Introduction to quadratic forms over fields

Uniwersytet Śląski
http://www.math.us.edu.pl/~pgladki/

November 11, 2013

Quadratic forms

Let k be a field, $\mathrm{char} k \neq 2$, V a finitely dimensional vector spaces over k.

A **quadratic form** is a function $q : V \to k$ such that the associated function $b_q : V \times V \to k$ defined by

$$b_q(u, v) = \frac{1}{2}(q(u + v) - q(u) - q(v))$$

is bilinear, and

$$q(av) = a^2 q(v), \text{ for } a \in k \text{ and } v \in V.$$

The pair (V, q) shall be called a **quadratic space**.

The dimension of the space V will be called the **dimension** of the form q, $\dim q$.

Isometry of quadratic forms

Two quadratic forms q_1 and q_2 are called **isometric** if for their respective quadratic spaces (V_1, q_1) and (V_2, q_2) there is an isomorphism of vector spaces $\phi : V_1 \to V_2$ such that

$$q_2(\phi(v)) = q_1(v) \text{ for } v \in V_1.$$

Two isometric forms will be denoted by $q_1 \cong q_2$.

Diagonalizable forms

Let (V, q) be a quadratic space.

If $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a basis of V, then the matrix $B = [b_q(v_i, v_j)]$ will be called the **matrix of** q with respect to the basis $\mathcal{B}$.

If $\mathcal{B}_1$ and $\mathcal{B}_2$ are two different bases of V, and B_1 and B_2 two different matrices of q in $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively, then $B_2 = PB_1P^T$ for a nonsingular matrix P.

If $\mathrm{char}k \neq 2$ then there exists a basis $\mathcal{D}$ where q has a diagonal matrix D, that is, q is **diagonalizable**.

If $(d_1, \ldots, d_n)$ are the entries on the main diagonal of D, then the form q will be identified with the tuple $(d_1, \ldots, d_n)$.

Value sets of quadratic forms

For a quadratic form q on V, the set of nonzero values of the form q is denoted as $D_k(q)$.

The elements in $D_k(q)$ are said to be **represented** by q over k.

Since $q(av) = a^2 q(v)$ for $a \in F$, it follows that the set $D_k(q)$ consists of whole cosets of the multiplicative group k^* modulo the subgroup k^{*2} of squares.

Hence, $D_k(q)$ can be viewed as a subset of the group k^*/k^{*2} of square classes of k.

Dimension and determinant

For a quadratic space (V, q), the dimension of V is said to be the **dimension** of the quadratic form q, written as $\dim q$.

If $\mathcal{B}_1$ and $\mathcal{B}_2$ are two different bases of V, and B_1 and B_2 two different matrices of q in $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively, then, since $B_2 = PB_1P^T$ for a nonsingular matrix P, $\det B_1$ and $\det B_2$, if nonzero, lie in the same coset $(\det B)k^{*2}$, which is said to be the **determinant** of the form q, written as $\det q$.

If $\det B = 0$ for some basis $\mathcal{B}$, we set $\det q = 0$.

Forms with nonzero determinant are called **nonsingular.**

This is equivalent to the fact that the map $V \to V^*$ given by

$$v \mapsto b_q(\cdot, v)$$

is an isomorphism of V onto the dual space V^*.

Orthogonal direct sum

If (V_1, q_1) and (V_2, q_2) are quadratic spaces, then so is $(V_1 \oplus V_2, q_1 \perp q_2)$, where

$$(q_1 \perp q_2)(v_1, v_2) = q_1(v_1) + q_2(v_2).$$

Direct orthogonal sum of nonsingular quadratic forms is nonsingular.

If $q_1 = (a_1, \ldots, a_n)$ and $q_2 = (b_1, \ldots, b_m)$ are diagonalized forms, then

$$q_1 \perp q_2 = (a_1, \ldots, a_n, b_1, \ldots, b_m).$$

The very useful Witt cancellation theorem states that if q is nonsingular and $q \perp q_1 \cong q \perp q_2$,then $q_1 \cong q_2$.

Tensor product

The tensor product $V_1 \otimes V_2$ can be equipped with the structure of a quadratic space $(V_1 \otimes V_2, q)$, where the associated bilinear form b_q equals the tensor product $b_{q_1} \otimes b_{q_2}$. Hence

$$b_q(v_1 \otimes v_2, v_1' \otimes v_2') = b_{q_1}(v_1, v_1') \cdot b_{q_2}(v_2, v_2')$$

for all simple tensors $v_1 \otimes v_2, v_1' \otimes v_2'$ in $V_1 \otimes V_2$.

The form q is then called the **tensor product** of the quadratic forms q_1 and q_2, written as $q_1 \otimes q_2$.

Tensor product of nonsingular quadratic forms is nonsingular.

If $q_1 = (a_1, \ldots, a_n)$ and $q_2 = (b_1, \ldots, b_m)$ are diagonalized forms, then

$$q_1 \otimes q_2 = (a_1 b_1, \ldots, a_1 b_m, a_2 b_1, \ldots, a_2 b_m, \ldots, a_n b_1, \ldots, a_n b_m).$$

Isotropic, anisotropic and hyperbolic forms

A quadratic form q is said to be **isotropic** if there exists a nonzero vector $v \in V$ so that $q(v) = 0$.

A simple but fundamental example of a nonsingular isotropic form is the **hyperbolic plane.** This is the two-dimensional form h with diagonalization $(1, -1)$ in some basis of the plane.

If a quadratic form q is isotropic, then it splits off a hyperbolic plane h_1, i.e.

$$q \cong h_1 \perp q_1$$

for some quadratic form q_1. Continuing with q_1, we ultimately obtain a decomposition

$$q \cong h_1 \perp \ldots \perp h_i \perp q_a,$$

where $h_1, \ldots, h_i$ are hyperbolic planes and q_a is anisotropic.

By Witt cancellation, the form q_a, called the **anisotropic part** of q, is unique up to isometry, and also, the number i (called the **Witt index** of q) is unique.

If $q_a = 0$, the form q is said to be **hyperbolic.**

Pfister forms

A quadratic form $(1, a)$, $a \in k^*$, is called **one-fold Pfister form,** and an n-fold tensor product $(1, a_1) \otimes \ldots \otimes (1, a_n)$ of one-fold Pfister form is called an n-**fold Pfister form.**

It is an important property of Pfister forms that if a Pfister form is isotropic, then it is necessarily hyperbolic.

Another fundamental property is that for a Pfister form q, the value set $D_k(q)$ is a group under multiplication.

Level of a field

Recall that for a ring A, the level $s(A)$ is the smallest natural number n such that $-1 \in A$ is a sum of n squares in A or ∞ if -1 is not a sum of squares in A.

The level of a nonformally real field (i.e. such that -1 is a sum of squares) is always a power of two.

This was proved by Pfister as a simple consequence of the fact that for a Pfister form q, the value set $D_k(q)$ is a group under multiplication.

Indeed, assume that k is a nonreal field with $s = s(k)$ and let $2^n \leq s < 2^{n+1}$.

Then $-1 = A + B$, where A is a sum of 2^n and B a sum of less than 2^n squares in k.

By the group property, it follows that $-1 = (1 + B)/A$ is a sum of 2^n squares in k , and so $s = 2^n$.

Similarity of quadratic forms

Two quadratic forms q and g over k are said to be **similar** (or **Witt equivalent**), written as $q \sim g$, if their anisotropic parts are isometric, $q_a \cong g_a$.

An easy observation is that for quadratic forms q and g over k:

$$\dim q = \dim g \text{ and } q \sim g \Rightarrow q \cong g.$$

For a nonsingular quadratic form q over k, we write $\langle q \rangle$ for the class of quadratic forms similar to q.

This is the **Witt class** of q.

