ON THE FOUNDATIONS OF QUASIGROUPS

BY

SHERMAN K. STEIN[1]

1. **Introduction.** Quasigroups have two fundamental properties which groups in general lack. First, a quasigroup may be homogeneous in the sense that its group of automorphisms may be transitive. The only group with this property has just one element. Second, a quasigroup has a rich outer symmetry (or duality) in the sense that to each quasigroup are associated six conjugate quasigroups (defined in §3), one for each element of the symmetric group on three letters. In general, only the transpose of a group is again a group.

Any constraint satisfied by a quasigroup yields a conjugate constraint satisfied by a conjugate quasigroup. The theory of conjugate constraints and conjugate quasigroups is developed and illustrated in §§2–8. Of special interest are constraints which are invariant, that is, constraints which are equivalent to their six conjugates. The constraints of associativity and commutativity are not invariant. In fact, as is pointed out in §5, one of the conjugates of associativity is the identity $ab \cdot ac = bc$. Thus, the theory of groups is equivalent to the theory of quasigroups satisfying the identity $ab \cdot ac = bc$. Considered from this point of view, the theory of groups may seem artificial. In any case, the existence of the tremendous theory of groups suggests that quasigroups satisfying other constraints than associativity and commutativity might merit consideration.

For example, the constraint of mediality $ab \cdot cd = ac \cdot bd$, implied by the conjunction of associativity and commutativity, is invariant and has been investigated. It shall be considered in detail in §§11–14. The constraint of left-distributivity $a \cdot bc = ab \cdot ac$, which is intertwined with mediality, has received less attention. It shall be treated in §§9, 10. The only left-distributive group is the trivial group. This serves to illustrate another of the attractions of quasigroups—they may satisfy identities which usually conflict with associativity. Also, in groups it is usually obvious whether a constraint is or is not satisfied; therefore, a theory of constraints has not been developed for groups.

In §§15, 16 the relation of orthogonality to an algebra is studied. In particular, a new technique for constructing orthogonal quasigroups is presented which may produce a counterexample to Euler's conjecture. Conjugates of

Received by the editors June 26, 1956.

[1] Part of the work on this paper was done while the author held a Summer Faculty Fellowship from the University of California. The translation of portions of Mituhisa [25], by Makoto Yaguchi, was sponsored by the Department of Mathematics at the University of California at Davis.

various constraints are listed in §§17, 18. In §19 conjugation is applied to varieties.

Historical remarks, comments, and suggestions for future work are collected in §§20, 21 under the title of Commentary.

I. Conjugation

2. **Algebras.** Let X be a set and $n \geqq 1$ be an integer. An algebra on X is a function $f: X^n \to X$ which is defined for all elements of X^n and is single-valued. In X^{n+1}, f defines a subset G which shall be called the graph of f:

$$G = \{(x_1, \cdots, x_n, f(x_1, \cdots, x_n)) \mid x_i \in X\}.$$

If $\pi_i: X^p \to X$ denotes projection parallel to the ith axis of X^p then a subset $H \subset X^{n+1}$ is the graph of an algebra if and only if

$$\pi_{n+1} \mid H: H \to X^n$$

is an equivalence (i.e., a one-one onto function).

Let S_k denote the symmetric group on the first k integers. Each $\sigma \in S_k$ induces an equivalence on X^k, again denoted σ, defined by

$$\sigma((x_1, \cdots, x_k)) = (x_{\sigma(1)}, \cdots, x_{\sigma(k)}).$$

If G is the graph of an algebra f and $\sigma \in S_{n+1}$ with $\sigma(n+1) = n+1$ then σG is also the graph of an algebra which shall be denoted σf. For example, if $n = 2$ and $\sigma = (12)$ then f is a binary algebra and σf is its transpose.

3. **Polyadic algebra.**

Definition 3.1. If the graph G of f satisfies the more stringent demand

$$\pi_i \mid G: G \to X^n \qquad 1 \leq i \leq n+1$$

are equivalence, f (or G) is a polyadic algebra.

For example, if $n = 1$, $f: X \to X$ is an equivalence. For $n = 2$, $f: X^2 \to X$ is a quasigroup. Explicitly, the fact that π_1 is an equivalence asserts the existence and uniqueness of the solution to the equation $xa = b$; the same property of π_2 implies the same for the equation $ax = b$ (the notation xy is the standard abbreviation for $f(x, y)$).

Definition 3.2. For each $\sigma \in S_{n+1}$ and polyadic algebra $G \subset X^{n+1}$, σG is a polyadic algebra and shall be called a conjugate of G (or of f) and may also be denoted σf.

The notion of conjugacy clearly includes that of transposition. There may be $n+1!$ nonisomorphic algebras conjugate to an n-ary algebra.

4. **Conjugate quasigroups.** The case $n = 2$ of polyadic algebras shall be the only one considered in what follows. If $f(a, b) = c$ then $(a, b, c) \in G$. If $\sigma \in S_3$, $\sigma(a, b, c) \in \sigma G$. For example, if $\sigma = (13)$ then $(c, b, a) \in \sigma G$. This fact may be written $(\sigma f)(c, b) = a$ or, with an ambiguity that shall be removed by the context, simply $cb = a$. The following table records the six quasigroup conjugate to a given quasigroup f.

(4.1)

σ	I	(12)	(13)	(23)	(123)	(132)
equation	$f(a, b)=c$	$(\sigma f)(b, a)=c$	$\sigma f(c, b)=a$	$\sigma f(a, c)=b$	$\sigma f(b, c)=a$	$\sigma f(c, a)=b$
abbreviation	$ab=c$	$ba=c$	$cb=a$	$ac=b$	$bc=a$	$ca=b$

DEFINITION 4.2. An associative quasigroup is a group. A quasigroup with a two-sided unit is a loop. A quasigroup in which the square of each element is itself is an idempotent quasigroup.

THEOREM 4.3. *The quasigroups conjugate to a group f may be defined in terms of f and the inverse operation in f as follows*:

(4.4)

σ	I	(12)	(13)	(23)	(123)	(132)
$\sigma f(a, b)$	$f(a, b)$	$f(b, a)$	$f(a, b^{-1})$	$f(a^{-1}, b)$	$f(b^{-1}, a)$	$f(b, a^{-1})$
abbreviation	ab	ba	ab^{-1}	$a^{-1}b$	$b^{-1}a$	ba^{-1}

where the last row refers to the law f.

Proof. Consider the case $\sigma=(132)$. Let $(\sigma f)(a, b)=c$. Then $(a, b, c)\in\sigma G$, where G is the graph of f. Solve the equation $(a, b, c)=\sigma(x, y, z)$ for x, y, z. That is, $(a, b, c)=(y, z, x)$. Thus, $y=a, z=b, x=c$. Hence, $(c, a, b)\in G$; equivalently, $b=ca$, or $c=ba^{-1}$. The five remaining cases are similar.

It should be observed that in general a conjugate of a group (loop) is not a group (loop), except for the cases $\sigma=I$, the group (loop) itself, and $\sigma=(12)$, its transpose, (and also a special case considered in §7).

5. Conjugate constraints.

DEFINITION 5.1. A constraint on f is a collection of assertions of the type; if $t_1, \cdots, t_k\in G$ then $t\in G$, where t depends on $t_1, \cdots, t_k$.

For example, the identity $a\cdot bc=ab\cdot c$ on f may be translated into the constraint:

$$(b, c, x), (a, x, y), (a, b, u)\in G \text{ imply } (u, c, y)\in G.$$

DEFINITION 5.2. A constraint on f induces an equivalent constraint on σf by the demand:

$$\text{if } \sigma t_1 \cdots, \sigma t_k \in \sigma G \quad \text{then} \quad \sigma t \in \sigma G,$$

where σt depends on $\sigma t_1, \cdots, \sigma t_k$. Such an equivalent constraint is a conjugate constraint.

For example, if $\sigma=(23)$ the constraint of associativity for f becomes for σf the constraint:

$$(b, x, c), (a, y, x), (a, u, b)\in\sigma G \text{ imply } (u, y, c)\in\sigma G.$$

This may be written in the functional notation of the algebra σf as

$$c = bx,\ x = ay,\ b = au \text{ imply } uy = c.$$

Or equivalently $c=au\cdot ay$ implies $c=uy$. This is simply the identity

$$au\cdot ay = uy. \tag{5.3}$$

Thus, the identity 5.3 is a conjugate of the identity of associativity; it of course can be written $ab\cdot ac=bc$.

THEOREM 5.4. *The conjugates of the constraint of associativity are the identities of the following table*:

(5.5)

σ	I	(12)	(13)	(23)	(123)	(132)
identity	$a\cdot bc=ab\cdot c$	$a\cdot bc=ab\cdot c$	$ba\cdot ca=bc$	$ab\cdot ac=bc$	$ba\cdot ca=bc$	$ab\cdot ac=bc$

Proof. The case $\sigma=(23)$ is discussed above. The remaining cases are similar.

COROLLARY 5.6. *The theory of groups is equivalent to the theory of quasigroups satisfying the identity* $ab\cdot ac=bc$.

As will be shown in §18 the conjugate of an identity, while it is of course a constraint, is not necessarily expressible as an identity.

6. **Symbolic logic of constraints.** An examination of the details involved in determining the constraints conjugate to associativity in the previous section shows that all the computations could be carried out in a completely formal manner, independently of the existence of algebras or quasigroups. The computations involve only certain properties of the sign "$=$", functions, and substitutions. It is the object of this section to define "constraint" and "conjugate of a constraint" formally and also more precisely than in the preceding section.

Let $\mathfrak{F}$ be an elementary functional calculus with no individual constants, individual variables $a, b, c, \cdots, x, y, z, \cdots$, one function symbol of degree 2, written "$\cdot$", and one relation symbol of degree 2, "$=$". The other symbols of $\mathfrak{F}$ are $\supset$, F, [,], (,), Λ standing respectively for "implies", "false", "left and right bracket", "left and right parentheses", and "all".

DEFINITION 6.1. A string is a finite sequence of symbols from the above list.

DEFINITION 6.2. A string α is a term if there is a sequence $\alpha_1, \cdots, \alpha_n=\alpha$ such that for all i, $1\leqq i\leqq n$, either

(1) α_i is an individual variable or (2) α_i is $(\alpha_j\cdot\alpha_k)$, with $j, k<i$.

The following lemma is usually tacitly assumed when interpreting a term in a model for $\mathfrak{F}$.

LEMMA 6.3. *If* A, B, A', B' *are terms and* $(A\cdot B)$ *is* $(A'\cdot B')$ *then* A *is* A' *and* B *is* B'.

