BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 42, Number 1, Pages 93–98
S 0273-0979(04)01033-X
Article electronically published on September 24, 2004

Cohomological invariants in Galois cohomology, by Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003, vii+168 pp., \$35.00, ISBN 0-8218-3287-5

Quadratic forms $q(x_1, \ldots, x_n)$ over a field k are the classical examples of nonlinear scalar-valued functions on a vector space $V = k^n$, and they lie at the foundation of nineteenth-century analytic geometry. Motivated by problems such as finding the axes of a conic, geometers studied quadratic forms under symmetries of V. Given two quadratic forms q, q' on V, how may we tell if q and q' are equivalent over k, that is, if $q' = q \circ T$ for $T \in GL_n(k)$?

The discriminant is a place to start. The *discriminant* $\operatorname{disc}(q)$ of a quadratic form over k (which we always assume is of characteristic not 2) is the square class of the determinant of the symmetric matrix A such that $q(x) = x^t Ax$, $x \in V$:

$$\operatorname{disc}(q) = \det(A) \bmod k^{*2} \ \in \ k^*/k^{*2} \cup \{0\}.$$

(Here k^* denotes the multiplicative group of the field k.) Applying the transformation $q \mapsto q \circ T$ induces a transformation $A \mapsto T^t AT$, and we deduce that $\operatorname{disc}(q') = \operatorname{disc}(q)$ from $\det(T^t AT) = \det(A)\det(T)^2$.

Bourbaki observes that it was the visibility of this sort of behavior of the determinant under linear transformations, thanks to Gauss [4, 301–302], that gave "la première impulsion à la théorie générale des invariants" [2, 163–164]. The basic question of invariant theory—going back to the nineteenth century as well—is to determine which polynomial functions $f\colon V^m \to k$ are left unchanged by composition with elements of a given group G of linear transformations on V. (See Weyl's landmark monograph [14].) Given a quadratic form q with symmetric matrix A, the determinant $\det(A)$ is a polynomial function of the quadratic form (and of A) unchanged by composition with elements from $SL_n(k)$. Then, working modulo squares, the discriminant $\operatorname{disc}(q)$ is an invariant unchanged by composition with elements of $GL_n(k)$—an invariant of *equivalence classes of quadratic forms.*[1]

A collection of additional *invariants of quadratic forms* emerged from what we now consider classical quadratic form theory, from the early to mid-twentieth century. Over certain fields, these invariants are enough to classify nondegenerate quadratic forms up to equivalence. Let q be a nondegenerate quadratic form, that is, with nonzero discriminant. The *rank* of q is the dimension of its underlying vector space. Due to Sylvester, the *signature* of q is, for $k \subset \mathbb{R}$, the pair (r, s) where r is the dimension of the maximal subspace P on which $q|_P \geq 0$ and s is the dimension of the maximal subspace N on which $q|_N \leq 0$; we have that $r + s = n$. The *Witt index* of q is the dimension of a maximal subspace on which the quadratic form is zero. For instance, the Witt index of $q(x_1, x_2) = x_1 x_2$ is 1.

2000 *Mathematics Subject Classification.* Primary 12G05, 11E72.

[1]The quadratic form $q(x_1, x_2, \ldots, x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$, considered as a function on $V = k^n$, is an invariant of O_n. By definition, each quadratic form q is an invariant of the subgroup $O(q)$ of $GL(V)$ consisting of elements that leave q fixed. We must distinguish, then, between invariants of quadratic forms and quadratic forms as invariants.

The most interesting of the classical invariants, however, is the Hasse-Witt invariant for quadratic forms. It is easiest to define when q is a diagonal form

$$q(x_1, \ldots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2,$$

and since every equivalence class of quadratic forms over k contains such a diagonal form, this is not a significant restriction. The *Hasse-Witt invariant* $\mathrm{hw}(q)$ of q is a certain class in the Brauer group of central simple algebras over k:

