

Master de Mathématiques approfondies

première année

Corrigé du devoir surveillé de **Théorie Algébrique des Nombres** du mardi 04 mars 2008

Exercice.

1. l'anneau A est intègre comme sous-anneau de l'anneau intègre $k[X]$. Son corps des fractions $\text{Frac } A$ est contenu dans $\text{Frac } k[X] = k(X)$. Puisque a et b sont premiers entre eux, il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$. Ainsi, $X = (X^a)^u (X^b)^v$ est contenu dans $\text{Frac } k[X^a, X^b]$. On a donc $\text{Frac } A = k(X)$.
2. Tout d'abord, on remarque que l'anneau $k[X^a]$ est isomorphe à $k[X]$. Il est donc noethérien (car principal). Ensuite, on constate que $k[X] = k[X^a] + Xk[X^a] + \cdots + X^{a-1}k[X^a]$ est un $k[X^a]$ -module de type fini. Il est donc noethérien, en tant que $k[X^a]$ -module, et A , qui en est un sous $k[X^a]$ -module, également. Soit alors I un idéal de A : c'est un sous $k[X^a]$ -module du $k[X^a]$ -module noethérien A ; il est donc de type fini en tant que $k[X^a]$ -module, et *a fortiori* en tant que A -module.
3. Soit $\mathfrak{p}$ un idéal premier non nul de A . Alors $\mathfrak{p} \cap k[X^a]$ est un idéal premier de $k[X^a]$: en effet, $k[X^a] / \mathfrak{p} \cap k[X^a]$ s'injecte dans $A/\mathfrak{p}$ qui est intègre par hypothèse, donc $k[X^a] / \mathfrak{p} \cap k[X^a]$ l'est également. De plus, $\mathfrak{p} \cap k[X^a]$ est non nul : en effet $A = k[X^a][X^b]$ est entier sur $k[X^a]$, puisque X^b est entier sur $k[X^a]$ ($(X^b)^a - (X^a)^b = 0$). Ainsi, si y est un élément non nul de $\mathfrak{p}$, alors il existe un entier naturel non nul n et des éléments $a_0, \dots, a_{n-1}$ dans $k[X^a]$ avec $a_0 \neq 0$, tels que

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$$

auquel cas $a_0 = -y(y^{n-1} + a_{n-1}y^{n-2} + \cdots + a_1)$ est un élément non nul de $\mathfrak{p} \cap k[X^a]$. On peut donc conclure que $\mathfrak{p} \cap k[X^a]$ est un idéal maximal puisque $k[X^a]$ est principal. En particulier, $k[X^a] / \mathfrak{p} \cap k[X^a]$ est un corps, que l'on note désormais K . Comme A est un $k[X^a]$ -module de type fini, on en déduit que $B = A/\mathfrak{p}$ est un K espace vectoriel de dimension finie. Par ailleurs, $B = A/\mathfrak{p}$ est un anneau intègre, donc une K -algèbre intègre de dimension finie sur K . Une telle algèbre est nécessairement un corps : en effet, si x est un élément non nul de B , la multiplication par x induit un K -endomorphisme *injectif* de B (intégrité), donc *bijectif* (dimension finie), donc il existe $y \in B$ tel que $xy = 1$, ce qui signifie que x est inversible.

4. On remarque que X est entier sur A , puisque racine du polynôme unitaire $Y^a - X^a \in A[Y]$. Si a et b sont > 1 , X n'est pas dans A et on conclut que A n'est pas intégralement clos, donc pas de Dedekind. Inversement, si a ou b vaut 1, alors $A = k[X]$ est principal, donc de Dedekind. Dans tous les cas, la clôture intégrale de A contient $k[X]$, mais elle est également contenue dans $k[X]$, car $\text{Frac } A = k(X)$, et tout élément de $k(X)$ entier sur A l'est également sur $k[X]$, qui est intégralement clos.

Problème.

