is moreover according to the independence theorem an intermediary integral of the system of equations (4). If now we choose any particular solution of equations (4) $y = \bar{y}(x)$, $z = \bar{z}(x)$, then a pair of values of α and β always exists, which we will write α_0, β_0, such that $p(x, \bar{y}(x), \bar{z}(x), \alpha_0, \beta_0) \equiv \bar{y}(x)$, $q(x, \bar{y}(x), \bar{z}(x), \alpha_0, \beta_0) \equiv \bar{z}(x)$. When we substitute for y, z, p and q in the identity (11) the functions $\bar{y}(x)$, $\bar{z}(x)$, $\bar{y}'(x)$, $\bar{z}'(x)$, we obtain an identity in x; but (11) becomes in this case the total differential quotient of m with respect to x.

$$\therefore \frac{dm}{dx} = 0, \quad m = \text{const.}$$

Since $\bar{y}(x)$, $\bar{z}(x)$ were chosen arbitrarily, every solution of the system of equations (4) substituted in m gives a constant; hence

$$m(x, y, z, y', z') \equiv \begin{vmatrix} F_{y'y'} & F_{y'z'} \\ F_{z'y'} & F_{z'z'} \end{vmatrix} \div \begin{vmatrix} F'_{y'y'} & F'_{y'z'} \\ F'_{y'z'} & F'_{z'z'} \end{vmatrix} = \text{const.}$$

is an integral of the system (4).

A substitution which leaves system (4) invariant transforms the integral of which (4) are the Lagrange equations either into itself or into a new integral which has the same Lagrange equations. In this latter case, the one integral being given, the construction of such a substitution is equivalent to the construction of an integral.

CORNELL UNIVERSITY,
December, 1906.

ALGEBRAIC NUMBERS AND FORMS.

Zahlentheorie. Fünfter Teil: *Allgemeine Arithmetik der Zahlenkörper.* By PAUL BACHMANN. Leipzig, B. G. Teubner, 1905. xxii + 548 pp.

Einleitung in die allgemeine Theorie der Algebraischen Grössen. By JULIUS KÖNIG. Leipzig, B. G. Teubner, 1903. x + 564 pp.

THERE has been but little activity in America in this important and fascinating field. It seems appropriate, therefore, to preface this review with an elementary introduction to the subject. We shall consider the simpler features of the theory of quadratic number systems, for which the phenomena are

typical of the general case, while the treatment may be made so simple that the fundamental ideas are not obscured by the algebraic intricacies and abstract character of the general theory. It is highly desirable that a very large circle of readers shall acquire a clear insight into the nature of this important field; it is hoped that not a few will be induced by this introduction to pursue this interesting subject in its generality, at least as far as developed in the admirable treatises under review.

Although the fundamental laws obeyed by integers, such as unique decomposition into primes, were observed by Gauss to hold true for his complex integers $a + bi$, this is rarely the case with the system of integral algebraic numbers determined by a root of a given algebraic equation with integral coefficients. Thanks to the genius of Kummer, Dedekind, and Kronecker, the introduction of "ideals" brought complete harmony out of chaos, and marked one of the greatest triumphs of mathematical endeavor. The elaboration and extension of the theory have given rise to an extensive literature, a detailed report of which has been prepared by Hilbert, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, volume 4 (1894–95), pages 175–546. In addition to its great theoretical importance, the subject has vital relations with other branches of mathematics, *e. g.*, Galois's theory of algebraic equations, algebraic functions and their integrals, and diophantine equations.

A number τ is called algebraic if it is the root of an equation

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

with $a_1, \cdots, a_n$ rational numbers. Of all such equations satisfied by τ, there is an unique one of minimum degree m, necessarily irreducible, and τ is called an algebraic number of the mth degree. When $m = 2$, τ is called quadratic.

If the above coefficients a_i are integers, τ is called an integral algebraic number. Examples are $\sqrt{2}$, $3\sqrt{-1}$, $\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

We consider the system $R(\tau)$ of all rational functions of τ with rational coefficients, where τ is a given quadratic algebraic number. We may set $\tau = r + s\sqrt{d}$, r and s rational numbers, $s \neq 0$, while d is an integer, other than $+1$, not divisible by a perfect square. Evidently the system $R(\tau)$ is identical with the system $R(\sqrt{d})$ of all rational functions of $\sqrt{d}$ with rational coefficients.

