REPRESENTATION OF INTEGRAL QUADRATIC FORMS BY INTEGRAL QUADRATIC FORMS

JEAN-LOUIS COLLIOT-THÉLÈNE (JOINT WORK WITH XU FEI)

1. Examples

In the book on quadratic forms by Cassels, one find the following:

Example 1.1. Let $m \equiv 3 \pmod{8}$. The equation $m^2 = X^2 - 2Y^2 + 64Z^2$ has a primitive solution in \mathbb{Z}_p for each p but no primitive solution in \mathbb{Z} . ("Primitive" means $\gcd(X, Y, Z) = 1$.)

Proof. We leave as an exercise that there exist local solutions. If $x, y, z \in \mathbb{Z}$ satisfy the equation and $\gcd(x, y, z) = 1$, then

$$(m - 8z)(m + 8z) = x^2 - 2y^2 \neq 0.$$

Suppose $p \mid m-8z$. Then $p \neq 2$. If $\left(\frac{2}{p}\right) = 1$, then $p \equiv \pm 1 \pmod{8}$. If $\left(\frac{2}{p}\right) = -1$ (so $p \equiv \pm 3 \pmod{8}$), then $x \equiv y \equiv 0 \pmod{p}$, so $p \nmid z$, so $p \nmid m+8z$; therefore $v_p(m-8z)$ is even, so

$$m - 8z = \prod_{p \equiv \pm 1 \pmod{8}} p^{n_p} \prod_{p \equiv \pm 3 \pmod{8}} p^{2n_p} \equiv 1 \pmod{8},$$

which contradicts the hypothesis on m.

What is going on?

Second proof. We have

$$(m - 8z)(m + 8z) = x^2 - 2y^2 \neq 0.$$

Let $\alpha=(m-8z,2)=(m+8z,2)\in \operatorname{Br}\mathbb{Q}$. We have $\alpha_{\mathbb{R}}=0$. If $p\neq 2$, and p does not divide both m-8z and m+8z, then $\alpha|_{\mathbb{Q}_p}=(\operatorname{unit},\operatorname{unit})=0\in \operatorname{Br}\mathbb{Q}_p$. If $p\neq 2$, and p divides both m-8z and m+8z, then $p|_{\mathbb{Z}}$, and p does not divide both x and y, so $\left(\frac{2}{p}\right)=1$, so $2\in \mathbb{Q}_p^{\times 2}$, so $\alpha|_{\mathbb{Q}_p}=0$. If p=2, then $(m-8z,2)=(m,2)=(\pm 3,2)\neq 0$, so $\alpha_{\mathbb{Q}_2}\neq 0$. This contradicts the exact sequence

$$\operatorname{Br} \mathbb{Q} \to \bigoplus_p \operatorname{Br} \mathbb{Q}_p \to \mathbb{Q}/\mathbb{Z}.$$

Theorem 1.2. Suppose that $m, n, k \ge 1$. Then $m^2x^2 + n^{2k}y^2 - nz^2 = 1$ has no solution over \mathbb{Z} if and only if

- $(n,m) \neq 1$, or
- $\bullet (n, m) = 1 \text{ but}$ $-n \equiv 5 \pmod{8} \text{ and } 2 \mid m, \text{ or}$

Date: IU Bremen, July 24, 2007.

$$-n \equiv 3 \pmod{8}$$
 and $4 \mid m$.

2. Representing quadratic forms by quadratic forms

More generally, one can consider the following problem. Consider two quadratic forms over \mathbb{Z} , say g of rank n over \mathbb{Q} and f of rank m over \mathbb{Q} , nondegenerate over \mathbb{Q} . Write $g \prec f$ if there exist linear forms ℓ_i with coefficients in \mathbb{Z} such that

$$g(x_1, \ldots, x_n) = f(\ell_1(x_1, \ldots, x_n), \ldots, \ell_m(x_1, \ldots, x_n)).$$

In the case n = 1, we are asking the classical question of whether a nonzero integer a is representable as $f(x_1, \ldots, x_n)$.

