Hasse Principle

Nirvana Coppola María Inés de Frutos-Fernández Mallory Dolorfino
Kate Finnerty Catherine Hsu Chi-Yun Hsu

July 27, 2026

Chapter 1

p-adic Fields

1.1 p-adic Equations

Definition 1.1.1. *Let R be a ring. An element $(x_1, \cdots, x_n) \in R^n$ is* primitive *if at least one of the x_i is invertible.*

Proposition 1.1.2. *Let $f^{(i)} \in \mathbb{Z}_p[X_1, \cdots, X_m]$ be homogeneous polynomials with p-adic integer coefficients. For each $n \geq 1$, denote by $f_n^{(i)}$ the reduction of $f^{(i)}$ modulo p^n. The following are equivalent:*

a) The $f^{(i)}$ have a nontrivial common zero in $\mathbb{Q}_p^m$.

b) The $f^{(i)}$ have a common primitive zero in $\mathbb{Z}_p^m$.

c) For all $n \geq 1$, the $f_n^{(i)}$ have a common primitive zero in $(\mathbb{Z}/p^n\mathbb{Z}_p)^m$.

Proof. The implication (b) $\implies$ (a) is trivial. Conversely, if $x = (x_1, \cdots, x_m) \in \mathbb{Q}_p^m$ is a nontrivial common zero of the $f^{(i)}$, put

$$h := \min(v_p(x_1), \cdots, v_p(x_m)) \quad \text{and} \quad y := p^{-h}x.$$

Then $y \in \mathbb{Z}_p^m$ is a common primitive zero of the $f^{(i)}$. For the equivalence (b) $\iff$ (c), Serre applies the first Lemma from [Ser73, §II.2.1]. However, using `Mathlib`'s `DirectLimit` definition here might be tricky. It could be easier to just prove this specific result; note that the file `Mathlib.NumberTheory.Padics.RingHoms` contains useful results relating $\mathbb{Z}_p$ and $\mathbb{Z}/p^n\mathbb{Z}$ (without relying on `DirectLimit`).

□

1.2 Squares in $\mathbb{Q}_p^\times$

Theorem 1.2.1. *${\mathbb{Q}_p^\times}^2$ is an open subgroup of $\mathbb{Q}_p^\times$.*

Proof. The only nontrivial part is to show that the squares form an open set. Since $\mathbb{Q}_p$ is a field, the unit topology agrees with the subspace topology, so it suffices to check that the set of nonzero squares in $\mathbb{Q}_p$ is open. Define r as 1 if p is odd, or as 2^{-2} if $p = 2$, and denote by $B_{1,r}$ the open ball with center 1 and radius r. For each $c \in B_{1,r}$, by applying Hensel's lemma with

the polynomial $X^2 - c$, we obtain that c is a square. Then, for each nonzero square $s \in \mathbb{Q}_p$, $s \cdot B_{1,r}$ is an open neighbourhood of s contained in the set of nonzero squares, which shows that the latter is open. See [Ser73, §II.3.3] for more details. □

Lemma 1.2.2. *Let p be a prime, let $f \in \mathbb{Z}_p[X_1, \cdots, X_m]$ be a polynomial with p-adic integer coefficients, and let $x \in (\mathbb{Z}/p\mathbb{Z})^m$ be a zero of f modulo p^n, for some positive integer n. Suppose that, for some $j \in \{1, \cdots, m\}$, the partial derivative $\frac{\partial f}{\partial X_j}(x)$ is nonzero modulo p^k, where $0 < 2k < n$. Then there exists a zero z of f in $\mathbb{Z}_p^m$ whose reduction modulo p^n is x, and such that $z - x$ is divisible by p^{n-k}.*

Proof. This is in Serre's [Ser73, §II.2 Theorem 1]. □

1.3 Units and Legendre symbols

Lemma 1.3.1. *Let p be a prime, let $x \in \mathbb{Q}_p^\times$, and let v_p denote the p-adic valuation. Then $\|x \cdot p^{-v_p(x)}\| = 1$.*

Proof. Straightforward. □

Definition 1.3.2. *Let p be a prime and $x \in \mathbb{Q}_p^\times$. The* unit part *of x is defined as the element of $\mathbb{Z}_p^\times$ corresponding to $x \cdot p^{-v_p(x)}$.*

Definition 1.3.3. *Let p be a prime and $u \in \mathbb{Z}_p^\times$. The* Legendre symbol $\left(\frac{u}{p}\right)$ *is defined as*

$$\left(\frac{u}{p}\right) = \left(\frac{\overline{u}}{p}\right),$$

where $\overline{u}$ is the image of u under the natural map $\mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$.

Chapter 2

Hilbert symbol

2.1 Hilbert symbol over a field

Definition 2.1.1. *Let k be a field and $a, b \in k$. If both a, b are nonzero, the* Hilbert symbol $(a, b)_k$ *is defined as follows: if there exist $x, y, z \in k$, not all zero, such that $z^2 = ax^2 + by^2$, then $(a, b)_k = 1$; otherwise, $(a, b)_k = -1$. If one of a, b is zero, we set $(a, b)_k = 0$.*

2.1.1 Basic properties of the Hilbert symbol

The Hilbert symbol has the following properties, useful for computing it in practice.

Lemma 2.1.2. *Let $a, b, a', b' \in k^\times$. Then $(aa'^2, bb'^2)_k = (a, b)_k$.*

Proof. Let $x, y, z \in k$ be such that $z^2 = aa'^2x^2 + bb'^2y^2$. Then, xa', yb', z are not all zero and satisfy $z^2 = ax^2 + by^2$. Conversely, if $x, y, z \in k$ are such that $z^2 = ax^2 + by^2$, then $x/a', y/b', z$ are not all zero and satisfy $z^2 = aa'^2x^2 + bb'^2y^2$. □

The following lemma uses the definition QuadraticAlgebra from `Mathlib`.

Lemma 2.1.3. *Let $a, b \in k^\times$. Then $(a, b)_k = 1$ if and only if there exists $t \in k(\sqrt{b})$ such that $a = N_{k(\sqrt{b})/k}(t)$.*

Proof.

