Quadratic forms and the Hasse-Minkowski Theorem

Juraj Milcak
University of Toronto
MAT477
Instructor: Prof. Milman

March 13, 2012

Our goal is the Hasse-Minkowski Theorem:

Recall: for a prime $p \in \mathbb{Z}$ we have the field of p-adic numbers $\mathbb{Q}_p$;

also, put $\mathbb{Q}_\infty := \mathbb{R}$. We have the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$, v prime or ∞.

Say $f := \sum_{i=1}^{n} a_i X_j^2$ on $\mathbb{Q}^n$, we associate to this a form f_v on $\mathbb{Q}_v$.

Thm. H-M.: There is a nonzero element $X \in \mathbb{Q}^n$ s.th $f(X) = 0$

iff for all v, there is a nonzero element $X_v \in \mathbb{Q}_v^n$ s.th $f(X_v) = 0$.

Now, in more details and much more definitions:

Def. A *quadratic module* (shortly q.m.) (V, Q):

is a module V over a comm. ring A with a quadratic form Q on V,

i.e. a function $Q : V \to A$ that satisfies the assumptions:

1) $Q(ax) = a^2 Q(x)$ for $a \in A$ and $x \in V$,

2) $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form.

$A = k$ field, $char(k) \neq 2 \Rightarrow$ the A-module V is a k-vector space.

We assume the k-vector space is finite dimensional.

We set the scalar product associated to Q: $(x, y) \mapsto x.y$ where

$x.y := \frac{1}{2}\{Q(x+y) - Q(x) - Q(y)\}$. So, $Q(x) = x.x$.

Thus *symmetric bilinear forms* on $V \longleftrightarrow$ *quadratic forms* on V.

For quad. modules (V, Q), (V', Q'), a map $f : V \to V'$

s.th. $Q' \circ f = Q$ is called a *morphism* $(V, Q) \to (V', Q')$.

Then $f(x).f(y) \equiv x.y$.

Matrix of a quadratic form w.r.to a basis $(e_i)_{1\leq i\leq n}$ of V,

is $A = (a_{ij})$ where $a_{ij} = e_i.e_j$, thus A is symmetric.

If $x = \sum x_i e_i \in V$, then $Q(x) = \sum_{i,j} a_{ij} x_i x_j$.

If $B \in GL(n,k)$, we can change the basis w.r.to B, the matrix A' of

Q w.r.to the new basis is BAB^t. Thus $\det(A)$ is an invariant of Q

in $k^*/k^{*2} \cup \{0\}$: $\det(A) =:$ *disc*(Q) is the *discriminant* of Q.

Orthogonality: $x, y \in V$ are *orthogonal* iff $x.y = 0$.

$H \subset V$, set H^0 to be the subspace of $x \in V$ s.th. $x.y = 0$, $\forall y \in H$.

V_1, V_2 subspaces of $V \Rightarrow V_1$ and V_2 are orthogonal iff $V_1 \subset V_2^0$.

$V^0 =: rad(V)$ is the radical of V, its codimension $=: rank(Q)$.

If $rad(V) = 0$, then we say Q is *nondegenerate* $\Leftrightarrow disc(Q) \neq 0$.

For $U \subset V$, $q_U : V \ni x \mapsto (U \ni y \mapsto x.y) \in U^* := Hom(U; k)$.

$\ker q_U = U^0$, so $disc(Q) \neq 0 \Leftrightarrow q_V : V \to V^*$ is an isomorphism.

$V := U_1 \hat{\oplus} \ldots \hat{\oplus} U_m$ iff $U_1, \ldots, U_m$ are pairwise

orthogonal subspaces of V and V is the sum of the U_i .

If x has components $x_i \in U_i$ then $Q(x) = \sum Q_i(x_i)$, $Q_i := Q|U_i$.

Def. $x \in V$ is *isotropic* if $Q(x) = 0$; $U \subset V$ isotropic $\Leftrightarrow$ $Q|U = 0$.

Q.m. with an isotropic basis x, y s.th. $x.y \neq 0 =:$ *hyperbolic plane*.

If (V, Q) is a hyperbolic plane, then $disc(Q) = -1$.

Prop. A: If $x \in V \setminus \{0\}$ is isotropic and $disc(Q) \neq 0$

$\Rightarrow \exists$ a subspace $U \subset V$, s.th. $x \in U$ and U is a hyperbolic plane.

