CONTRIBUTIONS TO GENERAL ALGEBRA
Proceedings of the Klagenfurt Conference, May 25 – 28, 1978

J. D. H. Smith

FINITE EQUATIONALLY COMPLETE ENTROPIC QUASIGROUPS

1. Introduction.

There is a belief current that the concept of quasigroup is so loose that one cannot hope to talk about the structure of a general quasigroup. In part this is due to the formidable number of non-isomorphic quasigroups of a given order. The author's contention is that one should not be daunted by this bewildering variety, but should attack it steadily with the tools at one's disposal, developing these tools as one proceeds. The present paper provides an example of such an attack, using the universal algebra of [Sm] together with some elementary number theory to classify the finite equationally complete entropic quasigroups up to isomorphism and enumerate the plain ones of given order.

The universal algebra reduces the study of equationally complete $\underline{\underline{Z}}$-quasigroups to linear algebra (see [Sm,Theorem 536]). The restriction to entropic quasigroups, which already lie in the class $\underline{\underline{Z}}$, ensures that this linear algebra is commutative, and therefore easy. The linear algebra for the general case is more difficult (Problem 5.1): it thus seems wise to get the quasigroup theory sorted out in the easy case first so that one develops a feel for precisely which of the more difficult questions require answering. That is the purpose of this paper.

2. Equationally complete Mal'cev varieties.

This section summarises briefly the major results of [Sm] that are needed. A variety $\underline{\underline{T}}$ of algebras is called a Mal'cev variety iff there is a ternary operation $(x,y,z)P$ of $\underline{\underline{T}}$ such that $(x,y,y)P = x$ and $(x,x,z)P = z$

are laws in $\underline{\underline{T}}$: the members of such a variety are called Mal'cev algebras. If $\underline{\underline{Set}}_0$ is the variety of pointed sets, $\underline{\underline{T}} \boxtimes \underline{\underline{Set}}_0 = \underline{\underline{T}}_0$ is the variety of $\underline{\underline{T}}$-algebras with singleton subalgebra selected by a nullary operation of $\underline{\underline{T}}_0$, the morphisms of $\underline{\underline{T}}_0$ respecting these pointed singleton subalgebras. $\underline{\underline{Z}}(\underline{\underline{T}})$, also written $\underline{\underline{Z}}$ if $\underline{\underline{T}}$ is clear from the context, is the subvariety of $\underline{\underline{T}}$ consisting of those $\underline{\underline{T}}$-algebras A for which the diagonal $\hat{A} = \{ (a,a) \mid a \in A \}$ is a normal subalgebra of the direct square ^2A , i.e. a congruence class for a congruence on ^2A . $\underline{\underline{Z}}_0$ is thus [Sm,Theorem 418] the variety of abelian groups in the category $\underline{\underline{T}}$.

Varieties of $\underline{\underline{T}}$-algebras are partially ordered by inclusion, and all varieties contain the trivial variety generated by the one-element $\underline{\underline{T}}$-algebra. The minimal (non-trivial) varieties with respect to this partial ordering are called equationally complete, as are algebras generating such a variety. A $\underline{\underline{T}}$-algebra A is simple if its only congruences are $\hat{A}$ and ^2A , and plain if it is finite, simple, non-trivial, and its only subalgebras are singletons or improper. Equationally complete Mal'cev varieties containing a non-trivial finite algebra are just those generated by a plain algebra, with the finite algebras just being the direct powers of this plain algebra [Sm,Chapter 5].

3. Quasigroups and piques.

A quasigroup $(A,.,/,\backslash)$ is a set A with three binary operations . , / , \ called respectively multiplication, right division, and left division satisfying the identities

$$\left.\begin{aligned} (x.y)/y = x\ , \quad & x\backslash(x.y) = y\ , \\ (x/y).y = x\ , \quad & (x/y)\backslash x = y\ , \\ x.(x\backslash y) = y\ , \quad & y/(x\backslash y) = x \end{aligned}\right\} \qquad (3.1)$$

[Br,page 9]. These identities imply that for each x in A the mappings $R.(x): A \to A;\ y \mapsto y.x$ and $L.(x): A \to A;\ y \mapsto x.y$ are bijective, with $R.(x)^{-1}: A \to A;\ y \mapsto y/x$ and $L.(x)^{-1}: A \to A;\ y \mapsto x\backslash y$. The subgroup of the permutation group on A generated by all these mappings as x ranges through A is called the multiplication group $Mlt(A,.,/,\backslash)$ of $(A,.,/,\backslash)$. Quasigroups are Mal'cev algebras by virtue of the operation $(x,y,z)P = (x/(y\backslash y)).(y\backslash z)$. If A is finite, its quasigroup structure is specified entirely by the multiplication, so one omits reference to the divisions.

