Théorie des Nombres TD3

M2 AAG 2021-2022

Warm-up

1. Show that the integer ring of $\mathbb{Q}(i)$ is principal. Deduce that the class number is one.

2. Show that there are integral elements in $\mathbb{Q}(i\sqrt{7})$ which are not in $\mathbb{Z}[i\sqrt{7}]$. Show that $\mathbb{Q}(i\sqrt{7})$ has class number one.

3. Show that $\mathbb{Q}(\sqrt{2})$ has class number one.

Exercises

Exercice 1 (Quadratic extensions). Let $\mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{N}_{>0}$ without square factors.

1. Show that $\mathbb{Z}[\sqrt{d}]$ is the ring of integer of $\mathbb{Q}(\sqrt{d})$ if and only if $d \not\equiv 1 \pmod 4$. What is the integer ring 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.

3. Calculate the discriminant of $\mathbb{Q}(\sqrt{d})$.

4. Show that a prime $p \in \mathbb{Z}$ is

$$\begin{cases} \text{inert if} & p \neq 2 \text{ and } p \text{ is not a square mod } d \text{ or } p = 2 \text{ and } d \equiv 5 \pmod 8 \\ \text{split if} & p \neq 2 \text{ and } p \text{ is a square mod } d \text{ or } p = 2 \text{ and } d \equiv 1 \pmod 8 \\ \text{ramified if} & p | d \text{ or } p = 2 \text{ and } \ d \not\equiv 1 \pmod 4. \end{cases}$$

in $\mathbb{Q}(\sqrt{d})$. ***Hint :** We can use the result of the next exercice.*

Exercice 2. We will prove the following theorem

Theorem 1 (Dirichlet). *Let A a Dedekind ring, with fraction field K and L/K a finite extension and B the integral closure of A in L. Assume $B = A[\alpha]$ for α with minimal polynomial P. Let $\mathfrak{p}$ be a prime ideal of A, and assume*

$$P \pmod{\mathfrak{p}} \equiv \prod_{i=1}^{r} P_i^{e_i} \pmod{\mathfrak{p}}.$$

where $P_i \pmod{\mathfrak{p}}$ *is irreducible. Then*

$$\mathfrak{q}_i = \mathfrak{p} + P_i(\alpha)\mathcal{O}_L,$$

is a maximal ideal of B *and* $\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$.

1. Show that the maximal ideal of B containing $\mathfrak{p}$ are in bijection with maximal ideals of $B/\mathfrak{p}B$.

2. Show that $\mathfrak{q}_i$ is maximal in B and doesn't depend on the choice of a lift of $P_i \pmod{\mathfrak{p}}$.

3. Conclude.

4. Extend this result when $K = \mathbb{Q}$, $L = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_L$ and $p \nmid [\mathcal{O}_L : \mathbb{Z}[\alpha]]$ (for p prime).

5. Find the prime decomposition of 2,3,5,7 in $\mathbb{Q}(\sqrt{10})$.

6. Let α a root of $x^3 - x - 1$. Find the decomposition of $5, 13, 59$ in $\mathbb{Q}(\alpha)$.

7. Find the decomposition of $3, 5, 7$ in $\mathbb{Q}[\sqrt[4]{2}]$.

Exercice 3. 1. Let K be a field, θ algebraic and separable over K, with polynomial P of degree n, and $L = K(\theta)$. Show that the discriminant of $(x, y) \mapsto \mathrm{tr}_{L/K}(xy)$ (in the basis $\theta^k, k = \{0, \dots, n-1\}$) is

$$(-1)^{\frac{n(n-1)}{2}} N_{L/K} P'(\theta).$$

2. Deduce the discriminant of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, for an odd prime, and primes that ramifies in $\mathbb{Q}(\zeta_p)$.

3. What is the discriminant of $\mathbb{Q}(\theta)$ for θ a root of $X^3 + 2X + 1$? Deduce that $\mathcal{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$.

