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

ALGEBRE

Examen terminal, 10 janvier 2019, 14h00–17h00

CORRIGE et BAREME

Exercice 1. a. De manière générale, on a vu que l'image d'une partie multiplicative par un morphisme d'anneaux est une partie multiplicative. **(2 pt)**

b. On a $1 = 1 \cdot 1 \in ST$ car $1 \in S$ et $1 \in T$. Soient $r, r' \in ST$. Il existe donc $s, s' \in S$ et $t, t' \in T$ tels que $r = st$ et $r' = s't'$. Du coup, $rr' = sts't' = ss' \cdot tt' \in ST$ car $ss' \in S$ et $tt' \in T$. **(2 pt)**

c. Soit $\lambda\colon S^{-1}A \to \iota(T)^{-1}(S^{-1}A)$ le morphisme de localisation de l'anneau $S^{-1}A$ par la partie multiplicative $\iota(T)$. On note

$$\mu = \lambda \circ \iota\colon A \to \iota(T)^{-1}(S^{-1}A)$$

la composition de λ et ι. Il suffit de montrer que le morphisme μ satisfait la propriété universelle de la localisation de l'anneau A par la partie multiplicative ST.

Tout d'abord, il faut vérifier que μ rend inversibles tous les éléments de ST. Comme $\mu(st) = \mu(s)\mu(t)$, il suffit de vérifier que μ rend inversibles les éléments de S et les éléments de T. Or, ι rend inversibles les éléments de S, et λ rend inversibles les éléments de $\iota(T)$, par construction de la localisation. Il s'ensuit que $\mu = \lambda \circ \iota$ rend inversibles les éléments de S et de T. **(3 pt)**

Ensuite, on vérifie l'universalité. Soit $f\colon A \to B$ un morphisme d'anneaux tel que $f(ST) \subseteq B^\times$. Comme $S \subseteq ST$, on a, en particulier, que $f(S) \subseteq B^\times$. D'après la propriété universelle de la localisation de A par S, il existe un unique morphisme $f'\colon S^{-1}A \to B$ tel que $f' \circ \iota = f$. Comme $T \subseteq ST$, on a

$$f'(\iota(T)) = f' \circ \iota(T) = f(T) \subseteq B^\times,$$

c-à-d, f' rend inversibles les éléments de $\iota(T)$. D'après la propriété universelle de la localisation de $S^{-1}A$ par $\iota(T)$, il existe un unique morphisme $f''\colon \iota(T)^{-1}(S^{-1}A) \to B$ tel que $f'' \circ \lambda = f'$. Il s'ensuit que

$$f'' \circ \mu = f'' \circ \lambda \circ \iota = f' \circ \iota = f. \quad \textbf{(3 pt)}$$

Il nous reste à montrer que f'' est l'unique morphisme ayant cette propriété. Supposons que $f'''\colon \iota(T)^{-1}(S^{-1}A) \to B$ est un morphisme d'anneaux avec $f''' \circ \mu = f$. On a donc $(f''' \circ \lambda) \circ \iota = f$. Par unicité de f', on a $f''' \circ \lambda = f'$. Par unicité de f'', on a $f''' = f''$. **(3 pt)**

d. Comme $ST = TS$, on obtient

$$\iota(T)^{-1}(S^{-1}A) \cong (ST)^{-1}A = (TS)^{-1}A \cong \kappa(S)^{-1}(T^{-1}A)$$

en appliquant le c deux fois. **(2 pt)**

Exercice 2. Comme le quotient et la localisation commutent, on a

$$(\mathbb{F}_2[X]/(X^4 - X))_{\bar{X}^5} \cong (\mathbb{F}_2[X]_{X^5})/(X^4 - X). \quad \textbf{(2 pt)}$$

Or, $\mathbb{F}_2[X]_{X^5} = \mathbb{F}_2[X]_X$, comme sous-anneaux du corps des fractions $\mathbb{F}_2(X)$. Du coup,

$$(\mathbb{F}_2[X]_{X^5})/(X^4 - X) \cong (\mathbb{F}_2[X]_X)/(X^4 - X). \quad \textbf{(2 pt)}$$

Comme X est inversible dans $\mathbb{F}_2[X]_X$, les idéaux $(X^4 - X)$ et $(X^3 - 1)$ sont égaux, et on a

$$(\mathbb{F}_2[X]_X)/(X^4 - X) \cong (\mathbb{F}_2[X]_X)/(X^3 - 1). \quad \textbf{(2 pt)}$$