A quasigroup with an additional nullary operation selecting an idempotent e, a singleton subquasigroup $\{e\}$, is called a pointed idempotent quasigroup or pique. Defining the operations $+$, $\sim$, $\backsim$ on a pique $(A,.,/,\backslash,e)$ by

$$\left.\begin{aligned} x + y &= (x/e).(e\backslash y)\ , \\ x \sim y &= (x/(e\backslash y)).e\ , \\ x \backsim y &= e.((x/e)\backslash y) \end{aligned}\right\} \qquad (3.2)$$

makes $(A,+,\sim,\backsim,e)$ a loop, i.e. a quasigroup $(A,+,\sim,\backsim)$ with a two-sided identity element e such that $e+x = x = x+e$ are identities. $(A,+,\sim,\backsim,e)$ is called the corresponding loop or cloop of the pique $(A,.,/,\backslash,e)$. Let $R = R.(e)$, $L = L.(e)$. Then the pique operations may be recovered from R, L, and the cloop operations as follows:

$$\left.\begin{aligned} x.y &= xR + yL\ , \\ x/y &= (x \sim yL)R^{-1}\ , \\ x\backslash y &= (xR \backsim y)L^{-1} \end{aligned}\right\} \qquad (3.3).$$

The multiplication groups of the pique and its cloop are thus connected by the equations

$$\left.\begin{aligned} R.(x) &= RR_+(xL) \\ L.(x) &= LL_+(xR) \end{aligned}\right\} \qquad (3.4).$$

In particular, the multiplication group of the cloop is a subgroup of the multiplication group of the pique. The stabiliser of the pointed idempotent in the multiplication group of the pique $(A,.,/,\backslash,e)$ is called the inner mapping group $Inn(A,.,/,\backslash,e)$. The reason for this nomenclature is that the inner mapping group of a group is just the group of inner automorphisms. Note that R and L lie in the inner mapping group.

4. $\underline{\underline{Z}}$-piques.

If the pique $(A,.,/,\backslash,0)$ is in the class $\underline{\underline{Z}}$ (and thus in $\underline{\underline{Z}}_0$), the Structure Theorem for $\underline{\underline{Z}}$-algebras [Sm,Theorem 418 and page 8] implies that its cloop is an abelian group on which the pique's inner mapping group acts as a group of automorphisms. R_+ becomes an isomorphism between the cloop and its multiplication group, inducing the action

$$R^{-1}R_+(x)R = R_+(xR)$$
$$L^{-1}R_+(x)L = R_+(xL)$$

of R and L on $Mlt(A,+,0)$, and thus an action of all of $H = \langle R,L\rangle$, the subgroup of $Inn(A,.,/,\backslash,0)$ generated by R and L. By (3.4) the pique's multiplication group is seen to be the split extension of the abelian group $Mlt(A,+,0)$ with H having this action, and its inner mapping group is just H. The pique is specified completely via (3.3) by the H-module $(A,+,0)$ together with the choice of R and L as elements of H such that $\{R,L\}$ generates H. In particular:

Theorem 4.1. The free $\underline{\underline{Z}}$-pique on a set X has as underlying set the free module on X over the integral group algebra of the free group on $\{R,L\}$. O is the pointed idempotent, and the quasigroup operations are defined as follows:-

$$\left.\begin{aligned} x.y &= xR+yL \\ x/y &= xR^{-1}-yLR^{-1} \\ x\backslash y &= xRL^{-1}-yL^{-1} \end{aligned}\right\} \qquad (4.1).$$

Remark 4.2. $\underline{\underline{Z}}$-groups are abelian groups, i.e. modules over the ring of integers, and on this basis (finite) group theory is sometimes viewed as having number theory at its heart. Non-abelian groups consist of abelian groups combined in extremely intricate ways. Theorem 4.1 suggests an analogous approach to quasigroup theory as having group theory at its heart, with non-$\underline{\underline{Z}}$ quasigroups consisting of representation modules combined in yet more intricate ways.

