the forms (10) become

$$\sum_{i=0}^{n}\sum_{j=0}^{n}\Delta^{(i+j)}f(c)\,\eta_i\eta_j. \tag{11}$$

If $\eta_0=\eta_1=\cdots=\eta_{n-1}=0$, $\eta_n=1$, we see that

$$\Delta^{(2n)}f(c)\geqq 0.$$

Since $f(x)$ is continuous by hypothesis, we may apply Lemma 2 and deduce that $f(x)$ is analytic in $a<x<b$. In (11) replace η_i by η_i/δ and let δ approach zero. We thus obtain

$$\sum_{i=0}^{n}\sum_{j=0}^{n}f^{(i+j)}(c)\,\eta_i\eta_j\geqq 0,$$

and by Lemma 3, the function $f(x)$ has the form (9). This completes the proof of the theorem.

HARVARD UNIVERSITY

ARITHMETIC AND IDEAL THEORY OF ABSTRACT MULTIPLICATION*

BY A. H. CLIFFORD

If we are given a ring R we may be called upon to answer the following two questions.

1. Is every element of R uniquely decomposable into prime elements?

2. If not can we introduce *ideal* elements into R such that the resulting system has this property?

Since these questions can be put in terms involving only the operation of multiplication, it is natural to attempt a solution in the same terms. We start, therefore, with a group-like system in which multiplication only is defined, namely a class S satisfying the following postulates:

---

* A statement of definitions and results of a thesis done under Professors E. T. Bell and Morgan Ward at the California Institute of Technology.

(Added in proof.) I find that ovoid ideals were first discovered by I. Arnold, *Ideale in kommutativen Halbgruppen*, Recueil Mathématique, Moscou, vol. 36 (1929), pp. 401–407. Arnold proves Theorem 4 for regular ova (which he calls commutative semi-groups), with a slightly different normal ideal arithmetic.

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* $ab = a'b'$.

P_3. $a(bc) = (ab)c$ *for all* a, b, c *in* S.

P_4. $ab = ba$ *for all* a, b *in* S.

P_5. *There exists an element* i *in* S *such that* $ia = ai = a$ *for all* a *in* S. This element, evidently unique, is called the *identity element* of S.

Following E. T. Bell, we call such a system an *ovum*.* An element a of S is said to divide an element b of S, written $a \mid b$, if the equation $ax = b$ has a solution x in S. Two elements a, b of S are *associate*, written $a \sim b$, if they divide each other. Elements associate to the identity i are called *unities*. Non-associate elements are called *essentially distinct*. We say that a is a proper divisor of b, written $a \| b$, if a divides b but b does not divide a. An element of S having a proper divisor in S other than i is called *reducible*; otherwise, *irreducible*. An element of S is called *decomposable* if it is the product of two proper divisors of itself; otherwise, *indecomposable*. An element of S is called *prime* if the relation $p \mid ab$ implies that either $p \mid a$ or $p \mid b$, and *completely prime* if the relation $p^r \mid ab$ implies that either $p^r \mid a$ or $p^r \mid b$, for every positive integer r. The *index* of an element of S is the number of essentially distinct powers thereof. If a is of index r, then its first r powers $a, a^2, \cdots, a^r$ are essentially distinct, and all higher powers are associate to a^r. If all the powers are essentially distinct, we say that a is of *infinite index*.

An element a of S is said to be *decomposable into irreducible elements* if a finite number of essentially distinct irreducibles $p_1, p_2, \cdots, p_r$ and a unit e exist in S such that

$$a = e p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

where the α_i are positive integers. The decomposition is said to be *unique* if the existence of another,

$$a = e' q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},$$

* E. T. Bell, *Unique decomposition*, American Mathematical Monthly, vol. 37 (1930), pp. 400–418. The non-commutative case has been treated by Morgan Ward, *Postulates for an abstract arithmetic*, Proceedings of the National Academy of Sciences, vol. 14 (1928), pp. 907–911.

implies that

(i) $$r = s,$$

and (by suitable numeration)

(ii) $$p_i \sim q_i, \quad p_i^{\alpha_i} \sim q_i^{\beta_i}, \qquad (i = 1, 2, \cdots, r).$$

The second of these is equivalent to the statement that either $\alpha_i = \beta_i$ or else neither α_i nor β_i is less than the index of P_i.

An ovum S is said to *admit unique decomposition* if every element of S is uniquely decomposable into irreducible elements of S. The ensuing theorem gives an elementary set of criteria in answer to question 1.

THEOREM 1. *The following conditions are necessary and sufficient that an ovum S admit unique decomposition*:

I. *Teilerkettensatz. If $a_{n+1} \| a_n$, then the sequence $a_1, a_2, \cdots$ must terminate.*

II. *Every reducible element of S is decomposable.*

III. *Every irreducible element of S is completely prime.*

If S is a ring, II *can be replaced* by*

IIA. *Vielfachenkettensatz. If $a_n \| a_{n+1}$, then either the sequence $a_1, a_2, \cdots$ terminates, or no element $\neq 0$ of S is divisible by every a_n.*

Let us denote by xA the class of elements xa as a ranges over the class A. A class A of elements of S is called an *ovoid ideal* if it includes all elements s of S such that, for every element x of S, xs is divisible by all the common divisors of xA in S. This is substantially equivalent to a definition given by H. Prüfer.† If S is a ring, every ovoid ideal is a Dedekind ideal, but the converse is not necessarily true. Ideals will be denoted by small German letters. An ideal is called a principal ideal if it is identical with the set of multiples of a single element of S.