Group rings

Recall the construction of a group ring.

Let G be a group, written multiplicatively, and let R be a ring.

The **group ring** of G over R, which we will denote by $R[G]$, is the set of mappings $f : G \to R$ of finite support, where the product αf of a scalar $\alpha \in R$ and a vector (or mapping) f is defined as the vector

$$x \mapsto \alpha \cdot f(x),$$

and the sum of two vectors f and g is defined as the vector

$$x \mapsto f(x) + g(x).$$

To turn the additive group $R[G]$ into a ring, we define the product of f and g to be the vector

$$x \mapsto \sum_{uv=x} f(u)g(v) = \sum_{u \in G} f(u)g(u^{-1}x).$$

The summation is legitimate because f and g are of finite support, and the ring axioms are readily verified.

Witt ring

Witt classes of nonsingular quadratic forms over k with addition and multiplication induced by direct orthogonal sum and tensor product form a commutative ring called the **Witt ring** of the field k and denoted as $W(k)$.

The Witt ring has the following description in terms of generators and relations.

Consider the integral group ring $\mathbb{Z}[k^*/k^{*2}]$ of the group of square classes of the field k.

Then

$$W(k) = \mathbb{Z}[k^*/k^{*2}]/J,$$

where J is the ideal in the group ring $\mathbb{Z}[k^*/k^{*2}]$ generated by the set,

$$\{[a] + [b] - [c] - [d] : (a, b) \cong (c, d)\} \cup \{[1] + [-1]\}.$$

Here $[a]$ denotes the sqare class of $a \in k^*$.

This is a straightforward consequence of the Witt theorem on chain equivalence of quadratic forms

Dimension index and discriminant

For a Witt class $\langle q \rangle$, we define the **dimension-index**

$$e\langle q \rangle = \dim q (\mod 2) \in \mathbb{Z}/2\mathbb{Z}$$

and the **discriminant**

$$d\langle q \rangle = (-1)^{\frac{1}{2}n(n-1)} \det q \in k^*/k^{*2},$$

where $n = \dim q$.

These are well-defined invariants of the similarity class.

Moreover,

$$e : W(k) \to \mathbb{Z}/2\mathbb{Z}$$

is a ring epimorphism.

Its kernel consists of the Witt classes $\langle q \rangle$ with even-dimensional q and is said to be the **fundamental ideal** of the Witt ring $W(k)$, written as $I(k)$.

Powers of fundamental ideal

Further,

$$d : W(k) \to k^*/k^{*2}$$

is a well-defined map, but it fails to be a homomorphism of the additive group $W(k)$ (for instance, take $k = \mathbb{R}$).

However, if we restrict the discriminant map to the fundamental ideal $I(k)$, we obtain a surjective group homomorphism

$$d : I(k) \to k^*/k^{*2}$$

of the additive group $I(k)$ onto the group of square classes.

Interestingly enough, the kernel of this homomorphism equals $I^2(k)$, the additive group of the square of the fundamental ideal.

This prompts looking at higher powers $I^n(k)$ of the fundamental ideal.

An elementary observation is that $I^n(k)$ is generated as an Abelian group by the Witt classes of all n-fold Pfister forms over k. Much deeper and difficult to prove is the following theorem known as the Hauptsatz:

Theorem (Arason-Pfister Hauptsatz)

For a positive-dimensional anisotropic quadratic form q over a field k, if $\langle q \rangle \in I^n(k)$, then $\dim q \geq 2^n$.

As a consequence, we get the intersection property in the Witt ring $W(k)$ of the field k:

$$\bigcap_{n=0}^{\infty} I^n(k) = 0.$$

Minimal prime ideals and orderings

Recall that a prime ideal $\mathfrak{p}$ of a commutative ring R is said to be a **minimal prime ideal over an ideal** I if it is minimal among all prime ideals containing I.

Note that we do not exclude I even if it is a prime ideal.

A prime ideal is said to be a **minimal prime ideal** if it is a minimal prime ideal over the zero ideal.

The set of all minimal prime ideals of R will be denoted by $MinSpec(R)$.

An **ordering** of the field k is a subset $P \subset k$ such that

1. $P + P \subset P$
2. $P \cdot P \subset P$
3. $P \cap -P = \{0\}$
4. $P \cup -P = k$

We can think of P as of the set of all non-negative elements with respect to a certain ordering relation.

Prime ideals in Witt rings

Theorem (Harrison, Lorenz, Leicht)

1. *If the Witt ring $W(k)$ has a prime ideal $\mathfrak{p} \neq I(k)$, then the field k is formally real and the set*

$$P = \{a \in k^* : \langle 1, -a \rangle \in \mathfrak{p}\}$$

   defines an ordering of the field k.

2. *Let k be a formally real field and let P be an ordering of k. Let $\mathfrak{p}_0$ be the ideal of the Witt ring $W(k)$ generated by the set*

$$\{\langle 1, -a \rangle \in W(k) : a \in P\}.$$

   Then $\mathfrak{p}_0$ is a minimal prime ideal of the Witt ring $W(k)$. Moreover, $\mathfrak{p}_0 \subset I(k)$ and $\mathfrak{p}_0 \neq I(k)$.

Hence, $MinSpecW(k) = \{I(k)\}$ when the field k is nonreal, and $MinSpecW(k)$ contains at least one nonmaximal minimal prime ideal when the field k is formally real.

Signatures

Each ordering P of a formally real field k gives rise to a signature homomorphism

$$sgn_P : W(k) \to \mathbb{Z}$$

sending the class $\langle q \rangle$ to the signature of the form q for the ordering P.

The map

$$\sigma : X(k) \to MinSpecW(k), P \mapsto \ker sgnP$$

is a bijective correspondence between the set $X(k)$ of all orderings of the field k and the minimal prime ideals of the Witt ring $W(k)$.

The set $X(k)$ can be given the induced Zariski topology from the prime spectrum and this turns $X(k)$ into a Boolean space (compact, Hausdorff, and totally disconnected).

Nilradical and torsion

For a nilpotent element $x \in W(k)$, we obviously have $e(x) = 0$ and hence $NilW(k) \subset I(k)$.

When k is non-formally real field, we actually have $NilW(k) = I(k)$.

When k is formally real, we observe that nilpotent elements in $W(k)$ have zero signatures at every ordering of k, and so the nilradical $NilW(k)$ is contained in the intersection of the kernels of all signature homomorphisms.

Since the latter are all minimal prime ideals in $W(k)$, their intersection actually equals the nilradical $NilW(k)$.

For a nonreal field k of level s, the unit element $\langle 1\rangle \in W(k)$ has finite order 2^s in the additive group $W(k)$ and so $2^s W(k) = 0$.

This is an immediate consequence of the theory of Pfister forms.

Thus, $W(k)$ is torsion group and every element is two-primary torsion.

When k is formally real, torsion elements have zero signatures at all orderings of the field, so it follows that $TorsW(k) \subset NilW(k)$.

A deeper result says that, in fact, for every formally real field k,

$$TorsW(k) = NilW(k).$$

This is a consequence of the local–global principle for torsion elements of Witt rings first proved by Pfister:

Theorem (Pfister local-global principle)

Let k be a formally real field and let q be an anisotropic quadratic form over k. For every ordering P of the field k, choose a real closure k_P inducing the ordering P on k. The following statements are equivalent.

1. $\langle q \rangle$ *is a torsion element of the Witt ring* $W(k)$.
2. $\langle q \rangle_{k_P} = 0$ *in the Witt ring* $W(k_P)$, *for every ordering* P *of the field* k.
3. $sgn_P \langle q \rangle = 0$ *for all orderings* P *of the field* k.

Moreover, every torsion element in W(F) is two-primary torsion.

Pythagorean fields

A field k is said to be Pythagorean when every sum of squares of nonzero elements of k is a square of a nonzero element in k .

