The Elements of a theory of abstract discrete Semi-groups.

By

H. S. VANDIVER (Austin, Texas).

(Als Manuskript eingegangen am 10. Januar 1940.)

The theory which I shall consider here was developed mainly during lectures on group theory, abstract algebras, and number theory which I gave at the University of Texas, with one semester at Princeton University, during the last ten years. I was aided and stimulated by discussions which grew out of these lectures. I shall give some specific references later to several attendante at said lectures, but I wish to mention in this connection particularly F. C. BIESELE, (who materially aided in the preparation of this paper), Dr. A. CHURCH, Dr. J. L. DORROH, Dr. O. H. HAMILTON, Dr. D. H. LEHMER, Miss H. C. MILLER, A. M. MOOD, C. F. MORAN and M. E. TITTLE.

It seems to have been noted for some time now by mathematicians that, in order to examine various algebraic systems, it is convenient to make use of a system of single composition which is more general than the group, this being in addition to the theory of lattices or structures. For example, although the elements of a ring form a group under addition, they do not in general form a group under multiplication; they are, however, closed under multiplication, and the associative law holds.

I imagine that the notion of semi-group, as defined below, would have been studied as much as groups have been studied, had GAUSS, for example, defined an abstract system based on the idea of multiplication of residue classes modulo m, where m is composite. Since a closed set of substitutions necessarily forms a group, the study of substitutions did not lead in the direction just mentioned.

CAUCHY[1]), in attempting to justify the use of complex numbers in ordinary algebra, employed polynomials with real coefficients, in an indeterminate x, and noted that, if $i^2 = -1$, then

$$(a + bi) + (c + di) = (a + c) + (b + d)\, i$$

corresponds to

$$(a + bx) + (c + dx) \equiv (a + c) + (b + d)\, x \pmod{x^2 + 1}$$

Now there is certainly a type of correspondence here, as CAUCHY indicates, since a corresponds to a, b corresponds to b, etc., and equality corresponds to congruence modulo $(x^2 + 1)$. This notion seems not to have influenced later writers; KRONECKER, in any logical discussion, at least, would apparently insist on using the modulus explicitly. DEDEKIND[2]) made use of the idea of classes of residues modulo m so that each integer a defines a unique class of integers ("Zahlklasse") of the form $a + km$, k being an integer. E. H. MOORE[3]) similarly used the idea of residue classes with respect to a modular system defined by a prime p and $f(x)$, where the latter is a polynomial in x with integral coefficients, and showed that these classes form a field. STEINITZ[4]) used residue classes with respect to the modulus $g(x)$, where $g(x)$ has rational coefficients and is irreducible in the rational field. He employed this to set up his theory of algebraic fields.

The above notion, with the exception of CAUCHY'S, always seemed to the writer to be unnecessarily involved. It seems a bit less complicated to speak of the set of incongruent integers modulo m, and of the group formed by them under addition modulo m, instead of setting up the notion of class and defining the equality of classes and the addition of classes. In view of this, we define a system called a semi-group in such a way that the symbol of relation ($\overset{\infty}{=}$) may stand not only for equality, but also for congruence, etc.

We begin with a certain set S of elements which may be denoted by letters, a symbol of conjunction, $\circ$, and a symbol of equivalence, $\overset{\infty}{=}$.

[1]) Oeuvres, 1st series, 10, pp. 317—319.

[2]) Werke, Bd. III, 74—76. He gives the idea for the more general case of algebraic numbers.

[3]) Trans. New York Math. Soc., May, 1893. Cf. also DICKSON, Linear Groups, TEUBNER, 1901, pp. 1—7, and WEBER, Algebra, 2nd ed., Bd. II, 60—61; 305—306.

[4]) Journal für Mathematik v. 137, 1910, pp. 193—194.

Consider a finite ordered set having the following properties:

1. The first element is a letter denoting an element of S.

2. The subsequent elements are alternately the symbol $\circ$ and letters denoting elements of S.

3. The last element is a letter denoting an element of S.

Such a set will be called a combination. Moreover, if a finite ordered set T is of such a nature that, by replacing a symbol of T by the set which this symbol denotes, we obtain a finite ordered set T_1, then by replacing a symbol of T_1 by the set which this symbol denotes, we obtain a finite ordered set T_2, and after a finite sequence of such steps we arrive at a finite ordered set T_n which has the properties 1.—3. stated above, then T will also be called a combination.

