HASSE-MINKOWSKI THEOREM

KIM, SUNGJIN

1. Introduction

In rough terms, a local-global principle is a statement that asserts that a certain property is true globally if and only if it is true everywhere locally. We will give a proof of Hasse-Minkowski theorem over $\mathbb{Q}$, which is the best known example for local-global principles

Theorem 1.1. (Hasse-Minkowski) Let K be a number field and let q be a quadratic form in n variables with coefficients in K. Then q represents 0 in K if and only if it represents 0 in every completion of K.

2. Basic results on quadratic forms

Let V be a K-vector space of finite dimension n. Recall that a quadratic form on V is a map q from V to K such that $q(ax) = a^2q(x)$ for all $x \in V$ and $a \in K$, and $b(x, y) = (q(x+y)-q(x)-q(y))/2$ is a bilinear form so that $q(x) = b(x, x)$. Thus, for a given basis $\{e_i\}$ for V, and $x = \sum_i x_ie_i$, we have $q(x) = X^tQX$, where X is the column vector of the x_i, and Q is a symmetric matrix having $b(e_i, e_j)$ as ij-th entry. If $\{e'_i\}$ is another bases of V and if P is the matrix expressing e'_i in terms of the e_i, then with $X = PX'$, we have $q(x) = X^tQX = X'^tP^tQPX'$; hence the matrix of q in the new basis is equal to P^tQP. In particular, $det(P^tQP) = det(Q)det(P)^2$, so the class of $det(Q)$ modulo nonzero squares of K is independent of the chosen basis and called the *discriminant* of q, denoted by $d(q)$. If $V = K^n$ and (e_i) is the canonical basis of V, we can identify a quadratic form on V with a homogeneous polynomial of degree 2 in n variables over K by the formula

$$q(x_1, \cdots, x_n) = \sum_{1\leq i,j\leq n} q_{i,j}x_ix_j,$$

where the $q_{i,j}$ are the entries of the symmetric matrix Q. We call Q the coefficient matrix of q.

Definition 2.1. Two quadratic forms q and q' with coefficient matrices Q, and Q' respectively, are *equivalent* if there exists $P \in GL_n(K)$ such that $Q' = P^tQP$. Denoted $q \sim q'$.

Using Gauss's reduction of quadratic forms into sums of squares, gives

Theorem 2.1. Let q be a quadratic form in n variables. There exists an equivalent form that is a diagonal quadratic form; in other words, there exist $a_i \in K$ such that $q \sim \sum_{1\leq i\leq n} a_ix_i^2$.

We say that a form q represents $a \in K$ if there exists $x \in K^n$ such that $q(x) = a$, with added condition that $x \neq 0$ when $a = 0$.

Theorem 2.2. Let q be a nondegenerate quadratic form in n variables and let $c \in K^*$. The following conditions are equivalent:
(1) The form q represents c.
(2) There exists a quadratic form q_1 in $n-1$ variables such that $q \sim cx_0^2 \oplus q_1$.
(3) The quadratic form $q \ominus cx_0^2$ represents 0 in K.

3. QUADRATIC FORMS OVER FINITE AND LOCAL FIELDS

We begin with the simplest possible fields, the finite fields. Let $q = p^k$ be a prime power, with $p \neq 2$.

Theorem 3.1. A quadratic form over $\mathbb{F}_q$ of rank $n \geq 2$ represents all elements of $\mathbb{F}_q^*$, and a quadratic form of rank $n \geq 3$ represents all elements of $\mathbb{F}_q$.

