Since vu is an isometrically isomorphic embedding, Y_1 is isometrically isomorphic to $C(S_1)$. Hence, by Theorem 1a, there are a subspace Z_1 of Y_1 such that Z_1 is isometrically isomorphic to $C(S_1)$ and a projection π_1 from X_1 onto Z_1 such that $\|\pi_1\| = 1$. Let $Z = v^{-1}(Z_1)$ and let $\pi = v^{-1}\pi_1 v$. Clearly π is a projection from X onto Z. Since $Y_1 \supset Z_1$, we have $Y = v^{-1}(Y_1) \supset v^{-1}(Z_1) = Z$. Since v is an isomorphism, all spaces Z, Z_1, $C(S_1)$, and $C(S)$ are isomorphic each to other. This completes the proof.

References

[1] S. Banach, *Théorie des opérations linéaires*, Monografie Matematyczne, Warszawa 1932.

[2] C. Bessaga and A. Pełczyński, *Spaces of continuous functions IV*, Studia Math. 19 (1960), p. 53-62.

[3] M. M. Day, *Normed linear spaces*, Berlin-Göttingen-Heidelberg 1958.

[4] J. Dugundji, *An extension of Tietze's theorem*, Pacific J. Math. 1 (1951), p. 353-367.

[5] N. Dunford and J. T. Schwartz, *Linear operators I*, London - New York 1958.

[6] K. Gęba and Z. Semadeni, *Spaces of continuous functions V*, Studia Math. 19 (1960), p. 303-320.

[7] L. Gillman and M. Jerison, *Rings of continuous functions*, New York 1960.

[8] W. Holsztyński, *Continuous mappings induced by isometries of spaces of continuous functions*, Studia Math. 26 (1966), p. 133-136.

[9] K. Kuratowski, *Topologie I*, Monografie Matematyczne, Warszawa 1958.

[10] S. Mazurkiewicz and W. Sierpiński, *Contributions à la topologie des ensembles dénombrables*, Fund. Math. 1 (1920), p. 17-27.

[11] A. A. Miljutin, *Isomorphism of spaces of continuous functions on compacts of the power continuum*, Teor. Funk. Funkcional. Analiz. i Priložen. 2 (1966), p. 150-156 (Russian).

[12] A. Pełczyński, *Projections in certain Banach spaces*, Studia Math. 19 (1960), p. 209-228.

[13] — *Linear extensions, linear averagings and their application to linear topological classification of spaces of continuous functions*, Rozprawy Matematyczne 58 (1968).

[14] W. Sierpiński, *Cardinal and ordinal numbers*, Monografie Matematyczne, Warszawa 1958.

Reçu par la Rédaction le 7. 11. 1967

STUDIA MATHEMATICA, T. XXXI. (1968)

Composition of binary quadratic forms*

by

IRVING KAPLANSKY (Chicago, Ill.)

1. Introduction. Gauss's complete discussion of the composition of binary quadratic forms over the integers ([6], sections 235 - 244 and several later sections) was a tour de force that makes remarkable reading to this day.

Several of the great mathematicians of the nineteenth and early twentieth centuries took up the theme and gave fresh accounts of the work. This material takes up twenty condensed pages in Dickson's history ([3], p. 60 - 79).

The idea of giving still another account of this venerable subject arose when I attempted to extend the theory to Bézout domains (integral domains where every finitely generated ideal is principal). Now the modern view of composition is that it is really just multiplication of suitable modules. (This idea is attributed by Dickson to Dedekind, quoting the eleventh supplement in [5]. A recent exposition is [1], p. 212 - 5.) But when one proceeds to a detailed execution, there are difficulties. The correspondence between quadratic forms and modules needs touching up. There is some trouble disentangling a module from its conjugate, overcome by "orienting" the module; there is also a need to use "strict" equivalence of modules, meaning multiplication by elements of *positive* norm. Both of these points seem to require an ordered integral domain, and on closer inspection one sees further obstacles if the base ring has units other than ± 1.

I might have concluded that ordering was indispensable for composition, had it not been for the existence of still another method, the technique of "united forms", also attributed by Dickson to Dedekind (tenth supplement in [5]; as late as 1929 Dickson [4], Ch. IX, thought this to be the best method to put in his book). It is a fact that this discussion is valid verbatim for any principal ideal domain of characteristic $\neq 2$. But I could not get it to work for Bézout domains (the difficulty comes

---

* Work on this paper was supported in part by the National Science Foundation.

up in the preliminary lemma asserting that forms can represent elements prime to any given element).

