Théorie des nombres - TD4

Exercise 1 (Hilbert's Symbol)**.** Let k be a field, and $a, b \in k^\times$. We define the *Hilbert Symbol* $(a,b)_k$ by

$$(a,b)_k = \begin{cases} 1 & \text{if } ax^2+by^2=z^2 \text{ has a non zero solution} \\ -1 & \text{otherwise} \end{cases}$$

1. Show the following relations

$$(a,b)=(b,a) \quad (a,c^2)=1$$

$$(a,-a)=1 \quad (a,1-a)=1$$

$$(a,b)=1 \Rightarrow (a'a,b)=(a',b)$$

$$(a,b)=(a,-ab)=(a,(1-a)b)$$

2. Show the following, for $k=\mathbb{R}$ or $\mathbb{Q}_p^\times$.

   Theorem 0.1. *If $k=\mathbb{R}$, then $(a,b)_\mathbb{R}=1$ except if $a,b<0$, in which case $(a,b)_\mathbb{R}=(-1,-1)_\mathbb{R}=-1$.*
   If $k=\mathbb{Q}_p$, show that, writing $a=p^\alpha u, b=p^\beta v$, $u,v\in\mathbb{Z}_p^\times$, we have

$$(a,b)=(-1)^{\alpha\beta\frac{p-1}{2}}\left(\frac{u}{p}\right)^\beta\left(\frac{v}{p}\right)^\alpha \quad \text{if } p\neq 2$$

$$(a,b)=(-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)} \quad \text{if } p=2$$

   with $\varepsilon(n)=\frac{n-1}{2}$ and $\omega(n)=\frac{n^2-1}{8}$.

   Hint : reduce to the cases $(\alpha,\beta)=(0,0),(1,0),(1,1)$.

3. Show that $(,)_k$ is a non degenerate bilinear form on the $\mathbb{F}_2$-vector space $k^\times/(k^\times)^2$ for $k=\mathbb{R}$ or $\mathbb{Q}_p$.
4. Show that given $a,b\in\mathbb{Q}^\times$, $(a,b)_v := (a,b)_{\mathbb{Q}_v}=1$ for almost all v and

$$\prod_v (a,b)_v = 1.$$

5. Show that given Q a quaternion algebra over $\mathbb{Q}$, show that the number of places v where Q is ramified (i.e. $Q\otimes\mathbb{Q}_v$ non split) is finite and even.
6. Can you find for any two distincts places of $\mathbb{Q}$ a quaternions algebra ramified exactly at these 2 places ?

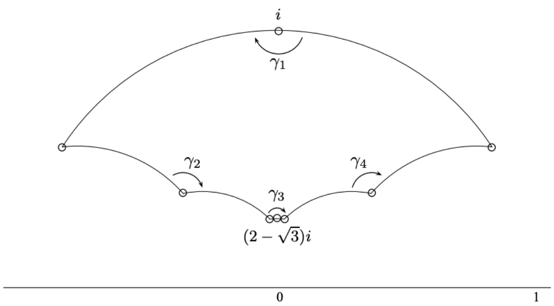
Exercise 2 (Courbes de Shimura)**.** 1. Let $\mathcal{O}$ be an order in a quaternion algebra D over $\mathbb{Q}$, such that $D\otimes\mathbb{R}=M_2(\mathbb{R})$. Show that $\mathcal{O}^1=\{o\in\mathcal{O} | N_{D_\mathbb{R}/\mathbb{R}}(o)=1\}$ acts on

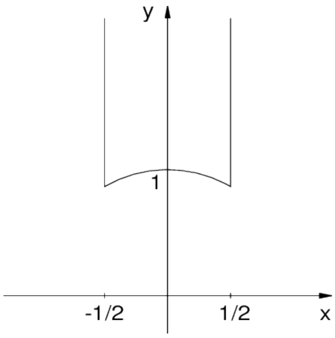
$$\mathbb{H} = \{x+iy\in\mathbb{C} \,|y>0\}.$$

2. Show that the action is properly discontinuous [1], and that we can define the quotient $\mathcal{O}^1\backslash\mathbb{H}$ (as a topological space). *Hint : Show first that $\mathcal{O}$ is discrete in $D_\mathbb{R}$*

1. i.e. for all $K\subset\mathbb{H}$ compact, $\{\gamma\in\mathcal{O}^1 |\ \gamma K\cap K\neq\emptyset\}$ is finite

3. Show that $\mathcal{O}^1\backslash\mathbb{H}$ is compact if and only if D is non split over $\mathbb{Q}$.
4. Here are "representations" of the quotient of $\mathbb{H}$ by the Norm 1 elements of the maximal order in $(-1,3)_{\mathbb{Q}}$ and in $M_2(\mathbb{Q})$ (socalled *fundamental domains*). Can you tell which is which ?





