ON THE COMPOSITION OF ALGEBRAIC FORMS OF HIGHER DEGREE

C. C. MACDUFFEE

1. **Introduction.** No discussion of composition can properly be introduced except by mentioning the complex numbers. From the relation

$$x_1 + ix_2 = (y_1 + iy_2)(z_1 + iz_2),$$

$$x_1 = y_1z_1 - y_2z_2, \qquad x_2 = y_1z_2 + y_2z_1,$$

we have, upon taking norms,

$$x_1^2 + x_2^2 = (y_1^2 + y_2^2)(z_1^2 + z_2^2).$$

Thus the quadratic form $y_1^2+y_2^2$ is composed with itself.

Similarly by using quaternions we achieve the composition of a sum of four squares with itself,[1] and by using Cayley's algebra of order 8, we obtain the composition of a sum of eight squares with itself. No further progress in this direction is possible.[2]

In general let us assume that

$$(1) \qquad x_k = \sum_{i,j} c_{ijk}y_iz_j \qquad (i, j, k = 1, 2, \cdots, n)$$

where the c_{ijk} are numbers of a commutative ring $\mathfrak{R}$ with unit element, and the y's and z's are indeterminates. If there exist three homogeneous forms f, g, h of degree k with coefficients in $\mathfrak{R}$ such that

$$(2) \qquad f(x) = g(y)\cdot h(z)$$

is an identity by virtue of the bilinear transformation (1), we say that g and h are *composable*, that f is *composite*, and that the transformation (1) is *admissible.*

The theory of composition appears in the mathematical literature under two rather distinct special cases, first where $\mathfrak{R}$ is a field, and second where $\mathfrak{R}$ is the ring of rational integers. The field case is the simpler and progress has been carried much further, but this is not the case in which we are here primarily interested.

An address presented at the invitation of the Program Committee at the meeting of the Society in Wellesley, August 13, 1944; received by the editors December 18, 1944.

[1] It seems certain that a knowledge of the fact that a sum of four squares is composable with itself, which had been proved by Euler in 1748, was one of the main clues which led Hamilton to the discovery of quaternions.

[2] See L. E. Dickson, Ann. of Math. (2) vol. 20 (1919) pp. 155–171.

The case where $\mathfrak{R}$ is the.ring of rational integers is intimately connected with some of the basic concepts of number theory, particularly with the class number in an algebraic field, and in spite of the large number of special results which have been obtained, composition theory here still appears to be in a primitive condition.

Fortunately it is not necessary to attempt a summary of the literature, for it is exhaustively given in Dickson's *History of the theory of numbers*.[3]

The aim of the present paper is very modest. While the problem of composition may be stated for an abstract ring, it seems as if only in the case of a principal ideal ring are there enough properties at hand to make the problem amenable to our methods. The comprehensive Dedekind-Weber composition, involving ideal classes in algebraic fields of degree n, is approached with the calculus of matrices with the result that certain aspects of the theory are thrown into higher relief. Finally the theory of ideals in more general algebras is shown to yield compositions, sometimes of a somewhat unorthodox type. But the existence of these compositions is sufficient to show that the complete determination of all compositions over a ring is likely to prove to be a complicated problem.

2. **The Dedekind-Weber theorem.** Let $\mathfrak{F}$ be an ordinary algebraic field of order n over the rational field $\mathfrak{R}$, and let $[\mathfrak{F}]$ be its maximal integral ring, with $[\mathfrak{R}]$-basis

$$\epsilon_1, \epsilon_2, \cdots, \epsilon_n.$$

We shall call

$$t(y) = y_1\epsilon_1 + y_2\epsilon_2 + \cdots + y_n\epsilon_n,$$

where the y's are indeterminates, the *general number* of $[\mathfrak{F}]$. By means of the multiplication table

$$\epsilon_i\epsilon_j = \sum_k c_{ijk}\epsilon_k$$

of $[\mathfrak{F}]$, it is possible to write

$$t(x) = t(y)\cdot t(z) \tag{3}$$

where

$$x_k = \sum_{i,j} c_{ijk}y_iz_j.$$

[3] L. E. Dickson, *History of the theory of numbers*, vol. 3, Washington, 1923, chaps. 3 and 14.

The norm $n(x)$ of $t(x)$ is an algebraic form of degree n in n indeterminates with coefficients in $[\mathfrak{R}]$, and from (3) it follows that

$$n(x) = n(y)\cdot n(z).$$

Thus the norm form $n(y)$ is composable with itself, and is the most obvious example of composition which we have.