- Case b is a square in k. Then $k(\sqrt{b}) = k$, and the norm map is the identity, so a is always the norm of itself. Let $c \in k^\times$ be such that $c^2 = b$. Then $c^2 = a \cdot 0^2 + b \cdot 1^2$, so $(a, b)_k = 1$.
- Case b is not a square in k. Then $k(\sqrt{b})$ is a quadratic extension of k, and the norm map is given by $N_{k(\sqrt{b})/k}(p + q\sqrt{b}) = p^2 - bq^2$. Suppose a is a norm, so it satisfies $a = p^2 - bq^2$ for some $p, q \in k$. Then $1, q, p$ are not all zero and satisfy $p^2 = a \cdot 1^2 + b \cdot q^2$, so $(a, b)_k = 1$. Conversely, if x, y, z are not all zero and satisfy $z^2 = ax^2 + by^2$, then $x = 0$, since otherwise b would be a square in k, which contradicts our assumption. Then $x \neq 0$, and we have $a = (z/x)^2 - b(y/x)^2$, so a is a norm.

□

Proposition 2.1.4. *The Hilbert symbol statisfies the following formulas:*

(i) For $a, b \in k$, we have $(a, b)_k = (b, a)_k$.

(ii) *Let $a, c \in k^\times$. Then $(a, c^2)_k = 1$.*

(iii) *For $a \in k^\times$, we have $(a, -a)_k = 1$.*

(iv) *Let $a \in k$ with $a \neq 0, 1$. Then $(a, 1-a)_k = 1$.*

(v) *Let $a, a', b \in k^\times$ and assume that $(a, b)_k = 1$. Then $(aa', b)_k = (a', b)_k$.*

(vi) *Let $a, b \in k$. Then $(a, -ab)_k = (a, b)_k$.*

(vii) *Let $a, b \in k^\times$ with $a \neq 1$. Then $(a, (1-a)b)_k = (a, b)_k$.*

Proof.

- Trivial if a or b are zero. Otherwise, if x, y, z is a solution to $z^2 = ax^2 + by^2$, then y, x, z is a solution to $z^2 = bx^2 + ay^2$.
- In this case, $c^2 = a \cdot 0^2 + b \cdot 1^2$, so $(a, b)_k = 1$. N.B. Alternatively: the same argument as in the first case of the proof of Lemma 2.1.3 applies.
- In this case, $0 = a \cdot 1^2 + (-a) \cdot 1^2$.
- In this case, $1 = a \cdot 1^2 + (1-a) \cdot 1^2$.
- We know, by Lemma 2.1.3, that there exists $t \in k(\sqrt{b})$ such that $a = N_{k(\sqrt{b})/k}(t)$. If $(a', b)_k = 1$, then a' is the norm of some $t' \in k(\sqrt{b})$, so $aa' = N_{k(\sqrt{b})/k}(tt')$, so $(aa', b)_k = 1$. Conversely, if $(aa', b)_k = 1$, then $aa' = N_{k(\sqrt{b})/k}(t'')$ for some $t'' \in k(\sqrt{b})$, so $a' = N_{k(\sqrt{b})/k}(t''/t)$, hence $(a', b)_k = 1$.
- Trivial if a or b are zero. Otherwise it follows from the previous steps, since $(a, -a)_k = 1$.
- Follows from the previous steps, since $(a, 1-a)_k = 1$.

□

2.1.2 Local Properties

We now specialize to the case where k is either $\mathbb{R}$ or $\mathbb{Q}_p$ for some prime p. In this case, the Hilbert symbol can be computed explicitly.

Theorem 2.1.5. *Let $a, b \in \mathbb{R}^\times$. Then $(a, b)_{\mathbb{R}} = 1$ if and only if $a > 0$ or $b > 0$; otherwise $(a, b)_{\mathbb{R}} = -1$.*

Proof. If $a > 0$, then $(1, 0, \sqrt{a})$ works. Similarly, if $b > 0$, then $(0, 1, \sqrt{b})$ works. If both a and b are negative, then $ax^2 + by^2 \leq 0$ for all x, y, so there is no nontrivial solution to $z^2 = ax^2 + by^2$. □

The following uses the `Mathlib` API for p-adic numbers and integers, as well as the results from the files HassePrinciple/Padics/Lemmas.lean and HassePrinciple/Padics/Legendre.lean.

For the statement of the theorem in the p-adic case, we need the following definitions.

Definition 2.1.6. *Let $u \in (\mathbb{Z}_2)^\times$. We define $\epsilon(u)$ to be the class modulo 2 of $\dfrac{u-1}{2}$.*

Definition 2.1.7. *Let $u \in (\mathbb{Z}_2)^\times$. We define $\omega(u)$ to be the class modulo 2 of $\dfrac{u^2-1}{8}$.*

For the proof, we will need the following lemma.

Lemma 2.1.8. *Let p be a prime and let $v \in (\mathbb{Q}_p)^\times$. Let $x, y, z \in \mathbb{Q}_p$ be such that $(x, y, z) \neq (0, 0, 0)$ and $z^2 - px^2 - vy^2 = 0$. Then there exist $z', y' \in (\mathbb{Z}_p)^\times$ and $x' \in \mathbb{Z}_p$ such that (z', y', x') is a nontrivial solution to the same equation.*

Proof. Let (x, y, z) be any nontrivial solution. For any $\lambda \neq 0$, also $(\lambda x, \lambda y, \lambda z)$ is a solution. Taking $\lambda = p^a$ for an appropriate a, we can assume that x, y, z are all in $\mathbb{Z}_p$ and at least one of them is a unit. Now, if z is not a unit, then $px^2 + vy^2$ is also not a unit, thus y is not a unit. Conversely if y is not a unit, then $z^2 - px^2$ is also not a unit, thus z is not a unit. This shows that if either y or z is not a unit, then they are both non units, but then p^2 would divide px^2, hence x would not be a unit either, contradicting the fact that one of x, y, z is a unit. □

We are now ready to compute the Hilbert symbol (a, b) in the p-adic case. We split the statement and the proof of the theorem for the p-adic into the cases where p is odd and where $p = 2$, and for each we first consider separately the cases where the valuations of a and b are both 0, both 1, or one of them is 0 and the other is 1.

Everywhere in the following, we assume that $a, b \in (\mathbb{Q}_p)^\times$, and denote by v_a and v_b their valuations, and by u_a and u_b their unit parts.

Theorem 2.1.9. *Let p be an odd prime and let $a, b \in (\mathbb{Q}_p)^\times$. Then*

$$(a, b) = (-1)^{v_a v_b \epsilon(p)} \left(\frac{u_a}{p}\right) \left(\frac{u_b}{p}\right),$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Proof. Since the Hilbert symbol is well defined up to squares, we can assume that $v_a, v_b \in \{0, 1\}$.

- Suppose $v_a = v_b = 0$. Then $a = u_a$ and $b = u_b$ are units. By the theorem of Chevalley–Warning, the equation $z^2 = u_a x^2 + u_b y^2$ has a nontrivial solution in $\mathbb{F}_p$, so it has a nontrivial solution in $\mathbb{Z}_p$ (by multivariate Hensel's lemma), so $(a, b) = 1$. Note: Chevalley–Warning is in `Mathlib` as char_dvd_card_solutions, in Mathlib.FieldTheory.ChevalleyWarning.

