for $i = 1, 2, \ldots, r$ imply $x \equiv y \pmod N$. The theorem will be proved if we show that no system $V_1 = \left(a^{(1)}, \ldots, a^{(g)}, (1, 1, \ldots, 1); A\right)$ with $A \geqslant N-1$ and $a^{(i)}$ corresponding for $i = 1, 2, \ldots, g$ to orbits of the form (X, X) can be admissible. Assume the contrary, and let

$$a^{(i)} = (\varepsilon_1^{(i)} h_1/2, \ldots, \varepsilon_g^{(i)} h_g/2, 0, \ldots, 0) \quad \text{with} \quad \varepsilon_j^{(i)} = 0, 1.$$

The vectors $\bar{e}_i = (\varepsilon_1^{(i)}, \ldots, \varepsilon_g^{(i)})$ are linearly independent over GF(2) (due to admissibility of V_1), thus we can find $\eta_1, \ldots, \eta_g = 0, 1$ such that with $M = \text{l.c.m.}\,(h_1/2, \ldots, h_g/2, h_{g+1}, \ldots, h_r)$ and some integral $n_1, \ldots, n_g$

$$\eta_1 \bar{e}_1 + \ldots + \eta_g \bar{e}_g = (2n_1 + 2M/h_1, \ldots, 2n_g + 2M/h_g).$$

Now an easy checking shows us that the kth component of

$$\eta_1 a^{(1)} + \ldots + \eta_g a^{(g)} + M(1, 1, \ldots, 1)$$

is congruent to zero $(\bmod h_k)$ for $k = 1, 2, \ldots, r$, which in view of admissibility of V_1 implies $M > A$, but clearly $M \leqslant N/2$, and as $A \geqslant N-1$, we obtain a contradiction. The theorem is thus proved.

References

[1] W. Narkiewicz, *On natural numbers having unique factorization in a quadratic number field*, Acta Arith. 12 (1966), pp. 1-22.

[2] — — II, ibidem, 13 (1967), pp. 123-139.

MATHEMATICS INSTITUTE OF THE WROCŁAW UNIVERSITY

Reçu par la Rédaction le 7. 11. 1967

ACTA ARITHMETICA
XV (1968)

Modules and binary quadratic forms

by

HUBERT S. BUTTS and GORDON PALL* (Baton Rouge, La.)

1. Introduction. The basic result of this article is Theorem 6.1, which gives an algorithm whereby the transformations T of a primitive binary quadratic form f into a multiple $e \cdot g$ of a primitive binary quadratic form g are uniquely related to representations of e by one of two specific forms according as $e(\det T)$ is positive or negative. Allowing e to vary, one deduces certain remarkable additive properties of the transformations of a binary quadratic form into an arbitrary multiple of another. These, it may be mentioned, are useful in a new theory of reduction of the quaternary quadratic forms which arise as norm forms of modules in quaternion rings.

The article developed when we sought to interpret these phenomena in connection with modules in a quadratic field. This led us to re-examine the Dedekind relations between classes of modules (or ideals) in a quadratic field under multiplication and classes of binary quadratic forms under composition. It appeared that Dedekind had somewhat artificially forced the one-one association between module and form classes, by adopting a different convention for definite and indefinite forms, by restricting bases artificially, and by defining a narrow module equivalence. Technically what he did was correct. But he did obscure the essential simplicity of the relationship, which we will describe in § 3, and which seems to us to be more natural and still pleasing. Our approach generalizes better. Dickson's *History of the Theory of Numbers* lists on p.70 of Vol. III several items concerned with the Dedekind relation (H. Weber [15], R. König [11], J. Sommer [14], who mentions in § 35 a paper by E. E. Kummer [10], P. Bachmann [1], R. Fricke [6]). Subsequent items that we know of are due to E. Hecke [8], E. Landau [12], and Z. I. Borevich and I. R. Shafarevich [2].

---

* This work was supported in part by National Science Foundation grants GP 6467 and GP 3956.

In his treatment of composition in the *Disquisitiones* [7], Gauss starts by generalizing the age-old identity expressing a product of two sums of two squares as a sum of two squares, and defines a form

$$f'' = a''x''^2+b''x''y''+c''y''^2$$

(of nonzero determinant Δ) to be compounded of the forms

$$f = ax^2+bxy+cy^2 \quad \text{and} \quad f' = a'x'^2+b'x'y'+c'y'^2$$

if there exists a primitive bilinear substitution

$$x'' = p_0xx'+p_1xy'+p_2x'y+p_3yy',$$

$$y'' = q_0xx'+q_1xy'+q_2x'y+q_3yy',$$

under which $f'' = ff'$. *Primitive* means that the coefficients are integers and that the six determinants $P = p_0q_1-p_1q_0$, $Q = p_0q_2-p_2q_0$, $R = p_0q_3-p_3q_0$, $S = p_1q_2-p_2q_1$, $T = p_1q_3-p_3q_1$, $U = p_2q_3-p_3q_2$ are coprime. Subsequently it is shown that if such a primitive substitution exists the determinants of f and f' have the form Δn^2 and $\Delta n'^2$ where n and n' are rational; and that the signs of n and n' can be chosen so that

$$Px^2+(R-S)xy+Uy^2 = n'f \quad \text{and} \quad Qx'^2+(R+S)x'y'+Ty'^2 = nf'.$$

If the primitive substitution can be chosen so that n and n' are positive, then f'' is in a strong sense the compound of f and f'; and if composition is defined in this strong sense the classes (provided class is defined under the group of transformations which are unimodular, i.e., have integral coefficients and determinant $+1$) of two of the three forms determine the class of the third. Then the primitive classes of a fixed discriminant d form an abelian group. It is this group, or a subgroup thereof of index 2, which is the famous class group.

Gauss actually studied composition for forms of different discriminants and was in large measure aware of the semigroup which we will develop in § 2, and which is needed to make the association between module and form classes complete. But the post-Gaussian literature on composition of binary quadratic forms has usually been restricted to forms of one discriminant. This is probably due to the fact that Dirichlet in his doctoral dissertation gave an alternative treatment of composition based on representation of numbers, or what is essentially equivalent, on united forms; and chose in his eminently readable and beautiful book [5] to treat composition only for forms of a fixed discriminant. Dirichlet also omitted square discriminants (which Gauss had treated — with a remark that any property which holds for definite and indefinite forms alike will extend to forms of nonzero square discriminants). As a result the

picture of composition in subsequent work has been somewhat incomplete and the connection with modules correspondingly imperfect.

Instead of focusing on the maximal ring we have tried to study the various orders of integral elements alike, and have used forms or modules, whichever seemed simpler. This has perhaps enabled us to uncover new and interesting aspects of an ancient subject.

Notations. Unless otherwise stated small Latin letters denote elements of Q (the field of rationals); w is a squarefree integer. If $w \neq 1, j$ denotes a fixed value of $\sqrt{w}$, and F_j is the quadratic field $Q(j)$. If $w = 1, j$ denotes a symbol (not a number) such that $j^2 = 1$, and F_j is the commutative associative algebra of order 2 over Q with the basis $1, j$. Small Greek letters denote elements of F_j. If $\alpha = a_0+a_1j$, $\bar{\alpha} = a_0-a_1j$, $N\alpha = \alpha\bar{\alpha} = a_0^2-wa_1^2$. Thus if $w \neq 1$, $\alpha = 0$ if and only if $N\alpha = 0$. Set $d_0 = w$ or $4w$ according as $w \equiv 1$ or $w \not\equiv 1 \pmod 4$. We will deal simultaneously with the set of discriminants

$$\mathscr{D} = \{d_0s^2 \mid s = 1, 2, 3, \ldots\}. \tag{1.1}$$

To each d in $\mathscr{D}$ corresponds an order (ring of integral elements with unity)

$$R_d = \{\text{all } x_0+x_1\omega \mid x_0, x_1 \text{ in } Z\}. \tag{1.2}$$

Here Z is the set of rational integers, and $\omega = \omega_d$ is

$$(1+sj)/2 \text{ if } d \equiv 1, \quad sj \text{ if } d \equiv 0 \pmod 4. \tag{1.3}$$

Thus $\omega = (\varepsilon+\sqrt{d})/2$, where $\varepsilon = 0$ or 1 according as $d \equiv 0$ or $1 \pmod 4$, and $\sqrt{d}$ means tj if $d = t^2$ $(t > 0)$. Also, $\omega+\bar{\omega} = \varepsilon$, $\omega^2 = \varepsilon\omega-(\varepsilon-d)/4$, and

$$N(x_0+x_1\omega) = x_0^2+\varepsilon x_0x_1+(\varepsilon-d)x_1^2/4.$$

2. The abelian semigroup $\mathscr{S}$ of primitive classes of binary quadratic forms with discriminants in $\mathscr{D}$.

THEOREM 2.1. *By a technique given below there is associated with any primitive classes C_1, C_2 with discriminants in $\mathscr{D}$ a unique primitive class C which may be called their product under composition. If the discriminants of C_1 and C_2 are $d_0s_1^2$ and $d_0s_2^2$, then the discriminant of C is d_0s^2 where $s = (s_1, s_2)$. Under composition the set of all primitive classes of discriminants in $\mathscr{D}$ form an abelian semigroup $\mathscr{S}$, which can be partitioned into subgroups consisting of the primitive classes of each discriminant in $\mathscr{D}$. The identities I_d in these subgroups are the only idempotents of $\mathscr{S}$.*

Proof. We will use two lemmas, the first easy and elementary.

