Counting Witts

Paweł Gładki
(joint work with Murray Marshall
and Przemysław Koprowski)

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

December 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:

Birational isomorphism of conics	Birational equivalence (isomorphism of their function fields)	Witt equivalence of their function fields

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:*

$$x^2 - r = 0, \quad r > 0,$$

   or

3. *an ellipse with no rational points:*

$$ax^2 + by^2 - 1 = 0, \quad a > 0, \ b > 0.$$

- 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

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

or to a curve of parallel type

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

or to a curve of elliptic (hyperbolic) type

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

Clearly, a function field of a parabola is just $\mathbb{Q}(x)$.

Moreover, two parallel lines with a rational point are not irreducible.

The "degenerated" ellipse (hyperbola) $ax^2 + by^2 = 0, a, b \in \mathbb{Q}^*$ is birationally isomorphic to two parallel lines via $(x, y) \mapsto (\frac{x}{y}, 1)$.

After some scaling, we might as well assume that two parallel lines are of the form $x^2 - r = 0, \qquad r \in \mathbb{Q}$.

The "non-degenerated" ellipse (hyperbola)

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

with a rational point $(q, r) \in \mathbb{Q}^2$ can be parametrized by $\frac{x-q}{y-r}$, i. e. is birationally isomorphic to $\mathbb{Q}(z)$ for $z = \frac{x-q}{y-r}$.
Finally, after scaling and/or interchanging x and y (if necessary), the "non-degenerate" ellipse (hyperbola) above clearly satisfies either:

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

or

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

but these are birationally isomorphic via $(x, y) \mapsto (\frac{y}{x}, \frac{1}{x})$.
Scaling some more, we can always assume $c = -1$.

Classes of birationally equivalent rational conics

Probably the first attempt to classify function fields of conics was due to Ernst Witt:

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

Roughly speaking, he showed that function fields K of conics over $\mathbb{Q}$ are in one-to-one correspondence with quaternion algebras C over $\mathbb{Q}$ such that K splits C.

This work paved the way to the theory of generic splitting fields, that basically started with the ultra-classical paper by Amitsur:

- S. Amitsur, Generic splitting fields of central simple algebras. *Annals of Math.* **62** (1955) 8–43.

Again, roughly speaking, he showed that to a given central simple algebra C over $\mathbb{Q}$ there corresponds an algebraic function field K in $n-1$ variables over $\mathbb{Q}$ which splits C.

By the way, his work, according to MathSciNet, has been so far cited over 300 times.

Following the footsteps of old masters, we shall accept the notation introduced in Witt's paper and write

$$\Omega_{a,b} := \mathrm{qf}\, \frac{\mathbb{Q}[x,y]}{(ax^2 + by^2 - 1)} \text{ and } \Omega_r := \mathrm{qf}\, \frac{\mathbb{Q}[x,y]}{(x^2 - r)}.$$

By the classification theorem discussed above, these are the only fields that are of our interest: the cases of $a > 0$, $b > 0$ and $r > 0$, $r \notin \mathbb{Q}^{*2}$, cover all situations when $\Omega_{a,b}$ or Ω_r are formally real, to include the formally non-real case we will allow $a, b \in \mathbb{Q}^*$ and $r \in \mathbb{Q}^* \backslash \mathbb{Q}^{*2}$.

We write $K \cong_{\mathbb{Q}} L$ to indicate that the field extensions K, L of $\mathbb{Q}$ are $\mathbb{Q}$-isomorphic.

Most of what we are doing here works equally well with the field $\mathbb{Q}$ replaced with any field Ω, but we shall restrict ourselves to the rational case.

The case of fields Ω_r

...is actually really easy.

Proposition

For $r \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$ the field of constants of Ω_r (i.e. the algebraic closure of $\mathbb{Q}$ in Ω_r) is $\mathbb{Q}(\sqrt{r})$.

Proof.

Clearly $\Omega_r = \mathbb{Q}(\sqrt{r})(x)$. □

Proposition

For $r, s \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$, the following are equivalent:

1. $r \equiv s \mod \mathbb{Q}^{*2}$;
2. $\mathbb{Q}(\sqrt{r}) \cong_{\mathbb{Q}} \mathbb{Q}(\sqrt{s})$;
3. $\Omega_r \cong_{\mathbb{Q}} \Omega_s$.

