ENS de Lyon — Master 1 – Introduction à la Théorie des Nombres

TD1 — 2020-2021

Number fields, traces, norms and diophantine equations

Exercise 1. [Trace and norm] Let L/K be a finite extension of fields. If $x \in L$, recall its *relative* trace $\mathrm{Tr}_{L/K}(x)$ and norm $N_{L/K}(x)$ are defined as the trace and the determinant of the K-linear map $y \mapsto xy$ from L to L.

1. Show that the trace map is K-linear from L to K, and the norm map is a group homomorphism from $L^\times$ to $K^\times$. Compute $\mathrm{Tr}_{L/K}(x)$ and $N_{L/K}(x)$ when $x \in K$.
2. Show that if M/L is a finite field extension, then for every $x \in M$,
$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)) = \mathrm{Tr}_{M/K}(x)$$
and
$$N_{L/K}(N_{M/L}(x)) = N_{M/K}(x).$$
3. Assume L/K is separable, and let $x \in L$ be of degree n over K. Let $x = x_1, \dots, x_n$ be the conjugates of x over K. Show that
$$\mathrm{Tr}_{L/K}(x) = \frac{[L:K]}{n} \sum_{i=1}^n x_i$$
and
$$N_{L/K}(x) = \left(\prod_{i=1}^n x_i \right)^{\frac{[L:K]}{n}}.$$
4. If $L = K(x)$ with x algebraic separable over K, provide another interpretation of $\mathrm{Tr}_{L/K}(x)$ and $N_{L/K}(x)$ in terms of the minimal polynomial of x over K.
5. Assume L is a number field, *i.e.* a finite extension of $\mathbb{Q}$. Let $\mathcal{O}_K$ be the set of algebraic integers in K (that is element of K integral over $\mathbb{Z}$). Show that if $x \in \mathcal{O}_L$, then $\mathrm{Tr}_{L/K}(x) \in \mathcal{O}_K$ and $N_{L/K}(x) \in \mathcal{O}_K$.

Exercise 2. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

1. Find $\alpha \in \mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$.
2. Compute the image of α in every embedding $K \hookrightarrow \mathbb{C}$. What are their traces and norms (over $\mathbb{Q}$) ?

Exercise 3. Let $K/\mathbb{Q}$ be a finite extension. Show that $\alpha \in \mathcal{O}_K$ is invertible if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. What can we say about α if $N_{K/\mathbb{Q}}(\alpha)$ is a prime number ?

Exercise 4. [Quadratic fields] Let d be a square-free integers, with $d \neq 0, 1$.

1. Let $a, b \in \mathbb{Q}$. Compute the trace, the norm, and the minimal polynomial of $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. (*Get used to the notation* $\mathbb{Q}(\sqrt{-1})$ *!*)
2. Show that the ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$ when $d \equiv 2, 3 \bmod 4$ and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ when $d \equiv 1 \bmod 4$.
3. Compute $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}$ when $d < 0$. What happens when $d > 0$?
4. Show that $\mathbb{Z}[i]$ is an euclidean domain with respect to its norm, and describe its irreducible elements.
5. Show that $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ is not factorial.
6. Show that any degree 2 extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{d})$. Show that if d' is another square-free integer with $d' \neq 0, 1, d$ then $\mathbb{Q}(\sqrt{d}) \not\simeq \mathbb{Q}(\sqrt{d'})$.

Exercise 5. [Pythagorean triples] We wish to find every triple of integers (x, y, z) such that $x^2 + y^2 = z^2$.

1. Show that we can assume $xyz \neq 0$, x, y and z positive and $\gcd(x, y, z) = 1$. We will call such a triple a *primitive* Pythagorean triple.
2. Let (x, y, z) be a primitive Pythagorean triple. Show that x or y is even.

3. Without loss of generality, assume x is even. Show that $\left(\frac{x}{2}\right)^2 = ab$ where a and b are positive and coprime integers.
4. Show that a and b are squares of integers, and conclude.

Exercise 6. [An example of Bachet-Mordell equation] We wish to solve in $\mathbb{Z}^2$ the equation $y^2 = x^3 - 1$. Assume (x, y) is a solution.

1. Show that $\gcd(y + i, y - i) = 1$ in $\mathbb{Z}[i]$.
2. Prove that $y + i$ and $y - i$ are both cubes in $\mathbb{Z}[i]$.
3. Conclude.

Exercise 7. [First attempt at Fermat's last theorem] We wish to prove that, for $n \geq 3$, the equation $(F)_n : x^n + y^n = z^n$ has no solution $(x, y, z) \in \mathbb{Z}^3$ such that $xyz \neq 0$ (but we won't actually do it).

1. Show that it suffices to prove that $(F)_4$ and $(F)_p$ admit no non-trivial solution in $\mathbb{Z}$, for every odd prime number p.
2. By using Exercise 5, show that $x^4 + y^4 = z^2$ admit no non-trivial solution in $\mathbb{Z}$. *Hint : Assume there is such a solution with $|z|$ minimal, and use the Pythagorean triple formula to build a solution with a smaller right-hand side.*
3. Let p be an odd prime number and ζ_p a primitive p^{th} root of unity in $\mathbb{C}$. Show that for any $x, y \in \mathbb{C}$, $x^p + y^p = \prod_{k=0}^{p-1}(x + \zeta_p^k y)$.
4. In this question, assume $\mathbb{Z}[\zeta_p]$ is factorial and p is prime to xyz. Assume (x, y, z) is a non-trivial solution of $(F)_p$ in $\mathbb{Z}$. Prove that the $x + \zeta_p^k y$ are pairwise coprime. Deduce that $x + \zeta_p y$ is (associated with) a p^{th} power.

   Remark. With some additional knowledge of $\mathbb{Z}[\zeta_p]$ we can deduce a contradiction...