Proof. It suffices to show that A is A'. By symmetry it can be assumed that A is an initial section of A'. However, the number of left parentheses

of a proper initial section of any term exceeds the number of right parentheses of this section by at least one. Thus, A must coincide with A'.

DEFINITION 6.4. A string A is a well-formed formula if there is a sequence $A_1, \cdots, A_n(=A)$ such that for all i, $1 \leqq i \leqq n$, either (1) A_i is F, (2) A_i is $\alpha=\beta$ where α, β are terms, (3) A_i is $[A_j \supset A_k]$, $j, k<i$ or (4) A_i is $(\wedge b)A_j$, $j<i$ where b is an individual variable.

Within the well-formed formulas are singled out certain ones, called theorems, by specifying axioms and the notion of proof. The axioms, for example, would assert that "$=$" is an equivalence relation and "$\cdot$" a quasigroup. Moreover, the logical operations $\sim$ (not), $\wedge$ (and), $\vee$ (or), $\equiv$ (equivalent), can be defined in terms of the symbols already introduced; for example, $\sim A$ is an abbreviation for $[A \supset F]$.

DEFINITION 6.5. A constraint is a well-formed formula of $\mathfrak{F}$.

DEFINITION 6.6. A constraint of the form $\alpha=\beta$, where α and β are terms, is an identity.

Henceforth, the symbols "(', ')", and "$\cdot$", will be deleted if ambiguity does not arise; $(a \cdot b)$ shall be written ab.

DEFINITION 6.7. An atomic constraint is a constraint such that each expression contained in it of the form $\alpha=\beta$ involves at most one multiplication (that is, is of the form $ab=c$ or $a=b$).

As the method of the following examples shows, any constraint is equivalent to an atomic constraint.

EXAMPLE. An atomic constraint equivalent to the identity $ab=ba$ is $[ab=x \supset ba=x]$.

EXAMPLE. Atomic formulas equivalent to the identity $a \cdot bc=ab \cdot c$ are

$$[(bc = x) \wedge (ax = y) \wedge (ab = z) \wedge (zc = w) \supset (y = w)] \tag{6.8}$$

and also

$$[(bc = x) \wedge (ax = y) \wedge (ab = z) \supset (zc = y)]. \tag{6.9}$$

DEFINITION 6.10. If $\sigma \in S_3$ and γ is a constraint then the conjugate constraint $\sigma\gamma$ is obtained by replacing γ by an equivalent atomic constraint and then replacing each expression of the type $x_1x_2=x_3$ by $x_{\sigma(1)}x_{\sigma(2)}=x_{\sigma(3)}$.

EXAMPLE. Let γ be $a \cdot bc=ab \cdot c$ and $\sigma=(23)$. An atomic form for γ is, say, (6.9). Therefore $\sigma\gamma$ is

$$[bx = c \wedge ay = x \wedge az = b \supset zy = c].$$

The logic of $\mathfrak{F}$ shows that this is equivalent to $ab \cdot ac=bc$.

DEFINITION 6.11. The subgroup of S_3 consisting of those σ such that $\sigma\gamma \equiv \gamma$ is the group belonging to γ. If the group of γ is S_3 then γ is invariant.

THEOREM 6.12. *If the constraint γ implies δ then $\sigma\gamma$ implies $\sigma\delta$.*

Proof. Application of σ to the steps of the proof that γ implies δ yields a proof that $\sigma\gamma$ implies $\sigma\delta$. (For example, see Corollary 11.8).

COROLLARY 6.13. *If the constraint γ implies the invariant constraint δ then $\sigma\gamma$ implies δ.*

COROLLARY 6.14. *If the invariant constraint γ implies the constraint δ then γ implies $\sigma\delta$.*

If f is an algebra on X and σ is a term with k distinct individual variables then σ induces a function $g: X^k \to X$, by interpreting "$\cdot$" as "f" and the individual variables in σ as running through X. That g is well-defined is a consequence of Lemma 6.3. Not only terms, but, in a similar manner, constraints can be interpreted in an algebra.

DEFINITION 6.15. The algebra f is a model for the constraint γ if the interpretation of γ in f is valid; f is also said to satisfy γ.

DEFINITION 6.16. If γ is a constraint, $J(\gamma)$ consists of the integers which are orders of quasigroup models of γ.

$J(\gamma)$ is clearly closed under multiplication if γ is an identity.

THEOREM 6.17. *If the quasigroup Q satisfies the constraint γ and $\sigma \in S_3$ then σQ satisfies the constraint $\sigma\gamma$.*

7. Illustrations of the technique of conjugate constraints. The following theorems are illustrations of the preceding observations on constraints.

THEOREM 7.1. *A quasigroup Q satisfies the identity $ab\cdot bc = ac$ if and only if it is a group which is a power of the group of order two.*

Proof. To show $ab\cdot c = a\cdot bc$ solve the equations $a = xy$, $b = yz$, $c = zt$. Then

$$ab\cdot c = (xy\cdot yz)zt = xz\cdot zt = xt,$$
$$a\cdot bc = xy(yz\cdot zt) = xy\cdot yt = xt.$$

Thus Q is a group. Let e be its unit element. Then $eb\cdot be = e^2$. Then $b^2 = e$ for all b, proving the theorem.

COROLLARY 7.2. $J(ab\cdot bc = ac) = \{2^i, i = 0, 1, 2, \cdots\}$.

COROLLARY 7.3. *If all the conjugates of a group G are groups, then G is a power of the group of order two (and conversely).*

Proof. Since $ae = a$, σG, for $\sigma = (23)$, satisfies the equation $a^2 = e$. Since σG is a group it must be a power of the group of order two, and hence satisfy $ab\cdot bc = ac$. This identity is invariant (see §17); by Theorem 7.1, G is itself a power of the group of order two. The converse follows from the invariance of $ab\cdot bc = ac$.

THEOREM 7.4. *A loop Q satisfies the identity $ab\cdot ac = db\cdot dc$ only if it is a group which is a power of the group of order two.*

Proof. Since d may equal e, which is a left unit, Q satisfies $ab\cdot ac = bc$,

which is conjugate by $\sigma=(23)$ to associativity. σQ is therefore a group. Also, since e is a right unit $xe=x$ in Q. Thus, $xx=e$ in σQ. Hence σQ is a power of the group of order two. Therefore, Q is also.

LEMMA 7.5 (Suschkewitsch [3]). *In a quasigroup Q the following two constraints are equivalent*:

$$B\colon ab\cdot c = a\cdot bd \text{ implies } a'b'\cdot c = a'\cdot b'd,$$

$$B'\colon ab = cd \text{ implies } a\cdot bx = c\cdot dx.$$

Proof. Assume Q satisfies B and let $ab=cd$. Then $a\cdot bx=c\cdot dy$ for some y. Also $a\cdot bx=ab\cdot z=cd\cdot z$. But the equations $ab\cdot z=a\cdot bx$, $cd\cdot z=c\cdot dy$, together with B, imply $y=x$, hence B'.

Assume Q satisfies B'. Choose e so $be=b$. For given a, b, d find c so $ab=cd$. By $B'a\cdot be=c\cdot de$. Thus e is a right unit. Now let $ab=q=qe$. By B'

$$a\cdot bc = q\cdot ec = ab\cdot ec.$$

Since ec is independent of a and b, B follows.

COROLLARY 7.6. *In a quasigroup the following two constraints are equivalent*:

$$A\colon ab = cd \text{ implies } xa\cdot xb = yc\cdot yd,$$

$$A'\colon ab\cdot ac = db\cdot dc.$$

Proof. For $\sigma=(23)$, $A'=\sigma B'$ (Table 18.1). Also, $A=\sigma B$. The corollary is a consequence of Lemma 7.5 and Theorem 6.12.

8. **Conjugates of commutativity.** A second well-known constraint is $ab=ba$. Straightforward computation yields the following table for the constraints conjugate to it.

(8.1)

σ	I	(12)	(13)	(23)	(123)	(132)
Constraint	$ab=ba$	$ab=ba$	$b\cdot ba=a$	$ab\cdot b=a$	$b\cdot ba=a$	$ab\cdot b=a$

DEFINITION 8.2. An algebra satisfying all the identities conjugate to commutativity is totally symmetric.

THEOREM 8.3. *A quasigroup f with graph G is totally symmetric if and only if $\sigma G=G$ (or $\sigma f=f$) for all $\sigma\in S_3$.*

Proof. The commutativity of f is equivalent to $\sigma G=G$, for $\sigma=(12)$. That f satisfies $ab\cdot b=a$ is equivalent to $\sigma G=G$, for $\sigma=(13)$. Since S_3 is generated by any two distinct transpositions the theorem is proved.

COROLLARY 8.4. *The quasigroup f is totally symmetric if and only if $ab=c$ implies $ba=c$ and $cb=a$.*

THEOREM 8.5. *There exist totally symmetric idempotent quasigroups only for orders $n\equiv 1, 3 \pmod 6$* [47].

THEOREM 8.6. *A totally symmetric algebra is a (totally symmetric) quasigroup.*

Proof. Since $ab \cdot b = a$, the equation $xb = a$ has at least one solution. Assume that $xb = yb$. Then $xb \cdot b = yb \cdot b$, which implies $x = y$. Similarly the constraint $b \cdot ba = a$ implies the equation $bx = a$ has precisely one solution.

COROLLARY 8.7. *An algebra f satisfying the constraints $ab \cdot b = a = b \cdot ba$ is a commutative quasigroup (hence totally symmetric quasigroup).*

Proof. In view of the preceding theorem and its proof it is sufficient to show that f is totally symmetric, and hence commutative. Since $\sigma f = f$ for $\sigma = (23)$ and $\sigma = (13)$ and any two transpositions generate S_3, f is totally symmetric.

II. DISTRIBUTIVITY

9. Self-distributivity.

DEFINITION 9.1. The algebra f is left- (right-) distributive if f satisfies $a \cdot bc = ab \cdot ac (bc \cdot a = ba \cdot ca)$.

The conjugates of left-distributivity are listed in the following table:

(9.2)

σ	I	(12)	(13)	(23)	(123)	(132)
Constraint	$a \cdot bc = ab \cdot ac$	$bc \cdot a = ba \cdot ca$	$ab = cd$ *implies* $ac \cdot bd = ab (= cd)$	$a \cdot bc = ab \cdot ac$	$bc \cdot a = ba \cdot ca$	$ab \cdot cd$ *implies* $ac \cdot bd = ab = cd$

Left-distributivity is an example of an identity possessing a conjugate constraint which is not an identity.

THEOREM 9.3. *A left-distributive quasigroup is idempotent.*

Proof. Set $a = b = c$. Then $a \cdot a^2 = a^2 \cdot a^2$. Cancellation implies $a = a^2$.

