1. Quadratic forms

1.1. Preliminaries.

Definition 1.1. Let k be a field of characteristic not equal to 2. Let V be a vector space over k of dimension n. A quadratic form is a function $Q : V \to k$ such that

(1) $Q(ax) = a^2 Q(X)$ for $x \in V$ and $a \in k^\times$.
(2) The pairing $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is bilinear.

We can associate a k-valued symmetric bilinear form $\langle\ ,\ \rangle_Q$ on $V \times V$ to Q defined by

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

It is clear that $\langle x, x\rangle_Q = Q(x)$. This gives a bijection between quadratic forms and symmetric bilinear forms

From now on, we assume that $k = \mathbf{Q}$ or $\mathbf{Q}_p$. Let $\underline{e} = \{e_i\}$ be a k-basis of V. The $n \times n$ matrix $Q(\underline{e})$ of Q associated to $\underline{e}$ is defined by

$$Q(\underline{e}) := (\langle e_i, e_j\rangle_Q)_{1 \le i,j \le n}.$$

It is easy to see that if $\underline{e'}$ is another basis of V, then there exists $J \in \mathrm{GL}_n(k)$ such that

$$Q(\underline{e'}) = J^t \cdot Q(\underline{e}) \cdot J.$$

We say (V, Q) is non-degenerate if $\det Q(\underline{e}) \neq 0$. We introduce an important invariant attached to (V, Q).

Definition 1.2. Suppose that (V, Q) is non-degenerate. We define the discriminant

$$\delta_k(Q) := \det Q(\underline{e}) \in k^\times/(k^\times)^2.$$

This definition is independent of the choice of a basis of V.

Definition 1.3. Let (V, Q) be a quadratic space. Then

(1) $x, v \in V$ are *orthogonal* if $(x, y)_Q = 0$
(2) Orthogonal complement: $U^\perp := \{x \in U \mid (x, U)_Q = 0\}$.
(3) Radical of V is defined to be $V^\perp$
(4) (V, Q) is non-degenerate if $V^\perp = 0$.
(5) Orthogonal sum: $V = U \oplus W$ such that $(U, W)_Q = 0$.
(6) If W is a subspace of V with $(W, Q|_W)$ is non-degenerate, then $V = W \oplus W^\perp$.
(7) A vector $x \in V$ is called *isotropic* if $Q(x) = 0$.
(8) We call (V, Q) a *hyperbolic plane* if $V = kx + ky$ such that x, y are isotropic and $(x, y)_Q = 1$.

Lemma 1.4. *Suppose (V, Q) is non-degenerate. For a isotropic vector x, there exists $y \in V$ such that $U := kx + ky$ is a hyperbolic plane.*

Proposition 1.5. *If (V, Q) is non-degenerate, then there exists a orthogonal basis $\underline{e} = \{e_1, e_2, \cdots, e_n\}$. In other words,*

$$Q(\underline{e}) = \mathrm{diag}(a_1, a_2, \cdots, a_n) \text{ with } a_i \in k^\times.$$

1.2. **Quadratic forms over local fields.** Let $k = \mathbf{Q}_p$ and (V, Q) be a non-degenerate quadratic space. Let $\underline{e} = \{e_i\}_{i=1,\dots,n}$ be a orthogonal basis and let $Q(\underline{e}) = \mathrm{diag}(a_1, \cdots, a_n)$. Then $\delta_k(Q) = a_1 a_2 \cdots a_n \in k^\times/(k^\times)^2$. We define the Hasse invariant $\mathrm{H}_k(Q)$ by

$$\mathrm{H}_k(Q) := \prod_{1 \le i < j \le n} (a_i, a_j)_p \in \{\pm 1\}.$$

Theorem 1.6. *The Hasse invariant $\mathrm{H}_k(Q)$ does not depend on the choice of a orthogonal basis.*

2. Solutions of the equation of quadratic forms over local fields

Let k be a field.