A subcombination of a given combination C is a combination which is either a symbol found in C, or such a symbol followed by others in order as they appear in C.

The set S will satisfy some or all of the following postulates:

1. If a and b denote elements of S, then an element of S, denoted by c, may be determined such that

$$a \circ b \cong c$$

2. If A denotes a combination, then $A \cong A$.

3. If A, B, C, D, denote combinations such that $A \cong B$ and $D \cong C$, with C a subcombination of B, and if B' denotes the combination obtained from B by replacing C by D, then $B' \cong A$.

4. An element of S, denoted by e, may be determined such that $e \circ a \cong a \circ e \cong a$, where a denotes any element of S.

5. If a, b, c, d denote elements of S, and if $c \circ a \cong c \circ b$, then $a \cong b$; if $a \circ d \cong b \circ d$, then $a \cong b$.

6. If a and b denote elements of S, we may determine elements of S denoted by x and y such that

$$a \circ x \cong b$$

and

$$y \circ a \cong b$$

7. We now introduce a new symbol of relation ($\supseteq|\cong$) and postulate that if A and B denote combinations, then either $A \cong B$ or $A \supseteq|\cong B$, these relations being mutually exclusive; and we shall employ the law of the excluded middle.

If the set S satisfies postulates 1, 2, 3, 7, it is called a semi-group. If it satisfies 1, 2, 3, 4, 7, it is called a gruppoid. If it satisfies 1, 2, 3, 5, 7, it is called a quasi-group. If it satisfies 1, 2, 3, 6, 7, it is called a group.

It will be noted that no provision is made for the use of any parantheses in connection with any of our symbols. The substitution postulate 3. covers what is equivalent to the associative law as ordinarily employed. There is no logical necessity for the use of parentheses in a system of single composition, and from our standpoint, if employed, they will be merely symbols of emphasis.

Suppose we have combinations denoted by M, N, such that $M \overset{\omega}{=} N$. By postulate 2. we also have $N \overset{\omega}{=} N$. Employing postulate 3., and noting that N, by definition, is a subcombination of itself, we obtain $N \overset{\omega}{=} M$. Hence we have

Theorem 1. (Symmetry) If M and N denote combinations, and $M \overset{\omega}{=} N$, then $N \overset{\omega}{=} M$.

From this theorem and the postulates we get easily the following: (capital letters denote combinations)

Theorem 2. (Transitivity) If $A \overset{\omega}{=} B$, and $B \overset{\omega}{=} C$, then $A \overset{\omega}{=} C$.

Theorem 3. (Composition) If $A \overset{\omega}{=} B$, then for any combination C, $C \circ A \overset{\omega}{=} C \circ B$ and $A \circ C \overset{\omega}{=} B \circ C$.

It also follows that if $A \circ B \overset{\omega}{=} D$, and $B \circ C \overset{\omega}{=} G$, then $D \circ C \overset{\omega}{=} A \circ G$. This is the ordinary associative law.

The systems I have defined above have been employed by a number of writers, but the terms used here have not always been employed by them. The system which I have called a quasi-group was termed a semi-group by DICKSON[5]), who proved several properties of this system. FROBENIUS and SCHUR[6]) used the term group for a system which is closed under an associative operation and consists of linear transformations in which the determinant of the transformation is not necessarily different from zero; the identity transformation is not necessarily included in the set. HILTON[7]) also used the term semi-group for the system we call a quasi-group. E. T. BELL[8]) used the name ova for systems defined by closure (our postulate 1). He also noted that in group theory and similar

[5]) Trans. Am. Math. Soc., 1905, v. 6, pp. 205—208.
[6]) Berlin. Sitzungsber. 1906, p. 209.
[7]) Finite Groups, Oxford, 1908, p. 51; ex. 6, 7, p. 52.
[8]) Proc. Nat. Acad. Sci. 1933, p. 577—579.

topics it was necessary to state a postulate which would enable us to pass from $A = B$ to $AC = BC$[9]). The term commutative semi-group was used by BELL[10]) in the same way we employ it in this paper. For a system defined by closure, the associative law, and the existence of an identity element, SPECHT[11]) used the term group; to the system we have called a group, he gave the name proper group. GARRETT BIRKHOFF[12]) used the term gruppoid as we have employed it here.