Thus, a Pythagorean field is automatically formally real.

For all fields k except for Pythagorean fields, the set $ZD(W(k))$ of zero divisors of the Witt ring $W(k)$ coincides with the ideal $I(k)$.

And for a Pythagorean field k, an element of the Witt ring of k is a zero divisor in $W(k)$ if and only if it lies in a minimal prime ideal of the ring $W(k)$.

Hence for a Pythagorean field F,

$$ZD(W(F)) = \bigcup \{\ker sgn_P : P \in X(k)\}.$$

The following theorem gives an important characterization of Pythagorean fields in terms of their Witt rings.

Theorem

For a formally real field k,

$$k \text{ is Pythagorean } \Leftrightarrow TorsW(k) = 0 \Leftrightarrow NilW(k) = 0.$$

Classification of quadratic forms over Pythagorean fields

The above theorem implies a solution of the classification problem for quadratic forms over Pythagorean fields.

If q and g are nonsingular quadratic forms over a Pythagorean field k, then $q \cong g$ if and only if $\dim q = \dim g$ and $sgn_P q = sgn_P g$ for every ordering P of the field k.

Connections with K-theory and group cohomology

Uniwersytet Śląski
http://www.math.us.edu.pl/~pgladki/

November 11, 2013

Quaternion algebras

Recall that a **central simple algebra** over a field k is a finite-dimensional associative k-algebra A, which is a **simple ring** (i.e. a non-zero ring that has no two-sided ideal besides the zero ideal and itself), and for which the center is exactly k.

A **quaternion algebra** over a field k is a central simple algebra A over k that has dimension 4 over k.

Every quaternion algebra becomes the matrix algebra by extending scalars, i.e. for a suitable field extension F of k, $A \otimes_k F$ is isomorphic to the 2×2 matrix algebra over F.

When the coefficient field k does not have characteristic 2, every quaternion algebra over k can be described as a 4-dimensional k-vector space with basis $\{1, i, j, k\}$, with the following multiplication rules: $i^2 = a$, $j^2 = b$, $ij = k$, $ji = -k$, where a and b are any given nonzero elements of k called **structure constants**.

Thus the quaternion algebra over k with structure constants shall be denoted by $\left(\frac{a,b}{k}\right)$.

A quaternion algebra $\left(\frac{a,b}{k}\right)$ is either a division algebra or isomorphic to the matrix algebra of 2×2 matrices over k, in which case it is termed **split.**

The **norm form**

$$N(t + xi + yj + zk) = t^2 - ax^2 - by^2 + abz^2$$

defines a structure of division algebra if and only if the norm is an anisotropic quadratic form.

The conic $C(a, b)$ defined by

$$ax^2 + by^2 = z^2$$

has a point (x, y, z) with coordinates in k in the split case.

Hasse algebra

For a nonsingular diagonal quadratic form $q = (a_1, \ldots, a_n)$ with the entries a_i in a field k of characteristic $\neq 2$, we define **the Hasse algebra** $H(q)$ of the form q as the following tensor product of quaternion algebras:

$$H(q) = \bigotimes_{1 \leq i \leq j \leq n} \left(\frac{a_i, a_j}{k} \right).$$

If $q = (a_1, \ldots, a_n)$ and $g = (b_1, \ldots, b_n)$ are equivalent quadratic forms, then $H(q) \cong H(g)$.

In other words, the Hasse algebra of a quadratic form q is uniquely determined up to algebra isomorphism and is an equivalence invariant.

Opposite algebra

Let A be an arbitrary k-algebra.

We associate with A a new k-algebra, the **opposite algebra** A^{op}, defined as follows: as a vector space the new algebra is identical with A, and a new multiplication is defined by

$$a \star b = b \cdot a, \text{ for all } a, b \in A.$$

The centers of A and A^{op} coincide.

Hence A is a central k-algebra if and only if A^{op} is a central k-algebra.

It is also obvious that every ideal I in the algebra A is also an ideal in the algebra A^{op} and conversely.

Hence the opposite algebra of a central simple algebra is itself a central simple algebra.

Theorem

Let A be a central simple algebra of dimesion n. Then

$$A \otimes A^{op} \cong M_n(k)$$

Observe that for every quaternion algebra A there is an algebra isomorphism:

$$A \cong A^{op}.$$

Indeed, for a quaternion algebra $A = \left(\frac{a,b}{k}\right)$ described as a 4-dimensional k-vector space with basis $\{1, i, j, k\}$ and the following multiplication rules: $i^2 = a$, $j^2 = b$, $ij = k$, $ji = -k$, consider the conjugation operation $c : A \to A$

$$c(p) = c(x_0 1 + x_1 i + x_2 j + x_3 k) = \overline{p} = x_0 1 - x_1 i - x_2 j - x_3 k.$$

It can be easily seen to be an automorphism of the k-vector space A.

Moreover

$$c(pq) = \overline{pq} = \overline{q} \cdot \overline{p} = \overline{p} \star \overline{q} = c(p) \star c(q).$$

Brauer group of a field

Two finite-dimensional k-algebras A and B are said to be **similar,** written $A \sim B$, if there are integers n and m such that

$$M_n(k) \otimes A \cong M_m(k) \otimes B.$$

This is an equivalence relation whose equivalence classes will be denoted by $[A]$, which is compatible with tensor product.

Denote by $Br(k)$ the set of all equivalence classes of all central simple algebras over k.

It is made into an Abelian group by defining the product of two similarity classes $[A], [B] \in Br(k)$ as follows:

$$[A] \cdot [B] = [A \otimes B].$$

The neutral element is the similarity class of the field k, which is equal to all matrix algebras, i. e. $[k] = [M_n(k)]$, for all positive integers n.

The inverse element of the class $[A]$ is the class of the opposite algebra $[A^{op}]$.

If A is a quaternion algebra, then $[A]^{-1} = [A]$, or, in other words, $[A]^2 = 1$ in the Brauer group.

Recall that a quaternion algebra A is either a division algebra or is isomorphic to the matrix algebra $M_2(k)$.

For a division quaternion algebra A the class $[A]$ has order 2 in $Br(k)$.

On the other hand, if $A \cong M_2(k)$, then $[A] = 1$ in $Br(k)$.

For the quaternion algebra $A = \left(\frac{a,b}{k}\right)$ we use the following simplified notation for the similarity class $[A]$:

$$[A] = [a, b]_k.$$

We will write $Br_2(k)$ for the subset of elements of order ≤ 2 in the Brauer group $Br(k)$.

Since $Br(k)$ is an Abelian group, it follows that $Br_2(k)$ is a subgroup of $Br(k)$.

All quaternion algebra classes belong to $Br_2(k)$.

By commutativity of the group, also the products of quaternion algebra classes belong to $Br_2(k)$.

This turns our attention to the subgroup $Quat(k)$ of Brauer group $Br(k)$ generated by all quaternion algebra classes.

We thus have:

$$Quat(k) \subset Br_2(k) \subset Br(k).$$

It is a deep theorem proved in 1981 by Merkurjev (to be discussed later) that actually $Quat(k) = Br_2(k)$ for every field k.

Hasse invariant

For a nonsingular quadratic form $q = (a_1, \ldots, a_n)$ over a field k of characteristic $\neq 2$, the **Hasse invariant** $h(q)$ of the form q is defined to be the similarity class of the Hasse algebra $H(q)$ of the form q in the Brauer group of the field k:

$$h(q) = [H(q)] = \prod_{1 \leq i \leq j \leq n} [a_i, a_j]_k \in Br(k).$$

Theorem (Classification theorem for quadratic forms of dimension ≤ 3)

Let q and g be nonsingular quadratic forms over a field k of characteristic $\neq 2$ and let $\dim q \leq 3$ and $\dim g \leq 3$. Then, we have

$$q \cong g \Leftrightarrow \dim q = \dim g, \det q = \det g, h(q) = h(g).$$

Witt invariant

The Hasse invariant, like the determinant, is an invariant for equivalence but not for similarity of quadratic forms.

