Université de Bretagne Occidentale
Département de Mathématiques
MAITRISE DE MATHEMATIQUES

ALGEBRE

Examen terminal, 12 janvier 2004, 14h00–18h00

CORRIGE et BAREME

Question de cours. (total : 8 pts)

a. **(4 pts)** Soit $R = A \setminus \{0\}$ la partie multiplicative des éléments non nuls de A. Soit K le corps des fractions de A, i.e. , K est la localisation $K = R^{-1}A$ de A par R. Soit $M_K = R^{-1}M$ la localisation de M par R. Comme M_K est un K-module et K est un corps, M_K est un K-espace vectoriel. Le rang de M est la dimension de M_K comme K-espace vectoriel.

b. **(4 pts)** Soit M un A-module de type fini. Il existe donc une famille $s_, \ldots, s_n$ d'éléments de M qui engendre M. On montre que la famille $\frac{s_1}{1}, \ldots, \frac{s_n}{1}$ est génératrice de M_K.
Soit $\frac{m}{r}$ un élément de M_K, où $m \in M$ et $r \in R$. Comme $m \in M$, il existe $a_, \ldots, a_n \in A$ tels que

$$m = a_1 s_1 + \cdots + a_n s_n.$$

On a donc aussi

$$\frac{m}{1} = \frac{a_1 s_1 + \cdots + a_n s_n}{1} = \frac{a_1}{1}\frac{s_1}{1} + \cdots + \frac{a_n}{1}\frac{s_n}{1}$$

dans M_K. Multiplier par $\frac{1}{r}$ donne

$$\frac{m}{r} = \frac{a_1}{r}\frac{s_1}{1} + \cdots + \frac{a_n}{r}\frac{s_n}{1}$$

dans M_K. Comme $\frac{a_1}{r}, \ldots, \frac{a_n}{r}$ appartiennent à K, la famille $\frac{s_1}{1}, \ldots, \frac{s_n}{1}$ est génératrice du K-espace vectoriel M_K. Par conséquent, la dimension de M_K est finie, i.e. M est de rang fini.

Exercice 1. (total : 8 pts) La décomposition en facteurs premiers de 2004 est $2004 = 2^2 \times 3 \times 167$ (167 est premier car non divisible par 2, 3, 5, 7 et 11, et $13^2 = 169 > 167$.) Soit $p = 167$. Soit s le nombre de p-sous-groupes de Sylow de G. D'après les Théorèmes de Sylow, $s \equiv 1 \pmod{p}$ et s divise $2^2 \times 3 = 12$. Comme $12 < 167$, $s = 1$. Par conséquent, G contient

exactement un p-sylow H. Par unicité, H est un sous-groupe distingué de G. Comme $|H| = p \neq 1$ et 2004, H est un sous-groupe distingué non trival de G, et le groupe G n'est pas simple.

Exercice 2. (total : 4 pts) La décomposition de 203 en facteurs premiers est $203 = 7 \times 29$. D'après le cours, le groupe des automorphismes de $\mathbb{Z}/29\mathbb{Z}$ est isomorphe à $\mathbb{Z}/28\mathbb{Z}$. Comme 7 divise 28, il existe un morphisme non trivial

$$\alpha \colon \mathbb{Z}/7\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/29\mathbb{Z}).$$

Comme α est non trivial, le produit semi-direct

$$\mathbb{Z}/29\mathbb{Z} \rtimes_\alpha \mathbb{Z}/7\mathbb{Z}$$

est un groupe non commutatif de cardinal $29 \times 7 = 203$.

Exercice 3. (total : 12 pts)

a. **(4 pts)** Soit v_1, v_2, v_3 les 3 générateurs de M. Soit π le morphisme quotient de $\mathbb{Z}^3$ dans $\mathbb{Z}^3/2\mathbb{Z}^3$. Comme M est engendré par v_1, v_2, v_3, $\overline{M} = \pi(M)$ est engendré par $\pi(v_1), \pi(v_2), \pi(v_3)$. Or, $\pi(v_1) = \pi(v_3) = 0$ et $\pi(v_2) \neq 0$ dans $\mathbb{Z}^3/2\mathbb{Z}^3$. Donc $\overline{M}$ est engendré par un seul élément non nul du $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel $\mathbb{Z}^3/2\mathbb{Z}^3$. Il s'ensuit que la dimension de $\overline{M}$ est égale à 1.

b. **(8 pts)** Par l'absurde, supposons que $\mathbb{Z}^3/M$ est cyclique. Comme π est surjectif et $\pi(M) \subseteq \overline{M}$, le morphisme π induit un morphisme surjectif

$$\overline{\pi} \colon \mathbb{Z}^3/M \longrightarrow (\mathbb{Z}^3/2\mathbb{Z}^3)/\overline{M}.$$

Par hypothèse, $\mathbb{Z}^3/M$ est cyclique. Comme $\overline{\pi}$ est surjectif, $(\mathbb{Z}^3/2\mathbb{Z}^3)/\overline{M}$ est cyclique. Mais ce dernier groupe est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension $3 - 1 = 2$ d'après le a. En particulier, $(\mathbb{Z}^3/2\mathbb{Z}^3)/\overline{M}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ qui n'est pas cyclique. Contradiction.

