Division, loops and principal isotopy

Local units. Let a be an element of a quasigroup Q. By the definition of quasigroups there exists exactly one $b \in Q$ such that $L_a(b) = a$. Denote this b by f_a. The equality $L_a(b) = a$ may be written as $a = af_a$. The element f_a is call the *right local unit* of a.

Similarly define the *left local unit* e_a such that $e_a a = a$.

Associative triples. Let Q be a quasigroup. A triple $(x, y, z) \in Q^3$ is said to be *associative* if $xy \cdot z = x \cdot yz$.

Claim. The triple (e_a, a, f_a) is associative.

Proof. $e_a a \cdot f_a = af_a = a = e_a a = e_a \cdot af_a$.

Corollary. A quasigroup of finite order n contains at least n associative triples.

Definitions. A quasigroup Q is said to be *idempotent* if $xx = x$ for every $x \in Q$. The quasigroup Q is said to be *maximally nonassociative* if

$$\forall x, y, z \in Q\colon\ xy \cdot z = x \cdot yz \ \Leftrightarrow\ x = y = z.$$

Exercise. Show that a maximally nonassociative quasigroup has to be idempotent. Show that a quasigroup of finite order n contains exactly n associative triples if and only if it is maximally nonassociative.

Existence of maximally nonassociative quasigroups. There are no maximally nonassociative quasigroups of orders $2, 3, 4, 5, 6, 7, 8, 10$. Maximally nonassociative quasigroups of other orders n are known to exist for $n = 9$, $n = 13$ and for all $n \geq 16$ such that $n \notin \{40, 42, 44, 56, 66, 77, 88, 90, 110\}$ if n is not of the form $2p$, p a prime, or $2p_1p_2$, $p_1 \leq p_2 < 2p_1$.

Challenge. Find a maximally nonassociative quasigroup of order $2p$, p a prime.

Global units. An element $e \in Q$ is a called a *left unit* if $e_a = e$ for all $a \in Q$. Similarly define the *right unit*. There is at most one left unit and at most one right unit. If there exist both of them, then they coincide since $e = ef = f$. An element $e \in Q$ is the left unit if and only if $L_e = \mathrm{id}_Q$. The right unit f is characterized by $R_f = \mathrm{id}_Q$. A both sided unit is also called the *neutral element*.

Loops and reduced latin squares. A quasigroup is called a *loop* if and only if it possesses a neutral element. Suppose that Q is a loop with unit equal to 1. If $a, b \in Q$ are such that $ab = b$, then $a = 1$. This means that if $a \neq 1$, then L_a fixes no point of Q. Similarly, if $a \neq 1$, then R_a is a fixed point free permutation.

Let Q be a loop on $\{1, 2, \dots, n\}$ with 1 the unit. The body of the multiplication table contains $1, 2, \dots, n$ in the first row (from the left to the right) and $1, 2, \dots, n$ in the first column (from the top to the bottom). This is exactly the condition when a latin square is called *reduced*.

Equational definition of quasigroups. Another way of saying that L_a is permutation is to say that for any $b \in Q$ there exists exactly one $x \in Q$ such that $ax = b$. This approach is used in another definition of a quasigroup which goes by saying that for any $a, b \in Q$ the equations

$$ax = b \text{ and } ya = b \text{ have unique solutions } x \text{ and } y.$$

How to express these x and y? We have $L_a(x) = b$ and $R_a(y) = b$. Thus $x = L_a^{-1}(b)$ and $y = R_a^{-1}(b)$. By convention, set

$$L_a^{-1}(b) = a\backslash b \qquad \text{(the left division), and}$$
$$R_a^{-1}(b) = b/a \qquad \text{(the right division).}$$

What are the properties of the divisons when seen as binary operations? Since $L_x L_x^{-1}(y) = y = L_x^{-1} L_x(y)$ and $R_x R_x^{-1}(y) = y = R_x^{-1} R_x(y)$ we get equations

$$x(x\backslash y) = y = x\backslash(xy) \text{ and } (y/x)x = y = (yx)/x. \tag{D}$$

Claim. If $(Q, \cdot, \backslash, /)$ fulfils (D), then $(Q, \cdot)$ is a quasigroup.
Proof. To show that $ax = b$ possesses a unique solution note first that $a(a\backslash b) = b$, and then observe that $ax_1 = ax_2$ implies $x_1 = a\backslash(ax_1) = a\backslash(ax_2) = x_2$.

We can thus regard (D) as an alternative definition of a quasigroup. This is a definition in the sense of universal algebra. A *quasigroup* is an algebra $(Q, \cdot, \backslash, /)$ where all operations are binary and the identities of (D) are satisfied.