However, as in the case of the determinant, one can correct this by multiplying the Hasse invariant with a suitable factor.

This works in all dimensions, but we shall restrict attention to even-dimensional forms.

We define

$$w(q) = h(q) \cdot [-1,-1]^{n(n+1)/2}, \text{ where } \dim q = 2n.$$

It turns out that the new function is a similarity invariant on the set of even-dimensional forms with discriminant $1 \in k^*/k^{*2}$ and this set is precisely $I^2(k)$.

Hence for $\langle q \rangle \in I^2(k)$, we set $w(\langle q \rangle) = w(q) \in Br(k)$, and call it the **Witt invariant** of the form q, and of the class $\langle q \rangle \in I^2(k)$.

Thus $w(q) = \begin{cases} h(q) \cdot [-1,-1], & \text{when } 2n \equiv 2,4 \mod 8, \\ h(q), & \text{when } 2n \equiv 0,6 \mod 8. \end{cases}$.

Notice that $w(q) \in Quat(k)$.
Since

$$\begin{aligned} w(x, -ax, -bx, abx) &= w(1, -a, -b, ab) = [a, b], \\ w((1, -a) \otimes (1, -b) \otimes (1, -c)) &= 1, \end{aligned}$$

forall $x, a, b, c \in k^*$, it easily follows that the map $w : I^2(k) \to Quat(k)$ is a group epimorphism and

$$I^3(k) \subset \ker w.$$

It has been of central importance for quadratic form theory whether actually $I^3(F) = \ker w$.

This was proved for various classes of fields k including local and global fields and fields of transcendence degree ≤ 1 over a real closed field.

The question whether $I^3(k) = \ker w$ was resolved by Merkurjev in 1981 as a part of an even more spectacular result discussed below.

Grothendieck group of a commutative monoid

Let M be a commutative monoid.

To construct the **Grothendieck group** one forms the Cartesian product

$$M \times M$$

and we say that (m_1, m_2) is equivalent to (n_1, n_2) if, for some element k of M,

$$m_1 + n_2 + k = m_2 + n_1 + k.$$

It is easy to check that the addition operation defined coordinate-wise is compatible with the equivalence relation.

The set of all equivalence classes with induced addition forms a group.

The identity element is now any element of the form (m, m), and the inverse of (m_1, m_2) is (m_2, m_1).

K_0

Let R be a ring.

The **functor** K_0 takes a ring R to the Grothendieck group of the set of isomorphism classes of its finitely generated projective modules, regarded as a monoid under direct sum.

Note that projective modules over a field k are simply vector spaces and $K_0(k)$ is isomorphic to $\mathbb{Z}$, by dimension.

K_1

The **infinite general linear group** is the direct limit of the inclusions $GL_n(R) \to GL_{n+1}(R)$ as the upper left block matrix.

It is denoted by $GL(R)$ and can be interpreted as invertible infinite matrices which differ from the identity matrix in only finitely many places.

Hyman Bass provided the following definition of $K_1(R)$: it is the abelianization of the infinite general linear group:

$$K_1(R) = \mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)]$$

The commutator subgroup agrees with the group generated by elementary matrices $E(R) = [GL(R), GL(R)]$, by Whitehead's lemma.

For a commutative ring R one can define a determinant $\det : GL(R) \to R^*$ to the group of units of R, which vanishes on $E(R)$ and thus descends to a map det:

$$K_1(R) \to R^*.$$

As $E(R) \lhd SL(R)$, one can also define the special Whitehead group $SK_1(R) = SL(R)/E(R)$.

The determinant map splits via the map

$$R^* \to GL_1(R) \to K_1(R)$$

(unit in the upper left corner), and hence is onto, and has the special Whitehead group as kernel, yielding the split short exact sequence:

$$1 \to SK_1(R) \to K_1(R) \to R^* \to 1,$$

which is a quotient of the usual split short exact sequence defining the special linear group, namely

$$1 \to \mathrm{SL}(R) \to \mathrm{GL}(R) \to R^* \to 1.$$

The determinant is split by including the group of units $R* = GL_1(R)$ into the general linear group $GL(R)$, so $K_1(R)$ splits as the direct sum of the group of units and the special Whitehead group:

$$K_1(R) \cong R^* \oplus SK_1(R).$$

When R is a Euclidean domain (e.g. a field, or the integers) $SK_1(R)$ vanishes, and the determinant map is an isomorphism from $K_1(R)$ to R^*.

This is false in general for PIDs, thus providing one of the rare mathematical features of Euclidean domains that do not generalize to all PIDs.

Steinberg group

For a given ring R the easiest way to define the Steinberg group is via generators and relations.

The **unstable Steinberg group** of order r over R, $St_r(R)$, is defined by the generators $x_{ij}(\lambda)$, $1 \leq i \neq j \leq r$, $\lambda \in R$, subject to the **Steinberg relations:**

$$\begin{aligned} x_{ij}(\lambda)x_{ij}(\mu) &= x_{ij}(\lambda+\mu) & \\ [x_{ij}(\lambda), x_{jk}(\mu)] &= x_{ik}(\lambda\mu) & \text{for } i \neq k \\ [x_{ij}(\lambda), x_{kl}(\mu)] &= 1 & \text{for } i \neq l, j \neq k \end{aligned}$$

The **stable Steinberg group,** $St(R)$, is the direct limit of the system $St_r(R) \to St_{r+1}(R)$.

Mapping $x_{ij}(\lambda) \mapsto e_{ij}(\lambda)$ yields a group homomorphism $\phi : St(R) \to GL(R)$, where $e_{pq}(\lambda) = I + a_{pq}(\lambda)$, I is the identity matrix, $a_{pq}(\lambda)$ is the matrix with λ in the (p, q) entry and zeros elsewhere, and $p \neq q$.

As the elementary matrices generate the commutator subgroup, this map is onto the commutator subgroup.

Chain and cochain complexes

A **chain complex** $(A_\bullet, d_\bullet)$ is a sequence of abelian groups or modules $\ldots, A_2, A_1, A_0, A_{-1}, A_{-2}, \ldots$ connected by homomorphisms (called **boundary operators**) $d_n : A_n \to A_{n-1}$, such that the composition of any two consecutive maps is zero:

$$d_n \circ d_{n+1} = 0 \text{ for all } n.$$

They are usually written out as:

$$\cdots \to A_{n+1} \xrightarrow{d_{n+1}} A_n \xrightarrow{d_n} A_{n-1} \xrightarrow{d_{n-1}} A_{n-2} \to \cdots \xrightarrow{d_2} A_1 \xrightarrow{d_1} A_0 \xrightarrow{d_0} A_{-1} \xrightarrow{d_{-1}} A_{-2} \xrightarrow{d_{-2}} \cdots$$

A variant on the concept of chain complex is that of **cochain complex.**

A cochain complex $(A^\bullet, d^\bullet)$ is a sequence of abelian groups or modules $\ldots, A^{-2}, A^{-1}, A^0, A^1, A^2, \ldots$ connected by homomorphisms $d^n \colon A^n \to A^{n+1}$ such that the composition of any two consecutive maps is zero:

$$d^{n+1} d^n = 0 \text{ for all } n.$$

This is usually written as

$$\cdots \to A^{-2} \xrightarrow{d^{-2}} A^{-1} \xrightarrow{d^{-1}} A^0 \xrightarrow{d^0} A^1 \xrightarrow{d^1} A^2 \to \cdots \to A^{n-1} \xrightarrow{d^{n-1}} A^n \xrightarrow{d^n} A^{n+1} \to \cdots .$$

The index n in either A_n or A^n is referred to as the **degree** (or dimension).