Proof. By Theorem2.1, we assume that $q = \sum_{1 \leq i \leq m} a_i x_i^2$ with $a_1 a_2 \neq 0$. Let $a \in \mathbb{F}_q$. We choose $x_i = 0$ for all $i \geq 3$. Since q is odd the map $x \mapsto x^2$ is a group homomorphism of $\mathbb{F}_q^*$ into itself, and its kernel has two elements. It follows that its image has $(q-1)/2$ elements, so adding 0, there are $(q+1)/2$ squares in $\mathbb{F}_q$. Since $a_1 a_2 \neq 0$ it follows that the subsets $\{a_1 x_1^2\}$ and $\{a - a_2 x_2^2\}$ of $\mathbb{F}_q$ also have $(q+1)/2$ elements. Hence they have nonempty intersection. □

Corollary 3.1. Let $c \in \mathbb{F}_q^*$ that is not a square. A nondegenerate quadratic form over $\mathbb{F}_q$ is equivalent to $x_1^2 + \cdots + x_{n-1}^2 + ax_n^2$ with $a = 1$ if its discriminant is a square, and with $a = c$ otherwise.

Proof. Use induction on n and previous theorem. □

Corollary 3.2. Two nondegenerate quadratic forms over $\mathbb{F}_q$ are equivalent if and only if they have the same rank and the same discriminant in $\mathbb{F}_q^*/\mathbb{F}_q^{*2}$.

4. DEFINITION OF THE LOCAL HILBERT SYMBOL

We introduce the Hilbert symbol, which will be sufficient for the local study of quadratic forms. We shall omit the proof here.

Definition 4.1. If a and b are in $\mathcal{K}^*$, we set $(a,b) = 1$ if the equation $ax^2 + by^2 = z^2$ has a nontrivial solution, and $(a,b) = -1$ otherwise. The number (a,b) is called the Hilbert symbol of a and b.

Proposition 4.1. Let a and b be in $\mathcal{K}^*$. We have $(a,b) = 1$ if and only if $a \in N(\mathcal{K}(\sqrt{b})^*)$.

Proposition 4.2. We have the following formulas, where all the elements that occur are assumed to be nonzero:
(1) $(a,b) = (b,a)$ and $(a,c^2) = 1$.
(2) $(a,-a) = (a,1-a) = 1$.
(3) $(a,b) = 1$ implies $(aa',b) = (a',b)$.
(4) $(a,b) = (a,-ab) = (a,(1-a)b)$.

We state the explicit computation of the Hilbert symbol when $\mathcal{K} = \mathbb{Q}_p$. We denote as usual by U_p the group of p-adic units.

Theorem 4.1. (1) For $\mathcal{K} = \mathbb{R}$, we have $(a, b) = 01$ if $a < 0$ and $b < 0$, and $(a, b) = 1$ if a or b is positive.
(2) For $\mathcal{K} = \mathbb{Q}_p$ with $p \neq 2$, write $a = p^\alpha a_1$, $b = p^\beta b_1$ with a_1 and b_1 in U_p. Then

$$(a, b) = (-1)^{\alpha\beta(p-1)/2}\left(\frac{a_1}{p}\right)^\beta\left(\frac{b_1}{p}\right)^\alpha.$$

(3) For $\mathcal{K} = \mathbb{Q}_2$, with the same notation we have

$$(a, b) = (-1)^{(a_1-1)(b_1-1)/4}\left(\frac{a_1}{2}\right)^\beta\left(\frac{b_1}{2}\right)^\alpha.$$

From this theorem, we know that the Hilbert symbol is bilinear on $\mathbb{F}_2$-vector space $\mathcal{K}^*/\mathcal{K}^{*2}$.

Proposition 4.3. Let $q(x, y, z) = ax^2 + by^2 + cz^2$ be a nondegenerate quadratic form in three variables with coefficients in $\mathbb{Q}_p$(including $p = \infty$). Set $\epsilon = \epsilon(q) = (a, b)(b, c)(a, c)$, and let $d = d(q) = abc$ be the discriminant of q. Then q represents 0 in $\mathbb{Q}_p$ if and only if $(-1, -d) = \epsilon$.

