XI.— Entiers algébriques

On dira qu'un nombre $z \in \mathbb{C}$ est un *entier algébrique* s'il est racine d'un polynôme unitaire à coefficients entiers.

Montrer que si $\alpha \in \mathbb{Q}$ est un entier algébrique, alors $\alpha \in \mathbb{Z}$.

Exercice 1 *a) Soient α, β deux entiers algébriques. Montrer que si $F(X,Y)$ est un polynôme à coefficients entiers, alors $F(\alpha,\beta)$ est aussi à coefficients entiers.*

b) Montrer qu'un nombre algébrique est entier si et seulement si son polynôme minimal unitaire est à coefficients entiers.

c) Soient $f, g \in \mathbb{Q}[X]$ deux polynômes unitaires tels que $fg \in \mathbb{Z}[X]$. Montrer que f, g sont à coefficients entiers.

Exercice 2 *Soit $d \neq 0$ un entier sans facteur carré. On note $\mathfrak{O}$ l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$.*

Montrer que :

$$\mathfrak{O} = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} \text{ si } d \neq 1 \bmod 4, \\ \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} \text{ si } d = 1 \bmod 4. \end{cases}$$

Exercice 3 *Soit A une matrice carrée à coefficients entiers telle que tous les coefficients de $A - I$ sont divisibles par $n \geq 2$. On suppose que $A \neq I$.*

a) Montrer que si $n > 2$, $A^m \neq I$ pour tout $m > 0$.

b) Si $n = 2$ et si $A^2 \neq I$, montrer que $A^m \neq I$ pour tout $m > 0$.

c) En déduire que pour tout r, il n'y a qu'un nombre fini de sous-groupes finis de $\mathrm{GL}_r(\mathbb{Z})$ à isomorphisme près.

Exercice 4 *Soit $f = X^n + a_1X^{n-1} + ... + a_n$ un polynôme à coefficients entiers unitaire. Montrer que le discriminant de f vérifie : $\Delta(f) = 0$ ou $1 \bmod 4$.*

(indications : introduire $\delta_1 := \prod_{i<j}(x_i + x_j)$; vérifier que δ_1 est un entier et que $\Delta(f) - \delta_1^2 = 4U(x_1, ..., x_n)$ où U est un polynôme à coefficients entiers symétrique).

Exercice 5 (Entiers des corps cyclotomiques) *a) Montrer que le discriminant du polynôme $\Phi_n(X)$ est :*

$$(-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\displaystyle\prod_{\substack{p|n \\ p \text{ premier}}} p^{\frac{\varphi(n)}{p-1}}}$$

b) Soient p un nombre premier et z une racine primitive $p-$ième de l'unité.

On note A l'anneau des entiers de $\mathbb{Q}(z)$. Montrer que :

$$p = (1-z)...(1-z^{p-1})$$

et en déduire que :

$$A(1-z) \cap \mathbb{Z} = p\mathbb{Z}$$

Montrer que pour tout $y \in A$, $\mathrm{tr}(y(1-z)) \in p\mathbb{Z}$.

On suppose que $x = a_0 + ... + a_{p-2}z^{p-2}$ est entier sur $\mathbb{Z}$ avec les $a_i \in \mathbb{Q}$. En calculant $\mathrm{tr}(x(1-z)$, montrer que $a_0 \in \mathbb{Z}$ puis que tous les a_i sont entiers (indication : calculer d'abord $\mathrm{tr}(z^j)$, $0 \leq j \leq p-1$). En déduire que $A = \mathbb{Z}[z]$.

c) Traiter le cas où z est une racine primitive p^r-ième de l'unité.

d) Traiter le cas général : montrer que si z est une racine primitive $n-$ième de l'unité, alors $\mathbb{Z}[z]$ est l'anneau des entiers de $\mathbb{Q}(z)$.