Fiche XII exo. 3 :

Soit $P := X^7 - 56X - 48$.

Rappelons deux formules pour le déterminant d'un polynôme unitaire de degré n (*cf.* fiche X (ATTENTION ! signe à corrigé (version correcte en ligne))) :

$$\Delta_P = (-1)^{n(n-1)/2} \prod_i (P'(x_i))$$

où les x_i sont les racines de P ;

$$\Delta_P = (-1)^{n(n-1)/2} n^n \prod_j P(y_j)$$

où les y_j sont les racines de P'.

Ici il est plus facile de calculer les racines de P' :

$$P' = 7X^6 - 56$$

ses racines y_j vérifient : $y_j^6 = 56/7 = 8$. Donc :

$$\begin{aligned}\Delta_P &= -7^7 \prod_{j=1}^{6} (y_j^7 - 56y_j - 48) \\ &= -7^7 \prod_j (y_j(8-56) - 48) \\ &= -7^7.48^6 \prod_j (y_j + 1)\end{aligned}$$

Or $P' = 7\prod_j (X - y_j)$. Donc $\prod_j (y_j + 1) = P'(-1)/7 = -7$. D'où : $\Delta_P = 7^8.48^6 \in (\mathbb{Q}^\times)^2$.

Donc le groupe de Galois de P sur $\mathbb{Q}$, noté G est contenu dans A_7.

En appliquant le critère d'Eisenstein à $P(X-1)$, on voit que P est irréductible.

Donc G est transitif et donc $7||G|$ donc G contient un $7-$cycle (les éléments d'ordre 7 dans S_7 sont les $7-$cycles).

La factorisation $\bmod 23$ montre que G contient un $3-$cycle.

On peut supposer que G contient le $7-$cycle $s = (1234567)$. Comme G agit transitivement sur $\{1,2,3,4,5,6,7\}$, on peut supposer que G contient un $3-$cycle de la forme :

$$t = (1ij)$$

$1 < i \neq j \leq 7$. Or s^{i-1} est encore un $7-$cycle (car 7 est premier) qui commence par :

$$(1i \cdot \cdot \cdot \cdot \cdot) \ .$$

Quitte à renuméroter (ce qui revient à remplacer G par un de ses conjugués), on peut donc supposer que G contient :

$$s = (1234567) \text{ et } t = (12j)$$

avec $3 \leq j \leq 7$.

Or :

$$\langle (123), (1234567) \rangle = A_7 \tag{1}$$

car $(123)^{-1}(1234567) = (34567)$ donc $(12k) \in \langle (123), (1234567) \rangle$ pour tout $3 \leq k \leq 7$ et les $3-$cycles $(12k)$ engendrent A_7.

Remarque : On en déduit plus généralement que si a est un $3-$cycle de la forme (ijk) et si b est un $7-$cycle qui commence par $(ijk...)$, alors $\langle a, b \rangle = A_7$.

On a aussi

$$\Big((124)(1234567)^3\Big)^2 = (34)(67)$$
$$\Rightarrow (123) \in \langle (124), (1234567) \rangle$$
$$\Rightarrow \langle (124), (1234567) \rangle = A_7$$

d'après (1).

On a encore :

$$((125)(1234567))^{-3} = (1253647)$$
$$\Rightarrow \langle (125), (1234567) \rangle \supseteq \langle (125), (1253647) \rangle$$
$$\Rightarrow \langle (125), (1234567) \rangle = A_7$$

d'après la remarque ci-dessus.

On a de plus :

$$\Big((126)^{-1}(1234567)^5\Big)^2 = (34)(67)$$
$$\Rightarrow (127) \in \langle (126), (1234567) \rangle$$

or :

$$\langle (127), (1234567) \rangle = A_7$$

en effet : d'une part :

$$(127)^{-1}(1234567) = (23456)$$
$$\Rightarrow (147) \in \langle (127), (1234567) \rangle$$

d'autre part : $(1234567)^3 = (147...)$ et on peut utiliser la remarque ci-dessus.