Morphisms of $\underline{\underline{Z}}$-piques can be dealt with similarly. Let

$$\theta: (A,.,/,\backslash,O) \to (B,.,/,\backslash,O)$$

be a morphism of $\underline{\underline{Z}}$-piques, with L, R denoting left and right multiplications by O in A and M, S the corresponding multiplications in B. Then for all x, y in A, $(x.y)\theta = x\theta.y\theta$. Putting $y = O$ and $x = O$ respectively in this gives that

$$L\theta = \theta M \quad \text{and} \quad R\theta = \theta S \qquad (4.2)$$

as mappings from A to B. Also $(x+y)\theta = (xR^{-1}.yL^{-1})\theta = xR^{-1}\theta.yL^{-1}\theta = x\theta S^{-1}.y\theta M^{-1} = x\theta+y\theta$. Thus θ is a group morphism from the cloop of A to the cloop of B. Conversely such a group morphism satisfying (4.2) yields a pique-morphism.

5. Equationally complete $\underline{\underline{Z}}$-quasigroups.

By [Sm,522] an equationally complete plain $\underline{\underline{Z}}$-quasigroup $(A,.,/,\backslash)$ has an idempotent e. Thus $(A,.,/,\backslash,e)$ may be regarded as a pique. If f is also an idempotent of $(A,.,/,\backslash)$, [Sm,414] shows that there is an automorphism of the quasigroup $(A,.,/,\backslash)$ sending e to f, i.e. an isomorphism of the piques $(A,.,/,\backslash,e)$ and $(A,.,/,\backslash,f)$. One may thus fix attention on one idempotent, say e. Clearly $(A,.,/,\backslash,e)$ is a plain $\underline{\underline{Z}}$-pique. Suppose conversely that $(A,.,/,\backslash,e)$ is a plain $\underline{\underline{Z}}$-pique. If the subset B of A is a subquasigroup of $(A,.,/,\backslash)$, then [Sm,234] shows that B is a normal subquasigroup, determining a quasigroup congruence on A. The equivalence class of e under this congruence is a subpique of A, and so is either $\{e\}$ or A. This means that B is either singleton or A. Thus $(A,.,/,\backslash)$ is plain as a $\underline{\underline{Z}}$-quasigroup. The gist of all this is that the equationally complete plain $\underline{\underline{Z}}$-quasigroups are precisely the plain $\underline{\underline{Z}}$-piques, and so to classify equationally complete $\underline{\underline{Z}}$-quasigroups up to isomorphism it suffices to classify equationally complete $\underline{\underline{Z}}$-piques up to isomorphism.

Combining the considerations of Section 4 with those of [Sm, proof of 536], the cloop of a plain $\underline{\underline{Z}}$-pique A is an elementary abelian p-group for some prime p. Let P be the Galois field of order p. Then A, which by Section 4 is a $\mathbb{Z}H$-module for $H = \langle R,L \rangle$, is in fact an irreducible PH-module. The unary operations of the equationally complete variety generated by A form a ring T (under addition and composition) for which A is a faithful T-module. The centre of T is a field E of order p^b say, A is a vector space over E of finite

dimension a say, and T is the ring of a×a matrices over E . If I is the annihilator of the PH-module A , I is a two-sided primitive ideal of the group algebra PH , and PH/I is isomorphic to T . Regarding the elements of H as matrices, the elements of PH are formal P-linear sums of matrices, and I consists of those formal P-linear sums which give the zero matrix when "worked out" - when evaluated in T . Classifying plain $\underline{\underline{Z}}$-piques in general thus comprises the following problem (of K-theory or modular representation theory):

Problem 5.1. Let p be a prime, and a , b positive integers. Let P , E be the Galois fields of orders p , p^b respectively. Classify all pairs of invertible a×a matrices L , R over E such that the quotient of the group algebra P<L,R> by the ideal consisting of elements which sum to zero as matrix sums is isomorphic to the full ring of a×a matrices over E .

