Γ. Let $\bar{\lambda}_1, \ldots, \bar{\lambda}_r$ be any set of complex numbers and let the resulting numerical equation

$$f(x; \bar{\lambda}_1, \ldots, \bar{\lambda}_r) \equiv x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad (2)$$

have the group Γ_0 with respect to $K(a_1, \ldots, a_n)$. Then Γ_0 is a sub-group of Γ.

We shall next consider a normal division algebra A, in n^2 units, over K. It is known that if $u_1, \ldots, u_m$ are a basis of A and $\lambda_1, \ldots, \lambda_m$ are independent variables in K, the general element of A,

$$a = \lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_m u_m, \; m = n^2$$

is a root of a uniquely defined rank equation $f(x, \lambda_1, \ldots, \lambda_m) = 0$ with leading coefficient unity and further coefficient polynomials, with coefficients in K, of $\lambda_1, \ldots, \lambda_m$. Also the degree of f is n. We have proved, using theorem 1 and the known theory of division algebras, the theorem:

THEOREM 2. Let A be a normal division algebra over K. Then the group of its rank equation with respect to K is the symmetric group.

Applying the Hilbert irreducibility theorem we have

THEOREM 3. Every normal division algebra A, in n^2 units, over F contains an infinity of elements each satisfying an equation of degree n, with leading coefficient unity and further coefficients in K, such that the group of the equation with respect to K is the symmetric group.

[1] NATIONAL RESEARCH FELLOW.

POSTULATES FOR AN ABSTRACT ARITHMETIC

BY MORGAN WARD

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY

Communicated October 29, 1928

1. *Introduction.*—In a previous communication ("General Arithmetic," These PROCEEDINGS, November, 1927) I have described an "arithmetic" as a system in which

(*a*) Every element is completely specified by a finite number of cardinal numbers.

(*b*) "Division" is not always possible, and we can find when one element divides another in a finite number of steps.

(*c*) Unique resolution into "prime factors" is always possible.

I here give a precise definition of an abstract arithmetic, that is, one whose elements are marks in the technical sense, and state a few of its simpler properties. The principal advance over the work summarized

in "General Arithmetic" lies in the fact that I no longer assume that "multiplication" is commutative.

2. *Definition of an Arithmetic.*—A system Σ consisting of a denumerable set of elements $a, b, \ldots$ and a function $x \circ y$ is said to form an *abstract arithmetic* if the following six conditions are satisfied:

POSTULATE 1; CLOSURE.—For any two elements a, b of Σ, $a \circ b$ is a uniquely determined element of Σ.

POSTULATE 2; ASSOCIATIVITY.—For any three elements a, b, c of Σ,

$$(a \circ b) \circ c = a \circ (b \circ c).$$

POSTULATE 3; EXISTENCE OF IDENTITY.—There exists an element i of Σ such that $i \circ i = i$.

POSTULATE 4; CANCELATIVITY.—If a, b, c, b', c' are any five elements of Σ, and if

$$b \circ a \circ c = b' \circ a \circ c',$$

then

$$b \circ c \backsim b' \circ c'. \tag{1}$$

(for the meaning of the symbol $\backsim$, see §4 (*iv*))

$$b = b' \quad \text{If} \quad c = c' \tag{2}$$

$$c = c' \quad \text{If} \quad b = b'. \tag{3}$$

POSTULATE 5; INTEGRALITY.—(1) There exists at least one integral element.

(2) Every integral element has only a finite number of distinct integral divisors. (For the meanings of *integral element* and *distinct integral divisor*, see §4(*iii*), (*iv*).)

POSTULATE 6; PRIMITIVITY.—If a divides $b \circ c$, then a is not prime to both b and c. (For meanings of *divide* and *prime*, see §4 (*v*), (*vii*).)

3. *Properties of the Postulates.*—The six postulates above are consistent; and, with the possible exception of Pos. 2, they are independent. Pos. 3, though not strictly necessary, greatly simplifies the statement of Pos. 4. It is satisfied in all the instances of an arithmetic of practical interest. If Pos. 5 (1) is contradicted, Pos. 5 (2) asserted, Σ is a finite group. If both parts of Pos. 5 are contradicted, omitting the word integral Σ is an infinite discrete group. The consequences of asserting the first part of Pos. 5 and contradicting the second are not known; they would appear to be trivial.

If Pos. 6 is contradicted, the introduction of ideals is necessary to restore unique factorization. These ideals can be constructed abstractly; they are additional marks which we adjoin to Σ. Their complete theory is known. Postulates 1, 2, 4—(2) (3) are due to Dickson (*Transactions A. M. S.*, vol. **6**, 1905, pp. 205–208) and serve to define a semi-group.

4. *Elementary Properties of an Arithmetic.*—The following results are easily deduced from the postulates in §2.

(*i*) THE IDENTITY.—The element i of Pos. 3 is unique. It is called the identity of Σ, and denoted by *1*. For every element s of Σ,

$$1 \circ s = s \circ 1 = s$$

(*ii*) UNITS.—If for any element a of Σ there exists an element a', such that

$$a \circ a' = 1,$$

a is called a *unit* and a' its inverse.

1 is a unit, and the units of Σ form a group, denoted by E. We use $\epsilon, \epsilon', \ldots$ to denote units. If

$$a \circ b \circ \ldots \circ k = \epsilon, \text{ then } a, b, \ldots k$$

are all units.

(*iii*) INTEGRAL ELEMENTS.—Every element of Σ which is not a unit is called an integral element, and Σ contains an infinite number of integral elements.

