Feuille 4 : Ramification

Exercice 1 (Extensions cyclotomiques) On note $r \geq 1$, p premier, ζ une racine primitive p^r-ième de l'unité, $K = \mathbb{Q}[\zeta]$ et $\mathcal{O}_K$ son anneau d'entiers.

1. Montrer que K est une extension normale et que l'on a un morphisme injectif du groupe de Galois G_K vers le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/p^r$. Montrer également que $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$ et que $[\mathbb{Q}[\zeta] : \mathbb{Q}] \leq \varphi(p^r) = p^{r-1}(p-1)$.
2. On appelle *polynôme cyclotomique* Φ_{p^r} le polynôme $\prod_{\zeta \in \mu_{p^r}\,\text{primitive}}(X-\zeta)$. Montrer que
$$\Phi_{p^r} = \prod_{[i]\in(\mathbb{Z}/p^r\mathbb{Z})^\times} (X - \zeta^i) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1}.$$
3. Soit ξ une autre racine primitive p^r-ième de l'unité. Montrer que $\frac{1-\zeta}{1-\xi}$ est une unité de $\mathcal{O}_K$ (*i.e.* est inversible dans $\mathcal{O}_K$).
4. Soit $\pi = 1 - \zeta$. En calculant $\Phi_{p^r}(1)$, montrer l'égalité d'idéaux dans $\mathcal{O}_K$, $(p) = (\pi)^{\varphi(p^r)}$. En déduire que le corps $\mathbb{Q}[\zeta]$ est de degré $\varphi(p^r)$ sur $\mathbb{Q}$ et que l'élément π est premier dans $\mathcal{O}_K$. Quels sont les premiers ramifiés dans $K/\mathbb{Q}$? Donner le degré résiduel f et l'indice de ramification e.
5. Calculer la valeur absolue du discriminant $|\operatorname{disc}(\mathbb{Z}[\zeta] : \mathbb{Z})| = \operatorname{Nm}_{K/\mathbb{Q}}(\Phi'_{p^r}(\zeta))$ (on pourra commencer par $r = 1$ avant de traiter le cas général). En déduire que $\operatorname{disc}(\mathcal{O}_k/\mathbb{Z})$ est une puissance de p et que $p^M\mathcal{O}_K \subset \mathbb{Z}[\zeta]$ pour tout entier M suffisamment divisible.
6. Montrer que $\mathbb{Z}[\zeta] + \pi^m\mathcal{O}_K = \mathcal{O}_K$ pour $m \geq 1$. En déduire que l'anneau des entiers de $\mathbb{Q}[\zeta]$ est $\mathbb{Z}[\zeta]$ et que le discriminant de $\mathcal{O}_K$ sur $\mathbb{Z}$ est de valeur absolue $p^{p^{r-1}(pr-r-1)}$.
7. Soit $p \neq 2$. On définit le symbole quadratique pour $n \in \mathbb{Z}$, par 0 si $(n,p) \neq 1$; et si $(n,p) = 1$ on pose
$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ est un carré} \mod p \\ -1 & \text{sinon} \end{cases}$$
Soit ζ une racine primitive p-ième de l'unité et $S = \sum_{v=0}^{p-1}\left(\frac{v}{p}\right)\zeta^v$. Montrer que $S^2 = \left(\frac{-1}{p}\right)p$. En déduire que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique.

Exercice 2 (Norme numérique) Soient K un corps de nombres et $\mathcal{O}_K$ son anneau d'entiers. Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. L'indice de $\mathfrak{a}$ dans $\mathcal{O}_K$ est fini et on note la *norme numérique* N :
$$\mathrm{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}).$$
Pour tout idéal $\mathfrak{p}$ premier de $\mathcal{O}_K$ au dessus d'un premier p, on pose $N_{K/\mathbb{Q}}(\mathfrak{p}) := p^{f(\mathfrak{p}/p)}$. On prolonge ceci multiplicativement aux idéaux fractionnaires de $\mathcal{O}_K$.