6. Equationally complete entropic quasigroups.

Entropic quasigroups are quasigroups in the variety of quasigroups: they satisfy the entropic law

$$(x.y).(z.t) = (x.z).(y.t) \qquad (6.1).$$

Mathematically they are quite amenable objects, but they do present one major problem which requires clarification - what to call them. The name "entropic" avoids any possible confusion, and is of many years' standing [Et,page 444]. However, the terms "Abelian" [M1], "abelian" [M2], "bisymmetric" [Ac], "alternation" [Sh], "symmetric" [Fr], "medial" [St], and "surcommutative" [So] have also been

used. Some disadvantages of "abelian", with or without an upper case "A", have been discussed in [Sm,318]. "Surcommutative" also avoids confusion, but is too much of a mouthful, especially when anglicised correctly to "supercommutative". Soublin uses "medial" with a different sense and then relates it to "surcommutativity" [So, Chapitre II]. Stein uses "abelian" with yet another meaning and then relates it to "mediality" [St,III]. All in all it seems advisable to adopt "entropic" which is untainted by these confusions.

As Murdoch has remarked [M1,page 517] [M2,1.4] all subquasigroups of an entropic quasigroup are normal. [Sm, 234] then implies that entropic quasigroups are $\underline{Z}$-quasigroups. If $(A,.,/,\backslash,e)$ is an entropic pique, setting e for x, y, t in (6.1) gives that $zRL = zLR$. Conversely, given two commuting automorphisms R, L of an abelian group $(A,+,0)$, equations (4.1) define an entropic pique structure $(A,.,/,\backslash,0)$. For example,

$$\begin{aligned}(x.y).(z.t) &= (xR+yL)R+(zR+tL)L\\ &= xR^2+yLR+zRL+tL^2\\ &= xR^2+zLR+yRL+tL^2 = (x.z).(y.t)\ .\end{aligned}$$

One may thus restate Murdoch's Second Structure Theorem [M2, Theorem 8] as an analogue of Theorem 4.1 with "free commutative group" replacing "free group".

Turning now to plain entropic piques, this commutativity greatly simplifies the difficulties encountered in Section 5 for general plain $\underline{Z}$-piques. In terms of Remark 4.2 it enables one to by-pass the group theory and get straight to the number theory. If R and L commute mutually then the group H they generate is abelian. This means that the group algebra PH, along with

all its quotients, is commutative. In particular the $a \times a$ matrix algebra T over the Galois field E of order p^b is commutative, so $a = 1$, $T = E$, and the abelian group $(A,+,0)$ is the underlying abelian group of the field E. R and L lie in T, i.e. in E, and so each is a multiplication by a non-zero element of E. The group H is thus a subgroup of the multiplicative group $E^\times$ of non-zero elements of E. $E^\times$ is cyclic, so H must be also, say with generator h. If the field extension $P(h)$ of the prime field P by h is a proper subfield F of E then $(F,.,/,\backslash,0)$ with operations defined by (4.1) is a proper subpique of A, contradicting the plainness. Thus $P(h) = E$: every element of E can be expressed as a polynomial function of h of degree less b with coefficients in P.

Suppose M, S is another pair of left, right multiplications by 0 yielding a pique on A isomorphic to that from L and R. Then by the considerations at the end of Section 4 there is an automorphism θ of A as a P-vector space conjugating L to M and R to S. h^θ is an element of $E^\times$ having the same multiplicative order as h, and so must be a power h^t of h. Let e, f be general elements of E, say

$$e = \sum_{i=0}^{b-1} e_i h^i$$

with the e_i in P. Then for all x in E,

$$(xe)\theta = \Big(\sum_{i=0}^{b-1} xe_i h^i\Big)\theta = \sum_{i=0}^{b-1} xe_i \theta h^{ti}$$

$$= \sum_{i=0}^{b-1} (x\theta)e_i h^{ti} = (x\theta)e^\theta$$

where $e^\theta = \sum_{i=0}^{b-1} e_i h^{ti}$. The mapping $e \mapsto e^\theta$ is P-linear,

and $1^\Theta = 1$. Also $(x\Theta)(ef)^\Theta = (xef)\Theta = (xe\Theta)f^\Theta = (x\Theta)e^\Theta f^\Theta$. Thus Θ is an automorphism of E over P . Conversely for any element Θ of the Galois group G of E over P the conjugates L^Θ and R^Θ yield a pique structure on A isomorphic to that from L and R . Thus in classifying the piques up to isomorphism one classifies the pairs (L,R) such that $P(L,R) = E$ up to conjugacy under the Galois group with pointwise action Θ: $(L,R) \mapsto (L^\Theta, R^\Theta)$.

