ANNALS OF MATHEMATICS
Vol. 36, No. 1, January, 1935

CONDITIONS FOR FACTORIZATION IN A SET CLOSED UNDER A SINGLE OPERATION

BY MORGAN WARD

(Received October 20, 1934)

1°. Consider a system S consisting of a set of elements $a, b, c, \cdots$ over which an equality relation and a binary operation multiplication have been defined satisfying the following four conditions.

P 1 *To every pair of elements a, b of S there corresponds an element c of S unique to within equal elements.* We write $c = ab$.

P 2 *If $a = a'$ and $b = b'$ then $ab = ab' = a'b = a'b'$.*

P 3 *$a(bc) = (ab)c$ for all a, b, c in S.*

P 4 *$ab = ba$ for all a, b in S.*

Recently A. H. Clifford[1] and others have considered the following problem: to determine what additional conditions it is necessary to impose on S in order that each integral element in it may be uniquely resolved into a product of powers of irreducible elements (up to unit factors) as in the case when S is the set of positive integers and the operation ordinary multiplication.[2]

I propose to show here that we can discard the requirement of *unicity* in the resolution into prime factors and still retain many of the essential features of common arithmetic. The set of conditions which I shall develop will assign to each integral element a certain canonical decomposition into prime factors to which it is equivalent. If we know this canonical decomposition, we know all divisors of the element and the canonical decomposition of each divisor. Any two elements of the system will have a least common multiple, and if they have any common divisors, a greatest common divisor. On the other hand, we cannot obtain the canonical decomposition of a product from a knowledge of the canonical decompositions of its factors, nor need irreducible elements be primes.[3]

We shall show that our system includes as special instances the arithmetics previously discussed by J. Koenig,[4] Clifford,[1] Fritz Klein[5] and others.

2°. We must first lay down a few definitions. a is said to divide b either if

---

[1] Bulletin Am. Math. Soc. 40 (1934), pp. 326–330. We shall refer to this paper as Clifford.

[2] We refer to this case hereafter as common arithmetic.

[3] An element of S is called a prime if it cannot divide the product of two elements of S without dividing at least one factor.

[4] *Algebraischen Grössen*, Leipzig (1903), Chapters 1, 4.

[5] Math. Annalen 106 (1932), pp. 114–130; Math. Zeitschr. 37 (1933), pp. 39–60.

$a = b$ or if there exists an element c such that $ac = b$. We write then $a \mid b$. We observe that

(1) If $a_i \mid b_i$, $(i = 1, \cdots, k)$, then $a_1 \cdots a_k \mid b_1 \cdots b_k$.

(1) is untrue if multiplication is not commutative.

If $a \mid b$ and $b \mid a$, a and b are said to be associate, written $a \backsim b$. Non-associate elements are said to be distinct. If $a \mid x$ for every x in S, a is called a unit. Non-units are called integral elements. A divisor of an element is called proper if it is neither a unit nor an associate. Units have no proper divisors. An integral element with no proper divisors is called an irreducible. An element with only one distinct irreducible divisor is called a power of that divisor. The number of distinct proper divisors of a power increased by unity is called its multiplicity. We write $p^{(n)}$ for a power of the irreducible p of finite multiplicity n. Thus $p^{(1)} \backsim p$.

An element a of S is called indecomposable if in every decomposition of a into a product of two or more factors, one of the factors is associate to a. An irreducible is necessarily indecomposable. To avoid trivialities, we shall assume

P 5 *S contains at least one integral element.*

We shall call a system which satisfies the five postulates P 1 – P 5 a band.[6]

3°. The next four postulates complete our definition of S.

P 6 *Every element of S has only a finite number of distinct divisors.*

P 7 *Two powers of the same irreducible are either equivalent or else one divides the other.*

P 8 *If an element of S is divisible by two distinct irreducibles, it is decomposable.*

P 9 *If an element of S is divisible by a number of other elements each of which is a power of a different distinct irreducible, then it is divisible by their product.*

We shall call any system satisfying all nine of our postulates an abstract arithmetic. The simplest such systems are common arithmetic with our operation interpreted either as addition, multiplication or the operation of finding a least common multiple of two or more integers.

All of our postulates save P 5 and P 9 are used by Fritz Klein in defining his "B-Menge."[7] But P 9 is also true in a B-Menge since multiplication there is idempotent. *Therefore every B-Menge containing integral elements is an abstract arithmetic.*

J. Koenig[8] and A. H. Clifford define a power of p of multiplicity n as $p \cdot p \cdots p$ to n factors. But since factorization is unique in both systems, a power of p in their sense will be a power of p in our sense, and P 7 and P 9 will be both satisfied in each system. P 6 is a postulate in Koenig's system, and P 8 is satisfied because Koenig's system is a semi-group. In Clifford's system P 6 is replaced by the weaker "Teilerketten" condition, but it is true by virtue

[6] This convenient term was suggested by Dr. A. H. Clifford.

[7] Math. Zeitschr., place cited, especially pp. 47–54.

[8] J. Koenig's system is identical with F. Klein's "A-Menge." (Math. Zeitschr., volume cited, pp. 42–47.)

of the unique factorization. P 8 obviously holds since no indecomposables save units appear in Clifford's system. Hence: *A band satisfying the Clifford conditions for unique decomposition*[9] *is an abstract arithmetic. A commutative semigroup*[10] *in which* P 6 *holds and in which all irreducibles are primes is an abstract arithmetic.*

4°. It follows from P 5 and P 6 that S contains at least one irreducible, and that every integral element has at least one irreducible divisor. Furthermore, every power is of finite multiplicity, and from P 7 it readily follows that the m distinct divisors of $p^{(m)}$ are equivalent to $p^{(1)}, p^{(2)}, \cdots, p^{(m)}$. Furthermore, $p^{(n)} \mid p^{(m)}$ when and only when $n \leqq m$.

