Théorie des nombres - TD3

Exercise 1. Let k be a field, and choose a separable closure of k, k^{sep}. Let $G_k = \mathrm{Gal}(k^{sep}/k)$ the Galois group of k with its topology. Show that if V is a $\mathbb{C}$-vector space, then any continuous map

$$G_k \longrightarrow \mathrm{GL}(V),$$

has finite image (i.e. factors through the Galois group $\mathrm{Gal}(L/k)$ of a finite extension L/k).

Exercise 2.

1. Let G be a topological group. Denote $[G, G]$ the closure of the commutator subgroup and $G^{ab} = G/[G, G]$ with its quotient topology. Show that any continous $\phi : G \longrightarrow A^\times$ with A an Hausdorff commutative topological ring [1] factors through G^{ab}.
2. Let k be a field and k^{sep} a fixed separable closure. Let k^{ab} the largest abelian (Galois) extension of k in k^{sep} : show that k^{ab} exists, is a Galois extension and $G_k^{ab} = \mathrm{Gal}(k^{ab}/k)$.
3. Show that a finite index subgroup of a (infinite) Galois group is not necessarily closed *Hint : Consider the extension of* $\mathbb{Q}$ *given by* $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$*, find its Galois group and consider a well chosen quotient of it.*

Exercise 3.

1. Show that if A is a finite dimensional k-algebra, and R a noetherian integral domain with $\mathrm{Frac}(R) = k$, then any sub-R-algebra of finite type of A is contained in an (R-)order. *Hint : Show that if* M *is a full-*R*-lattice in* A*, then* $\mathcal{O}_l(M) = \{x \in A | xM \subset M\}$ *is a left-order. Then if* B *is a sub-*R*-algebra of finite type, show that* B *is included in a full-*R*-lattice*
2. Show that if A/k is simple, and $\mathrm{char}\, k = 0$, then the reduced trace trd is non degenerate. *Hint : If* $K = Z(A)$*, then show that* $\mathrm{tr}_{A/k} = \mathrm{tr}_{K/k} \circ \mathrm{tr}_{A/K}$*.Then try to reduce to a matrix algebra.*

Exercise 4. Let $\mathbb{Q}(\sqrt{d})$, with d without square factors.

1. Show that $\mathbb{Z}[\sqrt{d}]$ is a maximal order if and only if $d \not\equiv 1 \pmod 4$. What is the maximal order if $d \equiv 1 \pmod 4$? *Hint : What are the trace and norm of an integral element ?*
2. Show that $\mathbb{Z}[i\sqrt{3}]$ is not UFD (factoriel, en français), but $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ is. Show that $\mathbb{Z}[i\sqrt{5}]$ is not UFD.

Exercise 5. We want to show that the ring of integers of $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$ is not of the form $\mathbb{Z}[\alpha]$.

1. Show that $K/\mathbb{Q}$ is Galois with group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
2. Let

$$\alpha_1 = (1 + \sqrt{7})(1 + \sqrt{10})$$
$$\alpha_2 = (1 - \sqrt{7})(1 + \sqrt{10})$$
$$\alpha_3 = (1 + \sqrt{7})(1 - \sqrt{10})$$
$$\alpha_4 = (1 - \sqrt{7})(1 - \sqrt{10})$$

Show that $3 | \alpha_i\alpha_j$ for $i \neq j$ but that $3 \nmid \alpha_i^n$ for any power n. *Hint : Look at the trace mod 3 !*

1. or an abelian topological group H such that 0_H is closed

3. Suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α, whose minimal polynomial is $f \in \mathbb{Z}[X]$. Show that for any polynomial $g \in \mathbb{Z}[X]$, $3|\ g(\alpha)$ if and only if $\overline{f}|\ \overline{g}$ in $\mathbb{F}_3[X]$.
4. Deduce that $\overline{f}$ has 4 distincts irreducible factors over $\mathbb{F}_3$. *Hint : Look at* $\alpha_i = f_i(\alpha), f_i \in \mathbb{Z}[X]$ *then show that* $\overline{f}|\overline{f}_i\overline{f}_j$
5. What is the degree of f ? Conclude !

Exercise 6. Let $G = \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ be a finite group. Let $A = \mathbb{Q}[G]$, it is a finite dimensional $\mathbb{Q}$-algebra. Show that as a $\mathbb{Q}[G]$-algebra (by left multiplication), $\mathbb{Q}[G]$ is semi-simple but not simple.