1. Le polynôme $P(X) = X^3 - 3X + 1$ est irréductible dans $\mathbb{Q}[X]$ car sans racine dans $\mathbb{Q}$: si $x = \frac{a}{b}$ avec a et b entiers premiers entre eux est une racine de $P(X)$, alors $a^3 - 3ab^2 + b^3 = 0$, donc $a(3b^2 - a^2) = b^3$, donc $a = \pm 1$ puisque a et b sont étrangers, et de même $b = \pm 1$, d'où $x = \pm 1$, or ni 1 ni -1 n'est racine de $P(X)$.¹ L'étude des variations de la fonction $x \mapsto P(x)$ montre qu'elle s'annule 3 fois sur $\mathbb{R}$.
2. L'anneau $\mathcal{O}_K$ est libre de rang 3 sur $\mathbb{Z}$ d'après un théorème du cours. Quant à $A = \mathbb{Z}[\theta]$, puisque $\theta^3 = 3\theta - 1$, on a $A = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2$. De plus la somme est directe car θ est algébrique de degré 3. Donc A est libre de rang 3 sur $\mathbb{Z}$. Pour établir la relation $\text{Disc}_A = (\mathcal{O}_K : A)^2 \text{Disc}_{\mathcal{O}_K}$, on peut utiliser le théorème de la base adaptée : il existe une $\mathbb{Z}$ -base $\{e_1, e_2, e_3\}$ de $\mathcal{O}_K$ et des entiers a_1, a_2, a_3 tels que $\{a_1e_1, a_2e_2, a_3e_3\}$ soit une $\mathbb{Z}$ -base de A . Par suite, $\text{Disc}_A = \det(\text{Tr}_{K/\mathbb{Q}}(a_ie_ia_je_j))_{1 \leq i,j \leq 3} = (a_1a_2a_3)^2 \det(\text{Tr}_{K/\mathbb{Q}}(e_ie_j))_{1 \leq i,j \leq 3}$, d'où la conclusion puisque $a_1a_2a_3 = (\mathcal{O}_K : A)$.
3. On peut, au choix, calculer $\text{Tr}_{K/\mathbb{Q}}(\theta^i\theta^j)$ pour $0 \leq i, j \leq 2$, ou utiliser la formule, vue en TD, pour le discriminant de $P(X)$. Les valeurs possibles, pour $(\mathcal{O}_K : A)$ sont donc 1, 3 ou 3^2 .
4. Puisque $(\mathcal{O}_K : A) = 3^i$ avec $i \leq 2$, le quotient $\mathcal{O}_K/A$ est d'exposant 3^i , et dans tous les cas

$$3^2\mathcal{O}_K \subset 3^i\mathcal{O}_K \subset \mathbb{Z}[\theta] \subset \mathcal{O}_K.$$

Comme 3 est inversible dans $S^{-1}\mathbb{Z}$, on conclut que

$$S^{-1}\mathcal{O}_K = S^{-1}3^2\mathcal{O}_K \subset S^{-1}\mathbb{Z}[\theta] \subset S^{-1}\mathcal{O}_K,$$

d'où $S^{-1}\mathcal{O}_K = S^{-1}\mathbb{Z}[\theta]$. En utilisant l'inclusion $\mathcal{O}_K \hookrightarrow S^{-1}\mathcal{O}_K$ on conclut que tout élément $x \in \mathcal{O}_K$ s'écrit de façon unique sous la forme

$$x = a + b(\theta + 1) + c(\theta + 1)^2$$

avec a, b et c dans $S^{-1}\mathbb{Z}$.

5. Soit $x \in \mathcal{O}_K$, et $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$ son polynôme minimal. On sait alors que $N_{K/\mathbb{Q}}(x) = ((-1)^n a_0)^{[K:\mathbb{Q}(x)]}$. Si $N_{K/\mathbb{Q}}(x) = \pm 1$, on a alors $a_0 = \pm 1$, auquel cas $x(x^{n-1} + a_{n-1}X^{n-2} + \dots + a_1) = \pm 1$ et x est inversible dans $\mathbb{Z}[x]$ et a fortiori dans $\mathcal{O}_K$ puisque $\mathbb{Z}[x] \subset \mathcal{O}_K$. Inversement si x est inversible dans $\mathcal{O}_K$, il existe $y \in \mathcal{O}_K$ tel que $1 = xy$, d'où $1 = N_{K/\mathbb{Q}}(xy) = N_{K/\mathbb{Q}}(x)N_{K/\mathbb{Q}}(y)$, ce qui implique que $N_{K/\mathbb{Q}}(x) = \pm 1$ puisque $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$.
6. On a $N_{K/\mathbb{Q}}(\theta) = -1$ puisque son polynôme minimal est $X^3 - 3X + 1$, donc θ est inversible. On peut également calculer la norme de $\theta + 2$ (c'est le déterminant de la matrice de la multiplication par $\theta + 2$ dans la base $\{1, \theta, \theta^2\}$) et constater qu'elle vaut -1 et donc que $\theta + 2$ est inversible. Il suit que

$$\mathfrak{p}^3 = 3\theta(\theta + 2)\mathcal{O}_K = 3\mathcal{O}_K. \quad (1)$$

¹Autre argument (plus rapide !) : si $x \in \mathbb{Q}$ est une racine de $P(X)$, alors x est entier sur $\mathbb{Z}$, puisque $P(X) \in \mathbb{Z}[X]$ est unitaire, donc $x \in \mathbb{Z}$ puisque $\mathbb{Z}$ est intégralement clos. Ainsi $x^3 - 3x + 1 = 0$, d'où $x(x^2 - 3) = -1$, ce qui implique que $x = \pm 1$ et on conclut comme précédemment puisque ni 1 ni -1 n'est racine de $P(X)$.