In general, given a scheme \mathcal{X} over \mathbb{Z} , we can ask about $\mathcal{X}(\mathbb{Z}) \neq \emptyset$. Assume that over each \mathbb{Z}_p we have $g \prec_{\mathbb{Z}_p} f$; does this imply $g \prec_{\mathbb{Z}} f$? This is a question of the type: does $\prod_p \mathcal{X}(\mathbb{Z}_p) \neq \emptyset$ imply $\mathcal{X}(\mathbb{Z}) \neq \emptyset$?

One reason to work with schemes: Let $\mathcal{X}_1 = \operatorname{Spec} \mathbb{Z}[x, y, z]/(f - a)$. Let $\mathcal{X} = \mathcal{X}_1 - \{x = y = z = 0\}$. Then $\mathcal{X}(\mathbb{Z})$ is the set of primitive integer solutions to a = f(x, y, z).

Let \mathcal{X} be a separated scheme. Let $X = \mathcal{X} \times_{\mathbb{Z}} \mathbb{Q}$. Then $\mathcal{X}(\mathbb{Z}) \hookrightarrow X(\mathbb{Q})$. Let \mathcal{X}' be the schematic closure of X in \mathcal{X} . Fact: $\mathcal{X}'(\mathbb{Z}) = \mathcal{X}(\mathbb{Z})$ and $\mathcal{X}'(\mathbb{Z}_p) = \mathcal{X}(\mathbb{Z}_p)$. Concretely, this is saying, for instance, that pf(x, y, z) = pa has the same integral solutions as f(x, y, z) = a.

Let k be a number field. Let $\mathcal{O} \subset k$ be the ring of integers. Let Ω be the set of places of k. Let \mathcal{X}/\mathcal{O} be a separated flat scheme. Let $X = \mathcal{X} \times_{\mathcal{O}} k$. Define the adèles of X as

$$X(\mathbb{A}_k) = \bigcup_{\text{finite } S \subset \Omega} \left[\prod_{v \in S} X(k_v) \times \prod_{v \notin S} \mathcal{X}(\mathcal{O}_v) \right] \subset \prod_{v \in \Omega} X(k_v).$$

This is the same as the set of k-morphisms $\operatorname{Spec} A_k \to X$.

Over an arbitrary field k with char k = 0, if X is a variety over k, then

$$k[X]^{\times} = H^{0}(X, \mathbb{G}_{m})$$

 $\operatorname{Pic} X = H^{1}_{\operatorname{Zar}}(X, \mathbb{G}_{m}) = H^{1}_{\operatorname{et}}(X, \mathbb{G}_{m})$ (Hilbert's theorem 90)
 $\operatorname{Br} X = H^{2}_{\operatorname{et}}(X, \mathbb{G}_{m}).$

If X/k is smooth and integral, there is an exact sequence

$$0 \to \operatorname{Br} X \to \operatorname{Br} k(X) \to \bigoplus_{\substack{Y \subset X \\ \text{invaduable so dim 1}}} H^1(k(Y), \mathbb{Q}/\mathbb{Z}).$$

For X/k and $F \supset k$, we have

$$X(F) \times \operatorname{Br} X \to \operatorname{Br} F = \operatorname{Br} \operatorname{Spec} F = H^2(\mathcal{G}_F, \overline{F}^{\times}).$$

Now let k be a number field. Suppose $A \in \operatorname{Br} X$.

$$X(k) \longrightarrow X(\mathbb{A}_k)$$

$$\downarrow^{\operatorname{ev}_A} \qquad \qquad \downarrow^{\operatorname{ev}_A} \qquad \qquad \downarrow^{\theta_A}$$

$$\operatorname{Br} k \longrightarrow \bigoplus_{v \in \Omega} \operatorname{Br} k_v \stackrel{\sum i_v}{\longrightarrow} \mathbb{Q}/\mathbb{Z}$$

Manin 1970: $X(k) \subset X(\mathbb{A})^{\operatorname{Br}} := \bigcap_{A \in \operatorname{Br} X} \ker \theta_A$.

Analogously, we have

$$\mathcal{X}(\mathcal{O}) \subset \left(\prod \mathcal{X}(\mathcal{O}_v)\right)^{\mathrm{Br}}$$

Let G be a connected linear algebraic group. Let X/k be a homogeneous space of G: this means that we have a group variety action $G \times X \to X$ and $G(\overline{k})$ acts transitively on $X(\overline{k})$.

