UNIVERSITÉ DE BORDEAUX
M1, Théorie des Nombres
2020-2021

## Feuille 7. Ramification

**Exercice 1.** Soit $A$ un anneau de Dedekind. On note $K$ son corps des fractions. Soit $K \subseteq F \subseteq L$ une tour d'extensions finies séparables. On note $B$ et $C$ les clôtures intégrales de $A$ dans $F$ et $L$ et on considère la tour $A \subseteq B \subseteq C$. Soient $\mathfrak{p} \subset A$, $\mathfrak{q} \subset B$ et $\mathfrak{P} \subset C$ des idéaux maximaux tels que $\mathfrak{p} \subseteq \mathfrak{q} \subseteq \mathfrak{P}$. Montrer que $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{q}) \cdot e(\mathfrak{q}/\mathfrak{p})$ et $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{q}) \cdot f(\mathfrak{q}/\mathfrak{p})$.

**Exemple.** Ramification dans les extensions $\mathbf{Q}[\sqrt{d}]$, $d \equiv 2, 3 \pmod 4$ (voir également le cours, Exemple 2.2.12).

Soit $d$ un entier sans facteur carré et tel que $d \equiv 2, 3 \pmod 4$. Soit $K = \mathbf{Q}[\sqrt{d}]$. On a $O_K = \mathbf{Z}[\sqrt{d}]$. Comme le polynôme minimal de $\sqrt{d}$ est $f(X) = X^2 - d$, on a

$$O_K \simeq \mathbf{Z}[X]/(X^2 - d).$$

Pour étudier la ramification des nombres premiers dans l'extension $K/\mathbf{Q}$ on remarque que par la Proposition 2.2.8 (ou 2.2.10) les décompositions possibles d'un nombre premier $p$ dans $O_K$ sont :

1) $pO_K = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$ ($p$ est décomposé dans $O_K$);

2) $pO_K = \mathfrak{p}$, ($p$ est inerte);

3) $pO_K = \mathfrak{p}^2$, ($p$ est ramifié dans $O_K$).

Le Théorème 2.2.11 donne la factorisation de $pO_K$ en termes de factorisation de la réduction $\bar{f}(X) \in \mathbf{F}_p[X]$ de $f(X)$ modulo $p$.

1) Supposons que $p$ ne divise pas $d$ et $p \neq 2$.

1a) Si le polynôme $\bar{f}(X) \in \mathbf{F}_p[X]$ a une racine dans $\mathbf{F}_p$, il se décompose en produit de deux facteurs distincts (à justifier):

$$\bar{f}(X) = (X - \bar{\alpha}_1)(X - \bar{\alpha}_2).$$

Alors $p$ est décomposé.

1b) Si $\bar{f}(X)$ n'a pas de racines dans $\mathbf{F}_p$, $p$ reste inerte.

2) Supposons que $p$ divise $d$. Alors $\bar{f}(X) = X^2$ et par le Théorème 3.2.11 $p$ est ramifié.

3) Supposons que $p = 2$. Si $d \equiv 2 \pmod 4$, on a $\bar{f}(X) = X^2$. Si $d \equiv 3 \pmod 4$, on a $\bar{f}(X) = X^2 + \bar{1} = (X + \bar{1})^2$. Dans les deux cas $p = 2$ est ramifié.

Remarquons que par le Théorème 2.2.14 un nombre premier $p$ est ramifié dans $K$ si et seulement si $p$ divise le discriminant $d_K = D_{O_K/\mathbf{Z}}$. On sait que $d_K = 4d$ si $d \equiv 2, 3 \pmod 4$.

Dans l'exercice suivant on étudie le cas $d \equiv 1 \pmod 4$.

**Exercice 2.** Soit $d$ un entier sans facteur carré et tel que $d \equiv 1 \pmod 4$. Soit $K = \mathbf{Q}[\sqrt{d}]$. Rappelons que $O_K = \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ et $d_K = d$.

1) Donner le polynôme minimal de $\frac{1+\sqrt{d}}{2}$ sur $\mathbf{Q}$.

2) Soit $p \neq 2$ un nombre premier. Supposons que $p \nmid d$. Montrer que $O_K/pO_K \simeq \mathbf{Z}[\sqrt{d}]/p\mathbf{Z}[\sqrt{d}]$. En déduire que $p$ est décomposé (respectivement reste inerte) dans $O_K$ si et seulement si $d$ est un carré (respectivement n'est pas un carré) modulo $p$.

3) Montrer que 2 est décomposé dans $O_K$ si $d \equiv 1 \pmod 8$ et que 2 est inerte si $d \equiv 5 \pmod 8$.

