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

ALGEBRE

Examen terminal, 8 janvier 2018, 9h00–12h00

CORRIGE et BAREME

Exercice 1. Comme la localisation et le passage au quotient commutent **(3 pt)**, on a un isomorphisme naturel

$$(\mathbb{Z}/15\mathbb{Z})_{10} = \mathbb{Z}_{10}/15\mathbb{Z}_{10}.$$

Notons que $15\mathbb{Z}_{10} = 3\mathbb{Z}_{10}$ **(4 pt)**. En effet, $3 = \frac{2}{10}15$. Donc $3 \in 15\mathbb{Z}_{10}$ et $3\mathbb{Z}_{10} \subseteq 15\mathbb{Z}_{10}$. Comme $15 = 5 \cdot 3$, on a aussi $15 \in 3\mathbb{Z}_{10}$ et $15\mathbb{Z}_{10} \subseteq 3\mathbb{Z}_{10}$. Du coup, on a

$$\mathbb{Z}_{10}/15\mathbb{Z}_{10} = \mathbb{Z}_{10}/3\mathbb{Z}_{10}.$$

Puis encore

$$\mathbb{Z}_{10}/3\mathbb{Z}_{10} = (\mathbb{Z}/3\mathbb{Z})_{10} = (\mathbb{Z}/3\mathbb{Z})_1 = \mathbb{Z}/3\mathbb{Z} \quad \textbf{(1 pt)}.$$

Donc on peut prendre $n = 3$.

Exercice 2. a. Tout d'abord, l'anneau A est non nul **(1 pt)**. En effet, si A était l'anneau nul, on aurait $0 = 1$ dans A et donc aussi dans $\mathbb{Q}[X]$ ce qui est absurde. Puis, si $f, g \in A$ tel que $fg = 0$ dans A, on a aussi $fg = 0$ dans $\mathbb{Q}[X]$. Comme $\mathbb{Q}[X]$ est intègre, on obtient $f = 0$ ou $g = 0$ dans $\mathbb{Q}[X]$, et donc aussi dans A **(1 pt)**. Cela montre que A est intègre.

b. Soit B le second membre, c-à-d, soit B le sous-ensemble de $\mathbb{Q}[X]$ défini par

$$B = \{a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n \mid a_0, a_1, a_2, \ldots, a_n \in \mathbb{Q},\ n \in \mathbb{N} \text{ avec } a_1 = 0\}.$$

On doit montrer que $B = \mathbb{Q}[X^2, X^3]$, le plus petit sous-anneau de $\mathbb{Q}[X]$ contenant $\mathbb{Q}$, X^2 et X^3.

On montre d'abord que B est un sous-anneau de $\mathbb{Q}[X]$. On a bien $0, 1 \in B$. Soient $f, g \in B$. Ecrivons

$$f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \quad \text{et} \quad g = b_0 + b_1X + b_2X^2 + \cdots + b_mX^m,$$

où $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{Q}$ et $m, n \in \mathbb{N}$. On peut supposer que $m, n \geq 1$.

Le coefficient devant X dans la somme $f + g$ est égal à $a_1 + b_1$. Comme $f, g \in B$, on a $a_1 = b_1 = 0$, et donc aussi $a_1 + b_1 = 0$. Cela montre que $f + g \in B$ si $f, g \in B$. Le coefficient de $-f$ est égal à $-a_1$. Comme $f \in B$, on a $a_1 = 0$, et donc aussi $-a_1 = 0$. Cela montre que $-f \in B$ lorsque $f \in B$. Le coefficient de fg est égal à $a_0b_1 + a_1b_0$. Comme $f, g \in B$, on a $a_1 = b_1 = 0$, et donc aussi $a_0b_1 + a_1b_0 = 0$. Cela montre que $fg \in B$ si $f, g \in B$. Par conséquent, B est un sous-anneau de $\mathbb{Q}[X]$ **(2 pt)**.

