QUASIGROUPS AND CUBIC CURVES

by I. M. H. ETHERINGTON

(Received 7th September 1964)

PART I

1. Introduction

A note on this subject was read to the Edinburgh Mathematical Society in June 1951. Subsequently I had the benefit of conversations and correspondence with J. G. Brennan and I. R. Porteous, and substantial contributions from them are incorporated here, more than are acknowledged in detail below.

In Part II it is shown that algebraic structures of a certain type—totally symmetric entropic quasigroups—arise naturally in the geometry of points on plane cubic curves, and that many of the properties of these quasigroups, which are described in Part I, can be interpreted as theorems on cubics. The proofs of a few facts mentioned in Part I which depend on the use of an abelian group isotopic to the quasigroup are postponed to Part III. Use of this abelian group for geometry on a cubic is well known, but the quasigroup has certain advantages in the simplicity, naturalness and compactness of the notation which it provides.

It is hardly to be expected that any essentially new properties of cubic curves would be discovered thus. On the other hand the geometrical interpretation is very suggestive in the study of totally symmetric entropic quasigroups, and attention will be mainly directed to algebraical properties which were in fact thus suggested. Proving them involves a gain in generality, since it is not the case that every such quasigroup can be interpreted as a set of points on a cubic.

The reader may find it convenient to read Part II alongside Part I.

2. Commutative entropic groupoids

A *groupoid* is a set of elements closed with respect to multiplication, which need not be commutative or associative. To avoid multiplicity of brackets let it be understood that a dot separates factors whose multiplication is to be delayed; e.g. $(ab \,.\, cd)e \,.\, fg$ means $[\{(ab)(cd)\}e](fg)$.

A groupoid is *entropic* if identically

$$ab \,.\, cd = ac \,.\, bd. \tag{2.1}$$

An immediate consequence of (2.1) is

$$(ab)^2 = a^2b^2. \tag{2.2}$$

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

It can be shown inductively from the entropic law (2.1) (**17**, **11**) that if a^N, a^M denote particular nonassociative powers of a, then

$$(ab)^N = a^N b^N, \quad (a^M)^N = (a^N)^M. \tag*{(2.3) (2.4)}$$

(2.3) asserts that powers are endomorphisms of the groupoid. For example, $a^{2\cdot 2+1}$ denotes $a^2a^2 \,.\, a$, and (2.3) asserts that $(ab)^{2\cdot 2+1} = a^{2\cdot 2+1}b^{2\cdot 2+1}$. (2.4) has been called the *palintropic* law (**10a**, **10**, **11**).

If the groupoid is commutative as well as entropic, then

$$ab \,.\, cd = ac \,.\, bd = ad \,.\, bc; \tag*{(2.5)}$$

in fact $ab \,.\, cd$ is a symmetric function of a, b, c, d, being equal to each of the 24 products derived by permuting the letters. We have indeed a sequence of symmetric functions

$$\text{(i) } ab, \quad \text{(ii) } ab \,.\, cd, \quad \text{(iii) } (ab \,.\, cd)(ef \,.\, gh), \; \ldots. \tag*{(2.6)}$$

3. Totally symmetric quasigroups

A groupoid is a *quasigroup* if division on either side is always possible and unique. Thus if any two of a, b, c are given elements of a quasigroup, $ab = c$ determines the third uniquely as an element of the quasigroup. The cancellation properties follow: $ab = ac$ and $ba = ca$ each imply $b = c$. Also the property of homogeneity: any element c is expressible as a product ab.

A groupoid is *totally symmetric* (t.s.) and is necessarily a quasigroup if any relation $ab = c$ between its elements implies all six of the relations derived by permuting a, b, c. Immediate consequences are the identities

$$ab = ba \tag*{(3.1)}$$

$$ab \,.\, b = a, \quad b \,.\, ba = a. \tag*{(3.2)}$$

The two laws (3.2) together imply the commutative law (3.1) thus:

$$ab = \{(ba) \,.\, (ba)a\}b = \{(ba) \,.\, b\}b = ba,$$

and the t.s. property is then also deducible. Thus a t.s. quasigroup can be defined as a groupoid obeying any two of the three identities (3.1), (3.2).

4. Historical remarks

Murdoch (**17**, **18**) and Bruck (**6**) called quasigroups with the property (2.1) *abelian* and studied their structure and their relation through isotopy to abelian groups, of which they are a generalisation. But " abelian " is also used by writers on quasigroups to mean " commutative ", and it does not seem an appropriate word for the property (2.1) generally. The name *entropic* was introduced in (**10**). Other names which have been applied to this property are *bisymmetric* (Aczél, **1**, **2**), *alternation* (Sholander, **27**), *symmetric* (Frink, **14**), *medial* (Stein, **28**).

T.s. quasigroups are included in " quasigroups with the inverse property " and were studied in this context by Bruck (**6**). For other results and literature on both entropic and t.s. quasigroups considered separately see Stein (**28**),

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

Sade (**22**). More recent studies relevant to the entropic law are by Minc (**16**), Evans (**13**), Aczél, Belousov and Hosszú (**3**), Osborn (**20**).

The identities (3.2) have been called the right and left laws of keis, the name *kei* (Japanese, pronounced kay, meaning " system ") having been given by Takasaki (**31**) to idempotent self-distributive systems obeying one of these laws. (The MR abstract of (**31**) indicates that entropic keis are discussed in this paper, which I am not able to read.)

5. Totally symmetric entropic quasigroups

Henceforward we shall be concerned with quasigroups which are both totally symmetric and entropic (t.s.e.q.'s). In a t.s.e.q. all the properties mentioned in §§ **2**, **3** hold. We begin with some examples.

A group is a quasigroup, entropic if and only if it is abelian, totally symmetric if and only if every element other than the identity is of period 2. Hence follows the result (a refinement of Bruck's Lemma 10; (**6**), p. 38):

Example 1. *A finite group is a t.s.e.q. if and only if it is the trivial group or is a direct power of the cyclic group C_2. Its order is then* 1 *or a power of* 2.

A t.s.e.q. can be constructed from any abelian group written additively by choosing a fixed element k and defining products by

$$ab = k-a-b. \tag{5.1}$$

Two such multiplication tables for residues mod. 3 are given below for subsequent reference. Example 2 ($k = 0$) shows a quasigroup in which every element x is idempotent (i.e. satisfies $x^2 = x$); such a quasigroup is called *idempotent*. On the other hand Example 3 ($k = 1$) has no idempotents, but each element satisfies $((x^2)^2)^2 = x$.

Example 2.

	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Example 3.

	0	1	2
0	1	0	2
1	0	2	1
2	2	1	0

The quasigroup of Example 2 will be denoted Q_3.