COROLLARY 9.4. *A quasigroup satisfying a constraint conjugate to left-distributivity is idempotent.*

Proof. Theorem 9.3 and Corollary 6.13.

THEOREM 9.5. *The center*(2) *of a left-distributive quasigroup Q is either void or all of Q.*

Proof. Let $b_0 c = c b_0$ for all $c \in Q$. Then, $a \cdot (b_0 c) = a \cdot (c b_0)$ or $ab_0 \cdot ac = ac \cdot ab_0$ for all a, $c \in Q$. Thus, ab_0 is in the center of Q for all a. Thus Q is abelian.

THEOREM 9.6. *An abelian left-distributive quasigroup Q satisfies all constraints conjugate to left-distributivity.*

Proof. That Q is right-distributive is clear. To show that $AB = CD$ implies

(2) The center of an algebra A is the set of elements which commute with all the elements of A.

$AC \cdot BD = AB$, solve the equations $x = A$, $xy = C$, $xz = D$ successively for x, y, z. Then, since $AB = CD$ and Q is left-distributive, $yz = B$. Then

$$AC \cdot BC = (x \cdot xy)(yz \cdot xz) = (x \cdot xy)(yx \cdot z) = (x \cdot xy)(z \cdot yx)$$
$$= (x \cdot xy)(z \cdot xy) = yz \cdot xy = x \cdot zy = x \cdot yz = AB,$$

proving the theorem.

THEOREM 9.7. *Q is an abelian left-distributive quasigroup if and only if it satisfies the identity γ, $ab \cdot ca = a \cdot bc$.*

Proof. Set $a = b = c$ in γ. Then, $a^2 \cdot a^2 = a \cdot a^2$, so Q is idempotent. Next set $a = b$ in γ. Then $bb \cdot cb = b \cdot bc$. Cancellation yields $bc = cb$. The remainder of the proof is equally direct.

LEMMA 9.8. *Let Q be a finite idempotent quasigroup of order n, and x an element of Q. Introduce on the nondiagonal elements, t, of G, containing x as one of its three coordinates a symmetric relation R defined by: tRt' if and only if there is i, $1 \leqq i \leqq 3$, so that $\pi_i t$ is the transpose of $\pi_i t'$. Let $\phi(x)$ equal the number of equivalence classes of the minimal equivalence relation generated by R. If $Z = \sum_x \phi(x)$ then*

$$Z \equiv \frac{n(n-1)}{2} \pmod 2.$$

Proof. The (topological) proof of this theorem is to be found in [46].

THEOREM 9.9. *There exist left-distributive quasigroups of order n only for $n \equiv 0, 1, 3 \pmod 4$.*

Proof. Existence will be established first. On the Galois field $GF(2^k)$, $k \geq 2$, introduce the law of composition $x \circ y = \alpha x + \beta y$ with α and β fixed nonzero elements satisfying the equation $\alpha + \beta = 1$. A simple computation shows that the algebra f defined by $f(x, y) = x \circ y$ is a left-distributive quasigroup.

On the cyclic group of odd order m introduce a law of composition $x \circ y = x^p y^q$, with $(p, m) = 1 = (q, m)$ and $p + q \equiv 1 \pmod m$. Again a simple computation shows that $x \circ y$ defines a left-distributive quasigroup.

Now $n \equiv 0, 1, 3 \pmod 4$ is equivalent to $n = 2^k \cdot m$, $k \neq 1$, m odd. The orders of the quasigroups constructed above and their direct products sweep out all such $2^k \cdot m$.

Nonexistence will next be considered. A left-distributive quasigroup has a transitive group of automorphisms. In fact, the left translations constitute a transitive set of automorphisms. It is not difficult to see that if, in an idempotent quasigroup, there is an automorphism α with $\alpha(x) = x'$ then $\phi(x) = \phi(x')$. Thus, if the group of automorphisms is transitive $Z \equiv 0 \pmod n$. If n is even Z is therefore even. But, if $n = 2m$, m odd, Z is odd, since $Z \equiv (n)(n-1)/2 \pmod 2$. This contradiction establishes the theorem.

DEFINITION 9.10. The algebra constructed from the $GF(2^k)$ by the multiplication $x \circ y = ax + \beta y$, where α, β are fixed in $GF(2^k)$ shall be denoted $A(GF(2^k), \alpha, \beta)$. The algebra constructed on the cyclic abelian group $G(n)$, of order n, by the multiplication $x \circ y = x^p \cdot y^q$, where $p, q \cdot \in J$ shall be denoted $A(G(n), p, a)$.

COROLLARY 9.11. *The group of automorphisms of a quasigroup of order* $n \equiv 2 \pmod 4$, *containing at least one idempotent element, is not transitive.*

Proof. A quasigroup with at least one idempotent element and possessing a transitive group of automorphisms is idempotent. The method of the preceding proof therefore applies.

THEOREM 9.12. *Let* Q *be a left-distributive quasigroup and* $a, b \in Q$. *The equivalence* $\phi: Q \to Q$ *defined by* $ax = b\phi(x)$ *is an automorphism.*

Proof. Like that of Theorem 9.13, to follow.

THEOREM 9.13. *Let* Q *be a left- and right-distributive quasigroup and* $a \in Q$ *be a fixed element. The equivalence* $\phi: Q \to Q$ *defined by* $ax = \phi(x)$ *a is an (inner) automorphism.*

Proof. Let $ax = \phi(x)a$ and $ay = \phi(y)a$. Then $a(xy) = ax \cdot ay = \phi(x)a \cdot \phi(y) \cdot a = \phi(x)\phi(y) \cdot a$. Thus $\phi(xy) = \phi(x)\phi(y)$.

THEOREM 9.14. *Let* Q *be a left- and right-distributive quasigroup and* $a, b \in Q$. *The equivalence* $\phi: Q \to Q$ *defined by* $ax = \phi(x) \cdot b$ *is an automorphism.*

Proof. Like that of Theorem 9.13.

10. Quasirings.

DEFINITION 10.1. A quasiring is a collection of distinct quasigroups $f_1, \cdots, f_k$, $k \geq 2$, defined on the same set, such that for $i \neq j$, $1 \leq i, j \leq k$, f_j is left-distributive over f_i, i.e., $f_j(a, f_i(b, c)) = f_j(f_i(a, b), f_i(a, c))$. Each f_j is clearly idempotent.

THEOREM 10.2. *There exist no quasirings of order* $n \equiv 2 \pmod 4$.

Proof. This is a consequence of Corollary 9.11.

THEOREM 10.3. *There exist quasirings of orders* $n \equiv 0, 1, 3 \pmod 4$, $n > 3$ *consisting of two quasigroups* f_1, f_2, *such that for all* i, j, $1 \leq i, j \leq 2$, f_i *is left- and right-distributive over* f_j.

Proof. Let f_1 be a left- and right-distributive noncommutative quasigroup of order n; for example, one of the nonabelian quasigroups of order n constructed in the proof of Theorem 9.8. Let $f_2 = (12)f_1$. Clearly, f_1 is left- and right-distributive over itself, $i = 1, 2$. Typical of the proofs of the remaining cases is the computation showing that f_1 is left-distributive over f_2.

For simplicity, denote $f_1(a, b)$ by ab and $f_2(a, b)$ by $a \circ b$. The assertion $a(b \circ c) = (ab) \circ (ac)$ is equivalent to the assertion $b \circ c = p$, $ap = q$, $ab = r$, $ac = s$, imply $r \circ s = q$. This is equivalent to the assertion that $cb = p$, $ap = q$, $ab = r$, $ac = s$ imply $sr = q$. This in turn is equivalent to $cb = p$, $ab = r$, $ac = s$ imply $ap = sr$, which is equivalent to $a \cdot cb = ac \cdot ab$, left-distributivity of f_1.

COROLLARY 10.4. *The quasigroup f is left-distributive if and only if* (12) *f is left-distributive over f.*

III. MEDIAL ALGEBRAS

11. Constraints related to mediality.

DEFINITION 11.1. An algebra is medial if it satisfies the identity $ab \cdot cd = ac \cdot bd$.

THEOREM 11.2. *An algebra with two-sided unit is medial if and only if it is abelian and associative.*

Proof. Let e be the unit of a medial algebra. Then $eb \cdot ce = ec \cdot be$; thus $bc = cb$, or the algebra is abelian. Also $ae \cdot cd = ac \cdot ed$; thus $a \cdot cd = ac \cdot d$, or the algebra is associative.

Conversely, let an algebra be associative and abelian. Then $ab \cdot cd = (ab \cdot c)d = (c \cdot ab)d = (ca \cdot b)d = (ac \cdot b)d = ac \cdot bd$.

COROLLARY 11.3. *An associative abelian algebra is medial.*

Proof. This is proved in the proof of Theorem 11.2.

THEOREM 11.4 (Hosszu [43]). *An algebra satisfying the identity $a \cdot bc = c \cdot ba$ is medial.*

Proof. $ab \cdot cd = d(c \cdot ab) = d(b \cdot ac) = ac \cdot bd$.

THEOREM 11.5 (Hosszu [43]). *If Q is a quasigroup satisfying $ab \cdot c = b \cdot ca$ then Q is a commutative group, hence medial.*

Proof. Assume e, $x \in Q$ satisfy $ex = x$. Then $x(ye) = (ex)y = xy$. Cancellation yields $ye = y$ for all y. Thus e is independent of x. Hence $ex = x$ for all x. Also $a(b \cdot cd) = a(db \cdot c) = ca \cdot db = (b \cdot ca)d$. If $d = e$ then $a \cdot bc = b \cdot ca$. But $b \cdot ca = ab \cdot c$. Thus $a \cdot bc = ab \cdot c$. Setting $c = e$ in $ab \cdot c = b \cdot ca$ yields $ac = ca$.

THEOREM 11.6. *An abelian quasigroup satisfying the identity $ab \cdot ac = db \cdot dc$ is medial.*

Proof. It shall first be shown that $ab = cd$ implies $ad = cb$. Let $ab = cd$ and $ad = cx$. Then $ab \cdot ad = cd \cdot cx$; thus $cb \cdot cd = cd \cdot cx$. Hence $cd \cdot cb = cd \cdot cx$, implying $x = b$.

Now assume $ab \cdot cd = ac \cdot bx$. Then $ab \cdot bx = ac \cdot cd$. Thus $ba \cdot bx = ca \cdot cd$, implying $ca \cdot cx = ca \cdot cd$ and hence $x = d$.

THEOREM 11.7. *A group is medial if and only if it is abelian.*

Proof. This is a consequence of Theorem 11.2.

