UNIVERSITÉ DE BORDEAUX I 2007-2008
MASTER DE MATHÉMATIQUES *1ère année*
Option : Théorie algébrique des nombres.

Corrigé du DM 2

Exercice.

1. Si p est inerte dans K, l'idéal $p\mathcal{O}_K$ est maximal. Si e, f et g désigne respectivement l'indice de ramification, le degré résiduel et le nombre d'idéaux maximaux au-dessus de p, on a donc
$$e = g = 1, \text{ et } f = [K : \mathbb{Q}].$$
Par suite , le sous-groupe de décomposition D_p de $p\mathcal{O}_K$ est égal à $\mathrm{Gal}(K/\mathbb{Q})$ tout entier et son sous groupe d'inertie I_p est trivial. Comme le quotient D_p/I_p est cyclique (il est isomorphe au groupe de Galois de l'extension $\mathbb{F}_{p^f}/\mathbb{F}_p$), on conclut que $\mathrm{Gal}(K/\mathbb{Q}) = D_p \simeq D_p/I_p$ est cyclique.
2. La décomposition de l'idéal $\mathfrak{p}$ dans K' peut s'écrire
$$\mathfrak{p}\mathcal{O}'_K = \prod_{i=1}^{g} {\mathfrak{p}'_i}^{e'_i} \tag{1}$$
en convenant, par exemple, que $\mathfrak{p}'_1 = \mathfrak{p}'$, et donc $e'_1 = e'$. De même, la décomposition de chacun des $\mathfrak{p}'_i$ dans K'' peut s'écrire
$$\mathfrak{p}'_i\mathcal{O}''_K = \prod_{j=1}^{g'_i} {\mathfrak{p}''_{ij}}^{e''_{ij}} \tag{2}$$
en convenant que $\mathfrak{p}''_{11} = \mathfrak{p}''$ et $e''_{11} = e''$. En combinant (1) et (2), on obtient la décomposition de $\mathfrak{p}$ dans K'' :
$$\mathfrak{p}\mathcal{O}''_K = \prod_{i=1}^{g}\prod_{j=1}^{g'_i} {\mathfrak{p}''_{ij}}^{e'_i e''_{ij}}$$
d'où il suit immédiatement que l'indice de ramification e de $\mathfrak{p}''$ dans K'' vérifie la relation
$$e = e'e''.$$
De même, la relation $f = f'f''$ suit de la formule
$$[\mathcal{O}''_K/\mathfrak{p}'' : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}''_K/\mathfrak{p}'' : \mathcal{O}'_K/\mathfrak{p}'][\mathcal{O}'_K/\mathfrak{p}' : \mathcal{O}_K/\mathfrak{p}].$$

Problème.

1. Les relations $y+\overline{y}=-x$ et $y\overline{y}=-\frac{1}{x}$ sont une conséquence immédiate de la factorisation $X^3-X+1=(X-x)(X-y)(X-\overline{y})$. Quant à la seconde relation, elle s'obtient en calculant le discriminant de $\{1,x,x^2\}$ de deux façons différentes : on a d'une part

$$\text{Disc}(1,x,x^2)=\text{Disc}P(X)=-27+4=-23$$

et d'autre part

$$\text{Disc}(1,x,x^2)=\begin{vmatrix}1 & x & x^2\\ 1 & y & y^2\\ 1 & \overline{y} & \overline{y}^2\end{vmatrix}^2=\left[(y-x)\left(\overline{y}-x\right)\left(y-\overline{y}\right)\right]^2.$$

Par suite, le corps $\mathbb{Q}\left[x,y,\overline{y}\right]$ contient les deux racines de l'équation $X^2+23=0$, donc $\mathbb{Q}\left[x,y,\overline{y}\right]$ contient $\mathbb{Q}\left[x\right]\left[\sqrt{-23}\right]=K\left[\sqrt{-23}\right]$. Par ailleurs, on a $\mathbb{Q}\left[x,y,\overline{y}\right]=Q\left[x,y\right]=K\left[y\right]$ puisque $y+\overline{y}=-x$, et l'extension $K\left[y\right]/K$ est de degré 2 de même que l'extension $K\left[\sqrt{-23}\right]/K$. On a donc égalité. Finalement, l'extension $L=\mathbb{Q}\left[x,y,\overline{y}\right]$ est galoisienne car elle contient les conjugués sur $\mathbb{Q}$ de ses trois générateurs. Un élément σ du groupe de Galois induit une permutation des racines x, y et $\overline{y}$ de $P(X)$, d'où l'on déduit un morphisme de $\text{Gal}_{L/\mathbb{Q}}$ dans le groupe des permutations S_3. Ce morphisme est clairement injectif, car si $\sigma\in\text{Gal}_{L/\mathbb{Q}}$ fixe x, y et $\overline{y}$, alors il fixe tous les éléments de L. Comme $\text{Gal}_{L/\mathbb{Q}}$ et S_3 ont même ordre, on conclut que $G=\text{Gal}_{L/\mathbb{Q}}$ est isomorphe à S_3. Explicitement, on peut engendrer G par les deux éléments suivants : d'une part la conjugaison complexe ι, qui correspond à la transposition échangeant y et $\overline{y}$, et d'autre part l'élément γ correspondant à la permutation circulaire de x, y et $\overline{y}$.