On a donc bien :

$$\langle (126), (1234567) \rangle = \langle (127), (1234567) \rangle = A_7 \ .$$

Toute démonstration plus courte sera bienvenue !

Finalement on en déduit que $G = A_7$.

Entiers algébriques :

Soient $A \subseteq B$ une inclusion d'anneaux (commutatifs avec des unités). On dit qu'un élément $b \in B$ est *entier sur A ou entier algébrique sur A* s'il existe $d \geq 1$, $a_1, ..., a_d \in A$ tels que :

$$b^d + a_1 b^{d-1} + ... + a_d = 0 \ .$$

Exemples :

— Pour tout entier s, $\sqrt{s}$ est entier sur $\mathbb{Z}$ car

$$(\sqrt{s})^2 - s = 0$$

.

— Soit $p/q \in \mathbb{Q}$ entier sur $\mathbb{Z}$. On suppose que la fraction est réduite *i.e.* $p, q \in \mathbb{Z}$, $q > 0$ et p, q sont premiers entre eux.

Soient $d \geq 1$, $a_1, ..., a_d \in \mathbb{Z}$ tel que :

$$(p/q)^d + a_1 (p/q)^{d-1} + ... + a_d = 0 \ .$$

Si on multiplie par q^d on obtient :

$$p^d + a_1 q p^{d-1} + ... + a_d q^d = 0$$

et donc $q | p^d$. D'après le lemme de Gauss, puisque p, q sont premiers entre eux, $q = 1$ et $p/q \in \mathbb{Z}$.

On dit que $\mathbb{Z}$ est intégralement clos (sous-entendu : dans son corps des fractions $\mathbb{Q}$).

Plus généralement, la même démonstration marche, mutatis mutandis, pour un anneau factoriel A et son corps des fractions K à la place de $\mathbb{Z}$ et de $\mathbb{Q}$.

Exo. 1 :

a) Soient $\alpha, \beta \in \mathbb{C}$ des entiers algébriques sur $\mathbb{Z}$. Alors $\alpha + \beta$ est aussi entier sur $\mathbb{Z}$.

En effet, soient :

$$P(X) = X^m + p_1 X^{m-1} + ... + p_m, Q(X) = X^n + q_1 X^{n-1} + ... + q_n \in \mathbb{Z}[X]$$

tels que :

$$P(\alpha) = Q(\beta) = 0 \ .$$

Notons $\alpha_1, ..., \alpha_m$, $\beta_1, ..., \beta_n$ les racines de P, Q dans $\mathbb{C}$:

$$P(X) = \prod_{i=1}^{m}(X - \alpha_i) \; Q(X) = \prod_{j=1}^{n}(X - \beta_j)$$

(on supposera que $\alpha_1 = \alpha$, $\beta_1 = \beta$).

Considérons le polynôme :

$$F(X) := \prod_{\substack{1 \le i \le m \\ 1 \le j \le n}} (X - \alpha_i - \beta_j) \ .$$

Si on développe, on trouve :

$$F(X) = X^{mn} + \sum_{k=1}^{mn} f_k(\alpha_1, ..., \alpha_m; \beta_1, ..., \beta_n) X^{mn-k}$$

où chaque f_k est un polynôme, *à coefficients entiers*, symétrique en les α_i et symétrique en les β_j.

Donc chaque f_k peut s'exprimer comme un polynôme *à coefficients entiers* en les fonctions symétriques élémentaires :

$$\sigma_1(\alpha_1, ..., \alpha_m), ..., \sigma_m(\alpha_1, ..., \alpha_m)$$

$$\sigma_1(\beta_1, ..., \beta_n), ..., \sigma_n(\beta_1, ..., \beta_n)$$

(on rapelle que $\sigma_l(t_1, ..., t_r) = \sum_{1 \le i_1 < ... < i_l \le r} t_{i_1} ... t_{i_l}$).