COROLLARY 11.8. *A quasigroup Q satisfying the identities $ab\cdot ac=bc$ and $ab\cdot b=a$ is medial.*

Proof. As will be shown in §12 the constraint of mediality is invariant. If $\sigma=(23)$ then, as Tables 5.4 and 8.1 indicate, σQ is an abelian group. Theorem 11.2 and Corollary 6.13 thus prove the corollary.

Alternate proof. It may be illuminating to present the direct proof of Corollary 11.8 provided by the conjugation of the second part of the proof of Theorem 11.2.

The proof of Theorem 11.2 can be decomposed into atomic steps in the following way. For all a, b, c, d define x, y, z by $ab=x$, $cd=y$, $xy=z$. Define t by $xc=t$. Then $td=z$. But $cx=t$. Define p by $ca=p$. Then $pb=t$. But $ac=p$. Define q by $bd=q$. Then $pq=z$. This reduces to $ab\cdot cd=ac\cdot bd$.

Conjugation of this proof by $\sigma=(23)$ is the following. For all a, b, c, d define x, y, z by solving $ax=b$, $cy=d$, $xz=y$. Define t by solving $xt=c$. Then $tz=d$. But $ct=x$. Define p by solving $cp=a$. Then $pt=b$. But $ap=c$. Define q by $bq=d$. Then $pz=q$.

From this proof mediality can be deduced by use of the computation observations in the Commentary on §5. To show $ap\cdot xz=ax\cdot pz$, define c, y, d, t, b, q by use of the above equations. Observe that the last two sentences of the proof can be inverted to read: "define q by $pz=q$. Then $bq=d$." Thus for all a, p, x, z, $ap\cdot xz=ax\cdot pz$.

Presumably, any proof of Corollary 11.8 would be more indirect than the proof of Theorem 11.2 since the conjugation by $\sigma=(23)$ of "evaluate" is "solve.".

The following lemma, theorem and proof is a recasting into the terminology of quasigroups of Knaster [36].

THEOREM 11.9. *An abelian left-distributive quasigroup possessing a linear ordering compatible with the algebra ($x<y$ implies $ax<ay$) is medial.*

The existence of the linear ordering is used only in the proof of the following lemma. As will be noted the lemma would also follow from incompatibility ($x<y$ implies $ax>ay$).

LEMMA 11.10. *Under the above assumption if*

$$A = xy = Bx\cdot Cy,$$
$$C = zt = Az\cdot Bt$$

then

$$A = B\ (=C).$$

Proof of Lemma 11.10. The equations $xy = Ax \cdot Ay$, $zt = Cz \cdot Ct$ follow immediately. Thus

(1) $$Ax \cdot Ay = Bx \cdot Cy \quad \text{and} \quad (2)\ Cz \cdot Ct = Az \cdot Bt.$$

Assume $B < A$. Then by (1) $A < C$, so $B < A < C$. But by (2) $A < C$ implies $C < B$, so $A < C < B$. This is a contradiction, unless $A = B (= C)$.

Proof of Theorem 11.9. To show $ab \cdot cd = ac \cdot bd$, observe that

$$ab \cdot cd = (a \cdot cd)(b \cdot cd) = (ac \cdot ad)(bc \cdot bd) = (ac \cdot da)(cb \cdot bd)$$

and

$$\begin{aligned} ab \cdot cd &= (ab \cdot c)(ab \cdot d) = (ac \cdot bc)(ad \cdot bd) = (ac \cdot cb)(da \cdot bd) \\ &= (ac(da \cdot bd)) \cdot (cb(da \cdot bd)) = ((ac \cdot da)(ac \cdot bd))((cb \cdot da)(cb \cdot bd)). \end{aligned}$$

Also

$$cb \cdot da = (cb \cdot d)(cb \cdot a) = (cb \cdot d)(a \cdot bc) = (cd \cdot bd)(ab \cdot ac)$$

and

$$\begin{aligned} cb \cdot da &= (c \cdot da)(b \cdot da) = (cd \cdot ca)(bd \cdot ba) = (cd \cdot ac)(bd \cdot ab) \\ &= ((cd \cdot ac) \cdot bd) \cdot (ab(cd \cdot ac)) = (cd \cdot bd)(ac \cdot bd)) \cdot (ab \cdot cd)(ab \cdot ac)). \end{aligned}$$

Now let

$$x = ac \cdot db, \qquad y = cb \cdot bd, \qquad z = ab \cdot bc, \qquad t = cd \cdot bd$$

and

$$A = ab \cdot cd, \quad B = ac \cdot bd, \quad C = cb \cdot da.$$

Then the equalities derived above can be written

$$\begin{aligned} A &= xy = xB \cdot Cy, \\ C &= tz = tB \cdot Az. \end{aligned}$$

Commutativity and Lemma 11.10 yield $A = B$, that is, $ab \cdot cd = ac \cdot bd$.

12. **Constraints equivalent to mediality.** This section is devoted primarily to alternative descriptions of the constraint of mediality.

THEOREM 12.1. *The identity $ab \cdot cd = ac \cdot bd$ is invariant. In fact, it may be characterized as the only identity of the form $ab \cdot cd = a'b' \cdot c'd'$, where a', b', c', d' is a permutation of a, b, c, d which is invariant (other than the tautologous identity corresponding to the identity permutation).*

Proof. If γ is the constraint of mediality then so is (23) γ. For γ is equivalent to

$$ab = p,\ cd = q,\ pq = r,\ ac = s,\ bd = t \text{ imply } st = r \text{ for all } a, b, c, d.$$

Or equivalently

$ab = p$, $cd = q$, $pq = r$, $ac = s$, $bd = t$ imply $st = r$ for all a, p, r, s.

This in turn is equivalent to

$ab = p$, $pq = r$, $ac = s$, $st = r$, $cd = q$ imply $bd = t$ for all a, p, r, s.

Conjugation of this constraint by $\sigma = (23)$ yields

$ap = b$, $pr = q$, $as = c$, $sr = t$, $cq = d$ imply $bt = d$ for all a, p, r, s.

This reduces to the identity $as \cdot pr = ap \cdot sr$, that is, (23) $\gamma \equiv \gamma$.

Obviously, (12) $\gamma \equiv \gamma$. Thus γ is invariant.

A mechanical check of the identities of the form $ab \cdot cd = a'b' \cdot c'd'$ shows that only the two mentioned in the statement of Theorem 12.1 are invariant.

THEOREM 12.2. *A quasigroup Q is medial if and only if it satisfies the constraint γ: $ab = a'b'$, $cd = c'd'$ imply $ac \cdot bd = a'c' \cdot b'd'$.*

Proof. Let Q be medial and satisfy the hypotheses of γ. Then $ab \cdot cd = a'b' \cdot c'd'$ and hence $ac \cdot bd = a'c' \cdot b'd'$.

Conversely, let Q satisfy γ. To show $ab \cdot cd = ac \cdot bd$ define u by $bd = cu$. Then $ac = ac$ and $bd = cu$. Application of γ yields $ab \cdot cd = ac \cdot cu = ac \cdot bd$.

THEOREM 12.3. *A quasigroup Q is medial if and only if it satisfies the constraint γ: $pq = rs$ implies $xp \cdot yq = xr \cdot ys$.*

Proof. Let Q be medial and $pq = rs$. Then $xp \cdot yq = xy \cdot pq = xy \cdot rs$, $= xr \cdot ys$.

Conversely, let Q satisfy γ and $a, b, c, d \in Q$. Define s by $bd = cs$. Then $ab \cdot cd = ac \cdot cs = ac \cdot bd$.

THEOREM 12.4. *A quasigroup Q is medial if and only if it satisfies the two constraints*

(12.5) $$xa = by,\ za = bw \text{ imply } xw = zy$$

and

(12.6) $$\text{The simultaneous equations } ab \cdot x = y \cdot bc,\ ad \cdot x = y \cdot dc \text{ have a solution } x, y.$$

Proof. Assume Q is medial and $xa = by$, $za = bw$. Then $xw \cdot ab = xa \cdot wb = by \cdot wb = bw \cdot yb = za \cdot by = zy \cdot ab$. Cancellation of ab yields (12.5). Since Q is medial (12.6) has the solution $x = bc$, $y = ab$.

Conversely, assume that Q satisfies (12.5) and (12.6). To show $ab \cdot cd = ac \cdot bd$ solve the simultaneous equations $ab \cdot x = y \cdot bd$ and $ac \cdot x = y \cdot cd$ for x, y. Application of (12.5) yields $ab \cdot cd = ac \cdot bd$.

REMARK. Either an associative, left-distributive, right-distributive or medial algebra A satisfies (12.6). The solutions x, y are respectively, (c, a), (ac, a), (c, ac), and, as already noted, (bc, ab).

DEFINITION 12.7. If X is a set and A is an algebra and $f, g: X \to A$, then the product fg is defined by

$$fg(x) = f(x) \cdot g(x) \text{ for all } x \in X.$$

THEOREM 12.8. *An algebra A is medial if and only if for any algebra B and homomorphisms $f, g: B \to A$, fg is again a homomorphism.*

Proof. Let A be medial and $f, g: B \to A$ be homomorphisms. For $x, y \in B$, $fg(xy) = f(xy)g(xy) = (f(x)f(y))(g(x)g(y)) = (f(x)g(x))(f(y)g(y)) = fg(x)fg(y)$. Thus the product of two homomorphisms is again a homomorphism.

Assume that the product of any two homomorphisms into A is again a homomorphism. Let a, b, c, d be in A. Let B be the free algebra on two generators x, y. Let $f: B \to A$ be the homomorphism defined by $f(x) = a$, $f(y) = b$ and $g: B \to A$ be similarly defined by $g(x) = c$, $g(y) = d$.

Since fg is a homomorphism

$$ab \cdot cd = f(xy)g(xy) = fg(xy) = fg(x) \cdot fg(y) = (f(x)g(x))(f(y)g(y)) = ac \cdot bd.$$

13. Consequence of mediality.

DEFINITION 13.1. If B is an algebra and A is a medial algebra then Hom (B, A) is the (medial) algebra of homomorphisms from B into A, where the product is given by Definition 12.7.

THEOREM 13.2. *If B is an algebra and Q is a medial quasigroup then* Hom (B, Q) *is a (possibly void) medial quasigroup.*

Proof. The only point of interest is the fact that if $f, g: B \to Q$ are homomorphisms and $h: B \to Q$ is defined by $f(x) = h(x)g(x)$ then h is a homomorphism.

