University of Bordeaux **Number Theory**
M2 AGNT/ALGANT, 2026–2027

Exercise sheet n°4

Hasse–Minkowski theorem

Exercise 1 – In this exercise, we consider the regular form $Q = X^2 + Y^2 - pZ^2$, where p is a fixed odd prime number.

1) Recall why Q is isotropic over $\mathbb{Q}_\ell$ for all $\ell \neq 2, p$.

2) Show that Q is isotropic over $\mathbb{Q}_p$ if and only if $p \equiv 1 \pmod 4$.

3) Show that Q is isotropic over $\mathbb{Q}_2$ if and only if $p \equiv 1 \pmod 4$.

4) Show that p is a sum of two rational squares if and only if $p \equiv 1 \pmod 4$.

Exercise 2 – Recall the proofs of the following properties :

1) A regular isotropic form over a field K of odd characteristic is universal (i.e. represents all $a \in K$.)

2) The form $X^2 + aY^2$ $(a \neq 0)$ is universal over $\mathbb{F}_p$. Is it isotropic ?

3) Any regular form in three variables over $\mathbb{F}_p$ is isotropic.

Exercise 3 – Does either of the forms $3X^2 + 5Y^2 - 7Z^2$, $3X^2 - 5Y^2 - 7Z^2$ represent zero over $\mathbb{Q}$?

Exercise 4 – Let $n \in \mathbb{Z}$ be a nonzero integer. Write n in the form $n = 4^a m$, where $m \equiv 1, 2, 3, 5, 6, 7 \pmod 8$. Show that n is the sum of three rational squares if and only if $m \neq 7 \pmod 8$.

Exercise 5 – Find all solutions of the equation $X^2 + Y^2 - 2Z^2 = 0$ in rational numbers.

Exercise 6 – (Cassels–Davenport theorem). The goal of this exercise is to prove the following theorem. *Let Q be a positive defined quadratic form over $\mathbb{Z}$ in m variables. Assume that for each $\vec{x} \in \mathbb{Q}^m$ there exists $\vec{y} \in \mathbb{Z}^m$ such that $Q(\vec{x} - \vec{y}) < 1$. Then every integer which is rationally represented by Q, is also integrally represented by Q. Namely, if $n = Q(\vec{a})$ for some $\vec{a} \in \mathbb{Q}^m$, then there exists $\vec{b} \in \mathbb{Z}^m$ such that $n = Q(\vec{b})$.*

Let Q be a positive defined quadratic form over $\mathbb{Z}$. For any two vectors $\vec{x}, \vec{y} \in \mathbb{R}^m$, we set $(\vec{x}, \vec{y}) = \frac{1}{2}(Q(\vec{x}+\vec{y}, \vec{x}+\vec{y}) - Q(\vec{x}, \vec{x}) - Q(\vec{y}, \vec{y}))$. Recall that $(\ ,\ ) : \mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}$ is a scalar product on $\mathbb{R}^m$ and that $(\vec{x}, \vec{x}) = Q(\vec{x})$ for each $\vec{x}$.

1) Let $\vec{r} \in \mathbb{R}^m$ be a nonzero vector and let H be the hyperplane orthogonal to $\vec{r}$ and passing through the origin. Show that the reflection τ across H is given by the formula

$$\tau(\vec{x}) = \vec{x} - 2\frac{(\vec{x}, \vec{r})}{(\vec{r}, \vec{r})}\vec{r}.$$

2) Show that the reflection preserves scalar products, namely $(\tau(\vec{x}), \tau(\vec{y})) = (\vec{x}, \vec{y})$ for all $\vec{x}, \vec{y} \in \mathbb{R}^m$.

In questions 3-5) below, we assume that an integer n is rationally represented by Q, namely, that $n = Q(\vec{x})$ for some $\vec{x} = (x_1, \ldots, x_m) \in \mathbb{Q}$. We denote by d the lowest common multiple of the denominators of x_i and assume that $d > 1$.

3) Assume that $\vec{y} \in \mathbb{Z}^m$ is such that $Q(\vec{x} - \vec{y}) < 1$. Write $\vec{x}$ in the form $\vec{x} = \vec{y} + \vec{z}$ and set $\vec{r} = d\vec{z}$. Show that

$$\tau(\vec{x}) = \vec{y} - \left(\frac{1}{d} + 2\frac{(\vec{y}, \vec{r})}{(\vec{r}, \vec{r})}\right)\vec{r}$$

and deduce that

$$\tau(\vec{x}) = \vec{y} - d\frac{(\vec{x}, \vec{x}) - (\vec{y}, \vec{y})}{(\vec{r}, \vec{r})}\vec{r}.$$

4) Show what $\frac{(\vec{r},\vec{r})}{d} \in \mathbb{Z}$ and that $\frac{(\vec{r},\vec{r})}{d} < d$.

5) Set Show that n is rationaly represented by $\tau(\vec{x})$ and that $\tau(\vec{x}) = (x'_1, \ldots, x'_m)$, where the lowest common divisor of the denominators of x_i is $< d$.

6) Prove the theorem of Cassels–Davenport.

Exercise 7 –

1) (Fermat). Show that an odd prime p is a sum of two integer squares if and only if $p \equiv 1 \pmod 4$.

2) (Gauss). Show that positive integer n is a sum of three integer squares if and only if n can not be written in the form $4^a(8b - 1)$ with $a, b \in \mathbb{N}$.

3) (Legendre). Show that every positive integer is a sum of of four integer squares.