There is a natural notion of a morphism between chain complexes called a **chain map.**

Given two complexes $M*$ and $N*$, a chain map between the two is a series of homomorphisms from M_i to N_i such that the entire diagram involving the boundary maps of $M*$ and $N*$ commutes.

Group cohomology and homology

Let G be a finite group.

A G-module is an abelian group M together with a group action of G on M, with every element of G acting as an automorphism of M.

In the sequel we will write G multiplicatively and M additively.

For $n \geq 0$, let $C^n(G, M)$ be the group of all functions $G^n \to M$.

This is an abelian group; its elements are called the n-**cochains.**

The **coboundary homomorphisms** $d^n : C^n(G, M) \to C^{n+1}(G, M)$ are defined as

$$\begin{aligned}
&(d^n\varphi)(g_1, \ldots, g_{n+1}) \\
&\quad = \quad g_1 \cdot \varphi(g_2, \ldots, g_{n+1}) \\
&\quad + \quad \sum_{i=1}^{n} (-1)^i \varphi(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) \\
&\quad + \quad (-1)^{n+1} \varphi(g_1, \ldots, g_n)
\end{aligned}$$

The crucial thing to check here is $d^{n+1} \circ d^n = 0$, thus we have a cochain complex.

For $n \geq 0$, define the group of n-**cocycles** as:

$$Z^n(G, M) = \ker(d^n)$$

and the group of n-**coboundaries** as

$$\begin{cases} B^0(G, M) = 0 \\ B^n(G, M) = \mathrm{im}(d^{n-1}), \ \ n \geq 1 \end{cases}$$

and the n-**th cohomology group** as:

$$H^n(G, M) = Z^n(G, M)/B^n(G, M).$$

The n-**th homology groups** $H_n(G, M)$ can be defined dually via chain complexes.

K_2

The right definition of K_2 was given by John Milnor.

It can be defined in three equivalent ways as:

1. the center of the Steinberg group $St(R)$, or
2. the kernel of the map $\phi\colon\ \mathrm{St}(R) \to \mathrm{GL}(R)$, or
3. the **Schur multiplier** of the group of elementary matrices, that is the second homology group $H_2(E(R), \mathbb{Z})$.

Matsumoto's theorem states that for a field k, the second K-group is given by

$$K_2(k) = k^\times \otimes_{\mathbb{Z}} k^\times / \langle a \otimes (1-a) \mid a \neq 0, 1 \rangle.$$

Tensor algebra

Let V be a vector space over a field k.

For any nonnegative integer k, we define the k-th tensor power of V to be the tensor product of V with itself k times:

$$T^k V = V^{\otimes k} = V \otimes V \otimes \cdots \otimes V.$$

We then construct $T(V)$ as the direct sum of $T^k V$ for $k \in \mathbb{N}$:

$$T(V) = \bigoplus_{k=0}^{\infty} T^k V = K \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots .$$

The multiplication in $T(V)$ is determined by the canonical isomorphism

$$T^k V \otimes T^\ell V \to T^{k+\ell} V$$

given by the tensor product, which is then extended by linearity to all of $T(V)$.

This multiplication rule implies that the tensor algebra $T(V)$ is naturally a graded algebra with $T^k V$ serving as the graded k-subspace.

Milnor K-theory

The calculation of K_2 of a field k led Milnor to the following ad hoc definition of "higher" K-groups by considering the quotient of the tensor algebra of the multiplicative group $F^\times$ by the two-sided ideal, generated by the $a \otimes (1-a)$, for $a \neq 0, 1$:

$$K_*^M(F) := T^*F^\times/(a \otimes (1-a)),$$

and then defining n-th Milnor K-groups K_n as graded $n-$subspaces of the above quotient.

For $n = 0, 1, 2$ these coincide with Quillen's K-groups of a field, but for $n \geq 3$ they differ in general.

We define the symbol $\{a_1, \ldots, a_n\}$ as the image of $a_1 \otimes \cdots \otimes a_n$.

Brauer group revisited

Consider the Milnor K-theory group $K_2(k)$ and its factor group, the elementary Abelian two-group

$$k_2(k) = K_2(k)/2K_2(k).$$

One shows that $k_2(k)$ is generated by the cosets of symbols $\{a, b\}$ with $a, b \in k^*$.

The correspondence $\{a, b\} \mapsto [a, b]$ induces a group homomorphism

$$h : k_2(k) \to Br_2(k).$$

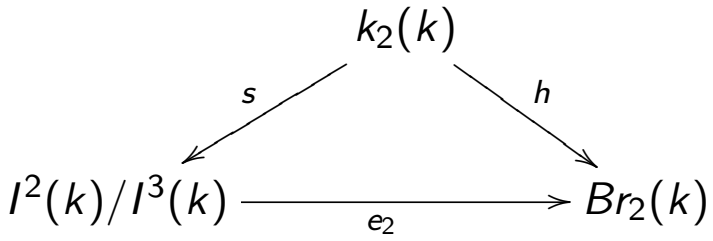
Moreover the correspondence $\{a, b\} \mapsto \langle 1, -a, -b, ab\rangle$ induces a group homomorphism

$$s : k_2(k) \to I^2(k)/I^3(k),$$

and the Witt invariant induces a homomorphism

$$e_2 : I^2(k)/I^3(k) \to Quat(k) \subset Br_2(k).$$

These homomorphisms yield the commutative diagram



It was proved by Milnor that s is an isomorphism.

Theorem (Merkurjev, 1981)

The homomorphism h is an isomorphism for all fields k of characteristic $\neq 2$.

It follows that the homomorphism e_2 is also an isomorphism and consequently $I^3(k) = \ker w$.

Thus, we get a complete characterization of quadratic forms in $I^3(k)$: these are even dimensional forms with trivial discriminant and trivial Witt invariant.

Merkurjev's proof that $h : k_2(k) \to Br_2(k)$ is an isomorphism depended on a result of Suslin on the quadratic norm residue symbol available at that time only through deep results in Quillen's K-theory.

New proofs were given subsequently by Arason, Wadsworth, and Merkurjev and they do not depend on Quillen's K-theory.

Milnor's conjecture

Consider the Milnor K-theory groups $K_n(k)$ and its factor groups:

$$k_n(k) = K_n(k)/2K_n(k),$$

and the cohomology groups

$$H^n(k) = H^n(Gal(\overline{k}/k), \mathbb{Z}/2\mathbb{Z}),$$

where k denotes a separable closure of k.

Milnor defined homomorphisms

$$s_n : k_n(k) \to I^n(k)/I^{n+1}(k)$$

induced by the map sending the pure symbol $\{a_1, \ldots, a_n\} \in K_n(k)$ onto the Witt class of the Pfister form
$(1, -a_1) \otimes \ldots \otimes (1, -a_n) \in I^n(k)$.

Since $I^n(k)$ is additively generated by all n-fold Pfister forms, every s_n is surjective, and Milnor proved that s_1 and s_2 are bijective.

He also defined homomorphisms

$$h_n : k_n(k) \to H^n(k)$$

induced by the map sending the pure symbol $\{a_1, \ldots, a_n\} \in K_n(k)$ onto the cup product $(a_1) \cup \ldots \cup (a_n) \in H^n(k)$.

For $n = 0, 1, 2$, the groups $H^n(k)$ can be identified with $\mathbb{Z}/2\mathbb{Z}$, k^*/k^{*2}, $Br_2(k)$.

Assuming Merkurjev's theorem, dimension index, discriminant, and Witt invariant can be viewed as surjective group homomorphisms

$$e_n : I^n(k) \to H^n(k)$$

satisfying $\ker e_n = I^{n+1}(k)$.