That $h(xy) = h(x) \cdot h(y)$ is a consequence of the equations:

$$f(xy) = h(xy) \cdot g(xy)$$

and

$$\begin{aligned} f(xy) &= f(x)f(y) = (h(x)g(x))(h(y)g(y)) = (h(x)h(y))(g(x) \cdot g(y)) \\ &= (h(x) \cdot h(y))(g(xy)). \end{aligned}$$

THEOREM 13.3. *If B is an algebra and A is a medial algebra and $a \in A$ is an idempotent element, then the constant function $f: B \to A$ defined by $f(x) = a$ is a homomorphism.*

COROLLARY 13.4. *If A contains an idempotent element* Hom (B, A) *is not empty.*

COROLLARY 13.5. *The algebra A is idempotent if and only if for each algebra B, each constant function $f: B \to A$ is a homomorphism.*

THEOREM 13.6. *Any subquasigroup N of a medial quasigroup Q is normal in Q in the sense that for each $a, b \in Q$, $aN \cdot bN = ab \cdot N$ and $Na \cdot Nb = N \cdot ab$.*

Proof. If $m, n \in N$, then $am \cdot bn = ab \cdot mn$. Thus $aN \cdot bN \subset ab \cdot N$. Conversely, let $n \in N$. Represent $n = n_1 n_2$, $n_1, n_2 \in N$. Thus

$$ab \cdot n = ab \cdot n_1 n_2 = an_1 \cdot bn_2 \text{ and } ab \cdot N \subset aN \cdot bN.$$

The remainder of the theorem is proved similarly.

THEOREM 13.7. *Let N be a subquasigroup of the medial quasigroup Q and $a, b \in Q$. Then, if $aN \cap bN \neq \phi$, $aN = bN$. Also if $Na \cap Nb \neq \phi$, $Na = Nb$.*

Proof. Since $aN \cap bN \neq \phi$ there are $n_1, n_2 \in N$ such that $an_1 = bn_2$. Define c by $a = bc$. Then

$$bc \cdot N = bc \cdot n_2 N = bn_2 \cdot cN = an_1 \cdot cN = ac \cdot n_1 N = ac \cdot N,$$

and thus

$$bc \cdot N = ac \cdot N.$$

Let $n_0 \in N$ be a fixed element of N. Then

$$aN \cdot cn_0 = ac \cdot Nn_0 = ac \cdot N = bc \cdot N = bc \cdot Nn_0 = bN \cdot cn_0.$$

Cancellation of cn_0 yields $aN = bN$.

THEOREM 13.8. *If N is a subquasigroup of a medial quasigroup A then the cosets $\{aN\}$ are a medial quasigroup under the law $aN \cdot bN = ab \cdot N$. N is idempotent in this quasigroup.*

Proof. This may be deduced from Theorems 13.6 and 13.7. Clearly N is idempotent.

THEOREM 13.9. *An idempotent medial algebra is left- and right-distributive.*

Proof. $ab \cdot ac = aa \cdot bc = a \cdot bc$. Similarly for right-distributivity.

THEOREM 13.10. *The center of a medial quasigroup Q is either empty or else all of Q.*

Proof. Let a be in the center of Q. Then $bb \cdot ax = bb \cdot xa$ for all $x, b \in Q$. Thus, $ba \cdot bx = bx \cdot ba$ for all x, b. Since for arbitrary $u, v \in Q$ the simultaneous equations $u = ba$, $v = bx$ may be solved for b and x, $uv = vu$. Hence, Q is abelian.

THEOREM 13.11 (Frink [44, p. 704]). *If A is a medial algebra and S and T are subalgebras of A then $U = \{st \mid s \in S, t \in T\}$ is a subalgebra of A.*

Proof. Let $s, s' \in S$ and $t, t' \in T$. Then $st \cdot s't' = ss' \cdot tt'$. So $UU \subset U$.

14. **Examples of medial algebras.** In addition to abelian groups there is a variety of sources of medial algebras. We present several examples, most of which have appeared elsewhere.

EXAMPLE 1. In the terminology of Definition 9.10 $A(G(n), p, q)$ is a medial

algebra. If $(p, n)=1=(q, n)$ then A is a quasigroup. If $p+q\equiv 1 \pmod{n}$ then A is idempotent. A similar construction can be made with $A(GF(2^k), \alpha, \beta)$.

EXAMPLE 2. (Murdoch [21], Toyoda [22], Bruck [26], Frink [44]). Let G be an arbitrary group, $k\in G$ be fixed, and S, T: $G\to G$ be commuting automorphisms. Then the quasigroup defined by $a\circ b=kS(a)T(b)$ is medial. Example 1 is a special case of this.

EXAMPLE 3 (Aczel [31]). Let R be a commutative ring and f: $R\to R$ be an equivalence and p, q, $t\in R$, fixed. Define

$$a\circ b = f^{-1}(pf(a) + qf(b) + t). \tag{14.1}$$

If R is a field and $pq\neq 0$ then this medial algebra is also a quasigroup. The following theorem is pertinent here.

THEOREM 14.2 (Aczel [31]). *A continuous medial quasigroup on the space X of real numbers must be of the form* 14.1, *where f is a homeomorphism of X.*

EXAMPLE 4 (Sholander [35]). Let E_2 be the Euclidean plane. Define an algebra on E_2 by setting $x\cdot y=$midpoint of the segment xy. That this quasigroup is medial is equivalent to the theorem asserting that the midpoints of the sides of a quadrilateral are the vertices of a parallelogram. (This example is simply the direct product of two copies of Example 3 with $f=$identity, $p=1/2=q$, $t=0$.)

EXAMPLE 5 (Sholander [35]). Let ABC be a fixed oriented triangle in E_2. If x, $y\in E_2$ define $xy=z$ by the demand that the triangle xyz is similar to ABC and has the same orientation (set $xx=x$).

EXAMPLE 6 (Sholander [35]). Let s be a fixed number of the real projective line P_1 and r a real number. For x, $y\in P_1$ define $xy=z$ by the demand $R(s, x, y, z)=r$. This example generalizes $(x+y)/2$ (a special case of Example 3), since the midpoint is the harmonic conjugate of the point at infinity.

EXAMPLE 7 (Mituhisa [25]). On C, the circumference of a circle, define $xy=z$ if z is the mirror image of y in the diameter through x.

EXAMPLE 8 (Mituhisa [25]). On P, a parabola, define $xy=z$ by the demand that $z\in P$ and that the line yz is parallel to the tangent at x (set $xx=x$). This turns P into a medial quasigroup.

EXAMPLE 9. Let C be a conic in the real projective plane and L a line not meeting C. If x, $y\in C$ define $xy=z$ by the demand that $z\in C$, $z\neq y$, and that L, the tangent to C at x, and the line zy be concurrent (set $xx=x$). That this defines a medial algebra on C may be proved in the following way. If C is a circle and L the line at infinity this is simply Example 6. An appropriate projectivity shows that the more general construction produces a medial algebra.

EXAMPLE 10. Let C be a conic in the real projective plane and L a tangent to C. Let Q denote C minus the point of contact of L. If x, $y\in Q$ define $xy=z$ by the demand that $z\in Q$, $z\neq y$ and that L, the tangent at x, and the line zy

be concurrent (set $xx=x$). Since this is the limiting case of the preceding example continuity yields that Q is a medial quasigroup. (This generalizes Example 8).

Applying $\sigma=(13)$ to the Q of Example 10, one deduces the following theorem.

THEOREM 14.3. *Let Q denote a conic minus the point of contact of a tangent L. If $x, y\in Q$ define $xy=z$ by the demand that L, the tangent at z, and the line xy be concurrent (set $xx=x$). Then Q is a medial, abelian, idempotent quasigroup.*

This suggests the following theorem.

THEOREM 14.4. *Let K denote a smooth convex closed curve without line segments minus the point of contact of a tangent L. If $x, y\in K$ define $xy=z$ by the demand that L, the tangent at z, and the line xy be concurrent (set $xx=x$). Then K is an abelian idempotent quasigroup. It is medial if and only if the curve is a conic.*

EXAMPLE 11. Let C be a line conic in the real projective plane and F a point of contact of C. Let Q denote C minus the tangent at F. If $x, y\in Q$ define $xy=z$ be the demand that F, the point of contact of z, and intersection of x and y be collinear (set $xx=x$). Then Q is a medial, abelian, idempotent quasigroup (it is simply the projective dual of the quasigroup of Theorem 14.3).

(Moreover, it can be shown that Example 11 is isomorphic to the quasigroup of Theorem 14.3; in fact, the function which assigns to each tangent its point of contact is an isomorphism.)

IV. ORTHOGONAL ALGEBRAS

15. Implication of orthogonality on an algebra.

DEFINITION 15.1. Two algebras f, g defined on the same set X are orthogonal if

$$f\times g: X\times X\to X\times X$$

defined by $f\times g(x, x')=(f(x, x'), g(x, x'))$ is an equivalence. The algebra g is an orthogonal complement to f.

For X finite f and g are orthogonal if and only if $f\times g$ is onto (or $f\times g$ is one-one). For arbitrary X, f and g are orthogonal if and only if: for every $a, b\in X$ the simultaneous equations $f(x, y)=a$, $g(x, y)=b$ have a unique solution x, y.

THEOREM 15.1. *A finite commutative algebra A is a quasigroup if and only if it is orthogonal to the algebra A^* whose multiplication is given by $x*y=x\cdot xy$.*

Proof. Let A be a quasigroup and $a, b\in X$. Then there exists x so $xa=b$, and then y so $xy=a$. Thus, the simultaneous equations $xy=a$, $x*y=b$ have a solution x, y.

Conversely, let A be orthogonal to A^*. Assume $xy=xz$. Then $x\cdot xy=x\cdot xz$, or $x*y=x*z$, thus $y=z$. Since A is commutative it is a quasigroup.

THEOREM 15.2. *Every quasigroup has an orthogonal complement (which is not necessarily a quasigroup).*

Proof. Similar to the first part of the proof of Theorem 15.1.

16. **Constraints implying orthogonality.** This section presents various methods of associating with a quasigroup a few specific algebras as candidates for orthogonal quasigroup complements.

THEOREM 16.1. *A quasigroup Q, satisfying the constraint $x\cdot xz=y\cdot yz$ implies $x=y$, possesses an orthogonal complement which is a quasigroup.*

Proof. It is sufficient to show that Q^*, defined in the statement of Theorem 15.1, is a quasigroup. The equation $s*z=x*y$ is equivalent to $x\cdot xz=x\cdot xy$, which, since Q is a quasigroup, implies $y=z$. The equation $z*x=y*x$ is equivalent to $z\cdot zx=y\cdot yx$, which by assumption implies $y=z$.