Lemma I. In $R(\sqrt{d})$, the integral algebraic numbers are given by $x + y\theta$, where x and y are integers, and

$$\theta = \sqrt{d}, \text{ if } d \equiv 2 \text{ or } d \equiv 3 \pmod 4;$$

$$\theta = \tfrac{1}{2}(1 + \sqrt{d}), \text{ if } d \equiv 1 \pmod 4.$$

Consider $a + b\sqrt{d}$, a and b being rational, $b \neq 0$. It and its conjugate $a - b\sqrt{d}$ satisfy the equation

$$z^2 - 2az + a^2 - db^2 = 0.$$

Assuming that the coefficients are integers, we determine the character of a and b. Since $2a$ and $4a^2 - 4db^2$ are integers, while d has no square factor, $2b$ must be integral. Hence

$$a = \alpha/2,\ b = \beta/2, \qquad (\alpha \text{ and } \beta \text{ integers}).$$

It remains to require that $a^2 - db^2$, viz., $\frac{1}{4}(\alpha^2 - d\beta^2)$, be integral. If $d \equiv 2 \pmod 4$, α^2 must be even and hence α and β both even. If for $d \equiv 3 \pmod 4$ α were odd, $\frac{1}{4}(1 - 3\beta^2)$ could not be integral. If $d \equiv 1 \pmod 4$, α and β must both be even or both odd, so that $a + b\sqrt{d}$ is of the respective forms $\lambda + \mu\sqrt{d}$, $\lambda + \mu\sqrt{d} + \theta$, where λ and μ are integers and $\theta = \frac{1}{2}(1 + \sqrt{d})$. Setting $x = \lambda - \mu$, $y = 2\mu$ or $2\mu + 1$, respectively, we get $x + y\theta$. The lemma is therefore proved.

Given two integral algebraic numbers α and β of a domain* $R(\theta)$, we shall say that α is divisible by β if there exists in $R(\theta)$ an integral algebraic number q such that $\alpha = \beta q$.

For $d = -1$, the integral algebraic members of $R(i)$ are Gauss's complex integers $x + yi$. Two complex integers α and α_1 have a greatest common divisor δ, defined by the two properties:

1. α and α_1 are divisible by δ;
2. Every common divisor of α and α_1 is a divisor of δ.

Here δ may be determined (uniquely up to a factor $\pm 1, \pm i$) by the following process: Set $\alpha/\alpha_1 = a + bi$ and determine a complex integer $\xi = x + yi$ such that the norm $(a - x)^2 +$

*Our interest will always center in a domain defined by a root θ of a given algebraic equation. There is little interest in the arithmetic of the system of all integral algebraic numbers of all degrees. In fact, decomposition is then unlimited. Thus $\alpha = \alpha^{1/2}\alpha^{1/2}$, where $\alpha^{1/2}$ is integral algebraic when α is.

$(b-y)^2$ of $\alpha/\alpha_1 - \xi$ shall be less than unity; we have only to select integers x and y such that $|a-x| \leqq \frac{1}{2}, |b-y| \leqq \frac{1}{2}$. Then

$$\alpha = \xi\alpha_1 + \alpha_2, \quad \text{norm } \alpha_2 < \text{norm } \alpha_1,$$

where α_2 is a complex integer. If $\alpha_2 \neq 0$, we proceed similarly with α_1 and α_2, and determine complex integers ξ_1 and α_3 such that

$$\alpha_1 = \xi_1\alpha_2 + \alpha_3, \quad \text{norm } \alpha_3 < \text{norm } \alpha_2.$$

Since the norms of $\alpha_1, \alpha_2, \alpha_3, \cdots$ form a series of decreasing positive integers, we must reach a term α_{r+1} of zero norm. Then α_r is the required number δ. It is now a simple matter to prove* that every complex integer can be expressed as a product of primes in one way and essentially but one way (*i. e.*, up to a factor $\pm 1, \pm i$).

In general, the state of affairs is entirely different. For illustration, we take Dedekind's simple example $d = -5$ (Dedekind, l. c., page 451 and 547; König, pages 19, 93). In $R(\theta)$, where $\theta = \sqrt{-5}$, the integral algebraic numbers are $x + y\theta$, x and y integers (Lemma I). Here there are two ways of factoring 9, viz.,

$$3 \cdot 3 = (2+\theta)(2-\theta), \tag{1}$$

while 3, $2 \pm \theta$ differ from the units (here ± 1) and each is indecomposable in $R(\theta)$, *i. e.*, has no factor other than itself, its negative, and ± 1. For example, if

$$2 + \theta = (x + y\theta)(z + w\theta),$$

then

$$2 - \theta = (x - y\theta)(z - w\theta).$$

By multiplication (or by taking the norms in the first equation),

$$9 = (x^2 + 5y^2)(z^2 + 5w^2). \tag{2}$$

But $x^2 + 5y^2 = 3$ is not solvable in integers. Hence one of the assumed factors of $2 + \theta$ must be ± 1. This discussion of