This definition is usually called *equational.* The original definition may be called *combinatorial.* The equational definition of loop involves a nullary operation 1, and the laws $x \cdot 1 = x = 1 \cdot x$.
Claim. If Q is a quasigroup and $x, y \in Q$, then $x/(y\backslash x) = y = (x/y)\backslash x$. If Q is a loop, then $x/1 = x = 1\backslash x$.
Proof. Indeed, $y = (y(y\backslash x))/(y\backslash x) = x/(y\backslash x)$ and $y = (x/y)\backslash((x/y)y) = (x/y)\backslash y$. If 1 is the unit, then $x = (x \cdot 1)/1 = x/1$ and $x = 1\backslash(1 \cdot x) = 1\backslash x$.

Subquasigroups and congruences. Passing between combinatorial and equational definition is usually done informally. However, it is worth remembering that the equational definition exhibits in a clear fashion that *subquasigroups* have to be closed under divisions and *congruences of quasigroups* have to be compatible with divisions.

Exercises. (1) If Q is a finite quasigroup, then a subset closed under multiplication is a subquasigroup and an equivalence compatible with $\cdot$ is a congruence of the quasigroup.
(2) Let Q be a quasigroup. Show that an equivalence $\sim$ on Q is a congruence if and only if for all $x, y, z \in Q$

$$x \sim y \;\Rightarrow\; xz \sim yz,\; zx \sim zy,\; x/z \sim y/z \text{ and } z\backslash x \sim z\backslash y.$$

Quasigroup words and reduction. Let X be a set of symbols. Denote by $W(X)$ the absolutely free algebra over X in signature $(\cdot, \backslash, /)$. The elements of $W(X)$ are called *quasigroup words.* A quasigroup word is called *reduced* if it contains no subword (subterm) of one of the forms

$$(st)/t,\; (s/t)t,\; t(t\backslash s),\; t\backslash(ts),\; t/(s\backslash t) \text{ and } (t/s)\backslash t. \tag{R}$$

For $u, v \in W(X)$ write $u \to v$ if u contains a subterm that has a form that occurs in (R), and if v arises from u by replacing this term by s. The transitive closure of $\to$ is denoted by $\to^*$. A word is thus reduced if and only if it is terminal with respect to $\to^*$.

The reduction decreases the size of the term. Hence for each $u \in W(X)$ there exists a reduced $v \in W(X)$ such that $u \to^* v$. The following fact appears in various contexts. Our proof will be hence brief.

Lemma. *Let $u, w_1, w_2 \in W(X)$ be such that $u \to^* w_1$ and $u \to^* w_2$. If both w_1 and w_2 are reduced, then $w_1 = w_2$.*

Proof. Let u be the smallest counterexample. To get a contradiction it suffices to show that if $u \to u_1$ and $u \to u_2$, then there exists u_3 such that $u_1 \to^* u_3$ and $u_2 \to^* u_3$. Indeed, if $u_i \to^* w_i$, $i \in \{1, 2, 3\}$, then $w_1 = w_3 = w_2$ since both u_1 and u_2 are smaller (with respect to the length of the quasigroup word) then u.

Let u_i be obtained from u by replacing a subterm v_i by s_i, where v_i takes the form $(s_i t_i)/t_i$, $(s_i/t_i)t_i$, etc., as listed in (R), $i \in \{1, 2\}$. The situation is easy to solve if v_2 is a subterm of an occurence of t_1. In that case make $v_2 \to s_2$ in both occurence of t_1 and then replace the changed subterm by s_1. This means that $u_2 \to^* u_1$. If v_2 is a subterm of s_1, then define u_3 by making the replacement $v_2 \to s_2$ within the occurence of s_1 in u_2. Both $u_1 \to^* u_3$ and $u_2 \to^* u_3$ are then true.

If there exists a subterm a_1a_2 of u such that v_1 is a subterm of a_1 and v_2 a subterm of a_2, then the reductions commute and the existence of u_3 is obvious.

What remains are situations that are usually called *critical*. These are the situations when one of the terms has a root within the other term. Suppose that v_2 sits within v_1. We shall consider only the case when $v_1 = (s_1t_1)/t_1$. The other cases are similar. The only nontrivial possibility in (R) with / at the top is $t_2/(s_2\backslash t_2)$. However $t_2 = s_1t_1$ and $t_1 = s_2\backslash s_2$ is impossible. Therefore there must be $v_2 = s_1t_1$. If $s_1t_1 = (s_2/t_2)t_2$, then $t_1 = t_2$ and both replacements change v_1 to $s_1 = s_2/t_1$. Thus $u_1 = u_2$ and nothing has to be constructed.

