Existence of solutions of quadratic rational polynomials as quadratic hypersurfaces in $\mathbb{P}^n$

Yao Hurui

12/23/2025

Contents

1 Introduction **2**
1.1 Examples 2
1.2 Treatment of homogeneous quadratic polynomials 5

2 Main Theorem **8**
2.1 Statement of main theorem 8
2.2 Proof of main theorem in arithmetic 9
2.2.1 Preliminaries 9
2.2.2 Key lemmas 10
2.2.3 Proof of main theorem 11
2.3 Another way to understand the main theorem 13
2.3.1 Preliminary Definitions and Theorems 13
2.3.2 Brauer–Manin Obstruction 15

Chapter 1

Introduction

1.1 Examples

Number theory is one of the oldest and most dynamic branches of mathematics. One of its central goals is the study of integer or rational solutions to polynomial equations—the so-called Diophantine problems. These problems often appear simple in form but reveal profound mathematical structures. From the Pythagorean theorem in ancient Greece to Fermat's Last Theorem in the 17th century, the search for solutions has not only driven the development of number theory itself but also spurred the growth of modern fields such as algebra and algebraic geometry.

Among Diophantine equations, quadratic equations play a special and fundamental role. Compared to higher-degree equations, the theory of quadratic equations is relatively complete, and their solution sets often exhibit clear algebraic and geometric structures. More importantly, the study of rational points on quadratic equations serves as a key bridge connecting classical number theory with modern arithmetic geometry.

Here, we have a classical example about quadratic equations:

Example 1 (Pythagorean Triples)**.** Consider

$$x^2 + y^2 = z^2.$$

When we study elementary number theory, by using right triangles and algebraic transformations, we can prove that for any $m, n \in \mathrm{Z}$, the solutions of Pythagorean equation has such a formula:

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Now, we can use another way to solve this equation. Clearly, the Pythagorean equation is a **homogeneous equation**, i.e. for any $\lambda \in \mathrm{R}$, if $[x, y, z]$ is a solution of Pythagorean equation, then $[\lambda x, \lambda y, \lambda z]$ is still a solution of Pythagorean equation. So, we can define the equation in the **projective plane** $\mathbb{P}^2$. The projective plane consists of homogeneous coordinates $[x : y : z]$, where x, y, z are not all zero, and two triples represent the same point if they are scalar multiples: $[x : y : z] = [\lambda x : \lambda y : \lambda z]$ for any $\lambda \neq 0$.

The equation $x^2 + y^2 = z^2$ defines a projective curve in $\mathbb{P}^2$, denoted by C.

For the curve $C : x^2+y^2 = z^2$, we verify that the point $P = [-1 : 0 : 1]$ is a rational point (it satisfies the equation). Using this point, we construct a parametrization as follows:

1 Consider lines through P and a variable point, with slope controlled by a parameter t. In projective coordinates, a more rigorous approach uses homogeneous parameters $[m : n] \in \mathbb{P}^1$.

A common choice: take the line through P with equation $y = t(x + z)$, where $t \in \mathbb{Q}$. Homogenize by setting $t = m/n$ (with m, n not both zero), then the line equation becomes $ny = m(x + z)$.

2 Solve the system of the line equation and the curve equation. Substitute $y = t(x + z)$ into $x^2 + y^2 = z^2$:

$$x^2 + t^2(x + z)^2 = z^2.$$

Simplify:

$$x^2 - z^2 + t^2(x + z)^2 = 0 \quad \Rightarrow \quad (x - z)(x + z) + t^2(x + z)^2 = 0.$$

Factor out $(x + z)$:

$$(x + z)\big[(x - z) + t^2(x + z)\big] = 0.$$

The first factor $x + z = 0$ gives the known point P. The second factor gives:

$$x - z + t^2(x + z) = 0 \quad \Rightarrow \quad (1 + t^2)x + (t^2 - 1)z = 0.$$

Solve for x in terms of z: $x = \frac{1-t^2}{1+t^2}z$. Substitute back into the line equation $y = t(x + z)$:

$$y = t\left(\frac{1 - t^2}{1 + t^2}z + z\right) = t \cdot \frac{2z}{1 + t^2} = \frac{2t}{1 + t^2}z.$$