Definition 2.1. A quadratic form of rank n over k is a n-variable homogeneous quadratic polynomial

$$f(x_1, \cdots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j, \quad a_{ij} = a_{ji} \in k.$$

To a quadratic space (V, Q), we can associate a quadratic form of rank n

$$f(x_1, \cdots, x_n) := \sum_{1 \le i,j \le n} \langle e_i, e_j \rangle_Q \cdot x_i x_j$$

for a choice of basis $\underline{e} = \{e_i\}$ of V. Conversely, given a quadratic form f of rank n over k, we define a quadratic space (k^n, Q_f) by

$$Q_f(\sum_{i=1}^n a_i e_i) = f(a_1, \cdots, a_n).$$

For f, f' two quadratic forms of rank n, we say $f \sim f'$ (f is equivalent to f') if $(k^n, Q_f) \simeq (k^n, Q_{f'})$, or equivalently, there exists a quadratic space (V, Q) with $\dim V = n$ and bases $\{e_i\}$ and $\{f_i\}$ such that

$$f(x_1, \cdots, x_n) = Q(\sum_{i=1}^n x_i e_i); \quad f'(x_1, \cdots, x_n) = Q(\sum_{i=1}^n x_i f_i).$$

We say f is *non-degenerate* if Q_f is non-degenerate or equivalently $\delta_k(Q_f) \neq 0$. In what follows, we assume f is a non-degenerate quadratic form of rank n over a field k.

Definition 2.2. For $a \in k$, we say f represents a in k if $f(x) = a$ has a nonzero solution $x \in k^n$. Equivalently,

$$\begin{aligned} & f \text{ represents } a \\ \iff & Q_f(v) = a \text{ for some nonzero } v \in V = k^n \\ \iff & f \sim f' + aX_n^2 \text{ for some quadratic form } f' \text{ of rank } n-1. \end{aligned}$$

Lemma 2.3. *(1) If f represents 0, then f represents every element in k.*
(2) Let $a \in k^\times$. Then f represents a if and only $f - aX_{n+1}^2$ represents 0.

Now we let $k = \mathbf{Q}_p$ (p is allowed to be ∞). Let $\delta(f) := \delta_{\mathbf{Q}_p}(Q_f) \in k^\times/(k^\times)^2$ be the determinant and $\mathrm{H}(f) := \mathrm{H}_{\mathbf{Q}_p}(Q_f)$ be the Haase invariant of f.

Example 2.4. If $f \sim f' + aX_n^2$ with f' quadratic form of rank $n-1$, then

$$\delta(f) = \delta(f') \cdot a \text{ and } \mathrm{H}(f) = \mathrm{H}(f') \cdot (a, \delta(f'))_p.$$

Theorem 2.5. *f represents 0 in k if and only if*

(1) $n = 2$ and $\delta(f) = -1$.
(2) $n = 3$ and $(-1, -\delta(f))_p = \mathrm{H}(f)$.
(3) $n = 4$ and $\delta(f) \neq 1$ or $\delta(f) = 1$ and $\mathrm{H}(f) = (-1, -1)_p$.
(4) $n \geq 5$ and $p < \infty$.

Example 2.6. $x^2 + 2y^2 = 7$ has no solution in $\mathbf{Q}_2$.

Corollary 2.7. *Let $a \in k^\times$. Then f represents a in k if and only if*

(1) $n = 1$ and $\delta(f) = a$.
(2) $n = 2$ and $(a, -\delta(f))_p = \mathrm{H}(f)$.
(3) $n = 3$ and either $a \neq -\delta(f)$ or $a = -\delta(f)$ and $(-1, -\delta(f))_p = \mathrm{H}(f)$.
(4) $n \geq 4$ and $p < \infty$.