1. Soit $\mathcal{O}_K$ l'anneau des entiers d'un corps de nombres K. Soit $\mathfrak{a}$ un idéal dans $\mathcal{O}_K$, montrer que $N_{K/\mathbb{Q}}(\mathfrak{a}) = \mathrm{N}(\mathfrak{a})$; en déduire $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$.

2. En déduire (*cf.* Samuel p.62) que pour tout entier $x \in \mathcal{O}_K$, on a $N_{K/\mathbb{Q}}(x) = \pm \mathrm{N}_{K/\mathbb{Q}}(x\mathcal{O}_K)\mathbb{Z}$.
3. Soient $\mathfrak{b} \subset \mathfrak{a}$ des idéaux fractionnaires de K. Montrer que $(\mathfrak{a} : \mathfrak{b}) = \mathrm{N}(\mathfrak{a}^{-1}\mathfrak{b})$.
4. Montrer que $\alpha \in K$ est une unité si et seulement si $\alpha \in \mathcal{O}_K$ et $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.
5. Soit $\alpha \in K$. Si $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, α est-il forcément une unité dans K ?

Exercice 3 (Borne de Minkowski et ramification) Soient K une extension de degré n de $\mathbb{Q}$, d_K le discriminant de $K/\mathbb{Q}$, $2s$ le nombre de plongements complexes non réels de K. On rappelle le résultat suivant appelé *borne de Minkowski* : il existe un ensemble de représentants du groupe des classes de K composé d'idéaux entiers $\mathfrak{a}$ de K tels que

$$\mathrm{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |d_K|^{1/2}$$

1. Trouver le nombre de classes des corps suivants : $K = \mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{-5}]$.
2. Soient $x = (11)^{1/3}$ et $K = \mathbb{Q}(x)$. Notons $\mathcal{O}_K$ l'anneau des entiers de K, U_K son groupe d'unités et C_K son groupe des classes d'idéaux.
   Montrer[1] que $\mathcal{O}_K = \mathbb{Z}[x]$. Montrer que C_K est engendré par au plus deux éléments (on pourra étudier la décomposition en premiers de $2\mathcal{O}_K, \ldots, 13\mathcal{O}_K$). En considérant l'idéal $\mathfrak{p}_2 = (2, x-1)$, montrer que $x^2 - 5$ est dans $\mathfrak{p}_2^2$ et de norme 4. En déduire que $|C_K| \leq 2$.
3. Montrer[2] qu'il n'existe pas d'extension non ramifiée de $\mathbb{Q}$.

Exercice 4 (Nombre de classes de $\mathbb{Q}[\zeta_{23}]$)

1. Décrire le groupe de Galois $\mathrm{Gal}(\mathbb{Q}[\zeta_{23}]/\mathbb{Q})$. En déduire l'unique extension quadratique K de $\mathbb{Q}$ contenue dans K.
2. On admet que le nombre de classes de K vaut 3. En déduire que le nombre de classes de $\mathbb{Q}[\zeta_{23}]$ est strictement supérieur à 1 (on pourra étudier l'idéal $2\mathcal{O}_K$).

Exercice 5 (Clôture algébrique de $\mathbb{Q}_p$) Notons $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$. Supposons par l'absurde que $\overline{\mathbb{Q}}_p$ est complet et posons $\alpha = \sum_{n=1}^{\infty} \zeta_{n'} p^n$ avec $n' = \begin{cases} n & \text{si } (n,p) = 1 \\ 1 & \text{sinon} \end{cases}$ où ζ_m est une racine primitive m-ieme de l'unité. Posons $K = \mathbb{Q}_p(\alpha)$.

1. Montrer que $\forall m \in \mathrm{N}$, $\zeta_{m'} \in \mathcal{O}_K$.
2. En déduire que $\overline{\mathbb{Q}}_p$ n'est pas complet.