If $s_1t_1 = t_2(t_2\backslash s_2)$, then $s_1 = t_2$ and $t_1 = t_2\backslash s_2$. Thus

$$v_1 \to s_1 = t_2 \text{ and } v_1 = v_2/t_1 \to s_2/t_1 = s_2/(t_2\backslash s_2) \to t_2.$$

The latter replacement shows that $u_2 \to u_1$. □

Denote by $\equiv$ the least congruence of $W(X)$ such that $W(X)/\equiv$ is a quasigroup. This is a free quasigroup with basis $\{[x]_\equiv;\, x \in X\}$. Denote by $F(X)$ the subset of $W(X)$ that is formed by all reduced words. By the Lemma for each $w \in W(X)$ there exists a unique reduced word $\rho(w)$ such that $w \to^* \rho(w)$. If $u \to v$, then $\rho(u) = \rho(v)$. From that it follows that $u \equiv v$ if and only if $\rho(u) = \rho(v)$. Hence defining operations by

$$u \cdot v = \rho(uv),\ u/v = \rho(u/v) \text{ and } u\backslash v = \rho(u\backslash v)$$

makes $F(X)$ a **free quasigroup** with basis X.

To get a **free loop** consider loop words in $\cdot$, $\backslash$, $/$ and 1, and add reduction rules that change each of $s/1$, $s \cdot 1$, $1 \cdot s$ and $1\backslash s$ to s.

Loops from quasigroups. Let Q be a quasigroup, and let e and f be elements of Q. Set $x * y = x/f \cdot e\backslash y$, for all $x, y \in Q$. Translations of $(Q, \cdot)$ are denoted by L_x and R_x, while translations of $(Q, *)$ will be denoted by λ_x and ρ_x, $x \in Q$. Clearly,

$$\lambda_x = L_{x/f}L_e^{-1} \text{ and } \rho_y = R_{e\backslash y}R_f^{-1},$$

for each $x, y \in Q$. Note that $x * (ef) = x/f \cdot f = x$ and $(ef) * y = e \cdot e\backslash y = y$. This means that $(Q, *)$ *is a loop, and* ef *is the neutral element of this loop.*

Principal isotopes. An isotopy of quasigroups $(\alpha, \beta, \gamma)\colon Q_1 \to Q_2$ is called *principal* if the underlying sets of Q_1 and Q_2 coincide and $\gamma = \mathrm{id}_{Q_1}$. Call Q_2 a *principal isotope* of Q_1 if there exists a principal isotopy $Q_1 \to Q_2$.

Let $(Q, *)$ be a principal isotope of $(Q, \cdot)$. There thus exist $\alpha, \beta \in \mathrm{Sym}(Q)$ such that $x * y = \alpha(x)\beta(y)$. The translations of $(Q, \cdot)$ are denoted by L_x and R_x, and those of $(Q, *)$ by λ_x and ρ_x, $x \in Q$. Clearly,

$$\lambda_x = L_{\alpha(x)}\beta \text{ and } \rho_y = R_{\beta(y)}\alpha,$$

for each $x, y \in Q$. If $(Q, *)$ is a loop, then there must exist $x \in Q$ such that $\lambda_x = \rho_x = \mathrm{id}_Q$. If this true, then there exist $e, f \in Q$ such that $\beta = L_e^{-1}$ and $\alpha = R_f^{-1}$. If such e, f exist, then $x * y = \alpha(x)\beta(y) = x/f \cdot e\backslash y$. This is a loop, as observed above. We have proved the following statement:

Proposition 1. *Let $(Q, \cdot)$ be a quasigroup. A principal isotope $(Q, *)$ of $(Q, \cdot)$ is a loop if and only if there exist $e, f \in Q$ such that $x * y = x/f \cdot e\backslash y$ for all $x, y \in Q$.*

Quasigroups induced by isomorphism and isotopy. Suppose that Q is a quasigroup and S a set. Suppose also that there exists a bijection $\gamma\colon Q \to S$. Then there is only one way how to define a quasigroup operation upon S, and that is by $st = \gamma(\gamma^{-1}(s)\gamma^{-1}(t))$ for all $s, t \in Q$. The quasigroup $(S, \cdot)$ is called *isomorphically induced* by γ.

Similarly, if α, β, γ are bijections $Q \to S$, then $st = \gamma(\alpha^{-1}(s)\beta^{-1}(t))$ yields the only quasigroup upon S for which (α, β, γ) is an isotopy $(Q, \cdot) \to (S, \cdot)$. This is the quasigroup *isotopically induced* by (α, β, γ).