J. KÖNIG[13]) discussed factorization in a holoidal domain ("holoides Bereich"); the quantities in such a domain form a quasi-group under multiplication as defined in the present paper. The divisibility properties of these elements are defined without reference to addition, and the greatest common divisor of two quantities is defined on this basis. Factorization in a commutative semi-group has been considered by BELL and WARD[14]), and also by CLIFFORD[15]). The term semi-group has been applied to various systems in analysis in which the product of two transformations is a transformation included in the set[16]).

Factorization and related topics connected with semi-groups will not be discussed in this paper. We shall be more interested in the relation of a semi-group to its included quasi-groups and groups.

It was noted by WARD[17]) that the adjunction of an identity element to the set is not in all cases desirable, such adjunction being, for example, inconvenient in ideal theory. The study of the cyclic semi-group generated by an element a is also needlessly encumbered by the adjunction of an identity element.

---

[9]) As we have noted, this follows from our postulate 3.

[10]) Amer. Math. Monthly 37, 1930, p. 401.

[11]) Math. Zeitschr. v. 37, 1933, p. 321.

[12]) Annals of Math. v. 35, 1934, p. 351.

[13]) Einleitung in die Allgemeine Theorie der Algebraischen Grössen pp. 13, 15. This reference was pointed out to me by Professor E. T. BELL. See also DEDEKIND, Werke, Bd. II, p. 126.

[14]) Annals of Math. v. 36, 1935, pp. 36—39; Amer. Math. Monthly, v. 37, 1930, p. 401; Bull. Am. Math. Soc. v. 14, 1928, pp. 907—911.

[15]) Annals of Math. v. 39, 1939, pp. 594—610; Bull. Amer. Math. Soc. v. 40, 1934, pp. 326—330.

[16]) See for example EISENHART, L. P., Riemannian Geometry, Princeton, 1926, p. 221.

[17]) Annals of Math. v. 36, 1935, pp. 36—39.

In what follows we shall assume the arithmetic of the natural numbers, although the theory of the natural numbers may be developed independently, using semi-group concepts, in a manner which we hope to be able to describe elsewhere.

Adopting the usual exponent notation, we let a^2 denote the combination $a \circ a$, etc. The order of an element a of a semi-group is defined as the maximum number of non-equivalent elements (combinations) contained in the set $a, a^2, a^3, \ldots$, provided such a number exists; if there are infinitely many non-equivalent combinations in the set, a is said to be of infinite order; if not, a is said to have finite order. If an element a has finite order, then there is a least positive integer s such that $a^s \eqq a^k$, where $0 < k < s$. Such a k will necessarily be unique. The period of a is defined as $(s - k)$; the order of a will be $(s - 1)$.

An element e of a semi-group is said to be a left (right) identity provided that if a denotes any element of the semi-group, then $e \circ a \eqq a$ $(a \circ e \eqq a)$. An element which is both a right and a left identity is called simply an identity element.

An element h of a semi-group is said to be a left (right) annihilator (or annulator) provided that if a denotes any element of the semi-group, then $h \circ a \eqq h$ $(a \circ h \eqq h)$. An element which is both a right and a left annihilator is said to be an annihilator.

Note that if a semi-group has two non-equivalent left identities, then it has no right identity. For, if e_1, e_2 denote such left identities, and e_r denotes a right identity, then

$$e_1 \eqq e_1 \circ e_r \eqq e_r \eqq e_2 \circ e_r \eqq e_2 .$$

This shows also that if a semi-group has both a right and a left identity, then the two are equivalent. From this follows also that if a semi-group has two identity elements, they are equivalent. Similar theorems hold for annihilators in place of identities in the above.

If S is a semi-group, we define a sub-semi-group of S as a subset of S which is itself a semi-group with the same symbol of conjunction and symbol of equivalence as in S. It follows that the set of left identities, if any, of a semi-group form a sub-semi-group of the given semi-group. In this sub-semi-group, each element is a left identity and a right annihilator. For, if e_1, e_2 denote two such left identities, then $e_1 \circ e_2 \eqq e_2$.