Therefore, the intersection point (excluding P) has coordinates:

$$[x : y : z] = \left[\frac{1 - t^2}{1 + t^2} : \frac{2t}{1 + t^2} : 1\right].$$

3 To clear denominators, set $t = m/n$ and multiply by $m^2 + n^2$ (note: $1 + t^2 = \frac{m^2+n^2}{n^2}$):

$$x = \frac{1 - \frac{m^2}{n^2}}{1 + \frac{m^2}{n^2}} = \frac{n^2 - m^2}{m^2 + n^2}, \quad y = \frac{2\frac{m}{n}}{1 + \frac{m^2}{n^2}} = \frac{2mn}{m^2 + n^2}, \quad z = 1.$$

To obtain integer coordinates, we scale by $m^2 + n^2$ to get homogeneous coordinates:

$$[x : y : z] = [n^2 - m^2 : 2mn : m^2 + n^2].$$

Adjusting signs (swap m and n or change sign) yields the familiar Pythagorean triple formula:

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

P.S.:The above process defines a map from parameters $[m : n] \in \mathbb{P}^1$ to points on C (except for parameters that make denominators zero, such as $t = \pm i$, which are not considered over the rationals). Conversely, from a point (x, y, z) on C (other than P), we can recover the parameter $t = \frac{y}{x+z}$. Thus, the map is birational, establishing an isomorphism between C and $\mathbb{P}^1$.

How about the nonhomogeneous quadratic equations? We can do homogenization on them.

Example 2 (Pell's equation)**.** Pell's equation is the Diophantine equation of the form

$$x^2 - dy^2 = 1,$$

where d is a positive non-square integer.

We homogenize the equation to

$$E : x^2 - dy^2 = z^2,$$

which defines a conic in the projective plane. The integer points of the original equation correspond to points on E with $z = 1$. The curve E has genus zero and is isomorphic over $\mathbb{Q}$ to the projective line $\mathbb{P}^1$; hence it possesses infinitely many rational points.

Fix the obvious rational point $O = (1, 0)$ (with $z = 1$). Let a line through O have slope m:

$$y = m(x - 1).$$

Substituting into $x^2 - dy^2 = 1$ gives

$$x^2 - dm^2(x-1)^2 = 1.$$

Since $x = 1$ is a solution, the other intersection point is found by factoring:

$$x = \frac{1 + dm^2}{1 - dm^2}, \qquad y = \frac{2m}{1 - dm^2}.$$

As m runs through the rational numbers, we obtain all rational points on E (the point O corresponds to $m = 0$).

P.S.: Actually, suppose $u_1 = x_1 + y_1\sqrt{d}$, where for some $m \in \mathrm{R}$, we have solution $P_1 = (x_1, y_1)$. Then we can compute all the solution $P_n = (x_n, y_n)$ given by

$$\begin{cases} x_{n+1} = x_1 x_n + d\, y_1 y_n, \\ y_{n+1} = x_1 y_n + y_1 x_n. \end{cases}$$

1.2 Treatment of homogeneous quadratic polynomials

More generally, consider the homogeneous quadratic polynomial

$$Q(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j \quad (a_{ij} \in \mathbb{Q})$$

which defines a projective quadric hypersurface:

$$X : Q(x_1, \ldots, x_n) = 0 \subset \mathbb{P}^{n-1}_{\mathbb{Q}}.$$

The polynomial Q can be written in matrix form as:

$$Q(\mathbf{x}) = \mathbf{x}^T A \mathbf{x}, \quad \mathbf{x} = (x_0, \ldots, x_n)^T,$$

where A is a symmetric matrix with coefficients in $\mathbb{Q}$. Since the characteristic of $\mathbb{Q}$ is not 2, any symmetric matrix can be **congruently diagonalized** over $\mathbb{Q}$: there exists an invertible matrix $P \in \mathrm{GL}_{n+1}(\mathbb{Q})$ such that:

$$P^T A P = D = \mathrm{diag}(a_0, \ldots, a_n).$$

Setting $\mathbf{y} = P^{-1}\mathbf{x}$ (i.e., $\mathbf{x} = P\mathbf{y}$), we obtain:

$$Q(\mathbf{x}) = \mathbf{x}^T A \mathbf{x} = \mathbf{y}^T (P^T A P)\mathbf{y} = \mathbf{y}^T D \mathbf{y} = a_0 y_0^2 + \cdots + a_n y_n^2.$$

Thus, via the linear transformation $\mathbf{x} = P\mathbf{y}$, the quadratic form becomes diagonal.