It is shown in § **19** that every t.s.e.q. can be obtained by the construction (5.1) from a suitable abelian group.†

Notation. In the remainder of Part I it is assumed where not always stated explicitly that small italic letters a, b, ... denote elements of a t.s.e.q. Q, except for m, n, r, s which are positive integers.

† This is a special case of Bruck's form (**6**, Theorems 1, 11, 12) of Murdoch's result (**18**, Theorem 11) that every entropic quasigroup is isotopic to an abelian group. At the same time it is a special case of Bruck's construction (**6**, Theorem 3 and Theorem 7, Corollary 2) of certain inverse property quasigroups and t.s. quasigroups from groups. (At the end of the Corollary quoted, (53) would seem to be a misprint for (52).)

Sade (**21**, No. 72; **22**, p. 171) discusses the construction (5.1) and calls quasigroups so constructed *anticyclic*.

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

6. Symmetries

See (**12**) for a different treatment of the subject of this Section, leading to an equivalent but differently expressed general formulation.

Consider a t.s.e.q. Q. We have symmetric functions as in (2.6), and symmetric equations such as

$$\text{(i) } ab = c, \quad \text{(ii) } ab \, . \, cd = ef, \quad \text{(iii) } (ab \, . \, cd)(ef \, . \, gh) = ij \, . \, kl, \ldots \tag{6.1}$$

(symmetric in the sense that they are invariant under any permutation of the elements involved). For example, (ii) is by the symmetry of its left side symmetric in a, b, c, d; and since by the t.s. law we can exchange cd with ef, it is symmetric in a, b, e, f and hence in a, b, c, d, e, f.

From these symmetries a host of others can be deduced. Thus (ii) can be rewritten

$$(ab \, . \, cd)e = f \tag{6.2}$$

which is therefore also a symmetric equation. Consequently the left side

$$(ab \, . \, cd)e \tag{6.3}$$

is a symmetric function. From this it follows that

$$(ab \, . \, c)d \text{ is symmetric in } a, b, d; \tag{6.4}$$

for by a quasigroup property c can be factorised into c_1c_2 and the product is then symmetric in a, b, c_1, c_2, d.

From the symmetry of (6.3) and (2.6, iii) it follows that the equation

$$(ab \, . \, cd)(ef \, . \, gh) = i \tag{6.5}$$

is symmetric in all the nine letters involved; for it is symmetric in a, b, c, d, e, f, g, h, and since it can be written $(ab \, . \, cd)i = ef \, . \, gh$ it is symmetric in a, b, c, d, i.

The result (6.4) in the form of the identity

$$(ab \, . \, c)d = (ad \, . \, c)b \tag{6.6}$$

is a fundamental property of t.s.e.q.'s, being equivalent to the entropic law in the presence of total symmetry; it could be used in place of entropy in the definition. The following is an alternative derivation of (6.6) from (2.1), (3.1), (3.2):

$$(ab \, . \, c)d = (ab \, . \, c)(a \, . \, ad) = (ab \, . \, a)(c \, . \, ad) = b(c \, . \, ad) = (ad \, . \, c)b.$$

Conversely (6.6) with (3.1), (3.2) implies the entropic law thus (using (6.6) at the third step):

$$ab \, . \, cd = dc \, . \, ab = (b \, . \, bd)c \, . \, ab = (b \, . \, ab)c \, . \, bd = ac \, . \, bd.$$

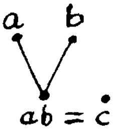
Let us now generalise these results and sum them up in the following rule, due essentially to I. R. Porteous. Let a nonassociative product be regarded as "descended from" its factors, which are thus placed on a "pedigree", or bifurcating root-tree. Examples are given below. Then (A) *two factors in a product may be exchanged if their altitudes in the tree have the same parity;* (B) *two factors on opposite sides of an equation may be exchanged if their altitudes*

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

have opposite parities. (Altitudes are counted upwards from the root, which has zero altitude.)

A formal proof could be given on the following lines. We use the homogeneous property of a quasigroup (§ 3) and the symmetry of the products (2.6) to show that factors at the *same* altitude can be exchanged. For example (see fig. 4), $\{(ab\,.\,cd)e\,.fg\}h$ is of the form $(xe\,.fg)h$, which can be expanded into $(xe\,.fg)(h_1h_2\,.\,h_3h_4)$ and is therefore symmetric in $ab\,.\,cd(=x)$, e, f, g, and these are its factors at altitude 3. Then (A) is established by repeated application of (6.4). We deduce (B) on similar lines, using the symmetry of equations (6.1) to exchange factors on opposite sides. I refrain from giving this in more detail in view of the fuller treatment already given in (**12**).

Fig. 1



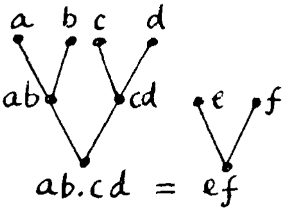


Fig. 2

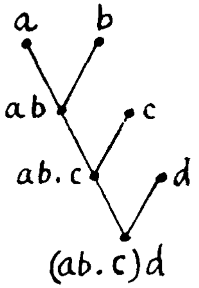


Fig. 3

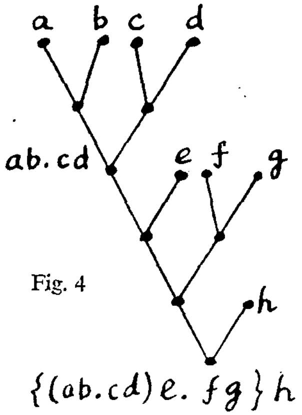


Fig. 4

FIG. 1.—The single element c is represented by the trivial tree consisting of a single vertex at zero altitude. Here a, b, c are permutable.

FIG. 2.—In the equation $ab.cd = ef$, a, b, c, d, e, f are permutable; so are ab, cd, ef; and $ab.cd$ can be exchanged with e or f.

FIG. 3.—In the product $(ab.c)d$, the factors a, b, d, are permutable; so is ab with c, and $ab\cdot c$ with d.

FIG. 4.—The product represented is symmetric in all eight letters. It is in fact identical with the symmetric function (2.6 iii); for we can interchange h with $ab.cd$, so that

$$\{(ab.cd)e.fg\}h = (he.fg)(ab.cd) = (ab.cd)(ef.gh). \tag{6.7}$$

7. Idempotents

If we have $i^2 = i, j^2 = j, i \neq j$, then by (2.2)

$$(ij)^2 = i^2j^2 = ij.$$

Also ij is distinct from i and j, e.g. $ij = i = i^2$ would imply $j = i$. Thus the product of two idempotents is a third idempotent.

