indeterminates. Use

$$\sum_{i=0}^{\infty} s_i t^i = \prod_{k=1}^{q} (1 + \xi_k t) \quad \text{and} \quad \sum_{i=0}^{\infty} \sigma_i t^i = \prod_{k=1}^{r} (1 + \eta_k t)$$

to define the *elementary symmetric functions*

$$s_i(\xi_1, \dots, \xi_q), \qquad \sigma_i(\eta_1, \dots, \eta_r).$$

Then define $P_n(s_1, \dots, s_n; \sigma_1, \dots, \sigma_n)$ to be the coefficient of t^n in

$$\prod_{i=1}^{q} \prod_{j=1}^{r} (1 + \xi_i \eta_j t) .$$

Define $P_{n,d}(s_1, \dots, s_{nd})$ to be the coefficient of t^n in

$$\prod_{1 \le i_1 < \dots < i_d \le q} (1 + \xi_{i_1} \dots \xi_{i_d} t) .$$

Definition 3.3. A λ-ring is said to be *special* if it satisfies the identities

$$\lambda^n(xy) = P_n\left(\lambda^1(x), \dots, \lambda^n(x); \lambda^1(y), \dots, \lambda^n(y)\right)$$

and

$$\lambda^m\left(\lambda^n(x)\right) = P_{m,n}\left(\lambda^1(x), \dots, \lambda^{mn}(x)\right) \tag{3.2}$$

for all $m, n \ge 0$.

Remark 3.4. Setting $n = 0$ in (3.2) yields $\lambda_t(1) = 1 + t$. Thus the λ-ring structure of Example 3.1 is the unique special λ-ring structure on the ring $\mathbb{Z}$ of integers.

Theorem 3.5 ([6, p. 54])**.** *The ring $R(G)$ of complex class functions on a finite group G forms a special λ-ring.*

4. Automorphism annihilators

In order to make relations like (4.2) below as clear as possible, the value of a symmetric group class function χ at a permutation π will be written with a "pairing" notation as $\langle \pi, \chi \rangle$. For a partition τ of a positive integer n, there are two class functions on S_n associated with τ. We will write χ_τ for the characteristic function of the set of permutations of cycle type τ, while χ^τ will denote the irreducible character of S_n determined by τ (according to the procedure of [6, §III.4], for example). Let $\mathcal{C}$ be an abstract class of quasigroups. In particular, let $\mathcal{Q}$ be the class of all quasigroups.

Definition 4.1. A class function α on the symmetric group S_n is a $\mathcal{C}$-*automorphism annihilator* if $\langle \theta, \alpha \rangle = 0$ for each automorphism θ of a $\mathcal{C}$-quasigroup of order n.

For each $n \geq 0$, define the *automorphism kernel* $AK_n(\mathcal{C})$ to be the complex vector space that consists of all the $\mathcal{C}$-automorphism annihilators on S_n.

Example 4.2. (a) The space $AK_2(\mathcal{Q})$ is spanned by $\chi^{2^1} - \chi^{1^2}$ or the characteristic function χ_{2^1} of the set consisting of the permutation of cycle type 2^1.

(b) The space $AK_3(\mathcal{Q})$ is trivial.

(c) The space $AK_4(\mathcal{Q})$ is spanned by the character

$$\chi^{4^1} - \chi^{3^1 1^1} + \chi^{2^1 1^2} - \chi^{1^4}$$

— or by the characteristic function χ_{4^1} of the set of permutations of cycle type 4^1.

The following proposition shows how automorphism annihilators are used to identify quasigroup automorphisms.

Proposition 4.3. *For a $n \geq 0$, let π be an element of S_n. Then π is an automorphism of an n-element $\mathcal{C}$-quasigroup if and only if*

$$\forall\ \alpha \in AK_n(\mathcal{C}),\ \langle \pi, \alpha \rangle = 0. \tag{4.1}$$

Proof: The "only if" direction is immediate from Definition 4.1. For the converse, suppose that a permutation π satisfies (4.1). Let N be the subset of S_n consisting of permutations which are not $\mathcal{C}$-quasigroup automorphisms. By Lemma 2.2, the characteristic function χ_N is a class function on S_n. It is certainly a $\mathcal{C}$-automorphism annihilator. By (4.1), χ_N takes the value zero on π. Thus π is identified as a $\mathcal{C}$-quasigroup automorphism. $\square$

Remark 4.4. To verify that (4.1) holds for a permutation π, it suffices to check the condition $\langle \pi, \alpha \rangle = 0$ for α from a basis of the automorphism kernel $AK_n(\mathcal{C})$.

