

Exercices - Feuille 3

Entiers cyclotomiques

Soit $n > 0$ un entier. On définit la fonction d'Euler $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, on sait que $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ si n_1 et n_2 sont premiers entre eux, et $\varphi(p^r) = p^{r-1}(p-1)$. Les polynômes cyclotomiques $\Phi_n(X) = \prod (X - \zeta^m) = \prod (X - \zeta')$, où ζ est une racine n -ième primitive de 1 et $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ et ζ' parcourt les racines n -ième primitives de 1. On a $\deg(\Phi_n) = \varphi(n)$. Le corps $K = \mathbb{Q}(\zeta)$ est le corps de décomposition de $X^n - 1$, il est une extension galoisienne de \mathbb{Q} de groupe G .

I. Le cas $n = p^r$

On va montrer que $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

1. Comme G permute les ζ' alors $\Phi_n \in \mathbb{Q}[X]$. Conclure que $[K : \mathbb{Q}] \leq \varphi(n)$. Montrer que $\Phi_n \in \mathbb{Z}[X]$. (Ça marche aussi pour n général.)
2. Montrer que $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$, alors $\Phi_{p^r}(1) = \Phi_p(1) = p$.
3. Soient ζ et ζ' des racines n -ième primitives de 1, montrer que $\frac{1-\zeta}{1-\zeta'}$ et $\frac{1-\zeta'}{1-\zeta}$ sont des unités de $\mathbb{Z}[\zeta]$ et de \mathcal{O}_K .
4. En utilisant 2 et 3, étudier la décomposition de l'idéal (p) dans \mathcal{O}_K et déduire :
 - $[K : \mathbb{Q}] = \varphi(p^r)$, $\Phi_{p^r}(X)$ est alors le polynôme minimal de ζ .
 - il n'y a qu'un idéal premier de \mathcal{O}_K au-dessus de p , il est engendré par $\pi = 1 - \zeta$, l'indice de ramification $e_{\pi/p} = \varphi(p^r)$.
 - l'extension de corps résiduel \mathcal{O}_K/π de \mathbb{F}_p est de degré 1, i.e. $\mathbb{Z}/(p) \rightarrow \mathcal{O}_K/(\pi)$ est un isomorphisme.
5. Montrer par récurrence que $\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi^m \mathcal{O}_K$ pour tout entier $m > 0$, en déduire que $\mathcal{O}_K = \mathbb{Z}[\zeta] + p^m \mathcal{O}_K$ pour tout entier $m > 0$.

Pour toute forme bilinéaire b sur un \mathbb{Z} -module libre de type fini M (par exemple $M = \mathcal{O}_K$ avec $b : (x, y) \mapsto \text{Tr}_{K/\mathbb{Q}}(xy)$), on peut définir le *discriminant* $\text{disc}(M/\mathbb{Z}) := \det(b(m_i, m_j)) \in \mathbb{Z}$ où m_i est une \mathbb{Z} -base de M . (c'est la même définition comme dans la feuille 2 à signe près, voir n'importe quel livre sur la théorie algébrique des nombres si vous êtes intéressés, on admet quelques faits et on continue à faire les exercices) On a montré dans la feuille 2 que $\text{disc}(\mathcal{O}_K/\mathbb{Z}) \cdot [\mathcal{O}_K : \mathbb{Z}[\zeta]]^2 = \text{disc}(\mathbb{Z}[\zeta]/\mathbb{Z})$ et on admet que ce sont $= \pm N_{K/\mathbb{Q}}(\Phi'_{p^r}(\zeta))$.

6. En calculant la norme, montrer que $\text{disc}(\mathcal{O}_K/\mathbb{Z})$ et $[\mathcal{O}_K : \mathbb{Z}[\zeta]]^2$ sont des puissances de p (à ± 1 près).
7. En déduire que $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Remarque. On voit, dans le cas ci-dessus, que p est ramifié lorsqu'il divise $\text{disc}(\mathcal{O}_K/\mathbb{Z})$. En fait, la réciproque est aussi vraie. De plus, pour tout corps de nombres K/\mathbb{Q} , le premier p est ramifié dans K si et seulement si $p \mid \text{disc}(\mathcal{O}_K/\mathbb{Z})$. En particulier, il n'y a qu'un nombre fini de tels p . Dans la suite, on admet cet énoncé sans preuve.

