IMPOSSIBILITY OF RESTORING UNIQUE FACTORIZATION IN A HYPER-COMPLEX ARITHMETIC

BY L. E. DICKSON

1. *Introduction.* Most numbers $a + be$, where a and b are integers and $e^2 = 0$, admit of several factorizations into indecomposable numbers. It is proved in § 3 that we cannot restore unique factorization by defining hypercomplex ideals analogous to algebraic ideals, nor (§ 4) by the introduction of any sort of ideals obeying the laws of arithmetic. L. G. du Pasquier* has made statements, omitting proofs, concerning the failure of unique factorization after introducing ideals, apparently meaning those analogous to algebraic ideals.

2. *Hypercomplex Integers.* Consider the hypercomplex numbers $x = a + be$ with rational coordinates a, b, where $e^2 = 0$. Thus $(x - a)^2 = 0$. This quadratic equation has integral coefficients if and only if a is integral. As our integral hypercomplex numbers we shall take those of an infinite system of numbers $a + be$, where a is integral and b rational, such that the system has a basis† $1, ce$, i.e., is composed of their linear combinations with integral coefficients. Since we may take ce as a new unit e whose square is zero, we may assume that $a + be$ is integral if and only if a and b are both integers.

* VIERTELJAHRSSCHRIFT, ZÜRICH, vol. 54 (1909), pp. 116–148.
L'ENSEIGNEMENT, vol. 17 (1915), pp. 340–3; vol. 18 (1916), pp. 201–260.
NOUVELLES ANNALES, (4), vol. 18 (1918), pp. 448–461.
COMPTES RENDUS DU CONGRÈS INTERNATIONAL (Strasbourg), 1921.

† We obtain uninteresting results if we omit the assumption of a basis and call $a + be$ integral if a is integral and b rational. It is a unit if $a = \pm 1$. If $r \neq 0$, $\rho = r + se$ is "associated" with its product r by the unit $1 - es/r$. Hence the classes of associated numbers whose real coordinates are not zero are in (1, 1) correspondence with the real integers and obey the laws of divisibility of integers. But se is associated only with $\pm se$. Now te is divisible by every $r + se$, $r \neq 0$, the quotient being et/r.

The units (integral divisors of 1) are $\pm 1 + be$, where b is integral. A simple example shows that the laws of divisibility fail. Let p be any odd prime. Then

$$(1) \qquad p \cdot p = (p + ke)(p - ke),$$

and $p + te$ is indecomposable and is associated with $p + le$ if and only if $t \equiv l \pmod{p}$. The product of $p - ke$ by the unit $1 + e$ is $p + (p - k)e$. Hence if we give to k the values $0, 1, \cdots, \frac{1}{2}(p - 1)$ in (1), we obtain the $\frac{1}{2}(p + 1)$ essentially different ways of factoring p^2 into indecomposables. As a generalization of (1),

$$(p + ke)(p + le) = (p + xe)(p + ye), \qquad x + y = k + l.$$

3. *Hypercomplex Ideals.* As in the theory of algebraic numbers, define an ideal to be an infinite set of our hypercomplex integers which is closed under addition and subtraction and is such that the product of any number of the set by any hypercomplex integer is equal to a number of the set. Since $(r + se)e = re$, every ideal contains a number te, where $t \neq 0$. Let m be the minimum positive integer such that me is in the ideal. The products xme of me by all hypercomplex integers $x + ye$ constitute a principal ideal, denoted by $[me]$. Consider an ideal I which contains xme, where x ranges over all integers, and further numbers $r_i + s_ie$, where each $r_i \neq 0$. The positive greatest common divisor r of the r_i is a linear combination of them with integral coefficients. The same linear combination of the $r_i + s_ie$ is a number $r + se$ of I. Write q_i for the integer r_i/r. Then I contains

$$r_i + s_ie - q_i(r + se) = k_ie, \qquad k_i \equiv s_i - q_is.$$

Hence $k_i = p_im$, where p_i is an integer. Thus

$$r_i + s_ie = p_i(me) + q_i(r + se),$$

so that I is composed of linear combinations of me and $r + se$ with integral coefficients (i.e., has a basis). Finally, the product of every number of I by every hypercomplex integer must belong to I, which will be true if the products by e belong to I, i.e., if re is in I. Thus $r = qm$, where q is an integer. Hence

$$(2) \quad I = [me, qm + se], \qquad q > 0,\ m > 0,\ 0 \leqq s < m,$$

where the bracket signifies all the linear combinations of the two enclosed numbers with integral coefficients.

The product of two ideals is defined to be the totality of linear combinations with integral coefficients of the various products of numbers of the first ideal by numbers of the second. Hence

$$[te]I = [tqme] = [te]P, \qquad P \equiv [qme,\ qm].$$

The ideal P is distinct from I unless $q = 1, s = 0$. Hence the laws of arithmetic do not hold for our ideals.*

The preceding special difficulty may be obviated by excluding one-based ideals $[te]$. Hence we shall supplement our definition of an ideal by making the assumption that it contains numbers which are not divisors of zero, i.e., multiples of e. Now every ideal is of the form (2).

If $q = 1$, (2) is composed of the products of $m + se$ by all hypercomplex integers and hence is called a principal ideal $\{m + se\}$. If $q > 1$, (2) is not a principal ideal. We shall call q the *mass* of the ideal (2). Hence an ideal is a principal ideal if and only if its mass is unity.