Basic example: X = G/H where H is a subgroup of G (note: forming the quotient variety is not a trivial operation).

Back to our general problem: Let $\mathcal{X} = \operatorname{Mor}_{\mathcal{O}}(g, f)$. Witt: Then $X = \operatorname{Mor}_{k}(g_{k}, f_{k})$ is a homogeneous space of the orthogonal group $O(f_{k})$.

- If n < m, then X is a homogeneous space of SO(f).
- If n = m and $X(k) \neq \emptyset$, then $X = X_0 \cup X_1$ where X_0 is a homogeneous space of SO(f).

We are assuming $\prod \mathcal{X}(\mathcal{O}_v) \neq \emptyset$. So $\prod X(k_v) \neq \emptyset$. By Hasse's theorem (1924/25), $X(k) \neq \emptyset$. Fix a point $P_0 \in X(k)$; then $X = SO(f)/H_1$, where H_1 is the stabilizer of P_0 .

Suppose that $m \geq 3$. Then we can also write $SO(f)/H_1 = Spin(f)/H$ for some $H \leq Spin(f)$. Write $f \simeq g \perp h$, where f, g, h are of ranks m, n, m - n, respectively.

- If $m n \ge 3$, then H = Spin(h).
- If m n = 2, then $H = \hat{R}_{K/k}^1 \mathbb{G}_m$ where $K = k(\sqrt{-\det f \cdot \det g})$.
- If $m n \le 1$, then $H = \mu_2$, and X = SO(f).

General situation: Let X = G/H where G is a semisimple simply connected group that is absolutely simple.

For X = G, we have

- $k^{\times} = k[G]^{\times}$
- Pic G = 0
- Br $k \stackrel{\sim}{\to} Br G$.

In general,

- $\bullet \ k^{\times} \stackrel{\sim}{\to} k[X]^{\times}.$
- $\hat{H}(k) \stackrel{\sim}{\to} \operatorname{Pic} X$, where $\hat{H} := \operatorname{Hom}_{k\text{-groups}}(H, \mathbb{G}_m)$.
- $H^1(\mathcal{G}_k, \hat{H}(\overline{k})) \simeq \ker (\operatorname{Br} X \to \operatorname{Br} \overline{X})$, where $\overline{X} := X \times_k \overline{k}$.

If H is connected, there is an isomorphism $\operatorname{Pic} H \xrightarrow{\sim} \operatorname{Br} X/\operatorname{Br} k$: these are finite groups. We return to the situation $g \prec f$ with g, f of ranks n, m.

- If $m n \ge 3$, then $-\operatorname{Pic} X = 0$ $-\operatorname{Br} k \xrightarrow{\sim} \operatorname{Br} X$.
- If m n = 2, then
 If $-\det f \cdot \deg g$ is a square, then
 - $* \operatorname{Pic} X = \mathbb{Z}$ $* \operatorname{Br} k = \operatorname{Br} X.$
 - If not a square, then Br X/ Br $k = \mathbb{Z}/2\mathbb{Z}$.
- If $m-n \le 1$, then $\operatorname{Br} X/\operatorname{Br} k = k^{\times}/k^{\times 2}$.

3. General Theorem

Theorem 3.1. Let k be a number field. Let X = G/H where G is semisimple, simply connected and absolutely simple, and H is either connected or finite abelian. Assume that v_0 is a place of k such that $G(k_{v_0})$ is not compact: one says then that $G_{k_{v_0}}$ is "isotropic". Suppose \mathcal{X}/\mathcal{O} and $X := \mathcal{X} \times_{\mathcal{O}} k \simeq G/H$. Assume that

$$\left(\prod_{v\in\omega}\mathcal{X}(\mathcal{O}_v)\right)^{\operatorname{Br}X}\neq\emptyset.$$

Let $\mathcal{O}_{\{v_0\}}$ be the subring of elements of k that are integral away from v_0 . Then $X(\mathcal{O}_{\{v_0\}}) \neq \emptyset$.