Theorem 2.8 (Classification of quadratic forms over local fields)**.** *Two quadratic forms f and f' of rank n are equivalent if and only if $\delta(f) = \delta(f')$ and $\mathrm{H}(f) = \mathrm{H}(f')$.*

3. Hasse-Minkowski theorem and applications

Theorem 3.1 (Strong approximation)**.** *Let S be a finite set of primes and let $q \leq \infty$ be a prime not in S. Give any $\epsilon > 0$ and $x_p \in \mathbf{Q}_p$ for each $p \in S$. Then there exists $x \in \mathbf{Q}$ such that*

$$|x - x_p| < \epsilon \text{ for all } p \in S; \quad |x|_p \leq 1 \text{ for all } p \notin S \cup \{q\}.$$

Theorem 3.2. *Let f be a quadratic form of rank n over $\mathbf{Q}$. Then f represents 0 in $\mathbf{Q}$ if and only f represents 0 in $\mathbf{Q}_p$ for all p (including $p = \infty$).*

Proof. We sketch a proof here.

The case $n = 2$: Since f represents 0 in $\mathbf{R}$, we may assume $f = X^2 - aY^2$ with $a > 0 \in \mathbf{Q}$. Then it is not difficult to see that f represents 0 in $\mathbf{Q}_p$ for all primes p if and only if the p-adic valuation $v_p(a)$ is even for all p. This is equivalent to saying that $a \in (\mathbf{Q}^\times)^2$, and hence f represents 0 in $\mathbf{Q}$.

The case $n = 3$: We may assume $f = X^2 - aY^2 - bZ^2$. We may assume that a and b are co-prime square-free integers with $|a| \leq |b|$. Let $m = |a| + |b| \geq 2$. We prove the theorem by induction on m. In other words, we will show that if f represents 0 in $\mathbf{Q}_p$ for all p, then f represents 0 in $\mathbf{Q}$. If $m = 2$, then $a, b = \pm 1$, then $f = X^2 \pm Y^2 \pm Z^2$. It can be checked directly that f represents 0 in $\mathbf{Q}$ except for $f = X^2 + Y^2 + Z^2$ which do not represent 0 in $\mathbf{Q}_\infty = \mathbf{R}$.

We suppose that $m > 2$. Write $b = \pm p_1 \cdots p_s$, where p_i are distinct primes. For each $p_i | b$, f represents 0 in $\mathbf{Q}_{p_i}$, so $X^2 - aY^2 - bZ^2 = 0$ has a solution $X, Y \in \mathbf{Z}_{p_i}^\times$ and $Z \in \mathbf{Z}_{p_i}$, which in particular implies that $a \in (\mathbf{Z}_{p^i}^\times)^2$. By Chinese remainder theorem, we conclude that $a \pmod b$ is a square. Thus we may write

$$t^2 = a + bb' \text{ for some } b' \in \mathbf{Z},\ |t| \leq \frac{b}{2}.$$

In particular, bb' is a norm of $\mathbf{Q}(\sqrt{a})$. Thus we can deduce that

$$f \text{ represents } 0 \text{ in } k \text{ if and only if } X^2 - aY^2 - b'Z^2 \text{ represents } 0 \text{ in } k,$$

where k can be $\mathbf{Q}$ or $\mathbf{Q}_p$. On the other hand,

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

Write $b' = u^2 b''$ for some $u \in \mathbf{Z}$ and square-free b''. Then

$$X^2 - aY^2 - b'Z^2 \text{ represents } 0 \text{ in } k \text{ if and only if } X^2 - aY^2 - b''Z^2 \text{ represents } 0 \text{ in } k.$$

We thus reduced the problem to $X^2 - aY^2 - b''Z^2$ with $|b''| \leq |b'| < |b|$. The usual induction argument completes the proof for the case $n = 3$.

The case $n = 4$: We may assume $f = g - \ell$, where $g = a_1X^2 + a_2X_2^2$ and $\ell = a_3X_3^2 + a_4X_4^2$ with $a_1, a_4 > 0$. For $k = \mathbf{Q}$ or $\mathbf{Q}_p$, we know that f represents 0 in k if and only if there exists $x \in k^\times$ such that x is represented by g and ℓ. Let $N = 4p_1p_2 \cdots p_s$, where p_i are odd prime divisors of the product $a_1a_2a_3a_4$. We have assumed that f represents 0 in $\mathbf{Q}_p$ for all p. In particular, for $p|N$, there exists $b_p \in \mathbf{Z}_p - p^2\mathbf{Z}_p$ which is represented by g and ℓ in $\mathbf{Q}_p$. By the Strong approximation theorem with $S = \{2, p_1, \ldots, p_s\}$ and $q = \infty$(or Chinese remainder theorem), there exists $a_0 \in \mathbf{Z}_{\geq 0}$ such that