Proof. The form q represents 0 if and only if the form $-cq$ does, hence if and only if $-acx^2 - bcy^2 = z^2$ has a nontrivial solution, in other words by definition $(-ac, -bc) = 1$. By bilinearity this condition is

$$1 = (-ac, -bc) = (-1, -1)(-1, a)(-1, b)(a, b)(a, c)(b, c)(c, c),$$

and since $(c, c) = (-1, c)$, this can be written $(-1, -abc) = (a, b)(b, c)(a, c)$, proving the proposition. $\square$

Corollary 4.1. Let $c \in \mathbb{Q}_p^*$, and let $q(x, y) = ax^2 + by^2$ be a nondegenerate quadratic form in two variables. Then q represents c in $\mathbb{Q}_p$ if and only if $(c, -ab) = (a, b)$.

Proof. Use above proposition. $\square$

5. QUADRATIC FORMS OVER $\mathbb{Q}_p$

We define a second invariant. Up to equivalence, we can assume that q is in diagonal form as $q(x) = \sum_{1 \leq i \leq n} a_i x_i^2$, and we set

$$\epsilon((a_1, \cdots, a_n)) = \prod_{1 \leq i,j \leq n} (a_i, a_j),$$

where (a_i, a_j) is the Hilbert symbol. We have the following theorem.

Theorem 5.1. The value of $\epsilon((a_1, \cdots, a_n))$ is independent of the linear change of variables that transforms q into diagonal form, hence is an invariant of the quadratic form itself, which we will denote by $\epsilon(q)$.

It follows from this theorem that just as for the discriminant $d(q)$, $\epsilon(q)$ is an invariant of the equivalence class of q.

Theorem 5.2. Let q be a nondegenerate quadratic form in n variables, and set $d = d(q)$, and $\epsilon = \epsilon(q)$. Then q represents 0 nontrivially in $\mathbb{Q}_p$ if and only if one of the following holds:
(1) $n = 2$ and $d = -1$.
(2) $n = 3$ and $(-1, -d) = \epsilon$.
(3) $n = 4$ and either $d \neq 1$, or $d = 1$ and $(-1, -d) = \epsilon$.
(4) $n \geq 5$.

Corollary 5.1. Let $c \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. A nondegenerate form q in n variables with invariants d and ϵ represents c if and only if one of the following holds:
(1) $n = 1$ and $c = d$.
(2) $n = 2$ and $(c, -d) = \epsilon$.
(3) $n = 3$ and either $c \neq -d$ or $c = -d$ and $(-1, -d) = \epsilon$.
(4) $n \geq 4$.

Corollary 5.2. Two quadratic forms over $\mathbb{Q}_p$ are equivalent if and only if they have the same rank, discriminant, and invariant $\epsilon(q)$.

6. Quadratic forms over $\mathbb{Q}$

Theorem 6.1. If a and b are in $\mathbb{Q}^*$ then $(a, b)_v = 1$ for almost all $v \in P$, and we have the product formula

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

Proof. Use Theorem 4.1. □

Theorem 6.2. Let $(a_i)_{i \in I}$ be a finite set of elements of $\mathbb{Q}^*$ and let $(\epsilon_{i,v})_{i \in I, v \in P}$ be a set of numbers equal to ± 1. There exists $x \in \mathbb{Q}^*$ such that $(a_i, x) = \epsilon_{i,v}$ for all $i \in I$ and all $v \in P$ if and only if the following three conditions are satisfied:
(1) Almost all of the $\epsilon_{i,v}$ are equal to 1.
(2) For all $i \in I$ we have $\prod_{v \in P} \epsilon_{i,v} = 1$.
(3) For all $v \in P$ there exists $x_v \in \mathbb{Q}_v^*$ such that $(a_i, x_v)_v = \epsilon_{i,v}$ for all $i \in I$.

Theorem 6.3. (Hasse-Minkowski Theorem for $n \leq 2$)

Lemma 6.1. Over any field K of characteristic diffferent from 2 the form $ax^2 + bxy + cy^2$ represents 0 nontrivially if and only if $b^2 - 4ac$ is a square in K.