Comme $\mathbb{Q} \subseteq B$ et $X^2, X^3 \in B$, le sous-anneau B de $\mathbb{Q}[X]$ est un sous-anneau de $\mathbb{Q}[X]$ contenant $\mathbb{Q}$, X^2 et X^3. Montrons que B est le plus petit sous-anneau de $\mathbb{Q}[X]$ contenant $\mathbb{Q}$, X^2 et X^3. Soit C un sous-anneau quelconque de $\mathbb{Q}[X]$ contenant $\mathbb{Q}$, X^2 et X^3. On doit montrer que $B \subseteq C$. Soit $f \in B$. Ecrivons

$$f = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n,$$

où $a_0, \ldots, a_n \in \mathbb{Q}$ et $n \in \mathbb{N}$. Comme $f \in B$, on a $a_1 = 0$. On peut donc écrire

$$f = a_0 + a_2X^2 + a_3X^3 + \cdots + a_nX^n.$$

On montre que chacun de ces monômes appartient à C, afin de montrer que f appartient à C. Comme C contient $\mathbb{Q}$ et X^2, l'anneau C contient

$$a_{2k} \cdot (X^2)^k = a_{2k}X^{2k},$$

quel que soit $k \in \mathbb{N}$. Les termes restants de f sont les termes de la forme $a_{2k+1}X^{2k+1}$ avec $k \in \mathbb{N}$, $k \geq 1$. Comme C contient $\mathbb{Q}$, X^2 et X^3, et comme $k \geq 1$, l'anneau C contient

$$a_{2k+1}X^3(X^2)^{k-1} = a_{2k+1}X^{2k+1},$$

quel que soit $k \geq 1$. Il s'ensuit que tous les monômes de f appartiennent à C, et que $B \subseteq C$ **(2 pt)**. Par conséquent, B est le plus petit sous-anneau de $\mathbb{Q}[X]$ contenant $\mathbb{Q}$, X^2 et X^3, c-à-d, $B = \mathbb{Q}[X^2, X^3]$.

c. Rappelons que $\mathbb{Q}[X]^\times = \mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$. Comme A est un sous-anneau de $\mathbb{Q}$, le groupe multiplicatif $A^\times$ de A est un sous-groupe de $\mathbb{Q}[X]^\times = \mathbb{Q}^\times$. Comme $\mathbb{Q}$ est un sous-anneau de A, on a aussi $\mathbb{Q}^\times \subseteq A^\times$. Par conséquent $A = \mathbb{Q}^\times$. **(1 pt)**

d. Notons que $X^2 \neq 0$ et que $X^2 \notin \mathbb{Q}^\times = A^\times$ **(1 pt)**. Supposons que $f, g \in A$ tels que $fg = X^2$. On a donc aussi $fg = X^2$ dans $\mathbb{Q}[X]$. D'après l'unicité de la décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$, on a 3 possibilités : soit f est inversible dans $\mathbb{Q}[X]$, soit f est associé à X dans $\mathbb{Q}[X]$, soit f est associé à X^2 dans $\mathbb{Q}[X]$. Le deuxième cas est exclu, sinon le polynôme f comporterait le monôme X avec un coefficient non nul. Du coup, soit f est inversible dans $\mathbb{Q}[X]$, soit f est associé à X^2 dans $\mathbb{Q}[X]$. Comme $A^\times = \mathbb{Q}[X]^\times$, et comme $f \in A$ et $X^2 \in A$, soit f est inversible dans A, soit f est associé à X^2 dans A **(2 pt)**. Cela montre bien que X^2 est irréductible dans A.

e. Comme $X^6 = X^2 \cdot X^4$ et $X^4, X^6 \in A$, l'élément X^2 divise X^6 dans A. L'élément X^6 est égal à $(X^3)^2$ dans A, mais X^2 ne divise pas X^3 dans A. En effet, s'il existait $f \in A$ tel que $X^2 f = X^3$, on aurait $f = X$ dans $\mathbb{Q}[X]$ et $X \in A$ ce qui est absurde. L'élément X^2 n'est donc pas premier dans A. **(3 pt)**

f. Dans un anneau factoriel, tout élément irréductible est premier. Comme A contient un élément irréductible non premier, A n'est pas factoriel. **(1 pt)**