LEMMA 2.2a. *The g.c.d. (a, b, c) of the coefficients of a form $ax^2+bxy+cy^2$ (which we write as $[a, b, c]$) is an invariant of its class, and is called the divisor of the class. If the divisors h_1 and h_2 of the classes K_1 and K_2*

of discriminant d are coprime, then the classes contain infinitely many united forms

$$(2.1)\qquad [a_1, b, a_2c] \text{ in } K_1, \quad [a_2, b, a_1c] \text{ in } K_2, \quad \text{with } a_1a_2 \neq 0.$$

LEMMA 2.2b. *For all such pairs of united forms the "product form"*

$$(2.2)\qquad [a_1a_2, b, c]$$

belongs to a unique class h_1h_2C, which has discriminant d and divisor h_1h_2.

Classical proofs of Lemma 2.2b use the Gauss Lemma (see [4], pp. 89, 136 or [13] (a)). Following a suggestion of our student, Carter Waid, we will deduce Lemma 2.2b from our method of forming the product of unit-classes in § 3; hence associativity is obvious.

To define the product C of primitive classes C_1, C_2, take $s_1, s_2 > 0$, set $(s_1, s_2) = s$, $s_1 = sk_1$, $s_2 = sk_2$; thus k_2C_1 and k_1C_2 have discriminant $d_0(sk_1k_2)^2$ and coprime divisors. By the lemma their product is k_2k_1C, with C primitive of discriminant d_0s^2.

The group properties (other than associativity) for the primitive classes of discriminant d are worth sketching. Since 1 can only be represented primitively, and any forms $[1, b, (b^2-d)/4]$ and $[1, b', (b'^2-d)/4]$ with $b \equiv b' \equiv d \pmod 2$ are obviously equivalent, there is only one class, I_d, which represents 1. Since

$$[1, b, ac][a, b, c] = [a, b, c], \qquad I_dC = C.$$

Since $[a, b, c]$ is primitive,

$$[a, b, c][c, b, a] = [ac, b, 1], \qquad \text{in } I_d.$$

Hence the inverse of the class of $[a, b, c]$ is that of $[c, b, a]$, hence that of $[a, -b, c]$.

Similarly the forms of discriminant d which represent -1 also constitute a unique class, say $-I_d$.

THEOREM 2.3. *Let $d' = dv^2$ $(v \geqslant 1)$. For any primitive class C of discriminant d, $I_{d'}C = C$; thus $I_{d'}$ acts as identity for primitive classes of discriminants dividing d'. If C contains $[a, b, c]$, then $(-I_d)C$ contains $[-a, b, -c]$.*

Proof. We have

$$[1, vb, v^2ac][va, vb, vc] = [va, vb, vc] = v[a, b, c],$$

and

$$[-1, vb, -v^2ac][va, vb, vc] = [-va, vb, -vc] = v[-a, b, -c].$$

THEOREM 2.4. *The mapping $C \to CI_d$ maps the group of primitive classes C of discriminant dv^2 homomorphically onto the group of primitive classes of discriminant d.*

Proof. Since $(1, v) = 1$, CI_d is primitive and of discriminant d. If H also has discriminant dv^2, $H \to HI_d$, $CH \to CHI_d = CI_dHI_d$, which proves the homomorphism into. We can suppose for the primitive form $[a, b, c]$ of discriminant d that $(a, 2v) = 1, v > 0$. Then $[a, bv, cv^2]$ is primitive and of discriminant dv^2, and

$$[a, bv, cv^2][v, vb, vac] = [va, vb, vc] = v[a, b, c].$$

Hence the map is onto.

THEOREM 2.5. *The class CI_d onto which a primitive class C of discriminant dv^2 is mapped can be characterized as the unique primitive class of discriminant d which can be carried into C by some integral transformation T of determinant $|v|$.*

Proof. We may take v positive. Any primitive form of discriminant dv^2 is equivalent to a form $[a, bv, cv^2]$ with $(a, 2v) = 1$. For the form represents an integer prime to $2v$ primitively, hence we can suppose $(a, 2v) = 1$, and then a translation will make the middle coefficient divisible by v. Thus the class of $[a, bv, cv^2]$ maps onto that of $[a, b, c]$, and evidently the latter form transforms into $[a, bv, cv^2]$ by replacing y by vy. If another form of discriminant d can be carried into $[a, bv, cv^2]$ by a transformation T of determinant v, an equivalent form will be so transformed by UT, U unimodular. By choice of U we can make

$$UT = \begin{bmatrix} v_1 & k \\ 0 & v_2 \end{bmatrix}, \qquad v = v_1v_2, \qquad v_1 > 0, \qquad v_2 > 0, \qquad 0 \leqslant k < v_2.$$

Thus $(UT)^{-1}$ must replace $[a, bv, cv^2]$ by an integral form g. In g the term in x^2 is $(a/v_1^2)x^2$. Hence $v_1 = 1$ and $v_2 = v$. The term $(b-2ak/v)xy$ shows that $k = 0$, or $k = \frac{1}{2}v$ (v even). But in the latter case the coefficient $a/4+b/2+c$ of y^2 is not integral. Hence $g = [a, b, c]$.

An examination of this proof gives a corollary:

COROLLARY 2.5.1. *If f and g are primitive, f in C, g in CI_d, and if T is the matrix of one transformation of determinant v carrying g into f, then every such transformation is expressed by WT, where W runs through the unimodular automorphs of g.*

By Theorem 2.1, if C_i is primitive of discriminant d_i $(i = 1, 2)$, then $C = C_1C_2$ has discriminant $d = (d_1, d_2)$. Also, $(I_dC_1)(I_dC_2) = C$, that is we can form the product of C_1 and C_2 by multiplying their images at the d-level. In particular $(-I_{d_1})(-I_{d_2}) = I_d$.

If we identify C with $(-I_d)C$ we obtain a semigroup $\mathscr{S}^*$. One may of course verify that the product of the pairs $\{(-I_{d_1})C_1, C_1\}$ and $\{(-I_{d_2})C_2, C_2\}$ is the pair $\{(-I_d)C, C\}$, where $C = C_1C_2$. We will show presently that $\mathscr{S}^*$ is isomorphic to the group of equivalence classes of two-dimensional modules in F_f.

3. The association between ordered pairs in F_j and binary quadratic forms. We consider only ordered pairs $\langle a_1, a_2\rangle$ of elements of F_j for which a_1, a_2 are linearly independent over Q. We define the *norm form of* $A = \langle a_1, a_2\rangle$ by

$$f_A = (xa_1+ya_2)(x\bar{a}_1+y\bar{a}_2) = a'x^2+b'xy+c'y^2. \tag{3.1}$$

The coefficients $a' = a_1\bar{a}_1$, $b' = a_1\bar{a}_2+a_2\bar{a}_1$, $c' = a_2\bar{a}_2$ are in Q. The norm form of $B = \langle 1, \sqrt{w}\rangle$ is x^2-wy^2. Since a_1 and a_2 are linear combinations of 1 and $\sqrt{w}$ with rational coefficients, we have:

LEMMA 3.1. *The norm form of any linearly independent ordered pair is in the rational class of* x^2-wy^2 *and so has a determinant* $-ws^2$ $(s \neq 0)$.

Proof. By a rational class we mean a set of forms obtained from one by nonsingular rational linear transformations. If, in the linear form xa_1+ya_2, we put $a_1 = \beta_1t_1+\beta_2t_3$ and $a_2 = \beta_1t_2+\beta_2t_4$, or in matrix notations

$$\langle a_1, a_2\rangle = \langle \beta_1, \beta_2\rangle T, \quad \text{where} \quad T = \begin{bmatrix} t_1 & t_2 \\ t_3 & t_4 \end{bmatrix}, \tag{3.2}$$

obviously f_A $(A = \langle a_1, a_2\rangle)$ is obtained from f_B $(B = \langle \beta_1, \beta_2\rangle)$ by replacing x and y by xt_1+yt_2 and xt_3+yt_4.

If d is nonsquare there are forms of determinant $-ws^2$ which are not norm forms; but any such can be transformed into $k(x^2-wy^2)$ for some nonzero rational k. Hence:

LEMMA 3.2. *If* g *is of determinant* $-ws^2$ $(s \neq 0)$, *and* k_1g *and* k_2g *are norm forms, then* k_1k *and* k_2k *are represented rationally by* x^2-wy^2, *and hence* $k_1/k_2 = N\gamma$ *for some* γ *in* F_j.

Removing a rational factor from a', b', c' in (3.1) we can write

$$f_A = l(ax^2+bxy+cy^2) \quad (l \text{ in } Q;\ a, b, c \text{ in } Z;\ (a, b, c) = 1) \tag{3.3}$$

and except that we can use $-l(-ax^2-bxy-cy^2)$ this expression is unique.

Writing $a_1 = a_1+a_1'j$, $a_2 = a_2+a_2'j$, we call $a_1a_2'-a_2a_1'$ the *determinant of* $\langle a_1, a_2\rangle$; and its sign ± 1 the *sign of* $\langle a_1, a_2\rangle$. We adopt the

CONVENTION. *l in* (3.3) *is to have the sign of* $\langle a_1, a_2\rangle$.