THEOREM 16.2. *There exist quasigroups satisfying the constraint $x\cdot xz=y\cdot yz$ implies $x=y$ for orders $n\equiv 0, 1, 3 \pmod 4$.*

Proof. If $\alpha\beta(1+\beta)\neq 0$ and $k\geqq 2$ then $A(GF(2^k), \alpha, \beta)$ satisfies the constraint. Direct product of these with abelian groups of odd order proves the theorem.

THEOREM 16.3. *A quasigroup satisfying the identity $a\cdot ab=ba$ has an orthogonal complement.*

Proof. This is a consequence of Theorem 16.1.

THEOREM 16.4. *Let Q be a finite quasigroup and $\sigma\in S_3$. Then Q is orthogonal to σQ if and only if Q satisfies the constraint γ, depending on σ as is indicated by the following table.*

(16.5)

σ	γ
(12)	$ab=a'b'$, $ba=b'a'$ *imply* $a=a'$, $b=b'$
(13)	$ab\cdot b=ac\cdot c$ *implies* $b=c$
(23)	$b\cdot ba=c\cdot ca$ *implies* $b=c$
(123)	$b\cdot ab=c\cdot ac$ *implies* $b=c$
(132)	$ba\cdot b=ca\cdot c$ *implies* $b=c$

Proof. The case $\sigma=(13)$ is typical. Designate by $*$ the algebra of σQ. Q is orthogonal to σQ if and only if the simultaneous equation $xy=a$, $x*y=b$ have a solution x, y for all a, b. In Q this translates into the demand that the equations $xy=z$, $by=x$ have solutions or equivalently $by\cdot y=a$ has a solution. Since Q is finite, this is equivalent to the constraint γ listed in the table.

THEOREM 16.6. *Let Q be a finite quasigroup and $\sigma, \tau\in S_3$, $\sigma\neq\tau$. Then σQ is*

orthogonal to τQ if and only if Q satisfies the constraint listed in the following table.

(16.7)

σ \ τ	(13)	(23)	(123)	(132)
(12)	$b\cdot ab=c\cdot ac\Rightarrow b=c$	$ba\cdot b=ca\cdot c\Rightarrow b=c$	$ab\cdot b=ac\cdot c\Rightarrow b=c$	$b\cdot ba=c\cdot ca\Rightarrow b=c$
(13)		$a\cdot xb=x$ has solution (1)	$a\cdot bx=x$ has solution	$ax=xb$ has solution
(23)			$xa=bx$ has solution	$xb\cdot a=x$ has solution
(123)				$a\cdot xb=x$ has solution (1)

(1) *Equivalently $ax\cdot b=x$ has solution.*

Proof. Like that of preceding theorem.

COROLLARY 16.8. *If a finite quasigroup of order n satisfies at least one of the constraints in* (16.5) *and* (16.7) *then there is a pair of orthogonal quasigroups of order n.*

COROLLARY 16.9. *If a finite quasigroup of order n satisfies all of the constraints in* (16.5) *and* (16.7) *then there are six mutually orthogonal quasi-groups of order n.*

V. CONJUGATES OF VARIOUS CONSTRAINTS

17. **Examples of invariant constraints.** The following identities are invariant: $ab\cdot cd=ac\cdot bd$; $ab\cdot ca=ac\cdot ba$; $aa=a$; $ab\cdot ba=a$; $ab\cdot bc=ac$.

The following constraints are invariant: $ab\cdot ca=a$ implies $ac\cdot ba=a$; $ca=bd$, $ea=bf$ imply $cf=ed$; $ab=a'b'$, $ac=a'c'$, $bd=b'd'$ imply $cd=c'd'$.

18. **Examples of noninvariant constraints.** The list of conjugates of associativity and commutativity is to be found in (8.1) and (9.2). The following table is a list of conjugates of some other constraints that have been considered in the literature.

(18.1)

I	(12)	(13)	(23)	(123)	(132)
$ab\cdot ba=b$	$ab\cdot ba=b$	$a\cdot bc=c\Rightarrow$ $bc\cdot b=a$	$ab\cdot c=a\Rightarrow$ $b\cdot ab=c$	$a\cdot bc=c\Rightarrow$ $bc\cdot b=a$	$ab\cdot c=a\Rightarrow$ $b\cdot ab=c$
$a\cdot bc=ca\cdot b$	$a\cdot bc=ca\cdot b$	$(a\cdot bc)ab=c$	$((ab\cdot c)a)b=c$	$(a\cdot bc)cb=c$	$((ab\cdot c)a)b=c$
$ab\cdot c=ad\Rightarrow$ $eb\cdot c=ed$	$c\cdot ba=da\Rightarrow$ $c\cdot be=de$	$ab\cdot c=ad\Rightarrow$ $eb\cdot c=ed$	$ca=c'b$ $da=d'b$ $cd=c'd'$	$ca=c'b$ $da=d'b$ $cd=c'd'$	$a\cdot bc=dc\Rightarrow$ $a\cdot be=de$
$ab\cdot ac=db\cdot dc$	$ca\cdot ba=cd\cdot bd$	$ax\cdot b=xc\Rightarrow$ $ay\cdot b=yc$	$ab=cd\Rightarrow$ $a\cdot bx=c\cdot dx$	$ab=cd\Rightarrow$ $xa\cdot b=xc\cdot d$	$a\cdot xb=cx\Rightarrow$ $a\cdot yb=cy$

VI. Varieties

19. **Application of conjugation to varieties.** Let A, Q, G, C denote the class of all algebras, quasigroups, groups and commutative groups respectively. Then $A \supset Q \supset G \supset C$.

Definition 19.1. A class S of algebras is a variety in a class T of algebras if there is an identity γ such that S consists of precisely those members of T satisfying γ.

Theorem 19.2. *For $\sigma = I$ or (12), σG is not a variety in A but for all other σ, σG is a variety in A.*

The proof is to be found in Higman and Neumann [40].

Theorem 19.3. *If $\sigma \neq I$, (12) then the subclass of σG satisfying an identity γ is a variety in A.*

The proof is to be found in Higman and Neumann [40].

Theorem 19.4. *The class G_2 of groups in which every element is of order 2 is a variety in A.*

Proof. Let $\sigma = (13)$. By Theorem 19.3 σG_2 is a variety in A. But, by Corollary 7.3, $\sigma G_2 = G_2$.

Theorem 19.5. *If $\sigma \neq I$, (12) then σC is a variety in A.*

Proof. Higman and Neumann [40] offer two proofs of this. The first consists of noting that it is a consequence of Theorem 19.3 and the second consists of presenting a short identity for σC. For $\sigma = (13)$ this identity is $a(bc \cdot ba) = c$, which is $\sigma\gamma$, where γ is the identity $ab \cdot c = b \cdot ca$ distinguishing C as a variety in Q (Theorem 11.5).

VII. Commentary

20. **Remarks.** On §3. The phrase "Polyadic Group" was used by E. L. Post [18] who observed the similarity between the notions "single valued" and "unique solution." The observation that the symmetric group operates on graph to yield a new graph was exploited by Lefschetz [23, p. 175] in a neat presentation of the relation between cup and cap product.

On §4. That quasigroups come in sextuplets was observed most recently by D. A. Norton and the author in developing the theory of cycles [46; 47] which is based directly on the graph G. Bruck [26, p. 24] pointed out the presence of the five additional quasigroups. H. W. Norton [16], in his table of quasigroups of order 7 lists those which are "identical with their adjugates" ("totally symmetric" in the sense of Definition 8.2). See in particular [16, pp. 272, 282–285]. Bruck investigated totally symmetric quasigroups, especially their relation to loops, in [26]. Several times, in the theory of groups,

the quasigroups $(132)Q$, $(23)Q$ have been studied, especially in axiomatizing groups in terms of the inverse operations (e.g. [5; 9; 11; 12; 14; 45]).

As is well-known, Definition 4.2 of a group can be weakened to: π_1, π_2 are onto, π_3 is an equivalence and associativity holds. Various conditions which give rise directly or indirectly to groups have been studied. (1) As Theorem 5.4 indicates, there is a one-one correspondence between groups and quasigroups satisfying the identity $ab \cdot ac = bc$. (2) (Suschkewitsch [3]). If a quasigroup satisfies the constraint that the solution, c, of $xa \cdot b = xc$ is independent of x (that is, $xa \cdot b = xc$ implies $ya \cdot b = yc$ (see third row of 18.1 and related B of Lemma 7.5) then the quasigroup defined by $a \circ b = c$ is a group. (3) (Evans [37]). A loop for which there exist equivalences P_i, Q_i, $1 \leqq i \leqq 5$, satisfying

$$P_5(P_1(x)P_4(P_2y \cdot P_3z)) = Q_5(Q_3(Q_1x \cdot Q_2y)Q_4z)$$

is a group. (4) Murdoch [21] obtains an abelian group from a medial quasigroup. If Q is a medial abelian quasigroup and $a = aa$ is a fixed element of Q then a special example of his method is the quasigroup given by $ax \circ ay = xy$. That this quasigroup is an abelian group is a consequence of the easily verified facts that it is a medial loop (with unit "a").

On §5. In the computation and simplification of conjugate constraints, the following observations are of aid. Usually the atomic form of a constraint takes the form $E_1, \cdots, E_k$ imply E_{k+1} where

1. E_j is an equation of the form $ab = c$ where a, b, c are distinct variable $(1 \leqq j \leqq k+1)$. 2. E_i and E_j have at most one variable in common $(i \neq j)$. 3. Each variable appearing in the E_i appears at least twice. 4. For any E_i, E_j there is a sequence $E_i = E_{k_1}, E_{k_2}, \cdots, E_{k_n} = E_j$ where E_{k_α} and $E_{k_{\alpha+1}}$ $(1 \leqq \alpha \leqq n-1)$ have a variable in common.

For such systems one can easily see that

(a) Any k of the equations imply the remaining one,

(b) The universal operatory "$\wedge$" can be assumed to run over all the variables or any subset of them. (If the variables in the subset, S are "independent" and define the remaining variables by successive application of the E_j, then their number is independent of S).

The identity $ab \cdot ac = bc$ is to be found in Suschkewitsch [3, p. 213], Tarski [12, p. 254], Higman and Neumann [40] and Furstenberg [45].

Corollary 5.5 raises several questions. It shows that, though we define a function rigorously as a subset of X^k, we tend to look at X^k along one preferred axis. In our bias, we develop a multiplicative notation based on operations with parentheses. Since we would like to dispense with parentheses, we demand associativity. As Corollary 5.6 shows, the study of associative quasigroups is equivalent to the study of quasigroups satisfying a rather uninviting identity.