Proof. Use the identity $(2ax + by)^2 - y^2(b^2 - 4ac) = 4a(ax^2 + bxy + cy^2)$. □

Since q represents 0 nontrivially in $\mathbb{R}$, we must have $d \geq 0$. If $d = 0$ then q is a square of a linear form hence represents 0 nontrivially. If $d > 0$ then let $d = \prod_i p_i^{v_i}$ be the prime power decomposition of d. Since q represents 0 nontrivially in every $\mathbb{Q}_p$, by above lemma d is a square in $\mathbb{Q}_p$. This implies that $v_{p_i}(d) = v_i$ is even for all i, hence that d is a square.

Theorem 6.4. (Hasse-Minkowski Theorem for $n = 3$)

Proof. We may assume that our quadratic form is a diagonal form $q(x, y, z) = ax^2 + by^2 + cz^2$. If one of the coefficients is 0 then q has a nontrivial zero in $\mathbb{Q}$ by the case $n = 2$. Thus we may assume $abc \neq 0$. Furthermore, we may assume that $q(x, y, z) = x^2 - ay^2 - bz^2$ with a, b square-free integers, where we assume $|a| \leq |b|$. We prove the theorem by induction on $m = |a| + |b|$. If $m = 2$ then $q(x, y, z) = x^2 \pm y^2 \pm z^2$, and since the case $x^2 + y^2 + z^2$ is excluded since q represents 0 in $\mathbb{R}$, in other cases the form represents 0.
Thus assume now that $m > 2$, in other words $|b| \geq 2$, and let $b = \pm \prod_{1 \leq i \leq k} p_i$ be the prime factorization of the square-free number b. Let $p = p_i$ for some i. We claim that a is a square modulo p. This is trivial if $a \equiv 0 \pmod{p}$. Otherwise a is a p-adic unit, and by assumption there exists a nontrivial p-adic solution to $ay^2 + bz^2 = x^2$, where $x, y, z \in \mathbb{Z}_p$, and at least one in U_p. Thus $x^2 \equiv ay^2 (\text{mod } p\mathbb{Z}_p)$. Now y is a p-adic unit. It follows that $a \equiv (x/y)^2 \pmod{p\mathbb{Z}_p}$, so a is a square modulo p. Since

this is true for all $p|b$, by the Chinese remainder theorem this implies that a is a square modulo b, in other words that there exist b' and k such that $k^2 = a + bb'$, where k may be chosen such that $|k| \leq |b|/2$. Since $bb' = k^2 - a$, bb' is a norm in the extension $K(\sqrt{a})/K$, where $K = \mathbb{Q}$ or any $\mathbb{Q}_v$. Thus, q represents 0 in K if and only if the same is true for $q'(x, y, z) = x^2 - ay^2 - b'z^2$. In particular, by assumption q' represents 0 in all the $\mathbb{Q}_v$. But since $|b| \geq 2$ and $|a| \leq |b|$, we have

$$|b'| = \left|\frac{k^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|.$$

Thus we may apply our induction hypothesis to the form q'(more precisely to the form q'', where b' is replaced by its square-free part);hence q' represents 0 in $\mathbb{Q}$, and so the same is true for the form q. □

Theorem 6.5. (Hasse-Minkowski Theorem for $n = 4$)

Before the proof in this case, we slightly strengthen the case $n = 3$.

Proposition 6.1. Let $q(x, y, z)$ be a quadratic form in three variables, and assume that $q(x, y, z) = 0$ has a nontrivial solution in every completion of $\mathbb{Q}$ except perhaps in one. Then it has a nontrivial solution in $\mathbb{Q}$, hence in all places.