Pf. $disc(Q) \neq 0 \Rightarrow \exists\, z \in V$ s.th. $x.z = 1$. Let $y = 2z - (z.z)x$,

$\Rightarrow y$ is isotropic and $x.y = 2$. Put $U = k\{x\} \oplus k\{y\}$. $\square$

Cor. A1: $\exists\, x \in V \setminus \{0\}$ isotropic and $disc(Q) \neq 0 \Rightarrow Q(V) = k$.

Pf. If V is a hyperbolic plane with basis x, y with $x.y = 1$ and

$a \in k \Rightarrow a = Q(x + \frac{a}{2}y)$. $\dim_k V > 2$ case follows from Prop. A.$\square$

$(e_i) \subset (V, Q)$ is an *orthogonal basis* when $V = \hat{\bigoplus}_i k\{e_i\}$.

Theorem 1. Every quad. module (V, Q) has an orthogonal basis.

Def. Bases $(e_i), (e'_i)$ are *contiguous* if $e_i = e'_j$ for some i, j.

Fact 1. Given two orthogonal bases $(e_i), (e'_1)$ there is a finite

sequence of orthogonal bases starting with (e_i) ending with (e'_i)

s.th every two consecutive ones are contiguous.

Def. For two forms f, g let $f \dot{+} g = f(x_1, \ldots, x_n) + g(x_{n+1}, \ldots, x_m)$.

Prop. B: g, h nondegen. of *rank* ≥ 1, $f = g \dot{+} (-h) \Rightarrow$

TFAE:

(a) f represents 0, i.e. $\exists\, x \in V \setminus \{0\}$ s.th. $f(x) = 0$.

(b) $\exists\, a \in k^*$ represented by both g and h.

(c) $\exists\, a \in k^*$ such that $g \dot{+} (-aZ^2)$ and $h \dot{+} (-aZ^2)$ represent 0.

Pf. (b) $\Leftrightarrow$ (c) and (b) $\Rightarrow$ (a) are direct. $f(x, y) = 0 \Rightarrow$

$g(x) = h(y) =: b$. If $b \in k^*$ we are done, if $b = 0$, then

$g(V) = h(V) = k$ by Cor. A1 $\Rightarrow g(x') = h(y') =: a \in k^*$ for some

$x', y' \in V$. $\square$

The Hilbert Symbol: let $a, b \in k^*$ put:

$(a, b) := 1$ if $z^2 - ax^2 - by^2 = 0$ has a nontrivial solution in k^3,

and $(a, b) := -1$ otherwise.

The Hilbert symbol is a bilinear map $k^*/k^{*2} \times k^*/k^{*2} \to \{\pm 1\}$.

For an orthogonal basis $\mathbf{e} = (e_i)$ of (V, Q) with $a_i := e_i.e_i$:

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

Theorem 3. $\epsilon(\mathbf{e})$ does not depend on the choice of $\mathbf{e}$.

Pf. Induction on *rank* n: $n = 1 \Rightarrow \epsilon(\mathbf{e}) = 1$. If $n = 2 \Rightarrow \epsilon(\mathbf{e}) = 1$

$\Leftrightarrow Z^2 - a_1X^2 - a_2Y^2$ represents $0 \Leftrightarrow a_1X^2 + a_2Y^2$ represents 1

$\Leftrightarrow \exists v \in V$ s.th. $Q(v) = 1$, which is independent of basis.

If $n \geq 3$, enough to show $\epsilon(\mathbf{e}) = \epsilon(\mathbf{e}')$ when $\mathbf{e}$, $\mathbf{e}'$ are contiguous.

WLOG assume $e_1 = e_1' \Rightarrow a_1 = a_1'$. Since $disc(Q) = a_1 \ldots a_n$,

$$\epsilon(\mathbf{e}) = (a_1, a_2 \cdots a_3) \prod_{2 \leq i < j} (a_i, a_j) = (a_1, disc(Q)a_1) \prod_{2 \leq i < j} (a_i, a_j)$$

Repeat: $\epsilon(\mathbf{e}) = (a_1, disc(Q)a_1) \prod_{2 \leq i < j} (a_i, a_j)$

Similarly, $\epsilon(\mathbf{e}') = (a_1, disc(Q)a_1) \prod_{2 \leq i < j} (a'_i, a'_j)$.