With this, the l and the primitive form $[a, b, c]$ in (3.3) become unique. We will call $[a, b, c]$ the *primitive norm form*, or *primitive norm, of* A; and may call $|l|$ the *norm of* A (cf. Corollary 4.7.2).

LEMMA 3.3. *The determinant of* $\langle \gamma a_1, \gamma a_2\rangle$ *is the product of* $N\gamma$ *and the determinant of* $\langle a_1, a_2\rangle$. *Hence if* $N\gamma \neq 0$, *the sign of* $\langle \gamma a_1, \gamma a_2\rangle$ *is the product of the signs of* $N\gamma$ *and* $\langle a_1, a_2\rangle$.

Proof. $(c_0+c_1j)(a_i+a_i'j) = (c_0a_i+wc_1a_i')+(c_0a_i'+c_1a_i)j$,

$$\begin{vmatrix} a_1c_0+wa_1'c_1 & a_1c_1+a_1'c_0 \\ a_2c_0+wa_2'c_1 & a_2c_1+a_2'c_0 \end{vmatrix} = \begin{vmatrix} a_1 & a_1' \\ a_2 & a_2' \end{vmatrix} \begin{vmatrix} c_0 & c_1 \\ wc_1 & c_0 \end{vmatrix}.$$

COROLLARY 3.3.1. *If* $N\gamma \neq 0$, A *and* γA *have the same primitive norm.*

DEFINITION. A *unit-class* is a set of ordered pairs obtained from one such $\langle a_1, a_2\rangle$ by unimodular transformations and multiplication by elements of F_j of nonzero norm; i.e., a set

$$\{\gamma\langle a_1, a_2\rangle T |\ \gamma \text{ such that } N\gamma \neq 0,\ T \text{ integral, } t_1t_4-t_2t_3 = +1\}.$$

COROLLARY 3.3.2. *A unit-class yields a unique class of primitive norms.*

THEOREM 3.4. *All ordered pairs with a given primitive norm* $[a, b, c]$ *are given by* $\langle \gamma a_1, \gamma a_2\rangle$ $(N\gamma \neq 0)$, *where* $\langle a_1, a_2\rangle$ *is one such pair.*

Proof. We can assume that $a \neq 0$. Consider

$$\begin{aligned} N(xa_1+ya_2) &= k_1(ax^2+bxy+cy^2), \\ N(x\beta_1+y\beta_2) &= k_2(ax^2+bxy+cy^2), \end{aligned} \tag{3.4}$$

k_1 having the sign of $\langle a_1, a_2\rangle$, k_2 that of $\langle \beta_1, \beta_2\rangle$. By Lemma 3.2 we may put $k_2/k_1 = N\delta$. Hence $N(x\delta a_1+y\delta a_2) = k_2(ax^2+bxy+cy^2)$, and $\langle \delta a_1, \delta a_2\rangle$ and $\langle \beta_1, \beta_2\rangle$ have the sign of k_2. Set $\sigma = a_2/a_1$, $\tau = \beta_2/\beta_1$. Since $N(\delta a_1) = N(\beta_1) = k_2a$, $\langle 1, \sigma\rangle$ and $\langle 1, \tau\rangle$ have the same sign. Also, $(x+\sigma y)(x+\bar{\sigma}y) = (x+\tau y)(x+\bar{\tau}y)$. It follows easily (put $\sigma = s_0+s_1j$, etc.) that $\sigma = \tau$ or $\bar{\tau}$. But $\langle 1, \tau\rangle$ and $\langle 1, \bar{\tau}\rangle$ have opposite signs. Hence $\sigma = \tau$. Thus β_1/a_1 and β_2/a_2 have a common value γ, $\beta_i = \gamma a_i$ $(i = 1, 2)$.

Further, if $a \neq 0$, the primitive form $[a, b, c]$ of discriminant d arises from $A = \langle a, (b-\varepsilon)/2+\omega\rangle$. Hence:

THEOREM 3.5. *With our sign convention the procedure in* (3.3) *sets up a bi-unique association between unit-classes of ordered pairs and classes of primitive forms.*

The term *module*, unless otherwise indicated will denote a two-dimensional Z-module

$$M = [\beta_1, \beta_2] = \{x_1\beta_1+x_2\beta_2|\ x_1, x_2 \text{ in } Z\}. \tag{3.5}$$

The various bases of M are obtained from any one of them by unit-modular transformations, i.e., by integral transformations of determinant ± 1.

A class of modules consists of all modules obtained from one by multiplication by elements of F_j of nonzero norm. Thus the various bases in a module class appear to be distributable into two unit-classes; if one is generated from $\langle a_1, a_2\rangle$ the other arises from $\langle a_1, -a_2\rangle$. Can these unit-classes coincide? For this to occur it is clearly necessary and suffi-

cient that there shall exist an element γ of F_j of nonzero norm, and an integral matrix T of determinant -1, such that

$$\langle a_1, a_2\rangle T = \gamma\langle a_1, a_2\rangle. \tag{3.6}$$

The question will be answered in Corollary 3.7.1.

The bases of positive sign in a module M form a set which we may denote by M^+, and those of negative sign by M^-. Hence $\gamma(M^+) = (\gamma M)^+$ or $(\gamma M)^-$ according as $N\gamma$ is positive or negative; similarly for $\gamma(M^-)$.

If $\langle a_1, a_2\rangle$ gives $[a, b, c]$, $\langle a_1, -a_2\rangle$ gives $[-a, b, -c]$. Hence if M^+ gives the class of $[a, b, c]$, M^- gives the class $(-I_d)C$ of $[-a, b, -c]$.

The product MN of the modules $M = [a_1, a_2]$ and $N = [\beta_1, \beta_2]$ is the module P generated from $a_1\beta_1, a_1\beta_2, a_2\beta_1, a_2\beta_2$; and can (cf. next paragraph) be given a two-term basis. Clearly the product is independent of the choice of Z-bases of M and N; and if M or N is multiplied by γ so is P. Thus module multiplication extends to their classes. We also define products of unit-classes by proceeding according to the rule of signs:

$$M^+N^+ = P^+ = M^-N^-, \quad M^+N^- = P^- = M^-N^+. \tag{3.7}$$

Evidently this is consistent with multiplication by γ, and with multiplication of module classes.

In fact, an elegant way of forming the product of two unit-classes is by means of united forms (Lemma 2.2a). Suppose that the classes of the associated primitive norms are C_1 and C_2 with discriminants $d_0s_1^2$ and $d_0s_2^2$. As in Lemma 2.2a we choose in k_2C_1 and k_1C_2 united forms $[a_1, b, a_2c]$ and $[a_2, b, a_1c]$, where since the divisors are coprime, $(a_1, b, a_2) = 1$. Consider the ordered pairs

$$A_1 = \langle a_1, r+\omega\rangle, \quad A_2 = \langle a_2, r+\omega\rangle, \quad A_3 = \langle a_1a_2, r+\omega\rangle, \tag{3.8}$$

where $b = 2r+\varepsilon$, $d = b^2-4a_1a_2c$, $\omega = \omega_d$, hence $N(r+\omega) = a_1a_2c$. Thus A_i is in the unit-class associated with C_i $(i = 1, 2)$. Since

$$(r+\omega)^2 = b(r+\omega) - N(r+\omega) \tag{3.9}$$

and $(a_1, a_2, b) = 1$, $r+\omega$ is in the product of the modules $[a_1, r+\omega]$, $[a_2, r+\omega]$, hence this product is $[a_1a_2, r+\omega]$, and so A_3 determines the unit-class which is the product of the unit-classes of A_1 and A_2. The primitive norm of A_3 is the quotient by k_1k_2 of $[a_1a_2, b, c]$. This proves Lemma 2.2b and also

THEOREM 3.6. *The system of unit-classes over F_j under multiplication is isomorphic to the semigroup $\mathcal{S}$. The system of module classes under multiplication is isomorphic to the semigroup $\mathcal{S}^*$ obtained from $\mathcal{S}$ by identifying each primitive class C of discriminant d with its "negative" $(-I_d)C$.*

Three obvious remarks are useful at this point:

(3.10) If the elements α_1 and α_2, β_1 and β_2, of F_j are linearly independent over Q, then there is a unique nonsingular rational matrix T satisfying (3.2);

(3.11) $[\alpha_1, \alpha_2] \subset [\beta_1, \beta_2]$ if and only if $\langle\beta_1, \beta_2\rangle T = \langle\alpha_1, \alpha_2\rangle$ for some integral matrix T of nonzero determinant;

(3.12) For given nonzero discriminant d, each element γ of F_j is uniquely expressible as $(t+u\sqrt{d})/2$, t and u in Q. Here γ is in R_d if and only if t and u are integers such that $t \equiv du \pmod 2$.

THEOREM 3.7. *Assume α_1, α_2 linearly independent over Q, and let $[a, b, c]$ be the primitive norm of $\langle\alpha_1, \alpha_2\rangle$, $d = b^2-4ac$. Let $\gamma = (t+u\sqrt{d})/2$, t, u in Q, $N\gamma \neq 0$. Then*

$$T_\gamma = \begin{bmatrix} (t-bu)/2 & -cu \\ au & (t+bu)/2 \end{bmatrix} \tag{3.13}$$

is the unique rational matrix T satisfying (3.6). Also, T_γ is integral if and only if γ is in R_d. Also, $|T_\gamma| = N\gamma$.