Exercice 4. (total : 6 pts) Montrons d'abord que $A \neq \{0\}$. Comme K est un corps, $0 \neq 1$ dans K. Comme A est un sous-anneau de K, on a aussi $0 \neq 1$ dans A. En particulier, A est non nul **(2 pt)**.

Montrons maintenant que tout élément non nul a de A admet un inverse. Comme $a^{-1} \in K$ est entier sur A, il existe $n \in \mathbb{N}$ et $a_0, \ldots, a_{n-1} \in A$ tels que

$$(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_0 = 0$$

dans K. Multiplier par a^n donne

$$1 + a_{n-1}a + \cdots + a_0 a^n = 0$$

dans K est donc aussi dans A. Ecrit différemment,

$$a(-a_{n-1} - \cdots - a_0 a^{n-1}) = 1.$$

Comme $-a_{n-1} - \cdots - a_0 a^{n-1}$ appartient à A, a est inversible dans A. Par conséquent, A est un corps **(4 pts)**.

Exercice 5. (total : 12 pts)

a. **(3 pts)** Le polynôme $P = X^2 + 1$ dans $\mathbb{F}_3[X]$ est unitaire et de degré 2. De plus, P n'a pas de racine dans $\mathbb{F}_3$. Comme $\deg(P) \leq 3$, P est irréductible.

b. **(6 pts)** Comme P est irréductible de degré 2, le quotient $\mathbb{F}_3[X]/(P)$ est une extension de $\mathbb{F}_3$ de degré 2. D'où $\mathbb{F}_3[X]/(P) = \mathbb{F}_9$. On écrit x pour la classe de X modulo P. La famille $1, x$ est une $\mathbb{F}_3$-base de $\mathbb{F}_9$.

Comme $\mathbb{F}_9^\star$ est cyclique de cardinal $8 = 2^3$, le nombre de générateurs de $\mathbb{F}_9^\star$ est égal à $\varphi(8) = 4$, où φ est la fonction totient d'Euler. Comme $x^2 = -1$ dans $\mathbb{F}_9$, x est d'ordre 4 dans $\mathbb{F}_9^\star$. Donc, ni x ni $-x = 2x$ n'est un générateur de $\mathbb{F}_9^\star$. Comme 1 et 2 ne sont pas générateurs de $\mathbb{F}_9^\star$ non plus, tout élément de $\mathbb{F}_9^\star$ différent de $1, 2, x, 2x$ est un générateur de $\mathbb{F}_9$. Par conséquent $y = x + 1$ est un générateur de $\mathbb{F}_9^\star$.

c. **(3 pts)** Soit m le polynôme minimal de $x + 1$. L'image de $x + 1$ par le morphisme de Frobenius est également une racine de m, i.e., $(x+1)^3 = x^3 + 1 = -x + 1 = 2x + 1$ est racine de m. Comme m est unitair de degré 2,

$$m = (X - (x + 1))(X - (2x + 1)) = X^2 + X + 2,$$

dans $\mathbb{F}_3[X]$.

(L'autre réponse correcte à cette question est $X^2 + 2X + 2$.)

Exercice 6. (total : 16 pts)

a. **(4 pts)** Soit $m = \mu(x)$ le polynôme minimal de x sur $\mathbb{F}_p$. On doit montrer que m est un polynôme unitaire irréductible de degré n. Par définition du polynôme minimal, m est unitair. On a l'isomorphisme

$$\mathbb{F}_p[x] \cong \mathbb{F}_p[X]/(m).$$

Comme $\mathbb{F}_p[x]$ est intègre, m est irréductible. Comme $x \notin \mathbb{F}_p$, $\mathbb{F}_p[x]$ est un sous-corps de $\mathbb{F}_{p^n}$ contenant $\mathbb{F}_p$ strictement. Comme l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est de degré premier, $\mathbb{F}_p[x] = \mathbb{F}_{p^n}$. D'où

$$\deg(m) = \dim_{\mathbb{F}_p} \mathbb{F}_p[X]/(m) = \dim_{\mathbb{F}_p} \mathbb{F}_p[x] = \dim_{\mathbb{F}_p} \mathbb{F}_{p^n} = n.$$