Inductive hypothesis applied to the orthogonal complement of e_1

$$\Rightarrow \prod_{2 \leq i < j} (a_i, a_j) = \prod_{2 \leq i < j} (a'_i, a'_j) \Rightarrow \epsilon(\mathbf{e}) = \epsilon(\mathbf{e}'). \quad \square$$

Thus we write $\epsilon(Q)$ instead of $\epsilon(\mathbf{e})$.

Fact 2. Forms f, g are equivalent iff $rank(f) = rank(g)$,

$disc(f) = disc(g)$, $\epsilon(f) = \epsilon(g)$.

Quadratic forms over $\mathbb{Q}$, let $f(X) = a_1 X^2 + \cdots + a_n X_n^2$

We assume from now that forms are nondegenerate.

Let V be the set of prime numbers along with ∞, we put $\mathbb{Q}_\infty = \mathbb{R}$.

For $v \in V$, $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$ allows us to view f over $\mathbb{Q}_v$, denoted f_v,

$\mathbb{Q}^*/\mathbb{Q}^{*2} \hookrightarrow \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$, gives $disc(f) \mapsto disc(f_v) := disc_v(f)$,

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

Fact 2. (sadly): Hilbert's Theorem: $a, b \in \mathbb{Q}^* \Rightarrow (a, b)_v = 1$ for all

but finitely many v and $\displaystyle\prod_{v \in V}(a, b)_v = 1$.

Hasse-Minkowski Theorem:

$\exists\ x \in \mathbb{Q}^n$ s.th $f(x) = 0 \Leftrightarrow \forall v \in V\ \exists\ x_v \in \mathbb{Q}_v^n$ s.th $f_v(x_v) = 0$.

Lazy notation: Write $a \in Im(f)$ to mean "f represents 0."

Pf. "$\Rightarrow$" is trivial. For the converse, write $f = a_1X_1^2 + \dots a_nX_n^2$,

Replacing f by a_1f, we may assume $a_1 = 1$. Note we have $a_i \in \mathbb{Q}^*$.

$\underline{n = 2:}$ We have $f = X_1^2 - aX_2^2$, since $0 \in Im(f_\infty)$, $a > 0$.

Write $\prod_p p^{v_p(a)}$, $0 \in Im(f_p) \Rightarrow 2|v_p(a) \Rightarrow a \in \mathbb{Q}^{*2} \Rightarrow 0 \in Im(f)$.

$\underline{n=3:}$ $f = X_1^2 - aX_2^2 - bX_3^2$. WLOG a, b are squarefree, $|a| \leq |b|$.

Put $m = |a| + |b|$. $m = 2 \Rightarrow f = X_1^2 \pm X_2^2 \pm X_3^2$, since $0 \in Im(f_\infty)$,

the case $f = X_1^2 + X_2^2 + X_3^2$ is excluded, others are trivial.

$m > 2 \Rightarrow |b| \geq 2 \Rightarrow b = \pm p_1 \dots p_k$, p_i distinct primes, $p := p_i$:

We show $a \in (\mathbb{Z}/p\mathbb{Z})^2$. If $a \equiv 0 \pmod{p}$ obvious. Else, $a \in \mathbb{Q}_p^*$.

$\exists (x, y, z) \in \mathbb{Q}_p^3$ s.th $z^2 - ax^2 - by^2 = 0$, WLOG (x, y, z) primitive.

$\Rightarrow z^2 - ax^2 \equiv 0 \pmod{p}$, thus $p|x \Rightarrow p|z \Rightarrow p^2|by^2 \Rightarrow p|y$?!

Thus we have $p \nmid x \Rightarrow a$ is a square modulo p.

$\mathbb{Z}/b\mathbb{Z} \simeq \prod \mathbb{Z}/p_i\mathbb{Z} \Rightarrow a$ is a square modulo $b \Rightarrow \exists\ t, b' \in \mathbb{Z}$ s.th.

$|t| \leq \frac{|b|}{2}$ and $t^2 = a + bb'$. Thus $bb' \in Nk(\sqrt{a})^* :=$ the group of

norms of elements of the extension $k(\sqrt{a})/k$, $k = \mathbb{Q}$ or $\mathbb{Q}_v$

$\Rightarrow 0 \in Im(f)$ in k iff $0 \in Im(f' = X_1^2 - aX_2^2 - b'X_3^2)$

$\Rightarrow 0 \in Im(f'_v)\ \forall v \in V$, but $|b'| = \left|\frac{t^2-a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|$.