It follows that the set of idempotents of Q, if any exist, is closed under multiplication and forms an idempotent subquasigroup Q_0.

Q may have no idempotents, or just one (§ 5, Examples 3, 1). If it has two, then it has a third as above, and the three idempotents i, j, ij form a subquasigroup isomorphic to Q_3 (Example 2).

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

If there is a fourth idempotent k, then we can deduce the existence in Q of nine idempotents

$$i,\ j,\ k,\ jk,\ ki,\ ij,\ i\,.\,jk,\ j\,.\,ki,\ k\,.\,ij. \tag{7.1}$$

This set is closed under multiplication. We have for example using (2.5)

$$(ij)(ki) = ii\,.\,jk = i\,.\,jk, \text{ hence } (ij)(i\,.\,jk) = ki; \tag{7.2}$$

and using (6.6)

$$i(j\,.\,ki) = k(j\,.\,ii) = k\,.\,ij, \text{ hence } (j\,.\,ki)(k\,.\,ij) = i. \tag{7.3}$$

Thus the nine idempotents form an idempotent t.s.e. sub-q., which is in fact isomorphic to the direct square † $Q_3 \times Q_3$.

Generally, it is shown in § **21** that an idempotent t.s.e.q. Q_0 of finite order $n_0 > 1$ is a direct power $Q_3 \times Q_3 \times \ldots$. Hence the number of idempotents in Q, if finite, is 0, 1 or a power of 3.

Suppose that Q is of finite order n and contains n_0 idempotents. Then of the n^2 entries in its complete multiplication table, n_0 are of the form $i^2 = i$, and the rest occur either in threes ($a^2 = b$, $ab = a$, $ba = a$) or in sixes ($ab = c$, etc.). Hence $n^2 - n_0 \equiv 0 \pmod{3}$. Assuming that the possible values for n_0 are as stated above 0, 1, 3, 9, 27, ..., it follows that

$$\left.\begin{array}{lll} \textit{either} & n \equiv 0 \ (\text{mod. } 3), & n_0 = 0, 3, 9, 27, \ldots, \\ \textit{or} & n \not\equiv 0 \ (\text{mod. } 3), & n_0 = 1. \end{array}\right\} \tag{7.4}$$

8a. Associative triples

Although multiplication is nonassociative, it can happen that $ax\,.\,b = a\,.\,xb$ for particular elements a, x, b in a t.s.e.q. We have identically

$$ax\,.\,b = ax\,.\,b^2b = ab^2\,.\,xb, \quad a\,.\,xb = aa^2\,.\,xb.$$

These are equal if and (by cancellation) only if $a^2 = b^2$. Thus:

$$\left.\begin{array}{r} a^2 = b^2 \Rightarrow ax\,.\,b = a\,.\,xb \ (x \text{ arbitrary}); \\ ax\,.\,b = a\,.\,xb \Rightarrow a^2 = b^2,\ ay\,.\,b = a\,.\,yb \ (y \text{ arbitrary}). \end{array}\right\} \tag{8.1}$$

8b. Generalisation

The following gives a generalisation and at the same time indicates an alternative proof of (8.1).

Suppose $ax\,.\,d = bx\,.\,c$. Then $(ax\,.\,d)y = (bx\,.\,c)y$, where y is arbitrary. By (6.6) this implies $(ay\,.\,d)x = (by\,.\,c)x$, and hence $ay\,.\,d = by\,.\,c$. So $ax\,.\,d = bx\,.\,c$ holds for arbitrary x if it holds for any particular x. Taking $x = c$, we see that a necessary and sufficient condition for this is $ac\,.\,d = b$,

† The direct product $P \times Q$ of two quasigroups is defined as the set of all couples (p, q) with p in P, q in Q, with the multiplication rule $(p, q)(p', q') = (pp', qq')$. It is a quasigroup. The above mentioned isomorphism with $Q_3 \times Q_3$ is exhibited by the change of notation

$$\begin{bmatrix} i & j & ij \\ k & i.jk & j.ki \\ ki & k.ij & jk \end{bmatrix} \rightarrow \begin{bmatrix} i_{00} & i_{01} & i_{02} \\ i_{10} & i_{11} & i_{12} \\ i_{20} & i_{21} & i_{22} \end{bmatrix}.$$

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

or $ac = bd$. Thus:

$$\left.\begin{aligned} ac = bd \Rightarrow ax\,.\,d = bx\,.\,c \text{ (x arbitrary)}; \\ ax\,.\,d = bx\,.\,c \Rightarrow ac = bd,\ ay\,.\,d = by\,.\,c \text{ (y arbitrary)}. \end{aligned}\right\} \tag{8.2}$$

8c. Further generalisation

In (8.2) $ax\,.\,d = bx\,.\,c$ may be written $((ax\,.\,d)c)b = x$, and the result can be generalised further as follows. Suppose that

$$(\ldots((xa_{2m})a_{2m-1})a_{2m-2}\ldots)a_1 = x. \tag{8.3}$$

In the tree for the product on the left the factor a_r appears at altitude r. Hence by rule (B) of § **6**, x on the right (at zero altitude) can be exchanged with a_{2m-1} on the left. By (3.2) the two factors x then cancel each other, or both can be replaced by y's. Thus (8.3) *holds for arbitrary x if it holds for any particular x; and a necessary and sufficient condition for this is that the product on the left with x and a_{2m-1} omitted should equal a_{2m-1}*.

(8.3) can be written in other forms by transferring the factors one at a time to the right. Case (a) is given by $m = 2$, $a_4 = a_2 = a$, $a_3 = a_1 = b$.

(§ **8** and its interpretation in § **15** are due to suggestions by J. G. Brennan.)

9. Square roots

By (2.2) the product of two squares is a square. Thus those elements of Q which are squares form a non-null subquasigroup † Q_1, of order say n_1. These n_1 elements all have in Q the same number s of square roots; and if the order n of Q is finite

$$n = n_1 s. \tag{9.1}$$

For suppose

$$a_1^2 = \ldots = a_s^2 = p, \quad b^2 = q$$

where $a_1, \ldots, a_s$ are distinct. Then

$$(a_\alpha\,.\,a_\beta b)^2 = a_\alpha^2\,.\,a_\beta^2 b^2 = p\,.\,pq = q.$$

With β fixed and $\alpha = 1, \ldots, s$, this gives s distinct square roots $a_\alpha\,.\,a_\beta b$ of q. So q has at least as many square roots as p, and vice versa. $n = n_1 s$ follows at once.

[In view of (2.3) there are similar theorems concerning Nth powers and roots. The same theorems for abelian groups are proved similarly by considering $(a_\alpha a_\beta^{-1} b)^N$.]

