Université Paris Diderot — Arithmétique – Année 2011-12
ENS Cachan
M1 mathématiques

Feuille d'exercices 3

Décomposition des idéaux premiers dans les corps quadratiques, entiers cyclotomiques

I

Soit K une extension quadratique de $\mathbf{Q}$. Soit p un nombre premier. Notons $\mathcal{O}_K$ l'anneau des entiers de K. Soit $\mathcal{Q}$ un idéal premier au dessus de p. On note $e_\mathcal{Q}$ l'indice de ramification de $\mathcal{Q}$. Notons g_p le nombre d'idéaux premiers de $\mathcal{O}_K$ au dessus de p.

On rappelle que si $K = \mathbf{Q}(\sqrt{d})$, avec $d \neq 0, 1$ entier sans facteur carré, on a $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$ si $d \equiv 2$ ou $3 \pmod 4$ et $\mathcal{O}_K = \mathbf{Z}[(1+\sqrt{d})/2]$ si $d \equiv 1 \pmod 4$. On rappelle qu'il existe un polynôme $Q_d \in \mathbf{Z}[X]$ de discriminant $\mathcal{D}$, où est $\mathcal{D} = d$ si $d \equiv 1 \pmod 4$ et $\mathcal{D} = 4d$ si $d \equiv 2$ ou $3 \pmod 4$.

1. Montrer que $\mathbf{F}_\mathcal{Q} = \mathcal{O}_K/\mathcal{Q}$ est un corps fini à p ou p^2 éléments. Notons $f_\mathcal{Q}$ le degré résiduel $[\mathbf{F}_\mathcal{Q} : \mathbf{F}_p]$.

2. Montrer que le discriminant de K sur $\mathbf{Q}$ est $\mathcal{D}$.

3. Montrer que si $\mathcal{D}$ est un carré non nul modulo p, on a $f_\mathcal{Q} = 1$, $e_\mathcal{Q} = 1$ et $g_p = 2$. On dit que p est *décomposé* dans K.

4. Montrer que si $\mathcal{D}$ n'est pas un carré modulo p, on a $f_\mathcal{Q} = 2$, $e_\mathcal{Q} = 1$ et $g_p = 1$. On dit que p est *inerte* dans K.

5. Montrer que si $\mathcal{D}$ est nul modulo p, on a $f_\mathcal{Q} = 1$, $e_\mathcal{Q} = 2$ et $g_p = 1$. On dit que p est *ramifié* dans K.

II

Soit n un entier ≥ 1. Le n-ème polynôme cyclotomique est le polynôme Φ_n défini par récurrence sur n par la formule $\Phi_n(X) = (X^n - 1)/\Pi_{d|n, d\neq n, d>0}\Phi_d(X)$. Ainsi, on a $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, $\Phi_6(X) = X^2 - X + 1$. On sait que Φ_n est un polynôme irréductible sur $\mathbf{Q}$, à coefficients entiers, et que ses racines sont les racines primitives n-èmes de l'unité.

Un *n-ème corps cyclotomique* est un corps de décomposition de Φ_n, ou, ce qui revient au même, un corps de décomposition de $X^n - 1$. Il est commode de plonger un tel corps dans $\mathbf{C}$. Le n-ème corps cyclotomique est alors unique : il est égal à $\mathbf{Q}(\zeta)$ où ζ est une racine primitive n-ème de l'unité dans $\mathbf{C}$. Par exemple on peut poser $\zeta = e^{2i\pi/n}$.

Supposons que $n = p^k$ avec k entier ≥ 1. Notons $\mathcal{O}$ l'anneau des entiers de $\mathbf{Q}(\zeta)$. Posons $d = p^k - p^{k-1} = \phi(p^k)$. C'est le degré de l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$.

1. Montrer qu'on a $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$.

2. Montrer que $\mathrm{N}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(1 - \zeta) = p$.

3. En utilisant la formule $1 - \zeta^i = (1 - \zeta)(1 + \zeta + ... + \zeta^{i-1})$, montrer que p est un multiple de $(1 - \zeta)^d$ dans $\mathcal{O}$.

4. Comparer les décompositions en produits d'idéaux premiers de p et de $1 - \zeta$ dans $\mathcal{O}$. En déduire que l'idéal $(1 - \zeta)\mathcal{O}$ est premier et que $p\mathcal{O} = (1 - \zeta)^d\mathcal{O}$.