Exercise 7 (Jacobi's Formula)**.** $\mathbb{H} = (-1,-1)_{\mathbb{Q}}$ be the *Hurwitz quaternions*, and denote N the reduced norm.

1. Where is $\mathbb{H}$ ramified (i.e. for which places v – primes p corresponding to $\mathbb{Q}_p$, or ∞ corresponding to $\mathbb{Q}_\infty = \mathbb{R}$– is $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}_v$ nonsplit) ? *Hint : Use the previous exercice on the non-finite-typeness (?) of the Brauer group to prove that it is split at* $p \neq 2$*.Try to use a similar argument congruence argument to show that it is ramified at* $p = 2$
2. Let $\mathcal{O}' = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$. Show that $\mathcal{O}'$ is an order. Is it maximal ?
3. Show that $\mathcal{O} = \{x + yi + zj + tk | x, y, z, t \in \mathbb{Z} \text{ or } x, y, z, t \in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}\}$ is a maximal order containing $\mathcal{O}'$. *Hint : Again, (reduced) traces and norms are usefull here*
4. What are the units of $\mathcal{O}$, i.e. $\mathcal{O}^\times$?
5. Show that $\mathcal{O}$ has class number 1 (i.e. $C\ell(\mathcal{O}) = \{\mathcal{O}\}$). *Hint : prove that there is some kind of euclidean division on* $\mathcal{O}$ *with respect to the reduced norm*
6. Denote $\tau = \frac{1+i+j+k}{2}$. Show that $(1+i)\mathcal{O}$ is two-sided and
$$\mathcal{O}/(1+i)\mathcal{O} \xrightarrow{\sim} \mathbb{F}_2[\overline{\tau}] \simeq \mathbb{F}_4,$$
is an isomorphism, which sends $\mathcal{O}'$ to $\mathbb{F}_2$.
7. Show that for p odd, we have the following equalities,
$$|\{\, x \in \mathcal{O} |\ N(x) = p\}\,| = 3\,|\,\{x \in \mathcal{O}' |\ N(x) = p\}| = 3|\{(a, b, c, d) \in \mathbb{Z}^4 |\ a^2+b^2+c^2+d^2 = p\}|,$$
and that $N(x) = p$ if and only if $x\mathcal{O}$ has index p^2 in $\mathcal{O}$.
8. Show that if p is odd $\mathcal{O}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p = M_2(\mathbb{Z}_p)$, and that $\mathcal{O}_p$ has $p+1$ index p^2 ideals. *Hint : we can show that there are bijections, writing* $\mathcal{O}_p \simeq (\mathbb{Z}_p^2 \oplus \mathbb{Z}_p^2)$ *as a left* $\mathcal{O}_p$*-module,* $\{I \subset \mathcal{O}_p \text{ of index } p^2\} \simeq \{L \subset \mathbb{Z}_p \oplus \mathbb{Z}_p \text{ sub-}\mathbb{Z}_p\text{-module of index } p\} \simeq \{\ell \subset \mathbb{F}_p \oplus \mathbb{F}_p \text{ a line}\}$.
9. Show that $\Lambda \subset \mathbb{H} \mapsto (\Lambda \otimes \mathbb{Z}_p)_p$ induces an index-preserving bijection between lattices of $\mathbb{H}$ and collection (L_p) of lattices of $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ such that $L_p = \mathcal{O}_p$ for almost all p. Furthermore Λ is an order, a maximal order, or an ideal for $\mathcal{O}$ if and only if Λ_p has this property for all p.
10. Deduce the following theorem of Jacobi

    Theorem 0.1 (Jacobi)**.** *Let* p *be an odd prime. Then*
$$|\{(a, b, c, d) \in \mathbb{Z}^4 |\ a^2 + b^2 + c^2 + d^2 = p\}| = 8(p + 1).$$
11. Deduce Lagrange's Theorem : every integer is a sum of 4 squares.

Remark 0.2. Actually there is a more general version of Jacobi's formula for sum's of 4 squares, for every integer $n \in \mathbb{N}\backslash\ \{0\}$,
$$\{(a, b, c, d) \in \mathbb{Z}^4 |\ a^2 + b^2 + c^2 + d^2 = n\} = 8 \sum_{d|n, 4\nmid d} d.$$

It is best proven using modular forms (precisely of weight 2 and level $\Gamma_0(4)$), and the same method (only easier) gives the formula for sums of $2k$ squares, $k \geq 2$. See the lecture of Zagier in the book *The 1-2-3 of Modular Forms.*