This process is readily extensible to linear algebras which have the norm property, whether they are associative or not, and leads to the composition of forms in n indeterminates with themselves. If the algebra is associative but not commutative, these forms are of degree less than n.

But not all composition is of a form with itself, and the most general result in this direction is due to Dedekind and Weber.[4]

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of $[\mathfrak{F}]$ with respective $[\mathfrak{R}]$-bases

$$\alpha_1, \alpha_2, \cdots, \alpha_n, \qquad \beta_1, \beta_2, \cdots, \beta_n$$

and let the product ideal $\mathfrak{c}=\mathfrak{a}\mathfrak{b}$ have the basis $\gamma_1, \gamma_2, \cdots, \gamma_n$. Then rational integers c_{ijk} exist such that

$$\alpha_i\beta_j = \sum_k c_{ijk}\gamma_k.$$

Define

$$t(\mathfrak{a}) = y_1\alpha_1 + y_2\alpha_2 + \cdots + y_n\alpha_n, \qquad t(\mathfrak{b}) = z_1\beta_1 + z_2\beta_2 + \cdots + z_n\beta_n$$

where the y's and z's are indeterminates. Then

$$t(\mathfrak{a})\cdot t(\mathfrak{b}) = t(\mathfrak{c})$$

where

$$t(\mathfrak{c}) = x_1\gamma_1 + x_2\gamma_2 + \cdots + x_n\gamma_n, \qquad x_k = \sum_{i,j} c_{ijk}y_iz_j.$$

Let $nt(\mathfrak{a})$ denote the norm of the number $t(\mathfrak{a})$ in $[\mathfrak{F}]$. It can be shown that

$$nt(\mathfrak{a}) = n(\mathfrak{a})\cdot g(y)$$

where $n(\mathfrak{a})$ is the norm of the ideal $\mathfrak{a}$ and $g(y)$ is an n-ary n-ic form with coefficients in $[\mathfrak{R}]$. Similarly

$$nt(\mathfrak{b}) = n(\mathfrak{b})\cdot h(z), \qquad nt(\mathfrak{c}) = n(\mathfrak{c})\cdot f(x).$$

Since $nt(\mathfrak{c}) = nt(\mathfrak{a})\cdot nt(\mathfrak{b})$, it follows that

$$f(x) = g(y)\cdot h(z), \qquad x_k = \sum c_{ijk}y_iz_j.$$

[4] H. Weber, *Lehrbuch der Algebra*, 2d ed., Braunschweig, 1908, p. 335.

We are thus led to the composition of the forms $g(y)$ and $h(z)$, which are in general different.

It is shown, further, that if $\mathfrak{a}$ and $\mathfrak{a}'$ are ideals of the same class, the corresponding forms $g(y)$ and $g'(y)$ are equivalent, and that a change of basis of $\mathfrak{a}$ leads to an equivalent $g(y)$. But if $\mathfrak{a}$ and $\mathfrak{a}'$ belong to different classes, $g(y)$ and $g'(y)$ are not equivalent. Thus as many non-equivalent forms are obtained in this way as there are classes of ideals in $[\mathfrak{F}]$.

3. **The general problem.** In the type of composition which is accomplished through ideal multiplication in an algebraic field, the admissible bilinear transformations (1) satisfy two conditions[5] which are sometimes but not always demanded in composition theory—first that the $x_1, x_2, \cdots, x_n$ shall be linearly independent when the y's and z's are independent indeterminates, and second that there shall exist elements a_{ijk} in the principal ideal ring $\mathfrak{R}$ such that

$$y_iz_j = \sum_k a_{ijk}x_k. \tag{4}$$

We might say that the composition is *non-trivial* if these conditions are satisfied. We shall show that one simple hypothesis will insure both of these conditions.

Let us stream-line the notation by introducing the vectors

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix}, \qquad y = \begin{bmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{bmatrix}, \qquad z = \begin{bmatrix} z_1 \\ z_2 \\ \cdots \\ z_n \end{bmatrix},$$

and the matrices

$$R(y) = y_1R_1 + y_2R_2 + \cdots + y_nR_n,$$
$$S(z) = z_1S_1 + z_2S_2 + \cdots + z_nS_n$$

where

$$R_i = (c_{isr}), \qquad S_i = (c_{ris}).$$

In this notation the bilinear transformation (1) can be written

$$x = R(y)\cdot z = S^{\mathrm{T}}(z)\cdot y. \tag{5}$$

The hypothesis which we shall introduce is that *the matrices S_1, S_2, $\cdots$, S_n are relatively prime on the right.*

[5] Weber, loc. cit.