In due course a workable idea presented itself: the technique of *pairs* consisting of a module and an element. The use of pairs shrinks the need for orientation down to the picking of a square root of the discriminant; it builds strict equivalence harmlessly into the definitions; and it accommodates units other than ± 1. Even over the ring of integers the present discussion may have expository merit.

2. Modules. Let K be a field, L a separable quadratic extension of K. We shall in general use early letters of the alphabet for elements of K, late letters for L.

We write $*$ for the automorphism of L over K, T for the trace, N for the norm. N equips L with the structure of a quadratic form over K. The mapping $*$ preserves N, and multiplication by an element x of L multiplies all norms by Nx. We shall need the well-known converse

LEMMA 1. *Let f be a one-one linear transformation of L onto itself which multiplies all norms by a fixed factor. Then f is multiplication by a non-zero element of L, or such a multiplication followed by $*$.*

Let R be an integral domain with quotient field K. We study R-submodules of L. The extra structure on L endows these modules with additional structure. For instance, if A is an R-submodule of L we write A^* for the set of all x^* with $x \in A$; A^* is again an R-module. The elements Nx, x ranging over A, generate a (possibly fractional) ideal in R which we call NA, the norm of A. When A and B are R-modules, so is their product AB (this meaning as usual the set of sums of terms xy, $x \in A$, $y \in B$).

When A is free of dimension 2, we define DA, the *discriminant* of A as follows: take a basis x, y and set $DA = (xy^* - x^*y)^2$. Note that $DA \in K$. (More accurately, DA should be called the *discriminant relative to the chosen basis*; a change of basis will multiply DA by the square of a unit in R.)

The expression $xy^* - x^*y$ will also play a role. We note that if $u = ax+by$, $v = cx+dy$, then $uv^* - u^*v = (ad-bc)(xy^* - x^*y)$.

We finally note a natural equivalence relation: A and B are *equivalent* f $B = xA$ with x a non-zero element of L.

3. Pairs. A pair $[A, a]$ consists of an R-submodule A of L and a non-zero element a in K. We extend to pairs the various concepts introduced in Section 2:

$$[A, a]^* = [A^*, a], \quad N[A, a] = NA/a,$$
$$[A, a][B, b] = [AB, ab], \quad D[A, a] = DA/a^2,$$

the last being defined when A is free 2-dimensional.

Equivalence of pairs is defined as follows: $[A, a] \sim [B, b]$ if there exists a non-zero element x in L with $B = xA$, $b = (Nx)a$. It is an easy exercise to see that conjugation, norm, product, and discriminant are all well defined on equivalence classes of pairs.

4. Quadratic forms. A "concrete" binary quadratic form over a commutative ring with unit R is an expression $ax^2+bxy+cy^2$, $a,b,c \in R$. Abstractly, the structure is that of a quadratic form on a free 2-dimensional R-module together with a distinguished basis. When the basis is changed, we pass to an equivalent form; if the change of basis has determinant 1, we speak of *proper* equivalence.

The discriminant is b^2-4ac. Under equivalence it gets multiplied by the square of a unit, and under proper equivalence it is invariant.

In the setup of Section 2, take a free module A. The norm puts a quadratic form on A. When we take a basis of A, we get a concrete form (with coefficients in K), and it is easily checked that the two discriminants introduced coincide.

With a pair $[A, a]$ we associate the quadratic form on A given by the norm divided by a. Again the two discriminants coincide.

5. The correspondence. In this section we have to assume characteristic $\neq 2$.

With an equivalence class of pairs we wish to associate a proper equivalence class of binary quadratic forms. Our aim does not extend beyond doing this for a fixed discriminant, say Δ (on pairs this is meaningful only up to the square of a unit, of course, but for the concrete forms we mean discriminant exactly Δ).

Δ is an element of K having a square root in L. Arbitrarily fix a square root δ. Let a pair $[A, a]$ of discriminant Δ be given. We say that the basis x, y of A is *admissible* if $(xy^* - x^*y)/a = \delta$. Admissible bases exist: with any choice of basis x, y we have $(xy^* - x^*y)^2/a^2 = u^2\Delta$, u a unit in R, so that $(xy^* - x^*y)/a = \pm u\delta$. We need only replace x by $\pm u^{-1}x$.

On A relative to an admissible basis we take the form N/a; the result is a concrete quadratic form f whose proper equivalence class we take as the image of the equivalence class of $[A, a]$.

Suppose we pass to a different admissible basis of A. Then since the change of basis must have determinant 1, the proper equivalence class of f is unaffected.