We use the Hasse principle for semisimple simply connected groups G:

Theorem 3.2 (Eichler, Kneser, Harder, Chernousov). For a semisimple simply connected group G, the map

$$H^1(k,G) \hookrightarrow \prod_{v \in \Omega} H^1(k_v,G)$$

is injective.

We use also the strong approximation theorem:

Theorem 3.3 (Eichler, Kneser, Platonov). Let G/k be semisimple simply connected and absolutely simple. If $G(k_{v_0})$ is not compact, then $G(k).G(k_{v_0})$ is dense in $G(\mathbb{A}_k)$.

We use also

Theorem 3.4 (Kottwitz). Let H be connected. Then there is an exact sequence

$$H^1(k,H) \to \bigoplus_{v \in \Omega} H^1(k_v,H) \to \operatorname{Hom}(\operatorname{Pic} H, \mathbb{Q}/\mathbb{Z}).$$

(The last map is constructed from the following, given for k, but which applies also to k_v :

$$H^1(k,H) \times \operatorname{Pic} H \to \operatorname{Br} k$$

defined by using $\operatorname{Ext}(H,\mathbb{G}_m) \xrightarrow{\sim} \operatorname{Pic} H$: an extension

$$1 \to \mathbb{G}_m \to E \to H \to 1$$

induces $H^1(k,H) \to H^2(k,\mathbb{G}_m) = \operatorname{Br} k$.)

One can also look at $H^1_{\text{et}}(X, H) \times \text{Pic } H \to \text{Br } X$. For μ finite abelian we have

$$H^1(k,\mu) \to \prod' H^1(k_v,\mu) \to \operatorname{Hom}(H^1(k,\hat{\mu}),\mathbb{Q}/\mathbb{Z})$$

where $\hat{\mu} := \text{Hom}(\mu, \mathbb{G}_m)$.

Proof of Theorem 3.1. Recall that X = G/H, so $G \to X$ is a torsor under H. We have

$$G(k) \longrightarrow G(\mathbb{A}_{k})$$

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow$$

$$X(k) \longrightarrow X(\mathbb{A}_{k}) \xrightarrow{\operatorname{Manin}} \operatorname{Hom}(\operatorname{Br} X/\operatorname{Br} k, \mathbb{Q}/\mathbb{Z})$$

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow$$

$$H^{1}(k, H) \longrightarrow \bigoplus_{v \in \Omega} H^{1}(k_{v}, H) \xrightarrow{\operatorname{Kottwitz}} \operatorname{Hom}(\operatorname{Pic} H, \mathbb{Q}/\mathbb{Z})$$

$$\downarrow \qquad \qquad \downarrow$$

$$H^{1}(k, G) \longrightarrow \prod_{v \in \Omega} H^{1}(k_{v}, G)$$

and the bottom map is injective by the Hasse principle.

Easy: If $(M_v) \in X(\mathbb{A})^{\text{Br}}$, then there exist $M \in X(k)$ and $(g_v) \in G(\mathbb{A}_k)$ such that $g_v M = M_v \in X(k_v)$ for each v. Use $(M_v) \in \prod \mathcal{X}(\mathcal{O}_v)$ and the fact that $G(k_0)G(k)$ is dense in $G(\mathbb{A}_k)$ (strong approximation). to find some $g_0 \in G(k)$ such that $g_0 M \in \mathcal{X}(\mathcal{O}_v)$ for any $v \neq v_0$.

One can play the same game with G/μ for μ finite abelian, using a sequence from class field theory.

Effectivity: Can we check the hypothesis

$$\left(\prod_{v\in\omega}\mathcal{X}(\mathcal{O}_v)\right)^{\operatorname{Br}X}\neq\emptyset?$$

Suppose that we are in the case where H is connected. The group $\operatorname{Pic} H \simeq \operatorname{Br} X/\operatorname{Br} k$ is finite. If one chooses $S \subset \Omega$ large enough, where $\mathcal{X} \times_{\mathcal{O}} \mathcal{O}_S \simeq \underline{G}/\underline{H}$, then it is enough to check

$$\operatorname{ev}_{A_i} : \prod_{v \in S} \mathcal{X}(\mathcal{O}_v) \to (\mathbb{Q}/\mathbb{Z})^v.$$