* Dirichlet-Dedekind, Zahlentheorie, 1894, pp. 434–450. On p. 450 Dedekind cites eight further examples of quadratic number systems in which an analogous g. c. d. process holds. For the case of negative discriminant, Birkhoff has determined geometrically (*Amer. Math. Monthly*, Aug., 1906) all such quadratic number systems.

(2) shows that also 3 is indecomposable. Hence 9 has two sets of indecomposable factors (1). There are other respects in which the laws of arithmetic here fail. Although 3 is indecomposable it does not have the true nature of a prime, since by (1) 3 divides the product $(2+\theta)(2-\theta)$ but does not divide either factor. Again as König points out, the numbers 9 and $3-6\theta$ have no greatest common divisor in the sense 1, 2, above. In fact the only factors (apart from sign) of 9 are 1, 3, 9, $2\pm\theta$; the only factors of $3-6\theta$ are 1, 3, $1-2\theta$, $2-\theta$, $4-\theta$, $3-6\theta$. The common factors are 1, 3, $2-\theta$, no one of which is divisible by the other two, as seen above.

To overcome these difficulties Kummer would introduce "ideal prime numbers" α, β, γ, such that

$$3=\alpha\beta, \quad 2+\theta=\alpha^2, \quad 2-\theta=\beta^2, \quad 1-2\theta=\beta\gamma.$$

Thus each member of (1) decomposes further into $\alpha^2\beta^2$, so that there is only one decomposition of 9 into ideal primes. Again, there is now a greatest common divisor of 9 and $3-6\theta=\alpha\beta^2\gamma$, viz., $\alpha\beta^2$. Dedekind* has given a complete treatment by Kummer's ideals of the laws of divisibility in the system of integral algebraic numbers of this domain $R(\sqrt{-5})$; he emphasizes, however, the delicacy of the problem and the necessity of "the greatest circumspection." Kummer and his followers succeeded in applying his method to but few types of domains (cf. Bachmann, pages 150–159). In addition to the practical difficulties, there is the logical objection to Kummer's theory that an ideal number is not defined in itself, but merely its presence or absence as a factor of an existing integral complex number (the criteria being congruential conditions). As Kummer's work is now of mere historical interest, we pass to Dedekind's method which is open to none of the objections cited. We shall go into details only for quadratic domains.

Let θ denote a fixed quadratic number defined as in Lemma I, and consider the system $I(\theta)$ of integral algebraic numbers $\xi=x+y\theta$, x and y being integers. If μ is a fixed number of $I(\theta)$, the set of products $\xi\mu$ is closed under addition and subtraction, since $\xi_1\mu\pm\xi_2\mu=(\xi_1\pm\xi_2)\mu$; and also under multiplication by any number ρ of I, since $\rho(\xi\mu)=(\rho\xi)\mu$, and since

* *Bulletin des Sciences mathématiques et astr.*, ser. 2, vol. 1 (1877), p. 69. In a series of five articles in this and the preceding volume Dedekind gives an elementary account of Kummer's method and the origin of his own theory.

the product $\rho\xi$ of two numbers of I belongs to I. This particular set of all the multiples of μ will be called a principal ideal (μ). In general, we define as an ideal any system S of numbers * of $I(\theta)$ which have the two properties stated, viz.,

(A) The sum and difference of any two (equal or distinct) numbers of the system S are themselves members of this system S;

(B) Every product of a number of the system S and a number of the system $I(\theta)$ is a number of the system S.

We proceed to give a simple formula for the numbers of such an ideal S. We first investigate systems S having property (A) only. The numbers of S fall into two sets: $k_1, k_2, k_3, \cdots$, and $l_1 + m_1\theta, l_2 + m_2\theta, \cdots$, where no $m_i = 0$. Let k be the greatest common divisor of the integers $|k_1|, |k_2|, \cdots$, and m that of $|m_1|, |m_2|, \cdots$ A suitably chosen linear combination of the $l_i + m_i\theta$ gives $l + m\theta$, l an integer. Hence the system S contains k and $l + m\theta$. Conversely, any number $x + y\theta$ of S is a linear function of k and $l + m\theta$. For if $y = 0$, x must be a multiple of k; while if $y \neq 0$, then $y = qm$, so that

$$(x + y\theta) - q(l + m\theta) \equiv x - ql$$

is an integer and hence of the form $q'k$. We thus have

Lemma II. Any system of numbers of $I(\theta)$ which has property (A) may be exhibited as the set $[k, l + m\theta]$ of all linear homogeneous functions with integral coefficients of k and $l + m\theta$, where k and m are positive integers and l an integer.

