BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 10, Number 2, April 1984

COMPOSITION AND GENERA OF NORM-TYPE FORMS

BY WILLIAM C. WATERHOUSE[1]

M. Kneser has recently discovered a way to define a composition of binary quadratic forms in general [5]. His basic idea can be described as expanding the structure to include a specified action of a ring of similitudes. This approach avoids the traditional problem of "orienting" the forms, since the "proper equivalences" can be defined simply as the isometries that preserve the action of the similitude ring. But more is true: when we view his idea in this way, we can extend it to norm-type forms of higher degrees. Besides throwing a new light on the quadratic case, this extension reveals a natural concept of genus underlying the "genus fields" already known in number theory.

Fix a base ring R (commutative with unit). If P is a free R-module, then a "form" of degree m supported by P is of course a homogeneous polynomial f of degree m in the coordinates on P; technically, this means that f is an element of the symmetric power $S^m(P^*)$, and in this version we can (and do) extend the definition to projective P of finite rank. Carrying over the usual terminology for quadratic forms, we call (P, f) *primitive* if f is not identically zero modulo any maximal ideal of R.

Now fix an extension C of R, and assume that C is projective of rank m as an R-module. A *form of type* C/R will be a pair (P, f) where

(1) P is an invertible C-module (and hence projective of rank m over R),

(2) f is a primitive form of degree m on the R-module P, and

(3) there is a formal identity $f(cp) = N(c)f(p)$, where N is the norm from C to R.

Two such forms are equivalent if there is a form isometry preserving the C-module structure. Let $F(C/R)$ be the set of equivalence classes. If $R \to S$ is any ring homomorphism, then $\bigotimes_R S$ induces a map $F(C/R) \to F(C \otimes S/S)$. There is always at least one form of type C/R, the *trivial* form (C, N), and in a sense this is the basic one:

THEOREM 1. *For any form of type C/R there is a faithfully flat $R \to S$ such that the form becomes trivial after extension to S.*

This is proved in two steps, first making the C-module free and then making the value of f on a generator into an mth power. Several results then follow by descent theory (see for instance [7]):

COROLLARY 1. *The classes $F(C/R)$ correspond to the (flat) cohomology classes in $H^1(R, \mathrm{Aut}(C, N))$.*

Received by the editors May 16, 1983 and, in revised form, November 16, 1983.

1980 *Mathematics Subject Classification.* Primary 10C02, 10C10, 12A65.

[1]This work was partially supported by the National Science Foundation, Grant MCS 8102967. Some of it was done while the author was a Visiting Scholar at Harvard.

0273-0979/84 $1.00 + $.25 per page

COROLLARY 2. *There is a natural abelian group structure on* $F(C/R)$.

This second corollary holds because $\mathrm{Aut}(C/N)$ consists of multiplications by elements in C^* of norm 1, an abelian group. This explains why in the quadratic case we can only compose "oriented" binary forms: there we have H^1 of an abelian group, while the ordinary isometry classes are H^1 of a larger, nonabelian group. Finally, since $\mathrm{Aut}(C, N)$ is the kernel of a group scheme epimorphism, we automatically get an associated sequence:

COROLLARY 3. *There is an exact sequence*

$$C^* \xrightarrow{N} R^* \to F(C/R) \to \mathrm{Pic}(C) \to \mathrm{Pic}(R).$$

Here $\mathrm{Pic}(C) \to \mathrm{Pic}(R)$ is a norm map induced by $N\colon C \to R$ applied functorially to cocycles. In the quadratic case, this corollary is the ultimate result reached by Kneser [5].

Let us now specialize back to number theory, with $R = \mathbf{Z}$ and C an order in a finite extension field L of $\mathbf{Q}$. We say that two forms of type $C/\mathbf{Z}$ are in the same genus if they are equivalent after extension to each completion $\mathbf{Z}_v$ (including $\mathbf{Z}_\infty = \mathbf{R}$). The rings C_v are semilocal, so by Corollary 3 the local equivalence classes are described by $\mathbf{Z}_v^*/NC_v^*$ (which is trivial unless v is ramified in C). Using class field theory, we can compute the genera:

THEOREM 2. *The group of genera of forms of type* $C/\mathbf{Z}$ *is the kernel of the map*

$$\Pi_{v\,\mathrm{ramified}}(\mathbf{Z}_v^*/NC_v^*) \to \mathrm{Gal}(L^a/\mathbf{Q}),$$

where L^a *is the largest abelian subextension in* L *and the map on each* $\mathbf{Z}_v^*/NC_v^*$ *is the norm residue map.*

This theorem can be extended to replace $\mathbf{Z}$ by any maximal order.

For binary integral quadratic forms, Gauss originally defined genera using characters, which in essence were tests of local equivalence. But as Hasse emphasized [3], these genera also correspond to certain unramified extensions of quadratic number fields. Following this idea, Leopoldt [6] defined "genus fields" for all abelian $L/\mathbf{Q}$ and Fröhlich [1, 2] extended the definition to arbitrary finite $L/\mathbf{Q}$. (See also the book by Ishida [4].) The genus field of $L/\mathbf{Q}$ is defined to be the largest field of the form LL_0, where L_0 is abelian over $\mathbf{Q}$ and LL_0 is unramified over all finite places of L. By class field theory then $\mathrm{Gal}(LL_0/L)$ is a certain quotient of the strict ideal class group. Our forms now allow us to connect this idea back with the original idea of local equivalence.

THEOREM 3. *Let* C *be the maximal order in a finite extension* L *of* $\mathbf{Q}$.

(1) *If* L *has a real place, there is a homomorphism of the strict ideal class group onto* $F(C/\mathbf{Z})$, *and it induces an isomorphism from the Galois group of the genus field onto the group of form genera.*

(2) *If* L *is totally complex, the distinction between positive and negative definite forms splits* $F(C/\mathbf{Z})$ *into* $(\mathbf{Z}/2\mathbf{Z}) \times \mathrm{Pic}(C)$. *The genera of positive definite forms are mapped isomorphically onto the Galois group of the genus field.*

The most important step in proving this theorem is to derive an idelic expression for $F(C/\mathbf{Z})$. Details of all these results will appear elsewhere.

References

1. A. Fröhlich, *The genus field and genus group in finite number fields*, Mathematika **6** (1959), 40–46.

2. ——, *The genus field and genus group in finite number fields.* II, Mathematika **6** (1959), 142–146.

3. H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3** (1951), 45–51.

4. M. Ishida, *The genus fields of algebraic number fields*, Lecture Notes in Math., vol. 555, Springer-Verlag, New York, 1976.

5. M. Kneser, *Composition of binary quadratic forms*, J. Number Theory **15** (1982), 406–413.

6. H. W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9** (1953), 350–362.

7. W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Math., vol. 66, Springer-Verlag, New York, 1979.

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802