Proof. Obviously T_γ is integral if $\gamma \in R_d$. If T_γ is integral, then since $(a, b, c) = 1, t, au, bu, cu$, hence u, and $(t-du)/2$ are integral. Since l in (3.3) has the sign of $\langle\alpha_1, \alpha_2\rangle$, and

$$(a_1\bar{a}_2 - a_2\bar{a}_1)^2 = (a_1\bar{a}_2 + a_2\bar{a}_1)^2 - 4a_1\bar{a}_1a_2\bar{a}_2 = l^2d,$$

we have $\bar{a}_1a_2 - \bar{a}_2a_1 = l\sqrt{d}$. Also, $\bar{a}_1a_2 + \bar{a}_2a_1 = lb$. Hence

$$\bar{a}_1a_2 = l(b+\sqrt{d})/2, \quad \bar{a}_2a_1 = l(b-\sqrt{d})/2,$$

and so

$$aa_2 = a_1(b+\sqrt{d})/2, \quad a_1(t-bu)/2 + a_2au = a_1(t+u\sqrt{d})/2 = a_1\gamma;$$

similarly,

$$-a_1cu + a_2(t+bu)/2 = a_2\gamma.$$

If in (3.6) T is to be integral and to have determinant -1, γ must be in R_d and $N\gamma$ must be -1. Hence

COROLLARY 3.7.1. *The two unit-classes into which the bases of the module class determined by $\langle\alpha_1, \alpha_2\rangle$ subdivide coincide if and only if there is a unit of norm -1 in R_d. Here d denotes the discriminant of the primitive norm of $\langle\alpha_1, \alpha_2\rangle$.*

COROLLARY 3.7.2. *$[\alpha_1, \alpha_2] = \gamma[\alpha_1, \alpha_2]$ if and only if γ is a unit in R_d of norm ± 1.*

COROLLARY 3.7.3. *$\gamma[\alpha_1, \alpha_2] \subset [\alpha_1, \alpha_2]$ if and only if γ is in R_d.*

Under what condition is $[a_1, a_2] = [\bar{a}_1, \bar{a}_2]$? Then $[a_1, -a_2]$ and $[\bar{a}_1, \bar{a}_2]$ have the same sign. Hence the primitive norms $[-a, b, -c]$ and $[-a, -b, -c]$ are in the same class. Hence $[a, -b, c]$ and $[a, b, c]$ are in the same class K. Thus $K^2 = I_d$ or $K = K^{-1}$.

Dr. Olga Taussky-Todd drew our attention to § 76 of Hilbert's "Die Theorie der algebraischen Zahlkorper", where Hilbert counts classes which are self-inverse and yet do not contain an ambiguous ideal (which Hilbert defines as a self-conjugate ideal). In the Gaussian theory, which Hilbert used as a model in his study of ideals in quadratic fields, an ambiguous form-class is characterized as containing an ambiguous form (a form $[a, b, c]$ in which $a|b$). The explanation of the apparent paradox is that Hilbert in effect identified a class C with $(-I)C$, and so his self-inverse classes K in a sense may satisfy $K^2 = -I$ rather than $K^2 = I$. The Gaussian theory is here simpler.

We mention what happens in one case where the coefficients a, b, c are taken in some other ring than Z. If the coefficient ring is $Q[t]$ (polynomials in t with rational coefficients), the module classes correspond to the system of classes of forms $[ka, b, c/k]$, where k may be any squarefree integer.

4. Ideals, or fractional ideals, in the various orders R_d. For our purposes we may think of a *fractional ideal in R_d* as the product of a two-dimensional ideal in R_d by an element of F_f of nonzero norm, or as a two-dimensional Z-module closed under multiplication by R_d. Evidently,

LEMMA 4.1. *The fractional ideal $[\alpha_1, \alpha_2]$ in R_d is an ideal in R_d if and only if α_1 and α_2 are in R_d.*

Any two-dimensional Z-module M can be written as $k[\alpha_1, \alpha_2]$, where α_1 and α_2 are in R_d, and k is in Q. Hence M can be given a Z-basis $k[m, r+s\omega]$, where $\omega = \omega_d$, m and s are positive integers, and r is an integer. In the Z-module $[m, r+s\omega]$,

(4.1) $\left\{\begin{array}{l} s \text{ is the least positive integer coefficient of } \omega \text{ among the elements} \\ \text{of the module; } m \text{ is the least positive integer in the module; } r \text{ is} \\ \text{unique mod } m. \end{array}\right.$

Moving a factor into k if necessary, we can suppose that $(m, r, s) = 1$.

THEOREM 4.2. *The module $[m, r+s\omega]$, with $(m, r, s) = 1$, is an ideal in R_d if and only if*

(4.2) $$s = 1 \quad \text{and} \quad m \mid N(r+\omega) \ (= r^2 + \varepsilon r + \tfrac{1}{4}(\varepsilon - d)).$$

Proof. If $[m, r+s\omega]$ is an ideal in $[1, \omega]$, it contains $r+s\omega$, $m\omega$, $\omega(r+s\omega) = (r+s\varepsilon)\omega - \frac{1}{4}s(\varepsilon - d)$, with the three coefficients of ω coprime. Hence $s = 1$. Since the module contains $(r+\overline{\omega})(r+\omega)$, $m \mid N(r+\omega)$. Conversely, if (4.2) holds, $[m, r+\omega]$ contains $m\omega = m(r+\omega) - rm$ and $(r+\omega)\omega = (r+\omega)(-r-\overline{\omega}) + (r+\omega)(r+\varepsilon)$. Hence the module is an ideal in $[1, \omega]$.

COROLLARY 4.2.1. *The ideals in R_d can be characterized as having a module basis $k[m, r+\omega]$, where k and m are positive integers and $m \mid N(r+\omega)$.*

The discriminant d of the primitive norm of a Z-basis of a module M will be called the *discriminant of the module*, and denoted by $\partial(M)$. From Theorems 2.1 and 3.6 follows that if P is the product of the modules M, N then $\partial(P) = (\partial(M), \partial(N))$.

THEOREM 4.3. *A module M in F_f is a fractional ideal in the order $R_{d'}$ if and only if d'/d is an integer, where $d = \partial(M)$.*

Proof. Multiplying by a rational factor we can suppose $M = [m, r+s\omega']$ with $(m, r, s) = 1$, $\omega' = (\varepsilon' + \sqrt{d'})/2$. Set $B = \langle m, r+s\omega' \rangle$.

Assume M is a fractional ideal in $R_{d'}$. Then $[m, r+s\omega']$ is an ideal there. By Theorem 4.2, $s = 1$ and $N(r+\omega') = mc'$, c' in Z. Thus $f_B = N(xm + y(r+\omega')) = mf'$, where $f' = mx^2 + (2r+\varepsilon')xy + c'y^2$ is an integral form of discriminant d'. Since $d = \partial(M)$ and f' must be an integral multiple uf of the primitive norm f of B, $d' = du^2$.

Suppose conversely that d'/d is a square. By definition of $\partial(M)$ and the primitive norm of B, we can write f_B as

$$t(a'x^2 + b'xy + c'y^2), \quad \text{with } t \text{ in } Q;\ a', b', c' \text{ in } Z;\ d' = b'^2 - 4a'c'.$$

Hence

(4.3) $$m^2x^2 + m(2r+\varepsilon')xy + N(r+s\omega')y^2 = t(a'x^2 + b'xy + c'y^2).$$

But B is obtained from $\langle 1, \omega' \rangle$ by an integral transformation of determinant ms. Hence the same transformation carries $x^2 + \varepsilon' xy + \frac{1}{4}(\varepsilon'^2 - d')y^2$ into f_B. Equating discriminants in (4.3) gives $d'(ms)^2 = t^2 d'$. Hence $t = \pm ms$, and t is an integer; and ms divides the three coefficients m^2, $m(2r+\varepsilon')$, $N(r+s\omega')$; and $s \mid (m, r^2)$. Since $(m, r, s) = 1$, $s = 1$. Hence $m \mid N(r+\omega')$ and $[m, r+s\omega']$ is an ideal in $R_{d'}$.

COROLLARY 4.3.1. *If $d = \partial(M)$, R_d is the largest order within which M is a fractional ideal; and M is a fractional ideal in $R_{d'}$ if and only if $d \mid d'$, or $R_{d'} \subset R_d$.*

If $\partial(M) = d_1$ and $d \mid d_1$, one can find a module N such that $MN = R_d$ by considering the corresponding problem for primitive forms.

A fractional ideal M in $R_{d'}$ is said to be *invertible in $R_{d'}$* if there exists a fractional ideal N in $R_{d'}$ such that $MN = R_{d'}$. If $d = \partial(M)$, then $d \mid d'$ by Theorem 4.3, and $d' \mid d$ since $\partial(R_{d'}) = (\partial(M), \partial(N))$. Hence $\partial(M) = \partial(N) = d'$.

THEOREM 4.4. *A module M is an invertible fractional ideal only in the order R_d where $d = \partial(M)$.*

For any module M, $MR_{d'}$ is obviously a fractional ideal in $R_{d'}$.