$$\mathrm{hw}(q) = [\otimes_{i<j}(a_i, a_j)] \in \mathrm{Br}(k).$$

Here (a_i, a_j) denotes the generalized quaternion algebra over k, generated as a k-algebra by z and w such that $z^2 = a_i$, $w^2 = a_j$ and $wz = -zw$. This invariant, relatively easy to calculate, is nevertheless surprisingly powerful in classifying nondegenerate quadratic forms. For instance, over the rational numbers $\mathbb{Q}$, two such forms q and q' are equivalent if and only if they have the same rank, discriminant, Hasse-Witt invariant, and signature. In general, these four invariants classify all quadratic forms over k if and only if every quadratic form $x_1^2 + ax_2^2 + bx_3^2 + abx_4^2$ with $a, b \in k^*$ represents every totally positive element of k (that is, every sum of squares) [3, Classification Thm. 3]. See [11, Ch. IV] for a treatment of these invariants of quadratic forms.

At this point, a tantalizing idea arises: there may be additional invariants of quadratic forms—and perhaps also of objects, like quadratic forms, which themselves are invariants of certain groups $G \subset GL_n$—but where to look? One such place is Galois cohomology, a dictionary by which we write standard objects in a different language, and the grammar of this language aids in writing sentences that turn out to express some new results. What's more, our two invariants $\mathrm{disc}(q)$ and $\mathrm{hw}(q)$ are very easily described in this way.

Galois cohomology adopts a formalism from topology, employing cohomology groups and exact sequences connecting them.[2] The main object is the cohomology set $H^i(G, M)$, where G is the Galois group of a field extension and M is a discrete space on which G acts. (For abelian M, $i \geq 0$, but for nonabelian M, basic definitions allow for only $i = 0$ and $i = 1$.) We say that we are considering the cohomology of G with coefficients in M. As in topology, we have natural maps between cohomology sets induced by maps of spaces M or of groups G. Of primary importance here is the fact that for small i or cyclic M, these cohomology sets represent very natural algebraic structures, such as the space of quadratic forms over a field or the nth-power classes of the multiplicative group of a field.

Consider, for instance, the set $H^1(G, M)$ in the case where M is the automorphism group of a quadratic form. For example, let q be a quadratic form in n variables with coefficients in a field k, G the Galois group of a Galois extension l/k, and $M = \mathrm{Aut}(q) = O_l(q)$ the group of $n \times n$ matrices T over l which leave the quadratic form q unchanged under composition with T. Then the set $H^1(G, M)$ is in one-to-one correspondence with the set of all equivalence classes of quadratic forms q' in n variables over k, subject to the restriction that the forms q' are equivalent to q over l. Moreover, the set is *pointed*: there is a natural distinguished element corresponding to the class of q itself.

---

[2]The definitive monograph is Serre's [12], the successive editions of which present a history of the subject. For an introductory overview of Galois cohomology in the number field case, see Gouvêa's book review [5], and for a historical consideration of group cohomology, see Mac Lane's essay [7].

When $l = k_s$, the separable closure of k, *all* nondegenerate quadratic forms in n variables are equivalent over l, and in this case the set $H^1(G, M)$ represents *every* equivalence class of nondegenerate quadratic forms over k. Moving in this way from spaces defined over k_s and fixed by a Galois group to spaces defined over an extension of k is known as *Galois descent* ([13, §X.2], [6, §18]). In this situation, we write $G_k = \mathrm{Gal}(k_s/k)$, the absolute Galois group, in place of G. For simplicity we may, for instance, take $q(x) = x_1^2 + \cdots + x_n^2$ and $M = O_n(k_s)$, the usual orthogonal group over the separable closure.

We may consider other algebraic groups M as well. When $M = \mu_2 = \{\pm 1\} \cong O_1(l)$, the elements of $H^1(G, M)$ are in one-to-one correspondence with nonzero square classes of k which become equivalent to 1 over l: these are classes of nonzero elements of k whose square roots lie in l. This set $H^1(G, M)$ is in fact a group:

$$H^1(G, \mu_2(l)) = H^1(G, \{\pm 1\}) \cong (k^* \cap l^{*2})/k^{*2}.$$

In the special case $l = k_s$, $H^1(G, \mu_2)$ is isomorphic to k^*/k^{*2}. More generally, if $G = G_k$ and $M = \mu_p \subset k^*$, where μ_p is the set of pth roots of unity in k_s, then $H^1(G_k, \mu_p)$ is isomorphic to k^*/k^{*p}, and this relationship is known simply as *Kummer theory*.