From this hypothesis it follows[6] that n matrices A_i with elements in $\mathfrak{R}$ exist such that

$$A_1S_1 + A_2S_2 + \cdots + A_nS_n = I, \qquad A_i = (a_{sir}).$$

That is,

$$\sum_{i,j} a_{ijr}c_{ijs} = \delta_{rs}$$

where δ_{rs} is Kronecker's delta. Now a relation $\sum b_kx_k = 0$ would imply

$$\sum_{i,j,k} b_kc_{ijk}y_iz_j = 0$$

and, since the y's and z's are independent indeterminates,

$$\sum_k b_kc_{ijk} = 0 \qquad (i, j = 1, 2, \cdots, n).$$

Then

$$\sum_{i,j,k} a_{ijr}b_kc_{ijk} = \sum_k b_k\delta_{rk} = b_r = 0$$

for every r, so that $x_1, x_2, \cdots, x_n$ are linearly independent.

We may now verify that equations (4) with the a_{ijk} as defined above actually constitute a solution of (1). For upon substituting we have

$$\sum_{i,j,l} c_{ijk}a_{ijl}x_l = \sum_l \delta_{kl}x_l = x_k.$$

Thus our hypothesis is sufficient that (1) be non-trivial.

That it is necessary is quite evident, for if (4) exists,

$$x_k = \sum_{i,j} c_{ijk}\sum_l a_{ijl}x_l,$$

and if the x's are linearly independent,

$$\sum_{i,j} c_{ijk}a_{ijl} = \delta_{kl},$$

which in matric form is

$$A_1S_1 + A_2S_2 + \cdots + A_nS_n = I.$$

An equivalent condition is that the matrices $R_1, R_2, \cdots, R_n$ be relatively prime on the left.

An implication of this condition is that we may assume f, g and h to be primitive. For if

$$f(x) = a\cdot f'(x), \qquad g(y) = b\cdot g'(y), \qquad h(z) = c\cdot h'(z)$$

[6] Bull. Amer. Math. Soc. vol. 39 (1933) p. 573.

where a, b and c are the contents and f', g' and h' primitive, then by (1)

$$f'(x) = p(y, z)$$

where p has coefficients in $\mathfrak{R}$. Since

$$a \cdot p(y, z) = bc \cdot g'(y) \cdot h'(z),$$

it follows that $a | bc$. By (4)

$$g'(y) \cdot h'(z) = q(x)$$

has coefficients in $\mathfrak{R}$ so that

$$bc \cdot q(x) = a \cdot f'(x),$$

whence $bc | a$. Then $bc = ua$ where u is a unit of $\mathfrak{R}$, and

$$u \cdot f'(x) = g'(y) \cdot h'(z).$$

A linear homogeneous transformation on the variables of a form f may be written

$$x = Ax', \qquad |A| \neq 0, \tag{6}$$

where A is a matrix with elements in $\mathfrak{R}$. If $|A|$ is a unit of $\mathfrak{R}$, then

$$x' = A^{-1}x$$

is again a transformation of the same type. If by virtue of (6)

$$f(x) = f'(x'), \qquad A \text{ unimodular},$$

then the form $f'(x)$ is called *equivalent* to $f(x)$. Clearly the totality of numbers of $\mathfrak{R}$ which f and f' represent is the same.

If $M_1, M_2, \cdots, M_n$ are $n \times n$ matrices with elements in $\mathfrak{R}$, then

$$| x_1M_1 + x_2M_2 + \cdots + x_nM_n |$$

is a homogeneous form of degree n in the n indeterminates $x_1, x_2, \cdots, x_n$. A form which can be written as the determinant of such a matrix will be called *amenable*.

Let us consider the effect of a transformation of the variables on the bilinear transformation (1). If $y = Ay'$, then from (5)

$$x = S^{\mathsf{T}}(z) \cdot Ay',$$

so that

$$S'(z) = A^{\mathsf{T}} \cdot S(z). \tag{7}$$

Similarly if we take $z = Bz'$, we have

$$R'(y) = R(y) \cdot B. \tag{8}$$

The following theorem was obtained by Gauss[7] for quadratic forms and generalized by Dedekind.