Or, on a :

$$\sigma_i(\alpha_1, ..., \alpha_m) = \pm p_i \in \mathbb{Z}$$

$$\sigma_j(\beta_1, ..., \beta_n) = \pm q_j \in \mathbb{Z}$$

Donc le polynôme $F(X)$ est à coefficients entiers. Il est clair que $F(\alpha+\beta) = 0$ et donc $\alpha + \beta$ est entier sur $\mathbb{Z}$.

On montre de même que $\alpha\beta$ est entier sur $\mathbb{Z}$.

c) Soient $f, g \in \mathbb{Q}[X]$ *unitaires* tels que $fg \in \mathbb{Z}[X]$. Alors $f, g \in \mathbb{Z}[X]$.

En effet, les coefficients de f, par exemple, sont des polynômes à coefficients entiers en les racines de f (car f est unitaire). Or les racines de f sont des racines de fg donc sont entières sur $\mathbb{Z}$. Donc les coefficients de f sont entiers sur $\mathbb{Z}$. Or ce sont aussi des rationnels donc les coefficients de f sont dans $\mathbb{Z}$.

b) Soit $\alpha \in \mathbb{C}$ entier sur $\mathbb{Z}$. Alors α est en particulier algébrique sur $\mathbb{Q}$ et son polynôme minimal unitaire sur $\mathbb{Q}$, notons-le M_α, est à coefficients entiers. En effet, soit $P \in \mathbb{Z}[X]$ unitaire qui annule α. On a $M_\alpha | P$ dans $\mathbb{Q}[X]$. Donc d'après la question c), $M_\alpha \in \mathbb{Z}[X]$.

Exo. 2 : Soit $d \neq 0, 1$ un entier sans facteur carré. On note $K := \mathbb{Q}(\sqrt{d})$ et $\mathfrak{O}$ l'anneau des entiers de K (l'anneau formé par les éléments de K entiers sur $\mathbb{Z}$).

Soit $\sigma : K \to K$, l'automorphisme de corps qui envoie $\sqrt{d}$ sur $-\sqrt{d}$. Soit $x = a + b\sqrt{d} \in \mathfrak{O}$, $a, b \in \mathbb{Q}$.

L'élément $\sigma(x) = a - b\sqrt{d}$ (le conjugué de x si $b \neq 0$) est aussi entier sur $\mathbb{Z}$ car il vérifie la même équation de dépendance intégrale que x.

Donc $x + \sigma(x) = 2a$ et $x\sigma(x) = a^2 - db^2$ sont aussi entiers sur $\mathbb{Z}$. Or, $x + \sigma(x)$, $x\sigma(x) \in \mathbb{Q}$ donc :

$$(*) \quad 2a,\ a^2 - db^2 \in \mathbb{Z}$$

Réciproquement si $2a$, $a^2 - db^2 \in \mathbb{Z}$, alors $x \in \mathfrak{O}$ car x est racine du polynôme $(X - x)(X - \overline{x}) = X^2 - 2aX + (a^2 - db^2) \in \mathbb{Z}[X]$.

$(*) \Rightarrow 4a^2 - 4db^2 \in \mathbb{Z} \Rightarrow 4db^2 = d(2b)^2 \in \mathbb{Z}$. Mais alors, $2b \in \mathbb{Z}$. En effet, si $2b = r/s$ avec r, s des entiers premiers entre eux, alors $d(2b)^2 \in \mathbb{Z} \Leftrightarrow dr^2/s^2 \in \mathbb{Z} \Leftrightarrow s^2 | dr^2 \Leftrightarrow s^2 | d$ (car r^2, s^2 sont premiers entre eux). Or d est sans facteur carré donc $s = \pm 1$ et $2b \in \mathbb{Z}$.