$$a_0 \equiv b_2 \,(\mathrm{mod}\ 16),\ a_0 \equiv b_{p_i} \,(\mathrm{mod}\ p_i^2) \text{ for } i = 1, \cdots s. \tag{3.1}$$

Let $m = N^2 = 16p_1^2p_2^2 \cdots p_s^2$. Any a satisfying the congruence relation must be of the form $a = a_0 + mk$ for $k \in \mathbf{Z}$, and

$$b_2^{-1}a \equiv 1 \,(\mathrm{mod}\ 8),\ b_{p_i}^{-1}a \equiv 1 \,(\mathrm{mod}\ p_i) \text{ for all } i = 1, \cdots s.$$

In particular, $b_p^{-1}a \in (\mathbf{Z}_p^\times)^2$ for all $p|N$. We recall the following theorem of Dirichlet:

Theorem (Dirichlet)**.** *Let a, b be two co-prime integers. Then there exist infinitely primes of the form $a + bn$, $n \in \mathbf{Z}$.*

Let $d = (a_0, m)$ be the G.C.D. of a_0 and m. Then by the above theorem, there exists a prime $q = \frac{a_0}{d} + \frac{m}{d} \cdot k$ for some $k \in \mathbf{Z}_{>0}$ and $q \nmid N$. Let $a := dq = a_0 + mk$. Consider two rank 3 quadratic forms:

$$g' := g - aX_5^2,\ \ell' = \ell - aX_5^2.$$

Then g' and ℓ' both represent 0 in $\mathbf{Q}_p$ for all $p|N$. On the other hand, if $p \nmid Nq$, then the coefficients of g' and ℓ' all belong to $\mathbf{Z}_p^\times$. It follows that g' and h' represent 0 in $\mathbf{Q}_p$ for all $p \nmid Nq$ by Theorem 2.5 (2). To sum up, we have proved that g' and ℓ' both represent 0 for all $\mathbf{Q}_p$ with $p \neq q$. Again by Theorem 2.5 (2) combined with the quadratic reciprocity law, we conclude that g' and ℓ' represent 0 in $\mathbf{Q}_q$ as well, and hence g' and ℓ' represent 0 in $\mathbf{Q}$ by the solution to Hasse-Minkowski's theorem for $n = 3$, which is equivalent to saying that g and ℓ represent a in $\mathbf{Q}$. This completes the proof for the case $n = 4$.

The case $n \geq 5$: The proof is similar to the case $n = 4$. □

Homework (Due date: 11/18)

Exercise 1 (10 pts)**.** Determine if the following equations have a non-zer0 solution in $\mathbf{Q}$

(1) $3x^2 + 5y^2 = z^2$,
(2) $5x^2 + 7y^2 = 13z^2$.

Exercise 2 (5pts)**.** Find conditions for $a \in \mathbf{Z}$ such that the quadratic form $x^2 + 2y^2 - az^2$ represents 0 in $\mathbf{Q}$.

Exercise 3 (5pts)**.** Let $a, b, c \in \mathbf{Z}$ be three *square-free* integers. Suppose that a, b, c are relatively prime to each other and $abc < 0$ but a, b and c are not all negative. Let

$$f(x, y, z) = ax^2 + by^2 + cz^2.$$

Then f represents 0 in $\mathbf{Q}$ if and only if the following congruence equations

$$x^2 \equiv -bc \,(\mathrm{mod}\ a)$$
$$x^2 \equiv -ca \,(\mathrm{mod}\ b)$$
$$x^2 \equiv -ab \,(\mathrm{mod}\ c)$$

have solutions in $\mathbf{Z}$.