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

ALGEBRE

Examen terminal, 9 janvier 2006, 13h30–17h30

CORRIGE et BAREME

Question de cours. (20 pts)

Exercice 1. La décomposition de 2006 en facteurs premiers est $2006 = 2 \times 17 \times 59$. Celle de 2006^2 est donc $2^2 \times 17^2 \times 59^2$ **(1 pt)**. Les groupes abéliens de cardinal 2006 à isomorphisme près sont, d'après le cours, les groupes suivants

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/59\mathbb{Z} \times \mathbb{Z}/59\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/3481\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/289\mathbb{Z} \times \mathbb{Z}/59\mathbb{Z} \times \mathbb{Z}/59\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/289\mathbb{Z} \times \mathbb{Z}/3481\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/59\mathbb{Z} \times \mathbb{Z}/59\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/3481\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/289\mathbb{Z} \times \mathbb{Z}/59\mathbb{Z} \times \mathbb{Z}/59\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/289\mathbb{Z} \times \mathbb{Z}/3481\mathbb{Z}$$

(1 pt pour chaque groupe) Ces groupes sont deux-à-deux non isomorphes. Il y a donc exactement 8 groupes abéliens de cardinal 2006^2 **(1 pt)**.

Exercice 2. Soit $f\colon S_5 \to G$ un morphisme. Le noyau de f est un sous-groupe distingué de S_5 **(1 pt)**. Or, d'après le cours, les seuls sous-groupes distingués de S_5 sont $\{1\}$, A_5 et S_5 **(1 pt)**. On doit montrer que $\ker(f) = S_5$. On raisonne par l'absurde. On suppose que $\ker(f) \neq S_5$. Donc $\ker(f) = \{1\}$ ou A_5.

Si $\ker(f) = \{1\}$, le morphisme f est injectif, et $\mathrm{im}(f)$ est donc un sous-groupe de G isomorphe à S_5 **(1 pt)**. Comme S_5 n'est pas commutatif, $\mathrm{im}(f)$ ne l'est pas non plus **(1 pt)**. Contradiction, car G est commutatif **(1 pt)**.

Si $\ker(f) = A_5$, le morphisme f induit un morphisme injectif $\overline{f}$ du quotient S_5/A_5 dans G **(1 pt)**. Comme S_5/A_5 est de cardinal 2, l'image $\mathrm{im}(\overline{f})$ est un sous-groupe de G de cardinal 2 **(1 pt)**. D'après le Théorème de Lagrange,

le cardinal de G est divisible par 2 **(1 pt)**. Contradiction, car le cardinal de G est impair **(1 pt)**.

Comme les deux cas $\ker(f) = \{1\}$ et $\ker(f) = A_5$ aboutissent à une contradiction, la seule possibilité est que $\ker(f) = S_5$, i.e., f est trivial **(1 pt)**.

Exercice 3. a. On pourrait suivre la méthode générale du cours, ou plus simplement la suivante. Soit $v_1' = v_1 - 2v_3 = (-8, 0)$ et $v_2' = v_2 - 3v_3 = (-16, 0)$. La famille v_1', v_2', v_3 est aussi génératrice de A. Comme $v_2' = 2v_1'$, la famille v_1', v_3 est toujours génératrice de A. Comme $v_1' = (-8, 0)$ et $v_3 = (16, 18)$, la famille v_1', v_3 est bien libre. Elle est donc une base de A **(6 pts)**.

b. Soit $v_3' = v_3 + 2v_1' = (0, 18)$. La famille v_1', v_3' est toujours une base de A. Du coup, A est le sous-groupe $(-8\mathbb{Z}) \times (18\mathbb{Z})$ de $\mathbb{Z} \times \mathbb{Z}$ **(1 pts)**. Le quotient $\mathbb{Z}^2/A$ est donc isomorphe à

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/18 \cong \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \cong \mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \textbf{(2 pts)}.$$

Ses diviseurs élémentaires sont $72, 2$ **(1 pt)**.