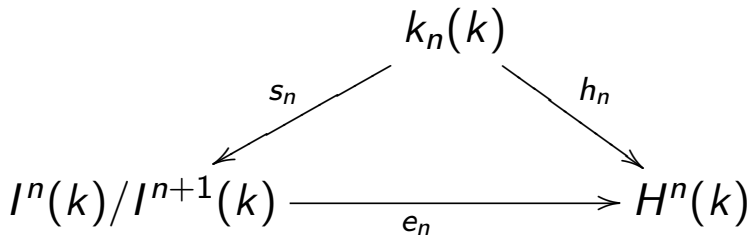
Hence in these cases, we have isomorphisms

$$e_n : I^n(k)/I^{n+1}(k) \to H^n(k).$$

It was an open problem whether such isomorphisms exist for $n \geq 3$.

In 1975, Arason proved the existence of the group homomorphism e_3, and in 1989 Jacob and Rost and independently Szyjewski proved the existence of e_4.

The homomorphisms s_n, h_n, and the supposed maps e_n combine into the diagram



The Milnor conjecture asserts that s_n and h_n are isomorphisms for all n and all fields k of characteristic not 2.

Thus, the difficult and, in fact, intractable question in quadratic form theory about the existence of the invariants en has been transferred to K-theory and cohomology theory.

The bijectivity of h_n for all n was proved by Voevodsky in 1996 and the bijectivity of s_n shortly thereafter by Orlov, Vishik and Voevodsky.

Equivalence of quadratic forms

The class of fields for which classical invariants (i. e. dimension, determinant, Hasse invariant, and the total signature) classify quadratic forms is characterized as follows:

Theorem (Elman, Lam, 1974)

Quadratic forms over a field k are classified by their dimension, determinant, Hasse invariant, and total signature if and only if the ideal $I^3(k)$ of the Witt ring $W(k)$ is torsion-free.

When the field k is nonreal, the Witt ring $W(k)$ is the torsion so that torsion-freeness of $I^3(k)$ is to be interpreted as $I^3(k) = 0$.

The above theorem was proved before Merkurjev's theorem.

Using Merkurjev's theorem, the proof would become much easier.

Voevodsky's theorem gives new possibilities for the classification of quadratic forms.

When we want to check whether two quadratic forms q, g over a field k of characteristic different from 2 are equivalent, we may assume that $\dim q = \dim g = n$ and consider the class $\phi = \langle q \perp -g \rangle$. Then $q \cong g \Leftrightarrow \phi = 0 \in W(k)$.

We shall write e^n for the composition $I^n(k) \to I^n(k)/I^{n+1}(k) \to H^n(k)$ and view the values of the homomorphisms e^n as invariants of quadratic forms in $I^n(k)$.

In order to compute $e^n(\phi)$, we need to know that $\phi \in I^n(k)$.

The latter is equivalent to requiring that $e^i(\phi) = 0$ for $i = 0, 1, \ldots, n-1$.

Theorem (General classification theorem)

Let q, g be quadratic forms over a field k of characteristic different from 2 and assume that $\dim q = \dim g = n$. Set $\phi = \langle q \perp -g \rangle$, and let j satisfy $2^j \leq 2n < 2^{j+1}$.

1. *If $e^i(\phi) \neq 0$ for some $i \leq j$, then q and g are not equivalent forms.*
2. *If $e^i(\phi) = 0$ for $i = 1, \ldots, j$, then q and g are equivalent forms.*

Proof.

The class ϕ is even-dimensional and hence lies in $I(k)$ and so $e^0(\phi) = 0$.

If $e^1(\phi) = 0$, we have $\phi \in I^2(k)$, and if ℓ is the smallest index for which $e^\ell(\phi) \neq 0$, then necessarily $\phi \neq 0 \in W(k)$ and so q and g are inequivalent.

If $e^i(\phi) = 0$ for $i = 1, \ldots, j$, then by Voevodsky's theorem $\phi \in I^{j+1}(k)$.

However, $\dim \phi = 2n < 2^{j+1}$ implies $\phi = 0 \in W(k)$ by the Arason–Pfister Hauptsatz, but $\phi = 0 \in W(k)$ and $\dim q = \dim g$ imply $q \cong g$. □

Quotients of fundamental ideal revisited

For a quadratic form $\phi = (a_1, \ldots, a_n)$ over k set:

$$k(\phi) = k(x_2, \ldots, x_n)\left(\sqrt{-\frac{a_2x_2^2 + \ldots + a_nx^2}{a_1}}\right).$$

Moreover, let $I_\phi(k)$ denote the ideal in $W(k)$ generated by all the $\langle 1, -t\rangle$, where t lies in $D(\phi)$.
Orlov, Vishik and Voevodsky proved the following:

Theorem

Let ω be an anisotropic m-fold Pfister form over k and denote by $L(\omega)$ its class in $k_m(k)$. Then the kernel of $k_*^M(k) \to k_*^M(k(\omega))$ is $k_*(k)L(\omega)$, and the annihilator of $L(\omega)$ in $k_*^M(k)$ is generated by the $\{t\}$, where t runs through the non-zero elements in k represented by ω.

This combined with the isomorphisms $k_n(k) \to I^n(k)/I^{n+1}(k)$ yields:

Theorem

Let ω be an anisotropic m-fold Pfister form over k and let n be a positive integer. Then:

1. *The kernel of the natural morphism*

$$I^{n+k}(k)/I^{n+k+1}(k) \to I^{n+k}(k(\omega))/I^{n+k+1}(k(\omega))$$

   equals the image of $I^n(k)\omega$ in $I^{n+k}(k)/I^{n+k+1}(k)$.

2. *The kernel of the morphism*

$$I^n(k)/I^{n+1}(k) \to I^{n+k}(k)/I^{n+k+1}(k)$$

   given by multiplication by ω equals the image of $I^{n-1}(k)I_\omega(k)$ in $I^n(k)/I^{n+1}(k)$.

Lam's Open Problem B follows almost directly from part 2 of the above theorem (Arason, Elman, Dickmann, Miraglia and others).

Units of Witt ring

Theorem

1. *If the field k is nonreal, then $U(W(k)) = 1 + I(k)$.*
2. *If k is formally real, then $\langle q \rangle \in U(W(k))$ if and only if $sgn_P \langle q \rangle = \pm 1$ for all orderings P of k.*

Finally, for any field k , 0 and 1 are the only idempotents of the Witt ring $W(k)$.

Counting Witts

Paweł Gładki
(joint work with Murray Marshall)

Uniwersytet Śląski
http://www.math.us.edu.pl/~pgladki/

November 20, 2013

If K is a field, let X_K be the topological space of orderings in K. Recall that the u-invariant $u(K)$ of a field is defined as

$$u(K) = \sup\{\dim q : q \text{ is an anisotropic torsion quadratic form over } K\},$$

where q is torsion if its Witt class is a torsion element in $W(K)$. Grenier-Boley, Hoffmann and Scheiderer have recently proven:

Theorem

Let K and L be two SAP fields such that $u(K), u(L) \leq 2$. Then the following are equivalent:

1. *There is a ring isomorphism $W(K) \cong W(L)$.*
2. *There is a homeomorphism $X_K \cong X_L$ and a group isomorphism $\sigma : \sum K^{*2}/K^{*2} \cong \sum L^{*2}/L^{*2}$.*

- N. Grenier-Boley, D. Hoffmann, C. Scheiderer, *Isomorphism criteria for Witt rings of real fields,* Forum Math. **25** (2013), 1–18.

In particular, the above theorem covers the case of Witt equivalence of algebraic function fields of curves over $\mathbb{R}$.

A very natural question to ask is what happens if we increase the stability index by one, for example by considering algebraic function fields of **curves** over $\mathbb{Q}$?