Lemma 3. Through coordinate transformation, we can transform any homogeneous quadratic polynomial Q into the following form:

$$Q(\mathbf{y}) = a_0 y_0^2 + \cdots + a_n y_n^2.$$

Example 4. Consider

$$Q(x, y, z) = 2x^2 + 3xy + y^2 - xz + 2z^2.$$

The symmetric matrix A such that $Q(\mathbf{x}) = \mathbf{x}^T A \mathbf{x}$ is:

$$A = \begin{pmatrix} 2 & \frac{3}{2} & -\frac{1}{2} \\ \frac{3}{2} & 1 & 0 \\ -\frac{1}{2} & 0 & 2 \end{pmatrix}.$$

(Cross-term coefficients are halved: e.g., $3xy = 2 \cdot \frac{3}{2}xy$, so $a_{12} = a_{21} = \frac{3}{2}$.)

Treat Q as a polynomial in x:

$$Q = 2x^2 + (3y - z)x + (y^2 + 2z^2).$$

Complete the square for x:

$$\begin{aligned} 2x^2 + (3y - z)x &= 2\left[x^2 + \frac{3y - z}{2}x\right] \\ &= 2\left[\left(x + \frac{3y - z}{4}\right)^2 - \left(\frac{3y - z}{4}\right)^2\right]. \end{aligned}$$

Substitute back:

$$Q = 2\left(x + \frac{3y - z}{4}\right)^2 - \frac{(3y - z)^2}{8} + y^2 + 2z^2.$$

Introduce new variable $X = x + \frac{3y - z}{4}$ and the remaining part is:

$$R(y, z) = -\frac{1}{8}(3y - z)^2 + y^2 + 2z^2.$$

Expand $(3y - z)^2 = 9y^2 - 6yz + z^2$:

$$R = -\frac{9}{8}y^2 + \frac{6}{8}yz - \frac{1}{8}z^2 + y^2 + 2z^2 = -\frac{1}{8}y^2 + \frac{3}{4}yz + \frac{15}{8}z^2.$$

Write R as a polynomial in y:

$$R = -\frac{1}{8}y^2 + \frac{3}{4}z \cdot y + \frac{15}{8}z^2.$$

Complete the square:

$$\begin{aligned} -\frac{1}{8}y^2 + \frac{3}{4}zy &= -\frac{1}{8}\left(y^2 - 6z \cdot y\right) \\ &= -\frac{1}{8}\left[(y-3z)^2 - 9z^2\right] \\ &= -\frac{1}{8}(y-3z)^2 + \frac{9}{8}z^2. \end{aligned}$$

Thus,

$$R = -\frac{1}{8}(y-3z)^2 + \frac{9}{8}z^2 + \frac{15}{8}z^2 = -\frac{1}{8}(y-3z)^2 + 3z^2.$$

Introduce new variables $Y = y - 3z$ and $Z = z$. Then we obtain the diagonal form:

$$Q = 2X^2 - \frac{1}{8}Y^2 + 3Z^2.$$

This is $aX^2 + bY^2 + cZ^2$ with $a = 2$, $b = -\frac{1}{8}$, $c = 3$ and the transformation matrix P (satisfying $\mathbf{x} = P\mathbf{y}$ where $\mathbf{y} = (X, Y, Z)^T$) is:

$$P = \begin{pmatrix} 1 & -\frac{3}{4} & -2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}.$$

.

Since P is invertible with entries in $\mathbb{Q}$, this transformation defines an **automorphism** of projective space $\mathbb{P}^n$, preserving the existence of rational points: $X(\mathbb{Q}) \neq \emptyset$ if and only if the diagonalized equation has a nontrivial rational solution.