If $s \geqq 2$ the result (8.1) applies. Consider now the case when an element p is known to have three distinct square roots a, b, c:

$$a^2 = b^2 = c^2 = p. \tag{9.2}$$

† Those elements of Q_1 which are squares of elements of Q_1 form a subquasigroup Q_2, and so on. In view of the identity $aa^2 = a$ (consequence of (3.2)), this sequence of subquasigroups coincides here with the sequence of " right unit subquasigroups " which figures in Murdoch's analysis (**18**) of the structure of entropic quasigroups.

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

By (8.1) their product is associative:

$$ab\,.\,c = a\,.\,bc = b\,.\,ac = d \text{ (say)} \tag{9.3}$$

and $$d^2 = a^2b^2\,.\,c^2 = pp\,.\,p = p.$$

From (9.3) $$ab = cd,\ ac = bd,\ ad = bc. \tag{9.4}$$

Also a, b, c, d are distinct, e.g. $d = a$ would by (9.4) imply $b = c$.

Thus if p has three square roots it has four, related as in (9.4).

It may be shown in the same way that if p has a fifth square root e, then it has three more f, g, h ($= ab\,.\,e$, $ac\,.\,e$, $ad\,.\,e$), making 8 square roots, which satisfy 7 ($= 2^3 - 1$) sets of relations such as $ab = cd = ef = gh$.

This suggests that s, the number of square roots of any square, is always if finite 1 or a power of 2. This is proved very easily in the next Section on the assumption that Q contains an idempotent, and is proved generally in § **20**. Assuming this it follows from (9.1) that if Q is finite and of odd order, $s = 1$, i.e. every element of Q has one and only one square root.

10. Square roots of idempotents

Suppose that Q contains an idempotent i, and that

$$a^2 = b^2 = \ldots = i^2 = i.$$

Since $a^2 = i$, $b^2 = i$ imply $(ab)^2 = i$, the set of square roots of i (including i) is closed under multiplication and forms a subquasigroup Q_i of Q. By (8.1) Q_i is an associative quasigroup, i.e. a group, in which i being idempotent is the unit element and every other element has period 2. Hence Q_i if finite either consists of i only or is the group $C_2 \times C_2 \times \ldots$ mentioned in Example 1; and then s, the number of square roots of i or of any other square in Q, is 1 or a power of 2. It follows also that the quasigroups Q_i, Q_j associated with different idempotents are isomorphic.

If a, b are square roots of different idempotents, say

$$a^2 = i^2 = i, \quad b^2 = j^2 = j,$$

then $(ab)^2 = a^2b^2 = ij$, so that ab is a square root of a third idempotent ij (cf. § **7**). Thus the square roots of idempotents of Q, including the idempotents themselves, form a subquasigroup. It is not difficult to show that this subquasigroup is isomorphic with the direct product $Q_0 \times Q_i$, where Q_0 is the quasigroup of idempotents (which if finite either consists of a single element i or is a direct power of the quasigroup Q_3 of Example 2), and Q_i is the group of square roots of one idempotent i (which if finite either consists of a single element i or is as above a direct power $C_2 \times C_2 \times \ldots$).

For example, $Q_3 \times Q_3 \times C_2 \times C_2$ is a t.s.e.q. of order 36 containing 9 idempotents and 27 other square roots of idempotents.

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

PART II

11. Quasigroups on a cubic curve

Let C denote a non-degenerate plane cubic curve with the double point if any omitted. Let $a, b, \ldots$ be points of C. Let multiplication be defined by the *chord and tangent process*: ab is the third point in which the chord joining a and b meets C, coinciding with a or b if the chord is tangent there; a^2 is the tangential of a, the point where the tangent at a meets C again.

Collinearity of a, b, c (points of C) is thus expressed by writing $ab = c$, or equally $ac = b$, etc. With multiplication thus defined the totality of points of C, or any subset closed under the chord and tangent process, forms a totally symmetric quasigroup Q. Let it be emphasised that, here and throughout Part II, Q may be the whole of C or may be some infinite or finite subset closed under multiplication.

Given four points a, b, c, d of C, consider the eight points $a, b, c, d, ab, cd, ac, bd$. They all lie on C and on each of two degenerate cubics C_1, C_2 as indicated schematically in fig. 5. Now it is well known that all cubics, including degenerate cubics, through eight points have a ninth common point; hence

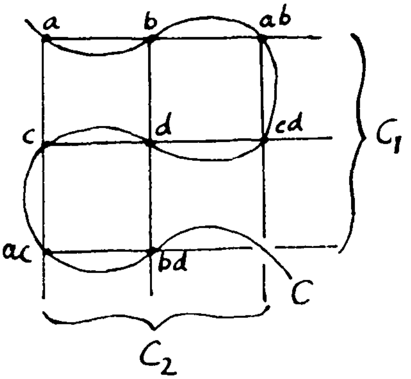


Fig. 5

$$ab \, . \, cd = ac \, . \, bd. \qquad (11.1)$$

The figure is drawn with the eight points distinct. However if there are coincidences among them the result (11.1) is either trivial (for example if $a = d$ or if $a = bd$), or holds in virtue of some special case of the theorem quoted (for example if $a = b$ or $a = ab$). The totally symmetric quasigroup Q is therefore also entropic.

An important such special case is (2.2):

$$(ab)^2 = a^2b^2, \qquad (11.2)$$

which is the theorem concerning the satellite of a line: the tangentials a^2, b^2, $(ab)^2$ of three collinear points a, b, ab are collinear. A generalisation of this

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

theorem is given by (2.3). The mapping $a \to a^N$ represents a chord and tangent construction leading from a point a of C to a "generalised tangential" a^N, and (2.3) asserts that such a construction maps three collinear points a, b, ab on three collinear points a^N, b^N, $(ab)^N$. (2.4) asserts that any two such constructions commute.

12. Interpretation of the symmetric properties (cf. § 6)

The identity $(ab \,.\, c)d = (ad \,.\, c)b$ of (6.6) has the same geometric content as the entropic law (11.1), as may be seen by relabelling fig. 5 thus:

$$\begin{array}{ccccccccc} & a, & b, & ab, & c, & d, & cd, & ac, & bd \\ \to & a, & ab, & b, & ad, & c, & ad\,.\,c, & d, & ab\,.\,c. \end{array}$$

The symmetry of the relation (6.1, ii) $ab \,.\, cd = ef$ in the six points a, b, c, d, e, f is explained as follows. It asserts in the first place that the points ab, cd, ef lie on a line L. Consider the conic S through five of the six points. Then the nine points

$$a, \quad b, \quad c, \quad d, \quad e, \quad f, \quad ab, \quad cd, \quad ef$$

lie on the cubic C and also on the degenerate cubic which consists of the three lines

$$(a, b, ab), \quad (c, d, cd), \quad (e, f, ef);$$

and eight of these points lie on the degenerate cubic (S, L). It follows that S passes through the remaining point. Thus the equation

$$ab \,.\, cd = ef \tag{12.1}$$

asserts that a, b, c, d, e, f are the six points of intersection of C with a conic.