If $d \mid d'$ and M is a fractional ideal in R_d, then

$$MR_{d'} = (MR_d)R_{d'} = M(R_dR_{d'}) = MR_d = M. \tag{4.4}$$

THEOREM 4.5. *Let $d \mid d'$. The function φ which maps each fractional ideal M' in $R_{d'}$ on the "extended" fractional ideal $M'R_d$ in R_d is a homomorphism from the semigroup S'_0 of fractional ideals in $R_{d'}$ onto the semigroup S_0 of fractional ideals in R_d.*

Proof. $(M'R_d)(N'R_d) = (M'N')(R_dR_d) = (M'N')R_d$ for any two fractional ideals M', N' in $R_{d'}$. The map is onto: for if A is in S_0, $AR_{d'}$ is in S'_0 and $(AR_{d'})R_d = A$.

THEOREM 4.6. *The ideal $A = [m, r+\omega]$ in R_d is invertible in R_d if and only if $A\bar{A} = mR_d$.*

Proof. The form $mx^2+(2r+\varepsilon)xy+y^2N(r+\omega)/m$ is primitive if and only if

$$\begin{aligned}[m, r+\omega][m, r+\bar{\omega}] &= [m^2, m(r+\omega), m(r+\bar{\omega}), N(r+\omega)] \\ &= [m^2, m(2r+\varepsilon), N(r+\omega), m(r+\omega)] \\ &= m[1, r+\omega] = mR_d.\end{aligned}$$

THEOREM 4.7. *Let $A_i = [m_i, r_i+\omega_i]$ be invertible ideals in R_{d_i} $(i = 1, 2)$. Write $A = A_1A_2 = k[m, r+\omega]$, $\omega = \omega_d$, $d = (d_1, d_2)$. Then $m_1m_2 = k^2m$.*

Proof. $R_{d_1}R_{d_2} = R_d$; $\bar{A}_1\bar{A}_2 = \bar{A}$, $m_1R_{d_1}m_2R_{d_2} = k^2mR_d$, $m_1m_2 = k^2m$.

We define the norm of the module M to be h^2m, where $M = h[m, r+\omega]$, h rational, $\omega = \omega_d$, $d = \partial(M)$. If h is an integer, h^2m is the number of residue classes mod M in the ring R_d.

COROLLARY 4.7.1. *For any modules M, N in F_f, the norm of MN is the product of the norms of M and N.*

COROLLARY 4.7.2. *In* (3.3), *the number $|l|$ is the norm of $[\alpha_1, \alpha_2]$.*

5. The relation between invertible fractional ideals in R_d and $R_{d'}$, $d' = dn^2$ $(n > 0)$. Let $R = R_d = [1, \omega]$, $R' = R_{d'} = [1, \omega']$; and let S, S' denote their respective groups of invertible fractional ideals under multiplication. We will study the function φ: $S' \to S$ defined by $\varphi(A') = A'R$ for A' in S'.

An ideal $k[m, r+\omega]$ is *invertible in R* if and only if the form $[m, 2r+\varepsilon, N(r+\omega)/m]$ is primitive. Since $d = (2r+\varepsilon)^2-4N(r+\omega)$, the last condition can be replaced by

$$(m, d, N(r+\omega)/m) = 1. \tag{5.1}$$

We will study the relationship $A = A'R$ where A' is invertible in R'. By multiplying by a nonzero rational number we can assume that

$$A = [m, r+\omega], \quad m > 0,\ m \mid N(r+\omega),\ (m, d, N(r+\omega)/m) = 1; \tag{5.2}$$

$$A' = k[m', r'+\omega'], \tag{5.3}$$

$$m' > 0,\ m' \mid N(r'+\omega'),\ (m', d', N(r'+\omega')/m') = 1;$$

$$k[m', r'+\omega'][1, \omega] = [m, r+\omega], \quad k \text{ rational}. \tag{5.4}$$

LEMMA 5.1. *If $A' = [a, r'+\omega']$ is an invertible ideal in R', an integer s exists such that $r'+\omega' = s+n\omega$, and*

$$A'R = e[a/e^2, r+\omega], \tag{5.5}$$

where $e = (a, s, n)$ and r is defined by

$$n'r \equiv s' \pmod{a/e^2}. \tag{5.6}$$

Here $s' = s/e$, $n' = n/e$, and a/e^2 is an integer.

Proof. Since $\omega' = n\omega+(\varepsilon'-n\varepsilon)/2$, $r'+\omega' = s+n\omega$ with s an integer. Hence

$$A'[1, \omega] = e[a', s'+n'\omega, a'\omega, -n'\omega\bar{\omega}+(s'+n'\varepsilon)\omega], \tag{5.7}$$

where $a' = a/e$, $\omega\bar{\omega} = (\varepsilon-d)/4$. Since $(n', a', s'+n'\varepsilon) = 1$, we have

$$1 = v_1n'+v_2a'+v_3(s'+n'\varepsilon) \tag{5.8}$$

for certain integers v_1, v_2, v_3. Hence $A'[1, \omega] = e[m, r+\omega]$, where

$$r = v_1s'-v_3n'(\varepsilon-d)/4 \tag{5.9}$$

and m is the g.c.d. of the four numbers a', $s'+n'\omega-n'(r+\omega)$, $a'\omega-a'(r+\omega)$, $u'+t'\omega-t'(r+\omega)$, where $u' = -n'(\varepsilon-d)/4$ and $t' = s'+n'\varepsilon$. By (5.8) and (5.9),

$$\begin{aligned}s'-n'r &= v_2a's'+v_3N(s'+n'\omega), \\ u'-t'r &= -v_2a'n'(\varepsilon-d)/4-v_1N(s'+n'\omega).\end{aligned} \tag{5.10}$$

For any prime p in e denote the precise exponent in a, e by α, β. Since A' is invertible,

$$p^\alpha \| e^2N(s'+n'\omega), \quad \alpha \geqslant 2\beta, \quad p^{\alpha-2\beta} \| N(s'+n'\omega), \quad p^{\alpha-\beta} \mid a'.$$

Thus $\alpha > \beta$, $p \nmid (v_1, v_3)$ by (5.8). Hence by (5.10), $p^{\alpha-2\beta}$ is the precise power of p in $(s'-n'r, u'-t'r)$. Thus $m = a/e^2$ and (5.6) follows from $(5.10)_1$.

THEOREM 5.1. *If A' in* (5.3) *is an invertible fractional ideal in R' and $A = [m, r+\omega]$ is an invertible ideal in R such that $A = A'R$, then there exists a matrix H such that*

$$k\langle m', r'+\omega'\rangle = \langle m, r+\omega\rangle H, \qquad H = \begin{bmatrix} e & h \\ 0 & n_1 \end{bmatrix}, \tag{5.11}$$

where e, h, n_1 are integers such that $n = en_1$, $e > 0$, $n_1 > 0$, $0 \leqslant h < e$. Conversely, if A is an invertible ideal in R and A' is an invertible fractional ideal in R' obtained from (5.11), *then $A = A'R$.*

Proof. As in Lemma 5.1 we can write $r'+\omega' = s+n\omega$, $e = (m', s, n)$, and define t by $nt \equiv s \pmod{m'/e}$, $k[m', r'+\omega']R = ke[m'/e^2, t+\omega]$. Hence $A = A'R$ reduces to

$$k = 1/e, \qquad m = m'/e^2, \qquad r \equiv t \pmod m. \tag{5.12}$$

Thus if $A = A'R$, then $A' = [me, s_1+n_1\omega]$ where $n = en_1$ and $s = es_1$, and since $A' \subset A$ there is an integer h such that $s_1+n_1\omega = mh+(r+\omega)n_1$. We can adjust the mh modulo me, and suppose $0 \leqslant h < e$. Thus (5.11) follows. The converse follows from Lemma 5.1.

Remarks. The matrix H in (5.11) is a canonical "Hermite matrix": any integral matrix N of determinant n and order 2 can, by multiplying on the right by unimodular matrices U, be carried into a unique H. We can of course also multiply both A and A' by a nonzero rational factor. Two corollaries result, the first being merely a reformulation of Theorem 5.1.

COROLLARY 5.1.1. *Consider invertible fractional ideals, $A = [a_1, a_2]$ in R, $A' = [a_1', a_2']$ in R'. Then $A = A'R$ if and only if for some integral matrix N of determinant $\pm n$,*

$$\langle a_1', a_2'\rangle = \langle a_1, a_2\rangle N.$$

COROLLARY 5.1.2. *Let $\langle a_1, a_2\rangle$ and $\langle \beta_1, \beta_2\rangle$ both have discriminant d, and let both of $\langle a_1, a_2\rangle T_1$ and $\langle \beta_1, \beta_2\rangle T_2$ have discriminant dn^2, where T_1 and T_2 are integral matrices of determinant n or $-n$. Then $\langle a_1, a_2\rangle T_1 = \langle \beta_1, \beta_2\rangle T_2$ requires that $[a_1, a_2]$ and $[\beta_1, \beta_2]$ be the same module.*

THEOREM 5.2. *If $d' = dn^2$ and $n = p_1^{k_1} \dots p_u^{k_u}$ in powers of distinct primes, then the number of invertible fractional ideals A' in R' such that $A'R = R$ is*

$$\varkappa = \prod_{i=1}^{u} p_i^{k_i-1}\{p_i-(d|p_i)\}. \tag{5.13}$$

Proof. We take $A = R$ in Theorem 5.1, and need only count the number of pairs e, h such that $e|n$ and $0 \leqslant h < e$, and (with $n_1 = n/e$) $[e, h+n_1\omega]$ is an invertible fractional ideal in R'. By (5.1) the condition for the last is $(e^2, dn^2, N(h+n_1\omega)) = 1$, or since $e|n$,

$$h^2+\varepsilon n_1 h+\tfrac{1}{4}(\varepsilon-d)n_1^2 \text{ is prime to } e. \tag{5.14}$$

For each q $(= 1, \dots, k_i+1)$, the qth term of the expression

$$E_i = 1+(p_i-1)+p_i(p_i-1)+\dots+p_i^{k_i-2}(p_i-1)+p_i^{k_i-1}\{p_i-(d|p_i)-1\},$$

gives the number of residues $h \pmod{p_i^{q-1}}$ for which (5.14) holds with $e = p_i^q$, $i = 1, \dots, u$. In the distributed product of the u factors, each choice of one term from each factor corresponds to a divisor e of n, and for that e the product of the corresponding terms is the number of residues h modulo e which satisfy (5.14). Hence (5.13) follows.