Soient $u, v \in \mathbb{Z}$ tels que : $a = u/2, b = v/2$.

On a $(*) \Leftrightarrow u^2 - dv^2 \in 4\mathbb{Z}$.

Si v est pair, alors u aussi et $a = u/2, b = v/2 \in \mathbb{Z}$. Si v est impair, alors $v^2 = 1 \bmod 4$ et donc $u^2 = d \bmod 4$. Or, d est sans facteur carré donc n'est pas divisible par 4. Ainsi $u^2 = 1 \bmod 4$ (un carré $\bmod 4$ est soit 0 soit $1 \bmod 4$).

En résumé, si $d \neq 1 \bmod 4$, alors $x \in \mathfrak{O} \Rightarrow x = a + b\sqrt{d}$ avec $a, b \in \mathbb{Z}$ et dans ce cas on a :

$$\mathfrak{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$$

.

Si $d = 1 \bmod 4$, alors $x = u/2 + v/2\sqrt{d}$ avec $u, v \in \mathbb{Z}$ de même parité. Dans ce cas, on vérifie facilement que $\frac{1+\sqrt{d}}{2} \in \mathfrak{O}$ donc on a bien :

$$\mathfrak{O} = \mathbb{Z} \oplus \mathbb{Z}\frac{1 + \sqrt{d}}{2} \ .$$

Par exemple si $d=-3$, $K=\mathbb{Q}(\sqrt{-3})=\mathbb{Q}(\frac{-1\pm i\sqrt{3}}{2})$ et $\mathfrak{O}=\mathbb{Z}+\mathbb{Z}\frac{1\pm i\sqrt{3}}{2})=\mathbb{Z}[\frac{-1+i\sqrt{3}}{2}]$.

Plus généralement, nous allons voir que si z est une racine primitive $n-$ième de l'unité, l'anneau des entiers du corps cyclotomique $\mathbb{Q}(z)$ est $\mathbb{Z}[z]$ ...

Exo. 5 :

Calcul du discriminant du polynôme cyclotomique :

Soit $n\geq 2$. Soit Δ le discriminant de $\Phi_n(X)$, le $n-$ième polynôme cyclotomique. On connaît déjà le signe de Δ : c'est $(-1)^{\varphi(n)/2}$ car $\Phi_n(X)$ n'a que des racines complexes conjuguées (*cf.* la fiche X).

Calculons $|\Delta|$:

$$|\Delta|=\prod_{\epsilon}|\Phi_n'(\epsilon)|$$

où ϵ décrit les racines primitives $n-$ièmes de l'unité.

Or, d'après la formule d'inversion de Möbius :

$$\Phi_n(X)=\prod_{d|n}(X^d-1)^{\mu(n/d)}$$

$$=(X^n-1)\prod_{\substack{d|n\\ d<n}}(X^d-1)^{\mu(n/d)}$$

où $\mu(n/d)=\begin{cases}(-1)^r \text{ si } n/d=p_1...p_r \text{ avec } p_1<...<p_r \text{ premiers}\\ 0 \text{ sinon}\end{cases}$.

Donc :

$$\Phi_n'(X)=nX^{n-1}\prod_{\substack{d|n\\ d<n}}(X^d-1)^{\mu(n/d)} \bmod (X^n-1)$$

$$\Rightarrow \Phi_n'(\epsilon)=n\epsilon^{n-1}\prod_{\substack{d|n\\ d<n}}(\epsilon^d-1)^{\mu(n/d)}$$

pour toute racine primitive $n-$ième de l'unité ϵ.

Ainsi :

$$|\Delta|=n^{\varphi(n)}\prod_{\substack{d|n\\ d<n}}\prod_{\epsilon}|\epsilon^d-1|^{\mu(n/d)}$$

or, lorsque ϵ est une racine primitive $n-$ième de l'unité, ϵ^d est une racine primitive $(n/d)-$ième de l'unité. Plus précisément, si on note Π_k l'ensemble des racines primitives $k-$ièmes de l'unité, le morphisme :

$$\Pi_n \to \Pi_{n/d} \ \ \epsilon \mapsto \epsilon^d$$

est surjectif.