- Suppose $v_a = 1$ and $v_b = 0$. Then $a = pu_a$ and $b = u_b$. Since by the previous case, we have $(u_a, u_b) = 1$, we have $(a, b) = (pu_a, u_b) = (p, u_b)$. We just need to show that this is equal to $\left(\frac{u_b}{p}\right)$. Observe that a unit is a square in $\mathbb{Q}_p$ if and only if it is a square modulo p. Now, if u_b is a square, then both terms are 1, see 2.1.4. Otherwise, both terms are -1. In fact, if $z^2 - p^2x^2 - u_b y^2$ has a nontrivial solution, we can assume that z and u_b are units, so we can reduce modulo p to get $u_b = (zy^{-1})^2$, which is a contradiction.

- Suppose $v_a = v_b = 1$. Then $a = pu_a$ and $b = pu_b$. This case follows from the properties of the Hilbert symbol and the previous case: $(pu_a, pu_b) = (pu_a, -p^2 u_a u_b) = (pu_a, -u_a u_b) = \left(\frac{-u_a u_b}{p}\right)$. By the properties of the Legendre symbol, this is equal to $\left(\frac{-1}{p}\right)\left(\frac{u_a}{p}\right)\left(\frac{u_b}{p}\right)$, as claimed.

□

We proceed similarly for the case $p = 2$.

Theorem 2.1.10. *Let $x, y \in (\mathbb{Q}_2)^\times$. Then*

$$(a,b) = (-1)^{\epsilon(u_a)\epsilon(u_b)+v_a\omega(u_b)+v_b\omega(u_a)}.$$

Proof. Similarly to the previous case, we can assume that $v_a, v_b \in \{0,1\}$.
Case 1 Suppose $v_a = v_b = 0$. Then $a = u_a$ and $b = u_b$ are units. The claim is $(u_a, u_b) = (-1)^{\epsilon(u_a)\epsilon(u_b)}$, which is 1 exactly when at least one of u_a and u_b is congruent to 1 modulo 4 and -1 otherwise. Suppose first, without loss of generality, that $u_a \equiv 1 \pmod 4$. Then its residue class modulo 8 is either 1 or 5. In the first case, u_a is a square, so $(u_a, u_b) = 1$. In the second case, $u_a + 4u_b \equiv 1 \pmod 8$, so it is the square of some $win\mathbb{Z}_2$, so

$$w^2 - u_a \cdot 1^2 - u_b \cdot 2^2 = 0$$

and thus $(u_a, u_b) = 1$.

If $u_a \equiv u_b \equiv -1 \pmod 4$, then suppose there exist (x, y, z) not all zero, coprime, such that

$$z^2 - u_a x^2 - u_b y^2 = 0.$$

Reducing modulo 4, we obtain $z^2 + x^2 + y^2 \equiv 0 \pmod 4$, which is impossible, since the only squares modulo 4 are 0 and 1, and the sum can be 0 only if x, y, z are all even, contradicting the fact that they are coprime. Thus, $(u_a, u_b) = -1$. This proof uses ZMod.exists_sq_eq_two_iff from Mathlib.NumberTheory.LegendreSymbol.QuadraticReciprocity and hensels_lemma in Mathlib.NumberTheory.
Case 2 Suppose $v_a = 1$ and $v_b = 0$. Then $a = 2u_a$ and $b = u_b$. We first show that

$$(2, u_b) = (-1)^{\omega(u_b)},$$

i.e. that $(2, u_b) = 1$ if an only if $u_b \equiv \pm 1 \pmod 8$. Suppose that $(2, u_b) = 1$. Equivalently, there exist x, y, z not all zero, coprime, such that

$$z^2 - 2x^2 - u_b y^2 = 0.$$

By Lemma 2.1.8, we can assume that z and y are units. Reducing modulo 8, we get $1 - 2x^2 - u_b \equiv 0 \pmod 8$. Since squares modulo 8 are $0, 1$ and 4, we have $2x^2 \equiv 0$ or $2 \pmod 8$, so $u_b \equiv 1$ or $-1 \pmod 8$.

Conversely, if $u_b \equiv 1 \pmod 8$, then it is a square, so $(2, u_b) = 1$. If $u_b \equiv -1 \pmod 8$, then $z^2 - 2x^2 - u_b y^2 = 0$ has a solution modulo 8, namely $(1, 1, 1)$, which can be lifted to a solution in $\mathbb{Z}_2$ by Hensel's lemma (1.2.2), so $(2, u_b) = 1$. Now, if we prove that $(2u_a, u_b) = (u_a, u_b)(2, u_b)$, then we are done. If either factor is 1, by Proposition 2.1.4, we are done. Otherwise, both factors are -1, so by the above we know $u_a \equiv -1 \pmod 4$ and $u_b \equiv 3 \pmod 8$. Up to multiplying by squares, we can consider the following two cases:

- $u_a = -1, u_b = 3$. Then $(1, 1, 1)$ is a nontrivial solution to $z^2 + 2x^2 - 3y^2 = 0$.
- $u_a = 3, u_b = -5$. Then $(1, 1, 1)$ is a nontrivial solution to $z^2 - 6x^2 + 5y^2 = 0$.

Case 3 Suppose $v_a = v_b = 1$. Using Proposition 2.1.4 and the proof of the previous case, we have

$$(2u_a, 2u_b) = (2u_a, -4u_a u_b) = (2u_a, -u_a u_b) = (-1)^{\epsilon(u_a)\epsilon(-u_a u_b)+\omega(-u_a u_b)},$$

and a direct calculation shows that

$$\epsilon(u_a)\epsilon(-u_a u_b) + \omega(-u_a u_b) = \epsilon(u_a)\epsilon(u_b) + \omega(u_b) + \omega(u_a).$$

□

Theorem 2.1.11. *The Hilbert Symbol is bilinear in both variables, i.e. for all $a, a', b, b' \in k^\times$, we have*

$$(aa', b) = (a, b)(a'b) \quad \textit{and} \quad (a, bb') = (a, b)(a, b').$$

Proof. By symmetry, it is enough to show the first equality. If any of a, a', b is zero, then both sides are zero. We will assume that $a, a', b \neq 0$.