Exercice 4. a. D'après les Théorèmes de Sylow, le nombre de 7-sylows de G est congru à 1 (mod 7), et divise 6. Du coup, G contient exactement un 7-sylow **(2 pts)**.

b. Soit H un 3-sylow de G, et soit K un 7-sylow de G. Comme G ne contient qu'un seul 7-sylow, le 7-sylow K de G est distingué. Du coup, le sous-ensemble $N = HK$ de G est un sous-groupe **(1 pt)**. Comme 3 et 7 sont premiers entre eux, le cardinal de N est égal à 21 **(1 pt)**.

c. Comme N est d'indice 2 dans G, le sous-groupe N est distingué dans G **(1 pt)**.

d. Soit N' un autre sous-groupe de G de cardinal 21. Un 7-sylow de N' est de cardinal 7, et est donc aussi un 7-sylow de G **(1 pt)**. D'après le a, ce 7-sylow de G est égal à K. D'où $K \subseteq N'$ **(1 pt)**. Soit H' un 3-sylow de N'. On a $H'K = N'$ **(1 pt)**. Comme H' est de cardinal 3, H' est aussi un 3-sylow de G. D'après les Théorèmes de Sylow, il existe $g \in G$ tel que $gHg^{-1} = H'$ **(1 pt)**. Du coup,

$$gNg^{-1} = g(HK)g^{-1} = (gHg^{-1})(gKg^{-1}) = H'K = N' \quad \textbf{(1 pt)}.$$

e. Soit N' un sous-groupe de G de cardinal 21. D'après le d, il existe $g \in G$ tel que $gNg^{-1} = N'$ **(1 pt)**. D'après le c, $gNg^{-1} = N$ **(1 pt)**. Il suit que $N' = gNg^{-1} = N$.

Exercice 5. Supposons que $f\colon M \to N$ est surjectif. Comme A est non nul, A contient un idéal maximal I **(1 pt)**. Le morphisme f induit un morphisme de A-modules $\overline{f}\colon M/IM \to N/IN$ **(1 pt)**. Le morphisme $\overline{f}$ est A/I-linéair

(1 pt). de plus, $\overline{f}$ est surjectif car f l'est **(1 pt)**. Comme A/I est un corps **(1 pt)**, et M/IM et N/IN sont des A/I-espaces vectoriels de dimension finie **(1 pt)**, on a $\dim(M/IM) \geq \dim(N/IN)$ **(1 pt)**. Comme M et N sont des A-modules libres de rang fini, on a $\mathrm{rang}(M) = \dim(M/IM)$ et $\mathrm{rang}(N) = \dim(N/IN)$ **(1 pt)**. Il vient que $\mathrm{rang}(M) \geq \mathrm{rang}(N)$.

Exercice 6. a. Dans $\mathbb{Q}(\sqrt{6})[X]$ on a $P = (X^2 - (1+\sqrt{6}))(X^2 - (1-\sqrt{6}))$ **(1 pt)**. Soient $A = X^2 - (1+\sqrt{6})$ et $B = X^2 - (1-\sqrt{6})$. On doit montrer que A et B sont irréductibles dans $\mathbb{Q}(\sqrt{6})[X]$

Ceci est clair pour B. En effet, $\mathbb{Q}(\sqrt{6})$ est un sous-corps de $\mathbb{R}$ **(1 pt)**, et $1-\sqrt{6}$ est strictement négatif dans $\mathbb{R}$. Du coup, le polynôme $B = X^2 - (1-\sqrt{6})$ n'a pas de racine dans $\mathbb{R}$. Comme il est de degré 2, il est irréductibe dans $\mathbb{R}[X]$ **(1 pt)**, et donc aussi dans $\mathbb{Q}(\sqrt{6})[X]$ **(1 pt)**.

Pour montrer que A est irréductible dans $\mathbb{Q}(\sqrt{6})[X]$, supposons que $A = CD$, où $C, D \in \mathbb{Q}(\sqrt{6})[X]$. Soit ρ l'automorphisme non trivial de l'extension $\mathbb{Q}(\sqrt{6})$, i.e., $\rho(a+b\sqrt{6}) = a - b\sqrt{6}$, pour tout $a, b \in \mathbb{Q}$. On a

$$C^\rho D^\rho = (CD)^\rho = A^\rho = B.$$

On a vu ci-dessus que B est irréductible dans $\mathbb{Q}(\sqrt{6})[X]$. Donc $\deg(C^\rho) = 0$ ou $\deg(D^\rho) = 0$. Comme $\deg(C) = \deg(C^\rho)$ et $\deg(D) = \deg(D^\rho)$, on a $\deg(C) = 0$ ou $\deg(D) = 0$. Cela montre que A est irréductible dans $\mathbb{Q}(\sqrt{6})[X]$ **(4 pts)**.