An element a of a semi-group is said to be left (right) cancellable provided that if

$$a \circ b \underline{\underline{\sim}} a \circ c \quad (b \circ a \underline{\underline{\sim}} c \circ a)$$

then $b \underline{\underline{\sim}} c$, where b and c denote any elements of the semi-group. A cancellable element is one which is both right and left cancellable. An element a of a semi-group is said to be left non-cancellable if there exist non-equivalent elements b and c of the semi-group such that $a \circ b \underline{\underline{\sim}} a \circ c$. A similar definition holds for right non-cancellable.

The set of cancellable elements of a semi-group S forms a sub-semi-group of S. For, if a and b denote two cancellable elements, and $a \circ b \circ c \underline{\underline{\sim}} a \circ b \circ d$, then $b \circ c \underline{\underline{\sim}} b \circ d$, and hence $c \underline{\underline{\sim}} d$; likewise if $c \circ a \circ b \underline{\underline{\sim}} d \circ a \circ b$, then $c \circ a \underline{\underline{\sim}} d \circ a$, and $c \underline{\underline{\sim}} d$.

If a, a' are left non-cancellable, then $a \circ a'$ and $a' \circ a$ are also left non-cancellable. For, since a' is left non-cancellable, there exist non-equivalent elements f, g such that $a' \circ f \underline{\underline{\sim}} a' \circ g$, from which $a \circ a' \circ f \underline{\underline{\sim}} a \circ a' \circ g$, but $f \not\underline{\underline{\sim}} g$, hence $a \circ a'$ is left non-cancellable. A similar argument shows that $a' \circ a$ is also left non-cancellable. A like result holds for two right non-cancellable elements. The same argument as above shows that if a' is left non-cancellable, and a is arbitrary, then $a \circ a'$ is left non-cancellable.

Theorem 4. If a semi-group S contains a cancellable element of finite order, then S is a gruppoid.

Proof: If c denotes a cancellable element of finite order, then for some integers h, k, $h > k > 0$,

$$c^k \underline{\underline{\sim}} c^h$$

and since c is cancellable

$$c \underline{\underline{\sim}} c^{h-k+1}.$$

Then for a arbitrary in S

$$a \circ c \underline{\underline{\sim}} a \circ c^{h-k+1};$$

and since c is cancellable

$$a \underline{\underline{\sim}} a \circ c^{h-k};$$

similarly[18])

$$a \underline{\underline{\sim}} c^{h-k} \circ a.$$

If we define a unit of a gruppoid S as an element u for which there can be determined elements u', u'' of S such that

[18]) The proof of this result is due to A. M. MOOD. The result itself is a generalization of a theorem of the writer's. Cf. Bull. Am. Math. Soc., v. 40, 1934, p. 917.

$u' \circ u \underline{=} u \circ u'' \underline{=} e$, where e denotes the identity element of the gruppoid, then it follows that any cancellable element of finite period is a unit.

We have as a corollary that if a quasi-group contains an element of finite order, it must contain an identity element. As another corollary of the previous theorem we may state that if a quasi-group contains a sub-gruppoid, then the quasi-group itself is a gruppoid, with the same identity element as the sub-gruppoid[18a]).

Consider a semi-group S with symbol of conjunction $\circ$ and symbol of relation $\underline{=}$, such that if $a \underline{=} b$, then a and b denote the same element of S; consider also a semi-group S' with symbol of conjunction $\circ'$ and symbol of relation $\underline{=}'$, such that if $c' \underline{=}' d'$, then c' and d' denote the same elements of S'. Let there be a correspondence between the elements of S and the elements of S' satisfying these conditions:

1. To each element a of S there corresponds just one element a' of S'.

2. Each element of S' is the image of at least one element of S under this correspondence.

3. If the elements a, b, c of S correspond respectively to a', b', c' of S', and if

$$a \circ b \underline{=} c$$

then

$$a' \circ' b' \underline{=}' c'.$$

Under these conditions S is said to be homomorphic with S'.

If the correspondence is one-to-one, and the relation 3. is reversible, then S and S' are said to be isomorphic.