Chapter 2

Main Theorem

2.1 Statement of main theorem

We have a homogeneous quadratic polynomial

$$Q(\mathbf{y}) = a_0 y_0^2 + \cdots + a_n y_n^2$$

and a quadratic hypersurface X in $\mathbb{P}^{n-1}$, i.e.

$$X : Q(\mathbf{y}) = a_0 y_0^2 + \cdots + a_n y_n^2 = 0.$$

Theorem 1 (Hasse–Minkowski Theorem)**.** $X(\mathbb{Q}) \neq \varnothing$ if and only if $X(\mathbb{R}) \neq \varnothing$ and $X(\mathbb{Q}_p) \neq \varnothing$ for every prime number p.

However, there is a very strange sense for this theorem: we have $\mathbb{Q}$ is dense in $\mathbb{R}$. Then, $X(\mathbb{Q})$ is dense in $X(\mathbb{R})$ (which is actually wrong), which implies that if $X(\mathbb{R}) \neq \varnothing$, then $X(\mathbb{Q}) \neq \varnothing$?

Here is a counterexample:

Example 5. Consider

$$x^2 + y^2 = 3z^2.$$

1 Real Solutions:

Taking $z = 1$, the equation becomes $x^2 + y^2 = 3$, which represents a circle of radius $\sqrt{3}$. There are infinitely many real points, so

$$X(\mathbb{R}) \neq \emptyset.$$

2 Rational Solutions:

Suppose there exists a non-trivial rational solution, i.e., integers x, y, z not all zero with $\gcd(x, y, z) = 1$ satisfying

$$x^2 + y^2 = 3z^2.$$

If $z = 0$, then $x^2 + y^2 = 0$ forces $x = y = 0$, contradiction. So $z \neq 0$.

- **Modulo 3 analysis:** Squares modulo 3 are either 0 or 1. The equation modulo 3 gives
$$x^2 + y^2 \equiv 0 \pmod 3.$$
If $x^2 \equiv 1$, then we would need $y^2 \equiv 2$, impossible. Hence $x^2 \equiv 0$ and $y^2 \equiv 0$, so $3 \mid x$ and $3 \mid y$.
- Write $x = 3a$, $y = 3b$. Substituting:
$$9a^2 + 9b^2 = 3z^2 \implies 3(a^2 + b^2) = z^2.$$
Thus $3 \mid z^2$, and since 3 is prime, $3 \mid z$. Write $z = 3c$. Then
$$3(a^2 + b^2) = 9c^2 \implies a^2 + b^2 = 3c^2.$$
So (a, b, c) is another integer solution. But then $\gcd(a, b, c) = \frac{1}{3}\gcd(x, y, z)$, contradicting the coprimality of (x, y, z). Hence no non-trivial integer solution exists, so
$$X(\mathbb{Q}) = \emptyset.$$

2.2 Proof of main theorem in arithmetic

2.2.1 Preliminaries

Local fields and completions

For the rational numbers $\mathbb{Q}$, we consider the following completions:

- The real field $\mathbb{R}$, denoted by $\mathbb{Q}_\infty$.
- The p-adic fields $\mathbb{Q}_p$ for each prime number p.

Let V denote the set of all such *places* v (including the infinite place). For a quadratic form f over $\mathbb{Q}$ and a place $v \in V$, we denote by f_v the quadratic form obtained by extending scalars to $\mathbb{Q}_v$.

The Hilbert symbol

For a local field k (either $\mathbb{R}$ or $\mathbb{Q}_p$) and $a, b \in k^*$, the *Hilbert symbol* $(a,b)_v \in \{\pm 1\}$ is defined by

$$(a,b)_v = 1 \iff \text{the equation } z^2 - ax^2 - by^2 = 0 \text{ has a nontrivial solution in } k^3.$$

The Hilbert symbol is bilinear, nondegenerate, and satisfies the product formula for $a, b \in \mathbb{Q}^*$:

$$\prod_{v \in V} (a,b)_v = 1.$$

Local invariants of quadratic forms

For a quadratic form $f \sim a_1 x_1^2 + \cdots + a_n x_n^2$ over a local field k, we define:

- The *discriminant* $d(f) = a_1 \cdots a_n \in k^*/k^{*2}$.
- The *invariant* $\varepsilon(f) = \prod_{1 \le i < j \le n} (a_i, a_j)_v \in \{\pm 1\}$.