Exercise 3 (Minkowski)**.** 1. Using Minkowski's theorem, show that p is sum of two square if $p \equiv 1 \pmod 4$. *Hint : Suppose $p \equiv 1 \pmod 4$. Let $u \in \mathbb{Z}$ such that $u^2 \equiv -1 \pmod p$. Let $L = \{(a,b) \in \mathbb{Z}^2 | a \equiv ub \pmod p\}$. Show that it is a lattice, and calculate its covolume. Apply Minkowski theorem with the disc of radius $\sqrt{2p}$. What can you say about a^2+b^2 for $(a,b) \in L$?*

2. Show that if n has no square factor, -1 is a sum of two squares modulo n, thus $1+u^2+v^2 \equiv 0 \pmod n$. Let $L = \{(a,b,c,d) \in \mathbb{Z}^4 | c \equiv au+bv \pmod n, d \equiv av-bu \pmod n\}$. Reprove that any integer is a sum of 4 squares. *Hint : Show that you can reduce to n without square factors, that L is a lattice of covolume n^2, then use a well chosen disc and apply Minkowski's theorem. Use (or prove) that the disc of radius r in $\mathbb{R}^4$ has volume $\frac{\pi^2}{2}r^4$.*
3. Prove the following approximation theorem

   Theorem 0.2 (Dirichlet)**.** *Let $\alpha_1, \dots, \alpha_d \in \mathbb{R}$, and $N \in \mathbb{N}_{>0}$. Then there exists $p_1, \dots, p_d \in \mathbb{Z}$ and $1 \leq q \leq N$ an integer such that*

   $$|\alpha_i - \frac{p_i}{q}| \leq \frac{1}{qN^{1/d}}.$$

   Hint : Use Minkowski's theorem with

   $$C = \{(x, y_1, \dots, y_d) \in \mathbb{R}^{d+1} |\ x \in [-N-\frac{1}{2}, N+\frac{1}{2}], |\alpha_i x - y_i| \leq \frac{1}{N^{1/d}}\}.$$

Exercise 4 (Classification of projective finite type $\mathcal{O}_K$-modules)**.** If A is a commutative ring, a A-module of finite type P is projective if for every projective map of A-module $f : M \twoheadrightarrow N$, and every $g : P \to N$, there is a $h : P \to M$ such that $g = f \circ h$[2]. Let A be a Dedekind ring.

1. Show that a fractional ideal I of A is projective. *Hint : Use that $\mathfrak{a}(\mathfrak{a}^{-1}) = A$ to find generators $\mathfrak{a} = \sum Ax_i$ and to construct a lift $h :\ \mathfrak{a} \longrightarrow M$ of $g : \mathfrak{a} \longrightarrow N$ along $f : M \twoheadrightarrow N$.*
2. Show that a torsion-free, finitely generated A-module is a direct sum of ideals in A. Deduce that for finite type A-module, torsion-free and projective are equivalent notions. *Hint : Find an injective map $M \longrightarrow A^r$ for a well chosen r. What are the image on each component ?*
3. Show that for fractional ideals $\mathfrak{a}, \mathfrak{b}$, we have as A-module,

   $$\mathfrak{a} \oplus \mathfrak{b} \simeq A \oplus \mathfrak{a}\mathfrak{b}.$$

   Hint : Show that you can assume $\mathfrak{a}, \mathfrak{b}$ are inside A. Then show that you can assume that $\mathfrak{a}, \mathfrak{b}$ are coprime. For this, try to find $a \in \mathfrak{a}^{-1}$ such that $a\mathfrak{a} + \mathfrak{b} = A$, and for this use the decomposition of $\mathfrak{b}$ as a product of prime ideals (you want $a\mathfrak{a} \not\subset \mathfrak{p}$ for any $\mathfrak{p} \supset \mathfrak{b}$). Then find the obvious exact sequance and show it is split.

2. Equivalently (why ?) P is a direct factor in a free of finite rank A-module

4. Show that if two torsion-free finitely generated A-modules are written as $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ and $\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_m$, they are isomorphic if and only if $n = m$ and $\mathfrak{a}_1 \ldots \mathfrak{a}_n = \mathfrak{b}_1 \ldots \mathfrak{b}_n \in C\ell(A)$. *Hint : Show that* $\det(\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n) := \bigwedge^n(\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n) \simeq \mathfrak{a}_1 \ldots \mathfrak{a}_n$
5. By the morphism $M = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n \mapsto (n, \mathfrak{a}_1 \ldots \mathfrak{a}_n)$, to what is sent $M \oplus N$?