THEOREM 5.3. *The function φ is a homomorphism of S' onto S.*

Proof. If A_1' and A_2' are invertible fractional ideals in R', then $A_1'A_2'$ is an invertible fractional ideal in R', and $A_1'R$ is an invertible fractional ideal in R. By Lemma 4.5, φ is a homomorphism from S' into S. To prove that φ is onto, consider an invertible ideal $A = [m, r+\omega]$ in R. The primitive norm of A is $f = [m, 2r+\varepsilon, N(r+\omega)/m]$ and has discriminant d. The class of f contains a form $[a, b, c]$ with $(a, n) = 1$. The ideal $B = [a, \frac{1}{2}(b-\varepsilon)+\omega]$ has $[a, b, c]$ as its primitive norm, hence by Theorem 3.6, $A = \gamma B$ with γ in F_f. The form $[a, nb, n^2c]$ is also primitive of discriminant dn^2, and the corresponding fractional ideal $[a, n(r+\omega)]$ is invertible in R' and maps onto A.

COROLLARY 5.3.1. *If A is an invertible fractional ideal in R, then the number of invertible fractional ideals A' in R' such that $A'R = A$ is given by* (5.13).

Proof. This is the number of elements in the kernel of the group homomorphism φ.

We defined two fractional ideals A, B of the order R to be equivalent if there is an element γ in F_f of nonzero norm such that $A = \gamma B$. This equivalence relation partitions S, S' into collections H, H' respectively of equivalence classes; and H, H' are abelian groups under the natural operations determined by multiplication. Define a function Φ: $H' \to H$ as follows. If A' is a fractional ideal in a class Γ' of H' and $\varphi(A')$ is in the class Γ of H, set $\Phi(\Gamma') = \Gamma$. Clearly Φ is a homomorphism from H' onto H.

THEOREM 5.4. *Let G, G' denote the groups of units in R, R' respectively, and let σ be the index of G' in G. Then σ is finite, $\sigma|\varkappa$, and the kernel of Φ contains exactly $\varkappa/\sigma$ elements.*

Proof. The kernel of Φ consists of elements of H containing an invertible fractional ideal A' such that $\varphi(A') = R$. Since there are only $\varkappa$ such fractional ideals A', the kernel of Φ contains at most $\varkappa$ elements.

If A' and B' are in the same equivalence class and their images are equal, then $\varphi(A') = \varphi(B')$ and $A' = \gamma B'$ for some γ of nonzero norm in F_j. Then also $B'R = \gamma B'R$, $R = \gamma R$, hence γ is in R. Since $B' = \gamma^{-1}A'$, similarly γ^{-1} is in R, hence γ is in G. Conversely, if γ is in G and B' is in S', then $\varphi(\gamma B') = \varphi(B')$.

Further, $\gamma_1 B' = \gamma_2 B'$ with γ_1 and γ_2 in G if and only if $\gamma_1 R' = \gamma_2 R'$ (since $B'C' = R'$ for a certain C' in S'). Hence $\gamma_1 B' = \gamma_2 B'$ if and only if $\gamma_2^{-1}\gamma_1$ and $\gamma_1^{-1}\gamma_2$ are both in R', i.e. $\gamma_2^{-1}\gamma_1$ is a unit in R'. Thus, $\gamma_1 B' = \gamma_2 B'$ if and only if γ_1 and γ_2 are in the same coset of G modulo G'.

Let A_i' $(i = 1, \ldots, t)$ be representatives of the distinct elements of H' forming the kernel of Φ such that $\varphi(A_i') = R$ $(i = 1, \ldots, t)$. If $G = \bigcup_\alpha \theta_\alpha G'$ is the coset decomposition of G modulo G', then the ideals $\theta_\alpha A_i'$ are distinct and $\varphi(\theta_\alpha A_i') = R$. It follows that the index σ of G' in G is finite and that $\varkappa = \sigma l$.

COROLLARY 5.4.1. *If h and h' denote the orders of H and H' respectively, then $\varkappa h = \sigma h'$.*

6. Transformations of binary quadratic forms.

THEOREM 6.1. *Let f and g be primitive binary quadratic forms of nonzero discriminants d, dv^2 respectively, $v > 0$; A and B their matrices. Let e be a nonzero integer. We will give an algorithm by which each integral matrix T such that*

$$T'AT = eB \tag{6.1}$$

is associated one-to-one with each integral representation of e by a form in the class KL^{-1} if $\det T = ev$, and by a form in KL if $\det T = -ev$. Here K is the class of f, L that of g.

Remarks. 1. By Theorem 2.5 we may take L to be the class of discriminant d which can be transformed into g by an integral transformation of determinant v. 2. If d is nonsquare the theorem also holds with $e = 0$; for, if d is nonsquare, 0 is only represented with both variables 0, and $T = 0$ is the only solution of (6.1) with $e = 0$.

Proof. The problem is not changed if we replace f, g by equivalent forms. Hence we can assume $ac' \neq 0$, $(c', 2avd) = 1$, $f = [a, b, c]$, $g = [a', b', c']$. If $t_1, \ldots, t_4$ are the elements of T in the usual order, (6.1) expands as follows:

$$\begin{aligned} ea' &= at_1^2 + bt_1t_3 + ct_3^2, \quad ec' = at_2^2 + bt_2t_4 + ct_4^2, \\ eb' &= 2at_1t_2 + b(t_1t_4 + t_2t_3) + 2ct_3t_4. \end{aligned} \tag{6.2}$$

Taking determinants, (6.1) gives $t_1t_4 - t_2t_3 = \pm ev$.

We construct from the columns of T the two elements

$$a_1 = t_1a + t_3(r+\omega), \quad a_2 = t_2a + t_4(r+\omega), \tag{6.3}$$

of the ideal $[a, r+\omega]$, where $r+\omega = \frac{1}{2}(b+\sqrt{d})$. Hence:

$$Na_1 = a(at_1^2 + bt_1t_3 + ct_3^2), \quad Na_2 = a(at_2^2 + bt_2t_4 + ct_4^2), \tag{6.4}$$

$$a_1\bar{a}_2 + a_2\bar{a}_1 = a\{2at_1t_2 + b(t_1t_4 + t_2t_3) + 2ct_3t_4\}, \tag{6.5}$$

$$a_1\bar{a}_2 - a_2\bar{a}_1 = -a\sqrt{d}(t_1t_4 - t_2t_3). \tag{6.6}$$

Hence if $\det T = ev$, (6.1) implies the "factorization"

$$ea\tfrac{1}{2}(b' - v\sqrt{d}) = a_1\bar{a}_2, \quad Na_1 = eaa', \quad Na_2 = eac'; \tag{6.7}$$

and if $\det T = -ev$, the same with v replaced by $-v$. Note that $(6.7)_1$ implies that $ea\frac{1}{2}(b' + v\sqrt{d}) = a_2\bar{a}_1$. Hence if a_1, a_2 are elements of $[a, r+\omega]$ satisfying (6.7), and $t_1, \ldots, t_4$ are defined by (6.3), then T is an integral matrix of determinant ev satisfying (6.1).

Each pair a_1, a_2 satisfying (6.7) is associated one-to-one with each a_2 in $[a, r+\omega]$ satisfying

$$(1/c')a_2(b' - v\sqrt{d})/2 \text{ is in } [a, r+\omega], \quad Na_2 = eac'. \tag{6.8}$$

For if $a_1 = (1/c')a_2(b' - v\sqrt{d})/2$, $Na_1 = eaa'$. Further,

$$\big(t_2a + t_4(r+\omega)\big)(b' - v\sqrt{d})/2 = aE_1 + (r+\omega)E_2, \tag{6.9}$$

where

$$E_1 = t_2(b' + vb)/2 + t_4cv, \quad E_2 = -t_2av + t_4(b' - vb)/2.$$

Here $avE_1 + \frac{1}{2}(b' + vb)E_2 = a'c't_4$. Hence both E_1 and E_2 will be divisible by c' if E_2 is. Thus (6.8) reduces to

$$t_2(-av) + t_4(b' - vb)/2 \equiv 0 \pmod{c'}, \tag{6.10}$$

$$at_2^2 + bt_2t_4 + ct_4^2 = ec'. \tag{6.11}$$

We can choose an integer i such that

$$avi \equiv \tfrac{1}{2}(b' - vb) \pmod{c'}, \quad \text{or} \quad v(2ai + b) \equiv b' \pmod{2c'}. \tag{6.12}$$

Thus (6.10) reduces to $t_2 \equiv it_4 \pmod{c'}$, or to

$$t_2 = c'x + iy, \quad t_4 = y, \quad \text{with } x \text{ and } y \text{ integral}; \tag{6.13}$$

and (6.11) then becomes

$$ac'x^2 + (2ai + b)xy + sy^2 = e, \tag{6.14}$$

where s (cf. (6.12)) is the integer determined by $c's = ai^2 + bi + c$, or by $d = (2ai + b)^2 - 4sc'a$. From this follows easily that the forms $f_1 = [a, 2ai + b, c's]$ and $f_2 = [c', 2ai + b, as]$ are primitive and of discrim-

inant d, and have the compound $[ac', 2ai+b, s]$. Evidently f_1 is in K, and f_2 is carried by a transformation of determinant v into $[c', v(2ai+b), sv^2]$ in the class of $[c', b', a']$, or L^{-1}. Changing v to $-v$ gives the result for $\det T = -ev$.