We next require that S shall have also property (B). The necessary and sufficient conditions are that $k\theta$ and $(l + m\theta)\theta$ shall belong to S. By Lemma I, there are two cases

$$\theta^2 - d = 0\,;\ \theta^2 - \theta + \tfrac{1}{4}(1 - d) = 0. \tag{3}$$

In either case, the preceding conditions require that k and l be divisible by m. Hence $S = [ma, m(b + \theta)]$, where a and b are integers, $a > 0$. In this notation, we examine more minutely the condition that $m(b + \theta)\cdot\theta$ shall belong to S. For case (3_1), this equals $md + mb\theta$. But $b \cdot m(b + \theta)$ occurs in S. By subtraction, we get the integer $mb^2 - md$, which occurs in S if and only if $b^2 - d$ is a multiple of a. Treating case (3_2) similarly, we obtain

* We exclude the system composed of zero only.

Lemma III. For a quadratic domain defined by a root of one of the equations (3), the ideals are given by $[ma, m(b+\theta)]$, where a, b and m are integers subject to the respective conditions

$$(3') \quad b^2 - d \equiv 0 \pmod{a}; \quad b^2 + b + \tfrac{1}{4}(1-d) \equiv 0 \pmod{a}.$$

Multiplication of ideals is defined as follows: If μ ranges over the numbers of an ideal S, and μ' over the numbers of an ideal S', then the products $\mu\mu'$ and their sums form an ideal S'', called the product of the factors S, S', and designated SS'.

In particular, for $\theta^2 = d$, the product of

$$S = [ma, m(b+\theta)], \quad b^2 \equiv d \pmod{a},$$

and the conjugate ideal

$$S_1 = [ma, m(-b+\theta)]$$

is the ideal SS_1, expressed initially in the form

$$[m^2a^2, m^2a(-b+\theta), m^2a(b+\theta), m^2(-b^2+d)],$$

viz., the aggregate of the linear homogeneous functions with integral coefficients of these four numbers. Let c denote the integer $(b^2-d)/a$. After obvious modifications, we have

$$SS_1 = [m^2a^2, 2m^2ab, m^2ac, m^2a(b+\theta)].$$

The greatest common divisor of the first three numbers is m^2ag, where g denotes that of a; $2b$, c. If a and c had the common factor 2, then $b^2 - d = ac \equiv 0 \pmod{4}$, and $b^2 \not\equiv 0 \pmod{4}$ since d has no square factor; hence would $b^2 \equiv 1$, $d \equiv 1 \pmod{4}$, which contradicts the present hypothesis (Lemma I). Hence g is odd. If $g > 1$, $b^2 - d = ac \equiv 0 \pmod{g^2}$, and d would have a square factor g^2. Hence $g = 1$. Since a, $2b$, c have the greatest common divisor 1, a suitable linear combination of them equals 1. Hence

$$SS_1 = [m^2a, m^2a(b+\theta)] = [m^2a, m^2a\theta],$$

and hence is formed of all the complex integral multiples of m^2a, *i. e.*, is the principal ideal (m^2a).

For the case (3_2), we denote the second number $(3')$ by ac, and find similarly that the greatest common divisor of a, $2b+1$, c is unity, since $d=(2b+1)^2-4ac$. Setting $S_1=[ma, m(b+\bar{\theta})]$, where $\bar{\theta}$ is the second root of (3_2), we find as before that SS_1 is the principal ideal (m^2a). Hence we have

Theorem I. For a quadratic domain, the product of any ideal and its conjugate is a principal ideal.

Corollary. If $SS'=SS''$, then $S'=S''$.

For, if S_1 is the ideal conjugate to S, then SS_1 is a principal ideal, say (t), where t is an integer. Then

$$S_1SS'=S_1SS'',\ (t)S'=(t)S'',$$

so that the ideals S' and S'' include the same numbers.

Theorem II. If all the numbers of an ideal C belong to an ideal A, there exists an ideal B such that $AB=C$, and conversely.