We define the terms commutative, Abelian and centrum (central) as in group theory.

A semi-group S is said to be imbedded in a semi-group T if T contains a sub-semi-group S' isomorphic to S. We may note that a semi-group containing non-cancellable elements cannot be imbedded in any quasi-group. HOWEVER[19]), if a semi-group S contains cancellable elements all of which belong to the central of S, then S may be imbedded in a gruppoid S' whose cancellable elements form an Abelian group G such that the identity element of G is the identity element of S'.

[18a]) This result was noted by Dr. BARKLEY ROSSER.

[19]) VANDIVER, Amer. Jour. Math., 1940.

From now on we shall write AB for $A \circ B$, where no ambiguity arises from our doing so.

Let a semi-group S contain a sub-semi-group S', and let the non-equivalent elements of the latter be denoted by

(1) $$N_1, N_2, N_3, \ldots$$

Let C denote an element of S, and suppose that

(2) $$A_1, A_2, A_3, \ldots$$

denote all the non-equivalent elements of (1) such that

$$C \overset{\omega}{=} CA_1 \overset{\omega}{=} CA_2 \overset{\omega}{=} \ldots$$

The elements (2) form a semi-group which we shall call the right semi-group in S belonging to C with respect to S', with an analogous definition for left semi-group in S belonging to C with respect to S'. We call the number of elements in (2) the right spread of C in S with respect to S', with an analogous definition of left spread. We now prove[20])

Theorem 5. Let a semi-group S contain a sub-group G consisting of the elements (1), and let C denote any element of S. Further, suppose the identity element of G is a right identity of S. Let G' be the right semi-group in S belonging to C with respect to G. (G' is necessarily a group.) Assume that the elements of G can be distributed into right co-sets with respect to G'. Then the non-equivalent elements in the set

(2a) $$CN_1, CN_2, CN_3, \ldots$$

are the elements

$$CB_1, CB_2, CB_3, \ldots$$

where $B_1, B_2, B_3, \ldots$ are the multipliers of the distinct right co-sets of G with respect to G'.

We show first that the semi-group G' is a group. Since the identity element of G is a right identity of S, G' contains a right identity element. Since G is a group, each A_i has an inverse A_i^{-1} in G, and from $C \overset{\omega}{=} CA_i$ follows

$$CA_i^{-1} \overset{\omega}{=} CA_i A_i^{-1} \overset{\omega}{=} CE \overset{\omega}{=} C ,$$

where E is the identity of G, which was assumed to be a right identity of S. Hence each element of (2) has an inverse which belongs to G'; consequently G' is a group, and since it is con-

[20]) This theorem was stated without proof in Proc. Nat'l. Acad. Sci. v. 23, 1937, p. 553.

tained in G we may speak of the co-sets of G with respect to G' as in ordinary group theory. If we represent the right co-sets of G with respect to G' by

$$G' B_i , \; i = 1, 2, \ldots , s ,$$

where s is the index of G' in G, then the non-equivalent elements in CG are the elements CB_i. Since the $B's$ are in G, each CB_i is in CG. Also, since any N_i is in some right co-set, $N_i \eqq A B_j$, where A is in G'. Then $C N_i \eqq C A B_j \eqq C B_j$; hence every element of CG is included in the $CB's$. Finally, if

$$C B_r \eqq C B_t$$

then

$$C B_r B_t^{-1} \eqq C E \eqq C ,$$

where B_t^{-1} is the inverse of B_t in G. From this it follows that $B_r B_t^{-1}$ is an element of (2); that is,

$$B_r B_t^{-1} \eqq A, \text{ where } A \text{ is in } G',$$

whence

$$B_r \eqq A B_t, \text{ which is a contradiction,}$$

unless $r = t$. A similar result holds if we change the order of C and N_i in (2a).