In general, for M an algebraic group over k, we say that the elements of the set $H^1(G_k, M)$ are M-torsors (over G_k). With this terminology, the μ_n-torsors for subgroups μ_n of roots of unity in k^* are cyclic covers of k of degree n, which by Kummer theory are in one-to-one correspondence with nth-power classes of k^*, as above. More complicated algebraic groups M produce still more interesting torsors. For example, if $M = S_n$ (the constant algebraic group, independent from the base field), then the S_n-torsors are k-isomorphism classes of étale k-algebras of degree n; PGL_n-torsors are classes of central simple k-algebras of degree n; and if M is a simple split group of type F_4, the M-torsors are classes of simple exceptional Jordan algebras of dimension 27.

Moving to the second cohomology sets $H^2(G, M)$, we have interpretations for certain M, and we can then make use of natural connecting homomorphisms. For instance, when $M = \mu_2 \subset k^*$, the set $H^2(G_k, \mu_2)$ classifies central simple algebras of exponent 2 over k. In other words, the set is the 2-torsion in the Brauer group of k. With this interpretation we may simply express the Hasse-Witt invariant in cohomological language: $\mathrm{hw}(q) = \delta(q)$, where δ is the coboundary homomorphism

$$\delta \colon H^1(G_k, O_n) \longrightarrow H^2(G_k, \mu_2)$$

associated to a certain exact sequence of algebraic groups over the separable closure

$$1 \longrightarrow \{\pm 1\} \longrightarrow \tilde{O}_n \longrightarrow O_n \longrightarrow 1.$$

At this point, to simplify intuition, we move away from the general group cohomology notation $H^i(G, M)$. Instead, we use G to denote an algebraic group, not a Galois group, and write $H^i(k, G)$ for the ith cohomology set of the absolute Galois group $\mathrm{Gal}(k_s/k)$ with coefficients in a group G over k. This notation emphasizes the natural functorial nature of H^i: the map

$$l \longmapsto H^i(l, G)$$

is a functor from the category of field extensions of k to the category of pointed sets. Moreover, instead of describing an invariant by referring to the equivalence classes classified by $H^1(k, G)$ on which the invariant takes its values—as in "an invariant of quadratic forms"—we simply say that we are considering invariants of the algebraic group G; hence the discriminant and Hasse-Witt invariants are "invariants of O_n".

To make clear the difference between a polynomial invariant of O_n, such as a quadratic form, and an invariant of equivalence classes classified by $H^1(k, O_n)$, such as the discriminant, we will call the latter type a *cohomological invariant*. Indeed, a *cohomological invariant of a group G* is defined to be a transformation of functors

$$H^1(\quad, G) \longrightarrow H^i(\quad, M),$$

where M is a torsion discrete $\mathrm{Gal}(k_s/k)$-module, most often a small cyclic group with trivial action. We write $\mathrm{Inv}^d(G, M)$ for the set of all cohomological invariants of dimension d (that is, in H^d) of the algebraic group G with coefficients in M. In this way we say that the discriminant and the Hasse-Witt invariant are cohomological invariants of O_n with coefficients in $\mathbb{Z}/2\mathbb{Z}$ of dimensions 1 and 2, respectively.

Cohomological Invariants in Galois Cohomology is divided into two parts. The first part is a foundation for theory of cohomological invariants. Drawing on results from a series of lectures of Serre at the Collège de France, this presentation originated from Serre's course at UCLA in 2001, and Garibaldi wrote these expanded lecture notes. Readers may wish to have available an introduction to Galois cohomology such as [6, Ch. VII] or [12], as well as Serre's excellent overview of the problems motivating this area [10]. This first part also contains, as appendices, three letters—from M. Rost to Serre in 1991, from Serre to Garibaldi in 2002, and from B. Totaro to Serre in 2002—that illuminate some of the history of cohomological invariants as well as a geometric interpretation of the group of cohomological invariants.

