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

ALGEBRE

Examen terminal, 16 juin 2006, 8h30–12h30

CORRIGE et BAREME

Question de cours. (20 pt) Voir Théorème 1.8.2 du Lang.

Exercice 1. a. La décomposition de 1003 en facteurs premiers est $1003 = 17 \times 59$. Comme $17 \neq 59$ et 17 ne divise pas $59 - 1$, tout groupe de cardinal 1003 est cyclique d'après le cours **(4 pt)**.

b. Soit G un groupe de cardinal 2006. Comme la décomposition de 2006 en facteurs premiers est $2006 = 2 \times 17 \times 59$ **(1 pt)**, le groupe G contient au moins un 17-sylow H et au moins un 59-sylow K **(1 pt)**. Le nombre de 17-sylow de G est congru à 1 modulo 17 et divise 2×59 **(1 pt)**. Il s'ensuit que G ne contient qu'un seul 17-sylow **(1 pt)**. Par conséquent, le sous-groupe H de G est distingué **(1 pt)**. Du coup, le sous-ensemble HK est un sous-groupe de G de cardinal $17 \times 59 = 1003$ **(1 pt)**. D'après le a, HK est cyclique **(1 pt)**.

c. Un groupe de cardinal 2006 n'est pas forcément cyclique **(2 pt)**. Le groupe diédral D_{1003} fournit un contre-exemple **(2 pt)**.

Exercice 2. a. Soient $e = \mathrm{ppcm}(k, \ell)$ et $d = \mathrm{pgcd}(k, \ell)$. Ecrire $k = dm$ et $\ell = dn$ avec $m, n \in \mathbb{Z}$. Comme $d = \mathrm{pgcd}(k, \ell)$, les entiers m et n sont premiers entre eux. Du coup, il existe $u, v \in \mathbb{Z}$ tels que $mu - nv = 1$. Montrons que la famille $(\overline{m}, \overline{n}), (\overline{v}, \overline{u})$ engendre $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Soit $(\overline{a}, \overline{b})$ un élément de $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. On voit que

$$(ua - vb) \cdot (\overline{m}, \overline{n}) + (-na + mb) \cdot (\overline{v}, \overline{u}) = (\overline{a}, \overline{b}).$$

Cela montre bien que la famille $(\overline{m}, \overline{n}), (\overline{v}, \overline{u})$ engendre $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

Soit $f \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ le morphisme de groupes défini par

$$f(x, y) = x \cdot (\overline{m}, \overline{n}) + y \cdot (\overline{v}, \overline{u}).$$

D'après ce qui précède, f est surjectif. De plus, $d\mathbb{Z} \times e\mathbb{Z}$ est contenu dans le noyau de f. Du coup, f induit un morphisme

$$\overline{f} \colon (\mathbb{Z} \times \mathbb{Z})/(d\mathbb{Z} \times e\mathbb{Z}) \longrightarrow \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

Comme f est surjectif, $\overline{f}$ est surjectif. Le groupe quotient $(\mathbb{Z}\times\mathbb{Z})/(d\mathbb{Z}\times e\mathbb{Z})$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}\times\mathbb{Z}/e\mathbb{Z}$. En particulier, son cardinal est égal à $de = k\ell$. Il s'ensuit que $\overline{f}$ est un isomorphisme. Comme $d|e$, les diviseurs élémentaires de $\mathbb{Z}/k\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$ sont alors e, d **(5 pt)**.

b. Soient $d = \mathrm{pgcd}(k,\ell,m)$ et $f = \mathrm{ppcm}(k,\ell,m)$. Comme df divise $k\ell m$, il existe un entier e tel que $def = k\ell m$. On a $d|e$ et $e|f$. Les diviseurs élémentaires du groupe $\mathbb{Z}/k\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ sont f, e, d **(2 pt)**.

