ISOTOPY AND PARASTROPHY OF QUASIGROUPS

R. ARTZY

1. It has been noted that every quasigroup \((Q, \cdot)\) belongs to a set of 6 quasigroups, called adjugate by Fisher and Yates \([4]\), conjugate by Stein \([6]\), parastrophic by Sade \([5]\). If in \((Q, \cdot), xy = z\), then in the parastrophic quasigroups \((x\pi)(y\pi) = z\pi\), where \(\pi\) is one of the 6 permutations of \(\{x, y, z\}\), \(v\pi\) the image of \(v \in \{x, y, z\}\) under \(\pi\), and \((\cdot)\) the operation in the parastrophic quasigroup \((Q, \pi)\). Let \(\rho\) be the permutation \((\pi\rho\pi\tau)\), \(\tau = (\pi\rho\pi\tau)\). Then every \(\pi\) is generated by \(\rho\) and \(\tau\), the generators of the symmetric group \(S_3\), and defining relations are \(\tau^2 = (\rho\tau)^2 = \rho^3 = I\), the identity permutation. The mappings of quasigroups \((Q, \pi)\) on each other will be called parastrophisms.

If \(\alpha, \beta, \gamma\) are permutations of the elements of \(Q\), then \((Q, \kappa)\) with the operation \((\kappa)\) such that \((x\alpha)(\kappa)(y\beta) = (xy)\gamma\) is an isotope of \((Q, \cdot)\). The mappings of the quasigroups \((Q, \kappa)\) onto each other are the isotopisms of \(Q\), with the notation \(\kappa = [\alpha, \beta, \gamma]\) for the isotope \((Q, \cdot) \rightarrow (Q, \kappa)\). Since the parastrophisms and the isotopisms are permutations, both the parastrophisms and the isotopisms of \(Q\) form groups, the parastrophism group being isomorphic to \(S_3\) or to one of its subgroups. The parastrophism \((Q, \cdot) \rightarrow (Q, \pi)\), induced by the permutation \(\pi\), will also be called \(\pi\). The group generated by all the parastrophisms and isotopisms of \(Q\) will be called \(G\).

**Theorem 1.** The isotopism group, \(T\), of \(Q\) is normal in \(G\).

**Proof.** Since \(G\) is generated by \(\rho, \tau\) and \(T\), it is sufficient to prove \(\rho^{-1}T\rho \in T, \rho^{-1}T\rho \in T\) and, in view of \(\tau = \tau^{-1}, \tau T\tau \in T\). Let \([\alpha, \beta, \gamma]\) be an isotopism. Then, by a well-known rule for permutations, \(\rho^{-1}[\alpha, \beta, \gamma]\rho = [\beta, \gamma, \alpha] \in T\) and \(\rho[\alpha, \beta, \gamma]\rho^{-1} = (\rho^{-1})^{-1}[\alpha, \beta, \gamma]\rho^{-1} = [\gamma, \alpha, \beta] \in T\). Moreover, \(\tau[\alpha, \beta, \gamma]\tau = [\beta, \alpha, \gamma] \in T\).

**Corollary.** If a quasigroup \(Q_1\) is carried into a quasigroup \(Q_2\) by a parastrophism \(\pi\), then every quasigroup isotopic to \(Q_1\) is carried by \(\pi\) into an isotope of \(Q_2\).

**Proof.** Let \(Q_1\kappa\) be the isotope of \(Q_1\). We have \(Q_2 = Q_1\pi\), hence \(Q_1\kappa\pi = Q_2\pi^{-1} \kappa\pi = Q_2\lambda\), with \(\lambda = \pi^{-1} \kappa \pi \in T\), by Theorem 1.

The Corollary provides a theoretical basis for the practical rules by which Latin squares of a given order were classified and tabulated by Fisher and Yates \([4]\) and which were followed in the later publica-

---

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Presented to the Society, April 19, 1962 under the title "Net motions and quasigroups; received by the editors February 7, 1962."
tions in this field. The procedure started with the determination of isotopy classes. Then for every isotopy class of Latin squares, i.e., Cayley tables of quasigroups, the \( \leq 6 \) parastrophic isotopy classes were determined. For instance, in the case of quasigroups of order 6, there are 22 distinct isotopy classes, which appear in 5 parastrophic triples, and 7 self-parastrophic isotopy classes. Parastrophic sextuples of isotopy classes were found for quasigroups of order 7.

2. If the quasigroup is a loop, i.e., has a two-sided unit element, a related concept has been introduced. In a loop \((Q, \cdot)\) let the permutations \(L(x)\) and \(R(y)\) be defined by \(xR(y) = yL(x) = xy\), and \(xJ\) and \(xJ^{-1}\) by \(x \cdot xJ = xJ^{-1} \cdot x = 1\), the unit element, for all \(x\) and \(y\) in \(Q\). Now define \(x(\sigma)y = yR^{-1}(xJ)\). With the operation \((\sigma)\), \(Q\) is again a loop, \((Q, \sigma)\). It is shown in [2] and can be easily ascertained directly that \(x(\sigma^{-1})y = xL^{-1}(yJ^{-1})\) and that \((Q, \sigma^{-1})\) is a loop. These loops have been studied for loop-theoretic reasons [1], as well as for considerations in geometry [2]. The mapping that takes \((Q, \cdot)\) into \((Q, \sigma)\) will be called \(\sigma\). The mapping \(\tau\), as defined above, preserves the unit element, hence maps loops on loops. Every product of a finite number of \(\sigma, \sigma^{-1}\) and \(\tau\) is called an isostrophism. The isostrophisms form a group, \(R\), which by [1] is the infinite dihedral group or one of its homomorphs.