The interpretation of associativity in the Cayley multiplication table (Andreas Speiser, *Die Theorie von Gruppen von endlicher Ordnung*, New York,

Dover, 1943, p. 14) does not compare in simplicity to that of commutativity. On the other hand, associativity can be expressed in terms of commutativity. Specifically, an algebra is associative if its left and right translations commute with each other.

It would be illuminating to know what are the implications of associativity which give it such a prominence before all other identities. For example, if an algebra is a homomorphic image of a group it is a group. On the other hand, arbitrary quasigroups or even loops do not have this property [32]. The free group on m generators is easily obtained from the free algebra on m generators by "removing parentheses," adjoining a unit e, and introducing solutions to the m equations $xg_i=e$, where g_i is a generator. The free quasigroup on m generators is obtained from the free algebra by introducing solutions to an infinity of equations [29]. There is an analogy of this situation to that of the algebraic closure of the real field and the rational field. Another implication of associativity is that the equivalence, ϕ, defined by $ax=\phi(x)a$, is an automorphism. (This is also a consequence of other identities [see Theorem 9.12]).

On §6. The use of Lemma 6.3 is discussed in the paragraph following Corollary 6.14.

On §7. Theorem 7.4 is due to Sade [38, p. 13]. Statements B, B′ of Lemma 7.5 are some of Suschkewitsch's generalizations of associativity [3]. Another of his generalizations is: the solution "d" to $a\cdot bc=ab\cdot d$ is independent of b. The case $d=ac$ is left-distributivity.

On §8. The identities $a\cdot ab=b$ and $b\cdot ba=a$ are called the left and right law of keys respectively, Mituhisa [25], Sade [38, p. 3]. The phrase "totally symmetric" is due to Bruck [26, p. 34]. The author has been informed that Theorem 8.5 also appears in an inaccessible paper by R. H. Bruck: *A note on Steiner triple systems*, SCAMP working paper 1953. The proof is the same as in [47].

Conjugation of the well-known theorem that there are no commutative idempotent quasigroups of even order is the theorem: there are no quasigroups of even order satisfying the left (right) law of keys.

On §9. C. Burstin and W. Mayer studied quasigroups which are left- and right-distributive [4]. They stated that there are none of orders 2 and 6, observed that the group of automorphisms is transitive, and showed that such a quasigroup is idempotent. A problem of Bourbaki [39, p. 62] is based on their paper. The only other places where self-distributivity was investigated seem to be in Mituhisa [25], Frink [44], Bruck [28] and in the study of functional equations in real variables (see [31; 36; 41]).

Since the relation R is preserved under homomorphisms, it may be used as a local test for the nonexistence of homomorphisms from one quasigroup onto another. For example, if $x'\in Q'$ has an equivalence class with more members than any equivalence class defined on any $x\in Q$, then Q' cannot be the homomorphic image of Q.

The construction of quasigroups from Galois fields dates back at least to Bose [13] 1933, and the construction based on abelian groups at least to Burstin and Mayer [4] 1929.

In groups the equivalences of Theorems 9.12 and 9.14 are automorphisms if and only if $a=b$.

On §10. A quasiring is remotely related to a lattice. It is also related to a structure introduced by Suschkewitch [7]. He considered two commutative, associative algebras with units such that each algebra distributes over the other. In his proofs he does not use associativity.

On §11. The identity $ab\cdot cd=ac\cdot bd$ has been studied by Murdoch [21], Toyoda [22], Etherington [24], Bruck [26], Aczel [31], Knaster [36] Frink [44], under a variety of names. The word "medial" is appropriate for two reasons: (1) The middle two terms are interchanged in $ab\cdot cd$ to obtain $ac\cdot bd$ and (2) The arithmetic mean is a medial operation and most of the examples of §14 are generalizations of this algebra. The connotation of "midness" is therefore not inappropriate. Since there are abelian nonmedial algebras, the name "quasi-abelian" which has been used is misleading.

Theorem 11.2 and Corollary 11.3 are to be found in Etherington [24], Bruck [26], Dubreil [42, p. 84]. Theorem 11.5 is proved in Hosszu [43]. Theorem 11.6 is stated in Sade [38, p. 13].

The author came across the work of Knaster, Aczel, and Hosszu quite by chance. It may well be that other work on functional equations in real variables may impinge on the theory of quasigroups.

Lemma 11.10 is not necessarily true for arbitrary left- and right-distributive quasigroups as the example $A(G(7), 3, 5)$ shows.

On §12. Constraint 12.5 and part of the proof of Theorem 12.4 is to be found in Toyoda [22]. Part of Theorem 12.8 is to be found in Frink [44, p. 701].

On §13. Theorem 13.3 is analogous to the theorem in topology asserting that any constant function is continuous. Two theorems of Bates and Kiokemeister [32] also have topological analogs. The analog of Lemma 3 of [32, p. 1184] is the theorem asserting that the number of sheets in covering space is well defined. The analogs of Lemma 5 [32, p. 1184] are the various theorems on continuous functions with the property that $f^{-1}(y)$ is compact.

If one preferred to study only structures which were preserved under conjugation one would study quasigroups but not groups and idempotent quasigroups but not loops.

Weaker definitions of normality exist. Garrison [19] defines a subset N of a finite quasigroup Q to be normal in Q if for every a, $b\in Q$ there is c so $aN\cdot bN=cN$. Kiokemeister [30] defines a subset N of a quasigroup Q to be normal in Q if there is an equivalence relation R on Q satisfying (1) aRb, $cRd\Rightarrow acRbd$ (2) $acRbc\Rightarrow aRb$ and (3) $caRba\Rightarrow cRb$ with N as one of the equivalence classes of R. Both observe that their definitions are equivalent to the

definition: there exists a quasigroup Q' and homomorphism $f: Q \to Q'$, onto Q', with N as preimage of an element of Q'. This last definition readily shows that normality is invariant under conjugation, i.e., for $\sigma \in S_3$, N is normal in σQ if N is normal in Q. In fact f is also a homomorphism from σQ onto $\sigma Q'$. By letting $\sigma = (12)$ one obtains Garrison's theorem that the product of two right cosets is also a right coset. It is interesting to note that Kiokemeister's conditions (1), (2), (3), are not individually invariant under conjugation. If one wishes N to be a normal subquasigroup then one could demand that N be the preimage under f of an idempotent element of Q'.

Results and methods similar to Theorems 13.6, 13.7, 13.8 appear in Murdoch [15; 20; 21], and Bruck [26].

On §14. Curtis Fulton has obtained a purely projective synthetic proof of Theorem 14.2, and has pointed out that Example 6 yields an analytic proof since the algebra of P_1 may be introduced on C itself.

Application of Murdoch's method (see Commentary on §4) for constructing an abelian group from a medial quasigroup has some interesting geometric consequences. For example, if C is a parabola, L the tangent at infinity, and a the vertex of C, then projection of the abelian group thus defined on C from infinity upon the tangent at a, produces an abelian group G on the tangent with unit "a". It is easy to see that G is ordinary addition.

Addition on the line minus a point is usually defined projectively by the choice of one point on the line and three lines, a total of four arbitrary constructions. The medial quasigroup on a conic minus a point involves no arbitrary choice. In view of these facts, it is reasonable to suggest that the medial algebra on the conic in some respects is more "natural" than addition on the line.

On §16. Euler conjectured that there are no orthogonal quasigroups of order $4k+2$. MacNeish [1, p. 221] conjectured that there are at most $a-1$ mutually orthogonal quasigroups of order n, where $a>1$ is the smallest divisor of n such that $(a, n/a)=1$. He showed that the number $a-1$ is always assumed.

The constraint of Theorem 16.1 is the opposite of the identity $a \cdot ab = b$ in the sense that the identity $a \cdot ab = b$ is equivalent to the constraint: $a \cdot ab$ is independent of a. Indeed, assume $a \cdot ab$ is independent of a. Choose c so $cb = b$. Then $c \cdot cb = cb = b$; so $a \cdot ab = b$ for all a.

Quasigroups satisfying $a \cdot ab = ba$ of Theorem 16.3 have several interesting properties. They are idempotent and distinct elements do not commute. Some models for this identity are

$$\begin{pmatrix} a & c & d & b \\ d & b & a & c \\ b & d & c & a \\ c & a & b & d \end{pmatrix}$$

and $A(G(n), p, a)$ where $p=q^2$, $(2q+1)^2\equiv 5 \pmod{n}$ and n is odd (such systems exist if and only if 5 is a quadratic residue of n); also $A(GF(p^k), \alpha, \beta)$ can be used if $5^{(p^k-1)/2}=1$. For example $(1, 4, 5, 11, 13, 16)\subset J(a\cdot ab=ba)$ and $2, 3, 6\notin J(a\cdot ab=ba)$.

One way to assure that the equation $ax=xb$ of Table 16.7 has a solution is to demand that the identity $a\cdot ab=ab\cdot b$ be satisfied. This identity is satisfied by $A(GF(2^k), \alpha, \beta)$ where $k\geq 2$ and $\alpha=1+\beta$ (hence $\beta=1+\alpha$), and $\beta\cdot(1+\beta)\neq 0$. Or, one could demand that the identity $a\cdot ba=ba\cdot b$ be satisfied. $A(G(n), p, q)$ can be constructed satisfying this identity if -1 is a quadratic residue of n (i.e. n is a product of primes of the form $4k+1$) and $A(GF(p^k), \alpha,\beta)$ can be, if $p\neq 2$ and $(-1)^{(p^k-1)/2}=1$.

On §17. Observe the similarity of the last constraint of §17 to Malcev's condition $ab=a'b'$, $ac=a'c'$, $db=d'b'$, imply $dc=d'c'$ (Dubreil [42, p. 267]), which is a necessary condition that a semigroup be imbeddable in a group.

On §18. The identity $(a\cdot bc)ab=c$ has an unusual property. It is equivalent to the identity $a(bc\cdot ba)=c$, which cannot be deduced from it by cancellation or left or right multiplication. This is a counterexample to the conjecture: if a constraint reduces to an identity then is this identity unique (up to the obvious changes of variables, etc.)? That the two identities are equivalent can be proved in the following manner. The first is

$$bc = x,\ ax = y,\ ab = z \text{ imply } yz = c$$

or equivalently

$$yz = c,\ ax = y,\ ab = z \text{ imply } bc = x$$

which reduces to $x=b(ax\cdot ab)$, which is equivalent to the identity $a(bc\cdot ba)=c$.

The first condition of the third row of 18.1, due to Suschkewitsch [3], asserts that the product of two right translations is a right translation, hence generalizes associativity.

