Théorie des Nombres TD1 - Ring of integers

M2 AAG 2026-2027

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.
4. Show that a Dedekind ring which is UFD is principal.

Exercice 1. 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

$$\mathfrak{q}_i = \mathfrak{p}B + P_i(\alpha)B,$$

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

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 2 (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 surjective map of A-module $f : M \twoheadrightarrow N$, and every $g : P \to N$, there is a $h : P \to M$ such that $g = f \circ h$[1]. Let A be a Dedekind ring.

1. Show that a fractional ideal $\mathfrak{a}$ 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,

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

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.*

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 $\mathfrak{a}_1 \dots \mathfrak{a}_n = \mathfrak{b}_1 \dots \mathfrak{b}_n \in C\ell(A)$. *Hint : Show that* $\det(\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n) := \bigwedge^n (\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n) \simeq \mathfrak{a}_1 \dots \mathfrak{a}_n$

5. By the morphism $M = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n \mapsto (n, \mathfrak{a}_1 \dots \mathfrak{a}_n)$, to what is sent $M \oplus N$?

Exercice 3. Show that if A is a Dedekind ring, any ideal of A is generated by at most 2 elements.

Exercice 4 (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 $\mathbb{Q}(\sqrt{d})$.

[1]Equivalently (why?) P is a direct factor in a free of finite rank A-module

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

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

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

Exercice 5. 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. Let p be an odd prime and $n \geqslant 1$. Deduce the discriminant of $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$, that the integer ring $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^n}]$, and primes that ramifies in $\mathbb{Q}(\zeta_{p^n})$.

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 6. 1. Let L, L', K three number fields. Assume L/K and L'/K are finite, Galois, extensions of degree n, n' respectively such that $L \cap L' = K$. Let w_i,w'_i respective integral basis with respect to K, with respective discriminant $d, d' \in \mathcal{O}_K$. Assume that d, d' are relatively prime in the sense that

$$ud + vd' = 1,$$

for some $u, v \in \mathcal{O}_K$. Prove that $w_i w'_j$ is an integral basis of LL'/K with discriminant $d^{n'} d'^{n}$.

2. Show that the integer ring of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.

Exercice 7 (Quadratic reciprocity). Fix a prime $p \neq 2$. We denote $K = \mathbb{Q}(\zeta_p)$, and we recall that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ and $d_K = (-1)^{p-1} p^{p-2}$.

1. Let $n \in \mathbb{N}_{>1}$ and ℓ a prime, $\ell \nmid n$. Show that the Frobenius isomorphism $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}/n\mathbb{Z}^\times$ is given by the class of ℓ.

2. Deduce that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}^\times$.

3. Denote $p^* = (-1)^{\frac{p-1}{2}} p$. Show that there is a unique quadratic extension in $K = \mathbb{Q}(\zeta_p)$ and that it is $\mathbb{Q}(\sqrt{p^*})$.

4. Let p, q distincts odd prime numbers. Show that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. ***Hint : Have a look at ramified primes*** q ***in*** $\mathbb{Q}(\zeta_p)$ ***and*** $\mathbb{Q}(\sqrt{p^*})$.

5. Show that moreover $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

We recall the following result, which is a theorem of Minkowski giving a bound to effectively compute class groups.

Theorem 2 (Minkowski). ***Let*** $K/\mathbb{Q}$ ***be a number field,*** $n = [K : \mathbb{Q}]$ ***and*** $\alpha \in Cl(K)$. ***Then there exists an ideal*** I ***of*** $\mathcal{O}_K$ ***with class*** α ***such that***

$$N_{K/\mathbb{Q}}(I) \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}.$$

Exercice 8 (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.

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 $h_K := |C\ell(\mathcal{O}_K)| = 1$.

Exercice 9. Compute the class group of $\mathbb{Z}[\sqrt[3]{7}]$.

Exercice 10. 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
$$\begin{aligned}\alpha_1 &= (1+\sqrt{7})(1+\sqrt{10})\\ \alpha_2 &= (1-\sqrt{7})(1+\sqrt{10})\\ \alpha_3 &= (1+\sqrt{7})(1-\sqrt{10})\\ \alpha_4 &= (1-\sqrt{7})(1-\sqrt{10})\end{aligned}$$
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 !***

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 !

Exercice 11 (Steinitz' class). Let L/K be a degree d extension of number fields.

1. Justify that as $\mathcal{O}_K$-module, there exists an ideal I of $\mathcal{O}_K$ such that

$$\mathcal{O}_L \simeq \mathcal{O}_K^{d-1} \oplus I,$$

and that the class of I, $[I] \in C\ell(K)$ is well defined.

We call the class $[I] \in C\ell(K)$ ***the Steinitz' class of*** L/K.

Let $d \geqslant 2$ without square factors, and $p \equiv 3 \pmod 4$ not dividing d. Set $K = \mathbb{Q}(i\sqrt{dp})$ and $L = \mathbb{Q}(i\sqrt{p}, i\sqrt{dp})$. Denote $1 \neq \sigma \in \mathrm{Gal}(L/K)$. We assume that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module and set e_1, e_2 be an $\mathcal{O}_K$ basis.