Let the pair $[B, b]$ be equivalent to $[A, a]$ *via* the element z, so that $B = zA$, $b = (Nz)a$. If the basis x, y is admissible for A, we see at once that zx, zy is admissible for B. The concrete form thus obtained for $[B, b]$ is identical with the one for $[A, a]$.

We have now shown that we have a well defined map from equivalence classes of pairs to proper equivalence classes of forms. We proceed to show that it is one-to-one and onto.

As regards onto, we explicitly exhibit the inverse image. For $f = ax^2+bxy+cy^2$ of discriminant Δ we invent the pair $[A, a]$, where A is the module spanned by a and $(b-\delta)/2$. These elements are in fact an admissible basis for A and we find the image of $[A, a]$ to be f.

Suppose finally that $[A, a]$ and $[B, b]$ both have discriminant Δ and lead to properly equivalent forms. Now this means that after a change of basis of determinant 1, say on the first form, the two forms become identical. We can suppose that this change of admissible basis has already been done for A. We thus have admissible bases, say x, y for A and u, v for B, giving rise to identical concrete forms. This says that the mapping (say F) from A to B given by sending x into u and y into v multiplies norms by b/a. We can extend F to a mapping of L into L and then apply Lemma 1 to conclude that F is either multiplication by an element z (necessarily of norm b/a) or such a multiplication followed by $*$. We can check which it is by looking at determinants. Multiplication by z has determinant Nz; $*$ has determinant -1; since $(xy^*-x^*y)/a = (uv^*-v^*u)/b$, the determinant of F is b/a (see Section 2). Hence $*$ does not appear, and we have proved $[A, a]$ and $[B, b]$ to be equivalent, as required. We summarize:

THEOREM 1. *Let K be a field of characteristic $\neq 2$, L a quadratic extension of K. Let R be an integral domain with quotient field K. Fix a discriminant Δ and a square root of Δ. For a pair $[A, a]$ of discriminant Δ, A a free 2-dimensional R-submodule of L, pick an admissible basis as above, thus getting a binary quadratic form. This implements a one-to-one correspondence between all equivalence classes of pairs with discriminant Δ and all proper equivalence classes of binary quadratic forms with discriminant Δ.*

6. Composition. Let us suppose that to the concrete forms f, g of discriminant Δ we have associated the pairs $[A, a]$ and $[B, b]$. The obvious way to get a product for f and g is to look to the product pair $[AB, ab]$. But two difficulties arise. For a general integral domain R, AB need not be a free module. This difficulty disappears if R is a Bézout domain, so we assume this henceforth. Secondly, $[AB, ab]$ need not have discriminant Δ, and we have no procedure for meshing different discriminants. We shall not give the exact conditions for $[AB, ab]$ again to have discriminant Δ, but pass at once to the best behaved case: primitive forms. We say that a pair is *primitive* if its norm is R; a concrete form is *primitive* if its coefficients lie in R and generate R. One easily sees that the two notions correspond when we pass from pairs to forms as above.

Then the crucial fact is that *the primitive pairs of a fixed discriminant form a group under multiplication.* This is of course well known and goes back to Gauss. For the reader's convenience we state the relevant facts in a theorem, and sketch the proof.

One definition is needed: in our context an *order* is a free 2-dimensional module which is a ring containing 1.

THEOREM 2. *Let R be a Bézout domain with quotient field K, L a separable quadratic extension of K. Then*

(a) *two orders are identical if and only if they have the same discriminant (up to the square of a unit in R),*

(b) *a (free 2-dimensional) module A is an invertible ideal over the unique order P having the same discriminant as the pair $[A, NA]$, and $AA^* = N(A)P$,*

(c) *for any modules A and B, $N(AB) = N(A)\,N(B)$.*

Sketch of proof. (a) An order has a basis 1, r with r integral over R. Its discriminant is $(r-r^*)^2$. Given a second order with basis 1, t, suppose its discriminant $(t-t^*)^2 = u^2(r-r^*)^2$, u a unit in R. Then $t-t^* = \pm u(r-r^*)$, $t \pm ur$ is invariant under $*$, hence lies in K, hence in R (any Bézout domain is integrally closed). So the two orders coincide.

(b) We perform the brief computation of [2], Prop. 1.4.1. We pick a basis for A of the form a, z with $a \in K$, $Tz = b$, $Nz = c$. Then $NA = (a^2, ab, c) = (e)$, say, and $DA = a^2(b^2-4c)$. Let $t = az/e$. We find that the module P spanned by 1 and t is an order whose discriminant $a^2(b^2-4c)/e^2$ coincides with the discriminant of the pair $[A, e]$. We find $PA = A$ and $AA^* = eP$, showing that A is an invertible ideal over P. A cannot be an invertible ideal over a different order because quite generally an object cannot be an invertible ideal over two different integral domains.