Chapter I defines the notion of cohomological invariant and explores G-torsors, particularly *versal* G-torsors, which are suitably generic, specializing to G-torsors over extensions of the base field. Chapters II and III introduce the standard tools of Galois cohomology for local fields and function fields, respectively. Chapter IV proves the Compatibility Theorem, due to Rost, that cohomological invariants commute with base extension from the field k to discretely valued fields K with residue k. This result is used to prove a detection theorem: two cohomological invariants are identical if and only if they are identical on a versal torsor. After some results on restriction and corestriction of invariants in Chapter V, Chapter VI presents results on cohomological invariants of $(\mathbb{Z}/2\mathbb{Z})^n$, O_n, and SO_n, first with coefficients in $\mathbb{Z}/2\mathbb{Z}$ ("mod 2 invariants") and then with $\mathbb{Z}/2^m\mathbb{Z}$ coefficients. Chapter VI also gives invariants mod 2 for F_4 and discusses the case of hermitian forms.

Chapters VII–IX mainly consider the case of cohomological invariants of S_n, that is, invariants of étale algebras of rank n, denoted $\mathrm{Inv}(\mathrm{Et}_n, \ )$. Chapter VII presents, as Theorem 24.9, *Serre's splitting principle*. We say that an étale algebra is *multiquadratic* if it is decomposable as a product of étale algebras of rank 1 or 2. Then invariants of S_n with coefficients in any finite G_k-module M of order prime to the characteristic of k are detected on multiquadratic étale algebras:

Theorem. *If $a \in \mathrm{Inv}_k(\mathrm{Et}_n, M)$ satisfies $a(E) = 0$ for every multiquadratic étale algebra E/l (over every extension l of k), then $a = 0$.*

Recently F. Morel has announced a connection between a modified version of this principle and the motivic Barratt-Priddy-Quillen theorem.

After the splitting principle, Chapter VII proceeds to consider mod 2 and mod 2^m invariants of S_n. Chapter VIII broadens the notion of invariant to take values not in cohomology sets but in Witt rings of quadratic forms, and after giving examples of "Witt invariants" analogous to the cases of Chapter VI, treats the S_n case with applications to cubic resolvents of quartics and sextic resolvents of sextics.

Chapter IX gives explicit conditions for quadratic forms of rank ≤ 7 to be trace forms of étale algebras. It appears quite difficult to classify trace forms of étale algebras over a general base field. However, when k contains a primitive fourth root of unity, all trace forms of Galois étale algebras l/k are scaled Pfister forms [9]. Chapter IX applies the conditions for rank ≤ 7 to Noether's problem: whether for a finite group G, a field k_0, and an embedding $G \to GL_n(k_0)$, the subfield of $k_0(x_1, \ldots, x_n)$ fixed by G is a purely transcendental extension of k_0. Along the way, mod 2 cohomological invariants of 2-power cyclic groups and of double covers of A_6 and A_7 are introduced.

The second part of *Cohomological Invariants* is Merkurjev's exposition of Rost invariants of simply connected algebraic groups, with a section contributed by Garibaldi. These invariants, of dimension 3, represent a startling advance in a line of study begun with a suggestion of Serre that one seek a mod 3 invariant of F_4 and a mod 5 invariant of E_8, both in dimension 3. Dimension 3 invariants had previously been observed by Arason [1] for quadratic forms, and Merkurjev-Suslin proved that a natural dimension 3 invariant for SL_D, where D is a central simple algebra, is injective on algebras D of prime degree [8]. The exposition completes and expands the survey of Rost invariants contained in [6, §31B]—and certainly uses more advanced material than that of the first part of the book, relying on classifying varieties of algebraic groups, Chow groups, Rost's cycle modules, and K-cohomology groups.

Section 9 of Merkurjev's exposition defines Rost invariants, which take coefficients in a large $\mathrm{Gal}(k_s/k)$-module,

$$\mathbb{Q}/\mathbb{Z}(2) = \coprod_p \varinjlim \, (\mu_{p^m} \otimes \mu_{p^m}),$$

where μ_{p^m} denotes the group of p^m-th roots of unity in k_s^*. For a particular absolutely simple simply connected group G, however, the group $\mathrm{Inv}^3(G, \mathbb{Q}/\mathbb{Z}(2))_{\mathrm{norm}}$ of normalized (that is, trivial on the distinguished element of $H^1(k, G)$) dimension 3 invariants is finite and is generated by the Rost invariant. In this case, the coefficient module may be taken to be $\mu_{n_G} \otimes \mu_{n_G}$, where n_G is the order of the Rost invariant.