Under this first hypothesis, the numbers of CA_1 belong to the principal ideal $AA_1=(t)$, A_1 being the conjugate to A. Thus the numbers of CA_1 are $\lambda_1 t, \lambda_2 t, \cdots$, the λ's in $I(\theta)$. Since properties (A) and (B) hold for the ideal CA_1, we have, for every number ρ of $I(\theta)$,

$$\lambda_1 t+\lambda_2 t=\lambda_i t,\ \lambda_1 t-\lambda_2 t=\lambda_j t,\ \rho(\lambda_1 t)=\lambda_k t,$$

$\lambda_i, \lambda_j, \lambda_k$ belonging to the set $\lambda_1, \lambda_2, \cdots$. Since the factor t may be dropped, the numbers $\lambda_1, \lambda_2, \cdots$ themselves have the characteristic properties (A) and (B) of an ideal, and hence form an ideal B. From $CA_1=B(t)$ and $AA_1=(t)$ follows $C=AB$, by the preceding corollary.

The converse proposition that every number of AB belongs to A follows from the definition of multiplication of ideals and properties (B), (A).

According to Dedekind, who is followed by Bachmann, an ideal C is said to be divisible by an ideal A if all the numbers of C belong to (occur in) A. According to Hurwitz,* Hilbert, and others, an ideal C is divisible by an ideal A if there exists an ideal B such that $C=AB$. In Theorem II, we have shown (for quadratic domains) that the two definitions † are in complete accord.

* "Ueber die Theorie der Ideale," *Göttinger Nachrichten*, 1894, pp. 291–298.

† Dedekind's objections to the second definition are given in the *Göttinger Nachrichten*, 1895, pp. 106–113.

Lemma IV. A positive integer t occurs only in a finite number of ideals of a given quadratic number domain.

For, if $[k, l + m\theta]$ is an ideal containing t, it follows from the proofs of Lemmas II and III, that k is a divisor of t, and m a divisor of k, while obviously l can be reduced modulo k.

Theorem III. Any ideal A is divisible by only a finite number of ideals.

If A_1 is the ideal conjugate to A, then AA_1 is a principal ideal (t), by Theorem I. This integer t thus occurs in every ideal which divides A.

The principal ideal (1), which is evidently composed of all the integral algebraic numbers of the domain, plays the rôle ot unity in multiplication and division. An ideal, different from (1) and divisible by no ideal other than itself and (1), is called a prime ideal.

Theorem IV. If the prime ideal P divides the product AB, it divides A or B.

Suppose that P does not divide A. Then the ideal composed of the linear combinations of the numbers of both A and P divides P and yet is distinct from P, and hence is (1). Hence $1 = \alpha + \pi$, where α is some number of A, π some number of P. Let β be any number of B. Then $\beta = \alpha\beta + \pi\beta$. By hypothesis, $\alpha\beta$ occurs in P. Hence by the definition of ideals, β occurs in P. Hence B is divisible by P.

Theorem V. Every ideal A, other than (1), can be expressed in one and but one way as a product of a finite number of prime ideals.

If A is not itself a prime ideal, it has a divisor A_1 distinct from (1) and A, and $A = A_1A_2$, where A_2 is distinct from A and (1). If one of the ideals A_1 and A_2 is not a prime ideal, it equals the product of two ideals, and we get $A = A_1'A_2'A_3'$. This procedure ultimately terminates, so that A is divisible by a prime ideal. In fact, by Theorem III, A is divisible by only a finite number n of ideals. Hence A is not equal to a product of more than n ideals, equal or distinct, but $\neq (1)$, since a relation $A = B_1B_2 \cdots B_{n+1}$ would require the existence of the $n + 1$ distinct ideal divisors $B_1, B_1B_2, \cdots, B_1B_2 \cdots B_{n+1}$. We therefore obtain a factorization $A = P_1 \cdots P_r$ into prime ideals.

This factorization is unique in view of Theorem IV.

It now follows that ideals obey the fundamental laws of divisibility holding for integers. The arithmetic of ideals thus becomes a subject of decided interest and importance.

There remains the question of the disposition to be made of the difficulties encountered in the arithmetic of the integral algebraic numbers forming the system $I(\theta)$. To every number μ of $I(\theta)$ corresponds a principal ideal (μ), and conversely. If $\mu\lambda = \nu$, then $(\mu)(\lambda) = (\nu)$. To each non-principal ideal A we may make correspond * a fictitious entity called an "ideal number" α, such that $AB = C$ implies $\alpha\beta = \gamma$. When A is a prime ideal, α is called a "prime ideal number." This scheme is not to be confused with Kummer's. He required very complicated machinery which worked only for special domains. On the contrary, we are now throwing the burden on the simple theory of ideals and deriving by formal correspondence the needed properties of the ideal numbers.