(c) We have $AA^* = eP$, $BB^* = fQ$, where $(f) = NB$, and Q is the order attached to B. One easily sees that PQ is again an order. Then the equation $(AB)(AB)^* = ef\,PQ$ identifies PQ as the order attached to AB, showing that $(ef) = N(AB)$.

Consider now the primitive pairs with a given discriminant Δ, and let P be the order with discriminant Δ. It is immediate from Theorem 2 that these pairs form a group, with $[P, 1]$ as the unit. The pairs equivalent to $[P, 1]$ form a subgroup, and so the equivalence classes of primitive pairs also form a group, which we call the *extended class group* of P, say $H(P)$.

By the class group $G(P)$ of P we mean as usual the invertible ideals of P modulo principal ideals. The map $[A, a] \to A$ induces a homomorphism of $H(P)$ onto $G(P)$, the kernel being isomorphic to units of R modulo norms of units of P.

We summarize the situation. Let R be a Bézout domain of characteristic $\neq 2$, and let the setup be as above. Fix a discriminant Δ, a square root δ, and let P be the order with discriminant Δ. The equivalence classes of primitive pairs of discriminant Δ are in one-one correspondence with the proper equivalence classes of binary quadratic forms of discriminant Δ. On the former we have the group structure given by the extended class group $H(P)$. We transfer the group structure to the forms and we have defined composition.

What happens if we replace δ by the other square root $-\delta$? The correspondence changes (in a harmless way — each pair is replaced by its conjugate). However the group structure on the forms is unchanged; it is entirely intrinsic.

7. Connection with united forms. We verify that Dedekind's method of united forms, whenever applicable, gives the same composition as that obtained above.

In brief, the setup is this: we are given a, b, c, d in R with the first three generating R. We wish to see that $ax^2+bxy+cdy^2$ and $cx^2+bxy+ady^2$ compose to yield $acx^2+bxy+dy^2$. All three forms have the discriminant $\Delta = b^2-4acd$. Pick a square root δ of Δ. Then suitable corresponding pairs are $[A, a]$, $[B, c]$ and $[C, ac]$ where A, B, C are spanned by a, c, ac respectively and $z = (b-\delta)/2$. We have $z^2-bz+acd = 0$, so AB is spanned by $ac, az, cz, bz - acd$. The term acd can be deleted since it is a multiple of ac. The terms az, bz, cz combine to z. Hence $AB = C$ and the pair $[C, ac]$ is the product of the pairs $[A, a]$ and $[B, c]$.

8. The ordered case. Let R be an ordered integral domain. Suppose as in the discussion above that a fixed square root δ has been picked for one discriminant Δ. The other discriminants that are pertinent (i.e. that go with forms "embeddable" in our fixed field L) have the form $k^2\Delta$, k non-zero in K. For any such we have a natural choice for a square root: $k\delta$ with $k > 0$.

What we can get out of this is best described by going backwards from forms to pairs: we get a coherently defined map on all proper equivalence classes of binary quadratic forms to all equivalence classes of pairs. But we are not yet ready for composition, for the mapping is not necessarily one-one. Indeed, it is one-one if and only if ± 1 are the only units in R.

Suppose finally that R is an ordered integral domain, Bézout, and that its only units are ± 1. Then we get composition defined on all binary quadratic forms with discriminants having ratio a square, just as Gauss did for the ring of integers. The composition is quite intrinsic, at least granted the ordering of R. If R has a unique ordering, it is entirely intrinsic.

We briefly discuss other aspects of the ordered case. It is natural to distinguish two cases, according to the sign of Δ.

(1) $\Delta < 0$. All norms are positive. The extended class group divides into two cosets according to the sign of a in the pair $[A, a]$. Nothing essential is lost by insisting that a be positive, i.e. discarding the negative definite forms.

(2) $\Delta > 0$. Since there exists elements with negative norm, any pair is equivalent to one with a positive, and this normalization may be made if one prefers.

Things become simpler still when the only units are ± 1. If $\Delta < 0$, the positive part of the extended class group coincides with the class group; the pairs are superfluous. If $\Delta > 0$ and -1 is the norm of a unit in P, the pairs are again superfluous. If $\Delta > 0$ and -1 is not the norm of a unit in P, the use of pairs amounts to the same thing as to the customary notion of strict equivalence: $B = zA$ with $Nz > 0$. Even for the ring of integers, the pairs do have the merit of treating the various cases in a unified way.