The real case is trivial: if $b > 0$, then all the Hilbert symbols are 1; otherwise, if a and a' have the same sign, then $(aa', b) = 1$ because $aa' > 0$, and $(a, b) = (a', b)$, so the right-hand side is also 1; if a and a' have different signs, then $(aa', b) = -1$ because $aa' < 0$, and $(a, b) = -(a', b)$, so the right-hand side is also -1.

We now assume that $k = \mathbb{Q}_p$. Suppose first that p is odd. By the formula in Theorem 2.1.9,

$$\begin{aligned}
(aa, b) = (-1)^{v_{aa'} v_b \epsilon(p)} \left(\frac{u_{aa'}}{p}\right)^{v_b} \left(\frac{u_b}{p}\right)^{v_{aa'}} = \\
= (-1)^{v_a + v_{a'} v_b \epsilon(p)} \left(\left(\frac{u_a}{p}\right)\left(\frac{u_{a'}}{p}\right)\right)^{v_b} \left(\frac{u_b}{p}\right)^{v_a + v_{a'}} = \\
= (-1)^{v_a v_b \epsilon(p)} (-1)^{v_{a'} v_b \epsilon(p)} \left(\frac{u_a}{p}\right)^{v_b} \left(\frac{u_{a'}}{p}\right)^{v_b} \left(\frac{u_b}{p}\right)^{v_a} \left(\frac{u_b}{p}\right)^{v_{a'}} = \\
(a, b)(a', b).
\end{aligned}$$

If $p = 2$, we use the formula in Theorem 2.1.10.

$$(aa', b) = (-1)^{\epsilon(u_{aa'})\epsilon(u_b) + v_{aa'}\omega(u_b) + v_b\omega(u_{aa'})} = (\bullet)$$

Since ϵ and ω are group homomorphisms from a multiplicative group to an additive group, we have

$$\begin{aligned}
(\bullet) = (-1)^{(\epsilon(u_a) + \epsilon(u_{a'}))\epsilon(u_b) + (v_a + v_{a'})\omega(u_b) + v_b(\omega(u_a) + \omega(u_{a'}))} = \\
= (-1)^{(\epsilon(u_a) + \epsilon(u_{a'}))\epsilon(u_b)} (-1)^{(v_a + v_{a'})\omega(u_b)} (-1)^{v_b(\omega(u_a) + \omega(u_{a'}))} = \\
= (-1)^{\epsilon(u_a)\epsilon(u_b)} (-1)^{\epsilon(u_{a'})\epsilon(u_b)} (-1)^{v_a\omega(u_b)} (-1)^{v_{a'}\omega(u_b)} (-1)^{v_b\omega(u_a)} (-1)^{v_b\omega(u_{a'})} = (a, b)(a', b)
\end{aligned}$$

□

2.1.3 Global properties of the Hilbert symbol

The main goal of this section is to prove the product formula for the Hilbert symbol, which states that for every $a, b \in \mathbb{Q}^\times$, we have

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

and the Existence Theorem, that states the existence of a rational number with prescribed Hilbert symbols. Here, V is the union of the set of prime numbers and the symbol ∞, and for each prime p, the symbol $(a, b)_p$ is the Hilbert symbol computed in $\mathbb{Q}_p$, while $(a, b)_\infty$ is the Hilbert symbol computed in $\mathbb{R}$.

Theorem 2.1.12. *Let $a, b \in \mathbb{Q}^\times$. Then $(a, b)_p = 1$ for all but finitely many primes p.*

Proof. From the explicit formulas for the Hilbert symbol in the p-adic and in the real case, we see that it is multiplicative in both variables. In particular, it suffices to prove this theorem (and the following one) for a and b equal to -1 or a prime number. Using the formulas, we find:

- Case $a = -1$, $b = -1$. One has $(-1,-1)_\infty = (-1,-1)_2 = -1$ and $(-1,-1)_p = 1$ if $p \neq 2, \infty$;
- $a = -1$, $b = \ell$ with ℓ prime. If $\ell = 2$, one has $(-1,2)_v = 1$ for all places v; if $v \neq 2$, one has $(-1,\ell)_v = 1$ if $v \neq 2, \ell$, and $(-1,\ell)_2 = (-1,\ell)_\ell = (-1)^{e(\ell)}$;
- $a = \ell, b = \ell'$ with ℓ, ℓ' primes. If $\ell = \ell'$, by Proposition 2.1.4, $(\ell,\ell)_v = (-1,\ell)_v$ for all v and we are reduced to the case considered above. If $\ell \neq \ell'$ and if $\ell' = 2$, one has $(\ell,2)_v = 1$ for $v \neq 2$, ℓ and

$$(\ell,2)_2 = (-1)^{\omega(\ell)}, \qquad (\ell,2)_\ell = \left(\frac{2}{\ell}\right) = (-1)^{\omega(\ell)}, \quad \text{cf. chap. I, n° 3.2, th. 5.}$$

If ℓ and ℓ' are distinct and different from 2, one has $(\ell,\ell')_v = 1$ for $v \neq 2$, ℓ, ℓ' and

$$(\ell,\ell')_2 = (-1)^{\epsilon(\ell)\epsilon(\ell')}, \quad (\ell,\ell')_\ell = \left(\frac{\ell'}{\ell}\right), \quad (\ell,\ell')_{\ell'} = \left(\frac{\ell}{\ell'}\right).$$

□

Theorem 2.1.13. *Let $a, b \in \mathbb{Q}^\times$. Then $\prod_{v \in V}(a,b)_v = 1$.*

Proof. Follows immediately from the proof of Theorem 2.1.12 and quadratic reciprocity, which can be imported from Mathlib.NumberTheory.LegendreSymbol.QuadraticReciprocity. In all cases, the product is one. □

2.1.4 Approximation and Existence Theorem

Definition 2.1.14. *Let S be a finite set of prime numbers. We define the* finite embedding *of $\mathbb{Q}$ into $\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p$ as the diagonal map.*

Note: we will care about the product of finitely many completions of $\mathbb{Q}$, which do not necessarily include $\mathbb{R}$, but the proof of the Approximation Theorem assumes it without loss of generality, since we can always add ∞ to S.

Theorem 2.1.15. *Let S be a finite set of prime numbers. The image of the finite embedding of $\mathbb{Q}$ into $\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p$ is dense with respect to the product topology. More concretely, for every $\epsilon > 0$ and every $y \in \mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p$, there exists $x \in \mathbb{Q}$ such that the distance between y and the image of x is less than ϵ.*

Proof. Let $y = (y_\infty, (y_p)_{p \in S})$ be an element of $\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p$. We can assume $y_p \in \mathbb{Z}_p$ for all $p \in S$, since otherwise we can multiply all y_p's by an integer. Let $\varepsilon > 0$ and $N \geq 0$. We need to prove that there exists $x \in \mathbb{Q}$ such that $|y_\infty - x| \leq \varepsilon$ and $v_p(y_p - x) \geq N$ for all $p \in S$.