g. Soit $f \in A$ non nul. On montre que f s'écrit comme un produit d'irréductibles de A et d'un inversible de A. Par récurrence sur le degré. Si $\deg(f) = 0$, alors f est un inversible de A car $f \neq 0$, et l'énoncé est vrai dans ce cas. Supposons que $\deg(f) \geq 1$ et que l'énoncé est vrai pour tout élément de A de degré $< \deg(f)$. Si f est irréductible, l'énoncé est vrai pour f. Sinon, $f = gh$ pour des éléments non inversibles g et h de A. On a alors $\deg(g), \deg(h) < \deg(f)$. Par hypothèse de récurrence, g et h s'écrivent chacun comme un produit d'irréductibles de A et d'un inversible de A. Leur produit f alors également. **(3 pt)**

h. Notons que $X^3 \neq 0$ et que $X^3 \notin \mathbb{Q}^\times = A^\times$ **(1 pt)**. Supposons que $f, g \in A$ tels que $fg = X^3$. On a donc aussi $fg = X^3$ dans $\mathbb{Q}[X]$. D'après l'unicité de la décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$, on a 4 possibilités : soit f est inversible dans $\mathbb{Q}[X]$, soit f est associé à X dans $\mathbb{Q}[X]$, soit f est associé à X^2 dans $\mathbb{Q}[X]$, soit f est associé à X^3 dans $\mathbb{Q}[X]$. Les deuxième et troisième cas sont exclus, sinon le polynôme f ou le polynôme g comporterait le monôme X avec un coefficient non nul. Du coup, soit f est inversible dans $\mathbb{Q}[X]$, soit f est associé à X^3 dans $\mathbb{Q}[X]$. Comme $A^\times = \mathbb{Q}[X]^\times$, et comme $f \in A$ et $X^3 \in A$, soit f est inversible dans A, soit f est associé à X^3 dans A **(2 pt)**. Cela montre bien que X^3 est irréductible dans A.

i. Supposons, par l'absurde, que X^2 et X^3 sont associés. Il existe alors un inversible u de A tel que $X^2 = uX^3$. Mais, $A^\times = \mathbb{Q}^\times$. En particulier $u \in \mathbb{Q}^\times$. Donc $2 = \deg(X^2) = \deg(uX^3) = \deg(u) + \deg(X^3) = 0 + 3 = 3$. Contradction. **(1 pt)**

j. On a $(X^2)^3 = (X^3)^2$. Comme X^2 et X^3 sont des irréductibles de A non associés, les deux décompositions en irréductibles de l'élément X^6 de A sont distinctes. **(2 pt)**

k. On a

$$X^{6(n-1)} = (X^2)^{3i}(X^3)^{2(n-1)-2i}$$

pour $i = 0, \ldots, n-1$. Cela fait n décompositions en irréductibles distinctes de l'élément $X^{6(n-1)}$ dans A. **(3 pt)**

l. Comme sous-anneaux de $\mathbb{Q}(X)$, on a

$$A_{X^2} = \{\tfrac{a_0+a_1X+a_2X^2+\cdots+a_nX^n}{X^{2m}} \mid a_0, a_1, a_2, \ldots, a_n \in \mathbb{Q},\ m, n \in \mathbb{N} \text{ avec } a_1 = 0\},$$

et

$$\mathbb{Q}[X]_X = \{\tfrac{f}{X^\ell} \mid f \in \mathbb{Q}[X],\ \ell \in \mathbb{N}\}.$$

On a évidemment l'inclusion $A_{X^2} \subseteq \mathbb{Q}[X]_X$. Pour montrer l'inclusion inverse, soit $\frac{f}{X^\ell}$ un élément de $\mathbb{Q}[X]_X$. Si ℓ est pair, la fraction

$$\tfrac{X^2 f}{X^{\ell+2}} = \tfrac{f}{X^\ell}$$

appartient à A_{X^2} car $X^2 f$ a coefficient 0 devant X, et $\ell + 2$ est pair. Si ℓ est impair, la fraction

$$\tfrac{X^3 f}{X^{\ell+3}} = \tfrac{f}{X^\ell}$$

appartient à A_{X^2} car $X^3 f$ a coefficient 0 devant X, et $\ell + 3$ est pair. Dans les deux cas, $\frac{f}{X^\ell}$ appartient à A_{X^2}. Cela montre donc l'inclusion $A_{X^2} \supseteq \mathbb{Q}[X]_X$. **(3 pt)**