Since the number of solutions x, y of (6.14) can be infinite, when d is positive but not square, but the number of "automorphic sets" obtained by grouping solutions derived from one another by unimodular automorphs of the form is always finite, it is of interest to note:

THEOREM 6.2. *The bi-uniqueness of the association in Theorem* 6.1 *extends to automorphic sets.*

Proof. As is well known there is one unimodular automorph

$$W = \begin{bmatrix} \frac{1}{2}(t-bu) & -cu \\ au & \frac{1}{2}(t+bu) \end{bmatrix} \tag{6.15}$$

corresponding to each unit $\theta = \frac{1}{2}(t+u\sqrt{d})$ of norm 1 in R_d, for any primitive form $[a, b, c]$ of discriminant d. One easily verifies that if T is replaced by WT, α_1 and α_2 in (6.3) are replaced by $\alpha_1\theta$ and $\alpha_2\theta$. To prove Theorem 6.2 we observe what happens to a solution of (6.14) when T is replaced by WT. Then t_2 becomes $\frac{1}{2}(t-bu)t_2 - cut_4 = c'x' + iy'$ (say) and t_4 becomes $aut_2 + \frac{1}{2}(t+bu)t_4 = y'$ (say), and by (6.13),

$$x' = \tfrac{1}{2}\{t-(2ai+b)u\}x - suy, \qquad y' = ac'ux + \tfrac{1}{2}\{t+(2ai+b)u\}y,$$

where one recognizes the unimodular automorph of $[ac', 2ai+b, s]$ with the same θ.

COROLLARY 6.2.1. *If $e \neq 0$ the number of sets $\{WT|\ W$ in (6.15)$\}$ of solutions of* (6.1) *in which $e(\det T) > 0$ is equal to the number of automorphic sets of representations of e by a form in KL^{-1}; likewise with a form in KL, if $e(\det T) < 0$.*

In view of (6.4) and (6.5), (6.1) can also be written as

$$N(x\alpha_1 + y\alpha_2) = ea(a'x^2 + b'xy + c'y^2), \qquad \alpha_1 \text{ and } \alpha_2 \text{ in } [a, r+\omega]. \tag{6.16}$$

Also, if α_1 and α_2 are given by (6.3), $\langle \alpha_1, \alpha_2 \rangle$ has the sign of $a(\det T)$. Hence:

THEOREM 6.3. *Ordered pairs $\langle \alpha_1, \alpha_2 \rangle$ satisfying* (6.16) *which have the sign of ea correspond one-to-one to representations of e by a form in KL^{-1}; likewise, those having the sign of $-ea$, by a form in KL. Furthermore, automorphic sets of such representations of e correspond one-to-one to sets of ordered pairs*

$$\{\langle \alpha_1\theta, \alpha_2\theta \rangle|\ \theta \text{ any unit of norm } 1 \text{ in } R_d\}. \tag{6.17}$$

In Theorems 6.1-6.3 we regarded e as fixed. If we let it be free something quite remarkable happens:

THEOREM 6.4. *Let f and g be as in Theorem* 6.1, *and assume that d is not square. Consider the integral solutions T of* (6.1) *with e arbitrary. Those with $e(\det T) \geqslant 0$ form a two-dimensional Z-module $\mathfrak{M}_+$; and those with $e(\det T) \leqslant 0$ form a two-dimensional Z-module $\mathfrak{M}_-$.*

Proof. Since d is not square, only $T = 0$ corresponds to $e = 0$. What makes the theorem hold is the fact that if $e \neq 0$ (cf. (6.8))

$$a_2(b' - v\sqrt{d})/2 = c'a_1, \tag{6.18}$$

and hence either column of T (a_1 or a_2) determines the other uniquely, once the sign of v, or of $e(\det T)$, is fixed. The possible second columns of T are expressed in (6.13), for each sign of v. For each such second column, (6.18) determines a unique a_1 and the T that corresponds. If T_1 is so formed with $x = 1$ and $y = 0$, and T_2 with $x = 0$ and $y = 1$, then using arbitrary integers x and y will give $T = xT_1 + yT_2$. Thus the matrices T constitute a two-dimensional Z-module, with the zero matrix the only one of determinant 0.

This process applies when d is a nonzero square if we assume s not zero in (6.14); then $x = 0$ and $y = 1$ makes $\det T_2 \neq 0$. The matrices $T = xT_1 + yT_2$ will all satisfy (6.1), but may include only a proper subset of the matrices T such that $T'AT = 0$. Thus:

COROLLARY 6.4.1. *In this modified sense, Theorem* 6.4 *holds when d is a nonzero square.*

COROLLARY 6.4.2. *The rational matrices T satisfying* (6.1) *for arbitrary rational e can be distributed into two two-dimensional vector spaces over Q, $\mathfrak{N}_+$ and $\mathfrak{N}_-$; $\mathfrak{N}_+$ consists of all with $e(\det T) > 0$ along with the zero matrix, and if d is square other matrices T of determinant 0; $\mathfrak{N}_-$ similarly has $e(\det T) < 0$, or $e = 0 = \det T$.*

Clearly, any Z-basis given by our algorithm will serve as a Q-basis for $\mathfrak{N}_+$, or $\mathfrak{N}_-$. Any two non-proportional matrices in $\mathfrak{N}_+$, or $\mathfrak{N}_-$, will serve as a Q-basis. Since the set of all integral matrices in $\mathfrak{N}_+$ is closed under subtraction it is a Z-module and must coincide with $\mathfrak{M}_+$; similarly for $\mathfrak{N}_-$.

Let us consider as an example the case where $f = g = [a, b, c]$, $(a, b, c) = 1$. The four matrices (with respective determinants 1, ac, $-a^2$, $-ac$)

$$S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad S_2 = \begin{bmatrix} 0 & -c \\ a & b \end{bmatrix}, \quad S_3 = \begin{bmatrix} a & b \\ 0 & -a \end{bmatrix}, \quad S_4 = \begin{bmatrix} 0 & c \\ a & 0 \end{bmatrix}, \tag{6.19}$$

carry f into ef, with $e = 1, ac, a^2, ac$ respectively. Hence, if $ac \neq 0$,

$$\mathfrak{N}_+ = \{kS_1 + lS_2|\ k, l \text{ in } Q\}, \qquad \mathfrak{N}_- = \{kS_3 + lS_4|\ k, l \text{ in } Q\}. \tag{6.20}$$

But kS_1+lS_2 is integral if and only if k, l are in Z; hence

$$\mathfrak{M}_+ = \{kS_1+lS_2 |\ k, l \text{ in } Z\}. \tag{6.21}$$

It is not nearly so easy to deduce a Z-basis for $\mathfrak{M}_-$ from the Q-basis for $\mathfrak{N}_-$, although there are methods in the literature which may be applied to this type of problem (cf. [16], pp. 246-247); it is less tentative and easier to use our algorithm. A neat way in the present example is to transform f by a unimodular transformation into a form $[a, b, ac]$, whence $(a, b) = 1$. Then in place of (6.19) one writes the matrices

$$T_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad T_2 = \begin{bmatrix} 0 & -ac \\ a & b \end{bmatrix}, \quad T_3 = \begin{bmatrix} a & b \\ 0 & -a \end{bmatrix}, \quad T_4 = \begin{bmatrix} 0 & c \\ 1 & 0 \end{bmatrix}, \tag{6.22}$$

and has

$$\mathfrak{M}_+ = \{kT_1+lT_2 |\ k, l \text{ in } Z\}, \quad \mathfrak{M}_- = \{kT_3+lT_4 |\ k, l \text{ in } Z\}.$$

If $T = kT_1+lT_2$, $e = |T| = k^2+bkl+acl^2$; if $T = kT_3+lT_4$, $e = -|T| = a^2k^2+bkl+cl^2$.