En effet, on peut supposer que

$$k = \prod_{i=1}^{n} p_i^{a_i}, \quad \ell = \prod_{i=1}^{n} p_i^{b_i} \quad \text{et} \quad m = \prod_{i=1}^{n} p_i^{c_i},$$

où $a_i, b_i, c_i \in \mathbb{N}$, p_i premier, $p_i \neq p_j$ lorsque $i \neq j$, et $n \in \mathbb{N}$. Pour i fixé, soit $\alpha_i = \min\{a_i, b_i, c_i\}$, $\gamma_i = \max\{a_i, b_i, c_i\}$ et β_i l'autre entier des trois a_i, b_i, c_i. On a

$$d = \prod_{i=1}^{n} p_i^{\alpha_i}, \quad e = \prod_{i=1}^{n} p_i^{\beta_i} \quad \text{et} \quad f = \prod_{i=1}^{n} p_i^{\gamma_i}.$$

Il vient que

$$\begin{aligned}
\mathbb{Z}/k\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z} \cong & \\
\left(\prod_{i=1}^{n}\mathbb{Z}/p_i^{a_i}\mathbb{Z}\right)\times\left(\prod_{i=1}^{n}\mathbb{Z}/p_i^{b_i}\mathbb{Z}\right)\times\left(\prod_{i=1}^{n}\mathbb{Z}/p_i^{c_i}\mathbb{Z}\right) &\cong \\
\prod_{i=1}^{n}\left(\mathbb{Z}/p_i^{a_i}\mathbb{Z}\times\mathbb{Z}/p_i^{b_i}\mathbb{Z}\times\mathbb{Z}/p_i^{c_i}\mathbb{Z}\right) &\cong \\
\prod_{i=1}^{n}\left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\times\mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\times\mathbb{Z}/p_i^{\gamma_i}\mathbb{Z}\right) &\cong \\
\left(\prod_{i=1}^{n}\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)\times\left(\prod_{i=1}^{n}\mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)\times\left(\prod_{i=1}^{n}\mathbb{Z}/p_i^{\gamma_i}\mathbb{Z}\right) &\cong \\
\mathbb{Z}/d\mathbb{Z}\times\mathbb{Z}/e\mathbb{Z}\times\mathbb{Z}/f\mathbb{Z}. &
\end{aligned}$$

Par conséquent, les diviseurs élémentaires de $\mathbb{Z}/k\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ sont bien f, e, d **(3 pt)**.

Exercice 3. a. On a $1 = (\overline{X+1})^0$. Donc 1 appartient bien à S **(1 pt)**. De plus, si $x, y \in S$, on a $x = (\overline{X+1})^i$ et $y = (\overline{X+1})^j$, pour certains $i, j \in \mathbb{N}$. Du coup, $xy = (\overline{X+1})^{i+j}$ appartient bien à S **(1 pt)**. Il s'ensuit que S est une partie multiplicative de A.

b. Comme $\overline{X+1} \in S$ et

$$(\overline{X+1}) \cdot (\overline{X-1}) \cdot 1 = \overline{X^2-1} = 0 = (\overline{X+1}) \cdot 0 \cdot 1$$

dans A. On a bien

$$\frac{\overline{X-1}}{1} = \frac{0}{1}$$

dans $S^{-1}A$, par définition de la localisation **(2 pt)**.

c. On a $f((\overline{X+1})^i) = 2^i \in \mathbb{Q}^\star$ **(1 pt)**. D'après la propriété universelle de la localisation, f induit un morphisme d'anneaux $g\colon S^{-1}A \to \mathbb{Q}$. On a

$$g\left(\frac{\overline{P}}{(\overline{X+1})^i}\right) = 2^{-i} f(\overline{P}) = 2^{-i} P(1),$$

pour tout $i \in \mathbb{N}$ et pour tout $\overline{P} \in A$ **(2pt)**.

d. Comme f est surjectif, g est surjectif **(1 pt)**. Il suffit donc de montrer que g est injectif. Soit

$$\frac{\overline{P}}{(\overline{X+1})^i}$$

un élément du noyau de g. Ca veut dire que $P(1) = 0$. Du coup, le polynôme P est divisible par $X-1$. Ecrire $P = (X-1)Q$, où $Q \in \mathbb{Q}[X]$. On a

$$\frac{\overline{P}}{(\overline{X+1})^i} = \frac{(\overline{X-1}) \cdot \overline{Q}}{(\overline{X+1})^i} = \frac{\overline{X-1}}{1} \cdot \frac{\overline{Q}}{(\overline{X+1})^i} = \frac{0}{1} \cdot \frac{\overline{Q}}{(\overline{X+1})^i} = 0$$

dans $S^{-1}A$, d'après le b. Cela montre bien que g est injectif **(2 pt)**, et donc que g est un isomorphisme.