If $f(x)=g(y)\cdot h(z)$ *by virtue of* (1), *every irreducible factor of* $h(z)$ (*or of* $g(y)$) *of degree greater than* 0 *is a factor of* $|S^{\mathrm{T}}(z)|$ (*or of* $|R(y)|$). *If* $h(z)$ (*or* $g(y)$) *is irreducible of degree* n, *then it is amenable.*

From (5) we have

$$S^{\mathrm{T}}(z)\cdot y = x.$$

Upon multiplying through by adj $S^{\mathrm{T}}(z)$, we have

$$|S^{\mathrm{T}}(z)|\cdot y = \operatorname{adj} S^{\mathrm{T}}(z)\cdot x.$$

Since $g(y)$ is homogeneous of degree k,

$$|S^{\mathrm{T}}(z)|^{k}\cdot g(y) = P(z, x)$$

where $P(z, x)$ is a homogeneous polynomial in x and z with coefficients in $\mathfrak{R}$. Upon multiplying by $h(z)$ and making use of (2), we have

$$|S^{\mathrm{T}}(z)|^{k}\cdot f(x) = P(z, x)\cdot h(z).$$

If $\mathfrak{R}$ is a ring in which factorization into primes is unique, the same is true in the polynomial ring $\mathfrak{R}[x, z]$. Then

$$h(z)\,\Big|\,|S^{\mathrm{T}}(z)|^{k},$$

and the distinct irreducible factors of $h(z)$ occur among the distinct irreducible factors of $|S^{\mathrm{T}}(z)|$. If in particular $h(z)$ is irreducible of degree n,

$$h(z) = c\cdot|S^{\mathrm{T}}(z)|, \qquad c\in\mathfrak{R}.$$

Thus $h(z)$ is amenable. Similarly we find that, if $g(y)$ is irreducible of degree n,

$$g(y) = c\cdot|R(y)|, \qquad c\in\mathfrak{R}.$$

Another basic theorem in the theory of composition is the Theorem of Dickson.[8]

Let $f(x)=g(y)\cdot h(z)$ *by virtue of* (1). *If* $|S^{\mathrm{T}}(z)|$ *is not identically zero,* $g(y)$ *is equivalent to* $c\cdot f(x)$ *in the quotient field of* $\mathfrak{R}$. *If* $|R(y)|$ *is not identically zero,* $h(z)$ *is equivalent to* $c\cdot f(x)$ *in the quotient field of* $\mathfrak{R}$. *If furthermore* $h(z)$ *represents a unit* u *of* $\mathfrak{R}$ *and is irreducible of degree* n *in* n *variables,* $g(y)$ *is equivalent to* $u\cdot f(x)$ *in* $\mathfrak{R}$. *Similarly if* $g(y)$

[7] See, for instance, the exposition of A. Speiser, *Festschrift Heinrich Weber*, Teubner, Leipzig, 1912, pp. 375–395.

[8] L. E. Dickson, C. R. Acad. Sci. Paris vol. 172 (1921) pp. 636–640.

represents a unit u of $\mathfrak{R}$ and is irreducible of degree n in n variables, $h(z)$ is equivalent to $u\cdot f(x)$ in $\mathfrak{R}$.

Let $k_1, k_2, \cdots, k_n$ be n numbers of $\mathfrak{R}$ such that $|S^{\mathrm{T}}(k)|\neq 0$. In the relations

$$x = S^{\mathrm{T}}(z)\cdot y, \qquad f(x) = g(y)\cdot h(z)$$

set $z\rightarrow k$. Then

$$y = S^{-\mathrm{T}}(k)\cdot x, \qquad f(x) = g(y)\cdot h(k).$$

The first equation represents a transformation of the type $y=Ay'$ where $y'=x$, so that the second equation becomes

$$f(y') = h(k)\cdot g(y) = c\cdot g(y).$$

If $h(z)$ represents a unit of $\mathfrak{R}$, let $k_1, k_2, \cdots, k_n$ be so chosen that $h(k)=u$. Then $f(x)=u\cdot g(y)$. If $h(z)$ is irreducible of degree n, we have seen that $h(z)=c\cdot|S^{\mathrm{T}}(z)|$ so that $|S^{\mathrm{T}}(k)|$ is a unit of $\mathfrak{R}$ and the transformation $y=S^{-\mathrm{T}}(k)\cdot x$ is unimodular.