The following theorem characterizes the representation of zero by quadratic forms over local fields.

Theorem 1 (Local representation of zero)**.** Let f be a nondegenerate quadratic form over a local field k (with $k \neq \mathbb{Q}_2$ for simplicity). Then:

1. If $n = 2$, f represents zero if and only if $d(f) = -1$ in k^*/k^{*2}.
2. If $n = 3$, f represents zero if and only if $(-1, -d(f))_v = \varepsilon(f)$.
3. If $n = 4$, f represents zero unless $d(f) = 1$ and $\varepsilon(f) = -(-1,-1)_v$.
4. If $n \ge 5$, f always represents zero.

2.2.2 Key lemmas

We recall two important lemmas that will be used in the proof.

Lemma 6 (Approximation theorem)**.** Let $S \subset V$ be a finite set of places. The image of $\mathbb{Q}$ in the product $\prod_{v \in S} \mathbb{Q}_v$ is dense.

Lemma 7 (Existence of a global element with prescribed Hilbert symbols)**.** Let $(a_i)_{i \in I}$ be a finite family in $\mathbb{Q}^*$ and let $(\varepsilon_{i,v})_{i \in I, v \in V}$ be a family of numbers ± 1 such that:

1. For each i, almost all $\varepsilon_{i,v} = 1$.
2. For each i, $\prod_{v \in V} \varepsilon_{i,v} = 1$.
3. For each $v \in V$, there exists $x_v \in \mathbb{Q}_v^*$ such that $(a_i, x_v)_v = \varepsilon_{i,v}$ for all i.

Then there exists $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all i and all $v \in V$.

2.2.3 Proof of main theorem

Theorem 2 (Hasse–Minkowski in arithmetic way)**.** A quadratic form f over $\mathbb{Q}$ represents zero (nontrivially) if and only if for every place $v \in V$, the form f_v represents zero over $\mathbb{Q}_v$.

Proof. The necessity is obvious since $\mathbb{Q}$ embeds into each $\mathbb{Q}_v$. We prove the sufficiency by induction on the number of variables n. Without loss of generality, we assume f is nondegenerate and diagonalized:

$$f = a_1 x_1^2 + \cdots + a_n x_n^2, \quad a_i \in \mathbb{Q}^*.$$

Case $n = 2$

Let $f = x_1^2 - a x_2^2$. The condition that f_v represents zero for all v implies that a is a square in every $\mathbb{Q}_v$. In particular, $a > 0$ in $\mathbb{R}$, and for each prime p, the p-adic valuation $v_p(a)$ is even. Hence a is a square in $\mathbb{Q}$, so f represents zero over $\mathbb{Q}$.

Case $n = 3$ (Legendre's theorem)

Let $f = x_1^2 - a x_2^2 - b x_3^2$. We may assume a and b are square-free integers and $|a| \leq |b|$. We proceed by induction on $m = |a| + |b|$. If $m = 2$, the only possibilities (up to equivalence) are $x_1^2 - x_2^2 - x_3^2$, $x_1^2 - x_2^2 + x_3^2$, etc., all of which represent zero over $\mathbb{Q}$ except possibly $x_1^2 + x_2^2 + x_3^2$, but the latter does not represent zero over $\mathbb{R}$ and is excluded by hypothesis.

Assume $m > 2$. Write $b = \pm p_1 \cdots p_k$ with distinct primes p_i. For each $p = p_i$, since f represents zero over $\mathbb{Q}_p$, a standard argument shows that a is a square modulo p. By the Chinese remainder theorem, there exists an integer t such that

$$t^2 \equiv a \pmod{b}, \quad |t| \leq \frac{|b|}{2}.$$

Set $bb' = t^2 - a$. Then $|b'| < |b|$. Consider the form

$$f' = x_1^2 - a x_2^2 - b' x_3^2.$$

One checks that f' represents zero over every $\mathbb{Q}_v$ (using the fact that bb' is a norm from $\mathbb{Q}(\sqrt{a})$). By the induction hypothesis, f' represents zero over $\mathbb{Q}$, hence so does f.