Exercice 3. On déroule l'algorithme connu. Notons que

$$f = X_1^3 X_2^2 + \text{permutés}$$

et que

$$X_1^{e_1} X_2^{e_2} X_3^{e_3} = X_1^3 X_2^2$$

est le plus petit monôme de f **(1 pt)**. On a donc $e_1 = 3$, $e_2 = 2$ et $e_3 = 0$. Du coup, on retranche

$$\sigma_1^{e_1-e_2}\sigma_2^{e_2-e_3}\sigma_3^{e_3} = \sigma_1\sigma_2^2 = X_1^3X_2^2 + 2X_1^3X_2X_3 + 5X_1^2X_2^2X_3 + \text{permutés.} \quad \textbf{(5 pt)}$$

de f pour obtenir

$$f - \sigma_1\sigma_2^2 = -2X_1^3X_2X_3 - 5X_1^2X_2^2X_3 + \text{permutés.}$$

Le plus petit monôme de ce dernier est $-2X_1^3X_2X_3$. On a donc $e_1 = 3$ et $e_2 = e_3 = 1$. On rajoute donc

$$2\sigma_1^2\sigma_3 = 2X_1^3X_2X_3 + 4X_1^2X_2^2X_3 + \text{permutés} \quad \textbf{(5 pt)}$$

à $f - \sigma_1\sigma_2^2$ pour obtenir

$$f - \sigma_1\sigma_2^2 + 2\sigma_1^2\sigma_3 = -X_1^2X_2^2X_3 + \text{permutés.}$$

On y rajoute donc $\sigma_2\sigma_3$ pour obtenir

$$f - \sigma_1\sigma_2^2 + 2\sigma_1^2\sigma_3 + \sigma_2\sigma_3 = 0 \quad \textbf{(5 pt)}.$$

Autrement dit,

$$f = \sigma_1\sigma_2^2 - 2\sigma_1^2\sigma_3 - \sigma_2\sigma_3.$$

On prend donc

$$g = Y_1Y_2^2 - 2Y_1^2Y_3 - Y_2Y_3 \quad \textbf{(2 pt)}.$$

Exercice 4. Soit B une algèbre de décomposition de f sur A. On a donc

$$f = (T - x_1)\cdots(T - x_n) \quad \textbf{(2 pt)}$$

dans $B[T]$ pour certains $x_1, \ldots, x_n \in B$, et

$$\Delta(f) = \prod_{1\leq i<j\leq n}(x_i - x_j)^2 \quad \textbf{(2 pt)}$$

dans B.

Le polynôme Tf se décompose complètement dans $B[T]$ car

$$Tf = T(T - x_1)\cdots(T - x_n) = (T - 0)(T - x_1)\cdots(T - x_n) \quad \textbf{(4 pt)}.$$

dans $B[T]$. On en déduit, en posant $x_0 = 0$, que

$$\Delta(Tf) = \prod_{0\leq i<j\leq n}(x_i - x_j)^2 = \prod_{j=1}^{n}(0 - x_j)^2 \cdot \prod_{1\leq i<j\leq n}(x_i - x_j)^2 = f(0)^2\Delta(f) \quad \textbf{(4 pt)}$$

dans B. Comme A est un sous-anneau de B et $\Delta(Tf)$, $f(0)$ et $\Delta(f)$ appartiennent à A, on a également

$$\Delta(Tf) = f(0)^2\Delta(f)$$

dans A **(2 pt)**.