By the Chinese Remainder Theorem Nat.chineseRemainderOfFinset, there exists $x_0 \in \mathbb{N}$ such that $x_0 \equiv y_p \pmod{p^N}$ for all $p \in S$.

Fix q a prime number. By density of the numbers of the form a/q^m in $\mathbb{R}$, where $a \in \mathbb{Z}$ and $m \geq 0$, we can find a in $\mathbb{Z}$, q a prime not in S and $m \geq 0$, such that

$$|x_0 - x_\infty - \frac{a}{q^m}(p_1 \dots p_n)^N| \leq \varepsilon.$$

Then $x = x_0 + \frac{a}{q^m}(p_1 \dots p_n)^N$ satisfies the required conditions. □

Theorem 2.1.16. *Let $(a_i)_{i\in I}$ be a finite family of nonzero rational numbers, and let $e_{i,v} \in \{\pm 1\}$ for each $i \in I$ and each place v of $\mathbb{Q}$. There exists a rational number $x \in \mathbb{Q}^\times$ such that*

$$\forall i \in I, \forall v \text{ place of } \mathbb{Q}, (x, a_i)_v = e_{i,v}$$

if and only if the following conditions hold:

1. *For each $i \in I$, we have $e_{i,v} = 1$ for all but finitely many places v.*
2. *For each $i \in I$, we have $\prod_v e_{i,v} = 1$.*
3. *For each place v, there exists $x_v \in \mathbb{Q}_v^\times$ such that $(x_v, a_i)_v = e_{i,v}$ for all $i \in I$.*

The proof uses Nat.infinite_setOf_prime_and_modEq.

Proof. To show that the conditions are necesary, simply observe that 1. is Theorem 2.1.12, 2. is Theorem 2.1.13, and 3. is trivial since we can take $x_v = x$ for all v.

Conversely, suppose that 1., 2. and 3. hold. Up to multiplying by a square integer (which does not change the Hilbert symbols), we can assume that all a_i's are integers. Let S be the set of places 2, ∞ and all the prime divisors of the a_i's. Let T be the set of places v such that there exists $i \in I$ with $e_{i,v} = -1$. The set S is finite and, by 1., T is also finite.

Consider first the case where $S \cap T = \emptyset$. Then, we define

$$a = \prod_{\ell \in T} \ell, \quad m = 8 \prod_{\ell \in S \setminus \{2,\infty\}} \ell.$$

Since a, m are coprime, by Nat.infinite_setOf_prime_and_modEq, there exists a prime number p such that $p \equiv a \pmod m$ and $p \notin S \cup T$.

Taking $x = ap$ works.

- If $v = \infty$, then $x > 0$, so $(x, a_i)_\infty = 1$ for all i, and $\infty \notin T$, so $e_{i,\infty} = 1$.
- If $v = \ell \in S$, we have $x \equiv a^2 \pmod m$, so x is a square modulo any $\ell \in S$, hence by Hensel's lemma it is a square in $\mathbb{Q}_\ell$, and x is a square modulo 8, so again by Hensel's lemma it is a square in $\mathbb{Q}_2$. By Proposition 2.1.4, $(x, a_i) = 1$.
- If $v = \ell \notin T$ and $\ell \neq p$, $v_\ell(x) = 0$ and so $(x, a_i)_\ell = \left(\frac{a_i}{\ell}\right)_\ell^v (x) = 1$. On the other hand, $e_{i,\ell=1}$, since $v \notin T$.
- If $v = \ell \in T$, then $v_\ell(x) = 1$, so $(x, a_i)_\ell = \left(\frac{a_i}{\ell}\right)$. By 3., there exists $x_\ell \in \mathbb{Q}_\ell^\times$ such that $(x_\ell, a_i)_\ell = e_{i,\ell}$ for all i, and $v_\ell(x_\ell)$ is odd since at least one of the $e_{i,\ell}$'s is -1. Therefore, $(a_i, x)_\ell$ and $(a_i, x_\ell)_\ell$ are both equal to $\left(\frac{a_i}{\ell}\right)$.
- If $v = p$, since for all the other places the equality holds, by the product formula we also have $(x, a_i)_p = e_{i,p}$ for all i.

For the general case, since the image of $\mathbb{Q}^\times$ is dense in $\prod_{v\in S} \mathbb{Q}_v^\times$, by Theorem 2.1.15, and squares are open in $\mathbb{Q}_v^\times$, by Theorem 1.2.1, we can find $x' \in \mathbb{Q}^\times$ such that x'/x_v is a square in $\mathbb{Q}_v^\times$ for all $v \in S$. Then, $(x', a_i)_v = (x_v, a_i)_v = e_{i,v}$ for all i and all $v \in S$. Let $\eta_{i,v} = e_{i,v}(x', a_i)_v$. Then $\eta_{i,v} = 1$ for all $v \in S$ and conditions 1., 2. and 3. hold for the $\eta_{i,v}$'s, so we can apply the first part of the proof to find $y \in \mathbb{Q}^\times$ such that $(y, a_i)_v = \eta_{i,v}$ for all i and all v.

Finally, setting $x = x'y$, we have $(x, a_i)_v = (x', a_i)_v (y, a_i)_v = e_{i,v}$ (by the explicit formulas for the Hilbert symbol in the p-adic and in the real case) for all i and all v, as desired. □

Chapter 3

Quadratic Forms over $\mathbb{Q}$ and $\mathbb{Q}_p$

3.1 Quadratic Forms

The following definition is available in `Mathlib` under the name QuadraticForm:

Definition 3.1.1. *Let M be a module over a commutative ring A. A function $f : M \to A$ is called a* quadratic form *on M if*

1. *$f(ax) = a^2 f(x)$ for all $a \in A, x \in M$,*
2. *The function $(x, y) \mapsto f(x + y) - f(x) - f(y)$ is a bilinear form.*

The QuadraticForm folder of `Mathlib` contains definitions and results about quadratic forms, including the bilinear map

$$(x, y) \mapsto x \cdot y := \frac{1}{2}(f(x + y) - f(x) - f(y))$$

associated to a quadratic form (see QuadraticMap.associated) and the definition and characterization of nondegenerate quadratic forms (see QuadraticMap.Nondegenerate).