Case $n = 4$

Write $f = ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2)$. For each place v, since f_v represents zero, there exists $x_v \in \mathbb{Q}_v^*$ that is represented by both $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$. In terms of Hilbert symbols, this means

$$(x_v, -ab)_v = (a, b)_v \quad \text{and} \quad (x_v, -cd)_v = (c, d)_v.$$

The families $(a, b)_v$ and $(c, d)_v$ satisfy the product formula. By Lemma 2, there exists a global $x \in \mathbb{Q}^*$ such that

$$(x, -ab)_v = (a, b)_v \quad \text{and} \quad (x, -cd)_v = (c, d)_v \quad \text{for all } v.$$

Now consider the ternary form $ax_1^2 + bx_2^2 - xz^2$. It represents zero over every $\mathbb{Q}_v$ (by the condition on the Hilbert symbol), hence by the case $n = 3$, it represents zero over $\mathbb{Q}$. Therefore x is represented by $ax_1^2 + bx_2^2$ over $\mathbb{Q}$. Similarly, x is represented by $cx_3^2 + dx_4^2$ over $\mathbb{Q}$. Consequently, f represents zero over $\mathbb{Q}$.

Case $n \geq 5$

We proceed by induction on n. Write $f = h - g$ with

$$h = a_1x_1^2 + a_2x_2^2, \quad g = -(a_3x_3^2 + \cdots + a_nx_n^2).$$

Let S be the finite set of places consisting of ∞, 2, and all primes dividing any of the coefficients $a_3, \ldots, a_n$. For each $v \in S$, since f_v represents zero, there exists $a_v \in \mathbb{Q}_v^*$ represented by both h and g. By the approximation theorem (Lemma 6), we can choose $x_1, x_2 \in \mathbb{Q}$ such that if $a = h(x_1, x_2)$, then $a/a_v \in \mathbb{Q}_v^{*2}$ for all $v \in S$.

Consider the form $f_1 = az^2 - g$. For $v \in S$, since g represents a_v and a/a_v is a square, g represents a over $\mathbb{Q}_v$, so f_1 represents zero over $\mathbb{Q}_v$. For $v \notin S$, the coefficients of g are units at v, and one can show (using direct computation) that g represents a over $\mathbb{Q}_v$. Hence f_1 represents zero over every $\mathbb{Q}_v$. Since f_1 has rank $n - 1$, by the induction hypothesis, f_1 represents zero over $\mathbb{Q}$. Thus g represents a over $\mathbb{Q}$, and since h clearly represents a, it follows that f represents zero over $\mathbb{Q}$.

This completes the induction and the proof of the Hasse–Minkowski theorem. □

2.3 Another way to understand the main theorem

2.3.1 Preliminary Definitions and Theorems

The Brauer Group

Definition 8. A **central simple algebra (CSA)** over a field k is a finite-dimensional k-algebra that is simple and has centre k.

Definition 9. Two CSAs A and B over k are **similar**, denoted $A \sim B$, if there exist integers m, n such that

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

Definition 10. The set of similarity classes $[A]$ forms an abelian group under $\otimes_k$, called the **Brauer group** of k, denoted $\mathrm{Br}(k)$.

Local and Global Points

Let Ω_K be the set of all places (including infinite ones) of K. For each $v \in \Omega_K$, denote by K_v the completion. Define the **adele ring**:

$$\mathbb{A}_K = \left\{ (x_v)_v \in \prod_{v \in \Omega_K} K_v \;\middle|\; \text{for almost all finite places } v,\ x_v \in \mathcal{O}_v \right\},$$

where $\mathcal{O}_v$ is the ring of integers of K_v.

For an algebraic variety X/K, its set of **adèlic points** is defined as:

$$X(\mathbb{A}_K) = \left\{ (P_v)_v \in \prod_v X(K_v) \;\middle|\; P_v \in X(\mathcal{O}_v) \text{ for almost all finite places } v \right\}.$$

Splitting Fields

Definition 11. A field extension L/k is a **splitting field** for a CSA A if $A \otimes_k L \cong M_n(L)$ for some n.

Definition 12. For a Galois extension L/k, define

$$\mathrm{Br}(L/k) = \ker\left(\mathrm{Br}(k) \to \mathrm{Br}(L)\right),$$

the subgroup of $\mathrm{Br}(k)$ consisting of classes split by L.