4. **The theory of ideals.** The writer has approached the theory of ideals in linear associative algebras over a principal ideal ring through the matric calculus.[9] This leads to a theory of composition which extends the known theory.

First, when applied in algebraic fields it enriches the Dedekind-Weber theory by bringing to light the matrices whose determinants were the essential items in the older theory. The algebraic form is defined in terms of the basis of the ideal class rather than in terms of the single ideal, which comes more directly to the essential point of composition of classes.

Second, in the general case where the class group does not exist, some quite unorthodox examples of composition are obtained.

We assume that $\mathfrak{F}$ is the quotient field of the principal ideal ring $\mathfrak{R}$, and that $\mathfrak{A}$ is a finite algebra over $\mathfrak{F}$ with the $\mathfrak{F}$-basis $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$, and the constants of multiplication c_{ijk} which belong to $\mathfrak{R}$. These n^3 numbers can be arranged into sets of n matrices by defining

$$Q_i = (c_{rsi}), \qquad R_i = (c_{isr}), \qquad S_i = (c_{ris})$$

where r denotes the row and s the column in which an element lies.

The numbers

$$\alpha = a_1\epsilon_1 + a_2\epsilon_2 + \cdots + a_n\epsilon_n$$

[9] Monatshefte für Mathematik und Physik vol. 48 (1939) pp. 293–313. Amer. J. Math. vol. 64 (1942) pp. 646–652.

of $\mathfrak{A}$ whose coördinates a_i lie in $\mathfrak{R}$ constitute an integral domain of $\mathfrak{A}$ which we shall denote by $[\mathfrak{A}]$. Corresponding to each number α there are three matrices

$$Q(\alpha) = a_1Q_1 + a_2Q_2 + \cdots + a_nQ_n,$$
$$R(\alpha) = a_1R_1 + a_2R_2 + \cdots + a_nR_n,$$
$$S(\alpha) = a_1S_1 + a_2S_2 + \cdots + a_nS_n,$$

all of whose elements belong to $\mathfrak{R}$.

We shall assume that $\mathfrak{A}$ is a Frobenius algebra, that is, that there is in $\mathfrak{A}$ at least one number α such that $Q(\alpha)$ is nonsingular. In this case each of the correspondences

$$\alpha \rightleftarrows R(\alpha), \qquad \alpha \rightleftarrows S(\alpha)$$

is an isomorphism, the so-called first and second regular representations of $[\mathfrak{A}]$.

An additive group $\mathfrak{M}$ of numbers of $[\mathfrak{A}]$ which is closed under multiplication by the numbers of $\mathfrak{R}$ is called an *$\mathfrak{R}$-module*. An $\mathfrak{R}$-module which is closed under multiplication on the left by the numbers of $[\mathfrak{A}]$ is a *left ideal*. A *right ideal* is similarly defined.

Every left or right ideal $\mathfrak{a}$ of $[\mathfrak{A}]$ has an $\mathfrak{R}$-basis $\alpha_1, \alpha_2, \cdots, \alpha_n$ where

$$\alpha_i = a_{i1}\epsilon_1 + a_{i2}\epsilon_2 + \cdots + a_{in}\epsilon_n, \qquad a_{ij} \in \mathfrak{R}.$$

We define the matrix $A = (a_{rs})$, and say that A corresponds to the ideal $\mathfrak{a}$ by a *Poincaré correspondence*. If A is nonsingular, it is unique up to a left factor U which is a unimodular matrix with elements in $\mathfrak{R}$. The matrix $S(\alpha)$ corresponds to the principal left ideal $(\alpha]$, and $R^{\mathrm{T}}(\alpha)$ corresponds to the principal right ideal $[\alpha)$.

Let $\mathfrak{a}$ be a left ideal with $[\mathfrak{A}]$-basis $\alpha_1, \alpha_2, \cdots, \alpha_n$, and let A be the greatest common right divisor of the matrices

$$S(\alpha_1), S(\alpha_2), \cdots, S(\alpha_k),$$

which is unique up to a unimodular left factor U. Then A corresponds to $\mathfrak{a}$ by the Poincaré correspondence, and the rows of A determine an $\mathfrak{R}$-basis of $\mathfrak{a}$.