Exercice 4. a. On a bien $0 \in I^2$ car $0 = a_1b_1 + \cdot + a_0b_0$ **(1 pt)**. Lorsque $x, y \in I^2$, on a $x = a_1b_1 + \cdots + a_nb_n$ et $y = a_{n+1}b_{n+1} + \cdots + a_mb_m$, avec $a_1, \ldots, a_m \in I$, $b_1, \ldots, b_m \in I$, $n, m \in \mathbb{N}$, $n \leq m$. Du coup,

$$x + y = a_1b_1 + \cdots + a_mb_m \in I^2 \quad \textbf{(1 pt)}.$$

Lorsque, de plus, $a \in A$, on a

$$ax = (aa_1)b_1 + \cdots + (aa_n)b_n \in I^2,$$

car $aa_1, \ldots, aa_n \in I$ et $b_1, \ldots, b_n \in I$ **(1 pt)**.

b. Rappelons que la structure de A-module sur I/I^2 est définie par $a \cdot \overline{x} = \overline{ax}$ quels que soient $a \in A$ et $x \in I$ **(1 pt)**. On vérifie que la loi externe

$$A/I \times I/I^2 \longrightarrow I/I^2$$

définie par $\overline{a} \cdot \overline{x} = a \cdot \overline{x}$ est bien définie. Supposons que $\overline{a} = \overline{b}$ dans A/I, c-à-d que $a, b \in A$ tels que $a-b \in I$. Lorsque $\overline{x} \in I/I^2$ on a $x \in I$ donc $(a-b)x \in I^2$. Du coup,

$$0 = \overline{(a-b)x} = \overline{ax} - \overline{bx} = a \cdot \overline{x} - b \cdot \overline{x}$$

dans I/I^2. Cela montre que la loi externe ci-dessus est bien définie **(1 pt)**. Comme cette loi est induite par une loi de module, elle définit automatiquement une structure de A/I-module sur I/I^2 **(1 pt)**.

c. Soit $f\colon A \to \mathbb{Q}$ le morphisme d'évaluation en $(0,0)$, i.e. $f(P) = P(0,0)$ pour tout $P \in A$. Il est claire que f est surjectif **(1 pt)** et que son noyau est égal à I **(1 pt)**. Du coup, f induit un isomorphisme de A/I sur $\mathbb{Q}$ **(1 pt)**.

d. Comme $X, Y \in I$, on a bien $X^2, XY, Y^2 \in I^2$. Du coup,

$$(X^2, XY, Y^2) \subseteq I^2 \quad \textbf{(1 pt)}.$$

Réciproquement, soit $P \in I^2$. Par définition, $P = A_1B_1 + \cdots + A_nB_n$ où $A_1, \ldots, A_n, B_1, \ldots, B_n \in I$. On montre que $P \in (X^2, XY, Y^2)$. Pour cela, il suffit de montrer que $A_iB_i \in (X^2, XY, Y^2)$ pour $i = 1, \ldots, n$. Comme I est engendré par X, Y, on a $A_i = C_iX + D_iY$ et $B_i = E_iX + F_iY$ pour certains $C_i, D_i, E_i, F_i \in A$. Du coup,

$$A_iB_i = (C_iX + D_iY)(E_iX + F_iY) = C_iE_iX^2 + (C_iF_i + D_iE_i)XY + D_iF_iY^2.$$

Cela montre bien que $A_iB_i \in (X^2, XY, Y^2)$ et donc que $P \in (X^2, XY, Y^2)$. Par conséquent,

$$I^2 \subseteq (X^2, XY, Y^2) \quad \textbf{(2 pt)}.$$

e. Comme I est engendré par X, Y, le A/I-module I/I^2 est engendré par $\overline{X}, \overline{Y}$ **(1 pt)**. Comme A/I est isomorphe à $\mathbb{Q}$ d'après le a, la famille $\overline{X}, \overline{Y}$ est génératrice du $\mathbb{Q}$-espace vectoriel I/I^2 **(1 pt)**. Montrons qu'elle est également libre. Supposons que $a\overline{X} + b\overline{Y} = 0$ dans I/I^2 où $a, b \in \mathbb{Q}$. Ca veut dire que $aX + bY \in I^2$. Comme $I^2 = (X^2, XY, Y^2)$ d'après le d, on a

$$aX + bY = \sum_{i+j \geq 2} a_{ij} X^i Y^j,$$

pour certains $a_{ij} \in \mathbb{Q}$. Comme les monômes X^iY^j, $i, j \geq 0$, constituent une famille $\mathbb{Q}$-libre de $\mathbb{Q}[X, Y]$, on a forcément $a = 0$ et $b = 0$. Cela montre que la famille $\overline{X}, \overline{Y}$ est libre **(2pt)**. Il s'ensuit que $\dim_{\mathbb{Q}} I/I^2 = 2$.