Exercice 5. a. Le polynôme $X^n - 2$ dans $\mathbb{Q}[X]$ est non nul et s'annule en $\sqrt[n]{2}$. Le nombre complexe $\sqrt[n]{2}$ est donc algébrique sur $\mathbb{Q}$. **(1 pt)**

b. Le polynôme $X^n - 2$ satisfait le critère d'Eisenstein pour $p = 2$. Il est donc irréductible dans $\mathbb{Q}[X]$. Comme il est également unitaire et s'annule en $\sqrt[n]{2}$, c'est le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbb{Q}$. **(1 pt)**

c. Comme $\sqrt[n]{2}$ est algébrique sur $\mathbb{Q}$, on a $\mathbb{Q}(\sqrt[n]{2}) = \mathbb{Q}[\sqrt[n]{2}]$ et

$$[\mathbb{Q}[\sqrt[n]{2}] : \mathbb{Q}] = \deg_{/\mathbb{Q}}(\sqrt[n]{2}) = \deg(X^n - 2) = n \quad \textbf{(2 pt)}.$$

d. Si $K_m \subseteq K_n$, on a

$$n = [K_n : \mathbb{Q}] = [K_n : K_m] \cdot [K_m : \mathbb{Q}] = [K_n : K_m] \cdot m.$$

En particulier, m divise n **(2 pt)**.

Supposons réciproquement que m divise n, et soit $k \in \mathbb{N}$ tel que $km = n$. Alors

$$(\sqrt[n]{2})^k = 2^{\frac{k}{n}} = 2^{\frac{1}{m}} = \sqrt[m]{2}.$$

D'où $\sqrt[n]{2}$ appartient à K_n, et donc

$$K_m = \mathbb{Q}[\sqrt[m]{2}] \subseteq \mathbb{Q}[\sqrt[n]{2}] = K_n \quad \textbf{(2 pt)}.$$

e. Comme on a vu dans le d, si $K_m \subseteq K_n$, on a

$$[K_n : K_m] = \tfrac{n}{m} \quad \textbf{(2 pt)}.$$

f. Les racines de X^n-2 dans $\mathbb{C}$ sont les nombres complexes $z_1,\dots,z_6$. La clôture normale de $K_6/\mathbb{Q}$ dans $\bar{\mathbb{Q}}/\mathbb{Q}$ est donc

$$\mathbb{Q}(z_1,\dots,z_6)=\mathbb{Q}(\sqrt[6]{2},\xi)=K_6(\xi) \quad \textbf{(4 pt)}.$$

g. Le polynôme minimal de ξ sur $\mathbb{Q}$ est X^2-X+1. En effet, ξ est racine de X^2-X+1, le polynôme X^2-X+1 est unitaire et appartient à $\mathbb{Q}[X]$, et il est irréductible dans $\mathbb{Q}[X]$ n'ayant même pas de racine dans $\mathbb{R}$ et étant de degré ≤ 3. Comme $K_6=\mathbb{Q}(\sqrt[6]{2})$ est un sous-corps de $\mathbb{R}$, le polynôme minimal de ξ sur K_6 est X^2-X+1 par les mêmes raisons. Du coup, l'extension $K_6(\xi)/K_6$ est de degré 2 **(2 pt)**. Il s'ensuit que

$$[K_6(\xi):\mathbb{Q}]=[K_6(\xi):K_6]\cdot[K_6:\mathbb{Q}]=2\cdot 6=12 \quad \textbf{(2 pt)}.$$

h. Comme $K_6(\xi)$ est normale, la restriction à $K_6(\xi)$ de la conjugaison complexe est un automorphisme de l'extension $K_6(\xi)/\mathbb{Q}$ **(2 pt)**. On a

$$\sigma(\sqrt[6]{2})=\sqrt[6]{2}$$

car $\sqrt[6]{2}$ est réel, et

$$\sigma(\xi)=\overline{\xi}=\xi^{-1}$$

car $|\xi|=1$. Du coup,

$$\sigma(z_i)=\sigma(\xi^i\sqrt[6]{2})=\xi^{-i}\sqrt[6]{2}$$

pour $i=1,\dots,6$. Comme $\xi^6=1$, on a bien

$$\sigma(z_1)=z_5,\ \sigma(z_2)=z_4,\ \sigma(z_3)=z_3,\ \sigma(z_4)=z_2,\ \sigma(z_5)=z_1,\ \sigma(z_6)=z_6.$$

i. Comme $z_1=\xi\sqrt[6]{2}$ et $z_6=\sqrt[6]{2}$ ont tous les deux X^6-2 comme polynôme minimal sur $\mathbb{Q}$, il existe un morphisme d'extensions

$$\rho\colon \mathbb{Q}(z_6)/\mathbb{Q}\to\mathbb{Q}(z_1)/\mathbb{Q}$$

avec $\rho(z_6)=z_1$ **(2 pt)**.