A necessary and sufficient condition in order that a matrix A with elements in $\mathfrak{R}$ shall correspond to a left ideal is that there shall exist n matrices D_i with elements in $\mathfrak{R}$ such that

$$A\overset{\mathrm{T}}{R_i} = \overset{\mathrm{T}}{D_i}A \qquad (i = 1, 2, \cdots, n).$$

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *equivalent*, or to belong to the same *class*, provided two numbers τ_1 and τ_2 of $[\mathfrak{A}]$ exist such that

$$\mathfrak{a}\tau_1 = \mathfrak{b}\tau_2.$$

At least in the case where $\mathfrak{F}$ is the rational field, $\mathfrak{R}$ the ring of rational integers, and $\mathfrak{A}$ is semi-simple, the number of classes of left (or right) ideals is finite.[10]

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two left ideals with $\mathfrak{R}$-bases $\alpha_1, \alpha_2, \cdots, \alpha_n$ and $\beta_1, \beta_2, \cdots, \beta_n$, and let $\mathfrak{a}\rightleftarrows A$ so that matrices H_i exist such that $S(\alpha_i) = H_i A$. If and only if $\mathfrak{b}$ is equivalent to $\mathfrak{a}$, there exists a matrix B corresponding to $\mathfrak{b}$ such that

$$S(\beta_i) = H_i B \qquad (i = 1, 2, \cdots, n).$$

Then also

$$A\overset{\mathrm{T}}{R_i} = \overset{\mathrm{T}}{D_i} A, \qquad B\overset{\mathrm{T}}{R_i} = \overset{\mathrm{T}}{D_i} B.$$

If $\mathfrak{A}$ is a Frobenius algebra, every ideal class has a basis of order n in the following sense. There exist n matrices $B_1, B_2, \cdots, B_n$ such that every matrix

$$b_1B_1 + b_2B_2 + \cdots + b_nB_n, \qquad b_i \in \mathfrak{R},$$

corresponds to an ideal of the class, and conversely every ideal of the class corresponds (not uniquely) to a matrix of this linear system.

It is not usually true if $\mathfrak{a}\rightleftarrows A$ and $\mathfrak{b}\rightleftarrows B$ that $\mathfrak{a}\times\mathfrak{b}\rightleftarrows AB$. But if $[\mathfrak{A}]$ is of class number h, the Poincaré correspondence can be amplified so that to every ideal $\mathfrak{a}$ there correspond h matrices $A^1, A^2, \cdots, A^h$, one for each class, with the following property. If $\mathfrak{b}$ is in class b, and if $\mathfrak{a}\times\mathfrak{b} = \mathfrak{c}$, and if $\mathfrak{c}\rightleftarrows C$ by the Poincaré correspondence, then

$$A^bB = C.$$

Thus every ideal $\mathfrak{a}$ has, besides its principal norm

$$n(\mathfrak{a}) = \|A\|$$

where the double bars indicate the absolute value of the determinant, h other norms

$$n^i(\mathfrak{a}) = \|A^i\|.$$

If $\mathfrak{b}$ is in class b and $\mathfrak{a}\times\mathfrak{b} = \mathfrak{c}$, then

$$n^b(\mathfrak{a}) \cdot n(\mathfrak{b}) = n(\mathfrak{c}).$$

5. **The algebraic field.** Let us now restrict $\mathfrak{F}$ to be the rational

[10] M. Deuring, *Algebren*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 4, no. 1, Springer, Berlin, 1935, p. 90.

field, $\mathfrak{R}$ to be the ring of rational integers, and $[\mathfrak{A}]$ to be the maximal integral domain of a (commutative) algebraic field of order n over $\mathfrak{F}$. We can connect our results with the Dedekind-Weber theorem.

It is now true that every ideal is two-sided and the norm of the product of two ideals is equal to the product of their norms. Consequently all the norms of an ideal $\mathfrak{a}$ are equal,

$$n(\mathfrak{a}) = n'(\mathfrak{a}) = n^2(\mathfrak{a}) = \cdots = n^h(\mathfrak{a}).$$

Select two ideal classes, the ath and the bth, whose product class is the cth class. Select bases

$$A_1, A_2, \cdots, A_n; B_1, B_2, \cdots, B_n; C_1, C_2, \cdots, C_n$$

for these three classes, and define the n-ary n-ic forms

$$g(y) = | y_1A_1 + y_2A_2 + \cdots + y_nA_n |,$$
$$h(z) = | z_1B_1 + z_2B_2 + \cdots + z_nB_n |$$

where the y's and z's are indeterminates. The matrix A_i corresponds to an ideal $\mathfrak{a}_i$ by the Poincaré correspondence, and $\mathfrak{a}_i$ corresponds to $\overset{b}{A}_i$ under the extended correspondence. It can, moreover, be shown that

$$g(y) = | y_1\overset{b}{A}_1 + y_2\overset{b}{A}_2 + \cdots + y_n\overset{b}{A}_n |.$$