Now suppose instead that we are in the case $X = G/\mu$ with μ finite. Let S be big enough for μ . Then we have

$$H^1_{\mathrm{et}}(\mathcal{O}_S, \mu) \to \prod_{v \in S} H^1(k, \mu) \to \mathrm{Hom}(H^1_{\mathrm{et}}(\mathcal{O}_S, \hat{\mu}), \mathbb{Q}/\mathbb{Z}).$$

We get

$$\prod_{v \in S} \to \operatorname{Hom}(H^1_{\operatorname{et}}(\mathcal{O}_S, \hat{\mu}), \mathbb{Q}/\mathbb{Z}),$$

and the group $H^1_{\text{et}}(\mathcal{O}_S, \hat{\mu})$ is finite by Dirichlet's theorem and finiteness of the class number.

4. Application to quadratic forms

We want to know whether $g \prec f$ over \mathcal{O} , where the ranks are n and m, with $m \geq 3$. If $m - n \geq 3$, then Br X/ Br k = 0. Then $\prod_{v \in \Omega} \mathcal{X}(\mathcal{O}_v) \neq \emptyset$ implies $\mathcal{X}(\mathcal{O}_{\{v_0\}}) \neq \emptyset$ if $f_{k_{v_0}}$ is isotropic; over \mathbb{Q} we take $v_0 = \infty$. Suppose m - n = 2. Consider m = 3, n = 1. We want to solve a = f(x, y, z) with $a \neq 0$. This defines \mathcal{X} . Let $X = \mathcal{X} \times_{\mathcal{O}} k$. Then $\operatorname{Br} X / \operatorname{Br} k$ is 0 if $d := -a \cdot \det f$ is a square, and $\mathbb{Z}/2\mathbb{Z}$ if d is not a square. Consider the latter case.

$$\prod_{v \in \Omega} \mathcal{X}(\mathcal{O}_v) \to \mathbb{Z}/2\mathbb{Z}$$
$$(M_v) \mapsto \sum_v \operatorname{ev}_v(M_v).$$

How to find A? Since $\prod \mathcal{X}(\mathcal{O}_v) \neq \emptyset$, we have $\prod \mathcal{X}(k_v) \neq \emptyset$, so we can find a point $P_0 \in X(k)$. Let $Y \subset \mathbb{P}^3_k$ be defined by $q(x,y,z) - at^2 = 0$. Let $0 = \ell_1(x,y,z,t)$ be the tangent plane to Y at P_0 . We can show that $f(x,y,z) - at^2 = \ell_1\ell_2 + c(\ell_3^2 - \ell_4^2)$. Define $\alpha \in \operatorname{Br} k(X)$ by $\alpha = \left(\frac{\ell_1(x,y,z,t)}{t},d\right)$. We check that $\alpha \in \operatorname{Br} X - \operatorname{Br} k$. Let $K = k(\sqrt{d})$. Check the kernel of the map Θ obtained as the composition

$$\prod_{v \in \Omega} \mathcal{X}(\mathcal{O}_v) \to \bigoplus_{v \in \Omega} \frac{k_v^{\times}}{NK_v^{\times}} \to \mathbb{Z}/2\mathbb{Z}$$

where the first map sends M_v to $(\ell_1/t)(M_v)$. Assuming there exists a v_0 where f_{v_0} is isotropic, we have $\mathcal{X}(\mathcal{O}) \neq \emptyset$ if and only if there is a point in the kernel of Θ .

Let us apply this to

$$m^2x^2 + n^{2k}y^2 - nz^2 = 1.$$

This is solvable over each \mathbb{Z}_p if and only if (n, m) = 1; let us assume this. There is an obvious rational point, namely $P_0 := (0, -1/n^k, 0)$. Write the equation as

$$(1 + n^k y)(1 - n^k y) = m^2 x^2 - nz^2.$$

The tangent plane at P_0 is $1 + n^k y = 0$. In Br X, we have $\alpha = (1 + n^k y, n)$ (the number n is the old d). We have

$$\mathcal{X}(\mathbb{Z}_p) \to \operatorname{Br} \mathbb{Q}_p.$$

If $p \neq 2$, then $\operatorname{ev}_A(\mathcal{X}(\mathbb{Z}_p)) = 0$ always. If p = 2, then $\operatorname{ev}_A(\mathcal{X}(\mathbb{Z}_2)) = 1$ in $\mathbb{Z}/2\mathbb{Z}$ if and only if $n \equiv 5 \pmod 8$ and $2 \mid m$, or $n \equiv 3 \pmod 8$ and $4 \mid m$.