The text by Bachmann is very appropriately dedicated to Dedekind, as it develops Dedekind's original theory of integral algebraic numbers and employs almost exclusively the methods insisted upon by the latter. In a few instances, however, Bachmann departs from Dedekind's purely arithmetical standpoint which does not permit the use of arbitrary variables and undetermined coefficients. The deviations occur in the exposition of Hensel's work and in making use of the simplifications due to Hurwitz and others. In fact, König (page 482) insists that "die von verschiedenen Autoren für die Dedekind'sche Idealtheorie gegebenen 'Vereinfachungen' beruhen durchweg auf einer mehr oder weniger verhüllten Anwendung der Kroneckerschen Grundideen." The exposition by Dedekind (Zahlentheorie, pages 434–657) is in parts very elementary and amply illustrated by simple examples, but in other parts is very abstract, requiring the reader to hold in mind an array of technical concepts, symbols and names. By using fewer abstract proofs and adopting a more expansive style of presentation, Bachmann has produced a book everywhere readable. As noted above for ideals, so for the more general concept modulus, viz., a system of numbers closed under addition and subtraction, Dedekind says that if all the numbers of a modulus C occur also in the modulus A then C is divisible by A

* Instead of relying upon the principle of correspondence, it seems allowable to the reviewer to define our ideal "numbers" to be the ideals themselves. In thus speaking of an ideal (*viz.*, a certain aggregate of integral algebraic numbers) as a "number," we have the precedent that certain ordered aggregates $(a_1, a_2, \cdots, a_n)$ of real numbers $a_1, \cdots, a_n$ are called hypercomplex numbers, the customary limitation that n shall be finite not being essential. Again, we may define an irrational number to be the inferior class of rational numbers obtained by a Dedekind cut.

and C is a multiple of A, and writes $C > A$. Since the aggregate C is smaller than the aggregate A, the terms "divisible" and "multiple" are used in a technical sense, reverse to the usual numerical sense. While one may carry in mind the technical names it is asking too much to reason with a familiar symbol in the reverse of customary usage. We therefore welcome Bachmann's introduction of an entirely new symbol for "contained in" and replacing Dedekind's $>$. It would seem preferable, however, to the reviewer to use the symbol $a \equiv 0\ (A)$ to denote that the number a is contained in the modulus A, and similarly $C \equiv 0\ (A)$. In the spirit of modular systems, this notation would naturally mean that the numbers of C are contained in the modulus A, and also, as in the elements of congruences, that C is divisible by A. If Dedekind's theory of the modulus were presented with this notation, the reader would not find it necessary continually to struggle with himself. For the special case of ideals, the notation is used by Hilbert in his Report (page 183).

Bachmann states at the bottom of page 154 that for quadratic domains $R(\sqrt{d})$ the introduction of ideals is necessary if there is more than one class of quadratic forms of determinant d. There may however be two classes differing by the factor -1 (cf. Dedekind, l. c., page 451). A few misprints may be noted; page 227, line 7, contains a misprint for p; page 231, line 12, contains a misprint for γ.

The present volume by Bachmann serves admirably its purpose of affording a simple and attractive introduction to Dedekind's theory of the general arithmetic of algebraic numbers; there is promised a supplementary volume treating of special types of number domains.

The treatise by König is much more than a presentation of results contained in the memoirs of Kronecker and his followers; it must be regarded also in the light of an original contribution to the subject, containing new points of view, completing fragmentary results, replacing incomplete by adequate proofs, and undertaking new developments of fundamental nature. The text is far more than a commentary on Kronecker's fundamental "Festschrift zu Herrn E. E. Kummer's Doktor-Jubiläum, 10. Sept. 1881." The subjects treated include the divisibility of forms, factorization of forms, Kronecker's abstract formulation of the adjunction of a root of an algebraic equation, Galois's theory, Kronecker's method of

elimination, general theory of resultants, discriminants, functional determinants, algebraic manifolds, divisor systems (modular systems), algebraic and arithmetic theories of linear diophantine problems, theorems of Noether and Hilbert, and finally the theory of integral algebraic quantities. The concepts of this rich array of general material are so interwoven that a report upon a particular part would be entirely unsatisfactory, while the limitations of space here preclude a survey of the whole. Although the theory of ideals does not play as predominating a rôle in this subject as in the theory of algebraic numbers, a few remarks in this direction will afford a suitable sequel to the earlier part of this composite review. The introduction of "ideal quantities" to bring harmony into the laws of divisibility of integral algebraic forms is accomplished in a most pleasing manner by König.

