

Université de Bretagne Occidentale
UFR Sciences et Techniques
Département de Mathématiques
MASTER 1, MATHÉMATIQUES

ALGÈBRE

Examen terminal, 3 janvier 2005, 13h00–17h00

CORRIGE et BAREME

Question de cours. (20 μ t)

Exercice 1. a. Décomposer l'entier 2005 en facteurs premiers : $2005 = 5 \times 401$ (**1 μ t**). Soit s le nombre de 5-sous-groupes de Sylow de G . D'après les Théorèmes de Sylow, $s \equiv 1 \pmod{5}$ et s divise 401. Comme 401 est premier, s est égal à 1 ou 401 (**2 μ t**). Montrons que $s \neq 1$. Supposons, par l'absurde, que $s = 1$. Dans ce cas, G ne contient qu'un seul sous-groupe N de cardinal 5. Le sous-groupe N est donc nécessairement distingué dans G (**2 μ t**). D'après Cauchy, G contient aussi un sous-groupe de cardinal 401 (**2 μ t**). Par conséquent, G est produit semi-direct de N et H (**1 μ t**). Ce produit semi-direct est forcément trivial (**2 μ t**). En particulier, G est commutatif (**1 μ t**). Contradiction. Cela montre que $s = 401$, i.e., que le nombre de 5-sous-groupes de Sylow de G est égal à 401.

b. Tout élément d'ordre 5 est contenu dans un (**1 μ t**) et un seul (**1 μ t**) sous-groupe de G de cardinal 5. Tout sous-groupe de G de cardinal 5 contient exactement 4 éléments d'ordre 5 (**1 μ t**). Il s'ensuit que le nombre d'éléments de G d'ordre 5 est égal à $4 \times 401 = 1604$ (**1 μ t**).

Exercice 2. a. D'après le cours, $\{1\} \times H$ est un sous-groupe de $N \rtimes H$, et la loi de groupe induite sur $\{1\} \times H$ coïncide avec celle de H . Comme H' est un sous-groupe de H , il suit que $\{1\} \times H'$ est un sous-groupe de $\{1\} \times H$, et donc aussi de $N \rtimes H$ (**2 μ t**).

Montrons que $\{1\} \times H'$ est distingué. Soit $(1, h') \in \{1\} \times H'$ et soit $(n, h) \in N \rtimes H$. On calcule

$$\begin{aligned}(n, h) \cdot (1, h') \cdot (n, h)^{-1} &= (n, hh') \cdot (\alpha(h^{-1})(n^{-1}), h^{-1}) = \\ &= (n \cdot \alpha(hh') \circ \alpha(h^{-1})(n^{-1}), hh'h^{-1}) = (n \cdot \alpha(hh'h^{-1})(n^{-1}), hh'h^{-1}) = \\ &= (n \cdot \text{id}(n^{-1}), hh'h^{-1}) = (1, hh'h^{-1}) \in \{1\} \times H',\end{aligned}$$

car $hh'h^{-1} \in H'$ et H' est contenu dans le noyau de α . Il s'ensuit que $\{1\} \times H'$ est distingué dans $N \rtimes H$ (**4 μ t**).

Exercice 5. a. Comme $\sqrt{2} \notin \mathbb{Q}$ et $\sqrt{2}^2 \in \mathbb{Q}$, l'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est de degré 2 (**1 pt**). Montrons que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Supposons, par l'absurde, que $\sqrt{3} = a + b\sqrt{2}$, pour certains $a, b \in \mathbb{Q}$. On a donc $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Comme $\sqrt{2} \notin \mathbb{Q}$, $2ab = 0$, i.e., $a = 0$ ou $b = 0$. Si $b = 0$, $\sqrt{3} \in \mathbb{Q}$ ce qui est absurde. Donc $a = 0$, et $\sqrt{3} = b\sqrt{2}$. Mais cela implique que $\sqrt{6} \in \mathbb{Q}$, ce qui est absurde également. Cela montre que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (**2 pt**). Comme $\sqrt{3}^2 \in \mathbb{Q}(\sqrt{2})$, le degré de l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$ est égal à 2. Part conséquent,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4 \text{ (1 pt)}.$$

b. Comme $\sqrt{2} + \sqrt{3} \in K$, on a bien l'inclusion $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq K$ (**1 pt**). Soit $K' = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, et montrons l'inclusion $K \subseteq K'$.

On vérifie facilement que $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$. Donc

$$\sqrt{2} = \frac{1}{2}(\sqrt{2} + \sqrt{3})^3 - \frac{9}{2}(\sqrt{2} + \sqrt{3}) \in K', \text{ et}$$

$$\sqrt{3} = -\frac{1}{2}(\sqrt{2} + \sqrt{3})^3 + \frac{11}{2}(\sqrt{2} + \sqrt{3}) \in K'.$$

Par conséquent, $K \subseteq K'$ (**1 pt**).

c. On a $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$ et $(\sqrt{2} + \sqrt{3})^4 = 49 + 20\sqrt{6}$. Donc,

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 = -1.$$

Par conséquent, $\sqrt{2} + \sqrt{3}$ est racine du polynôme $X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$ (**1 pt**). Comme $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$, le polynôme minimal P de $\sqrt{2} + \sqrt{3}$ sur \mathbb{Q} est un polynôme unitaire de $\mathbb{Q}[X]$ de degré 4 divisant le polynôme $X^4 - 10X^2 + 1$. Il s'ensuit que $P = X^4 - 10X^2 + 1$ (**1 pt**).

d. Comme $\text{car}(\mathbb{Q}) = 0$, l'extension K/\mathbb{Q} est séparable (**1 pt**). Comme $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, K est le corps de décomposition du polynôme $(X^2 - 2)(X^2 - 3)$ sur \mathbb{Q} . Par conséquent, l'extension K/\mathbb{Q} est normale, et donc galoisienne (**1 pt**).