Since each product $\overset{b}{A}_iB_j$ corresponds to an ideal in the cth class, there exist rational integers c_{ijk} such that

$$\overset{b}{A}_iB_j = \sum_k c_{ijk}C_k.$$

Thus

$$g(y)\cdot h(z) = \left| \sum_{i,j} y_iz_j\overset{b}{A}_iB_j \right| = \left| \sum_k x_kC_k \right| = f(x)$$

where

$$x_k = \sum_{i,j} c_{ijk}y_iz_j.$$

Thus we have the composition of n-ary n-ic forms in a manner which is directly related to the composition of ideal classes.

This may be clearer to the reader if an example is given. In the quadratic field $\mathfrak{F}((-31)^{1/2})$, the maximal integral domain has the basis

$$\epsilon_1 = 1, \qquad \epsilon_2 = (1 + (-31)^{1/2})/2.$$

The class number is 3, and each of the ideals[11] (1), $(2, 2^{-1}(1+(-31)^{1/2})$

[11] L. W. Reid, *The elements of the theory of algebraic numbers*, Macmillan, 1910, p. 444.

$(4, (1+(-31)^{1/2})/2)$ is in a different class, which we shall denote as the first, second and third classes, respectively. The matrices

$$S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad S_2 = \begin{bmatrix} 0 & 1 \\ -8 & 1 \end{bmatrix}$$

form a basis for the first or principal class, while

$$A_1 = \begin{bmatrix} -1 & 1 \\ -4 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$$

form a basis for the second class, and

$$B_1 = \begin{bmatrix} -1 & 1 \\ -2 & 0 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix}$$

for the third class. Let

$$\begin{aligned} f(x) &= |x_1S_1 + x_2S_2| = x_1^2 + x_1x_2 + 8x_2^2, \\ g(y) &= |y_1A_1 + y_2A_2| = 4y_1^2 - y_1y_2 + 2y_2^2, \\ h(z) &= |z_1B_1 + z_2B_2| = 2z_1^2 - z_1z_2 + 4z_2^2. \end{aligned}$$

These represent the three positive reduced forms of discriminant -31.[12] Now

$$A_1^3 = \begin{bmatrix} -1 & 0 \\ 0 & -4 \end{bmatrix}, \quad A_2^3 = \begin{bmatrix} 0 & 1 \\ -2 & 1 \end{bmatrix},$$

and

$$|y_1A_1^3 + y_2A_2^3| = g(y).$$

We have

$$(y_1A_1^3 + y_2A_2^3)(z_1B_1 + z_2B_2) = x_1S_1 + x_2S_2$$

where

$$\begin{aligned} x_1 &= y_1z_1 - 4y_1z_2 - 2y_2z_1, \\ x_2 &= - y_1z_1 + y_2z_2. \end{aligned}$$

6. **A noncommutative ring.** A simple instance of an integral domain of a noncommutative algebra of class number greater than 1 was given by E. J. Finan.[13] The complete matric algebra of order 4 over the rational field has a non-maximal integral domain with basis

[12] L. E. Dickson, *Introduction to the theory of numbers*, University of Chicago Press, 1929, p. 140.

[13] Duke Math. J. vol. 1 (1935) pp. 484–490.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}.$$

The class number of this domain is 3, and the three left ideal classes may be represented by the matrices

$$A = \begin{bmatrix} a & b & 0 & 0 \\ 3d & c & 0 & 0 \\ 0 & 0 & c & d \\ 0 & 0 & 3b & a \end{bmatrix}, \quad B = \begin{bmatrix} 3a & b & 0 & 0 \\ 3d & c & 0 & 0 \\ 0 & 0 & c & d \\ 0 & 0 & b & a \end{bmatrix}, \quad C = \begin{bmatrix} a & b & 0 & 0 \\ d & c & 0 & 0 \\ 0 & 0 & 3c & d \\ 0 & 0 & 3b & a \end{bmatrix}$$

where A represents the principal class.