Definition 3.1.2. *A quadratic form $f : M \to A$ is called* isotropic *if there exists a nonzero $x \in M$ such that $f(x) = 0$.*

Definition 3.1.3. *Let R be a commutative ring, let V be an R-module and let Q be a quadratic form on V. We say that Q* represents *an element $r \in R$ if there exists $x \in V$ such that $Q(v) = r$ and $v \neq 0$.*

Lemma 3.1.4. *Let R be a commutative ring, let V be an R-module and let Q be a quadratic form on V. Then Q* represents *0 if and only if it is isotropic.*

Proof. This follows immediately from the definitions. □

Lemma 3.1.5. *Let Q and Q' be two equivalent quadratic forms over R and let $r \in$. Then Q represents r if and only if Q' represents r. In particular, Q is isotropic if and only if Q' is isotropic.*

Proof. By Lemma 3.1.4, it suffices to prove the first claim, which follows from the definition of equivalence of quadratic forms. □

3.1.1 Orthogonal basis

Let K be a field in which 2 is invertible and let V be a K-vector space.

The definition of orthogonal basis for V is available in `Mathlib` as LinearMap.IsOrtho$_i$. The lemma LinearMap.BilinForm.exists_orthogonal_basis proves that for any symmetric bilinear form B on V there exists an orthogonal basis with respect to B.

Definition 3.1.6. *Two bases of V are called* contiguous *if they have an element in common.*

Theorem 3.1.7. *Let V be a K-vector space of dimension at least 3, let Q be a nondegenerate quadratic form on V, and let b, b' be two Q-orthogonal bases of V. Then there exists a finite sequence $(b^{(0)}, \cdots, b^{(m)})$ of orthogonal bases of V such that $b^{(0)} = b$, $b^{(m)} = b'$ and $b^{(i)}$ is contiguous with $b^{(i+1)}$ for $0 \leq i < m$.*

Proof. See [Ser73, §IV.1.4, Theorem 2]. □

Definition 3.1.8. *A sequence of bases $(b^{(0)} = b, \cdots, b^{(m)} = b')$ as in Theorem 3.1.7 is called a* chain *of orthogonal bases contiguously relating b to b'.*

Lemma 3.1.9. *Let V be a K-vector space of dimension at least 3, let Q be a nondegenerate quadratic form on V, and let b, b' be two Q-orthogonal bases of V. Assume that*

$$(b_1 \cdot b_1)(b'_i \cdot b'_i) - (b'_i \cdot b'_i)^2 = 0 \text{ for } i = 1, 2.$$

There exists $x \in K$ such that $b_x := b'_1 + x b'_2$ is nonisotropic and generates with b_1 a nondegenerate plane.

Proof. See [Ser73, §IV.1.4, Lemma after Theorem 2]. □

3.1.2 Translations

Let R be a commutative ring, let V and W be R-modules and let Q and Q' be quadratic forms on V and W, respectively. Then $Q \dotplus Q'$ denotes the quadratic form on $V \times W$ obtained by applying Q on V and Q' on W. This is available in `Mathlib` as `QuadraticMap.prod`. Similarly, $Q \dotminus Q'$ denotes the form $Q \dotplus (-Q')$ on $V \times W$.

Definition 3.1.10. *A quadratic form is* hyperbolic *if it is equivalent to the form $X^2 - Y^2$.*

Lemma 3.1.11. *The quadratic form XY is hyperbolic.*

Proof. TODO. □

Proposition 3.1.12. *Let R be a commutative ring. If a quadratic form Q on an R-module V represents 0 and is nondegenerate, then Q is equivalent to $H + Q'$, where H is hyperbolic. Moreover, f represents all elements of R.*

Proof. Fix $x \in V$ such that $Q(x) = 0$. Since Q is nondegenerate, there exists $z \in V$ such that $x \cdot z = 1$. The element $y = 2z - (z \cdot z)x$ is isotropic and $x \cdot y = 2$. The restriction of Q to the submodule $U := Rx \oplus Ry$ is the desired hyperbolic form H. □

Corollary 3.1.13. *Let K be a field, let $r \in K^\times$ and let Q be a quadratic form on a free K-vector space V. Then Q represents r if and only if the form $Q' := Q \dotminus rZ$ represents 0.*

Proof. The forward implication is clear. For the second one, fix a basis for V and assume that $Q' := Q \dotminus rZ$ has a nontrivial zero $(x_1, \cdots, x_n, z) \in V \times K$. Then either $z = 0$, in which case Q represents zero and thus also r, or $Q(x_1/z, \cdots, x_n/z) = r$. □

Corollary 3.1.14. *Let K be a field and Q and Q' be nondegenerate quadratic forms over K of rank at least 1. Then the following properties are equivalent:*

a) $Q \perp -Q'$ represents 0.

b) There exists $r \in K^\times$ which is represented by Q and Q'.

c) There exists $r \in K^\times$ such that $Q \perp -rZ^2$ and $Q' \perp -rZ^2$ represent 0.

Proof. The equivalence (b) $\iff$ (c) follows from Corollary 3.1.13. The implication (b) $\implies$ (a) is trivial. To show (a) $\implies$ (b), write a nontrivial zero of $Q \perp -Q'$ in the form (x, y) with $Q(x) = Q'(y)$. If $Q(x) \neq 0$, we are done. If $Q(x) = 0$, then Q represents 0 and thus by Proposition 3.1.12 also all elements of K. In particular, it represents all nonzero values taken by Q'. □

3.2 Quadratic Forms over $\mathbb{Q}_p$

Definition 3.2.1. *Let p be a prime number and let f be a quadratic form of rank n over $\mathbb{Q}_p$. Take a diagonal quadratic form $a_1X_1^2 + \cdots + a_nX_n^2$ which is equivalent to f; then the* discriminant *of f is the element $d(f) = a_1 \cdots a_n \in \mathbb{Q}_p^\times / {\mathbb{Q}_p^\times}^2$.*

Note that `Mathlib` *contains QuadraticForm.discr, as an element of $\mathbb{Q}_p$. We might need to adjust some statements and proofs if we really need to regard it as an element in $\mathbb{Q}_p^\times / {\mathbb{Q}_p^\times}^2$.*

Definition 3.2.2. *Let p be a prime number and let f be a quadratic form of rank n over $\mathbb{Q}_p$. Take a diagonal quadratic form $a_1X_1^2 + \cdots + a_nX_n^2$ which is equivalent to f; then the* Hasse–Minkowski invariant *of f is the element*

$$\epsilon(f) := \prod_{i<j} (a_i, a_j).$$

Lemma 3.2.3. *The value $\epsilon(f)$ does not depend on the choice of diagonal quadratic form equivalent to f.*

Proof. Let $b = (b_1, \cdots, b_n)$ be an orthogonal basis for V such that $Q(x) = a_1x_1^2 + \cdots + a_nx_n^2$ for $x = \sum x_i b_i$. We denote $\epsilon(b) := \prod_{i<j}(a_i, a_j)$.