b. **(4 pts)** Soit P un polynôme unitaire et irréductible dans $\mathbb{F}_p[X]$ de degré n. Comme $n \neq 0$, P admet une racine x dans $\overline{\mathbb{F}}_p$. Comme P est unitaire et irréductible, P est le polynôme minimal de x sur $\mathbb{F}_p$. Il reste à montrer que $x \in \mathbb{F}_{p^n} \setminus \mathbb{F}_p$. Or, $\mathbb{F}_p[x]$ est un sous-corps de $\overline{\mathbb{F}}_p$ à p^n éléments car le polynôme minimal de x est de degré n. D'après le cours, $\mathbb{F}_p[x] = \mathbb{F}_{p^n}$. En particulier, $x \in \mathbb{F}_{p^n}$. Comme $n > 1$, $x \notin \mathbb{F}_p$.

c. **(4 pts)** Soient $x, y \in \mathcal{X}$ tels que $\mu(x) = \mu(y)$. Sopit m le polynôme $\mu(x) = \mu(y)$ dans $\mathbb{F}_p[X]$. On a une chaîne d'isomorphismes

$$\mathbb{F}_p[x] \to \mathbb{F}_p[X]/(m) \to \mathbb{F}_p[y].$$

Soit σ la composition. On a $\sigma(x) = y$. Par le même argument que celui du a, $\mathbb{F}_p[x] = \mathbb{F}_{p^n}$ et $\mathbb{F}_p[y] = \mathbb{F}_{p^n}$. Donc σ est un élément de $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ satisfaisant $\sigma(x) = y$.

Réciproquement, supposons qu'il existe $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ tel que $\sigma(x) = y$. Soit m le polynôme minimal de x. On a $m(y) = \sigma(m)(\sigma(x)) = \sigma(m(x)) = \sigma(0) = 0$. Comme m est un polynôme unitaire irréductible dans $\mathbb{F}_p[X]$ annulant y, m est le polynôme minimal de y. D'où $\mu(x) = m = \mu(y)$.

d. **(4 pts)** Soit G le groupe de Galois de $\mathbb{F}_{p^n}/\mathbb{F}_p$. Comme $\mathbb{F}_p = \mathrm{Fix}(G)$, $\sigma(x) \in \mathcal{X}$ quel que soit $x \in \mathcal{X}$. Par conséquent, G agit sur $\mathcal{X}$ si on définit $\sigma \cdot x = \sigma(x)$. Comme $\mathrm{Fix}(G) = \mathbb{F}_p$, le groupe G agit sans point fixe sur $\mathcal{X}$. Comme $|G| = n$ est premier, G agit librement sur $\mathcal{X}$. Par conséquent,

$$|G \setminus \mathcal{X}| = \frac{|\mathcal{X}|}{|G|} = \frac{p^n - p}{n}.$$

D'après les b et c, μ induit une bijection

$$\overline{\mu} \colon G \setminus \mathcal{X} \to \mathcal{P}.$$

Il s'ensuit que

$$|\mathcal{P}| = \frac{p^n - p}{n}.$$

Exercice 7. (total : 34 pts)

a. **(2 pts)** Soit $Q \in \mathbb{Q}[X]$ le polynôme $X^2 - 2X + 5$. On a $P(X) = Q(X^2)$. Donc, si $\alpha \in \mathbb{C}$ est une racine de P, α^2 est une racine de Q. Or, les racines de Q dans $\mathbb{C}$ sont $1 \pm 2i$. Donc au moins l'un des deux nombres complexes $1 \pm 2i$ appartient à L. Par conséquent, $\mathbb{Q}(i)$ est contenu dans L.

b. **(3 pts)** Si $\beta \in \mathbb{C}$ est une racine de Q, les deux racines carrées de β sont racines de P. Soit α une racine carrée de $1+2i$ et α' une racine carrée de $1-2i$ dans $\mathbb{C}$. On a $L = \mathbb{Q}(\alpha, \alpha')$ et

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}].$$

Comme chaque facteur est égal à 1 ou 2, $[L : \mathbb{Q}]$ divise 8.

c. **(4 pts)** Le sous-groupe $\mathrm{Gal}(L/\mathbb{Q}(i))$ est distingué dans $\mathrm{Gal}(L/\mathbb{Q})$ car $\mathbb{Q}(i)/\mathbb{Q}$ est normale. On a bien

$$\mathrm{Gal}(L/\mathbb{Q}(i)) \cap \{\mathrm{id}, \sigma\} = \{\mathrm{id}\},$$

car $\sigma(i) = -i$. Comme

$$|\mathrm{Gal}(L/Q(i))| \times |\{1, \sigma\}| = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(i) : \mathbb{Q}]} \times 2 = [L : \mathbb{Q}] = \mathrm{Gal}(L/\mathbb{Q}),$$