It might be noted that if the identity element of the sub-group G is not an identity element for the semi-group S, then the set CG need not contain any element equivalent to C itself. In view of this fact, we make the following definition of co-sets in a semi-group:

Let S be a semi-group having a sub-semi-group S' whose elements are $N_1, N_2, N_3, \ldots$, and let C_1 be an element of S. The left co-set $C_1 S'$ is the set of non-equivalent elements of the set

(3) $$C_1 , C_1 N_1 , C_1 N_2 , \ldots$$

If this set does not exhaust S, in the sense of equivalence, let C_2 be an element of S not equivalent to any of the elements in (3), and consider

(4) $$C_2 , C_2 N_1 , C_2 N_2 , \ldots$$

We determine the non-equivalent elements in this set none of which are equivalent to any elements of (3), thus obtaining what we shall call a second left co-set of S with respect to S'. It may be possible to proceed in this fashion until S is exhausted, in which case we shall say that S has been distributed into left co-sets with respect to S'. We call the $C's$ the multipliers of the co-sets. An analogous definition may be given for right co-sets.

This distribution into co-sets is not necessarily unique, as is seen if we take for S the semi-group consisting of the elements

$$A, A^2, A^3, \ldots$$

with $$A^s \equiv A^k;\ 1 < k < s,$$

and let S' be the group formed by the elements

$$A^k, A^{k+1}, \ldots, A^{s-1}.$$

However, if we take S' to be a group whose identity element E is a right identity of S, then (3) reduces to

(3a) $$C_1 N_1, C_1 N_2, \ldots$$

since one of the $N's$ is the identity E of S', and $C_1 E \equiv C_1$. Similarly, the set (4) reduces to

(4a) $$C_2 N_1, C_2 N_2, \ldots$$

None of the elements of (3a) is equivalent to any of the elements of (4a), for, if

$$C_1 N_i \equiv C_2 N_j$$

then $$C_1 N_i N_j^{-1} \equiv C_2 E \equiv C_2,$$

contrary to hypothesis. If (3a) and (4a) do not exhaust S, in the sense of equivalence, we proceed to an element of S not equivalent to any of the elements in the two co-sets already set up, and so on. In this manner, it may be possible to represent the elements of S in a series of co-sets. If S is finite, this may be carried out in a finite number of steps. Analogous remarks hold for right co-sets.

Now set G in place of S', and let s_i be the right spread of C_i, where C_i is the multiplier of the i-th co-set with respect to G as above described. If n is the order of G, then s_i divides n, since the right semi-group belonging to C_i with respect to G is a subgroup of G. Let $s_i t_i = n$, and let the order of S be g. The co-set $C_i G$ is merely the set of non-equivalent elements in the set

$$C_i N_1, C_i N_2, \ldots$$

which we have shown to be the set

$$C_i B_1, C_i B_2, \ldots$$

The number of elements in the latter set is the index with respect to G of the right semi-group belonging to C_i with respect to G, or $t_i \left(= \frac{n}{s_i}\right)$. Since the co-sets exhaust S, then g is the sum of these indices.

Since G is a group, $N_i N_k$ runs through the elements of G as N_k does, for a fixed i. Hence the co-set $(C_h N_i)\, G$ is the same as the co-set $C_h G$, and the values of the $s's$ are independent of the choice of the $C's$. Thus we have

Theorem 6. Let a finite semi-group S contain a sub-group G whose identity element is a right (left) identity of S. Then the non-equivalent elements of S may be distributed into unique left (right) co-sets with respect to G. If n is the order of G, then $s_i t_i = n$, where s_i is the right (left) spread of C_i (the multiplier of the i-th co-set) with respect to G. If g is the order of S, then

$$g = \sum_{i=1}^{h} \frac{n}{s_i}$$

where h is the number of co-sets[20a]).

It follows immediately from the above that for a given S and G each s is an invariant. As an application of this theorem to a special case, let S be the semi-group of residue classes modulo 24 under multiplication, and let G be the group of residue classes modulo 24 corresponding to the integers prime to 24. We may then set up a system of eight co-sets for S with respect to G; the spreads of the multipliers will be 1, 2, 2, 4, 4, 4, 8, 8,

We now consider the notion of a given element being cancellable with respect to a set of elements in a semi-group. If C denotes an element of S, and

$$A_1, A_2, A_3, \ldots$$

denote elements of S such that from $CA_i \overset{\omega}{=} CA_j$ follows $A_i \overset{\omega}{=} A_j$, we say that C is left cancellable with respect to the set of $A's$, with a similar definition for C on the right. For example, if S contains an identity element E, then E is right and left cancellable with respect to any subset of S.