Proof.

1. $\Leftrightarrow$ 2. is well-known.

2. $\Rightarrow$ 3. is clear since $\Omega_r = \mathbb{Q}(\sqrt{r})(x)$.

3. $\Rightarrow$ 2. is clear since, by the previous proposition, Ω_r is the algebraic function field in a single variable with the field of constants $\mathbb{Q}(\sqrt{r})$. □

The case of fields $\Omega_{a,b}$

...is also pretty easy, but already more interesting!

Proposition

For $a, b \in \mathbb{Q}^*$ the field of constants of $\Omega_{a,b}$ is $\mathbb{Q}$.

Proof.

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

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

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

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 $\mathbb{Q}$.

It follows that $f_1^2(\frac{1-ax^2}{b})$ is algebraic over $\mathbb{Q}$.

This is only possible when $f_1 = 0$.

Consequently, $f_0 \in \mathbb{Q}$ and $f \in \mathbb{Q}$. □

Observe that this implies

$$\Omega_{a,b} \ncong_{\mathbb{Q}} \Omega_r$$

for $a, b \in \mathbb{Q}^*$ and $r \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$.

In order to distinguish between the different fields $\Omega_{a,b}$, we need to go back to Witt's paper and use quaternion algebras.

Let K be a field of characteristic $\neq 2$.

For $a, b \in K^*$, $(\frac{a,b}{K})$ denotes the quaternion algebra over K, i.e., the 4-dimension central simple algebra over K generated by the elementsi, j subject to

$$i^2 = a, \quad j^2 = b, \quad ji = -ij.$$

We shall identify quaternion algebras over K, which are isomorphic as K-algebras, as equal elements of the Brauer group of K.

We start with the following:

Proposition

For $a, b \in K^*$ the following are equivalent:

1. $(\frac{a,b}{K}) = 1$ *(i.e., $(\frac{a,b}{K})$ splits over K).*
2. $\langle 1, -a \rangle \otimes \langle 1, -b \rangle \sim 0$ *over K.*
3. $1 \in D_K \langle a, b \rangle$.
4. *The conic $ax^2 + by^2 = 1$ has a K-rational point.*
5. $qf \frac{K[x,y]}{ax^2+by^2-1}$ *is purely transcendental over K.*

Proof.

1. $\Leftrightarrow$ 2. $\Leftrightarrow$ 3. $\Leftrightarrow$ 4. is, more or less, trivial.

4. $\Leftrightarrow$ 5. is a part of the classification theorem discussed earlier with the field $\mathbb{Q}$ replaced by K. □

Proposition (E. Witt)

Let C be a quaternion algebra over $\mathbb{Q}$.

Then C splits if and only if $C = (\frac{a,b}{\mathbb{Q}})$, for some $a, b \in \mathbb{Q}^*$, or if $C = 1$.

Proof.

($\Rightarrow$): is in

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

($\Leftarrow$): is, more or less, trivial; from the definition of $\Omega_{a,b}$ it is clear that $1 \in D_{\Omega_{a,b}}\langle a, b\rangle$, so $(\frac{a,b}{\mathbb{Q}})$ splits over $\Omega_{a,b}$.

Of course 1 splits over $\mathbb{Q}$, so it also splits over $\Omega_{a,b}$. □

Proposition (E. Witt)

For $a, b, c, d \in \mathbb{Q}^*$ the following are equivalent:

1. $(\frac{a,b}{\mathbb{Q}}) = (\frac{c,d}{\mathbb{Q}})$.
2. $\Omega_{a,b} \cong_{\mathbb{Q}} \Omega_{c,d}$.

Proof.

1. $\Leftrightarrow$ 2. is Satz on page 464 in:

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

2. $\Leftrightarrow$ 1.: Assume that $\Omega_{a,b} \cong_{\mathbb{Q}} \Omega_{c,d}$ and consider the algebras $(\frac{a,b}{\mathbb{Q}})$ and $(\frac{c,d}{\mathbb{Q}})$.

$(\frac{a,b}{\mathbb{Q}})$ splits over $\Omega_{a,b} \cong_{\mathbb{Q}} \Omega_{c,d}$, so it is either 1 or $(\frac{c,d}{\mathbb{Q}})$.