This seems to be a difficult question in general, so let's restrict ourselves to considering function fields of **conics** over $\mathbb{Q}$.

In this talk we shall count (some of the) non-isomorphic classes of Witt rings of function fields of rational conics.

Recall that we have the following obvious implications:

$$\begin{array}{ccccc} \text{Birational} & & \text{Birational} & & \text{Witt} \\ \text{isomorphism} & \Rightarrow & \text{equivalence} & \Rightarrow & \text{equivalence} \\ \text{of conics} & & \text{(isomorphism} & & \text{of their} \\ & & \text{of their} & & \text{function fields} \\ & & \text{function fields)} & & \end{array}$$

Classes of birationally isomorphic rational conics

Theorem

Let $f \in \mathbb{Q}[x, y]$ be an irreducible polynomial of degree 2 and consider the curve $\mathcal{C} : f(x, y) = 0$ whose function field $\mathbb{Q}(\mathcal{C})$ is formally real. Then $\mathcal{C}$ is birationally isomorphic either to

1. *a curve whose function field is isomorphic to $\mathbb{Q}(x)$, or*
2. *two parallel lines with no rational points:*

$$ax^2 + c = 0, \qquad a \in \mathbb{Q}^*, c \in \mathbb{Q},$$

or

3. *an ellipse with no rational points:*

$$ax^2 + by^2 + c = 0, \qquad a > 0, \;\; b > 0, \;\; c < 0.$$

- P. Gładki, M. Marshall. The pp conjecture for spaces of orderings of rational conics. *J. Algebra Appl.* **6** (2007) 245–257.

The proof is absolutely elementary.
From a standard course in linear algebra we know that $\mathcal{C}$ is affine isomorphic either to a curve of parabolic type

$$ax^2 + y = 0, \qquad a \in \mathbb{Q}^*, \tag{1}$$

or to a curve of parallel type

$$ax^2 + c = 0, \qquad a \in \mathbb{Q}^*, c \in \mathbb{Q}, \tag{2}$$

or to a curve of elliptic (hyperbolic) type

$$ax^2 + by^2 + c = 0, \qquad a, b \in \mathbb{Q}^*, c \in \mathbb{Q}. \tag{3}$$

If $\mathcal{C}$ is affine isomorphic to the parabola (1), then its function field $\mathbb{Q}(\mathcal{C})$ is a purely transcendental extension of $\mathbb{Q}$ of degree 1, for if $\mathbb{Q}(\mathcal{C}) \cong \mathbb{Q}(x, y)$ where $ax^2 + y = 0$, $a \neq 0$, then

$$\mathbb{Q}(\mathcal{C}) \cong \mathbb{Q}(x, y) = \mathbb{Q}(x, -ax^2) = \mathbb{Q}(x).$$

Further, if $\mathcal{C}$ has a rational point, then it is affine isomorphic to a parabola (1) or an ellipse (hyperbola) (3), for if a curve $ax^2 + c = 0$ has a rational point (q, r) then

$$ax^2 + c = ax^2 - aq^2 = a(x - q)(x + q),$$

so that $\mathcal{C}$ is reducible – a contradiction.
The "degenerated" ellipse

$$ax^2 + by^2 = 0, \qquad a, b \in \mathbb{Q}^*. \tag{4}$$

is birationally isomorphic to two parallel lines (2) without rational points via the mapping

$$(x, y) \mapsto (\frac{x}{y}, 1).$$

For the "non-degenerated" ellipse

$$ax^2 + by^2 + c = 0, \qquad a, b, c \in \mathbb{Q}^*. \tag{5}$$

with a rational point, $\mathbb{Q}(\mathcal{C}) \cong \mathbb{Q}(z)$ for a z transcendental over $\mathbb{Q}$; indeed, since $aq^2 + br^2 + c = 0$ for some rational point (q, r), then

$$ax^2 - aq^2 = br^2 - by^2.$$

Let $z = \frac{x-q}{y-r}$.
Hence $\mathbb{Q}(z) \subset \mathbb{Q}(x, y)$.

Conversely, we have:

$$az(x+q) = a\frac{x-q}{y-r}(x+q) = \frac{ax^2 - aq^2}{y-r} = -\frac{by^2 - br^2}{y-r} = -b(y+r),$$

and after rearranging:

$$azx + by = -azq - br. \tag{6}$$

On the other hand, the equation $z = \frac{x-q}{y-r}$ gives:

$$x - zy = q - zr. \tag{7}$$

The determinant $-az^2 - b$ of the system of equations (6) and (7):

$$\begin{cases} azx + by = -azq - br \\ x - zy = q - zr \end{cases}$$

is nonzero.

Indeed, if it was zero, then $a(x-q)^2 + b(y-r)^2 = 0$.

This implies that the irreducible polynomial $ax^2 + by^2 + c$ divides the polynomial $a(x-q)^2 + b(y-r)^2$ so, comparing coefficients, they are equal.

Then, comparing coefficients some more, $q = r = 0$ and $c = 0$, which contradicts $c \neq 0$. $\square$

Finally, after scaling and/or interchanging x and y (if necessary), the "non-degenerate" ellipse (hyperbola) (5) clearly satisfies either:

$$a > 0, \quad b > 0, \quad c < 0, \qquad \text{(elliptic type)}, \tag{8}$$

or

$$a > 0, \quad b < 0, \quad c < 0, \qquad \text{(hyperbolic type)}, \tag{9}$$

but these are birationally isomorphic via

$$(x, y) \mapsto (\frac{y}{x}, \frac{1}{x}).$$

Classes of birationally equivalent rational conics

Set $\Omega_{a,b} := \mathrm{qf}\ \frac{\Omega[x,y]}{(ax^2+by^2-1)}$, $\Omega_r := \mathrm{qf}\ \frac{\Omega[x,y]}{(x^2-r)}$.
We assume always that $a, b \in \Omega^*$ and $r \in \Omega^* \setminus \Omega^{*2}$.
We write $K \cong_\Omega L$ to indicate that the field extensions K, L of Ω are Ω-isomorphic.

Proposition

For $r, s \in \Omega^* \backslash \Omega^{*2}$, the following are equivalent:
(1) $r \equiv s \mod \Omega^{*2}$.
(2) $\Omega(\sqrt{r}) \cong_\Omega \Omega(\sqrt{s})$.
(3) $\Omega_r \cong_\Omega \Omega_s$.

Proof.

The equivalence of (1) and (2) is well-known.
For the equivalence of (2) and (3) use the fact that $\Omega_r = \Omega(\sqrt{r})(x)$, the field of rational functions in one variable x over the field $\Omega(\sqrt{r})$, and $\Omega(\sqrt{r})$ is the field of constants of Ω_r over Ω, i.e., the algebraic closure of Ω in Ω_r. □

Proposition

The field of constants of $\Omega_{a,b}$ over Ω is equal to Ω.

Observe that Proposition 9 implies $\Omega_{a,b} \ncong_{\Omega} \Omega_r$ for $a, b \in \Omega$ and $r \in \Omega^* \backslash \Omega^{*2}$.

Proof.

Clearly $\Omega_{a,b} = \Omega(x)(\sqrt{\frac{1-ax^2}{b}})$.

Suppose $f = f_0 + f_1\sqrt{\frac{1-ax^2}{b}}$, $f_0, f_1 \in \Omega(x)$, is algebraic over Ω.

Then $\overline{f} = f_0 - f_1\sqrt{\frac{1-ax^2}{b}}$ is also algebraic over Ω.

Consequently, $f_0 = (f + \overline{f})/2$ and $f_0^2 - f_1^2(\frac{1-ax^2}{b}) = f\overline{f}$ are algebraic over Ω.