Consider now any integral element a of S. If a is a power, it is uniquely representable in the form $a \backsim p^{(n)}$. In the contrary case, we deduce from P 8, P 6 and P 7 that a decomposition of a exists of the form

$$a \backsim p_1^{(\alpha_1)} p_2^{(\alpha_2)} \cdots p_k^{(\alpha_k)} \tag{2}$$

where $p_1, p_2, \cdots, p_k$ are distinct irreducibles.

In discussing such decompositions, it is convenient to allow powers to have the superscript zero, with the understanding that such a power is to be omitted from the decomposition.[11] Thus, for example, $a \backsim p_1^{(2)} p_2^{(4)} p_3^{(0)} p_4^{(0)} \backsim p_1^{(0)} p_2^{(0)} p_3^{(1)} p_4^{(1)}$ is to be taken merely as another way of writing $a \backsim p_1^{(2)} p_2^{(4)} \backsim p_3^{(1)} p_4^{(1)}$.

With this understanding, let $p_1, p_2, \cdots, p_k$ now stand for all the distinct irreducibles of S which divide a. These are finite in number by P 6. Suppose that a has in all s distinct decompositions of the form (2),

$$a \backsim p_1^{(\alpha_1)} p_2^{(\alpha_2)} \cdots p_k^{(\alpha_k)} \backsim p_1^{(\beta_1)} p_2^{(\beta_2)} \cdots p_k^{(\beta_k)} \backsim \cdots \backsim p_1^{(\lambda_1)} p_2^{(\lambda_2)} \cdots p_k^{(\lambda_k)} \tag{3}$$

when the superscripts $\alpha, \beta, \cdots, \lambda$ are now positive integers or zero. The number s of such sets is finite by P 6, since $p^{(n)}$ and $p^{(m)}$ are distinct if $n \neq m$.

Let $\mu_i = \max(\alpha_i, \beta_i, \cdots, \lambda_i), \quad (i = 1, \cdots, k)$.

Then $p_i^{(\mu_i)} \mid a$. Hence by P 9, $p_1^{(\mu_1)} \cdots p_k^{(\mu_k)} \mid a$. But $p_i^{(\alpha_i)} \mid p_i^{(\mu_i)}$, $(i = 1, \cdots, k)$. Therefore, by (1),

$$p_1^{(\alpha_1)} p_2^{(\alpha_2)} \cdots p_k^{(\alpha_k)} \mid p_1^{(\mu_1)} p_2^{(\mu_2)} \cdots p_k^{(\mu_k)}.$$

Hence

$$a \backsim p_1^{(\mu_1)} p_2^{(\mu_2)} \cdots p_k^{(\mu_k)}. \tag{4}$$

---

[9] Clifford, p. 328, Theorem 1.

[10] This system is merely a band with the additional condition that $ab = ac$ when and only when $b = c$.

[11] If S contains units, we would define $p^{(0)}$ as an associate to a unit. The simplification resulting from adjoining a unit or an identity element to the abstract system is lost in the applications to ring theory where the ring need contain no units, and the additive properties of the adjoined elements must be considered.

Thus the decomposition (4) appears among the set (3). We shall call it the canonical decomposition of a.

5°. If $b \backsim q_1^{(\nu_1)} q_2^{(\nu_2)} \cdots, q_e^{(\nu_e)}$, it is clear that necessary and sufficient conditions that $b \mid a$ are that every q be a p and that the multiplicity of each $q^{(\nu)}$ be less than or equal to the multiplicity of the corresponding $p^{(\mu)}$. Hence the divisors of a are given by the set of elements $p_1^{(n_1)} p_2^{(n_2)} \cdots p_k^{(n_k)}$, $(n_i = 0, 1, \cdots, \mu_i; i = 1, \cdots, k)$.

Given two integral elements c and d, let $s_1, s_2, \cdots, s_m$ be the distinct irreducible elements dividing either or both of them. With the convention adopted in section 4°, we may write their canonical decompositions in the form

$$c \backsim s_1^{(\gamma_1)} \cdots s_m^{(\gamma_m)}, \qquad d \backsim s_1^{(\delta_1)} \cdots s_m^{(\delta_m)}.$$

Then if $\theta_i = \max(\gamma_i, \delta_i)$, $\zeta_i = \min(\gamma_i, \delta_i)$, $(i = 1, \cdots, k)$ it is clear that

$$[c, d] \backsim s_1^{(\theta_1)} \cdots s_m^{(\theta_m)}, \qquad (c, d) \backsim s_1^{(\zeta_1)} \cdots s_m^{(\zeta_m)}$$

are the least common multiple and greatest common divisor of c and d in the sense of common arithmetic. Moreover $c \backsim [s_1^{(\gamma_1)}, s_2^{(\gamma_2)}, \cdots, s_m^{(\gamma_m)}]$.

If we assume that S contains a unit, so that c and d will always have a common divisor, it is easily verified that the operations $[x, y]$ and (x, y) just defined satisfy Klein's postulates for a "Sternverband."[12] Hence even if we do not have unique decomposition with respect to multiplication, we always have unique decomposition with respect to the least common multiple operation.

THE INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.

[12] Annalen paper already cited.