Loops isotopic to a quasigroup. Suppose that (α, β, γ) is an isotopy of quasigroups $Q_1 \to Q_2$. Let $(Q_1, *)$ be the quasigroup isomorphically induced by the bijection $\gamma^{-1}\colon Q_2 \to Q_1$. Isotopies may be composed. Hence

$$(\gamma^{-1}, \gamma^{-1}, \gamma^{-1})(\alpha, \beta, \gamma) = (\gamma^{-1}\alpha, \gamma^{-1}\beta, \mathrm{id}_{Q_1})$$

is a principal isotopy $(Q_1, \cdot) \to (Q_1, *)$, while $(Q_1, *) \cong (Q_2, \cdot)$. This gives immediately:

Proposition 2. *Each quasigroup isotopic to a quasigroup Q is isomorphic to a principal isotope of Q.*

Proposition 3. *Let $(Q, \cdot, \backslash, /)$ be a quasigroup. For each loop L isotopic to Q there exist $e, f \in Q$ such that L is isomorphic to a loop on Q with multiplication $x * y = x/f \cdot e\backslash y$, for all $x, y \in Q$.*

Proof. By the preceding statement every loop isotopic to Q is isomorphic to a principal isotope of Q. By Proposition 1, a principal isotope that is a loop has to be of the form $x/f \cdot e\backslash y$. $\square$

Exercise. Prove directly that each loop isotopic to a group G is isomorphic to G.

Notational remark: If H is a subgroup of a group G, then it is usual to write $H = 1$ if H is the trivial subgroup, that is if $|H| = 1$. Thus, if G is a permutation group on Ω, $H = 1$ means that $H = \{\mathrm{id}_\Omega\}$.

Regular groups. A permutation group on Ω is, by definition, every subgroup of $\mathrm{Sym}(\Omega)$. A permutation group $H \le \mathrm{Sym}(\Omega)$ is *transitive* if for all $\alpha, \beta \in \Omega$ there exists $h \in H$ such that $h(\alpha) = \beta$. Note that it suffices if the former holds for a single $\alpha \in \Omega$. In a transitive group all stabilizers $H_\alpha = \{h \in H;\ h(\alpha) = \alpha\}$ are conjugate one to another. Hence if $H_\alpha = 1$ for one $\alpha \in \Omega$, then $H_\alpha = 1$ for all $\alpha \in \Omega$.

The permutation group $H \le \mathrm{Sym}(\Omega)$ is called *regular* if it is transitive, and if $H_\alpha = 1$, for any $\alpha \in \Omega$. Note that the latter condition may also be expressed as $h = \mathrm{id}_\Omega$ whenever $h \in H$ fixes a point.

Let G be a group. Then $\{L_x;\ x \in G\}$ is a regular permutation group on G. It is called the *left regular representation of* G.

Each regular permutation group may be interpreted as a left regular representation of an abstract group. To see this consider a regular group G upon Ω. Fix a point $\omega \in \Omega$ and identify it with the unit element 1 of an abstract group $(\Omega, \cdot)$ that will be now described. For each $\alpha \in \Omega$ denote by ψ_α the element of G that sends $1 = \omega$ upon α. Since G is regular, the permutation ψ_α is determined by α uniquely. Furthermore, $G = \{\psi_\alpha;\ \alpha \in \Omega\}$. Define a binary operation $\cdot$ on Ω by $\alpha{\cdot}\beta = \psi_\alpha(\beta)$, and define $\Psi\colon G \to \Omega$ by $\Psi(\psi_\alpha) = \alpha$. Since $\psi_\alpha\psi_\beta(\omega) = \psi_\alpha(\beta) = \alpha{\cdot}\beta$, we have $\psi_\alpha\psi_\beta = \psi_{\alpha\cdot\beta}$. Therefore $\Psi(gh) = \Psi(g) \cdot \Psi(h)$ for all $g, h \in G$. Thus $\Psi\colon (G, \circ) \cong (\Omega, \cdot)$, and for each $\alpha \in \Omega$ the mapping ψ_α coincides with the left translation of α in $(\Omega, \cdot)$.

Note that denoting the neutral element by 1 is a matter of convention. If G is abelian, then it may be more natural to denote the neutral element by 0 and the binary operation by $+$.

Loops with translations closed under composition. A loop Q is said to have left translations *closed under composition* if

$$\forall x, y \in Q \ \exists z \in Q \text{ such that } L_x L_y = L_z.$$

If this is true, then $xy = L_x L_y(1) = L_z(1) = z$, implying $L_x L_y = L_{xy}$ for all $x, y \in Q$. But that is equivalent to associativity since $L_x L_y(v) = x \cdot yv$ and $L_{xy}(v) = xy \cdot v$. This proves that *a loop with left translations closed under composition has to be a group.*

Albert's Theorem. *A loop isotopic to a group G is isomorphic to G.*

Proof. By Proposition 3 only the principal isotopes $x/f \cdot e\backslash y$ may be considered. The set of the left translations of such an isotope is equal to

$$\{L_{x/f} L_e^{-1};\ x \in G\} = \{L_x L_e^{-1};\ x \in G\} = \{L_{xe^{-1}};\ x \in G\} = \{L_x;\ x \in G\}.$$

The set of left translations of the principal isotope thus coincides with that of G. The left translations are closed under composition. The principal isotope thus must be a group. The both groups are isomorphic since they have coinciding left regular representations. $\square$