ANNEAUX D'ENTIERS

Quelques notes sur certains exercices de la feuille 3 qui n'ont pas été traités dans le TD2.

Exercice 11.

On laisse en exercice l'irréductibilité du polynôme $P = X^3 - X - 1$.
Soit θ une racine de P. Il est clair que θ est un entier algébrique (donc aussi θ^2). Déterminons l'anneau des entiers du corps de nombres $K = \frac{\mathbb{Q}[X]}{(P)}$, identifié à l'extension $\mathbb{Q}(\theta)$.
On calcule d'abord le discriminant de la $\mathbb{Q}$-base $(1, \theta, \theta^2)$ de K. D'après le cours, cette quantité est donnée par la formule

$$Disc(1, \theta, \theta^2) = \det(Tr(\theta^{i+j}))_{0 \leq i,j \leq 2}),$$

soit encore

$$Disc(1, \theta, \theta^2) = \det \begin{bmatrix} Tr(1) & Tr(\theta) & Tr(\theta^2) \\ Tr(\theta) & Tr(\theta^2) & Tr(\theta^3) \\ Tr(\theta^2) & Tr(\theta^3) & Tr(\theta^4) \end{bmatrix}.$$

Afin d'expliciter les coefficients apparaissant dans cette matrice, calculons la trace d'un élément de K. A cet effet on rapelle que l'application

$$m_x : K \longrightarrow K; \quad y \mapsto yx$$

est un endomorphisme $\mathbb{Q}$-linéaire du $\mathbb{Q}$-espace vectoriel K et que la trace de x est la trace de m_x.
A titre d'exemple calculons la trace de θ^3. La matrice de m_{θ^3} dans la base $(1, \theta, \theta^2)$ est :

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

On a donc $Tr(\theta^3) = 3$. Tous calculs faits, il vient

$$Disc(1, \theta, \theta^2) = \det \begin{bmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{bmatrix} = -23.$$

La famille $(1, \theta, \theta^2)$ est donc une $\mathbb{Q}$-base de K constituée d'entiers algébriques et de discriminant -23, qui est sans facteur carré. D'après un théorème du cours, c'est une $\mathbb{Z}$-base de l'anneau des entiers de K.

Exercice 12.

1. Comme 6 et 12 sont congrus à 2 modulo 4, l'anneau des entiers de $\mathbb{Q}(\sqrt{6})$ est $\mathbb{Z}[\sqrt{6}]$, celui de $\mathbb{Q}(\sqrt{14})$ est $\mathbb{Z}[\sqrt{14}]$.
2. On remarque que

$$\alpha^2 = \frac{1}{4}(20 + 4\sqrt{21}) = 5 + \sqrt{21}.$$

Il en résulte que le polynôme $(X^2-5)^2-21$ est un polynôme unitaire à coefficients dans $\mathbb{Z}$ annulateur de α.

Exercice 13

1. Le discriminant de $\mathbb{Q}(\sqrt{3})$ est 12, celui de $\mathbb{Q}(\sqrt{5})$ est 5.
2. Il s'agit de vérifier que $\sqrt{3}$ et $\sqrt{5}$ sont dans l'extension $\mathbb{Q}(\zeta)$.
   On a

$$\zeta^2 = \frac{9}{2} + \frac{\sqrt{5}}{2} + \sqrt{3} + \sqrt{15},$$

puis

$$\zeta^2 - \zeta = \frac{9}{2} + \frac{\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2} + \sqrt{15} = 4 + \sqrt{15}.$$

Ainsi, $\sqrt{15} = \zeta^2 - \zeta - 4 \in \mathbb{Q}(\zeta)$.
On a également

$$(\zeta^2 - \frac{9}{2})^2 = \frac{77}{4} + \sqrt{15} + (6+\sqrt{15})\sqrt{5};$$

il en résulte que

$$\sqrt{5} = \frac{(\zeta^2 - \frac{9}{2})^2 - \frac{77}{4} - \sqrt{15}}{6+\sqrt{15}},$$

et donc $\sqrt{5}$ est bien un élément de $\mathbb{Q}(\zeta)$. On en tire imédiatement $\sqrt{3} \in \mathbb{Q}(\zeta)$.