Denote by $\mathfrak{a}_1$ the ideal whose basis is A with $a=1$, $b=c=d=0$; by $\mathfrak{a}_2$ the ideal whose basis is A with $a=0$, $b=1$, $c=d=0$, and so on. These basic ideals are singular, and in fact $\mathfrak{a}_1=\mathfrak{c}_1$, $\mathfrak{a}_2=\mathfrak{c}_2$, $\mathfrak{a}_3=\mathfrak{b}_3$, $\mathfrak{a}_4=\mathfrak{b}_4$. A nonsingular ideal can belong to but one class.

	A_1	A_2	A_3	A_4	B_1	B_2	B_3	B_4	C_1	C_2	C_3	C_4
A_1	C_1	C_2	C_3	$3C_4$	$3C_1$	C_2	C_3	$3C_4$	C_1	C_2	C_3	C_4
A_2	$3C_1$	$3C_2$	C_3	$3C_4$	$3C_1$	C_2	C_3	$3C_4$	$3C_1$	$3C_2$	$3C_3$	$3C_4$
A_3	B_1	$3B_2$	B_3	B_4	B_1	B_2	B_3	B_4	B_1	$3B_2$	$3B_3$	B_4
A_4	B_1	$3B_2$	$3B_3$	$3B_4$	$3B_1$	$3B_2$	$3B_3$	$3B_4$	B_1	$3B_2$	$3B_3$	B_4
B_1	B_1	$3B_2$	$3B_3$	$3B_4$	$3B_1$	$3B_2$	$3B_3$	$3B_4$	B_1	$3B_2$	$3B_3$	B_4
B_2	B_1	$3B_2$	B_3	B_4	B_1	B_2	B_3	B_4	B_1	$3B_2$	$3B_3$	B_4
B_3	B_1	$3B_2$	B_3	B_4	B_1	B_2	B_3	B_4	B_1	$3B_2$	$3B_3$	B_4
B_4	B_1	$3B_2$	$3B_3$	$3B_4$	$3B_1$	$3B_2$	$3B_3$	$3B_4$	B_1	$3B_2$	$3B_3$	B_4
C_1	C_1	C_2	C_3	$3C_4$	$3C_1$	C_2	C_3	$3C_4$	C_1	C_2	C_3	C_4
C_2	$3C_1$	$3C_2$	C_3	$3C_4$	$3C_1$	C_2	C_3	$3C_4$	$3C_1$	$3C_2$	$3C_3$	$3C_4$
C_3	$3C_1$	$3C_2$	C_3	$3C_4$	$3C_1$	C_2	C_3	$3C_4$	$3C_1$	$3C_2$	$3C_3$	$3C_4$
C_4	C_1	C_2	C_3	$3C_4$	$3C_1$	C_2	C_3	$3C_4$	C_1	C_2	C_3	C_4

From the accompanying multiplication table it may be noted that multiplication is associative[14] but that the class group fails to exist.

The examples of composition furnished by this ring are in a sense trivial, but they serve to show that the qualifying conditions attached to our earlier theorems are essential, and that the problem of determining all forms which admit composition in a ring is a complicated one.

By composing the third ideal class with the first, we obtain

[14] This follows from the definition of the product of two modules. Monatshefte für Mathematik und Physik, loc. cit. p. 304.

$$3(y_1+y_2+y_3+y_4)^2(y_1+3y_2+3y_3+y^4)^2(z_1z_3-3z_2z_4)^2=3(x_1x_3-x_2x_4)^2.$$

That each side would be a perfect square was predictable, since the algebra is of rank 2. This composition is essentially

$$x_1x_3 - x_2x_4 = (y_1 + y_2 + y_3 + y_4)(y_1 + 3y_2 + 3y_3 + y_4)(z_1z_3 - 3z_2z_4).$$

Let us see if this composition is in accord with the Theorem of Gauss. Here $|S^T(z)|$ vanishes identically and

$$|R(y)| = 3(y_1 + 3y_2 + 3y_3 + y_4)^2(y_1 + y_2 + y_3 + y_4)^2$$

so that $g(y)$ divides $|R(y)|$, while $h(z)$ divides $|S^T(z)|$ trivially.

The example is also of interest in connection with the Theorem of Dickson. Clearly $g(y)$ is not equivalent to $f(x)$, and since $|S^T(z)|$ vanishes identically, it is not expected to be. Since $|R(y)|$ does not represent ±1, $h(z)$ is not equivalent to $f(x)$ in the ring of rational integers, but is equivalent to $f(x)$ in the field of rational numbers.

University of Wisconsin