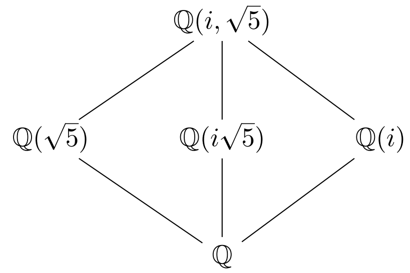
Théorie des nombres - TD5

Exercise 1. 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 $\mathbb{Z}(\sqrt[3]{7}) = \mathcal{O}_{\mathbb{Q}(\sqrt[3]{7})}$. If you are courageous find $C\ell(\mathbb{Z}(\sqrt[3]{7}))$. *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. For the class group calculation, in the end you should find $\mathbb{Z}/3\mathbb{Z}$. After classical reductions you should have 3 potential generators, so use the Norm and try to calculate product of ideals whose norm has a chance to be the norm of one element.*

Exercise 2. We want to prove that $\mathbb{Q}[i, \sqrt{5}]/\mathbb{Q}(i\sqrt{5})$ is unramified everywhere. We will consider the following extensions



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, 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 !

Exercise 3 (p-adic remarks)**.** 1. Show that for all $N \in \mathbb{N}_{>1}$, we have an isomorphism

$$\operatorname{proj\,lim}_{i \geqslant 0} \mathbb{Z}/N^i\mathbb{Z} \simeq \prod_{p|N} \mathbb{Z}_p.$$

2. Show that for all sequence $(u_n)_{n\in\mathbb{N}}$, $u_n \in \mathbb{Q}_p$ (or in $\mathbb{Q}$), $\sum_n u_n$ converges in $\mathbb{Q}_p$ if and only if $u_n \longrightarrow 0$ in $\mathbb{Q}_p$. Find an example of a sequence of rational whose sum converge in $\mathbb{Q}_p$ but not in $\mathbb{R}$.
3. Show that writing $x = \sum_i a_i p^i \in \mathbb{Q}_p$, with $a_i \in \{0, \ldots, p-1\}$ we have $x \in \mathbb{Q}$ if and only if the sequence $(a_i)_i$ is eventually periodic.
4. Show that there exists a continuous surjection $\mathbb{Z}_p \longrightarrow [0,1]$. Is there a continuous surjection $[0,1] \longrightarrow \mathbb{Z}_p$?