(*iv*) EQUIVALENCE.—Two integral elements a, b are said to be equivalent if there exists units ϵ, ϵ' such that

$$\epsilon \circ a \circ \epsilon' = b$$

NOTATION. $a \backsim b$

The relation $\backsim$ is transitive, symmetric and reflexive. It is trivial in E, but not all integral elements are equivalent. Two elements which are not equivalent are said to be distinct.

THEOREM A.—If $b \circ a \circ c \backsim b' \circ a' \circ c'$ and $a \backsim a'$, then $b \circ c \backsim b' \circ c'$.

(*v*) DIVISION.—a is said to divide b if there exists two elements x, y of Σ, such that

$$x \circ a \circ y = b.$$

NOTATION. $a \; D \; b$

The relation D is transitive, non-symmetric and reflexive. The necessary and sufficient condition that two elements of Σ be equivalent is that they both divide each other.

THEOREM B.—If $a \; D \; b$ and $a \backsim a'$, $b \backsim b'$, then $a' \; D \; b'$.

(*vi*) IRREDUCIBLE ELEMENTS.—An element of Σ whose only integral divisor is itself is said to be irreducible. Equivalent elements are simultaneously reducible or irreducible.

(*vii*) COMMON DIVISORS.—Let b, c be two distinct integral elements of Σ. Every integral element a which divides both b and c is called a common divisor of b and c.

(*viii*) CO-PRIME ELEMENTS.—Two elements a and b of Σ without any common divisors are said to be co-prime. We also say a is prime to b.

NOTATION. $a\ P\ b$

The relation P is intransitive, symmetric and irreflexive.

5. *Fundamental Theorem of Arithmetic.*—"Every integral element of Σ can be resolved in one way only into a product of irreducible elements, provided we take no account of unit factors, nor of the order in which the irreducible elements occur."

Proof.—Let s be any integral element of Σ. By Pos. 5, s has only a finite number of distinct irreducible divisors. Suppose that

$$s \backsim a_1 \circ a_2 \circ \ldots \circ a_k \backsim b_l \circ b_2 \circ \ldots \circ b_l$$

are two resolutions of s into products of irreducible factors, so that a, b' are irreducible, but not necessarily distinct. (See §4 (*v*).) Consider any a_u $(1 \leqq u \leqq k)$

Since $a_u\ D\ s$, $a_u\ D\ (b_1 \circ \ldots \circ b_l)$ by theorem B. Therefore, by Pos. 6, either

(a) a_u and b_1 have a common factor, or

(b) a_u and $b_2 \circ \ldots \circ b_l$ have a common factor. Now clearly if (a) is true $a_u \backsim b_1$; but if (a) is false

$$a_u\ D\ (b_2 \circ \ldots \circ b_l)$$

since a_u is irreducible. Hence, by Pos. 6 again, either

(a') a_u and b_2 have a common factor, or

(b') a_u and $b_3 \circ \ldots \circ b_l$ have a common factor. If (a') is true,

$$a_u \backsim b_2.$$

Proceeding in this way we see that

$$a_u \backsim b_v \qquad (1 \leqslant v \leqslant l).$$

But $a_1 \circ \ldots \circ a_k \backsim b_1 \circ \ldots \circ b_l$ hence

$$a_1 \circ a_2 \circ \ldots \circ a_{u-1} \circ a_{u+1} \circ \ldots \circ a_k \backsim$$
$$b_1 \circ b_2 \circ \ldots \circ b_{v-1} \circ b_{v+1} \circ \ldots \circ b_e$$

by theorem A.

Thus every a divides a b and, similarly, every b divides an a, so that $l =$

k and $b_1 \circ \ldots \circ b_l$ consists of the irreducible factors a of s taken perhaps in a different order.

6. *Instances of an Arithmetic.*—The rational integers, the complex integers and Dedekind ideals are instances of an abstract arithmetic. The set of all square non-singular matrices of order m taken over an arbitrary ring satisfy the first five of these postulates, with $\circ$ intrepreted as multiplication.

The first two requirements for an arithmetic in §1 are in part a limitation upon the possible instances of an arithmetic; for instance, if a set of marks is denumerable, each element may be completely specified by precisely one cardinal number, so that the first requirement is trivial. The second requirement is more complicated and cannot be discussed fully here.

ON THE CHARACTERISTIC VALUES OF LINEAR INTEGRAL EQUATIONS

BY EINAR HILLE AND J. D. TAMARKIN

PRINCETON UNIVERSITY AND BROWN UNIVERSITY

Communicated November 7, 1928

1. We consider the integral equation

$$f(x) = \varphi(x) - \lambda \int_a^b K(x, s)\varphi(s)ds, \qquad (1)$$

where the kernel is supposed to belong to the class (L^2), i.e., $K(x, s)$ and its square are Lebesgue integrable in $a \leqq x, s \leqq b$. The equation is known to possess a resolvent kernel which is the quotient of two entire functions of λ, defined by Fredholm's formulas with the modifications due to Hilbert.[1] The characteristic values of the equation are the zeros of the denominator $D_K^*(\lambda)$ in this quotient. The order ν of $D_K^*(\lambda)$ is $\leqq 2$, and if $\nu = 2$ the function belongs to the minimal type; its genus is at most unity. This result is due to Carleman.[2]

2. The proof given by Carleman is ingenious but also rather complicated. It is possible, however, to base the proof upon a simple and well-known method, namely, that of infinitely many equations in infinitely many unknowns. Let $\{\omega_i(x)\}$ be a complete orthonormal system for the interval (a, b). Then $\{\omega_i(x)\overline{\omega_j(s)}\}$ constitutes a complete orthonormal system for the square $a \leqq x, s \leqq b$. Put

$$f_i = \int_a^b f(s)\overline{\omega_i(s)}ds, \quad \varphi_i = \int_a^b \varphi(s)\overline{\omega_i(s)}ds,$$