Soit σ l'automorphisme non trivial de l'extension $K/\mathbb{Q}(\sqrt{3})$, et τ celui de $K/\mathbb{Q}(\sqrt{2})$. On a $\sigma^2 = \text{id}$, $\tau^2 = \text{id}$ et $\sigma\tau = \tau\sigma$. Par conséquent, le sous-groupe de $\text{Gal}(K/\mathbb{Q})$ engendré par σ et τ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Comme ce sous-groupe est de cardinal 4, on a $\langle \sigma, \tau \rangle = \text{Gal}(K/\mathbb{Q})$. Par conséquent, $\text{Gal}(K/\mathbb{Q})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (**2 pt**).

e. Supposons, par l'absurde que $\alpha \in K$. On a donc aussi $\tau(\alpha) \in K$, et $\tau(\alpha)^2 = \tau(\alpha^2) = \tau(\sqrt{2} + \sqrt{3}) = \sqrt{2} - \sqrt{3}$ est négatif. Contradiction, car $\tau(\alpha) \in K \subseteq \mathbb{R}$ (**2 pt**).

f. Soit $Q = P(X^2) \in \mathbb{Q}[X]$. Comme $\sqrt{2} + \sqrt{3}$ est racine de P , α est racine de Q . D'après le e, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$. Comme Q est de degré 8 et unitaire, Q est le polynôme minimal de α sur \mathbb{Q} (**2 pt**).

g. Les racines de P dans \mathbb{C} sont $\pm\sqrt{2} \pm \sqrt{3}$. Comme $-\sqrt{2} + \sqrt{3} = (\sqrt{2} + \sqrt{3})^{-1}$ et $\sqrt{2} - \sqrt{3} = -(\sqrt{2} + \sqrt{3})^{-1}$, les racines de P dans \mathbb{C} sont aussi $\pm(\sqrt{2} + \sqrt{3})^{\pm 1}$. De plus, les racines de Q dans \mathbb{C} sont $\pm\alpha^{\pm 1}$ et $\pm i\alpha^{\pm 1}$. Par conséquent, le corps de décomposition L de Q sur \mathbb{Q} est le corps $\mathbb{Q}(\alpha, i\alpha) = \mathbb{Q}(\alpha, i)$ (**1 pt**). Comme $i \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, on a

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 8 = 16 \text{ (1 pt)}.$$

h. Soit φ l'automorphisme $\mathbb{Q}(i)$ -linéaire de L défini par $\varphi(\alpha) = i\alpha$. Il est clair que φ est d'ordre 4 dans $\text{Gal}(L/\mathbb{Q}(i))$. Le sous-groupe $\langle \varphi \rangle$ de $\text{Gal}(L/\mathbb{Q}(i))$ est donc distingué et isomorphe à $\mathbb{Z}/4\mathbb{Z}$ (**1 pt**).

Soit ψ l'automorphisme $\mathbb{Q}(i)$ -linéaire de L défini par $\psi(\alpha) = \alpha^{-1}$. Il est clair que ψ est d'ordre 2 dans $\text{Gal}(L/\mathbb{Q}(i))$ (**1 pt**). Comme $\psi \notin \langle \varphi \rangle$, on a

$$\langle \varphi \rangle \cap \langle \psi \rangle = \{1\} \text{ (1 pt)} \quad \text{et} \quad \langle \varphi \rangle \cdot \langle \psi \rangle = \text{Gal}(L/\mathbb{Q}(i)) \text{ (1 pt)}.$$

Comme $\psi\varphi\psi^{-1} = \varphi^3$, le groupe $\text{Gal}(L/\mathbb{Q}(i))$ est isomorphe au produit semi-direct non trivial de $\mathbb{Z}/4\mathbb{Z}$ avec $\mathbb{Z}/2\mathbb{Z}$, i.e., le groupe diédral D_4 (**2 pt**).

i. Comme $\mathbb{Q}(i)/\mathbb{Q}$ est galoisienne, le sous-groupe $\text{Gal}(L/\mathbb{Q}(i))$ de $\text{Gal}(L/\mathbb{Q})$ est distingué (**1 pt**), et isomorphe à D_4 d'après le h.

Comme l'extension $L/\mathbb{Q}(\alpha)$ est de degré 2, elle est galoisienne de groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Le sous-groupe $\text{Gal}(L/\mathbb{Q}(\alpha))$ de $\text{Gal}(L/\mathbb{Q})$ est donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (**1 pt**). Il n'est pas distingué car l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ n'est pas galoisienne (**1 pt**).

Comme $L = \mathbb{Q}(\alpha, i)$,

$$\text{Gal}(L/\mathbb{Q}(i)) \cap \text{Gal}(L/\mathbb{Q}(\alpha)) = \{1\} \text{ (1 pt)}.$$

Il s'ensuit que $\text{Gal}(L/\mathbb{Q}(i)) \cdot \text{Gal}(L/\mathbb{Q}(\alpha)) = \text{Gal}(L/\mathbb{Q})$ (**1 pt**), et que $\text{Gal}(L/\mathbb{Q})$ est isomorphe à un produit semi-direct non trivial $D_4 \rtimes (\mathbb{Z}/2\mathbb{Z})$ (**1 pt**).