Further, (12.1) and the symmetry involved indicate that the 15 points such as ab are collinear in threes (such as ab, cd, ef) on 15 lines such as L, one line corresponding to each syntheme (or way of separating a, b, c, d, e, f into three pairs); and the 15 lines concur in threes [such as (ab, cd, ef), (ab, ce, df), (ab, cf, de)] in the 15 points. The figure is well known.

The symmetric equation $(ab \,.\, cd)e = f$ says the same as $ab \,.\, cd = ef$, and hence the symmetric function $(ab \,.\, cd)e$ denotes the sixth point in which the conic (a, b, c, d, e) meets C. By its structure $(ab \,.\, cd)e$ prescribes a linear construction for this sixth point; in fact because of the symmetry it affords $5 \times 3 = 15$ such constructions.

Suppose a, b, c, d in (12.1) kept fixed while e, f vary. We conclude: If a variable conic S be drawn through four fixed points a, b, c, d of C, then the chord joining the two remaining intersections of S with C passes through a fixed point, namely $ab \,.\, cd$. This point is called (**24**, p. 134) the *coresidual* of a, b, c, d and interprets the symmetric function $ab \,.\, cd$. Since

$$ab \,.\, cd = ac \,.\, bd = ad \,.\, bc,$$

we have three linear constructions for it.

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

As in (2.6, iii), $(ab\,.\,cd)(ef\,.\,gh)$ denotes a ninth point symmetrically determined by the eight points a, b, c, d, e, f, g, h; and as in (6.5) all nine points are symmetrically related. The interpretation can be found by means of the theory of residuation (**24**, pp. 136-140). The four points ab, cd, ef, gh form a set residual on C to the eight given points; hence $ab\,.\,cd$, $ef\,.\,gh$ form a set coresidual to the eight points; and finally $(ab\,.\,cd)(ef\,.\,gh)$ is a single point residual to the eight points. It must therefore coincide with the ninth point in which any cubic through the eight points cuts C.

Equation (6.5) therefore asserts that $a, b, c, d, e, f, g, h, i$ are the nine points of intersection of C with some other cubic. (6.7) gives another expression for the ninth associated point.

It may be shown similarly that (6.1, iii):

$$(ab\,.\,cd)(ef\,.\,gh) = ij\,.\,kl \tag{12.2}$$

is the condition that the 12 points involved should be the complete intersection of C with a quartic. (The argument uses first the fact that this equation is the condition for a conic to pass through the six points ab, cd, ef, gh, ij, kl, and hence for the sets $\{ab, cd, ef, gh\}$ and $\{ij, kl\}$ to be residual to each other.)

13. Flexes (cf. § 7)

An idempotent of Q is a flex of the curve. In § 7 we have shown in effect that if there are two flexes then there is a third collinear with them. If there is a fourth flex, then there are nine flexes lying by threes on twelve lines, namely the six lines which are apparent in the notation (7.1) and six more which follow from equations such as (7.2), (7.3).

If there is a tenth flex, we can show similarly that there are 27 lying on 117 lines, and so on. Actually this does not occur on a cubic: the total number of flexes on a cubic is in fact 1, 3 or 9 according as the cubic is cuspidal, nodal or nonsingular.

The last paragraph of § 7 gives information about the possible number n_0 of flexes in a finite set of n points of C, closed with respect to the chord and tangent process.

14. Some theorems

A sextactic point of C is by definition a point a at which some (non-degenerate) conic has 6-point contact. By (12.1) a is such a point if and only if $a^2a^2 = a^2$ $(a^2 \neq a)$, that is if a^2 (and not a) is a flex. Hence the sextactic points of C are the points of contact of tangents from flexes (excluding the flexes themselves).

If two points a, b of C are collinear with a flex (i.e. if ab is a flex), then there is a conic which osculates C at a and at b, and conversely. For these two properties are different ways of interpreting the same condition $ab\,.\,ab = ab$.

Similarly using (12.2) and interpreting in two ways the condition

$$(ab\,.\,cd)(ab\,.\,cd) = ab\,.\,cd,$$

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

we have the theorem: There exists a quartic which osculates C at each of four given points of C if and only if the coresidual of the four points is a flex. Since the condition can also be written $a^2b^2 \, . \, c^2d^2 = ab \, . \, cd$, the coresidual of the tangentials of the four points is the same flex.

The following are generalisations of the theorem concerning the satellite of a line. By repeated application of (11.2),

$$ab \, . \, cd = ef \Rightarrow a^2b^2 \, . \, c^2d^2 = e^2f^2.$$

Thus if six points of C lie on a conic, so do their tangentials. A similar result applies to points of intersection of C with another cubic, with a quartic, ... Again (cf. end of § **11**) all these results can be extended by considering a mapping $x \rightarrow x^N$ in place of $x \rightarrow x^2$.

Glancing again at equation (12.2) we see that, in addition to the cubic C and the quartic, there are various lines, conics and other cubics in the figure. For the equation asserts that the three coresiduals $ab \, . \, cd$, $ef \, . \, gh$, $ij \, . \, kl$ lie on a line, and also that the six points ab, cd, ef, gh, ij, kl lie on a conic. Indeed because of the symmetry of the equation in the 12 points, we can see $12!/(4!)^3 3! = 5775$ such lines on which the ${}^{12}\mathrm{C}_4 = 495$ coresiduals of tetrads lie in threes, and $12!/2^6 6! = 10395$ such conics on which the ${}^{12}\mathrm{C}_2 = 66$ residuals of pairs lie in sizes. There are also ${}^{12}\mathrm{C}_4 = 495$ cubics other than C, as for example through the 9 points a, b, c, d, e, f, g, h, $ij \, . \, kl$.

15. Inscribed polygons. Tangents from a point of the curve (cf. §§ 8, 9)

In § **9**, also in § **8(a)**, we are in effect considering tangents to C from a point on it, or tangents meeting on the curve.

(8.1) is the theorem of Steiner quadrilaterals (fig. 6). If the tangents at a and b meet on C, then an infinity of quadrilaterals can be inscribed in C with their sides passing alternately through a and b. Conversely this is the case if one such quadrilateral can be drawn.