Proof. Assume $q(x, y, z) = ax^2 + by^2 + cz^2$. By Proposition 4.3, q represents 0 in $\mathbb{Q}_v$ if and only if

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

By assumption this is true for all v except perhaps one. Since both sides satisfy the product formula(Theorem 6.1), it follows that this equality is true for all v; by 4.3 again, q represents 0 in $\mathbb{Q}_v$ for all v. Hence by the proof of case $n = 3$, q represents 0 in $\mathbb{Q}$. □

Proof. We may assume that $q = a_1x_1^2 + a_2x_2^2 - a_3x_3^2 - a_4x_4^2$. Let v be a place of $\mathbb{Q}$. Since q represents 0 in $\mathbb{Q}_v$, an application of Theorem 2.2 shows that there exists $c_v \in \mathbb{Q}_v^*$ that is represented both by $a_1x_1^2 + a_2x_2^2$ and by $a_3x_3^2 + a_4x_4^2$, and Corollary 4.1 implies that for all v we have

$$(c_v, -a_1a_2)_v = (a_1, a_2)_v \text{ and } (c_v, -a_3a_4)_v = (a_3, a_4)_v.$$

By the product formula for the Hilbert symbol, we deduce from Theorem 6.2 that there exists $c \in \mathbb{Q}^*$ such that for all places v,

$$(c, -a_1a_2)_v = (a_1, a_2)_v \text{ and } (c, -a_3a_4)_v = (a_3, a_4)_v.$$

The form $a_1x_1^2 + a_2x_2^2 - cx_0^2$ thus represents 0 in each $\mathbb{Q}_v$, hence by the proof of the case $n = 3$ also in $\mathbb{Q}$, so c is represented by $a_1x_1^2 + a_2x_2^2$. Similarly c is represented by $a_3x_3^2 + a_4x_4^2$, so q represents 0. □

Theorem 6.6. (Hasse-Minkowski Theorem for $n \geq 5$)

Proof. Write $Q = Q_1 - Q_2$ where

$$Q_1(x_1, x_2) = a_1x_1^2 + a_2x_2^2$$

and

$$Q_2(x_3, \cdots, x_n) = -a_3x_3^2 - \cdots - a_nx_n^2.$$

Let S be the set consisting of $v = 2, v = \infty$ and v such that not every $a_i \in \mathbb{Z}_v^*$ for $i \geq 3$. For all $v \in S$, Q_1 and Q_2 represent some common nonzero α_v over $\mathbb{Q}_v$ since Q represents 0 over $\mathbb{Q}_v$. The set of nonzero squares $\mathbb{Q}_v^{*2}$ is open so the coset of $\mathbb{Q}_v^{*2}$ containing α_v is an open set. The quadratic form Q_1 is continuous so the inverse image of the coset containing α_v is an open set A_v in $\mathbb{Q}_v \times \mathbb{Q}_v$. By the approximation theorem there are $x_1, x_2 \in \mathbb{Q}$ such that $(x_1, x_2) \in A_v$ for all $v \in S$. Thus $a := Q_1(x_1, x_2)$ is in $\mathbb{Q}$ and $a/\alpha_v \in \mathbb{Q}_v^{*2}$ for all $v \in S$. Consider the quadratic form $Q' = at^2 - Q_2$. There is a nontrivial solution to $Q' = 0$ over every $\mathbb{Q}_v$ for $v \in S$ since $a/\alpha_v \in \mathbb{Q}_v^{*2}$ for all $v \in S$. Furthermore, the equation $Q' = 0$ has a nontrivial solution over every $\mathbb{Q}_v$ where v is not in S since $\mathrm{char}(\mathbb{Q}_v) \neq 2$ and $n - 2 \geq 3$. So there is a nontrivial solution to $Q' = 0$ over $\mathbb{Q}$ by the induction hypothesis since Q' is an $(n-1)$-dimensional quadratic form. This means the equation $Q_2 = a$ has a solution over $\mathbb{Q}$. We now have solutions over $\mathbb{Q}$ to $Q_1 = a$ and $Q_2 = a$ so

$$Q = Q_1 - Q_2 = 0$$

has a nontrivial solution over $\mathbb{Q}$. $\square$

References

1. H. Cohen, Number Theory I, GTM 239 Springer