Exercise 5. Let p be a prime, and $\zeta = e^{2i\pi/p}$ a primitive p-th root of 1. Show that $\mathbb{Z}[\zeta]$ is the unique maximal order in $\mathbb{Q}(\zeta)$. *Hint : it is enough to show that $\mathbb{Z}[\zeta_p]$ is the ring of integers. Here are some steps*

1. *Show that $\frac{1-\zeta^r}{1-\zeta^s} \in \mathbb{Z}[\zeta]^\times$ for all $r, s \in \mathbb{Z}$ not divisible by p.*
2. *Deduce that $p = u(1-\zeta)^{p-1}$ for some $u \in \mathbb{Z}[\zeta]^\times$.*
3. *Let $\alpha = c_0 + c_1\zeta + \cdots + c_{p-2}\zeta^{p-2} \in \mathcal{O}_{\mathbb{Q}(\zeta)}, c_i \in \mathbb{Q}$. Using traces deduce $p\alpha \in \mathbb{Z}[\zeta]$.*
4. *Remark that if $\pi = 1-\zeta$, $\mathbb{Z}[\pi] = \mathbb{Z}[\zeta]$, then write $p\alpha = b_0 + b_1\pi + \cdots + b_{p-2}\pi^{p-2}, b_i \in \mathbb{Z}$. Show by induction that $p|b_i$ for all i using step 2.*

Exercise 6 (Calculation of some class groups)**.**

1. Let $K = \mathbb{Q}(i\sqrt{7})$. Show that $h_K := |C\ell(\mathcal{O}_K)| = 1$.
2. Let $K = \mathbb{Q}(\sqrt{-5})$. Show that $C\ell(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z}$.
3. Deduce that $Y^3 = X^2 + 5$ has no integral solution, but has a solution modulo n for all $n \in \mathbb{N}_{>0}$.
4. Let $K = \mathbb{Q}(\sqrt{-14})$. Show that $C\ell(\mathcal{O}_K) = \mathbb{Z}/4\mathbb{Z}$.
5. Let $K = \mathbb{Q}(\sqrt{2})$ or $K = \mathbb{Q}(\sqrt{7})$. Show that $h_K := |C\ell(\mathcal{O}_K)| = 1$.

Remark 0.3. Actually we know the full list of quadratic fields $K = \mathbb{Q}(\sqrt{d})$ for which the norm gives the structure of a euclidean ring for $\mathcal{O}_K$ (such a ring is called *norm euclidean*) :

$$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

But the story doesn't stop here : while we know that for quadratic *imaginary* field (i.e. $d < 0$) euclidean and norm euclidean are equivalent, thus giving the full list of quadratic imaginary field for which integral elements form an euclidean ring, the result is completely different for *real* quadratic fields ($d > 0$), as for $d = 14, 69$ the corresponding rings are euclidean but not Norm euclidean (a theorem of Harper and Clark respectively). Also, we know completely the list of *principal* integer rings for *imaginary* quadratic fields, adding

$$-19, -43, -67, -163,$$

to the previous list and we know that when $d \to -\infty$ then the class number h_K goes to infinity (Heilbronn), while for *real* quadratic fields this is widely open, and there is a conjecture of Gauss that $\mathcal{O}_K$ will be principal for an infinite number of real quadratic field (actually $\sim 75,4\%$ of them).

Exercise 7 (Maximal order in some matrix rings)**.** Let $R = \mathbb{Z}$ or $\mathbb{Z}_p$ (or a principal ring) and $K = \mathrm{Frac}(R)$, and consider $M_n(K)$. Show that conjugate (under $\mathrm{GL}_n(K)$) of $M_n(R)$ are maximal orders and that all maximal orders are of this form.

Hint : use the trace pairing $\mathrm{tr} : M_n(K) \times M_n(K) \longrightarrow K$ *and* $M^* = \{m \in M_n(K)| \ \mathrm{tr}(mM) \subset R\}$ *to prove that $M_n(R)^* = M_n(R)$, which is thus maximal. In the other direction, consider $M := \mathcal{O} \cdot R^n \subset K^n$ for some maximal order $\mathcal{O} \subset M_n(K)$, as a R-module. Use the structure theorem for finite type module over a principal ring to conclude.*