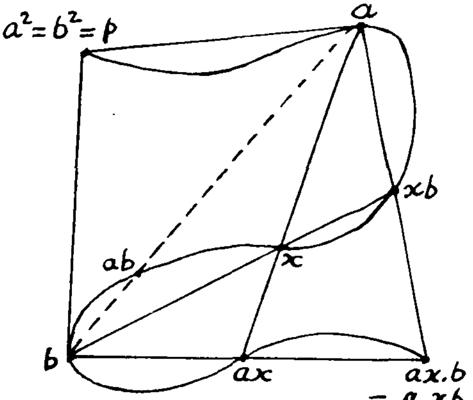


Fig. 6

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

The generalisations (8.2), (8.3) express similar known theorems referring to quadrilaterals or $2m$-gons inscribed in C with sides passing in order through 4 or $2m$ fixed points of C (**24**, pp. 337-338; **29**).

Returning to fig. 6, note that $a^2(=p)$ and ab form another pair of points whose tangentials coincide, for by (2.2) $a^2 = b^2 = p$ implies $(ab)^2 = p^2$.

If as in (9.2) three tangents can be drawn from p to C, we have shown in § **9** that there is a fourth, and that the four points of contact a, b, c, d form a quadrangle whose diagonal points (9.4) lie on C. Since $ab \,.\, cd = p^2$ the four points lie on a conic which touches C at p; and since $(ab)^2 = (ac)^2 = (ad)^2 = p^2$ the three diagonal points and p form another set of four points whose tangentials coincide, and form another such quadrangle. (The words " quadrangle " and " another " assume no three of a, b, c, d collinear, p not a flex.)

Continuing as in § **9**, if there is a fifth tangent from p to C, then we can prove that there are 8 such tangents; from their 8 points of contact can be picked in general 14 quadrangles whose 42 diagonal points coincide in sixes on C, giving 7 new points on C which along with p form another set of 8 points whose tangentials coincide; and so on.

Actually this does not occur on a cubic: the number of tangents from a point of the curve (including if the point is a flex the tangent there) is in fact 1, 2 or 4 according as the curve is cuspidal, nodal or nonsingular.

Consider now the first paragraph of § **9**. It should be remembered that the quasigroup Q which we are discussing is not necessarily the whole curve C, but may consist of any finite or infinite set of its points closed with respect to the chord and tangent process. We see that in any such set Q of n points, those n_1 points which are tangentials of points of the set form a non-null subset Q_1 closed with respect to the chord and tangent process, and are each the tangential of the same number s of points of Q. s is 1, 2 or 4; and if n is finite $n = n_1 s$.

16. Sextactic points (cf. § 10)

See the first theorem of § **14**. According as C is cuspidal, nodal or nonsingular, the number of flexes of C is 1, 3 or 9 while the number of tangents from each flex (excluding flex tangents) is $s-1 = 0$, 1 or 3. Hence the number of s.p.'s (sextactic points) of C is 0, 3 or 27. (The number in a quasigroup Q on C may be 0, 1, 3, 9 or 27.)

We can now interpret § **10**. On C, assumed non-cuspidal, associated with each flex i we have a four-group $C_2 \times C_2$ consisting of i and three collinear s.p.'s a, b, c. If a, b are two s.p.'s associated with the *same* flex i, then ab is the third; if with *different* flexes, a with i and b with j, then ab is either the collinear flex ij or one of its associated s.p.'s, and aj is one of those associated with ij. The t.s.e.q. of order 36 mentioned at the end of § **10** can be interpreted as consisting of the 9 flexes and 27 s.p.'s of a nonsingular cubic. (The figure can be analysed further, as was done by Hesse (**15**), correcting a misstatement by Steiner (**29**).)

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

17. Involute of a class cubic

Instead of building our algebra on collinearity of points on a cubic we could use concurrency of tangents to a curve of class 3, or of normals to its involute; or equally we could take the feet of these normals as the elements of our quasigroup. Thus for points $a, b, \ldots$ of a parabola, since its evolute is of class 3, we may define ab to be the point conormal with a and b, i.e. such that the normals at a, b, ab are concurrent. With this operation the points of the parabola form a t.s.e.q. The totally symmetric property is obvious, and the entropic property can be verified immediately by using the parametric representation $x = At^2$, $y = 2At$ $(t_{ab} = -t_a - t_b)$.

Consider what corresponds to the theorem about the satellite of a line. If a is any point on the curve, a^2 denotes the foot of the one other normal which can be drawn from the centre of curvature at a. The identity $(ab)^2 = a^2b^2$ thus asserts that if the normals at three points of the curve are concurrent, then so are the other normals which can be drawn from their three centres of curvature. The second point of concurrence might be called the satellite of the first. This result is valid for any curve whose evolute is of class 3.

18. Triple systems and finite geometries

A *triple system* on n elements (**30**; **19**, preferably 2nd edition; **9**) is a selection of triples of distinct elements such that every pair of distinct elements occurs in precisely one of the triples. Such a system exists for

$$n(>1) \equiv 1 \text{ or } 3 \pmod{6} = 3, 7, 9, 13, 15, 19, \ldots$$

and is unique to within isomorphism for $n = 3, 7, 9$ only.

A *loop* is a quasigroup containing an identity element 1.

Bruck observed in (**7**) and (**8**, p. 58) respectively that there is a one-one correspondence between triple systems on n elements and (i) idempotent t.s. quasigroups of order n, (ii) t.s. loops of order $n+1$. In each case triples (a, b, c) correspond to sets of equations $ab = c$, etc. In (i) we have also equations of type $a^2 = a$. In (ii) we have an extra element 1 and equations of type $1^2 = 1$, $1a = a1 = a$, $a^2 = 1$.

There is also a connection between certain triple systems and finite geometries having 3 points on a line, as explained in (**9**, pp. 425-426). Of course only triple systems of special type will correspond in the above ways to *entropic* quasigroups. It happens that these are just the triple systems which can be identified with finite geometries.

(i) The idempotent t.s.e.q. $Q_3 \times Q_3 \times \ldots$ (r factors, $r \geqq 1$) of §§ **7**, **13** corresponds to a triple system on 3^r elements. It may be identified with the finite geometry $EG(r, 3)$ (**9**, pp. 329, 426).

(ii) The abelian group, or entropic loop, $C_2 \times C_2 \times \ldots$ (r factors, $r > 1$) of §§ **10**, **16** corresponds to a triple system on $2^r - 1$ elements. The elements other than 1 may be identified with the points of the finite geometry $PG(r-1, 2)$ (**9**, pp. 323, 425).

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

In both cases any equation $ab = c$ with a, b, c distinct ($\neq 1$ in case ii) means that the points a, b, c are collinear.

