TD Bonus

Exercice 1. [Discriminant et ramification]

Soit A, B des anneaux commutatifs tels que $A \subset B$ et B est un A-module libre de type fini. Pour tout $b \in B$, on note $\mathrm{Tr}_{B/A}(b)$ la trace de la multiplication par b dans une base quelconque de B sur A, et pour une base $(b_1, \cdots, b_r)$ de B sur A, on note

$$\mathrm{disc}_{B/A}(b_1, \cdots, b_r) = \det(\mathrm{Tr}_{B/A}(b_i b_j))_{i,j}.$$

(a) Montrer que l'idéal $\mathrm{disc}(B/A) := \mathrm{disc}(b_1, \cdots, b_d)A$ de A est indépendant du choix de la base de B sur A.

(b) Montrer que si $B_1, \cdots, B_n$ sont des A-modules libres de type fini et $B = B_1 \times \cdots \times B_n$, alors

$$\mathrm{disc}(B/A) = \prod_{i=1}^{n} \mathrm{disc}(B_i/A).$$

(c) Montrer que si I est un idéal de A, alors B/IB est un A/I-module libre de type fini et que

$$\mathrm{disc}((B/IB)/(A/I)) = \mathrm{disc}(B/A)/I.$$

(d) Prouver que si B/A est une extension finie de corps de nombres ou de corps finis, $\mathrm{disc}(B/A) \neq (0)$.

(e) Montrer que si A est un corps et B une A-algèbre de dimension finie sur A, B est réduite (sans nilpotent non nul) si et seulement si c'est un produit de corps. En déduire que B est réduite si et seulement si $\mathrm{disc}(B/A) \neq (0)$.

(f) Montrer que pour tout corps de nombres K et tout nombre premier p, p est ramifié dans $\mathcal{O}_K$ si et seulement si p divise le discriminant de K.

Exercice 2. [Kronecker-Weber]

Dans ce problème, nous allons démontrer le théorème de Kronecker-Weber, à savoir que toute extension abélienne K de $\mathbb{Q}$ est incluse dans une extension cyclotomique.

(a) Montrer que le compositum de deux extensions abéliennes de $\mathbb{Q}$ est une extension abélienne, et que toute extension abélienne s'écrit comme produit d'extensions de degré de la forme p^m avec p premier. On peut donc supposer que $[K : \mathbb{Q}] = p^m$ avec p premier.

Pour L/K une extension finie galoisienne de corps de nombres, $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, on note $D(\mathfrak{P}/\mathfrak{p})$ le groupe de décomposition (formé des automorphisme de Galois fixant $\mathfrak{P}$)) et pour $n \in \mathbb{N}$

$$E_n(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma \equiv \mathrm{Id} \mod \mathfrak{P}^{n+1}\} \subset D(\mathfrak{P}/\mathfrak{p}).$$

(b) Montrer que les $E_n(\mathfrak{P}/\mathfrak{p})$ sont tous distingués dans $D(\mathfrak{P}/\mathfrak{p})$ et que leur intersection est triviale.

(*c*) Soit π une uniformisante de $\mathfrak{P}$ (dans $\mathcal{O}_{L,\mathfrak{P}}$). Montrer que pour tout $n \in \mathbb{N}$, si $\sigma \in E_n(\mathfrak{P}/\mathfrak{p})$, $\sigma(\pi)/\pi$ est une unité de $\mathcal{O}_{L,\mathfrak{P}}$ congrue à 1 modulo $\mathfrak{P}^n$. Réciproquement, pour $\sigma \in E_n(\mathfrak{P}/\mathfrak{p})$, montrer que si $\sigma(\pi)/\pi$ est congrue à 1 modulo $\mathfrak{P}^{n+1}$, alors $\sigma \in E_{n+1}(\mathfrak{P}/\mathfrak{p})$.

(*d*) En déduire pour tout $n \in \mathbb{N}^*$ une application injective ϕ_n de $E_n/E_{n+1}(\mathfrak{P}/\mathfrak{p})$ dans $(1+\mathfrak{P}^n\mathcal{O}_{L,\mathfrak{P}})/(1+\mathfrak{P}^{n+1}\mathcal{O}_{L,\mathfrak{P}})$ indépendante du choix de π.

(*e*) En déduire que $\mathfrak{P}/\mathfrak{p}$ est modérément ramifiée (i.e. $e(\mathfrak{P}/\mathfrak{p})$ est premier à p le nombre premier au-dessous de $\mathfrak{p}$) si et seulement si $E_n(\mathfrak{P}/\mathfrak{p})$ est nul pour tout $n > 0$.

(*f*) Montrer que si $D(\mathfrak{P}/\mathfrak{p})/E_1(\mathfrak{P}/\mathfrak{p})$ est abélien, alors $\sigma(\pi)/\pi$ appartient modulo $\mathfrak{P}$ à $(\mathcal{O}_K/\mathfrak{p})^*$ pour toute uniformisante π et tout $\sigma \in E_0(\mathfrak{P}/\mathfrak{p})$.

Supposons maintenant que l'extension $K/\mathbb{Q}$ est abélienne et que p est un nombre premier modérément ramifié dans K, soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_K$ au-dessus de p.

(*g*) Montrer que $E_0(\mathfrak{P}/\mathfrak{p})$ est isomorphe à un sous-groupe de $\mathbb{F}_p{}^*$.

(*h*) Soit e l'indice de ramification de p dans K et L l'unique sous-corps d'indice e de $\mathbb{Q}(\zeta_p)$. Montrer que p est totalement modérément ramifié dans L.

(*i*) Soit $\mathfrak{Q}$ un idéal premier de KL au-dessus de p et K' la sous-extension de KL fixée par le groupe d'inertie $E_0(\mathfrak{Q}/\mathfrak{P})$. Montrer que les nombres premiers non ramifiés dans K ne le sont pas non plus dans K', et que p est non ramifié dans K'.

(*j*) Montrer que $KL = K'L$, et en déduire qu'il suffit de démontrer le théorème de Kronecker-Weber pour K' au lieu de K.

(*k*) En déduire qu'il suffit de démontrer le théorème de Kronecker-Weber dans le cas où $[K : \mathbb{Q}] = p^m$ avec p premier, $\mathrm{Gal}(K/\mathbb{Q})$ cyclique, et p le seul nombre premier ramifié dans K.

(ℓ) En utilisant la théorie de Kummer, montrer que pour p impair, toute extension de $\mathbb{Q}$ de degré p telle que p est le seul nombre premier ramifié est incluse dans $\mathbb{Q}(\zeta_{p^2})$.

(*m*) Expliquer ce qui se passe pour $p = 2$.

(*n*) En déduire le cas général pour p^m, avec $m \geq 1$.