f. Si I était principal, i.e., s'il existait $P \in A$ tel que $I = (P)$, le A/I-module I/I^2 serait engenrdé par $\overline{P}$. Du coup, le $\mathbb{Q}$-espace vectoriel I/I^2 admettrait une famille génératrice de cardinal 1. Il s'ensuivrait que $\dim_{\mathbb{Q}} I/I^2 \leq 1$ **(1 pt)**.

Exercice 5. a. Comme M est engendré par $(X-4,2),\ (-3,X+1)$, l'image $\pi(M)$ est engendré par

$$\pi(X-4,2)=X-4 \quad \text{et} \quad \pi(-3,X+1)=-3 \quad \textbf{(1 pt)}.$$

Comme -3 est inversible dans $\mathbb{Q}[X]$, le sous-module de $\mathbb{Q}[X]$ engendré par $X-4,-3$ est égal à $\mathbb{Q}[X]$ tout entier. Par conséquent, $\mathrm{im}(\pi_{|M})=\mathbb{Q}[X]$ **(1 pt)**.

b. Le noyau de $\pi_{|M}$ est l'intersection de $\{0\}\times\mathbb{Q}[X]$ avec M **(1 pt)**. Déterminons cette intersection. Soit V un élément de l'intersection. Comme $V\in M$, il existe $P,Q\in\mathbb{Q}[X]$ tels que

$$V=P\cdot(X-4,2)+Q\cdot(-3,X+1)= \\ ((X-4)P-3Q,2P+(X+1)Q).$$

Comme V appartient à $\{0\}\times\mathbb{Q}[X]$, on a $(X-4)P-3Q=0$. Du coup, $Q=\frac{1}{3}(X-4)P$ et

$$V=(0,2P+(X+1)\tfrac{1}{3}(X-4)P)=(0,\tfrac{1}{3}(X^2-3X+2)P)= \\ \tfrac{1}{3}P\cdot(0,X^2-3X+2).$$

Il s'ensuit que

$$M\cap(\{0\}\times\mathbb{Q}[X])\subseteq\langle(0,X^2-3X+2)\rangle \quad \textbf{(1 pt)}.$$

Comme, $(0,X^2-3X+2)=3\cdot(X-4,2)+(X-4)\cdot(-3,X+1)$, on a aussi l'inlcusion inverse **(1 pt)**. Par conséquent, $\ker(\pi_{|M})$ est engendré par $(0,X^2-3X+2)$.

c. D'après le a et b, la famille $(0,X^2-3X+2),\ (-3,X+1)$ est une base de M **(1 pt)**. Montrons que $(\mathbb{Q}[X]\times\mathbb{Q}[X])/M$ est de torsion en montrant que por tout $(P,Q)\in\mathbb{Q}[X]\times\mathbb{Q}[X]$, il existe $R\in\mathbb{Q}[X]$, $\neq 0$, tel que $R\cdot(P,Q)\in M$. En effet, il suffit de prendre $R=X^2-3X+2$ car

$$(X^2-3X+2)\cdot(P,Q)=-\tfrac{1}{3}(X^2-3X+2)P\cdot(-3,X+1)+ \\ (\tfrac{1}{3}(X+1)P+Q)\cdot(0,X^2-3X+2)\in M \quad \textbf{(2 pt)}.$$

d. Comme $(X^2-3X+2)\cdot(0,1),(-3,X+1)$ est une base de M, et $(0,1),(-3,X+1)$ est une base de $\mathbb{Q}[X]\times\mathbb{Q}[X]$, le quotient $(\mathbb{Q}[X]\times\mathbb{Q}[X])/M$ est isomorphe à $\mathbb{Q}[X]/(X^2-3X+2)$. Le diviseur élémentaire de ce quotient est donc X^2-3X+2 **(2 pt)**.