An isostrophism mapping a loop onto another loop is called a loop-isotopism. The product of a finite number of loop-isotopisms and isostrophisms will be called a motion. The use of quasigroups, and in particular of Theorem 1, provides us with a simple proof of the following theorem, proved in [2] in a purely loop-theoretic way.

**Theorem 2.1.** If a loop-isotopism is transformed by a motion, the result is a loop-isotopism.

**Proof.** If \(\kappa\) is a loop-isotopism, we have to prove that \(\sigma^{-1}\kappa \sigma, \sigma\kappa \sigma^{-1}\) and \(\tau \kappa \tau\) are loop-isotopisms. Theorem 1 yields at once \(\tau \kappa \tau \in T\).

Since both \(\tau\) and \(\kappa\) preserve the loop property, \(\tau \kappa \tau\) is a loop-isotopism.

Now, \(x(\sigma)y = yR^{-1}(xJ)\) can be represented as a product of two mappings, namely, the parastrophism \(\rho: (x, y, z) \rightarrow (y, z, x)\), post-multiplied by the isotopism \(\iota = [J^{-1}, I, I]\). Indeed, the first step yields \(w(\rho)(vw) = v\), and with \(vw = y\), \(w(\rho)y = yR^{-1}(w)\). Then \((wJ^{-1})(\rho J)y = yR^{-1}(w)\), or, with \(wJ^{-1} = x\), \(x(\rho J)y = yR^{-1}(xJ) = x(\sigma)y\). Thus, if \(\kappa = [\alpha, \beta, \gamma]\),

\[
\sigma^{-1}\kappa \sigma = (\rho [J^{-1}, I, I])^{-1} [\alpha, \beta, \gamma] \rho [J^{-1}, I, I] \\
= [J^{-1}, I, I]^{-1} [\alpha, \beta, \gamma] \rho [J^{-1}, I, I] \\
= [J, I, I] [\beta, \gamma, \alpha] [J^{-1}, I, I] = [J\beta J^{-1}, \gamma, \alpha] \in T.
\]
This is a loop-isotopism because $\kappa$ is a loop-isotopism and because $\sigma$ and $\sigma^{-1}$ carry loops into loops. Similarly,

$$\sigma \kappa \sigma^{-1} = \rho[J^{-1}, I, I][\alpha, \beta, \gamma][J, I, I]\rho^{-1} = \rho[J^{-1}\alpha J, \beta, \gamma]\rho^{-1} = [\gamma, J^{-1}\alpha J, \beta],$$

a loop-isotopism. This completes the proof.

The following theorem clarifies the relation between isostrophy and parastrophy.

**Theorem 2.2.** Two isotopy classes $\mathcal{C}_1$ and $\mathcal{C}_2$ of quasigroups are parastrophic if and only if there exist two loops $Q_1 \in \mathcal{C}_1$ and $Q_2 \in \mathcal{C}_2$ which are isostrophic.

**Proof.** Every isostrophism can be written in the form $\sigma^n \tau^e$, $n$ an integer, $e = 0$ or 1 [1]. Let $Q_1 \in \mathcal{C}_1$ and $Q_2 \in \mathcal{C}_2$ be loops, and $Q_2 = Q_1 \sigma^n \tau^e = Q_1 (\rho[J^{-1}, I, I])^n \tau^e$. Theorem 1 implies that for every isomorphism $\kappa$, $\rho \kappa = \lambda \rho$, $\lambda$ also an isomorphism. Thus the $\rho$'s can be shifted successively to the right to yield $Q_2 = Q_1 \mu \rho \tau^s$, $\mu$ an isomorphism. Hence $Q_2$ is parastrophic to $Q_1 \mu$, that is, $\mathcal{C}_2$ parastrophic to $\mathcal{C}_1$. Conversely, let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two parastrophic isotopy classes of quasigroups. Each isotopy class is well known [3] to contain at least one loop. If $\mathcal{C}_2 = \mathcal{C}_1 \rho$, and $Q_1 \in \mathcal{C}_1$ and $Q_3 \in \mathcal{C}_2$ are loops, then there is an isomorphism $\kappa$ such that $Q_3 \kappa = Q_1 \rho = Q_1 \sigma [J, I, I]$, $Q_1 \sigma = Q_3 \kappa [J^{-1}, I, I]$, that is, the loop $Q_2 = Q_3 \kappa [J^{-1}, I, I] \in \mathcal{C}_2$ is isostrophic to $Q_1 \in \mathcal{C}_1$. If $\mathcal{C}_2 = \mathcal{C}_1 \rho^2$, then $\mathcal{C}_2 = \mathcal{C}_1$, and the argument can be repeated. If $\mathcal{C}_2 = \mathcal{C}_1 \rho \tau$, we have $Q_3 \kappa = Q_1 \sigma [J, I, I] \tau = Q_1 \sigma \tau [J, I, I]$ and $Q_1 \sigma \tau = Q_3 \kappa [J, J^{-1}, I] = Q_2$, a loop $\in \mathcal{C}_2$. If $\mathcal{C}_2 = \mathcal{C}_1 \sigma \tau$, then $Q_3 \kappa = Q_1 \sigma \tau [J, I, I]$, and $Q_2 \sigma = Q_3 \kappa [J^{-1}, I, I] = Q_2$, a loop $\in \mathcal{C}_2$. The cases $\mathcal{C}_1 \tau = \mathcal{C}_2$ and $\mathcal{C}_1 = \mathcal{C}_2$ are trivial.

**References**


Rutgers, The State University