21. **Questions and problems.** The proposals to follow may probably run from the trivial to the impossible. They are intended primarily to indicate some avenues of future investigation.

1. If associativity and commutativity imply the invariant identity γ, does mediality imply γ?

2. Is there an identity belonging to the alternating group?

3. Is a left-distributive quasigroup right-distributive?[3]

4. Does any combination of the hypotheses: left-distributivity, right-distributivity, commutativity imply mediality?

5. Can a quasigroup without idempotent elements and of order $4k+2$ be homogeneous?

---

[3] J. Erdös and M. Hosszu have constructed an infinite cancellation algebra which is left, but not right, distributive.

6. Discuss models for $a\cdot ab=ba$, $a\cdot ab=ab\cdot b$, $a\cdot ba=ba\cdot b$, in particular, their orders.

7. Show that none of the constraints of §16 can be satisfied by a quasigroup of order $4k+2$. (Or else use one to obtain a counter-example to Euler's conjecture.)

8. What medial algebra on the conic is related to the multiplicative group on the projective line (see Commentary on §14)([4])?

9. Let $y=f(x)$ be a differentiable function whose graph is a convex curve K containing no line segments. If P, $Q\in K$ define $P\circ Q$ to be the point of K whose tangent is parallel to $\overline{PQ}$ (set $P\circ P=P$). This quasigroup on K is idempotent and abelian and satisfies all identities deducible from these properties. What other identities can this quasigroup satisfy? (E.g. K is a conic if and only if it is medial.)

10. Is the class of groups satisfying the identity $x^3=1$ a variety in A?

Added in Proof. HISTORICAL ADDENDUM.

References I to VII below, especially the work of Schröder, show that the theory of identities on quasigroups has a history going back to the last century.

Briefly:

I: vectors introduced as elements of quasigroup conjugate to abelian group of points in Euclidean space; identities $AB+BC=AC$, $AA=BB$ appear.

II: identities between $(13)(G)$ and G studied.

III: notion of conjugate quasigroups appears (p. 305) and totally symmetric Q (p. 306); nonidempotent models exhibited of all orders.

IV: finite and infinite idempotent models of the identity $cb(b\cdot ac)=a$ treated; model of order 8 shows conjecture in [47] is wrong; conjugate identities (p. 194); invariance of preceding identity under alternating group (thus answering question 2).

V: list of external symmetries of quasigroups of orders 3 and 4.

VI: equivalence of totally symmetric Q with Q-models of the identity $a\cdot ab=bc\cdot c$; identity $ba\cdot ac=bc$ implies associativity, mediality, total symmetry (p. 250); models of preceding identity of orders 2^n exhibited; mentions right distributivity.

VII: $a\cdot ab=b$, $ac\cdot bc=ac$, $aa=bb$ shown to be conjugate to constraints of abelian group (pp. 56, 59).

I. Hermann Grassman, *Die lineale Ausdehnungslehre*, Leipzig, 1844; 2 Aufl., 1878.

II. H. Hankel, *Theorie der complexen Zahlensysteme*, Leipzig, 1867.

III. E. Schröder, *Rechnung mit Wurfen*, Math. Ann. vol. 10 (1876) pp. 289–317.

([4]) This question has been answered by Curtis Fulton and the author.

IV. ———, *Ueber eine eigentumliche Bextimmung einer Funktion durch formale Anforderungen*, J. Reine Angew. Math. vol. 90 (1880) pp. 189–220.

V. ———, *Tafeln der eindeutig umkehrbaren Funktionen zweier Variabeln auf den einfachsten Zahlengebieten*, Math. Ann. vol. 29 (1887) pp. 229–317.

VI. ———, *Ueber Algorithmen und Calculn*, Arch. der Math. und Physik 2 series. vol. 5 (1887) pp. 225–278.

VII. O. Stolz and J. A. Gmeiner, *Theoretische Arithmetik*, 1 Abteilung, 1911.

References

1. Harris F. MacNeish, *Euler squares*, Ann. of Math. (2) vol. 23 (1921–1922) pp. 221–227.

2. R. A. Fisher, *The arrangement of field experiments*, J. Minis. Ag. vol. 3 (1936) pp. 503–513.

3. Anton Suschkewitsch, *On a generalization of the associative law*, Trans. Amer. Math. Soc. vol. 31 (1929) pp. 204–214.

4. C. Burstin and W. Mayer, *Distributive Gruppen*, J. Reine Angew. Math. vol. 160 (1929) pp. 111–130.

5. Morgan Ward, *Postulates for the inverse operations in a group*, Trans. Amer. Math. Soc. vol. 32 (1930) pp. 520–526.

6. M. Zorn, *Theorie der alternitiven Ringe*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg (1930) pp. 123–147.

7. Anton Suschkewitsch, *Über ein Elementen-system, für welche zwei Distributivgesetze gelten*, Kharkovski Matematichnovo Tobarictba, series 4, VII (1934) pp. 29–32.

8. A. Adrian Albert, *On a certain algebra of quantum mechanics*, Ann. of Math. vol. 35 (1934) pp. 65–73.

9. David G. Rabinow, *Independent sets of postulates for abelian groups and fields in terms of the inverse operations*, Amer. J. Math. vol. 59 (1937) pp. 211–224.

10. B. A. Hausmann and Oystein Ore, *Theory of quasigroups*, Amer. J. Math. vol. 59 (1937) pp. 983–1004.

11. Herbert Boggs and G. Y. Rainich, *Note on group postulates*, Bull. Amer. Math. Soc. vol. 43 (1937) pp. 81–84.

12. Alfred Tarski, *Ein Beitrag zur Axiomatik der Abelschen Gruppen*, Fund. Math. XXX (1938) pp. 253–256.

13. Raj Chandra Bose, *On the application of the properties of Galois Field to the problem of construction of hyper graeco Latin squares*, Sankhya, vol. 3 pt. 4 (1938) pp. 323–338.

14. B. A. Bernstein, *Postulates for abelian groups and fields in terms of non-associative operations*, Trans. Amer. Math. Soc. vol. 43 (1938) pp. 1–6.

15. D. C. Murdoch, *Quasigroups which satisfy certain generalized associative laws*, Amer. J. Math. vol. 61 (1939) pp. 509–522.

16. H. W. Norton, *The 7×7 squares*, Annals of Eugenics vol. 9 (1939) pp. 269–307.

17. W. L. Stevens, *The completely orthogonalized Latin squares*, Annals of Eugenics vol. 9 (1939) pp. 82–93.

18. E. L. Post, *Polyadic groups*, Trans. Amer. Math. Soc. vol. 48 (1940) pp. 208–350.

19. G. N. Garrison, *Quasigroups*, Ann. of Math. vol. 41 (1940) pp. 474–487.

20. D. C. Murdoch, *Note on normality in quasigroups*, Bull. Amer. Math. Soc. vol. 47 (1941) pp. 134–138.

21. ———, *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. vol. 49 (1941) pp. 392–409.

22. Koshichi Toyoda, *On axioms of linear functions*, Proc. Imp. Acad. Tokyo XVII (1941) pp. 221–227.

23. S. Lefschetz, *Algebraic topology*, Amer. Math. Soc. Colloquium Publications, vol. 27, New York, 1942.

24. I. M. H. Etherinton, *Non-associative arithmetics*, Proceedings of the Royal Society of Edinburgh vol. 62 (1943–1944) pp. 442–453.

25. Takasaki Mituhisa, *Abstractions of symmetric functions*, Tôhoku Math. J. vol. 49 (1943) pp. 145–207 (in Japanese).

26. R. H. Bruck, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 19–52.

27. G. N. Garrison, *A note on invariant complexes of a quasigroup*, Ann. of Math. vol. 47 (1946) pp. 50–55.

28. R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. vol. 60 (1946) pp. 245–354.

29. Grace E. Bates, *Free loops and nets and their generalizations*, Amer. J. Math. vol. 69 (1947) pp. 495–550.

30. Fred Kiokemeister, *A theory of normality for quasigroups*, Amer. J. Math. vol. 70 (1948) pp. 99–106.

31. J. Aczel, *On mean values*, Bull. Amer. Math. Soc. vol. 54 (1948) pp. 392–400.

32. Grace E. Bates and Fred Kiokemeister, *A note on homomorphic mappings of quasigroups into multiplicative systems*, Bull. Amer. Math. Soc. vol. 54 (1948)

33. A. C. Choudhury, *Quasigroups and nonassociative systems*. I, Bulletin of the Calcutta Mathematical Society (1948) pp. 183–194.

34. T. Evans, *Homomorphisms of non-associative systems*, J. London Math. Soc. vol. 24 (1949) pp. 254–260.

35. Marlow Sholander, *On the existence of the inverse operations*, Amer. J. Math. vol. 59 (1949) pp. 211–224.

36. B. Knaster, *Sur une equivalence pour les fonctions*, Colloquium Mathematicum, vol. II, Fasc. 1, 1949, pp. 1–4.

37. T. Evans, *A note on the associative law*, J. London Math. Soc. vol. 25 (1950) pp. 196–201.

38. Albert Sade, *Quasigroups*, Boulevard du Jardin-Zoologique 14, Marseilles, France, 1950.

39. Bourbaki, IV, premier partie, *Les structures fondamentales de l'analyse*, Livre II, *Algèbre*, Chapitre I, *Structures algébriques*, (1951).

40. G. Higman and B. H. Neumann, *Groups as groupoids with one law*, Publicationes Mathematicae, Tomus 2, Fasc. 3–4 1952.

41. M. Hosszu, *On the functional equation of autodistributivity*, Publicationes Mathematicae, Tomas 3, Fasc. 1–2, Debrecen, 1953, pp. 83–86.

42. Paul Dubreil, *Algèbre*, Tome I, Paris, 1954.

43. M. Hosszu, *Some functional equations related with the associative law*, Publicationes Mathematicae, vol. 3, Fasc. 3–4, Debrecen, 1954, pp. 205–214.

44. Orrin Frink, *Symmetric and self-distributive systems*, Amer. Math. Monthly vol. 62 (1955) pp. 697–707.

45. Harry Furstenberg, *The inverse operation in groups*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 991–997.

46. D. A. Norton and Sherman K. Stein, *An integer associated with Latin squares*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 331–334.

47. ———, *Cycles in algebraic systems*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 999–1004.

48. S. K. Stein, *Foundations of quasigroups*, Proc. Nat. Acad. Sci. U. S. A. vol. 42 (1956) pp. 545–546.

49. M. Hosszu, *On the functional equation of transitivity*, Acta Sci. Math. vol. 15 (1954) pp. 203–208.

UNIVERSITY OF CALIFORNIA,
DAVIS, CALIF.