If $n = 1$, then $\epsilon(f) = 1$. If $n = 2$, then $\epsilon(f) = 1$ if and only if the form $Z^2 - a_1X^2 - a_2Y^2$ represents 0. By Corollary 3.1.13, this is equivalent to $a_1X^2 + a_2Y^2$ representing 1, which means that there exists $v \in V$ with $Q(v) = 1$; this is independent on b. For $n \geq 3$ we use induction on n. By Theorem 3.1.7, it suffices to prove that for any pair of contiguous bases b and b', we have $\epsilon(b) = \epsilon(b')$. Thanks to the symmetry of the Hilbert symbol, $\epsilon(b)$ is unchanged by permutation of the basis elements, so we may assume that $b_1 = b_1'$. Then $b_1' \cdot b_1' = a_1$, and we can write

$$\begin{aligned} \epsilon(b) &= (a_1, a_2 \cdots a_n) \prod_{2 \leq i < j} (a_i, a_j) = \\ &= (a_1, d(Q)a_1) \prod_{2 \leq i < j} (a_i, a_j). \end{aligned}$$

Analogously,

$$\epsilon(b') = (a_1', d(Q)a_1) \prod_{2 \leq i < j} (a_i', a_j').$$

The result follows by combining $a_1 = a_1'$ and the induction hypothesis applied to the orthogonal complement of e_1. □

Lemma 3.2.4. *Let k be either $\mathbb{Q}_p$ or $\mathbb{R}$. Let f be a quadratic form of rank 3 over k. Then f represents 0 if and only if $(-1, -d(f)) = \epsilon(f)$.*

Proof. f is equivalent to $aX^2 + bY^2 + cZ^2$ for some $a, b, c \in k^\times$, and f represents 0 if and only if the form $-caX^2 - cbY^2 - Z^2$ represents 0.

By the definition of Hilbert symbol, this last form represents 0 if and only if $(-ca, -cb) = 1$. This is equivalent to

$$(-1,-1)(-1,a)(-1,b)(c,c)(a,b)(a,c)(b,c) = 1.$$

By Proposition 2.1.4 (vi), $(c, c) = (-1, c)$, so this can be rewritten as

$$1 = (-1,-1)(-1,abc)(a,b)(a,c)(b,c) = (-1,-d(f))\epsilon(f),$$

or equivalently, $(-1, -d(f)) = \epsilon(f)$. □

Lemma 3.2.5. *Let k be either $\mathbb{Q}_p$ or $\mathbb{R}$. Let f be a quadratic form of rank 2 over k, and let $a \in k^\times/{k^\times}^2$. Then f represents a if and only if $(a, -d(f)) = \epsilon(f)$.*

Proof. Up to equivalence, we may assume $f = X^2 + bY^2$ for some $b \in k^\times$. By Corollary 3.1.14, f represents a if and only if $f_a := f \dot{-} aZ^2$ represents 0, which by Lemma 3.2.4 is equivalent to $(-1, -d(f_a)) = \epsilon(f_a)$.

A computation shows that $d(f_a) = -ad(f)$ and $\epsilon(f_a) = (a, -d(f))\epsilon(f)$. Combining this with Proposition 2.1.4, we conclude the result. □

3.3 Hasse–Minkowski

The goal of this section is to prove the Hasse–Minkowski theorem over the rational numbers. To simplify the formalization process, rather than including a single long proof of this theorem, we will split it into smaller lemmas that can be formalized independently.

Denote by V the union of the set of prime numbers and the symbol ∞, and denote $\mathbb{Q}_\infty = \mathbb{R}$.

Let f be a quadratic form over $\mathbb{Q}$. For each $v \in V$, the injection $\mathbb{Q} \to \mathbb{Q}_v$ allows one to view f as a quadratic form over $\mathbb{Q}_v$, which we will denote f_v.

Definition 3.3.1. *A quadratic form f with coefficients in $\mathbb{Q}$ is* everywhere locally isotropic *if f_v is isotropic for all $v \in V$.*

Theorem 3.3.2 (Hasse–Minkowski)**.** *Let f be a quadratic form over $\mathbb{Q}$. Then f is isotropic if and only if f is everywhere locally isotropic. In other words, f has a global zero if and only if f has everywhere a local zero.*

Proof. Follows from the results below. □

Theorem 3.3.3 (Hasse–Minkowski)**.** *Let f be a degenerate quadratic form over $\mathbb{Q}$. Then f is isotropic if and only if f is everywhere locally isotropic. In other words, f has a global zero if and only if f has everywhere a local zero.*

Proof. Follows from the fact that every anisotropic quadratic form is nondegenerate. □

From now on, given 3.3.3, we may assume that f is a nondegenerate quadratic form.

Lemma 3.3.4. *Let f be an isotropic quadratic form over $\mathbb{Q}$. Then f is everywhere locally isotropic.*

Proof. Any nontrivial solution over Q yields a solution over Q_v for any $v \in V$. □

Lemma 3.3.5. *Let f be a quadratic form over $\mathbb{Q}$ of rank zero which is everywhere locally isotropic. Then f is isotropic.*

Proof. Suffices to see that every rank zero quadratic form over a field is anisotropic. □

Lemma 3.3.6. *Let K be a field of characteristic not equal to 2, let M be a K-vector space of positive dimension n and let $f : M \to K$ be a nondegenerate quadratic form. Then there exists a form $X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$ for some $a_i \in K^\times$ such that it is isotropic if and only if f is.*

Proof. Note that `Mathlib` contains a similar statement[1], where the coefficient of X_1 is not assumed to be 1. □

Lemma 3.3.7. *Let K be a field of characteristic not equal to 2, let M be a K-vector space of positive dimension n and let $f : M \to K$ be a nondegenerate quadratic form. Then there exists a form $X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$, for some squarefree $a_i \in K^\times$ such that it is isotropic if and only if f is.*

Proof. Follows from Lemma 3.3.6. □

Lemma 3.3.8. *Let f be a quadratic form over $\mathbb{Q}$ of rank one which is everywhere locally isotropic. Then f is isotropic.*

Proof. Suffices to see that every nonzero quadratic form of rank one over a field is anisotropic. □

Lemma 3.3.9. *Let f be a quadratic form over $\mathbb{Q}$ of rank two which is everywhere locally isotropic. Then f is isotropic.*

Proof. f is equivalent to $X_1^2 - aX_2^2$, for some nonzero a, which is positive because f_∞ represents 0. Write

$$a = \prod_p p^{v_p(a)}.$$

Since f_p represents 0, a is a square in $\mathbb{Q}_p$, so $v_p(a)$ is even. It follows that a is a square in $\mathbb{Q}$ and f represents 0. □

Lemma 3.3.10. *Let f be a quadratic form over $\mathbb{Q}$ of rank three which is everywhere locally isotropic. Then f is isotropic.*

Proof. f is equivalent to $X_1^2 - aX_2^2 - bX_3^2$; since we can multiply a and b by squares, we can reduce to the case where a and b are square-free integers. We can also assume $|a| \leq |b|$. We use induction on $m := |a| + |b|$.