b. Soit α la racine $\sqrt{1+\sqrt{6}}$ de A. Comme A est irréductible sur $\mathbb{Q}(\sqrt{6})$, l'extension $\mathbb{Q}(\sqrt{6}, \alpha)$ de $\mathbb{Q}(\sqrt{6})$ est de degré 2 **(1 pt)**. Remarquons que $\mathbb{Q}(\sqrt{6}, \alpha) = \mathbb{Q}(\alpha)$. Du coup, l'extension $\mathbb{Q}(\alpha)$ de $\mathbb{Q}$ est de degré 4 **(1 pt)**. Comme le corps $\mathbb{Q}(\alpha)$ est un sous-corps de $\mathbb{R}$, le polynôme B est irréductible sur $\mathbb{Q}(\alpha)$ **(1 pt)**. Par conséquent, l'extension $\mathbb{Q}(\alpha, \beta)$ de $\mathbb{Q}(\alpha)$ est de degré 2 **(1 pt)**, où β est la racine $i\sqrt{\sqrt{6}-1}$ de B. Du coup, l'extension $\mathbb{Q}(\alpha, \beta)$ de $\mathbb{Q}$ est de degré 8 **(1 pt)**. Comme les racines de P dans $\mathbb{C}$ sont $\pm\alpha$, $\pm\beta$ **(1 pt)**, le corps de décomposition K de P sur $\mathbb{Q}$ est égal à $\mathbb{Q}(\alpha, \beta)$. En particulier, le degré de $K/\mathbb{Q}$ est égal à 8 **(1 pt)**.

c. Comme $A^\rho = B$, le $\mathbb{Q}$-morphisme $\rho\colon \mathbb{Q}(\sqrt{6}) \to K$ s'étend à un $\mathbb{Q}$-morphisme $\rho\colon \mathbb{Q}(\alpha) \to K$ avec $\rho(\alpha) = \beta$. Comme $B^\rho = A$, ce dernier $\mathbb{Q}$-morphisme s'étend à un $\mathbb{Q}$-morphisme $\rho\colon K \to K$ avec $\rho(\beta) = -\alpha$. On voit que ρ est un élément d'ordre 4 du groupe de Galois G de $K/\mathbb{Q}$ **(2 pt)**. Soit encore σ l'automorphisme non trivial de l'extension $K/\mathbb{Q}(\alpha)$ qui est de degrés 2. L'élément σ de G est d'ordre 2 **(2 pt)**. Le sous-groupe de G engendré par ρ, σ agit sur $\{\alpha, \beta, -\alpha, -\beta\}$ comme le groupe diédral D_4 sur le carré de sommets $\{\alpha, \beta, -\alpha, -\beta\}$. Comme les éléments de D_4 correspondants à ρ et σ engendrent D_4, il y a un morphisme surjectif f de $\langle \rho, \sigma \rangle$ dans D_4.

Comme G et D_4 sont tous les deux de cardinal 8, on a $\langle \rho, \sigma \rangle = G$ et f est un ismorphisme **(4 pt)**.

d. D'après la correpsondance de Galois, les sous-corps de K de degré 4 sur $\mathbb{Q}$ correspondent aux sous-groupes de G de cardinal 2 **(1 pt)**. On détermine donc d'abord les sous-groupes de G de cardinal 2.

D'après le c,

$$G = \{1, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}.$$

Les 4 derniers éléments ci-dessus, et l'élément ρ^2 sont les éléments d'ordre 2 de G. Donc, G contient exactement 5 sous-groupes de cardinal 2 :

$$\langle \rho^2 \rangle,\ \langle \sigma \rangle,\ \langle \sigma\rho \rangle,\ \langle \sigma\rho^2 \rangle,\ \langle \sigma\rho^3 \rangle \quad \textbf{(1 pt)}.$$

D'après ce qu'on a vu au b, une $\mathbb{Q}$-base de K est

$$1, \sqrt{6}, \alpha, \alpha\sqrt{6}, \beta, \beta\sqrt{6}, \alpha\beta, \alpha\beta\sqrt{6}.$$

Du coup, on voit que

$$\begin{aligned}
K^{\langle \rho^2 \rangle} &= \mathbb{Q}(1, \sqrt{6}, \alpha\beta, \alpha\beta\sqrt{6}) = \mathbb{Q}(\sqrt{6}, \alpha\beta), \\
K^{\langle \sigma \rangle} &= \mathbb{Q}(1, \sqrt{6}, \alpha, \alpha\sqrt{6}) = \mathbb{Q}(\alpha), \\
K^{\langle \sigma\rho \rangle} &= \mathbb{Q}(1, \alpha - \beta, \alpha\sqrt{6} + \beta\sqrt{6}, \alpha\beta) \\
K^{\langle \sigma\rho^2 \rangle} &= \mathbb{Q}(1, \sqrt{6}, \beta, \beta\sqrt{6}) = \mathbb{Q}(\sqrt{\beta}) \\
K^{\langle \sigma\rho^3 \rangle} &= \mathbb{Q}(1, \alpha + \beta, \alpha\sqrt{6} - \beta\sqrt{6}, \alpha\beta)
\end{aligned}$$

(1 pt par sous-corps)