$\mathrm{Gal}(L/\mathbb{Q}(i)) \cdot \{\mathrm{id}, \sigma\} = \mathrm{Gal}(L/\mathbb{Q})$ et $\mathrm{Gal}(L/\mathbb{Q})$ est le produit semi-direct de $\mathrm{Gal}(L/\mathbb{Q}(i))$ et $\{\mathrm{id}, \sigma\}$.

d. **(2 pts)** Les racines de P sont les racines carrées de $1+2i$ et $1-2i$ dans $\mathbb{C}$. Or, les racines carrées de $1+2i$ et $1-2i$ sont

$$\pm\sqrt{\omega} \pm i\sqrt{-\omega'},$$

où $\omega = \frac{1+\sqrt{5}}{2}$ et $\omega' = \frac{1-\sqrt{5}}{2}$.

e. **(6 pts)** On a

$$[\mathbb{Q}(\sqrt{\omega}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\omega}) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}].$$

Comme ce dernier degré est égal à 2, il suffit de montrer que $\sqrt{\omega} \notin \mathbb{Q}(\omega)$. Supposons, par l'absurde, qu'il existe $\eta \in \mathbb{Q}(\omega)$ tel que $\eta^2 = \omega$. Soit φ l'unique automorphisme non trivial de $\mathbb{Q}(\omega)$. On a $\varphi(\omega) = \omega' < 0$ et donc $\varphi(\eta)^2 = \omega' < 0$. Mais $\varphi(\eta) \in \mathbb{R}$. Contradiction.

f. **(4 pts)** D'après le d, $\sqrt{\omega} \in L \cap \mathbb{R} = L'$. D'où $\mathbb{Q}(\sqrt{\omega}) \subseteq L'$. On montre l'inclusion inverse en montrant que les deux extensions de $\mathbb{Q}$ ont même degré. En effet,

$$4 = [\mathbb{Q}(\sqrt{\omega}) : \mathbb{Q}] \leq [L' : \mathbb{Q}] = \frac{[L : \mathbb{Q}]}{[L : L']} \leq \frac{8}{2} = 4,$$

car $L' = \mathrm{Fix}(\{\mathrm{id}, \sigma\}$, donc $[L : L'] = 2$, et $L : \mathbb{Q}] \leq 8$ d'après le b. Il s'ensuit que $[\mathbb{Q}(\sqrt{\omega}) : \mathbb{Q}] = [L' : \mathbb{Q}]$ et $L' = \mathbb{Q}(\sqrt{\omega})$.

g. **(2 pts)** $[L : \mathbb{Q}] = [L : L'][L' : \mathbb{Q}] = 2 \times 4 = 8$.

h. **(5 pts)** Comme $[L : \mathbb{Q}] = 8$, $[L : \mathbb{Q}(i)] = 4$. D'où $[L : \mathbb{Q}(\alpha)] = 2$ et $[L : \mathbb{Q}(\alpha')] = 2$. Le groupe $\mathrm{Gal}(L/\mathbb{Q}(i))$ contient les deux sous-groupes $\mathrm{Gal}(L/\mathbb{Q}(\alpha))$ et $\mathrm{Gal}(L/\mathbb{Q}(\alpha'))$. Leur intersection est triviale car $L = \mathbb{Q}(\alpha, \alpha')$. Leur produit est égal à $\mathrm{Gal}(L/Q(i))$ car

$$|\mathrm{Gal}(L/\mathbb{Q}(\alpha))| \times |\mathrm{Gal}(L/\mathbb{Q}(\alpha')| = 2 \times 2 = 4 = |\mathrm{Gal}(L/\mathbb{Q}(i))|.$$

Comme les deux sous-groupes sont distingués, $\mathrm{Gal}(L/\mathbb{Q}(i))$ est isomorphe au produit des deux, i.e., $\mathrm{Gal}(L/\mathbb{Q}(i))$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

i. **(6 pts)** Soit τ l'élément non trival de $\mathrm{Gal}(L/\mathbb{Q}(\alpha'))$. Quitte à remplacer α' par $-\alpha'$ on peut supposer que $\sigma(\alpha) = \alpha'$. L'action de $\tau\sigma$ sur les racines $\alpha, \alpha', -\alpha, -\alpha'$ est une permutation cyclique d'orde 4. L'action de τ sur $\alpha, \alpha', -\alpha, -\alpha'$ est la transposition de α et $-\alpha$. Il s'ensuit que le sous-groupe engendreé par $\tau\sigma, \tau$ est isomorphe à D_4. Comme $|D_4| = 8$, ce sous-groupe engendré est égal à $\mathrm{Gal}(L/\mathbb{Q})$ tout entier.