Entropic quasigroups whose elements are points, with a, b, ab collinear, are also a feature of a type of finite geometry introduced by Sade (**23**, p. 109). His configuration contains n^2 points on nN lines, with n points on each line, N lines through each point, N depending on n. When $n = 3$, $N = 4$; the configuration is then that of the 9 flexes of a nonsingular cubic. It is only in this case that the quasigroup involved is totally symmetric and that ab is the *unique* point collinear with a and b.

Part III

19. The isotopic abelian group

Given a t.s.e.q. Q written multiplicatively, we can associate with it an abelian group G, defined on the same set of elements and for convenience written additively, as follows.

Choose a fixed element o of Q and define

$$a+b = ab \,.\, o. \tag{19.1}$$

Then the postulates for an abelian group are satisfied, for by (6.4) we have

$$(a+b)+c = (ab\,.\,o)c\,.\,o \text{ (symmetric in } a, b, c) = a+(b+c); \tag{19.2}$$

$$a+b = b+a;$$

$$a+o = ao\,.\,o = a, \text{ so that } o \text{ is the zero of } G;$$

$$a+ao^2 = (a\,.\,ao^2)o = o^2o = o, \text{ so that } -a = ao^2.$$

To express the quasigroup operation in terms of the group operation, put $c = ab$ in (19.2). The middle term then reduces to o^2. Thus

$$ab = o^2-a-b. \tag{19.3}$$

This confirms the statement in § **5** that every t.s.e.q. Q can be constructed from a suitable additively written abelian group by a formula of the form

$$ab = k-a-b. \tag{19.4}$$

Given Q, the element o is at our choice, and $k = o^2$ can be any element which is a square in Q.

It follows from (19.1), or equally from (19.3), that Q and G are isotopic,† and we shall call G *the isotopic abelian group* to Q, implying that it is unique to within isomorphism.‡

† Two groupoids defined on the same set of elements are by definition (**4**, **6**) isotopic if their operations ab, $a^\circ b$ are related by $a^\circ b = (a^U b^V)^W$ where U, V, W indicate one-one reversible mappings of the set onto itself. This is an equivalence relation, and any isotope of a quasigroup is a quasigroup. As remarked in the footnote to § **5** the results of this Section are specialisations of theorems of Murdoch (**18**) and Bruck (**6**); cf. also Toyoda (**32**).

‡ If a quasigroup is isotopic to groups G, G', then G and G' are isotopic, and by a theorem of Albert (**4**, Theorem 2) isotopic groups are isomorphic.

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

If Q contains an idempotent and this is chosen as o, so that $k = o^2 = o$ is the zero of G, (19.4) becomes

$$ab = -a-b. \tag{19.5}$$

In the geometrical interpretation o is then a flex of C, and (19.1), which can now also be written $a+b = ao \, . \, bo$, describes a well-known construction for defining addition of points on a cubic so as to obtain an abelian group (**33**, p. 191).

20. The number of square roots of an element

We can now complete § **9** by showing that s, the number of square roots in Q of any element k which has a square root, is always if finite 1 or a power of 2.

Suppose $s > 1$. Choose o to be a square root of k and form the isotopic abelian group with zero element o. By (19.4) $a^2 = k$ in Q if and only if $2a = o$ in G. Or changing to the multiplicative terminology for G, the square roots of k in Q are the square roots of the unit element in G. These form a subgroup of G in which each element other than the unit element has period 2, and which must therefore if finite be a direct power of the cyclic group C_2. The result follows.

[*Note.* It is clear from (19.4) that a subgroup of G is a subquasigroup of Q if and only if k belongs to it. The square roots of k in Q form a subgroup of G, but form a subquasigroup of Q if and only if k is idempotent in Q.]

In the case when Q, not merely s, is finite, we can give a more precise statement. From the general theory of abelian groups, G is then a direct product $C_{n_1} \times C_{n_2} \times \ldots \times C_{n_r}$ of cyclic groups whose orders are powers of primes. A square root of the unit element of G is a product of square roots of the unit elements picked one from each factor C_{n_i}, for which there are two choices when n_i is even, 1 when n_i is odd. The number of square roots is therefore $s = 2^m$ where m is the number of even numbers in the set $n_1, n_2, \ldots, n_r$.

21. Idempotent t.s.e.q.'s

We can now complete § **7**. It will be sufficient to consider the idempotent subquasigroup, but let us now denote it Q.

Let Q be a finite idempotent t.s.e.q. of order greater than 1. We form the isotopic abelian group and may assume that (19.5) holds. Since in Q every element satisfies $a^2 = a$, in G every element satisfies $-2a = a$, or $3a = 0$. (It will be convenient to write 0 now for the zero element.) Hence the finite abelian group G must be a direct sum of cyclic groups C_3, and its order—the number of idempotents in Q—is a power of 3.

Suppose that there are m direct summands C_3, with generators $a_1, \ldots, a_m$ each satisfying $3a_i = 0$. Every element a can be written uniquely as $a = \Sigma\alpha_i a_i$ with each $\alpha_i = 0$, 1 or 2 (residues mod. 3). By (19.5) the product in Q of two such expressions is

$$ab = (\Sigma\alpha_i a_i)(\Sigma\beta_i a_i) = \Sigma(-\alpha_i - \beta_i)a_i.$$

This shows that Q is the direct product of m quasigroups in any one of which elements and products are given by the same formulae with the Σ's omitted, i.e. of m quasigroups isomorphic to Q_3 (see how Q_3 was constructed in Example 2).

[*Note*. Without giving the proof in detail, Bruck (**6**, p. 40) stated essentially this result in the form of a necessary and sufficient condition for an idempotent t.s. quasigroup to be isotopic to a group.]

22. Conjecture

It is clear that not every t.s.e.q. can be interpreted as a set of points on a plane cubic curve, or, as we may say, can be placed on a cubic, consistently with the chord and tangent definition of multiplication. The question arises, how can we characterise those t.s.e.q.'s which can be so placed? I leave this unsolved but put forward the following conjecture: that a finite or finitely generated t.s.e.q. can be placed on a nonsingular plane cubic if and only if the isotopic abelian group is either cyclic or a direct product of *two* cyclic groups.

23. Generalisation

J. G. Brennan in a letter (14th January 1956) made the following observations which I quote by permission.

Consider a plane curve C of genus p, and on it a linear series g^{2p}_{3p}. Let a, b, ... denote sets of p points of C. Two such sets determine a third, consisting of the p remaining points in the set of the g^{2p}_{3p} determined by the $2p$ points of $a \cup b$. Then clearly we have a totally symmetric quasigroup Q. That Q is also entropic follows easily from the theory of linear equivalence of sets of points on an algebraic curve. (See, e.g., **25**.)