9. Final remarks. (1) All the results in this paper carry over to the case where L is the direct sum of two copies of K and the involution is the mapping interchanging the two summands (the corresponding binary quadratic forms have discriminants which are perfect squares). It was solely for expository reasons that this case was not incorporated in the body of the paper.

(2) Over a general Bézout domain (i.e. with no ordering or with units other than ± 1) can composition be defined without the restriction to a fixed discriminant? I see no natural way to do this. Perhaps impossibility could be proved rigorously by putting the matter in a functorial setting.

(3) If one is willing to make enough arbitrary choices, a product can be defined. For instance, this was done by Smith for the ring of Gaussian integers ([7], p. 423-427 in the pagination of his collected works).

(4) For characteristic 2 it is at present not clear whether composition is definable under any reasonable conditions.

(5) There is a different point of view on the whole subject, which has certain advantages, but represents a radical departure from the Gauss tradition. Allow equivalence of binary quadratic forms to mean that the determinant of the transformation can be any unit. Modify equivalence of pairs by identifying each pair $[A, a]$ with its conjugate $[A^*, a]$. Then: there is a one-one correspondence between equivalence classes of pairs and equivalence classes of binary quadratic forms. We can proceed forthwith to define composition, with no worries about discri-

minants and no special concern for characteristic 2; the only trouble is that the "product" is in general two-valued. On primitive pairs with a fixed discriminant the structure obtained is that of an abelian group in which every element has been identified with its inverse.

References

[1] H. Cohn, *A second course in number theory*, New York 1962.

[2] E. C. Dade, O. Taussky and H. Zassenhaus, *On the theory of orders*, Math. Ann. 148 (1962), p. 31-64.

[3] L. E. Dickson, *History of the theory of numbers*, Vol. III, New York 1934.

[4] — *Introduction to the theory of numbers*, Chicago 1929.

[5] G. R. Dirichlet and R. Dedekind, *Vorlesungen über Zahlentheorie*.

[6] C. F. Gauss, *Disquisitiones arithmeticae*.

[7] H. J. S. Smith, *On complex binary quadratic forms*, Proc. Roy. Soc. 13 (1864), p. 278-298 = *Collected works*, Vol. 1, p. 418-442.

Reçu par la Rédaction le 14. 12. 1967

STUDIA MATHEMATICA, T. XXXI. (1968)

The existence of the potential operator associated with an equicontinuous semigroup of class (C_0)

by

KÔSAKU YOSIDA (Tokyo)

Hunt [2] introduced the notion of potential operators V associated with transient Markov processes in a separable, locally compact, non-compact Hausdorff space. The present author gave an operator-theoretical treatment of Hunt's theory of potentials (see [4] and [5]). This treatment suggests us to give an *abstract definition of the potential operator which may be applied to transient as well as to some recurrent Markov processes.*

Let X be a locally convex, sequentially complete, linear topological Hausdorff space. Let a family $\{T_t; t \geqslant 0\}$ of continuous linear operators T_t on X into X satisfy the following three conditions:

(1) $T_t T_s = T_{t+s}$, $T_0 = I =$ the identity (the semigroup property);

(2) for any continuous seminorm $p(x)$ on X, there exists a continuous seminorm $q(x)$ on X such that $p(T_t x) \leqslant q(x)$ for all $t \geqslant 0$ and $x \in X$ (the equicontinuity);

(3) $\lim T_t x = T_{t_0} x$ for every $t_0 \geqslant 0$ and $x \in X$ (the class (C_0) property).

Thus $\{T_t; t \geqslant 0\}$ is an equicontinuous semigroup of class (C_0) in X (see [3]). We can prove the following existence theorem:

THEOREM. *The infinitesimal generator A of T_t defined through*

$$Ax = \lim_{h \downarrow 0} h^{-1}(T_h x - x) \tag{4}$$

admits a densely defined inverse A^{-1} if and only if

$$\lim_{\lambda \downarrow 0} \int_0^\infty \lambda e^{-\lambda t} T_t x \, dt = 0 \quad \text{for all } x \in X. \tag{5}$$

Moreover, (5) *is a consequence of an apparently weaker condition*

$$\text{weak-}\lim_{\lambda \downarrow 0} \int_0^\infty \lambda e^{-\lambda t} T_t x \, dt = 0 \quad \text{for all } x \in X. \tag{5'}$$