4. (More difficult) What is the discriminant of $\mathbb{Q}(\sqrt[3]{7})$? Prove that $\mathbb{Z}(\sqrt[3]{7}) = \mathcal{O}_{\mathbb{Q}(\sqrt[3]{7})}$. *To calculate* $\mathcal{O}_{\mathbb{Q}\sqrt[3]{7}}$ *we can show that both ring are equal away from* 21*, and localise at* 3 *and* 7 *to reduce to show the equality for some extension of* $\mathbb{Q}_3, \mathbb{Q}_7$ *where we can prove the result for the quotient ring mod* $3, 7$ *and using Nakayama's lemma. There will be a follow up to this exercice where we will calculate the class group of* $\mathbb{Q}(\sqrt[3]{7})$*!*

Exercice 4. We want to prove that $\mathbb{Q}[i, \sqrt{5}]/\mathbb{Q}(i\sqrt{5})$ is unramified everywhere. We will consider the following extensions

$$\begin{tikzcd}
 & \mathbb{Q}(i,\sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash] & \mathbb{Q}(i\sqrt{5}) \arrow[d, dash] & \mathbb{Q}(i) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

1. What are the ramified primes in the three quadratic extensions of $\mathbb{Q}$?

2. Prove that if $M/L/K$ is a tower of extensions of number fields (or local fields), and $\mathfrak{P} \mid \mathfrak{p}|p$ are primes in these extensions, then $e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|p)$.

3. Deduce that the maximum ramification index in $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}$ is 2.

4. Now fix a ramified prime $\mathfrak{P}$ for $L = \mathbb{Q}(i,\sqrt{5})$ over $\mathbb{Q}$, let $G_{\mathfrak{P}} \subset \mathrm{Gal}(L/\mathbb{Q})$ be the associated decomposition subgroup, and H the subgroup acting trivially on $\mathcal{O}_L/\mathfrak{P}$. Show that H is of index 2 in $\mathrm{Gal}(L/\mathbb{Q})$, and if K is the corresponding quadratic extension, $\mathfrak{P}$ ramifies for L/K.

5. Prove that $L/\mathbb{Q}(i\sqrt{-5})$ is everywhere unramified. *Hint : otherwise choose $\mathfrak{P}$ so that $K = \mathbb{Q}(i\sqrt{5})$ in the previous question. If $\mathfrak{P}|p$, then show that there is only one prime, which ramifies, above p in the other two quadratic extensions by letting H act on them.*

6. Alternatively, use discriminant and different to reprove this result !

Exercice 5 (The different ideal). Let A be a Dedekind ring, K its fraction field, and L/K be a separable extension and denote B the integral closure of A in L.

1. If $B = A[\alpha]$ with f a minimal polynomial for α of degree n, show that the different ideal $\mathcal{D}_{B/A} = (f'(\alpha))$. *Hint : Show that for all $0 \leqslant r \leqslant n-1$ $X^r = \sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)}$, where α_i are the conjugate of α.*

2. Calculate the different of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

3. Assume that L/K is a totally ramified extension of local fields of degree e. Show that $v(\mathcal{D}_{L/K}) \geqslant e-1$ with equality if and only if L/K is (totally) tamely ramified (i.e. $p \nmid e = n$).

4. Assume that L/K is an extension of local rings such that the extension of residue fields is separable. Show that $\mathcal{D}_{L/K} = \mathcal{O}_L$ if and only if L/K is unramified.

5. Let L/K be an extension of number field. Show that a prime ideal of $\mathcal{O}_K$ $\mathfrak{P}$ is ramified above K iff $\mathfrak{P}|\ \mathcal{D}_{L/K}$. Deduce that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ ramifies in $\mathcal{O}_K$ iff $\mathfrak{p}|\mathfrak{d}_{L/K} := N_{L/K}(\mathcal{D}_{L/K})$.