It follows that $f_1^2(\frac{1-ax^2}{b})$ is algebraic over Ω, i.e., $f_1 = 0$, and $f_0 \in \Omega$. □

For $a, b \in \Omega^*$, $(\frac{a,b}{\Omega})$ denotes the quaternion algebra over Ω, i.e., the 4-dimension central simple algebra over Ω generated by i, j subject to $i^2 = a$, $j^2 = b$, $ji = -ij$.
We identify quaternion algebras over Ω which are isomorphic as Ω-algebras, equivalently, are equal as elements of the Brauer group of Ω.

Proposition

The following are equivalent:
(1) $(\frac{a,b}{\Omega}) = 1$ *(i.e.,* $(\frac{a,b}{\Omega})$ *splits over* Ω*).*
(2) $\langle 1, -a\rangle \otimes \langle 1, -b\rangle \sim 0$ *over* Ω*.*
(3) $1 \in D_\Omega\langle a, b\rangle$*.*
(4) The conic $ax^2 + by^2 = 1$ *has a rational point.*
(5) $\Omega_{a,b}$ *is purely transcendental over* Ω*.*

Proof.

The equivalence of (1), (2), (3) and (4) is well-known from quadratic form theory.

If (p, q) is a rational point of $ax^2 + by^2 = 1$ then $\Omega_{a,b} = \Omega(z)$ where $z := \frac{y-q}{x-p}$.

Conversely, if $\Omega_{a,b} = \Omega(z)$ then, choosing $f(z), g(z), h(z) \in \Omega[z]$ so that $x = \frac{f(z)}{h(z)}$, $y = \frac{g(z)}{h(z)}$, and choosing $r \in \Omega$ so that $h(r) \neq 0$, one sees that $(\frac{f(r)}{h(r)}, \frac{g(r)}{h(r)})$ is a rational point of $ax^2 + by^2 = 1$.

Note: This argument fails if $|\Omega| < \infty$, but the conclusion continues to hold even in this case, since $|\Omega| < \infty \Rightarrow$ the quadratic form $\langle a, b \rangle$ is Ω-universal. $\square$

From the definition of $\Omega_{a,b}$ it is clear that $1 \in D_{\Omega_{a,b}}\langle a, b\rangle$, so $(\frac{a,b}{\Omega})$ splits over $\Omega_{a,b}$.
Of course, 1 also splits over $\Omega_{a,b}$ (since it splits over Ω).

Conversely one has the following:

Proposition (E. Witt)

The only quaternion algebras defined over Ω *which split over* $\Omega_{a,b}$ *are* $(\frac{a,b}{\Omega})$ *and* 1.

- E. Witt, Gegenbeispiel zum Normensatz. *Math. Zeit.* **39** (1934) 12–28.

Proposition (E. Witt)

The following are equivalent:
(1) $(\frac{a,b}{\Omega}) = (\frac{c,d}{\Omega})$.
(2) $\Omega_{a,b} \cong_{\Omega} \Omega_{c,d}$.

Proof.

Then implication (1) $\Rightarrow$ (2) is Satz on page 464 in:

- E. Witt, Gegenbeispiel zum Normensatz. *Math. Zeit.* **39** (1934) 12–28.

The implication (2) $\Rightarrow$ (1) is immediate from the Proposition 11. $\square$

Classes of Witt equivalent function fields of rational conics

The following is an ultra-classic:

Theorem

For K, L fields of characteristic $\neq 2$, the following are equivalent:
(1) $\mathrm{W}(K) \cong \mathrm{W}(L)$.
(2) There exists a group isomorphism $\alpha : K^*/K^{*2} \to L^*/L^{*2}$ *such that* $\alpha(-1) = -1$ *and* $\alpha(D_K\langle 1, a\rangle) = D_L\langle 1, \alpha(a)\rangle$ *for all* $a \in K^*/K^{*2}$.

- D.K. Harrison, Witt rings. *University of Kentucky Notes*, Lexington, Kentucky (1970).

Recall that the field of constants of $\Omega_{a,b}$ is equal to Ω and the field of constants of Ω_r is equal to $\Omega(\sqrt{r})$.
In:

- P. Koprowski, Local-global principle for Witt equivalence of function fields over global fields. *Colloq. Math.* **91** (2002) 293–302.

Koprowski proves the following:

Proposition

Let k and l be two global fields of characteristic $\neq 2$ and let K and L be algebraic function fields with fields of constans k and l that also have rational places. If K and L are Witt equivalent, then so are k and l.

It follows that $\Omega_{a,b} \not\sim \Omega_r$ and if $\Omega(\sqrt{r}) \not\sim \Omega(\sqrt{s})$ then $\Omega_r \not\sim \Omega_s$.

In:

- K. Szymiczek, Witt equivalence of global fields. II. Relative quadratic extensions. *Trans. Amer. Math. Soc.* **343** (1994) 277–303.

Szymiczek proves that every quadratic extension of $\mathbb{Q}$ is Witt equivalent to $\mathbb{Q}(\sqrt{r})$ for some $r \in \{-1, \pm 2, \pm 7, \pm 17\}$, and, moreover, these 7 quadratic extensions of $\mathbb{Q}$ are not Witt equivalent to each other.
It follows that for $\Omega = \mathbb{Q}$, the function fields Ω_r, $r \in \{-1, \pm 2, \pm 7, \pm 17\}$, are themselves not Witt equivalent.

We turn now to function fields of conics of the form $\Omega_{a,b}$, $a, b \in \Omega^*$.
We continue to assume $\Omega = \mathbb{Q}$.
The conics $x^2 + y^2 = 1$ and $3x^2 + 3y^2 = 1$ both have real points, but the former has rational points whereas the latter does not.
In:

- M. Dickmann, M. Marshall, F. Miraglia. Lattice-ordered reduced special groups. *Ann. Pure Appl. Logic.* **132** (2005) 27–49.
- P. Gładki, M. Marshall. The pp conjecture for spaces of orderings of rational conics. *J. Algebra Appl.* **6** (2007) 245–257.

it is proven that the pp conjecture holds for the space of orderings of $\Omega_{1,1}$ but not for the space of orderings of $\Omega_{3,3}$.
Since the space of orderings of a field is an invariant of its Witt ring, this implies that $\Omega_{1,1} \not\sim \Omega_{3,3}$.

The field $\Omega_{-1,-1}$ is not formally real (-1 is a sum of two squares in $\Omega_{-1,-1}$) so $\Omega_{-1,-1}$ cannot be Witt equivalent to $\Omega_{1,1}$ or $\Omega_{3,3}$.
Similarly, $\Omega_{-1,-3}$ cannot be Witt equivalent to $\Omega_{1,1}$ or $\Omega_{3,3}$.
We claim that $K := \Omega_{-1,-1}$ and $L := \Omega_{-1,-3}$ are Witt inequivalent.
For suppose they are.
Then $1 \in D_K\langle -1, -1\rangle$ so $1 \in D_L\langle -1, -1\rangle$, i.e., $(\frac{-1,-1}{\Omega})$ splits over L.
Since $(\frac{-1,-1}{\Omega}) \neq 1$, Proposition 11 implies that $(\frac{-1,-1}{\Omega}) = (\frac{-1,-3}{\Omega})$, i.e., $(\frac{-1,3}{\Omega}) = 1$, i.e., $3 \in D_\Omega\langle 1, 1\rangle$.
Of course, this is impossible.

Thus the 11 function fields

$$\Omega_{-1}, \Omega_2, \Omega_{-2}, \Omega_7, \Omega_{-7}, \Omega_{17}, \Omega_{-17}, \Omega_{1,1}, \Omega_{3,3}, \Omega_{-1,-1}, \Omega_{-1,-3}$$

over the field $\Omega = \mathbb{Q}$ are pairwise Witt inequivalent.

Question: Are there more, or is this the complete set?

Conjecture: There are infinitely many Witt inequivalent function fields of rational conics.