The mass of a product of two ideals is the least common multiple of their masses. For, the product of (2) by

$$J = [ne,\ pn + te]$$

is

$$IJ = [p \cdot mne,\ q \cdot mne,\ pqmn + ke], \qquad k = qmt + pns.$$

Let G be the greatest common divisor of $p = PG$ and $q = QG$, whence P and Q are relatively prime. Then G is a linear combination of p and q. The same linear combination of the first two entries in IJ is $Gmne$. Hence

$$IJ = [Gmne,\ PQGGmn + ke],$$

whose mass is PQG, i.e., the least common multiple of p and q.

It follows at once that the mass of the product of any number of ideals is the least common multiple of their masses. The latter is unity if and only if all the masses are unity. Hence a product is a principal ideal if and only if each factor is a principal ideal. In other words, every factor of a principal ideal is itself a principal ideal.

* More simply since $[e][\acute{e}]$ is not an ideal.

Consequently our ideals fail to explain our difficulty (1), or the equivalent in principal ideals:

$$(1') \qquad \{p\}\cdot\{p\} = \{p + ke\}\{p - ke\}.$$

Since we saw that $p + te$ is an indecomposable number, we conclude that $\{p + te\}$ is not a product of principal ideals and not a product of any ideals. The relation (1′) between distinct indecomposable ideals shows that our ideals do not obey the laws of arithmetic and do not explain our difficulty (1).

4. *Impossibility of the Restoration of Unique Factorization.* In § 3 we saw the futility of the introduction of hypercomplex ideals defined essentially as in the theory of algebraic numbers. We shall now prove that it is impossible to restore unique factorization by the introduction of ideals of any kind such that a number and its products by the units all correspond to a unique ideal (provided the number be not a divisor of zero) and such that the product of two numbers corresponds to the product of the corresponding ideals.

The numbers $a = 3$, $b = 3 + e$, $c = 3 + 2e$ are indecomposable and no two are associated. We have

$$(3) \qquad ac = b^2, \qquad bc = a^2(1 + e), \qquad ab = c^2(1 - e).$$

Let α, β, γ be the distinct ideals $\neq 1$ which correspond uniquely to a, b, c, respectively. Since $1 + e$ and $1 - e$ are units, we have

$$(4) \qquad \alpha\gamma = \beta^2, \qquad \beta\gamma = \alpha^2, \qquad \alpha\beta = \gamma^2.$$

A prime ideal divisor $\delta \neq 1$ of α must divide β and γ. Write

$$\alpha = \alpha_1\delta, \ \beta = \beta_1\delta, \ \gamma = \gamma_1\delta.$$

Then

$$(5) \qquad \alpha_1\gamma_1 = \beta_1^2, \qquad \beta_1\gamma_1 = \alpha_1^2, \qquad \alpha_1\beta_1 = \gamma_1^2.$$

No one of $\alpha_1, \beta_1, \gamma_1$ is unity. For, if $\alpha_1 = 1$, then $\beta_1\gamma_1 = 1$, whence $\beta_1 = \gamma_1 = 1$, whereas α, β, γ are distinct. Since the relations (5) are entirely similar to relations (4), it is impossible to restore, in a finite number of steps, unique factorization in (3) by the introduction of ideals.

5. *Factorization.* There is only a finite number of ways of factoring into indecomposables and each way involves only a finite number of factors. First, to obtain all pairs of factors of te, express t as a product of two integers x, w in all possible ways; the factors are $x + ye$, we, where $0 \leqq y < x$, if we retain only one of associated numbers. To factor $a + be$, where $a > 0$, express a in all possible ways as a product xz of two integers > 1. For each such pair x, z, and for $0 \leqq y < x$, $a + be$ has the factors $x + ye$ and $z + we$, where w is determined uniquely by $xw + yz = b$, the case of a fractional w being excluded.

The only pairs of factors of p^k ($k \geqq 2$), no one a unit, are

$$p^r + ye, \qquad p^{k-2r}(p^r - ye),$$

where r ranges over the positive integers $\leqq \frac{1}{2}k$, and $0 \leqq y < p^r$. The only pairs of factors of $p^k + se$ are

$$p^r + ye, \qquad p^{k-r} + (\sigma - p^{k-2r}y)e,$$

where $r \leqq \frac{1}{2}k$ and p^r divides $s = \sigma p^r$.

If p and q are distinct primes and $k \geqq l$, the only pairs of factors not units of $p^k q^l$ are J, $p^{k-2r}q^{l-2s}K$, where

$$J = p^r q^s + ye, \qquad K = p^r q^s - ye,$$

$0 \leqq r \leqq \frac{1}{2}k$, $0 \leqq s \leqq \frac{1}{2}l$, $0 \leqq y < p^r q^s$; and $p^{k-2r}J$, $q^{l-2s}K$ ($r < \frac{1}{2}k$). In particular pq has only the factors p, q.

Regarding factors of J, note that $pq + se$ has the unique factors, apart from unit factors, $p + ye$ and $q + we$, where $0 \leqq y < p$, $qy \equiv s \pmod{p}$, and w is determined by $pw + yq = s$. Next, $p^2q + se$ has the factors $p^2 + ye$ and $q + we$, where w is uniquely determined by $0 \leqq w < q$, $p^2w \equiv s \pmod{q}$, and y is then determined by $p^2w + qy = s$. It has no further pairs of factors if s is prime to p. But if $s = Sp$, the only additional pairs are the p pairs $p + ye$, $pq + we$, where $0 \leqq y < p$, $w = S - qy$.

The University of Chicago