In particular, consider the finite set of non-equivalent elements

(5) $$A_1, A_2, \ldots, A_t$$

and suppose that

(6) $$CA_1, CA_2, \ldots, CA_t$$

are equivalent in some order to the elements of (5); then (5) is called a left repetitive set in S, with multiplier C. The

[20a]) This theorem was stated by the writer in a more general form, without proof, in Proc. Nat'l. Acad. Sci., 23, 1937, p. 554.

element C is left cancellable with respect to (5). It is obvious that the set of multipliers of a left (right) repetitive set forms a semi-group. It is also clear that the set of all non-equivalent elements of a finite semi-group $\boldsymbol{S}$ forms a left (right) repetitive set with respect to any left (right) cancellable element of $\boldsymbol{S}$ as a multiplier.

If $\boldsymbol{R}$ is a repetitive set and C a multiplier, then C need not be in $\boldsymbol{R}$; neither is $\boldsymbol{R}$ necessarily a semi-group, as is seen from the example of the set of residues 3 and $3 \cdot 4$ modulo 5, with multiplier 4. Now 4 is not in the set; the product $3 \cdot 3 \cdot 4$ is likewise not in the set, so that the repetitive set in this case does not form a semi-group.

It is possible to generalize this notion. Adjoin to $\boldsymbol{S}$, if necessary, an identity element so as to obtain a gruppoid; then suppose that the elements of the set (6) are equivalent in some order to the non-equivalent elements

$$\varepsilon_1 A_1, \varepsilon_2 A_2, \ldots, \varepsilon_t A_t$$

where the $\varepsilon' s$ belong to a sub-semi-group $\boldsymbol{S}'$ of $\boldsymbol{S}$. We say then that (5) is a left repetitive set in $\boldsymbol{S}$ with respect to $\boldsymbol{S}'$ and with multiplier C. We have an analogous definition for right repetitive sets in $\boldsymbol{S}$ with respect to $\boldsymbol{S}'$. If $\boldsymbol{R}$ is both a right and a left repetitive set in $\boldsymbol{S}$ with respect to S' and with multiplier C, we say that $\boldsymbol{R}$ is a repetitive set in $\boldsymbol{S}$ with respect to $\boldsymbol{S}'$ and with multiplier C.

Use the notation for the multipliers of the co-sets employed in the proof of theorem 6, and assume that $\boldsymbol{S}$ is commutative and may be represented by means of a finite number of co-sets, and that said multipliers may, therefore, be written

$$C_1, C_2, \ldots, C_k \tag{7}$$

We shall now show that the above is a repetitive set in $\boldsymbol{S}$ with respect to the group $\boldsymbol{G}$, with any element of $\boldsymbol{S}$ as multiplier. Let D denote an arbitrary element of $\boldsymbol{S}$, and suppose further that $\boldsymbol{S}$ is a quasi-group. Consider

$$C_1 D, C_2 D, \ldots, C_k D \tag{8}$$

As in the proof of theorem 6, any one of these elements may be written in the form $C_i N_j$.

We now show that if $C_r D \equiv C_a N_{a_1}$ and $C_s D \equiv C_a N_{a_2}$ then $r = s$. For, the above relations give

$$C_a N_{a_2} C_r D \equiv C_a N_{a_1} C_s D$$

and since S is a quasi-group, we obtain

$$N_{a_2} C_r \equiv N_{a_1} C_s ,$$

whence $r = s$, since otherwise we have elements equivalent, yet in different co-sets. Hence the

Theorem 7. If a commutative quasi-group S contains a subgroup G, and S may be distributed into a finite number of co-sets with respect to G, and the multipliers of the co-sets are the elements of the set (7), then (7) forms a repetitive set with respect to G with any element of S as multiplier.