Theorem 4.5. *For each $n \geq 0$, the automorphism kernel $AK_n(\mathcal{C})$ forms a λ-ideal in the special λ-ring $R(S_n)$ of symmetric group class functions.*

Proof: Let θ be a $\mathcal{C}$-quasigroup automorphism. Suppose that α is a $\mathcal{C}$-automorphism annihilator. Then for each character χ of S_n,

$$\langle \theta, \alpha\chi \rangle = \langle \theta, \alpha \rangle \langle \theta, \chi \rangle = 0.$$

Thus the space $AK_n(\mathcal{C})$ is an ideal of the ring $R(S_n)$.

Now consider a positive integer k. The Adams operation ψ^k is defined on $R(S_n)$ by

$$\langle \pi, \psi^k(\chi) \rangle = \langle \pi^k, \chi \rangle \tag{4.2}$$

for each character χ [6, p. 54]. For each $\mathcal{C}$-quasigroup automorphism θ, one has

$$\langle \theta, \psi^k(\alpha) \rangle = \langle \theta^k, \alpha \rangle = 0$$

by (4.2) and Lemma 2.1. Thus the space $AK_n(\mathcal{C})$ is closed under the various Adams operations ψ^k for positive integers k. The corresponding λ-operations are given by

$$\lambda^k = \frac{1}{k!}\begin{vmatrix} \psi^1 & 1 & 0 & \dots & \dots & 0 \\ \psi^2 & \psi^1 & 2 & 0 & \dots & 0 \\ & & \ddots & & & \\ & & & \ddots & & \\ \psi^k & \psi^{k-1} & \dots & & & \psi^1 \end{vmatrix}$$

[6, p. 54]. Since each term of the determinant's Laplace expansion down the first column involves at least one Adams operation with positive index, the set $AK_n(\mathcal{C})$ is closed under the λ-operations λ^k for positive integers k. $\square$

Remark 4.6. The ideal $AK_6(\mathcal{Q})$ contains the character

$$\chi^6 - \chi^{5^1 1^1} + \chi^{4^1 2^1} - \chi^{3^2}$$

which takes nonzero values on the problematic conjugacy classes of cycle types 2^3 and $4^1 2^1$, as well as on 6^1.

Corollary 4.7. *For each $n \geq 0$, the quotient $R(S_n)/AK_n(\mathcal{C})$ is a special λ-ring whose dimension is equal to the number of conjugacy classes of $\mathcal{C}$-quasigroup automorphisms in S_n.*

Definition 4.8. For a $n \geq 0$ and abstract class $\mathcal{C}$ of quasigroups, we call the special λ-ring

$$ATR_n(\mathcal{C}) = R(S_n)/AK_n(\mathcal{C})$$

the *automorphism type ring* for $\mathcal{C}$ of order n.

Let $P(n)$ be the number of partitions of n. Corollary 4.7 gives the following *Duality Principle*.

Proposition 4.9. *Let n be a positive integer. Let A be a set of cycle types of automorphisms of n-element $\mathcal{C}$-quasigroups. Let L be a linearly independent subset of the automorphism kernel $AK_n(\mathcal{C})$. Then*

$$|A| + |L| \leq P(n). \tag{4.3}$$

Equality holds in (4.3) *if and only if L spans $AK_n(\mathcal{C})$ and A contains all $\mathcal{C}$-automorphism cycle types.*

We will illustrate the Duality Principle for $\mathcal{Q}$ in the case $n = 5$, aiming at the middle row of Table 1. Certainly the trivial 1^5 is an automorphism type. By Lemma 2.7(b), 5^1 is an automorphism type. By Lemma 2.5, $4^1 1^1$ is an automorphism type. By Lemma 2.1, it follows that $2^2 1^1$ is an automorphism type. This gives the set

$$A = \{1^5,\ 2^2 1^1,\ 4^1 1^1,\ 5^1\} \tag{4.4}$$

of automorphism types. On the other hand, the Fixpoint Condition (Lemma 2.4) shows that the characteristic function $\chi_{2^1 1^3}$ is an automorphism annihilator. By Theorem 4.5, it follows that

$$\psi^3\left(\chi_{2^1 1^3}\right) = \chi_{2^1 1^3} + \chi_{3^1 2^1}$$

also lies in $AK_5(\mathcal{Q})$, and we obtain the linearly independent subset

$$L = \{\chi_{2^1 1^3},\ \psi^3\left(\chi_{2^1 1^3}\right)\}$$

of $AK_5(\mathcal{Q})$.

