Some combinatorial problems of finite abstract algebra

By A. R. Richardson.

(*Received* 24*th September*, 1938. *Read* 4*th November*, 1938.)

(Communicated by Professor H. W. Turnbull.)

The elements of the abstract number systems termed groups, rings, ideals, modules and algebras are mere symbols arranged in systems by means of consistent and independent postulates which isolate these systems from the complete realm of abstract mathematics. The postulates are usually chosen so as to generalise the special number systems which have been noticed in traditional mathematics and their independence and consistency are usually proved by means of numerical examples. It is suggested in this note that the extents of the consistency and independence of a set of postulates should also be studied

The number systems determined by the same set of postulates will be termed species, and statements of properties common to all systems of the same species will be termed theorems. A theorem, true for one species, may also hold for others and may itself be used as a postulate to define species. Much recent work in abstract algebra has for its object the generalisation of theorems and their expression in terms of standard sets of postulates of familiar type such as the associative and commutative laws, the laws of transitivity, cancellation and idempotency.

The effect of an addition of an independent postulate to a set is to restrict the number of systems in a species and theorems which are independent in the larger species sometimes coalesce in the more restricted range. Well known examples are the independence of the additive and multiplicative properties of zero in general systems and the distinction between non-factorisable and prime numbers in the general ideal theory.

For the sake of simplicity and definiteness this note deals only with a restricted species of abstract systems, viz., the species of *finite groupoids of order* n which are sets of n symbols closed to a single operation. The following definitions are therefore *relative* and not absolute.

Definition 1. The *extent* of a theorem or postulate is the number of groupoids of order n which satisfy the theorem or postulate.

Definition 2. The *strength* of a theorem or postulate is the probability that it is *not* satisfied in a groupoid of order n chosen at random.

The extents of consistency, independence and redundance of a set of theorems or postulates may be defined similarly and are numbers which it is desirable to calculate.

There are n^{n^2} finite groupoids of order n not all of which are algebraically distinct since some may be obtained from others by mere interchange of symbols. For example, groupoids defined by the following multiplication tables show that some are altered by every interchange of elements whilst others remain unaltered by all such interchanges.

	a	b	c
a	a	a	c
b	a	b	c
c	a	a	c ,

	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c .

In the following numerical statements equivalent groupoids are counted as distinct. Nevertheless it is important to determine how many are algebraically distinct and how these are distributed in relation to the properties of the symmetric group of order $n!$ The numerical results have been calculated from an examination of the various multiplication tables, but, in view of the tedious nature of such calculations, have not been checked independently.

The extent of commutative groupoids of order n is $n^{n(n+1)/2}$ so that the strength of the postulate of commutativity is $1-n^{-n(n-1)/2}$.

Mention will now be made of some of the more important theorems and postulates of which it is desirable to calculate the strength.

(a) Every associative algebra contains at least one idempotent. The extent of groupoids of order n which have at least one idempotent is

$$n^{n^2}\left[1-\left(1-\frac{1}{n}\right)^n\right],$$

and its strength $\to e^{-1}$ when n is large.

(b) An idempotent e is a right-hand unit of Ge. For G_3 its extent is 5,859.

https://doi.org/10.1017/S0013091500008531 Published online by Cambridge University Press

(*c*) Gg is a principal ideal right sub-groupoid, (g), of G for all elements g of G.

(*d*) $(a)(b) = (ab)$.

For G_3 there are 1215 cases in which Ga is of order 1, and in 275 of these cases there are no sub-groupoids of order 2; 3,456 cases in which Ga is of order 2 and 4,374 cases in which it is of order 3, *i.e.* equal to G. Hence Ga is a groupoid in 9,045 cases.

Ga, Gb are both sub-groupoids of order 1 in 108 cases, Ga is of order 1 and Gb of order exactly 2 in 513 cases, Ga is of order 1 and Gb of order exactly 3 in 270 cases.

A theorem true for all groupoids is that the powers of any element are not all different. If this is adopted as a postulate it leads us outside the domain of finite groupoids into the algebras of Grassmann and others in which the product is not necessarily an element of the algebra or in which the order is not finite.

The postulates in most general use are those of associativity and commutativity. They are independent for finite groupoids as the following examples show, and it is desirable to determine not only their extents but also the extent of their independence.

	a	*b*	*c*
a	*b*	*a*	*a*
b	*a*	*c*	*a*
c	*a*	*a*	*a* ,

	a	*b*	*c*
a	*a*	*b*	*a*
b	*c*	*b*	*a*
c	*b*	*c*	*c* .

Of the 3^6 groupoids of G_3 which have 3 idempotents 3^3 are commutative, 38 are associative and of these 9 are commutative; 9 of the 38 are independent and associative and of these 2 are commutative.