At the outset we consider the two domains

$$(A, x_1, \cdots, x_m), \qquad [A, x_1, \cdots, x_m],$$

formed respectively of all rational, and all rational integral functions of the indeterminates $x_1, \cdots, x_m$ with coefficients in A, where (for the purely arithmetical theory) A denotes the system [1] of all integers, while (for the algebraic theory) A denotes a field * composed of real or complex numbers (some of which may be indeterminates other than the x's). Let $F_0, \cdots, F_n$ denote any forms in the domain $[A, x_i]$ such that

$$F_0 z^n + F_1 z^{n-1} + \cdots + F_n = 0$$

is irreducible in (A, x_i). Let its roots be $\alpha_1, \cdots, \alpha_n$. Let

$$\Gamma = (A, x_1, \cdots, x_m ; \alpha)$$

be the domain obtained by the adjunction of $\alpha = \alpha_1$ to (A, x_i). Then Γ is formed of the quantities

$$g(\alpha) = (G_0 + G_1\alpha + \cdots + G_{n-1}\alpha^{n-1}) \div H,$$

where the G's and H are any forms in $[A, x_i]$ such that $H \neq 0$. Then

$$\text{norm } g(\alpha) \equiv \prod_{i=1}^{n} g(\alpha_i)$$

equals the quotient of two quantities of $[A, x_i]$.

* An aggregate closed under the four rational operations, addition, etc.

Let $u_1, \cdots, u_m$ be new indeterminates and let $U_1, U_2, \cdots$ denote distinct products of powers of the u's subject only to the condition that $U_r = U_s$ implies $r = s$. We consider the general form

$$f(\alpha) \equiv \sum g_r(\alpha) U_r.$$

It satisfies the equation

$$\text{norm } (z - f) \equiv \prod_{i=1}^{n} [z - f(\alpha_i)] = 0$$

whose coefficients are forms in $u_1, \cdots, u_m$, the coefficients of these forms being quotients of quantities in $[A, x_i]$ and therefore quantities in (A, x_i). This norm is an exact power of a form $N(z)$, irreducible in (A, x_i, u_i) *, as follows readily from the irreducibility of the equation for the α's. We may suppose the coefficients in $N(z) = 0$ free of denominators. It is a fundamental theorem in Kronecker's theory that there exists a greatest common divisor process for two forms in a domain $[A, x_i, u_i]$, when there is such a process for numbers of A; the latter is obviously here the case since A is either a field or the system [1] of all integers. Hence our form f satisfies an equation $G_0 z^d + \cdots + G_d = 0$, irreducible in $[A, x_i, u_i]$, such that $G_0, \cdots, G_d$ have no common divisor. In case G_0 is a unit (divisor of 1), we may set $G_0 = 1$ and call the root f an "integral algebraic form" (with respect to the domain Γ). It is easy to establish the equivalence of this definition with the following. The form f is an integral algebraic form if and only if it satisfies some equation

$$z^d + G_1 z^{d-1} + \cdots + G_d = 0$$

whose coefficients are forms of the domain $[A, x_i, u_i]$. By suppressing the indeterminates u_i, we obtain the definition of the integral algebraic quantities of Γ. Denote by $[\Gamma]$ and $[\Gamma]_u$ the domains composed of all these integral algebraic quantities and forms, respectively. Each domain is closed under addition, subtraction and multiplication.

A non-field domain D is called complete (vollständig) when any two of its quantities have in D a greatest common divisor δ, in the sense 1, 2, above. As already noted, $[A, x_i]$ is a complete domain. But a domain $[\Gamma]$, just defined, is complete

* The u's should appear in the notations of the domains, bottom of p. 464 (König).

only in the very simplest cases; this point is illustrated in the above example of the numbers $a + b\sqrt{-5}$, a and b integers. Hence we cannot here define, as in algebra, a primitive form to be one in which the greatest common divisor of its coefficients is 1 (or a unit). Following Kronecker (Festschrift, § 15), we say that for a domain $[\Gamma]$ a form ϕ is "primitive" if norm ϕ is a primitive form of the indeterminates u_i in the elementary sense.