The second part culminates in section 10, which establishes in Theorem 10.7 an essential connection between the order n_G of $\mathrm{Inv}^3(G, \mathbb{Q}/\mathbb{Z}(2))_{\mathrm{norm}}$ and the Dynkin indices n_μ of representations μ of G:

Theorem. *For every absolutely simple simply connected group G,*

$$n_G = \gcd(n_\mu),$$

where μ ranges over all representations of G.

In sections 11–15 the orders n_G are calculated for all such groups G of classical type, and Garibaldi's section 16 gives n_G for G of exceptional type. Two appendices complete the exposition, the first defining $H^{d+1}(G, \mathbb{Q}/\mathbb{Z}(d))$, and the second giving Dynkin indices of absolutely simple simply connected algebraic groups, encapsulating the results of sections 11–16.

The volume is well written and is a substantial addition to the literature. It fashions a suitable foundation for a deep area of research still under development and provides, for the first time, details of a far-reaching advance achieved by Rost, to whom the volume is fittingly dedicated.

Acknowledgment

I thank E. Bayer-Fluckiger, J. Mináč, M. Mossinghoff, Z. Reichstein, M. Rost, A. Schultz, and B. Totaro for clarifications, comments, and corrections.

References

1. J. K. Arason. Cohomologische invarianten quadratischer Formen. *J. Algebra* **36** (1975), no. 3, 448–491. MR0389761 (52:10592)
2. N. Bourbaki. *Éléments d'histoire des mathématiques*, deuxième édition revue, corrigée, augmentée. Paris: Hermann, 1969. MR0243970 (39:5288)
3. R. Elman and T. Y. Lam. Classification theorems for quadratic forms over fields. *Comment. Math. Helv.* **49** (1974), 373–381. MR0351997 (50:4485)
4. C. F. Gauss. *Disquisitiones arithmeticae.* Sectio quarta de congruentiis secundi gradus, art. 268. *Werke*, vol. 1, 301–304. Hildesheim: Georg Olms Verlag, 1973. MR0837656 (87f:01105)
5. F. Q. Gouvêa (Reviewer). *Cohomology of number fields* by Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Bull. Amer. Math. Soc. (N.S.)* **39** (2002), no. 1, 101–107.
6. M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol. *The book of involutions.* Colloquium Publications, vol. 44. Providence, RI: American Mathematical Society, 1998. MR1632779 (2000a:16031)
7. S. Mac Lane. Origins of the cohomology of groups. *Enseign. Math.* (2) **24** (1978), no. 1-2, 1–29. MR0497280 (81j:01030)
8. A. S. Merkurjev and A. A. Suslin. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism (Russian). *Izv. Akad. Nauk SSSR* **46** (1982), 1011–1046. English translation, *Math. USSR Izv.* **21** (1983), 307–340. MR0675529 (84i:12007)
9. J. Mináč and Z. Reichstein. Trace forms of Galois extensions in the presence of a fourth root of unity. *Int. Math. Res. Not.* **2004**, no. 8, 389–410. MR2036337
10. J-P. Serre. Cohomologie galoisienne: progrès et problèmes. Séminaire Bourbaki, 46ème année, 1993–1994, n° 783. *Astérisque* **227** (1995): 229–257. MR1321649 (97d:11063)
11. J-P. Serre. *A course in arithmetic.* Translation (1973) of *Cours d'arithmétique.* New York: Springer-Verlag, 1973. MR0344216 (49:8956)
12. J-P. Serre. *Galois cohomology.* Translation (1997), subsequently corrected, of the fifth, revised edition (1994) of *Cohomologie galoisienne.* Berlin: Springer-Verlag, 2002. MR1324577 (96b:12010)
13. J-P. Serre. *Local fields.* Translation (1979) of the second edition (1968) of *Corps locaux.* Graduate texts in mathematics, vol. 67. New York: Springer-Verlag, 1979. MR0554237 (82e:12016)
14. H. Weyl. *The classical groups: their invariants and representations*, 2nd ed. Princeton: Princeton University Press, 1946. MR1488158 (98k:01049)

John Swallow
Davidson College
E-mail address: joswallow@davidson.edu