II. Le cas général

On va montrer par récurrence sur les nombres des facteurs premiers de n que

- $[K : \mathbb{Q}] = \varphi(n)$
- $\mathcal{O}_K = \mathbb{Z}[\zeta]$
- si un premier q est ramifié dans K alors q divise n

Soit ζ une racine n -ième primitive de 1. On écrit $n = p^r \cdot m$ avec p ne divise pas m . Alors $\zeta_m = \zeta^{p^r}$ est une racine m -ième primitive et $\zeta_{p^r} = \zeta^m$ est une racine p^r -ième primitive.

1. Montrer que $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_{p^r})$.

Par récurrence, supposons que $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$, que $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$ et que si q est ramifié dans $\mathbb{Q}(\zeta_m)$ alors $q|m$.

2. Étudier la factorisation de p dans $\mathbb{Q}(\zeta)$ et conclure que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

3. Admettre le lemme suivant sur les discriminants et déduire que $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ et que si q est ramifié dans $\mathbb{Q}(\zeta)$ alors $q|n$.

Lemme. Soient K et L des corps de nombres tels que $[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$. Notons $d = \text{pgcd}(\text{disc}(\mathcal{O}_K/\mathbb{Z}), \text{disc}(\mathcal{O}_L/\mathbb{Z}))$. Alors $d \cdot \mathcal{O}_{KL} \subset \mathcal{O}_K \cdot \mathcal{O}_L$. De plus, si $\mathcal{O}_{KL} = \mathcal{O}_K \cdot \mathcal{O}_L$, $\text{disc}(\mathcal{O}_{KL}/\mathbb{Z}) = \text{disc}(\mathcal{O}_K/\mathbb{Z})^{[L:\mathbb{Q}]} \cdot \text{disc}(\mathcal{O}_L/\mathbb{Z})^{[K:\mathbb{Q}]}$.

4. Soit ζ' (reps. ζ'') une racine n' -ième (reps. n'' -ième) primitive de 1. Admettons le fait que toute extension finie non-triviale K de \mathbb{Q} a un discriminant $\text{disc}(\mathcal{O}_K/\mathbb{Z}) \neq \pm 1$ (Minkowski). Montrer que $\mathbb{Q}(\zeta') \cap \mathbb{Q}(\zeta'') = \mathbb{Q}$ si n' et n'' sont premiers entre eux.

une référence (pour les discriminants) disponible sur l'internet : lecture notes de J. Milne sur sa page web.

III. Groupe de classes

Rappel. Soit K un corps de nombres de discriminant Δ_K , de degré $n = r_1 + 2r_2$. La constante (faible) de Minkowski est $c = (2/\pi)^{r_2} \sqrt{|\Delta_K|}$. Une telle constante nous permet de déduire la finitude du groupe de classes d'un corps de nombres. En fait, on obtiendra encore plus de informations sur les groupes de classes :

1. Montrer que le groupe de classes de $\mathbb{Q}(\sqrt{-1})$ est trivial, autrement-dit $\mathbb{Z}[\sqrt{-1}]$ est un anneau principal.
2. Étudier la factorisation de 2 dans le corps $K = \mathbb{Q}(\sqrt{2})$ et montrer que le groupe de classes de K est trivial, autrement-dit $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ est un anneau principal.
3. Montrer que la factorisation de l'idéal (2) de \mathcal{O}_K avec $K = \mathbb{Q}(\sqrt{-5})$ est $(2) = \mathfrak{p}^2$ où $\mathfrak{p} = (2, 1 + \sqrt{-5})$. Calculer la norme de \mathfrak{p} et montrer que ce n'est pas un idéal principal. Conclure que $Cl(K) = \mathbb{Z}/2\mathbb{Z}$.

Remarque. La constant de Minkowski $c = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$.