

EXAMEN , LUNDI 10 JANVIER 2011 : CORRIGÉ SUCCINT

A–

1. Le groupe abélien G/H est le conoyau de la matrice $H = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 3 \end{pmatrix}$. Par opérations élémentaires sur les lignes et les colonnes on obtient la forme normale de Smith $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 10 \end{pmatrix}$. Le groupe G/H est fini de cardinal 20 ; les facteurs invariants sont 2 et 10.

2. Le calcul de la forme normale s'écrit : $PHQ = D$, où Q (resp. P) est obtenu en appliquant à la matrice unité les opérations élémentaires précédentes sur les colonnes (resp. lignes). On a (par exemple) le résultat avec :

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -4 & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 0 & -1 \\ 0 & -1 & -1 \end{pmatrix}$$

Les vecteurs colonnes de $P^{-1} = \begin{pmatrix} 3 & 4 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ donnent une base répondant à la question.

B–

1. Le polynôme $P = X^3 + X^2 - 2X - 1$ est un polynôme à coefficients entiers, primitif. Il est donc irréductible sur $\mathbb{Q}$ si et seulement s'il l'est sur $\mathbb{Z}$. Le polynôme P étant primitif et de degré 3, une éventuelle réduction dans $\mathbb{Z}[X]$ aurait un facteur de degré 1 : $aX + b$, avec $a|1$ et $b|-1$. Cela donnerait une racine de P égale à ± 1 , ce qui est exclu.
2. Le discriminant de P est :

$$\Delta = (-1)^{\frac{3 \times 2}{2}} \begin{vmatrix} -1 & 0 & -2 & 0 & 0 \\ -2 & -1 & 2 & -2 & 0 \\ 1 & -2 & 3 & 2 & -2 \\ 1 & 1 & 0 & 3 & 2 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = 49$$

3. Le groupe de Galois G de P est un sous-groupe non trivial du groupe symétrique $\mathcal{S}_3$. Le discriminant Δ étant un carré dans $\mathbb{Q}$, le groupe de Galois est contenu dans le groupe alterné $\mathcal{A}_3$ qui est cyclique d'ordre 3 et n'a pas de sous-groupe propre. En conclusion, le groupe G est cyclique d'ordre 3.

C–

1. Le corps $\mathbb{Q}(\alpha)$ est contenu dans $\mathbb{R}$, il ne contient donc pas ζ ; l'extension $(\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha))$ est non triviale i.e de degré différent de 1. La relation $\zeta^2 - \alpha\zeta + 1$ montre que l'extension est quadratique (degré 2), de polynôme minimal $X^2 - \alpha X + 1$.
2. (a) Le polynôme minimal de ζ sur $\mathbb{Q}$ est le polynôme cyclotomique

$$\phi_7 = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6.$$

- (b) La tour $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$ nous montre que l'extension $(\mathbb{Q}(\alpha) : \mathbb{Q})$ est de degré 3. Le polynôme minimal de α sur $\mathbb{Q}$ est obtenu avec la relation :

$$1 + (\zeta + \zeta^6) + (\zeta^2 + \zeta^5) + (\zeta^3 + \zeta^4) = 1 + \alpha + (\alpha^2 - 2) + \alpha^3 - \alpha$$

Le polynôme minimal est : $P = X^3 + X^2 - 2X - 1$.

3. L'extension $(\mathbb{Q}(\alpha) : \mathbb{Q})$ est galoisienne. On peut voir que $\mathbb{Q}(\alpha)$ est corps de décomposition de P (en caractéristique 0 tout polynôme est séparable); les autres racines sont $\zeta^2 + \zeta^{-2} = \alpha^2 - 2$ et $\zeta^3 + \zeta^{-3} = \alpha^3 - 3\alpha$. On peut aussi considérer la correspondance de Galois. Le groupe de Galois $\text{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ est isomorphe au groupe de permutation $\mathcal{S}_3$. L'extension $(\mathbb{Q}(\alpha) : \mathbb{Q})$ correspond au seul sous-groupe de cardinal 3, le groupe alterné $\mathcal{A}_3$, qui est un sous-groupe normal.

D-

- Sur $\mathbb{F}_2[X]$, les polynômes irréductibles de degré au plus 3 sont : X , $X + 1$, $X^2 + X + 1$, $X^3 + X^2 + 1$, $X^3 + X + 1$. Le polynôme $P = X^6 + X^3 + 1$ n'est divisible par aucun d'entre eux. Il est irréductible dans $\mathbb{F}_2[X]$.
- (a) Le degré de l'extension $(K : \mathbb{F}_2)$ est 6. Le cardinal de K est $2^6 = 64$.
 (b) Le groupe multiplicatif K^* est de cardinal 63. L'ordre d'un élément dans ce groupe divise donc $63 = 7 \times 9$. On a $\beta = \alpha^3 \neq 1$, et $\alpha^9 = \beta^3 = 1$. Donc α est d'ordre 9 et β est d'ordre 3.
 (c) $\gamma^8 = \gamma$ (on peut utiliser l'homomorphisme de Frobenius); γ est d'ordre 7.
- Le groupe $\text{Gal}(K, \mathbb{F}_2)$ est cyclique d'ordre 6, engendré par l'homomorphisme de Frobenius $F : x \mapsto x^2$.
- Les sous-corps de K correspondent aux sous-groupes de $\text{Gal}(K, \mathbb{F}_2)$. En plus de $\mathbb{F}_2$ et K , on a deux sous-corps correspondant aux sous-groupes engendrés par F^3 et F^2 . Ces corps de cardinal 4 et 8 sont respectivement corps de décomposition de $X^4 - X$ et $X^8 - X$. On obtient $F_4 = \{0, 1, \beta, \beta^2\}$ et $F_8 = \{0, 1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5, \gamma^6\}$.

E-

- La variation de la fonction $x \mapsto x^5 - 6x + 3$ montre que $X^5 - 6X + 3$ a trois racines réelles.
- (a) Si α est une racine de P dans L , on a une tour d'extension : $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset L$. La première extension est de degré d car P est le polynôme minimal de α . L'extension $(L : \mathbb{Q})$ est galoisienne. Son degré est le cardinal du groupe de Galois G . C'est un multiple de d par multiplicativité du degré pour les tours d'extension.
 (b) G contient un sous-groupe H d'ordre d^k , avec $k > 0$ (théorème de Sylow). Un élément non trivial u de H est d'ordre d^l , $0 < l \leq k$; $u^{d^{l-1}}$ est d'ordre d .
 (c) Les deux racines non réelles de P sont conjuguées. La conjugaison définit un automorphisme de L d'ordre 2.
 (d) Le groupe de Galois G est isomorphe à un sous-groupe du groupe symétrique $\mathcal{S}_d$. Ce sous-groupe contient une transposition et un cycle d'ordre d ; ceux-ci engendrent $\mathcal{S}_d$.
- Le groupe de Galois sur $\mathbb{Q}$ du polynôme $X^5 - 6X + 3$ est isomorphe au groupe symétrique $\mathcal{S}_5$. Le sous-groupe $\mathcal{A}_5$ est simple (donc non résoluble). Le groupe $\mathcal{S}_5$ ne contient que $\mathcal{A}_5$ comme sous-groupe distingué propre : il n'est pas résoluble.