One easily verifies

THEOREM 6.5. *The module $\mathfrak{M}_+$ for $f = g = [a, b, c]$ is an integral domain if d is not square, a commutative ring if d is a nonzero square. Also $\mathfrak{M}_+ \cong R_d$.*

Let us re-examine Theorem 3.7. From $\langle\alpha_1, \alpha_2\rangle T_\gamma = \gamma\langle\alpha_1, \alpha_2\rangle$ and $\langle\alpha_1, \alpha_2\rangle T_\delta = \delta\langle\alpha_1, \alpha_2\rangle$ follows

$$\langle\alpha_1, \alpha_2\rangle(T_\gamma+T_\delta) = (\gamma+\delta)\langle\alpha_1, \alpha_2\rangle \quad \text{and} \quad \langle\alpha_1, \alpha_2\rangle T_\gamma T_\delta = \delta\gamma\langle\alpha_1, \alpha_2\rangle.$$

The uniqueness of the transformations implies that $T_\gamma+T_\delta = T_{\gamma+\delta}$, $T_\gamma T_\delta = T_{\gamma\delta}$, and it easily follows that

THEOREM 6.6. *The set $\mathscr{R}$ of matrices T_γ for γ in F_j is isomorphic to F_j, and the set $\mathscr{I}$ of integral matrices T_γ is isomorphic to R_d. Further, $\mathscr{I}$ is a two-dimensional Z-module and $\mathscr{R}$ is a two-dimensional vector space, with the expression*

$$T_\gamma = v\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + u\begin{bmatrix} 0 & -c \\ a & b \end{bmatrix}, \tag{6.23}$$

where for $\mathscr{R}$, $v = \frac{1}{2}(t-bu)$ and u are arbitrary rationals, and for $\mathscr{I}$, arbitrary integers.

COROLLARY 6.6.1. *Let β_1, β_2 also be linearly independent elements of F_j, and denote by $\mathscr{S}$ the set of all rational matrices S_γ such that*

$$\langle\alpha_1, \alpha_2\rangle S_\gamma = \gamma\langle\beta_1, \beta_2\rangle \quad (\gamma \text{ in } F_j), \tag{6.24}$$

and by $\mathscr{S}_0$ the subset of $\mathscr{S}$ consisting of integral matrices. Then $\mathscr{S}$ is a two-dimensional vector space over Q, and $\mathscr{S}_0$ is a two-dimensional Z-module.

Proof. If T is defined by $\langle\alpha_1, \alpha_2\rangle T = \langle\beta_1, \beta_2\rangle$, then clearly $S_\gamma = T_\gamma T$, and $\mathscr{S}$ has the Q-basis

$$T, \quad \begin{bmatrix} 0 & -c \\ a & b \end{bmatrix} T. \tag{6.25}$$

As for $\mathscr{S}_0$, it is clearly a Z-module, and the existence of a two-term basis follows by familiar methods [16].

Notice that $\mathscr{S}_0$ coincides with the module $\mathfrak{M}_+$ of Theorem 6.4. The module $\mathfrak{M}_-$ consists of the integral matrices V_0 such that $\langle\alpha_1, \alpha_2\rangle V_0 = \theta\langle\overline{\alpha}_1, \overline{\alpha}_2\rangle$, where $[a, b, c]$ is the primitive norm of $\langle\alpha_1, \alpha_2\rangle$, hence $[-a, -b, -c]$ is that of $\langle\overline{\alpha}_1, \overline{\alpha}_2\rangle$.

We made the assumption in Theorem 6.1 that the discriminant of f divides that of g. However, (6.1) can have solutions T in certain cases where this assumption does not hold. We show how to reduce the problem to a case where the assumption does hold.

THEOREM 6.7. *Let $d = d_0n^2$. If (6.1) has an integral solution T, then*

$$(e, n^2) \text{ is a square, say } e_0^2 \ (e_0 \text{ positive}); \tag{6.26}$$

and then if we write $d' = d/e_0^2$ and $e' = e/e_0^2$, the discriminant of g must have the form $d'v^2$ with v a positive integer. If these conditions hold, there exists A_0 of discriminant d', and R of determinant e_0, such that $A = R'A_0R$, and there is a one-to-one association between the solutions T of (6.1) and the solutions S of

$$S'A_0S = e'B, \tag{6.27}$$

defined by $T = RS$.

Proof. We can suppose that $(ac', 2n) = 1$. We show how to remove primes p dividing (e, n) one by one. By a translation we can make $p^2|b$. Then since $d = b^2-4ac$, $p^2|c$, or if $p = 2$ and $d \equiv 4 (\mathrm{mod}\, 16)$, $c \equiv -a (\mathrm{mod}\, 4)$. In the latter case, (6.2) shows that $t_2 \equiv t_4 (\mathrm{mod}\, 2)$, $4|e$, $t_1 \equiv t_3 (\mathrm{mod}\, 2)$, and we can put $A = R_1'A_1R_1$, where R_1 is the matrix with 2 1 on first row, 0 1 on second. In the former case, (6.2) gives $p|t_2$, $p^2|e$, $p|t_1$, and we can take A_1 to be the matrix of $[a, b/p, c/p^2]$ and R_1 the matrix with p 0 on first row, 0 1 on second. We thus remove the primes in (e, n) one by one. To prove that the discriminant of g is $d'v^2$, we equate discriminants in (6.1):

$$e^2(b'^2-4a'c') = dt^2, \quad t = \det T; \tag{6.28}$$

setting $t = e_0s$, $e = e_0^2e'$, we have

$$e'^2(b'^2-4a'c') = d's^2, \tag{6.29}$$

where e' has no prime factor such that $d'/p^2 \equiv 0$ or $1 \pmod 4$. Hence $e'^2 | s^2, e' | s$, and we can put $s = e'v$.

It may be noted that although the relation between matrices T, S is one-to-one, the relation between sets $\{WT |\ W$ any unimodular automorph of $A\}$ and $\{W_0 S |\ W_0$ any unimodular automorph of $A\}$ is σ to 1, where σ is the index of a subgroup isomorphic to the group of W's in the group of W_0's.

We would like to express our appreciation to our student, Dennis R. Estes, for various suggestions and help in the writing of this paper.

References

[1] P. Bachmann, *Grundlehren der Neueren Zahlentheorie*, 1907, p. 248.
[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, 1966, pp. 139-143.
[3] R. Dedekind, *Gesammelte Mathematische Werke*, vol. I.
[4] L. E. Dickson, *Introduction to the Theory of Numbers*, 1929.
[5] P. G. Lejeune Dirichlet and R. Dedekind, *Zahlentheorie*, Suppl. XI, ed. 4, 1894, p. 187.
[6] R. Fricke, *Elliptische Funktionen*, 2, 1922, p. 148.
[7] C. F. Gauss, *Disquisitiones Arithmeticae*, Arts., pp. 234-243.
[8] E. Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*, 1923, pp. 213-217.
[9] D. Hilbert, *Die Theorie der Algebraischen Zahlkörper*, § 76.
[10] E. E. Kummer, Jour. für Mathematik, 35, p. 325.
[11] R. König, Jahresbericht d. Deutschen Math.-Vereinigung, 22, 1913, pp. 239-254.
[12] E. Landau, *Vorlesungen über Zahlentheorie*, 1927, v. 3, pp. 187-196.
[13] G. Pall, (a) Bull. Amer. Math. Soc. 54 (1948), pp. 1171-1175; (b) Trans. Amer. Math. Soc. 35 (1933), pp. 491-509.
[14] J. Sommer, *Vorlesungen über Zahlentheorie*, 1907, pp. 197-220 (French transl. by A. Lévy, Paris, 1911, pp. 205-229).
[15] H. Weber, Math. Annalen, 48 (1897), pp. 459-462; Algebra III, 1908, pp. 330-337.
[16] O. Zariski and P. Samuel, *Commutative Algebra*, I, pp. 246-247.

LOUISIANA STATE UNIVERSITY
Baton Rouge, Louisiana

Reçu par la Rédaction le 1. 12. 1967

ACTA ARITHMETICA
XV (1968)

A reduction of the Čebotarev density theorem to the cyclic case

by

C. R. MacCluer (East Lansing, Mich.)

The two most useful theorems of Algebraic Number Theory are Kummer's Theorem on prime factorizations and the Čebotarev Density Theorem. Unfortunately until now Čebotarev's Theorem has been inaccessible to the beginning student because of its difficult proof. I present here a reduction of Čebotarev's Theorem to the case of cyclic extensions, a case that can be handled by *abelian L*-series. (See [1], page 165 and 218.)

Notation. If k is a number field and $\mathfrak{a}$ a fractional ideal of k, then $\|\mathfrak{a}\|_k$ will denote the absolute norm of $\mathfrak{a}$ (over the rational number field $\boldsymbol{Q}$). If K is a finite galois extension of k, $\mathfrak{p}$ a prime ideal of k, and $\mathfrak{P}$ a prime ideal of K, then

$$\left[\frac{K/k}{\mathfrak{P}}\right] \quad \text{and} \quad \left(\frac{K/k}{\mathfrak{p}}\right)$$

will denote the Frobenius and Artin symbol respectively. If G is a group, then $C_G(\sigma)$ and $\varkappa_G(\sigma)$ will denote the centralizer and the conjugacy class of σ in G respectively. Finally if S is a subset of G, then $|S|$ will denote the cardinality of S.

THEOREM (Čebotarev Density Theorem). *Let k be an algebraic number field and let K be a finite galois extension of k with galois group G over k. If σ is an element of G, then the Dirichlet density of all primes $\mathfrak{p}$ of k with*

$$\left(\frac{K/k}{\mathfrak{p}}\right) = \varkappa_G(\sigma)$$

is

$$|\varkappa_G(\sigma)|/(G:1).$$

Reduction to the case that K/k is cyclic. Let H denote the cyclic subgroup of G generated by σ. Suppose $\mathfrak{p}$ is a prime of k with

$$\left(\frac{K/k}{\mathfrak{p}}\right) = \varkappa_G(\sigma).$$