If $m = 2$, then $f \sim X_1^2 \pm X_2^2 \pm X_3^2$. The case $X_1^2 + X_2^2 + X_3^2$ is excluded by the hypothesis that f_∞ represents zero. In the other cases, f represents zero (take e.g. $(1, 1, 0)$ or $(1, 0, 1)$, respectively).

Suppose now that $m > 2$, that is, $|b| \geq 2$ and write $b = \pm p_1 \cdots p_k$, where the p_i are distinct primes. Let p be one of the p_i; we will show that a is a square modulo p. This is obvious if $a \equiv 0 \mod p$. Otherwise a is a p-adic unit, and by hypothesis there exists $(x, y, z) \in \mathbb{Q}_p^3$ such that $z^2 - ax^2 - by^2 = 0$. By Proposition 1.1.2, we can suppose that (x, y, z) is primitive. From $z^2 - ax^2 \equiv 0 \mod p$, we deduce that if $x \equiv 0 \mod p$, then $z \equiv 0 \mod p$ and p^2 divides by^2; since $v_p(b) = 1$, this implies $y \equiv 0 \mod p$, contradicting the assumption that (x, y, z) is primitive. Therefore $x \not\equiv 0 \mod p$ and a is a square modulo p.

[1] QuadraticForm.equivalent_weightedSumSquares_units_of_nondegenerate'

Since $\mathbb{Z}/b\mathbb{Z} = \prod_i \mathbb{Z}/p_i\mathbb{Z}$, we also have that a is a square modulo b, so there exist integers t, b' such that $bb' = t^2 - a$ and we can choose t so that $|t| \leq |b|/2$. Then bb' is a norm of the extension $k(\sqrt{a})/k$ for $k = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{Q}_p$. From this we conclude that f represents 0 in k if and only if the same is true for $f' := X_1^2 - aX_2^2 - b'X_3^2$ (see the proof of [Ser73, §III.1.1, Proposition 1]).

In particular, f' represents 0 in each $\mathbb{Q}_v$. But we have

$$|b'| = \left|\frac{t^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b| \quad \text{because } |b| \geq 2.$$

Write $b' = b''u^2$, with b'', u integers and b'' square-free, so $|b''| < |b|$. We can then apply the induction hypothesis to the form $X_1^2 - aX_2^2 - b''X_3^2$, which is equivalent to f'; hence f' represents 0 in $\mathbb{Q}$ and so does f. □

Lemma 3.3.11. *Let f be a quadratic form over $\mathbb{Q}$ of rank four which is everywhere locally isotropic. Then f is isotropic.*

Proof. Up to equivalence, we may assume $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. Fix a place $v \in V$. Since f_v represents 0, Corollary 3.1.14 shows that there exists $x_v \in \mathbb{Q}_v^\times$ which is represented both by $aX_1^2 + bX_2^2$ and by $cX_3^2 + dX_4^2$.

By Lemma 3.2.5, this is equivalent to saying that

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

Since $\prod_{v \in V} (a, b)_v = \prod_{v \in V} (c, d)_v = 1$ by Theorem 2.1.13, we can deduce from Theorem 2.1.16 the existence of $x \in \mathbb{Q}^\times$ such that

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

This shows that the form $aX_1^2 + bX_2^2 - xZ^2$ represents zero in each $\mathbb{Q}_v$, so by Lemma 3.3.10, it also represents 0 in $\mathbb{Q}$. By Corollary 3.1.13, x is represented by $aX_1^2 + bX_2^2$. The same argument shows that x is represented by $cX_1^2 + dX_2^2$. By applying Corollary 3.1.14 again, we conclude that f represents 0. □

Lemma 3.3.12. *Let f be a quadratic form over $\mathbb{Q}$ of rank $n \geq 5$ which is everywhere locally isotropic. Then f is isotropic.*

Proof. The proof uses induction on n. Write $f = h - g$, where $h = a_1X_1^2 + a_2X_2^2$, $g = -(a_3X_3^2 + \cdots + a_nX_n^2)$. Let S be the finite subset of V consisting of $\infty, 2$, and the primes p such that $v_p(a_i) \neq 0$ for $i \geq 3$. Let $v \in S$. Since f_v represents 0, there exists $c_v \in \mathbb{Q}_v^\times$ which is represented in $\mathbb{Q}_v$ by h and g, that is, there exist $x_i^v \in \mathbb{Q}_v$, $i = 1, \ldots, n$ (with $x_i^v \neq 0$ for $i = 1, 2$, and some $i \geq 3$) such that

$$h(x_1^v, x_2^v) = c_v = g(x_3^v, \cdots, x_n^v).$$

By Theorem 1.2.1, the squares of $\mathbb{Q}_p^\times$ form an open set. Combining this with the approximation theorem 2.1.15, we deduce the existence of $x_1, x_2 \in \mathbb{Q}^\times$ such that, denoting $c := h(x_1, x_2)$, one has $c/c_v \in {\mathbb{Q}_v^\times}^2$ for all $v \in S$.

Consider the form $f_1 := cZ^2 - g$. For each $v \in S$, g represents c_v in $\mathbb{Q}_v$, and hence also c because $c/c_v \in {\mathbb{Q}_v^\times}^2$, hence f_1 represents 0 in $\mathbb{Q}_v$ by Corollary 3.1.13. For $v \notin S$, the coefficients $-a_3, \ldots, -a_n$ of g are v-adic units, so the discriminant $d_v(g)$ is a v-adic unit and $\epsilon_v(g) = 1$.

In all cases, f_q represents 0 in all $\mathbb{Q}_v$, and since the rank of f is $n-1$, the inductive hypothesis shows that f_1 represents 0 in $\mathbb{Q}$, or equivalently by Corollary 3.1.13, g represents c in $\mathbb{Q}$. But h also represents c, so by Corollary 3.1.14 f represents 0.

□

Bibliography

[Ser73] J.-P. Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer New York, NY, New York, 1973 (cited on pages 1, 2, 11, 15).