At this stage, there is a single issue still to be resolved: Is $3^1 1^2$ a $\mathcal{Q}$-automorphism type? The Duality Principle alone is insufficient to show that it is. Indeed, if $3^1 1^2$ were not a $\mathcal{Q}$-automorphism type, then the characteristic function $\chi_{3^1 1^2}$ would be in $AK_5(\mathcal{Q})$, as would $\psi^2(\chi_{3^1 1^2})$. However, there is a relation

$$\psi^3\left(\chi_{2^1 1^3}\right) - \chi_{2^1 1^3} = \chi_{3^1 2^1} = \psi^2\left(\chi_{3^1 1^2}\right) - \chi_{3^1 1^2},$$

so the set

$$L'' = \{\chi_{2^1 1^3},\ \psi^3\left(\chi_{2^1 1^3}\right),\ \chi_{3^1 1^2},\ \psi^2\left(\chi_{3^1 1^2}\right)\}$$

prunes to the linearly independent subset

$$L' = \{\chi_{2^1 1^3},\ \psi^3\left(\chi_{2^1 1^3}\right),\ \chi_{3^1 1^2}\}$$

of $AK_4(\mathcal{Q})$, and then the relation

$$|A| + |L'| = 7 = P(5) \tag{4.5}$$

is still consistent with the Duality Principle. In fact, quasigroups with an automorphism of cycle type $3^1 1^2$ do exist [2, Theorem 2.3, $f = 2$]; for example, the quasigroup with the following Cayley table has (123) as an automorphism:

	1	2	3	4	5
1	1	4	5	2	3
2	5	2	4	3	1
3	4	5	3	1	2
4	2	3	1	4	5
5	3	1	2	5	4

Remark 4.10. The set A of (4.4) presents the full set of cycle types of automorphisms of 5-element entropic quasigroups (i.e., those satisfying $xy \cdot zt = xz \cdot yt$), including the abelian group $(\mathrm{GF}(5), +)$ of Lemma 2.5 and the arithmetic mean quasigroup of Lemma 2.7(b). For this reason, the sets A and L' combine to give the complete equality (4.5) for $n = 5$, in accordance with the Duality Principle for the class $\mathcal{E}$ of entropic quasigroups.

References

[1] Atiyah M.F., Tall D.O., *Group representations, λ-rings, and the J-homomorphism*, Topology **8** (1969), 253–297.
[2] Bryant D., Buchanan M., Wanless I.M., *The spectrum for quasigroups with cyclic automorphisms and additional symmetries*, Discrete Math. **309** (2009), 821–833.
[3] tom Dieck T., *Transformation Groups and Representation Theory*, Springer, Berlin, 1979.
[4] Falcón R.M., *Cycle structures of autotopisms of the Latin squares of order up to* 11, `arXiv:0709.2973v2 [math.CO]`, 2009; to appear in Ars Combinatoria.
[5] Falcón R.M., Martín-Morales J., *Gröbner bases and the number of Latin squares related to autotopisms of order* ≤ 7, J. Symbolic Comput. **42** (2007), 1142–1154.
[6] Knutson D., *λ-rings and the Representation Theory of the Symmetric Group*, Springer, Berlin, 1973.
[7] McKay B.D., Meynert A., Myrvold W., *Small Latin squares, quasigroups and loops*, J. Combin. Designs **15** (2007), 98–119.
[8] Smith J.D.H., *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.
[9] Smith J.D.H., Romanowska A.B., *Post-Modern Algebra*, Wiley, New York, NY, 1999.
[10] Wanless I.M., *Diagonally cyclic latin squares*, European J. Combin. **25** (2004), 393–413.

Department of Mathematics, University of Utah, Salt Lake City, Utah 84112, U.S.A.

E-mail: kerby@math.utah.edu

Department of Mathematics, Iowa State University, Ames, Iowa 50011, U.S.A.

E-mail: jdhsmith@iastate.edu

URL: `http://www.orion.math.iastate.edu/jdhsmith/`

(*Received* October 4, 2009, *revised* January 4, 2010)