Exercice 6. a. D'apès le crière d'Eisenstein avec $p = 5$, le polynôme $X^4 - 5$ est irréductible dans $\mathbb{Q}[X]$. Le degré de K/Q est donc égal à 4 **(2 pt)**.

b. Comme K est un sous-corps de $\mathbb{R}$ et $i \notin \mathbb{R}$, le degré de L/K est égal à 2 **(1 pt)**. Du coup,

$$[L : \mathbb{Q}] = [L : K] \times [K : \mathbb{Q}] = 2 \times 4 = 8 \quad \textbf{(1 pt)}.$$

c. Comme $\mathbb{Q}$ est de caractéristique 0, l'extension $L/\mathbb{Q}$ est séparable **(1 pt)**. Montrons qu'elle est également normale. Soit $\sigma\colon L \to \mathbb{C}$ un morphisme de corps $\mathbb{Q}$-linéaire. Comme i est racine de $X^2 + 1$, $\sigma(i)$ est aussi racine de $X^2 + 1$. Du coup, $\sigma(i) = \pm i$. De même, comme $\sqrt[4]{5}$ est racine de $X^4 - 5$, $\sigma(\sqrt[4]{5})$ est aussi racine de $X^4 - 5$. Du coup, $\sigma(\sqrt[4]{5}) = \pm\sqrt[4]{5}$ ou $\pm i\sqrt[4]{5}$. Il s'ensuit que $\sigma(i) \in L$ et que $\sigma(\sqrt[4]{5}) \in L$. Comme $L = \mathbb{Q}(i, \sqrt[4]{5})$, on en déduit que $\sigma(L) \subseteq L$. Cela montre bien que $L/\mathbb{Q}$ est normale **(3 pt)** et donc galoisienne.

d. Comme $L/\mathbb{Q}$ est galoisienne, L/K est galoisienne **(1 pt)**. Comme $[L : K] = 2$, le groupe de Galois de L/K est de cardinal 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$ **(1 pt)**.

e. Comme $L/\mathbb{Q}$ est galoisienne, $L/\mathbb{Q}(i)$ est galoisienne **(1 pt)**. On a

$$[L : \mathbb{Q}(i)] = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(i) : \mathbb{Q}]} = \frac{8}{2} = 4 \quad \textbf{(1 pt)}.$$

Comme $L = \mathbb{Q}(i)(\sqrt[4]{5})$ et $\sqrt[4]{5}$ est racine de $X^4 - 5 \in \mathbb{Q}(i)[X]$, le polynôme minimale de $\sqrt[4]{5}$ sur $\mathbb{Q}(i)$ est égal à $X^4 - 5$ **(1 pt)**. Du coup, il existe un automorphisme $\mathbb{Q}(i)$-linéaire τ de L avec $\tau(\sqrt[4]{5}) = i\sqrt[4]{5}$ **(1 pt)**. On a $\tau^2(\sqrt[4]{5}) = -\sqrt[4]{5}$, $\tau^3(\sqrt[4]{5}) = -i\sqrt[4]{5}$ et $\tau^4(\sqrt[4]{5}) = \sqrt[4]{5}$. Il s'ensuit que τ est d'ordre 4 **(1 pt)** et que τ engendre le groupe de Galois de $L/\mathbb{Q}(i)$. Par conséquent, ce groupe de Galois est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ **(1 pt)**.

f. Soit G le groupe de Galois de $L/\mathbb{Q}$. On a $\tau \in G$. Soit σ la restriction à L de la conjugaison complexe. On a $\sigma \in G$ **(1 pt)**. Le sous-groupe $\langle \sigma, \tau \rangle$ de G agit sur l'ensemble $\{\pm\sqrt[4]{5}, \pm i\sqrt[4]{5}\}$ comme le groupe diédral D_4 sur l'ensemble des sommets du carré **(2 pt)**. Il s'ensuit que $\langle \sigma, \tau \rangle$ est isomorphe à D_4. En particulier, il est un sous-groupe de G de cardinal 8. Comme $\#G = [L : \mathbb{Q}] = 8$, on a $\langle \sigma, \tau \rangle = G$ et G est ismorphe à D_4 **(1 pt)**.