[1] On rappelle le résultat suivant :

Théorème 0.1 Si A est un anneau de valuation discrète (DVR), d'idéal maximal $\mathfrak{p}$, de corps résiduel k ; si $f \in A[X]$ est de degré $n \geq 1$ et est d'Eisenstein pour $\mathfrak{p}$, alors, l'anneau $B := A[X]/(f)$ est DVR, d'idéal maximal engendré par x (image de X dans B), de corps résiduel k.

[2] Ceci n'est en général plus vrai pour des corps autres que $\mathbb{Q}$: c'est la notion de corps de classes de Hilbert.

Exercice 6 (Lemme de Krasner) Soit K un corps complet pour une valuation non-archimédienne. Soit α, β deux éléments d'une clôture algébrique $\overline{K}$ de K avec α séparable sur $K(\beta)$. On dit que α *appartient à* β si pour tout conjugé $\sigma\alpha \neq \alpha$ de α,

$$|\beta - \alpha| < |\sigma\alpha - \alpha|$$

(où $|\cdot|$ désigne l'unique extension de la valeur absolue de K).

1. Montrer que si α appartient à β alors $K(\alpha) \subset K(\beta)$.
2. Si $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, on pose $|f| := \max_{0 \leq i \leq n} |a_i|$. Soient f et g deux éléments de $K[X]$ unitaires, de même degré n. On suppose que f est irréductible sur K et séparable. Montrer que si $|f - g|$ est suffisamment petite, alors g est aussi irréductible. De plus dans ce cas, si α est une racine de f dans $\overline{K}$ montrer qu'il existe une racine β de g dans $\overline{K}$ telle que $K(\alpha) = K(\beta)$.

Exercice 7 (Extensions totalement ramifiées) Soit K un corps de caractéristique nulle, valué ultramétrique de valuation discrète, complet, d'anneau de valuation A, d'idéal maximal $\mathfrak{p}$, d'uniformisante π et de corps résiduel fini (ceci est notamment vérifiée par $\mathbb{Q}_p$). Montrer qu'il n'y a, à isomorphisme près, qu'un nombre fini d'extensions de K totalement ramifiées de degré fixé.

Exercice 8 (Applications de Krasner)

1. Soient $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$ et $\mathbb{C}_p$ la complétion de $\overline{\mathbb{Q}}_p$. Montrer que $\mathbb{C}_p$ est algébriquement clos.
2. Soit K une extension finie de $\mathbb{Q}_p$. Montrer qu'il existe une extension finie L de $\mathbb{Q}$ contenue dans K telle que $[L : \mathbb{Q}] = [K : \mathbb{Q}_p]$ et $L\mathbb{Q}_p = K$.

Exercice 9 (Polygone de Newton) Soit K un corps ultramétrique complet pour une valuation discrète. On étend sa valuation à la clôture algébrique de K : val :$\overline{K}^* \to \mathbb{Q}$. Pour

$$f(X) = \sum_{i=0}^{n} a_i X \quad a_i \in K \quad \text{et} \quad a_0 a_n \neq 0$$

on considère l'enveloppe convexe inférieure de l'ensemble des points $P_i := (i, \mathrm{val}(a_i))$ avec $i \in \{0, \ldots, n\}$, et on appelle *polygone de Newton de* f la chaine polygonale délimitant cette enveloppe convexe.

1. Comment est transformé le polygone de Newton quand on passe de f à $\frac{1}{a_n} f$?
2. (Cf. par exemple Neukirch *Algebraic Number Theory* p.145) Si le polygone de Newton de $f(X)$ a un segment de longueur n et de pente $-s$, montrer que f admet exactement n racines $\alpha_1, \ldots, \alpha_n \in \overline{K}$ telles que $\mathrm{val}(\alpha_i) = 0$ pour tout $i \in \{1, \ldots, n\}$.
3. Montrer que $f_i(X) := \prod_{\mathrm{val}(\alpha_i) = s_i} (X - \alpha_i)$ est à coefficients dans K.
4. Soit $K = \mathbb{Q}[\alpha]$ où α est une racine de $X^3 - X^2 - 2X - 8$. Montrer qu'il y a trois extensions de la valuations 2-adique dans K.