We may now make a clear statement of the problem of the association of ideal quantities. We seek to enlarge the domain $[\Gamma]$ into a complete domain $[G]$ in such a manner that not merely the additive and multiplicative combinations, but also the properties relating to divisibility of the quantities of $[\Gamma]$ shall remain valid in the new domain $[G]$. In symbols, if α, β, γ are any quantities in $[\Gamma]$, there shall exist quantities α', β', γ' in $[G]$ such that $\alpha + \beta = \gamma$ implies $\alpha' + \beta' = \gamma'$, $\alpha\beta = \gamma$ implies $\alpha'\beta' = \gamma'$, and conversely, while if α is [or is not] divisible by β then α' is [or is not] divisible by β', and conversely. The most exacting requirement is that $[G]$ shall be a complete domain.

All these conditions are met in the simplest manner by the domain $[G]$ of all the quotients γ_u/ϵ_v, where γ_u is an arbitrary form of $[\Gamma]_w$ and ϵ_v an arbitrary primitive form of $[\Gamma]_w$, addition and multiplication in $[G]$ being defined by

$$\frac{\gamma_u}{\epsilon_v} + \frac{\gamma'_{u'}}{\epsilon'_{v'}} = \frac{\gamma_u\epsilon'_{v'} + \gamma'_{u'}\epsilon_v}{\epsilon_v\epsilon'_{v'}}, \quad \frac{\gamma_u}{\epsilon_v} \cdot \frac{\gamma'_{u'}}{\epsilon'_{v'}} = \frac{\gamma_u\gamma'_{u'}}{\epsilon_v\epsilon'_{v'}}.$$

The sum and product belong to $[G]$ since the product of two primitive forms ϵ_v and $\epsilon'_{v'}$ is a primitive form, and since the domain $[\Gamma]_w$ is closed under addition and multiplication. The units of $[G]$ are the quantities ϵ'_u/ϵ_v, where also the numerator is primitive. One of the conditions that $[G]$ be a complete domain is that it be not a field,* and this is satisfied since $2x = 1$ is not solvable in $[G]$. In fact, $2\gamma_u = \epsilon_v$ is impossible since the norm of the primitive form ϵ_v is not divisible by 2. Finally, any two quantities γ_u/ϵ_v and $\gamma'_{u'}/\epsilon'_{v'}$ of $[G]$ have in $[G]$ a greatest common divisor, which (or any product of it by a unit) may be exhibited as the form

$$\delta_w = \sum_{(r)} C_r W_r + \sum_{(s)} C'_s W'_s,$$

* Were it not for this condition, we could take as $[G]$ simply the field $[\Gamma]$ composed of all quotients of the quantities of $[\Gamma]$.

where $C_1, C_2, \cdots$ denote the coefficients of the form γ_u; $C'_1, C'_2, \cdots$ the coefficients of $\gamma'_{u'}$; while W_r and W'_s denote distinct products of powers of the variables $w_1, w_2, \cdots$. Naturally, we do not enter here upon the proof* that δ_w has the properties 1, 2 of the greatest common divisor.

The quantities of $[G]$ are called "ideal quantities" of $[\Gamma]$, although some of them already occur in $[\Gamma]$. That the ideals here admit of addition as well as multiplication is a pleasing feature of König's theory not found in Dedekind's theory of ideals, nor in Kronecker's exposition. Ideals of the König type appear in Weber's treatment (Algebra, volume 2) of the more special theory of algebraic numbers.

L. E. DICKSON.

THE UNIVERSITY OF CHICAGO.

CORRECTION.

PROFESSOR Wilczynski has kindly called my attention to the following misstatements in my review of his Projective Differential Geometry (BULLETIN, pages 190–194).

P. 191. The second member of the expression for $\theta_{3,1}$ should be completed by adding $-27P_2\theta_3^2$.

P. 191, line 5 from bottom. Strike out first sentence and substitute "The osculating cubic may hyperosculate C_y."

P. 191. For last clause read: "If $\theta_{3,1} = 0$, then C_y is a curve of coincidence points."

P. 193, line 6. For θ_4 read θ_9.

P. 193, line 6 from bottom. For "second" read "same."

P. 193, line 2 from bottom. After "range" insert "in certain cases."

VIRGIL SNYDER.

NOTES.

AT the meeting of the London mathematical society held on February 14, the following papers were read: By G. A. MILLER, "Groups defined by the order of the generators and the order of their commutator"; by T. STUART, "On the reduction of the factorization of binary septans and octans to the

* König, p. 479. Misprints in the accents occur in the formula at the middle of this page; while at the top of p. 474, β_u should read β_v.