2. Avec les notations précédentes, on voit que G possède un unique sous-groupe d'ordre 3, à savoir $H=\langle\gamma\rangle$, qui est normal dans G. Par la correspondance de Galois, il lui correspond une unique sous-extension quadratique de L, à savoir $M=\mathbb{Q}\left[\sqrt{-23}\right]$ qui est elle-même galoisienne. Il y a par ailleurs 3 sous-groupes d'ordre 2, correspondant aux transpositions ι, $\iota\gamma$ et $\iota\gamma^2$, auquelles correspondent trois sous extensions cubiques, à savoir $K=\mathbb{Q}\left[x\right]$, $K'=Q\left[y\right]$ et $K'=Q\left[\overline{y}\right]$ qui ne sont pas galoisiennes (les sous-groupes correspondants ne sont pas normaux dans G).

3. D'après la question 1 de l'exercice, il n'y a pas de premiers inertes dans l'extension $L/\mathbb{Q}$, car le groupe de Galois de l'extension n'est pas cyclique.

4. Le discriminant de $\{1,x,x^2\}$ étant sans facteur carré, on conclut que $\mathcal{O}_K=Z\left[x\right]$.

5. On a $d_K=\text{Disc}(1,x,x^2)=-23$, donc 23 est le seul nombre premier ramifié dans K. De plus, le polynôme $P(X)=X^3-X+1$ admet la décomposition suivante modulo 23 :

$$X^3-X+1=(X+10)^2(X+3)\in\mathbb{F}_{23}[X].$$

On en déduit que

$$23\mathcal{O}_K=\mathfrak{p}_1^2\mathfrak{p}_2 \tag{3}$$

où $\mathfrak{p}_1=(23,x+10)$ et $\mathfrak{p}_2=(23,x+3)$.

6. Soit p un nombre premier ramifié dans L, et $\mathfrak{p}$ un idéal premier au-dessus de p. On note $\mathfrak{p}_K = \mathfrak{p} \cap \mathcal{O}_K$, $\mathfrak{p}_M = \mathfrak{p} \cap \mathcal{O}_M$, e_K l'indice de ramification de $\mathfrak{p}_K$ sur $\mathbb{Q}$, e_M celui de $\mathfrak{p}_M$ sur $\mathbb{Q}$, $e_{L/K}$ l'indice de ramification de $\mathfrak{p}$ sur K et $e_{L/M}$ celui de $\mathfrak{p}$ sur M. Grâce à la question (2) de l'exercice, on a les relations

$$e = e_{L/K} e_K \text{ et } e = e_{L/M} e_M \tag{4}$$

Supposons que p ne soit ramifié ni dans K ni dans M, auquel cas $e_K = e_M = 1$, soit $e = e_{L/K} = e_{L/M}$. Par ailleurs, les extensions L/K et L/M étant galoisiennes, on a, avec des notations évidentes, les relations

$$[L : K] = e_{L/K} f_{L/K} g_{L/K} \text{ et } [M : K] = e_{M/K} f_{M/K} g_{M/K}.$$

En particulier $e = e_{L/K} = e_{L/M}$ divise $[L : K] = 2$ et $[M : K] = 3$, ce qui implique que $e = 1$, et donc que p est non ramifié dans L. Les seuls premiers ramifiés dans L sont donc ceux qui sont ramifiés dans M ou dans K, condition remplie uniquement par $p = 23$.

Puisque $L/\mathbb{Q}$ est galoisienne, tous les idéaux premiers au-dessus de 23 ont même indice de ramification e. Considérons un idéal premier $\mathfrak{p}$ tels que $\mathfrak{p} \cap \mathcal{O}_K$ soit l'idéal $\mathfrak{p}_1$ de la formule (3). Avec les notations précédentes, on a alors $e_K = 2$, d'où l'on déduit, grâce à (4), que e est pair et ≥ 2. Par ailleurs, la formule (3) implique qu'il y a au moins deux idéaux premiers de $\mathcal{O}_L$ au-dessus de 23, soit $g \geq 2$. Enfin, prenant en considération la relation $efg = 6$, on conclut que $e = 2$, $g = 3$ et $f = 1$.

7. Soit $N = \mathbb{Q}\left[\sqrt{-23}\right]$ et $\mathfrak{q}$ un idéal maximal de $\mathcal{O}_N$ au-dessus d'un nombre premier q. Si $\mathfrak{q}$ était ramifié dans L/N alors, q serait ramifié dans $L/\mathbb{Q}$ ce qui implique (question précédente) que $q = 23$. Or 23 est ramifié dans N (le discriminant d_N de N sur $\mathbb{Q}$ est égal à -23). On aurait donc $23\mathcal{O}_N = \mathfrak{q}^2$. Finalement, l'indice de ramification de 23 dans L serait donc $e = e_{L/N} e_N = 2e_{L/N} > 2$ (l'hypothèse de ramification de $\mathfrak{q}$ dans L/N signifie que $e_{L/N} > 1$). Ceci est impossible car on vient de voir que l'indice de ramification de 23 dans L est égal à 2.