5. Montrer que l'anneau quotient $\mathcal{O}/(1-\zeta)\mathcal{O}$ est un corps à p éléments. Quel est le degré résiduel en $(1-\zeta)\mathcal{O}$ de l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$? Quel est l'indice de ramification de $(1 - \zeta)\mathcal{O}$? Combien y a-t-il d'idéaux premiers au dessus de p dans $\mathcal{O}$?

6. Montrer qu'on a $(1-\zeta)\mathcal{O}+\mathbf{Z}[\zeta]=\mathcal{O}$. En déduire par récurrence sur l'entier t qu'on a $(1-\zeta)^t\mathcal{O}+\mathbf{Z}[\zeta]=\mathcal{O}$ (t entier ≥ 1).

7. En utilisant que $(1,\zeta,...,\zeta^{d-1})$ est une base de $\mathbf{Z}[\zeta]$ et que $D(1,\zeta,...,\zeta^{d-1})$ est une puissance de p (voir feuille 2), montrer que $\mathbf{Z}[\zeta]$ est un sous-groupe d'indice une puissance de p de $\mathcal{O}$.

8. En déduire qu'on a $\mathcal{O}=\mathbf{Z}[\zeta]$.

III

Soit M un corps de nombres contenant deux sous-corps L_1 et L_2. Notons $\mathcal{O}_1$ et $\mathcal{O}_2$ les anneaux des entiers de L_1 et L_2 respectivement. Supposons que M soit engendré par L_1 et L_2 et qu'on a $[M:\mathbf{Q}]=[L_1:\mathbf{Q}][L_2:\mathbf{Q}]$ (on dit que les extension $L_1|\mathbf{Q}$ et $L_2|\mathbf{Q}$ sont *linéairement indépendantes*).

On suppose de plus que les discriminants $\mathcal{D}_1$ et $\mathcal{D}_2$ des corps L_1 et L_2 sont premiers entre eux. Montrons que l'anneau des entiers de M est l'anneau $\mathcal{O}_2\mathcal{O}_1$ engendré par $\mathcal{O}_1$ et $\mathcal{O}_2$.

1. Soit $(y_1,...,y_n)$ une base de $\mathcal{O}_2$ sur $\mathbf{Z}$. Montrer que c'est une base de M sur L_1. Montrer que $D(y_1,...,y_n)$ endendre $\mathcal{D}_2$.

2. Considérons la base $(y'_1,...,y'_n)$ de L_2 duale de $(y_1,...,y_n)$ pour la forme bilinéaire $(x,y)\mapsto \mathrm{Tr}_{L_2/\mathbf{Q}}(xy)$. Soit $x=\sum_{i=1}^n \alpha_i y'_i \in \mathcal{O}$ avec $\alpha_i\in L_1$. Montrer que $\mathrm{Tr}_{L/L_1}(xy_i)=\alpha_i$ ($i\in\{1,...,n\}$). En déduire que $\alpha_i\in\mathcal{O}_1$.

3. Notons A la matrice de passage de $(y_1,...,y_n)$ à $(y'_1,...,y'_n)$. Montrer que $A=\mathrm{Tr}_{L_2/\mathbf{Q}}(y_iy_j)_{1\leq i,j\leq n}$ et que $A^{-1}=\mathrm{Tr}_{L_2/\mathbf{Q}}(y'_iy'_j)_{1\leq i,j\leq n}$. En déduire que la matrice A^{-1} est à coefficients dans $D(y_1,...,y_n)^{-1}\mathbf{Z}$, puis que y'_1, ..., y'_n sont dans $D(y_1,...,y_n)^{-1}\mathcal{O}_2$

4. En déduire que $x\in\mathcal{D}_2^{-1}\mathcal{O}_2\mathcal{O}_1$, puis que $x\in\mathcal{D}_1^{-1}\mathcal{O}_2\mathcal{O}_1$.

5. Posons dans $\mathbf{Z}$, $1=d_1+d_2$, avec $d_1\in\mathcal{D}_1$ et $d_2\in\mathcal{D}_2$. Montrer que $x=d_1x+d_2x\in\mathcal{O}_2\mathcal{O}_1$. En déduire que $\mathcal{O}=\mathcal{O}_2\mathcal{O}_1$.

6. En utilisant l'exercice précédent, en déduire que l'anneau des entiers du corps cyclotomique $\mathbf{Q}(\zeta)$ est $\mathbf{Z}[\zeta]$, lorsque ζ est une racine de l'unité.

7. Montrer que le discriminant absolu de M est donné par la formule $\mathcal{D}_1^{[L_2:\mathbf{Q}]}\mathcal{D}_2^{[L_1:\mathbf{Q}]}$.