4) Montrer que $p$ est ramifié si et seulement si $p \mid d$.

**Exercice 3.** Soit $P(X) = X^3 - X + 1$.

1) Montrer que $P(X)$ est irréductible sur $\mathbf{Q}$ et possède une racine réelle $\alpha$ et deux racines complexes $\beta$ et $\bar{\beta}$.

On pose $K = \mathbf{Q}[\alpha]$ et $L = \mathbf{Q}[\alpha, \beta, \bar{\beta}]$.

2) Montrer que $[K : \mathbf{Q}] = 3$ et $[L : \mathbf{Q}] = 6$.

3) Calculer le discriminant de $P(X)$. En déduire que $\mathbf{Q}[\sqrt{-23}] \subset L$.

4) Montrer que $O_K = \mathbf{Z}[\alpha]$ et que 23 est le seul nombre premier ramifié dans $K$.

5) Montrer que $23O_K = \mathfrak{q}_1\mathfrak{q}_2^2$, où $\mathfrak{q}_1$ et $\mathfrak{q}_2$ sont des idéaux maximaux distincts.

6) Montrer que 23 est le seul nombre premier ramifié dans $L$.

7) Montrer qu'aucun idéal maximal de $\mathbf{Q}[\sqrt{-23}]$ ne se ramifie dans $L$.

**Remarque.** On peut montrer que $O_K$ est principal.

**Exercice 4.** Soit $L = \mathbf{Q}\left[i, \sqrt{5}\right]$, $i = \sqrt{-1}$.

1) Montrer que $O_L$ est un module libre de rang 2 sur $\mathbf{Z}[i]$.

2) Soit $A = \mathbf{Z}\left[i, \frac{1+\sqrt{5}}{2}\right]$. Montrer que $A \subseteq O_L$ et déterminer le discriminant $D_{A/\mathbf{Z}[i]}$.

3) Montrer que $A = O_L$.

4) Calculer le discriminant $d_L$ de $L/\mathbf{Q}$.

5) Montrer que les euls nombres premiers qui se ramifient dans $L$ sont 2 et 5 et que les indices de ramification correspondants sont égaux à 2.

6) Montrer que $\mathbf{Q}[\sqrt{-5}] \subset L$ et qu'aucun idéal premier de $\mathbf{Q}[\sqrt{-5}]$ ne se ramifie dans $L$.

**Exercice 5.** Soit $p \neq 2$ un nombre premier impair. On note $\zeta_p$ une racine primitive de l'unité d'ordre $p$ et on pose $K = \mathbf{Q}[\zeta_p]$.

1) Montrer que $\zeta_p - 1$ est une racine d'un polynôme d'Eisenstein de degré $p-1$. En déduire que $[K : \mathbf{Q}] = p - 1$.

2) Soit $\Phi_p(X) = X^{p-1} + \cdots + X + 1$. En utilisant l'identité $X^p - 1 = (X-1)\Phi_p(X)$, calculer $\Phi_p'(\zeta_p)$.

3) Montrer que le discriminant de $\Phi_p(X)$ est égal à $(-1)^{(p-1)/2}p^{p-2}$.

4) Soit $A = \mathbf{Z}[\zeta_p]$. On veut montrer que $A = O_K$. On pose $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbf{Q}}$ et $\mathrm{N} = \mathrm{N}_{K/\mathbf{Q}}$.

4a) Montrer que $\mathrm{Tr}(\zeta_p^k) = -1$ et $\mathrm{Tr}(1 - \zeta_p^k) = p$ pour $1 \leqslant k \leqslant p-1$.

4b) Montrer que $p = \mathrm{N}(1 - \zeta_p)$.

4c) Montrer que $O_K(1-\zeta_p) \cap \mathbf{Z} = p\mathbf{Z}$.

4d) En déduire que $\mathrm{Tr}(x(1-\zeta_p)) \in p\mathbf{Z}$ pour tout $x \in O_K$.

4e) Soit $x = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$, $a_k \in \mathbf{Q}$. Supposons que $x \in O_K$.

4f) Montrer que $a_0 \in \mathbf{Z}$.

4g) Montrer que $a_k \in \mathbf{Z}$ pour tout $0 \leqslant k \leqslant p-1$.

4h) Conclure.

5) Montrer que $d_K = (-1)^{(p-1)/2}p^{p-2}$.

6) Montrer que $pO_K = \mathfrak{p}^{p-1}$, où $\mathfrak{p}$ est un idéal maximal de $O_K$.