Exercise 4.1 (Schulze-Pillot). Take $k = \mathbb{Q}(\sqrt{35})$. If p is a prime such that $(\frac{p}{7}) = 1$, then $7p^2 = a^2 + b^2 + c^2$ over each \mathcal{O}_v but not over $\mathcal{O} = \mathbb{Z}[\sqrt{35}]$. Prove that this is given by a Brauer-Manin obstruction.

Exercise 4.2. Fix f(x, y, z). The elements $a \in \mathbb{Z}$ such that $a \prec f$ over each \mathbb{Z}_p but not over \mathbb{Z} fall into finitely many classes in $\mathbb{Q}^{\times}/\mathbb{Q}^{\times}$. (The same holds over any number field.)

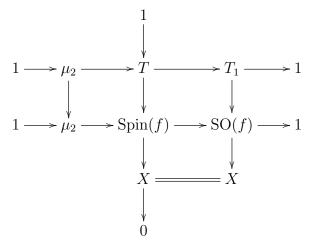
We now consider the case m = n + 2 with $n \ge 3$. So $X = \operatorname{Spin}(f)/T$ where $T := R^1_{K/k} \mathbb{G}_m$ is given by an equation $N_{K/k}(\) = 1$, where $K = k(\sqrt{d})$ (which we assume is a field), where $d := -\det f \cdot \det g$. We have $\operatorname{Pic} T = \mathbb{Z}/2\mathbb{Z}$. What, concretely, is the map

$$\prod_{v \in \Omega} X(k_v) \longrightarrow \bigoplus_{v \in \Omega} H^1(k_v, T) \longrightarrow \operatorname{Hom}(\operatorname{Pic} T, \mathbb{Q}/\mathbb{Z})$$

$$\downarrow \qquad \qquad \qquad \qquad \parallel$$

$$k_v^{\times}/NK_v^{\times} \longrightarrow \mathbb{Z}/2\mathbb{Z}?$$

Use



where $T_1 \simeq T$. We have

$$SO(f)(F) \longrightarrow F^{\times}/F^{\times 2}$$

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow$$

$$X(F) \longrightarrow H^{2}(F,T) = F^{\times}/N(F.K)^{\times}$$

where the top map is the spinor norm sending a product of (an even number of) reflections $\prod \tau_{v_i}$ to $\prod f(v_i)$.

Application to an example of Siegel:

$$x^2 + 32y^2 \prec x^2 + 128y^2 + 128yz + 544z^2 - 64t^2$$

over each \mathbb{Z}_p but not over \mathbb{Z} .

Classical problem: Suppose we have a quadratic space $(V/k, f_k)$ with f_k nondegenerate, and we have $N, M \subset V$ where M is a full lattice: $N_k \subset V$ and $M_k = V$. Assume that $f(M) \subset \mathcal{O}$ and $f(N) \subset \mathcal{O}$, and that $g := f|_{N_k}$ is nondegenerate. Let $\operatorname{Hom}((N, g), (M, f))(A)$ be the set of $\phi \colon N_A \to M_A$ such that $\phi^*(f) \simeq g$. Define $\mathcal{X} = \operatorname{Hom}((N, g), (M, f))$. We are given $P_0 \in X(k)$. The group $O(f)(\mathbb{A})$ acts on the full lattices in (V, f_k) .

"N is represented by the proper class of M" translates as $\mathcal{X}(\mathcal{O}) \neq \emptyset$.

"N is represented by the genus class of M" translates as $\prod_{v} \mathcal{X}(\mathcal{O}_{v}) \neq \emptyset$.

"N is represented by the proper spinor genus of M" translates as $(\prod_v \mathcal{X}(\mathcal{O}_v))^{\operatorname{Br} X} \neq \emptyset$.

There is also a weak approximation statement analogous to our Brauer-Manin obstruction statement for the integral Hasse principle.