A common divisor of a class A of elements of S is called a *greatest common divisor* (G.C.D.) thereof if it is divisible by all

* Thanks to a clever device invented by A. Fraenkel, *Über die Teiler der Null und die Zerlegung von Ringen*, Journal für Mathematik, vol. 145 (1915), pp. 139–176.

† H. Prüfer, *Untersuchungen über Teilbarkeitseigenschaften in Körpern*, Journal für Mathematik, vol. 168 (1932), pp. 1–36.

other common divisors of A. It is plainly unique to within associate elements.

THEOREM 2. *The condition* III *of Theorem* 1 *can be replaced by the condition that every ovoid ideal be a principal ideal. This in turn can be replaced by the two conditions*:

IIIA. *Every pair* a, b *of elements of* S *has a* G.C.D. (a, b) *in* S.

IIIB. $(a, b)c = (ac, bc)$ *for all* a, b, c *in* S.

By a *regular* ovum we mean one in which cancellation is permissable, that is, $ac = bc$ always implies $a = b$. Condition II is satisfied for regular ova, and IIIB is a consequence of IIIA, leaving only I and IIIA. These conditions are practically those given by J. Koenig,* so that Theorem 2 is simply an extension of Koenig's elegant result to the irregular case. The sets of criteria (I, IIA, III) and (I, IIA, IIIA, IIIB) for general commutative rings involve only multiplication, yet they are not applicable to unrestricted ova.

Most of the theory of Dedekind ideals can be carried over bodily to that of ovoid ideals. In particular, in the case of regular ova, Krull's form of Noether's conditions† that the set of Dedekind ideals in a ring admit unique decomposition goes over unchanged. For the irregular case we find, as in the proof of Theorem 4 below, that the following set of conditions is useful. This is simply a corollary of Theorem 2.

THEOREM 3. *The following conditions are necessary and sufficient that the set of ovoid ideals of an ovum* S *admit unique decomposition*:

I. *Teilerkettensatz*: *If* $\mathfrak{a}_{n+1} \supset \mathfrak{a}_n$ (*proper inclusion*) *then the sequence of ideals* $\mathfrak{a}_1, \mathfrak{a}_2, \cdots$ *of* S *must terminate.*

II. $\mathfrak{a} \supseteq \mathfrak{c}$ *implies the existence of an ideal* $\mathfrak{b}$ *of* S *such that* $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$.

III. *Every reducible ideal is decomposable.*

Proceeding now to the second question mentioned at the beginning, we say that an ovum S admits an ovum Σ as an *ideal arithmetic* if S is a subovum of Σ and Σ admits unique

* J. Koenig, *Algebraischen Grössen*, 1903, Chapters 1 and 4.

† See B. L. van der Waerden, *Moderne Algebra*, 1931, vol.2, pp. 97–104.

decomposition. An ideal arithmetic Σ of S is said to be *normal* if

(i) *every element of* Σ *divides some element of* S;

(ii) *if* $a \mid b$ *relative to* Σ, a *and* b *being in* S, *then* $a \mid b$ *relative to* S;

(iii) *every element of* Σ *is the G.C.D. of its multiples in* S.

THEOREM 4. *If an ovum* S *admits a normal ideal arithmetic* Σ, *then the set of ovoid ideals in* S *also constitutes a normal ideal arithmetic of* S, *being in fact simply isomorphic with* Σ.

This theorem gives only a partial answer to the question, in that it tells us only whether or not a given ovum admits a *normal* ideal arithmetic of any kind. It does, however, tell us that if an ovum (or ring) admits a normal ideal arithmetic, including Dedekind ideals and Prüfer's "finite" ideal numbers,* then there is essentially only one, which is completely characterized by the three requirements (i), (ii), and (iii). This extends Prüfer's isomorphism between his finite ideal numbers and Dedekind ideals, when these systems admit unique decomposition, to all possible normal ideal arithmetics.The conditions of Theorem 3 are thus criteria for the existence of a normal ideal arithmetic of any kind.

Ovoid ideals bear an important relation to question 1 because of the fact that the condition that every ideal be a principal ideal is necessary if S is to admit unique decomposition. They bear an important relation to question 2 because of the fact that *they* must admit unique decomposition if S is to admit a normal ideal arithmetic of *any* kind. The single (extreme) example of the ring of polynomials with integer coefficients shows that Dedekind ideals are far from having either of these properties. Whatever interesting and useful properties other types of ideals may have which ovoid ideals lack, there can be no doubt that, for the specific purpose of answering these two questions, the ovoid variety are in point of fact *ideal.*

CALIFORNIA INSTITUTE OF TECHNOLOGY

* H. Prüfer, *Neue Begründung der algebraischen Zahlentheorie*, Mathematische Annalen, vol. 94 (1925), pp. 198–243.