Finally, apply the induction hypothesis to the squarefree part of b'.

$\underline{n = 4:}$ We will need:

Fact 3. Let $a, b, c, d \in \mathbb{Q}^*$, let $\{\epsilon_{i,v}\}_{i \in I, v \in V} \in \{\pm 1\}$. Given that:

(1) all but finitely many $\epsilon_{i,v} = 1$,

(2) for all $i \in I$ we have $\prod_v \epsilon_{i,v} = 1$,

(3) for all $v \in V$ $\exists$ $x_v \in \mathbb{Q}_v^*$ s.th. $(a_i, x_v)_v = \epsilon_{i,v}$ $\forall v \in V$;

then there exists $x \in \mathbb{Q}^*$ s.th $(a_i, x)_v = \epsilon_{i,v}$ for all $i \in I, v \in V$.

Back to <u>$n = 4$:</u> Let $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. Pick $v \in V$.

Prop. B $\Rightarrow \exists\ x_v \in \mathbb{Q}_v^*$ represented by $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$

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

By Hilbert's Theorem: $\prod_v (a, b)_v = \prod_v (c, d)_v = 1$; Fact 3. $\Rightarrow$

$\exists\ x \in \mathbb{Q}^*$ s.th. $(x, -ab)_v = (a, b)_v$, $(x, -cd)_v = (c, d)_v$ for all v .

$\Rightarrow aX_1^2 + bY_2^2 - xZ^2$ represents 0 in each $\mathbb{Q}_v$, thus in $\mathbb{Q}$ by $n = 3$.

$\Rightarrow x$ is represented by $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$

$\Rightarrow f$ represents 0.

$\underline{n \geq 5:}$ By induction on n. Write $f = h \dot{+} (-g)$ with

$h = a_1 X_1^2 + a_2 X_2^2$ and $g = a_3 X_3^2 + \cdots + a + n X_n^2$.

Let $S = \{2, \infty\} \cup \{p \in V : v_p(a_i) \neq 0 \text{ for one } i \geq 3\}$. Let $v \in S$.

f_v represents $0 \Rightarrow \exists\ a_v \in \mathbb{Q}_v^*$ represented by h and g

$\Rightarrow \exists\ x_{i,v} \in \mathbb{Q}_v$ s.th. $h(x_{1,v}, x_{2,v}) = g(x_{3,v}, \cdots, x_{n,v}) = a_v$.

Fact 4.: $T \subset V$, $|T| < \infty \Rightarrow$ image of $\mathbb{Q}$ in $\prod_{v \in S} \mathbb{Q}_v$ is dense.

The square of $\mathbb{Q}_v^*$ form an open set (last lecture) and Fact 4. $\Rightarrow$

$\exists\ x_1, x_2 \in \mathbb{Q}$ s.th. if $a := h(x_1, x_2)$ then $\frac{a}{a_v} \in \mathbb{Q}_v^{*2}\ \forall\ v \in V$.

Put $f_1 := aZ^2 \dot{+} (-g)$. For $v \in S$ g represents a_v in $\mathbb{Q}_v \Rightarrow$

g represents a in $\mathbb{Q}_v \Rightarrow f_1$ represents 0 in $\mathbb{Q}_v$.

$v \notin S \Rightarrow a_3, \cdots, a_n \in \mathbb{Q}_v^*, \Rightarrow disc_v(g) \in \mathbb{Q}_v^* \Rightarrow \epsilon_v(g) = 1 \Rightarrow$

f_1 represents 0 in all $\mathbb{Q}_v$, $rank(f_1) = n - 1 \Rightarrow f_1$ represents 0 in $\mathbb{Q}$.

$\Rightarrow g$ represents a in $\mathbb{Q}$, but h represents $a \Rightarrow f$ represents 0 in $\mathbb{Q}$.

Corollaries:

Cor. B1: $a \in \mathbb{Q}$. Then f represents a in $\mathbb{Q}$ iff it does in each $\mathbb{Q}_v$.

Cor. B2: (Meyer). A quadratic for of rank ≥ 5 represents 0 in $\mathbb{Q}$

iff it does so in $\mathbb{R}$. (In such case 0 is represented in all $\mathbb{Q}_v$.)