2. Show that there exists a matrix $\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} \in M_2(\mathcal{O}_K)$ such that

$$\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} \begin{pmatrix} e_1 & \sigma(e_1) \\ e_2 & \sigma(e_2) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{1+i\sqrt{p}}{2} & \frac{1-i\sqrt{p}}{2} \end{pmatrix}.$$

We denote by x, y, z the respective determinants of the matrices above.

3. Compute $N_{K/\mathbb{Q}}(x)^2 N_{L/\mathbb{Q}}(y)$.

4. Show that the norm of an element of $\mathcal{O}_K$ can never be equal to p.

5. Deduce that $(1, \frac{1+i\sqrt{p}}{2})$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

6. Write $\sqrt{d}, \sigma(\sqrt{d})$ in this basis and get a contradiction.

7. Deduce that the integer ring of $\mathbb{Q}(\sqrt{-6}, \sqrt{-3})$ is not a free module over the integer ring of $\mathbb{Q}(\sqrt{-6})$, but that it is free over the one of $\mathbb{Q}(\sqrt{2})$. Compute the Steinitz class of $\mathbb{Q}(\sqrt{-6}, \sqrt{-3})/\mathbb{Q}(\sqrt{-6})$.

Exercice 12. The goal is to show the following theorem, due to Dedekind under the name *Dedekind index theorem.*

Theorem 3 (Dedekind). *Let $K = \mathbb{Q}(\alpha)$ where $\alpha \in \mathcal{O}_K$ with minimal monic polynomial $P(T) \in \mathbb{Z}[T]$ and let p be a prime. Denote*

$$P \pmod p = \overline{\pi_1}^{e_1} \dots \overline{\pi_g}^{e_g} \in \mathbb{F}_p[T],$$

the prime decomposition of $P(T) \pmod p$ and choose (monic) lifts $\pi_i(T) \in \mathbb{Z}[T]$ of $\overline{\pi_i}(T)$. Let $F(T) \in \mathbb{Z}[T]$ defined by

$$P = \pi_1^{e_1} \dots \pi_g^{e_g} + pF.$$

Then $p| \ [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ if, and only if, there exists j such that $e_j \geqslant 2$ and $\overline{\pi}_j| \ (F \pmod p)$.

We first assume $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. We denote $\mathfrak{p}_j = (p, \pi_j(\alpha))$ the primes above p.

1. Let j such that $\overline{\pi}_j | F \pmod p$. Show that $\mathfrak{p}_j | \ F(\alpha)$.

2. Prove the following equality of ideals
$$(\pi_1(\alpha))^{e_1} \dots (\pi_g(\alpha))^{e_g} = (p)(F(\alpha)).$$
3. Show that $\mathfrak{p}_j | \ (\pi_j(\alpha))$ but that, if $e_j \geqslant 2$, $\mathfrak{p}_j^2 \nmid (\pi_j(\alpha))$.
4. Show that $\mathfrak{p}_i \nmid \pi_j(\alpha)$ if $i \neq j$.
5. Deduce that if $e_j \geqslant 2$ then $\mathfrak{p}_j \nmid (F(\alpha))$. Conclude.

We now assume $p|[\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

6. Show that there exists $\beta \in \mathcal{O}_K$ not in $\mathbb{Z}[\alpha]$ such that $p\beta \in \mathbb{Z}[\alpha]$. We write $p\beta = c_0 + \ c_1\alpha + \dots + c_{n-1}\alpha^{n-1}$, $c_i \in \mathbb{Z}$.
7. Let $\overline{A}(T) = \gcd(\overline{c_0} + \ \overline{c_1}T + \dots + \overline{c_{n-1}}T^{n-1}, P \pmod p) \in \mathbb{F}_p[T]$. Show that $\overline{A}(T)$ is a proper factor of $P \pmod p$.

We write $P \pmod p = \overline{A}(T)\overline{B}(T)$ and choose A, B the monic lifts to $\mathbb{Z}[T]$ whose factors are among the π_j.

8. Show that $AB = P - pF$.
9. Show that $p| \ A(\alpha)$ in $\mathcal{O}_K$. We write $\alpha = p\alpha'$.
10. Using $\alpha' \in \mathcal{O}_K$, show that each factor of $\overline{B}$ also divides $\overline{A}$.
11. Let $\overline{\pi}_j$ be a factor of $\overline{B}$, show that $e_j \geqslant 2$ and $\overline{\pi}_j | \ (F \pmod p)$.
12. Application : let $K = \ \mathbb{Q}[\sqrt[3]{12}]$. Show that $\mathcal{O}_K \neq \mathbb{Z}[\sqrt[3]{12}]$ but that $3 \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{12}]]$ and deduce the factorisation of (3) in $\mathcal{O}_K$.
13. Application : let $P(T) = T^n + \ \sum_{i\geqslant 0}^{n-1} a_i T^i$ with $p| \ a_i$ for all i, for $n > 1$. Let α be a root of P and $K = \mathbb{Q}(\alpha)$. Show that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ if, and only if, P is an Eisenstein polynomial at p.

Remark 1. 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).