The nature of such problems is indicated by the following considerations. In a *quasi-group* both the right and left cancellation laws hold; consequently each number appears once in each row and in each column of the multiplication table. Hence the number of quasi-groups is the same as that of Latin squares; for G_3 there are 72, for G_4 there are 539,136. A weaker postulate is that of *homogeneity*, *i.e.* each number appears at least once in the multiplication table. The extent of this postulate is

$$n^{n^2}\left[1 - n\left(1 - \frac{1}{n}\right)^{n^2}\right].$$

https://doi.org/10.1017/S0013091500008531 Published online by Cambridge University Press

Evidently new types of generating functions are required for the solutions of the problems indicated here.

(*e*) The order of a sub-groupoid is a divisor of the order of the groupoid (Lagrange)[1].

(*f*) If $s \mid n$ then a groupoid of order n contains at least one sub-groupoid of order s (Sylow)[2].

These theorems are of limited extent for there are 2^{n^2-n} groupoids of order n such that every sub-set is also a sub-groupoid, and there are at least n^{n^2-n} groupoids for which no sub-set is a sub-groupoid. In G_3 Sylow's theorem is not true in $2^3 . 3^6$ cases; the theorems of both Lagrange and Sylow are not true in $2^3 . 3^5$ cases; Lagrange's theorem is not true in 10,000 cases. In 64 cases every sub-set of order 2 is also a sub-groupoid. In G_4 1,229,483,008 groupoids contain sub-groupoids of order 3 and therefore do not satisfy Lagrange's theorem.

Since the extent of G_3 is 19,683, the extent of at least one idempotent is 13,851 and Lagrange's theorem is not true in 10,000 cases, it follows that there are at least 4,168 groupoids which contain at least one idempotent element and for which Lagrange's theorem is not true.

(*g*) The extent to which a groupoid of order n contains maximal or minimal sub-groupoids of order r.

In G_3 a sub-groupoid of order 1 is maximal in 5,436 cases and a sub-groupoid of order 2 is minimal in 2,916 cases. In 972 cases a sub-groupoid of order 1 is maximal and a sub-groupoid of order 2 minimal. A sub-groupoid may of course be both maximal and minimal if $n \geqq 4$.

A specified sub-groupoid of order r is maximal in

$$r^{r^2}\, n^{n^2-r^2} \sum_{\lambda=0}^{n-1} (-1)^{\lambda} \sum_{s=1}^{n-r-1} \left(\frac{r+s_1}{n}\right)^{\sigma_1} \left(\frac{r+s_2}{n}\right)^{\sigma_2-\sigma_1} \cdots \left(\frac{r+s_\lambda}{n}\right)^{\sigma_\lambda-\sigma_{\lambda-1}}$$

cases, where $s_\lambda > s_{\lambda-1} > \ldots > s_2 > s_1$; $\sigma_s = 2rs + s^2$.

(*h*) The theorems relating to decomposition. A groupoid may be the *union* $[A, B]$, or the *cross-cut* (A, B), of groupoids A, B. In G_3 3024 are *directly decomposable, i.e.* are the unions of sub-groupoids having no common elements.

---

[1] *cf.* Burnside, *Theory of groups* (Cambridge 1897), p. 25.

[2] *cf.* Burnside, *op. cit.*, Chapter 6.

(i) The theorems relating to residuation, viz., the expression of a groupoid G as the sum of cosets, Hg_i, where H is a sub-groupoid.

(i_1) Every number of G lies in some coset.

(i_2) No coset contains equal elements.

(i_3) Different cosets have no common elements.

(i_4) The product of two cosets is a coset and the cosets may be taken to be the elements of a quotient groupoid G/H.

(j) The second law of isomorphism, viz.

$$[A, B]/A \cong B/(A, B).$$

The complete study of the extents of these theorems and of others suggested by them will be troublesome; thus cosets exist in which the theorems hold, but in which H is not a sub-groupoid. Thus there are 10,432 in G_3 which satisfy the theorems (i_1) .... (i_4) in which H is of order 1, and of these H is a sub-groupoid in 4,058 cases.

(k) The various generalisations of the theorem of Jordan-Hölder[1].

To what extent the above definitions may be used outside the particular domain of groupoids is a subject for further consideration, but enough has been sketched to show that there is a wide range of combinatorial algebra awaiting investigation.

(l) In G_n the n^3 postulates of associativity are not independent and it is desirable to determine how many are necessary. The extent of $a \,.\, bc = ab \,.\, c$ is

$$(n^2 + 2n - 2)\, n^{n^2-3};$$

of $ab \,.\, c = a \,.\, bc$ and $b \,.\, b^2 = b^2 \,.\, b$ is

$$(2n^3 + 3n^2 - 6n + 2)\, n^{n^2-5};$$

of $ab \,.\, c = a \,.\, bc$ and $a \,.\, a^2 = a^2 \,.\, a$ is

$$(2n^3 + 4n^2 - 8n + 3)\, n^{n^2-5}.$$

[1] O. Ore, *Trans. Amer. Math. Soc.*, **41** (1937), 266-275.

UNIVERSITY COLLEGE,
SWANSEA.

https://doi.org/10.1017/S0013091500008531 Published online by Cambridge University Press