The idempotents of Q are those sets of g^{2p}_{3p} consisting of p triple points. The number of such sets is 9^p. Also given any element a of Q, the equation $x^2 = a$ has 4^p solutions in Q. The last two statements are consequences of the formula of de Jonquières, which gives the number of sets of a linear series possessing various numbers of points of prescribed multiplicity (**26**, p. 243). The second number 4^p is the number of sets of a g^p_{2p} with p double points. For, fixing p points of g^{2p}_{3p} (i.e. given a), the remaining points vary in a g^p_{2p} whose sets with p double points are the x's.

Another way of looking at this t.s.e.q. is to consider the so-called Variety of Jacobi, whose points image sets of p points of a curve of genus p (**26**, p. 281).

Note added in proof

Following criticism by the referee § **23** has been the subject of further correspondence with J. G. Brennan. There may exist special sets of p points

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

on C, two of which do not determine a unique third set by the above construction. In the terminology of Bruck (**8**, p. 9) the system in general forms a halfgroupoid, i.e. a set in which products of some but not all pairs of elements are defined. In those cases in which the halfgroupoid is in fact a quasigroup, the remarks of § **23** are valid.

REFERENCES

" MR " indicates *Mathematical Reviews*

(**1**) J. Aczél, On mean values, *Bull. Amer. Math. Soc.* **54** (1948), 392-400; MR **9**, 501.

(**2**) J. Aczél, Some general methods for functional equations, *Uspehi Mat. Nauk* (N.S.), **11** (1956), No. 3 (69), 3-68 (Russian); MR **18**, 807.

(**3**) J. Aczél, V. D. Belousov and M. Hosszú, Generalized associativity and bisymmetry on quasigroups, *Acta Math. Acad. Sci. Hungar.* **11** (1960), 127-136; MR **25** # 4018.

(**4**) A. A. Albert, Quasigroups I, *Trans. Amer. Math. Soc.* **54** (1943), 507-519; MR **5**, 229.

(**5**) V. D. Belousov, Transitive distributive quasigroups, *Ukrain. Mat. Ž.* **10** (1958), No. 1, 13-22 (Russian); MR **20** # 2390.

(**6**) R. H. Bruck, Some results in the theory of quasigroups, *Trans. Amer. Math. Soc.* **55** (1944), 19-52; MR **5**, 229.

(**7**) R. H. Bruck reviewing Hall and Swift, MR **18** (1957), 192.

(**8**) R. H. Bruck, *A Survey of Binary Systems* (Berlin, 1958); MR **20** # 76.

(**9**) R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order* (Boston, U.S.A., 1937).

(**10a**) I. M. H. Etherington, Transposed algebras, *Proc. Edin. Math. Soc.* (2) **7** (1945), 104-121; MR **7**, 4.

(**10**) I. M. H. Etherington, Non-associative arithmetics, *Proc. Roy. Soc. Edin. A*, **62** (1949), 442-453; MR **10**, 677.

(**11**) I. M. H. Etherington, Groupoids with additive endomorphisms, *Amer. Math. Monthly* **65** (1958), 596-601; MR **20** # 5816.

(**12**) I. M. H. Etherington, Note on quasigroups and trees, *Proc. Edin. Math. Soc.* (2) **13** (1963), 219-222; MR **28** # 157.

(**13**) T. Evans, Properties of algebras almost equivalent to identities, *J. London Math. Soc.* **37** (1962), 53-59; MR **24** # A3225.

(**14**) O. Frink, Symmetric and self-distributive systems, *Amer. Math. Monthly* **62** (1955), 697-707; MR **17**, 458.

(**15**) O. Hesse, Über Curven dritter Ordnung und die Kegelschnitte, welche diese Curven in drei verschiedenen Puncten berühren, *J. Reine Angew. Math.* **36** (1847), 143-176.

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press

(16) H. Minc, The free commutative entropic logarithmetic, *Proc. Roy. Soc. Edin. A*, **65** (1959), 177-192; MR **22** # 11018.

(17) D. C. Murdoch, Quasi-groups which satisfy certain generalized associative laws, *Amer. J. Math.* **61** (1939), 509-522.

(18) D. C. Murdoch, Structure of abelian quasi-groups, *Trans. Amer. Math. Soc.* **49** (1941), 392-409; MR **2**, 218.

(19) E. Netto, *Lehrbuch der Combinatorik* (Leipzig, 1901; 2nd ed., 1927).

(20) J. Marshall Osborn, New loops from old geometries, *Amer. Math. Monthly* **68** (1961), 103-107; MR **23** # A1686.

(21) A. Sade, *Quasigroupes*, published by the author (Marseille, 1950); MR **13**, 203.

(22) A. Sade, Quasigroupes obéissant à certaines lois, *Rev. Fac. Sci. Univ. Istanbul A*, **22** (1957), 151-184; MR **21** # 4987.

(23) A Sade, Quasigroupes automorphes par la groupe linéaire et géométrie finie, *J. Reine Angew. Math.* **199** (1958), 100-120; MR **20** # 78.

(24) G. Salmon, *Higher Plane Curves* (3rd ed., Dublin, 1879).

(25) J. G. Semple and L. Roth, *Introduction to Algebraic Geometry* (Oxford, 1949); MR **11**, 535.

(26) F. Severi, *Trattato di Geometrica Algebrica* (Bologna, 1926).

(27) M. Sholander, On the existence of the inverse operation in alternation groupoids, *Bull. Amer. Math. Soc.* **55** (1949), 746-757; MR **11**, 159.

(28) S. K. Stein, On the foundations of quasigroups, *Trans. Amer. Math. Soc.* **85** (1957), 228-256; MR **20** # 922.

(29) J. Steiner, Geometrische Lehrsätze, *J. Reine Angew. Math.* **32** (1846), 182-184 = *Ges. Werke* II, 369-373.

(30) J. Steiner, Combinatorische Aufgabe, *J. Reine Angew. Math.* **45** (1853), 181-182 = *Ges. Werke* II, 435-436.

(31) M. Takasaki, Abstraction of symmetric transformations, *Tôhoku Math. J.* **49** (1943), 145-207 (Japanese); MR **9**, 8.

(32) K. Toyoda, On axioms of mean transformations and automorphic transformations of abelian groups, *Tôhoku Math. J.* **46** (1940), 239-251; MR **2**, 6.

(33) R. J. Walker, *Algebraic Curves* (Princeton, 1950); MR **11**, 387.

Mathematical Institute
The University
Edinburgh

https://doi.org/10.1017/S001309150000897X Published online by Cambridge University Press