Comme $z_1\in K_6(\xi)$ et $z_1\notin K_6$, l'élément z_1 de $K_6(\xi)$ est algébrique sur K_6 de degré 2. Déterminons le polynôme minimal de z_1 sur $\mathbb{Q}$. Comme $K_6(\xi)/K$ est une extension galoisienne, le corps fixe de σ défini ci-dessus est $K_6(\xi)^\sigma=K_6$. Le polynôme minimal de z_1 sur K_6 est donc

$$(X-z_1)(X-\overline{z_1})=(X-\xi\sqrt[6]{2})(X-\xi^{-1}\sqrt[6]{2})=X^2-\sqrt[6]{2}X+\sqrt[3]{2}.$$

Le polynôme

$$\rho(X^2-\sqrt[6]{2}X+\sqrt[3]{2})=X^2-\xi\sqrt[6]{2}X+\xi^2\sqrt[3]{2}\in\mathbb{Q}(z_1)[X]$$

a z_2 comme racine. En effet,

$$(\xi^2\sqrt[6]{2})^2-\xi\sqrt[6]{2}\cdot\xi^2\sqrt[6]{2}+\xi^2\sqrt[3]{2}=(\xi^2-\xi+1)\xi^2\sqrt[3]{2}=0.$$

Il existe donc une extension de ρ à $K_6(z_1)=K_6(\xi)$, de nouveau notée par ρ, avec $\rho(z_1)=z_2$. Comme $K_6(\xi)/\mathbb{Q}$ est normale, cette extension ρ est un automorphisme de $K_6(\xi)/\mathbb{Q}$ **(4 pt)**.

Comme

$$\rho(\sqrt[6]{2})=\xi\sqrt[6]{2} \quad \text{et} \quad \rho(\xi\sqrt[6]{2})=\xi^2\sqrt[6]{2},$$

on a

$$\rho(\xi)=\rho(\tfrac{\xi\sqrt[6]{2}}{\sqrt[6]{2}})=\tfrac{\xi^2\sqrt[6]{2}}{\xi\sqrt[6]{2}}=\xi.$$

D'où

$$\rho(z_1)=z_2,\ \rho(z_2)=z_3,\ \rho(z_3)=z_4,\ \rho(z_4)=z_5,\ \rho(z_5)=z_6,\ \rho(z_6)=z_1.$$

j. On définit un morphisme de groupes

$$\alpha\colon \mathrm{Gal}(K_6(\xi)/\mathbb{Q})\to S_6$$

en posant $\alpha(\tau)$ l'unique permutation χ de l'ensemble $\{1,2,3,4,5,6\}$ avec $\tau(z_i)=z_{\chi(i)}$ quel que soit i. Ce morphisme est injectif car l'extension $K_6(\xi)/\mathbb{Q}$ est engendrée par $z_1,\dots,z_6$ **(2 pt)**. Son image contient les permutations π et ω ci-dessus. Comme le sous-groupe engendré $\langle\pi,\omega\rangle$ de S_6 est isomorphe au groupe diédral D_6, on en déduit un morphisme de groupes injectif

$$\alpha'\colon \mathrm{Gal}(K_6(\xi)/\mathbb{Q})\to D_6.$$

Comme l'extension $K_6(\xi)/\mathbb{Q}$ est galoisienne,

$$|\mathrm{Gal}(K_6(\xi)/\mathbb{Q})|=[K_6(\xi):\mathbb{Q}]=12.$$

Comme $|D_6|=12$ également, le morphisme injectif α' ci-dessus est un isomorphisme **(2 pt)**.