This theorem leads to the abstract form of many patterns in number theory. In particular, if we take the elements of (8), and write them in the form

(8a) $$C_1 n_1 , C_2 n_2 , \ldots , C_k n_k$$

where the $n's$ are elements of G, and, further, suppose that S is Abelian or commutative, then (8) and (8a) give

$$D^k \prod_{s=1}^{k} C_s \equiv \prod_{s=1}^{k} n_s \prod_{s=1}^{k} C_s ,$$

and since S is a quasi-group, we obtain

$$D^k \equiv \prod_{s=1}^{k} n_s .$$

To apply the above to the theory of algebraic fields, let K be an algebraic field containing the cyclotomic field defined by

$$\zeta = e^{2\pi i/l} ,$$

l being a prime. If α is any integer in K prime to the prime ideal $\mathfrak{p}$ then

$$\alpha^{\frac{N(\mathfrak{p})-1}{l}} \equiv \zeta^h \pmod{\mathfrak{p}} ,$$

where $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$. The multiplicative group of the algebraic integers in K which are prime to $\mathfrak{p}$, of order $N(\mathfrak{p})-1 = l\,t$ contains as a subgroup the elements

$$1, \zeta, \zeta^2, \ldots, \zeta^{l-1} ,$$

A set of multipliers of the co-sets of this whole group with respect to the subgroup mentioned form a repetitive set with respect to the included group, with any integer in the field prime to p as

multiplier, and we may apply theorem 7. In particular, if K is the rational field, and $l = 2$, the subgroup consists of the elements 1 and -1 modulo the rational prime $p \neq 2$, and the multipliers of the co-sets may be taken as

$$1, 2, \ldots, \frac{(p-1)}{2}.$$

This gives GAUSS' lemma in the theory of quadratic residues.

Symmetric functions of the elements in a repetitive set contained in a finite ring, in particular elements of a Galois field with respect to a subgroup in the multiplicative field, are considered in another paper[21]).

We shall now extend an abstract form of the DEDEKIND inversion formula to semi-groups[22]). Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ is an integer greater than 1, the $p's$ being distinct primes. Let $h(d)$ be a function on the set of divisors of n to the elements of a commutative semi-group S. For n' any divisor of n, set, in the sense of a semi-group product,

$$F(n') = \prod_d h(d) ,$$

where d ranges over the distinct divisors of n'. Furthermore, let

$$\Pi_i = \Pi F\left(\frac{n}{p_{r_1} p_{r_2} \cdots p_{r_i}}\right) ; \; i > 0$$

the product being taken over all different combinations of i distinct primes from the set $p_1, p_2, \ldots, p_s$. Let

$$\Pi_0 = F(n) ,$$

Then

$$h(n) \prod_{q=1}^{\left[\frac{s+1}{2}\right]} \Pi_{(2q-1)} = \prod_{q=0}^{\left[\frac{s}{2}\right]} \Pi_{2q} \text{ for } s \geq 1 . \tag{9}$$

Let n_1 be any divisor of n. Rearrange the subscripts of the $p's$ so that $p_1, p_2, \ldots, p_{s_1}$ are the primes appearing in the factorization of the integer $\frac{n}{n_1}$. Then n_1 divides $\frac{n}{p_1 p_2 \cdots p_{s_1}}$ but does not divide $\frac{n}{p_j}$, $s_1 < j \leq s$. Consequently Π_k does not involve $h(n_1)$ for

[21]) Annals of Math., v. 18, 1917, pp. 105—114.

[22]) The writer gave the result proved here in the case when the semi-group employed is a group, in a lecture in Princeton in 1934. Dr. LEHMER, shortly after, pointed out that an analogous result held for semi-groups.

$k > s_1$, but for $k \leq s_1$, Π_k has $h(n_1)$ as a factor as many times as k integers can be chosen from the set $p_1, p_2, \ldots, p_{s_1}$; namely, $C_{s_1,k}$ times. Thus, the excess of the degree to which $h(n_1)$ appears in the right member of (9) over the degree to which $h(n_1)$ appears in the left member is

$$(1 + C_{s_1,2} + C_{s_1,4} + \cdots) - (C_{s_1,1} + C_{s_1,3} + \cdots),$$

or simply $(1-1)^{s_1} = 0$; and the identity (9) is established.

In particular, if $s = 1$, we have

$$h(n)\,\Pi_1 = \Pi_0,$$

or simply

$$h(n)\,h(1) = h(1)\,h(n).$$

In the excluded case $n = 1$, we have trivial relation

$$h(1) = F(1).$$

In the special case of a commutative group G, the relation (9) takes the form

$$h(n) = \prod_{t=0}^{s} \Pi_t^{(-1)^t}.$$