3. Tous calculs faits on obtient la matrice

$$Mat_{\mathcal{B}}(m_\zeta) = \begin{bmatrix} 0 & 3 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 3 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

La relation $\sqrt{15} = \zeta^2 - \zeta - 4$ obtenue au cours de la question précédente donne

$$(\zeta^2 - \zeta - 4)^2 = 15,$$

soit le polynôme $X^4 - 2X^3 - 7X^2 + 8X + 1$, annulateur de ζ.
Autrement, si $Q = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \lambda_3 X^3 + X^4$ est le polynôme minimal de ζ sur $\mathbb{Q}$ (son degré est 4 puisque ζ est un élément primitif de l'extension biquadratique $\mathbb{Q}(\sqrt{3}, \sqrt{5})$), la matrice de la multiplication par ζ dans la base $\mathcal{B}' = (1, \zeta, \zeta^2, \zeta^3)$ est

$$Mat_{\mathcal{B}'}(m_\zeta) = \begin{bmatrix} 0 & 0 & 0 & -\lambda_0 \\ 1 & 0 & 0 & -\lambda_1 \\ 0 & 1 & 0 & -\lambda_2 \\ 0 & 0 & 1 & -\lambda_3 \end{bmatrix}.$$

Or, il est aisé d'obtenir cette matrice grâce aux formules de changements de bases de l'algèbre linéaire. On obtient la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ grâce à $Mat_{\mathcal{B}}(m_\zeta)$:

$$P_{\mathcal{B}',\mathcal{B}} = \begin{bmatrix} 1 & 0 & 4 & 1 \\ 0 & 1 & 0 & 6 \\ 0 & 1 & 1 & 11 \\ 0 & 0 & 2 & 3 \end{bmatrix},$$

et la matrice de passage de $\mathcal{B}'$ à $\mathcal{B}$ en inversant la précédente:

$$P_{\mathcal{B},\mathcal{B}'} = \frac{1}{7}\begin{bmatrix} 7 & -10 & 10 & -19 \\ 0 & 19 & -12 & 6 \\ 0 & 3 & -3 & 5 \\ 0 & -2 & 2 & -1 \end{bmatrix}.$$

On obtient

$$Mat_{\mathcal{B}'}(m_\zeta) = P_{\mathcal{B},\mathcal{B}'} Mat_{\mathcal{B}}(m_\zeta) P_{\mathcal{B}',\mathcal{B}},$$

soit après calculs:

$$Mat_{\mathcal{B}'}(m_\zeta) = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -8 \\ 0 & 1 & 0 & 7 \\ 0 & 0 & 1 & 2 \end{bmatrix}.$$

En identifiant les deux expressions obtenues pour $Mat_{\mathcal{B}'}(m_\zeta)$, on obtient,

$$Q = X^4 - 2X^3 - 7X^2 + 8X + 1.$$

4. Soit Δ le discriminant recherché. Avec $\gamma := \frac{1+\sqrt{5}}{2}$ ($\bar{\gamma} = \frac{1-\sqrt{5}}{2}$), on a

$$\begin{aligned}
\Delta &= \begin{vmatrix} 1 & \sqrt{3} & \gamma & \sqrt{3}\gamma \\ 1 & -\sqrt{3} & \gamma & -\sqrt{3}\gamma \\ 1 & \sqrt{3} & \overline{\gamma} & \sqrt{3}\overline{\gamma} \\ 1 & -\sqrt{3} & \overline{\gamma} & -\sqrt{3}\overline{\gamma} \end{vmatrix}^2 \\
&= 3^2 \begin{vmatrix} 1 & 1 & \gamma & \gamma \\ 1 & -1 & \gamma & -\gamma \\ 1 & 1 & \overline{\gamma} & \overline{\gamma} \\ 1 & -1 & \overline{\gamma} & -\overline{\gamma} \end{vmatrix}^2 \\
&= 3^2 \begin{vmatrix} 1 & 1 & \gamma & \gamma \\ 2 & 0 & 2\gamma & 0 \\ 2 & 0 & 1 & 1-2\gamma \\ 2 & 0 & 2-2\zeta & 0 \end{vmatrix} \begin{matrix} \\ L_1 + L_2 \\ L_2 + L_3 \\ L3 + L4 \end{matrix} \\
&= 3^2 \times 4^2 \times (1-2\gamma)^2 \times (1-2\gamma)^2 = (12 \times 5)^2.
\end{aligned}$$

Exercice 14

1. La famille $(1, \sqrt[3]{2}, \sqrt[3]{4})$ est libre comme $\sqrt[3]{2}$ est de degré 3; la division euclidienne par le polynôme $X^3 - 2$ de coefficient dominant inversible dans $\mathbb{Z}[X]$ donne le caractère générateur de cette famille.
2. K est un corps puisque $X^3 - 2$ est irréductible sur $\mathbb{Q}$. Une base de K sur $\mathbb{Q}$ est $(1, \sqrt[3]{2}, \sqrt[3]{4})$.
3. Soit $j = e^{\frac{2i\pi}{3}}$.