Par ailleurs, la théorie générale des anneaux de Dedekind permet d'affirmer que l'idéal $\mathfrak{p}$ peut s'écrire de façon unique sous la forme

$$\mathfrak{p} = \prod_{i=1}^r \mathfrak{p}_i^{e_i} \quad (2)$$

où les $\mathfrak{p}_i$ sont des idéaux premiers et les e_i sont des entiers naturels non nuls. Combinée avec (1), cette relation entraîne, pour l'idéal $3\mathcal{O}_K$, la décomposition

$$3\mathcal{O}_K = \prod_{i=1}^r \mathfrak{p}_i^{3e_i}.$$

En notant f_i le degré résiduel de l'idéal premier $\mathfrak{p}_i$, on doit avoir en outre la relation

$$\sum_{i=1}^r 3e_i f_i = 3,$$

ce qui n'est possible que si $r = 1$ et $e_1 = f_1 = 1$. En particulier, $\mathfrak{p} = \mathfrak{p}_1$ est premier.

7. Remarquons tout d'abord que, pour $x \in K^\times$ et $n \in \mathbb{Z}$ on a les équivalences

$$x \in \mathfrak{p}^n \Leftrightarrow x\mathcal{O}_K \subset \mathfrak{p}^n \Leftrightarrow v_{\mathfrak{p}}(x) \geq n.$$

Ainsi, $v_{\mathfrak{p}}(x) = \max \{n \in \mathbb{Z}, x \in \mathfrak{p}^n\}$. Si on pose $v_{\mathfrak{p}}(x) = n$, $v_{\mathfrak{p}}(y) = m$, et $l = \min \{m, n\}$, il est clair que x et y appartiennent à $\mathfrak{p}^l$, donc $x + y \in \mathfrak{p}^l$ et $v_{\mathfrak{p}}(x + y) \geq l$. Si $m \neq n$, mettons par exemple $m < n$, alors x appartient à $\mathfrak{p}^{m+1}$, car $n \geq m + 1$, mais pas $x + y$, car sinon $y = (x + y) - x$ appartiendrait à $\mathfrak{p}^{m+1}$, contredisant la définition de $m = v_{\mathfrak{p}}(y)$. Donc $v_{\mathfrak{p}}(x + y) = m = l$ dans ce cas.

8. La $\mathfrak{p}$ -valuation de $x = a + b(\theta + 1) + c(\theta + 1)^2$ est positive ou nulle, car $x \in \mathcal{O}_K$. Par ailleurs, on a pour $x \in \mathbb{Q}$ la relation $v_3(x) = 3v_{\mathfrak{p}}(x)$, où v_3 désigne la valuation 3-adique d'un rationnel, et ceci grâce à la relation $\mathfrak{p}^3 = 3\mathcal{O}_K$. Comme $v_{\mathfrak{p}}((\theta + 1)) = 1$ et $v_{\mathfrak{p}}((\theta + 1)^2) = 2$, on conclut que $v_{\mathfrak{p}}(a)$, $v_{\mathfrak{p}}(b(\theta + 1))$ et $v_{\mathfrak{p}}(c(\theta + 1)^2)$ sont deux à deux non congrues modulo 3, donc a fortiori deux à deux distinctes. On a donc $0 \leq v_{\mathfrak{p}}(v_{\mathfrak{p}}(a + b(\theta + 1) + c(\theta + 1)^2)) = \min \{v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b(\theta + 1)), v_{\mathfrak{p}}(c(\theta + 1)^2)\}$. Par suite, les $\mathfrak{p}$ -valuations de a , b et c sont positives ou nulles, donc leurs valuations 3-adiques également. Par ailleurs, pour tout premier $p \neq 3$, les valuations p -adiques de a , b et c sont positives ou nulles, puisque a , b et c sont dans $S^{-1}\mathbb{Z} = \{\frac{n}{3^m}, n \in \mathbb{Z}, m \in \mathbb{N}\}$. On peut donc conclure que a , b et c sont dans $\mathbb{Z}$.
9. Ce qui précède entraîne immédiatement que $\mathcal{O}_K = \mathbb{Z}[\theta]$ et donc $\text{Disc}_{\mathcal{O}_K} = \text{Disc}_{\mathbb{Z}[\theta]} = 3^4$, ce qui montre que 3 est le seul premier ramifié dans K .
10. On sait (voir TD) que la décomposition d'un premier p "se lit" sur la réduction modulo p du polynôme minimal de θ . Pour $p = 2$, on a $X^3 - 3X + 1 = X^3 + X + 1 \in \mathbb{F}_2[X]$, irréductible car de degré 3 et sans racine dans $\mathbb{F}_2$, donc 2 est inerte. De même pour $p = 5$, $X^3 - 3X + 1 = X^3 + 2X + 1 \in \mathbb{F}_5[X]$ est irréductible pour la même raison, et 5 est inerte.