If it is $(\frac{c,d}{\mathbb{Q}})$, we're done, if it is 1, then $\Omega_{a,b}$ is just $\mathbb{Q}(x)$, and so is $\Omega_{c,d}$, hence $(\frac{c,d}{\mathbb{Q}})$ is 1.

Consequently, $(\frac{a,b}{\mathbb{Q}}) = (\frac{c,d}{\mathbb{Q}})$. □

Classes of Witt equivalent function fields of rational conics

The starting point for our next considerations is the following ultra-classic:

Theorem (Harrison, 1970)

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).

Using a number of results that emerged from the Harrison criterion, we shall start counting Witt rings of $\Omega_{a,b}$ and Ω_r.

Theorem (Koprowski, 2002)

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.

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

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

Thus, so far, we have at least 2 Witt non-equivalent fields, $\Omega_{a,b}$ and Ω_r.

Let us try to distinguish between Witt non-equivalent fields within these two classes.

The case of Ω_r is somewhat easier.

Theorem (Perlis, Szymiczek, Conner, Litherland, 1994)

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 Witt non-equivalent to each other.

- R. Perlis, K. Szymiczek, P.E. Conner, R. Litherland, Matching Witts with global fields, in: Recent Advances in Real Algebraic Geometry and Quadratic Forms (Proc. RAGSQUAD Year, Berkeley,CA, 1990-1991); (W. B. Jacob, T. Y. Lam, and R. O.Robson, eds.), *Contemp. Math* **155** (1994), 365–387.
- K. Szymiczek, Witt equivalence of global fields. II. Relative quadratic extensions. *Trans. Amer. Math. Soc.* **343** (1994) 277–303.

It follows that the function fields Ω_r, $r \in \{-1, \pm 2, \pm 7, \pm 17\}$, are themselves Witt non-equivalent.

Thus our count of Witt non-equivalent function fields of conics is up to 8.

We turn now to the fields $\Omega_{a,b}$, which are more tricky to handle.

We start with the following easy observation:

Proposition

For $a, b \in \mathbb{Q}^*$ and a number field k such that $-ab \in k^* \setminus k^{*2}$ the following are equivalent:

1. *there is a point $\mathfrak{p}$ of $\Omega_{a,b}$ with the residue field isomorphic to k;*
2. *the form $\langle a, b, -1 \rangle$ is isotropic over k.*

Proof.

1. $\Rightarrow$ 2.: Let $\mathfrak{p}$ be the point of $\Omega_{a,b}$ with the residue field k.

Then there are $x, y \in k$ such that $a \cdot x^2 + b \cdot y^2 - 1 \cdot 1^2 = 0$.

Consequently, the form $\langle a, b, -1 \rangle$ is isotropic over k.

1. $\Leftarrow$ 2.: Let $x, y, z \in k$ be such that $ax^2 + by^2 - z^2 = 0$.

If $z = 0$, then $-ax^2 = by^2$ and, consequently,

$-ab = \left(\frac{by}{x}\right)^2 \in k^{*2}$, which yields a contradiction.

Thus $z \neq 0$ and the point $\mathfrak{p}$ associated to $(\frac{x}{z}, \frac{y}{z})$ has the residue field k. $\square$

We will need the following improvement on the Harrison criterion:

Theorem (Koprowski, 2002)

Let k and l be two finite extensions of $\mathbb{Q}$, and K and L algebraic function fields with fields of constants k and l, respectively. Then K and L are Witt-equivalent iff the following conditions hold:

1. *there is an isomorphism $i : W(K) \to W(L)$ sending one-dimensional forms to one-dimensional forms;*
2. *there is a bijection $T : \mathbb{P}_K \to \mathbb{P}_L$ between places of K trivial on k and places of L trivial on l;*
3. *there are isomorphisms $i_\mathfrak{p} : W(K_\mathfrak{p}) \to W(L_{T(\mathfrak{p})})$ of Witt rings of the completions, for every place $\mathfrak{p} \in \mathbb{P}_K$, such that:*

$$\begin{array}{ccc} W(K) & \xrightarrow{\;i\;} & W(L) \\ \downarrow{\scriptstyle \theta_\mathfrak{p}} & & \downarrow{\scriptstyle \theta_{T(\mathfrak{p})}} \\ W(K_\mathfrak{p}) & \xrightarrow[i_\mathfrak{p}]{} & W(L_{T(\mathfrak{p})}) \end{array}$$

We start with distinguishing between the formally real and formally non-real case.