Cohomological Interpretation

Definition 13. For a finite Galois extension L/k with group $G = \mathrm{Gal}(L/k)$, let

$$H^2(L/k) = H^2(G, L^\times).$$

Theorem 3 (Theorem 3.14)**.** The map

$$\varphi \mapsto [A(\varphi)], \quad H^2(L/k) \xrightarrow{\sim} \mathrm{Br}(L/k)$$

is a group isomorphism, where $A(\varphi)$ is the **crossed-product algebra** associated to a 2-cocycle $\varphi : G \times G \to L^\times$.

Corollary 1 (Corollary 3.16)**.** For a separable algebraic closure k^{al} of k,

$$\mathrm{Br}(k) \cong H^2(k^{\mathrm{al}}/k) = \varinjlim_{L/k \text{ finite Galois}} H^2(L/k).$$

Maximal Subfields and Invariants

Let K be a nonarchimedean local field with residue field k of cardinality q. For a central division algebra D over K, let $n^2 = [D : K]$.

Proposition 14 (Proposition 3.8, Corollary 3.10 in J.S.Milne's CFT note)**.** D contains a maximal subfield L that is separable over K. For local fields, one can choose L to be **unramified** over K.

The valuation $|\cdot|$ on K extends uniquely to D, and we define $\mathrm{ord}(\alpha)$ for $\alpha \in D$ by $|\alpha| = q^{-\mathrm{ord}(\alpha)}$.

Theorem 4 (Noether–Skolem)**.** Let L be an unramified maximal subfield of D, and let σ be the Frobenius automorphism of L/K. There exists $\alpha \in D$ such that

$$\sigma(x) = \alpha x \alpha^{-1} \quad \forall x \in L.$$

Definition 15. Define

$$\mathrm{inv}_K(D) = \mathrm{ord}(\alpha) \bmod \mathbb{Z}.$$

This depends only on the isomorphism class of D, hence gives a well-defined map

$$\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

Example 1. For the unramified extension L/K of degree n and the 2-cocycle φ described in the text, we have

$$\mathrm{inv}_K(A(\varphi)) = \frac{1}{n} \bmod \mathbb{Z}.$$

2.3.2 Brauer–Manin Obstruction

Definition 16. Each element $\alpha \in \mathrm{Br}(X)$ defines a pairing:

$$\mathrm{ev}_\alpha : X(\mathbb{A}_K) \to \mathbb{Q}/\mathbb{Z}, \quad (P_v) \mapsto \sum_v \mathrm{inv}_v(\alpha(P_v)).$$

And the **Brauer set**:

$$X(\mathbb{A}_K)^{\mathrm{Br}} = \bigcap_{\alpha \in \mathrm{Br}(X)} \ker(\mathrm{ev}_\alpha).$$

It is known that:

$$\overline{X(K)} \subseteq X(\mathbb{A}_K)^{\mathrm{Br}} \subseteq X(\mathbb{A}_K),$$

where $\overline{X(K)}$ denotes the closure of the set of global points in the adelic space.

Theorem 5. Let $X \subset \mathbb{P}^m_K$ be a quadric hypersurface (defined by a quadratic form). Then the following are equivalent:

1. $X(\mathbb{A}_K) \neq \varnothing$ (existence of local points)
2. $X(K) \neq \varnothing$ (existence of a global point)
3. $X(\mathbb{A}_K)^{\mathrm{Br}} \neq \varnothing$ (vanishing of the Brauer–Manin obstruction)

Here we give a Proof sketch of this theorem, which involves some theorems in Globle Class Field Theory.

Proof.

- The equivalence (1) $\Leftrightarrow$ (2) is the Hasse–Minkowski theorem.
- Since X is rational $\Rightarrow \mathrm{Br}(X)/\mathrm{Br}(K) = 0$, for any adelic point (P_v) and any $\alpha \in \mathrm{Br}(X)$, we have

  $$\sum_v \mathrm{inv}_v(\alpha(P_v)) = 0$$

  (because α actually comes from $\mathrm{Br}(K)$, and global reciprocity ensures the sum vanishes). Hence $X(\mathbb{A}_K)^{\mathrm{Br}} = X(\mathbb{A}_K)$, so (1) $\Leftrightarrow$ (3).

□