The Galois group G is cyclic of order b , generated by the Frobenius automorphism, the P-automorphism of E which sends each element to its p-th power [Co, Section 5.7]. Let Θ in G have order c , a factor of b . By the main theorem of Galois theory [Co, Section 5.5] the fixed points of Θ acting on E form a subfield $GF(p^{b/c})$ with $p^{b/c}$ elements. Now a pair (L,R) in the direct square ^2E of E will generate a proper subfield $P(L,R)$ of E iff $(L,R) \in {}^2GF(p^d)$ for some $d < b$, $d \mid b$. Thus the Galois group G acts fixed point free on the set $X = {}^2E - \bigcup_{d<b,\, d\mid b} {}^2GF(p^d)$ of pairs (L,R) with $P(L,R) = E$. If $|X| = x$, Burnside's Lemma [Bu,Satz 2.1] shows that X breaks up into x/b orbits under the pointwise action of G . Thus to enumerate the isomorphism classes it suffices to specify x . Let $n(d)$ be the number of pairs in $^2GF(p^d)$ not lying in the direct square of any proper subfield of $GF(p^d)$, so that $x = n(b)$. Then

$$|{}^2E| = p^{2b} = \sum_{d\mid b} n(d) \ .$$

The Möbius inversion formula [Co,Section 2.3] then yields

$$x = n(e) = \sum_{d\mid b} p^{2d}\mu(b/d) \ .$$

All this can be summarised as

Theorem 6.1. Finite equationally complete entropic quasigroups are direct powers of (the underlying quasigroup of) a plain entropic pique of prime power order. The isomorphism classes of plain entropic piques of order p^b are in 1-1 correspondence with the orbits of the Galois group of E over P on the set of pairs (L,R) of elements of E such that $E = P(L,R)$, the orbit containing (L,R) corresponding to the isomorphism class of $(E,\circ)$ with $x\circ y = xR+yL$. Altogether there are

$$\frac{1}{b} \sum_{d|b} p^{2d} \mu(b/d)$$

isomorphism classes of plain entropic piques of order p^b.

References.

[Ac] J. Aczél, On mean values, Bull. Amer. Math. Soc. 54 (1948), 392 - 400.

[Br] R. H. Bruck, A Survey of Binary Systems, Springer, Berlin, 1971.

[Bu] N. G. de Bruijn, in K. Jacobs (ed.), Selecta Mathematica III, Springer, Berlin, 1971.

[Co] P. M. Cohn, Algebra Vol. 2, John Wiley, London, 1977.

[Et] I. M. H. Etherington, Non-associative arithmetics, Proc. Roy. Soc. Edin. 62 (1949), 442 - 453.

[Fr] O. Frink, Symmetric and self-distributive systems, Amer. Math. Monthly 62 (1955), 697 - 707.

[M1] D. C. Murdoch, Quasigroups which satisfy certain generalized associative laws, Amer. J. Math. 61 (1939), 509 - 522.

[M2] D. C. Murdoch, Structure of abelian quasigroups, Trans. Amer. Math. Soc. 49 (1941), 392 - 409.

[Sh] M. Sholander, On the existence of the inverse operation in alternation groupoids, Bull. Amer. Math. Soc. 55 (1949), 746 - 757.

[Sm] J. D. H. Smith, Mal'cev Varieties, Springer Lecture Notes 554, Berlin, 1976.

[So] J.-P. Soublin, Étude algébrique de la notion de moyenne, J. Math. pures et appl. 50 (1971), 53 - 264.

[St] S. K. Stein, On the foundations of quasigroups, Trans. Amer. Math. Soc. 85 (1957), 228 - 256.

Jonathan D. H. Smith
TH Darmstadt, FB4 AG1
Schloßgartenstr. 7
D-61 Darmstadt