Les plongements complexes de K sont

$$\sigma_1 : K \longrightarrow \mathbb{C}; \quad a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\sqrt[3]{2} + c\sqrt[3]{4},$$
$$\sigma_2 : K \longrightarrow \mathbb{C}; \quad a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + bj\sqrt[3]{2} + cj^2\sqrt[3]{4},$$
$$\sigma_3 : K \longrightarrow \mathbb{C}; \quad a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + bj^2\sqrt[3]{2} + cj\sqrt[3]{4}.$$

4. Déterminons la trace d'un élément $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ de K:

$$Tr(x) = Tr(a) + bTr(\sqrt[3]{2}) + cTr(\sqrt[3]{4}) = 3 + bTr\begin{bmatrix}0 & 0 & 2\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix} + cTr\begin{bmatrix}0 & 2 & 0\\ 0 & 0 & 2\\ 1 & 0 & 0\end{bmatrix} = 3a.$$

Déterminons la norme d'un élément $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ de K:

$N(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = (a+(b\sqrt[3]{2}+c\sqrt[3]{4}))(a+(jb\sqrt[3]{2}+cj^2\sqrt[3]{4}))(a+(bj^2\sqrt[3]{2}+cj\sqrt[3]{4}))$.

En développant on obtient

$$N(x) = a^3 + a^2Tr(b\sqrt[3]{2} + c\sqrt[3]{4}) + aZ + N(b\sqrt[3]{2} + c\sqrt[3]{4}),$$

où

$Z = (bj\sqrt[3]{2}+cj^2\sqrt[3]{4})(bj^2\sqrt[3]{2}+cj\sqrt[3]{4})+(b\sqrt[3]{2}+c\sqrt[3]{4})(bj^2\sqrt[3]{2}+cj\sqrt[3]{4})+(b\sqrt[3]{2}+c\sqrt[3]{4})(bj\sqrt[3]{2}+cj^2\sqrt[3]{4})$,

donc

$$Z = -6bc.$$

Enfin, on calcule $N(b\sqrt[3]{2} + c\sqrt[3]{4}) = 2b^3 + 4c^3$ (voir la page 53 "Anneaux d'entiers" sur le site de C. Mourougane).

On obtient finalement, et puisque $Tr(\sqrt[3]{2}) = Tr(\sqrt[3]{4}) = 0$,

$$N(x) = a^3 + 2b^3 + 4c^3 - 6abc.$$

5. La base $(1, \sqrt[3]{2}, \sqrt[3]{4})$ est constituée d'entiers algébriques.

Son discriminant est donné par la formule

$$Disc(1, \sqrt[3]{2}, \sqrt[3]{4}) = (\det(\sigma_i(\sqrt[3]{2})^l)_{1\leq i\leq 3, 0\leq l\leq 2})^2.$$

Le calcul du carré de ce déterminant 3×3 donne la valeur $-108 = -(2)^2 * (3)^3$.

Maintenant, un théorème du cours affirme que si la famille $(1, \sqrt[3]{2}, \sqrt[3]{4})$ n'est pas une $\mathbb{Z}$-base de l'anneau des entiers de K, alors il existe un entier de K de la forme $\frac{1}{2}(\lambda_1 + \lambda_2\sqrt[3]{2} + \lambda_3\sqrt[3]{4})$, pour $0 \leq \lambda_i \leq 1$ ou de la forme $\frac{1}{3}(\mu_1 + \mu_2\sqrt[3]{2} + \mu_3\sqrt[3]{4})$, pour $0 \leq \mu_i \leq 2$.

On montre finalement que la famille $(1, \sqrt[3]{2}, \sqrt[3]{4})$ est une $\mathbb{Z}$-base de l'anneau des entiers de K, par contraposée, ceci revient à prouver qu'aucun nombre de la forme $\frac{1}{2}(\lambda_1 + \lambda_2\sqrt[3]{2} + \lambda_3\sqrt[3]{4})$, pour $0 \leq \lambda_i \leq 1$, ou $\frac{1}{3}(\mu_1 + \mu_2\sqrt[3]{2} + \mu_3\sqrt[3]{4})$, pour $0 \leq \mu_i \leq 2$, n'est un entier algébrique.

Faisons-le pour les nombres $\frac{1}{3}(\mu_1 + \mu_2\sqrt[3]{2} + \mu_3\sqrt[3]{4})$, les autres sont laissés au lecteur. Il suffit de vérifier que la norme $\frac{1}{27}(\mu_1^3 + 2\mu_2^3 + 4\mu_3^3 - 6\mu_1\mu_2\mu_3)$ n'est pas un entier algébrique pour toutes les valeurs possibles des μ_i ...

Remarque: L'équivalence des formules pour la trace et la norme de x : somme des conjugués et trace de l'endomorphisme de multiplication par x (resp. produit des conjugués et déterminant de cet endomorphisme) est traitée à l'exercice 7.