En effet, posons $k := n/d$; on peut identifier Π_n à $(\mathbb{Z}/n\mathbb{Z})^\times$ et Π_k à $(\mathbb{Z}/k\mathbb{Z})^\times$ et le morphisme ci-dessus au morphisme de groupes :

$$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/k\mathbb{Z})^\times \ \ x \bmod n \mapsto x \bmod k \ .$$

Ce morphisme est surjectif ! C'est facile si $n = p^r$ pour un certain nombre premier p. Pour le cas général : $n = p_1^{r_1}...p_t^{r_t}$ pour des nombres premiers distincts p_i, $k = p_1^{s_1}...p_t^{s_t}$ avec $s_i \leq r_i$ et on utilise le théorème des isomorphismes chinois :

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{r_1})^\times \times ... \times (\mathbb{Z}/p_s^{r_s})$$

... on obtient un produit cartésien de morphismes surjectifs.

Donc le morphisme (de groupes (on munit Π_n, Π_k des structures de groupes de $(\mathbb{Z}/n\mathbb{Z})^\times, (\mathbb{Z}/k\mathbb{Z})^\times)$) :

$$\Pi_n \to \Pi_k \ \ \epsilon \mapsto \epsilon^d$$

est surjectif de noyau de cardinal :

$$|\text{noyau}| = \frac{|\Pi_n|}{|\Pi_k|}$$

$$= \varphi(n)/\varphi(k) = \varphi(n)/\varphi(n/d) \ .$$

Par conséquent :

$$\prod_\epsilon |\epsilon^d - 1| = \prod_{\epsilon'} |\epsilon' - 1|^{\varphi(n)/\varphi(n/d)}$$

où ϵ' décrit les racine primitives $(n/d)-$ièmes de l'unité.

Donc :

$$\prod_\epsilon |\epsilon^d - 1| = \prod_{\epsilon'} |\epsilon' - 1|^{\varphi(n)/\varphi(n/d)} = \Phi_{n/d}(1)^{\varphi(n)/\varphi(n/d)} \ .$$

Or pour un entier m, $\Phi_m(1) = \begin{cases} p \text{ si } m = p^r,\ r \geq 1,\ p \text{ premier} \\ 1 \text{ sinon} \end{cases}$. En effet d'une part :

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}) = 1 + X^{p^{r-1}} + ... + X^{p^{r-1}(p-1)} \ ,$$

et d'autre part, si $n = p_1^{a_1}...p_r^{a_r}$, avec des nombres premiers p_i deux à deux distincts :

$$n = \frac{X^n - 1}{X - 1}|_{X=1} = \prod_{\substack{d|n \\ d>1}} \Phi_d(1)$$

$$= \prod_i p_i^{a_i} \prod_d \Phi_d(1)$$

où d décrit les diviseurs de n qui ne sont pas une puissance d'un nombre premier. Ainsi $\Phi_d(1) = \pm 1$ si d n'est pas une puissance d'un nombre premier et donc dans ce cas $\Phi_d(1) = 1$ (par la formule d'inversion de Möbius il est facile de voir que $\Phi_d(1) \geq 0$).

Pour résumer :

$$|\Delta| = n^{\varphi(n)} \prod_{p \text{ premier}} \prod_{a>0} \prod_{\substack{d|n \\ n/d=p^a}} (p^{\varphi(n)/\varphi(p^a)})^{\mu(p^a)}$$

$$= n^{\varphi(n)} \prod_{\substack{p|n \\ p \text{ premier}}} p^{-\varphi(n)/(p-1)} \ .$$

Conclusion le discriminant du polynôme cyclotomique $\Phi_n(X)$ est donné par la formule :

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