Proposition

For $a, b, c, d \in \mathbb{Q}^*$ with $a, b > 0$ and $c, d < 0$, the fields $\Omega_{a,b}$ and $\Omega_{c,d}$ are Witt non-isomorphic.

First proof.

Not a "proof", really, just to indicate that we don't quite use the Koprowski criterion here..

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, say, $\Omega_{1,1}$. $\square$

Second proof.

Suppose that $\Omega_{a,b}$ is Witt equivalent to $\Omega_{c,d}$, for some $a, b > 0$ and $c, d < 0$.

The field $\Omega_{a,b}$ has a point $\mathfrak{p}$ with the formally real residue field $\mathbb{K}$.

By the Koprowski criterion, the field $\Omega_{c,d}$ has a point $\mathfrak{q}$ with the residue field $\mathbb{L}$ Witt equivalent to $\mathbb{K}$.

In particular, $\mathbb{L}$ is formally real.

By the previous proposition, the form $\langle c, d, -1 \rangle$ is isotropic over $\mathbb{L}$.

But the signature of this form is -3.

This is a contradiction. $\square$

Thus our count of Witt non-equivalent function fields of conics is up to 9.

Now it is time to distinguish between Witt non-equivalent fields $\Omega_{a,b}$ and $\Omega_{c,d}$, for $a, b > 0$ and $c, d < 0$, respectively.

Proposition

The fields $\Omega_{1,1}$ and $\Omega_{3,3}$ are Witt non-equivalent.

First proof.

The conic $x^2 + y^2 = 1$ has a rational point, and, by the classification theorem, its function field is just $\mathbb{Q}(x)$.
By:

- M. Dickmann, M. Marshall, F. Miraglia. Lattice-ordered reduced special groups. *Ann. Pure Appl. Logic.* **132** (2005) 27–49.

the pp conjecture holds for the space of orderings of the field $\Omega_{1,1}$.

The conic $3x^2 + 3y^2 = 1$ does not have any rational points, and, by:

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

the pp conjecture fails for the space of orderings of the field $\Omega_{3,3}$.

Since the space of orderings of a field is an invariant of its Witt ring, this concludes the proof. □

Second proof.

Suppose that $\Omega_{1,1}$ is Witt equivalent to $\Omega_{3,3}$.

The field $\Omega_{1,1}$ has a point $\mathfrak{p}$ with the residue field isomorphic to $\mathbb{Q}$.

By the Koprowski criterion, the field $\Omega_{3,3}$ has a point $\mathfrak{q}$ with the residue field Witt equivalent to $\mathbb{Q}$.

But since the degree of a point is an invariant of Witt equivalence, this means that the conic $3x^2 + 3y^2 = 1$ has a rational point. $\square$

Thus our count of Witt non-equivalent function fields of conics is up to 10.

How about the fields $\Omega_{c,d}$ with $c, d < 0$...?

Proposition

$\Omega_{-1,-1}$ and $\Omega_{-1,-3}$ are Witt non-equivalent.

Proof.

Suppose that $\Omega_{-1,-1}$ is Witt equivalent to $\Omega_{-1,-3}$.

Clearly $1 \in D_{\Omega_{-1,-1}}\langle -1,-1\rangle$.

Thus $1 \in D_{\Omega_{-1,-3}}\langle -1,-1\rangle$.

By one of the propositions, $(\frac{-1,-1}{\mathbb{Q}})$ splits over $\Omega_{-1,-3}$.

Since $(\frac{-1,-1}{\mathbb{Q}}) \neq 1$, this implies that $(\frac{-1,-1}{\mathbb{Q}}) = (\frac{-1,-3}{\mathbb{Q}})$.

But then $(\frac{-1,3}{\mathbb{Q}}) = 1$, or, equivalently, $3 \in D_{\mathbb{Q}}\langle 1,1\rangle$.

Of course, this is impossible. □

So, our count of Witt non-equivalent function fields of conics is up to 11.

Conjecture 1: There are 11 Witt non-equivalent function fields of rational conics.

Conjecture 2: There are infinitely many Witt non-equivalent function fields of rational conics.