En échangeant encore localisation et quotient, on a

$$(\mathbb{F}_2[X]_X)/(X^3 - 1) \cong (\mathbb{F}_2[X]/(X^3 - 1))_{\bar{X}}. \quad \textbf{(2 pt)}$$

Comme $\bar{X}^3 = 1$ dans le quotient $\mathbb{F}_2[X]/(X^3 - 1)$, l'élément $\bar{X}$ est inversible. Du coup,

$$(\mathbb{F}_2[X]/(X^3 - 1))_{\bar{X}} \cong \mathbb{F}_2[X]/(X^3 - 1). \quad \textbf{(2 pt)}$$

Il s'ensuit que le cardinal de l'anneau en question est égal à 2^3. **(2 pt)**

Exercice 3. a. Pour $d \in \mathbb{N}$, notons A_d le sous-ensemble des fractions de $\mathbb{R}(X,Y)$ de la forme $\frac{H}{(X^2+Y^2)^d}$ avec H homogène de degré $2d$. Ce sous-ensemble de $\mathbb{R}(X,Y)$ est évidemment un sous-groupe additif. Notons que $A_d \subseteq A_{d+1}$ car

$$\frac{H}{(X^2+Y^2)^d} = \frac{H(X^2+Y^2)}{(X^2+Y^2)^{d+1}}.$$

De plus,

$$A = \bigcup_{d\in\mathbb{N}} A_d,$$

et est donc un sous-groupe additif de $\mathbb{R}(X,Y)$ comme réunion croissante de sous-groupes additifs. **(1 pt)**

Il est clair que $1 \in A$ et que A est stable pour le produit **(1 pt)**. Le sous-ensemble A de $\mathbb{R}(X,Y)$ est donc un sous-anneau.

b. On sait que le polynôme $P \in \mathbb{R}[Z]$ s'écrit sous la forme

$$P = u \cdot Q_1 \cdots Q_r \cdot Q_{r+1} \cdots Q_{r+s},$$

où $u \in \mathbb{R}^\star$, $Q_1, \ldots, Q_{r+s} \in \mathbb{R}[Z]$, avec $Q_1, \ldots, Q_r$ de degré 1 et $Q_{r+1}, \ldots, Q_{r+s}$ de degré 2 et irréductibles, i.e., de discriminant strictement négatif **(1 pt)**. Notons que $\deg(P) = r+2s$. Comme $H = P(\frac{X}{Y})Y^{2d}$ est un polynôme en X et Y, le polynôme P est de degré au plus $2d$. En particulier, $r+2s \leq 2d$. Posons $t = 2d-(r+2s)$. Du coup,

$$H = \frac{H}{Y^{2d}} \cdot Y^{2d} = P(\tfrac{X}{Y}) \cdot Y^{2d} = \\ u \cdot Y^t \cdot Q_1(\tfrac{X}{Y})Y \cdots Q_r(\tfrac{X}{Y})Y \cdot Q_{r+1}(\tfrac{X}{Y})Y^2 \cdots Q_{r+s}(\tfrac{X}{Y})Y^2. \quad \textbf{(3 pt)}$$

Remarquons que $P_i = Q_i(\frac{X}{Y})Y$ est un polynôme homogène de degré 1 en X et Y pour $i = 1, \ldots, r$, et que $P_i = Q_i(\frac{X}{Y})Y^2$ est un polynôme homogène de degré 2 en X et Y pour $i = r+1, \ldots, r+s$. Comme Y^t est également un produit de polynômes homogènes de degré 1, l'écriture demandée en découle si on montre que les polynômes homogènes $P_{r+1}, \ldots, P_{r+s}$ sont bien irréductibles dans $\mathbb{R}[X.Y]$. Or, si P_i était réductible, pour i entre $r+1$ et $r+s$, il serait produit de deux polynômes homogènes R et S de degré 1. On aurait également

$$Q_i(\tfrac{X}{Y}) = \frac{P_i}{Y^2} = \frac{R}{Y} \cdot \frac{S}{Y} = T(\tfrac{X}{Y}) \cdot U(\tfrac{X}{Y}),$$

pour certains polynômes $T, U \in \mathbb{R}[Z]$. On aurait donc $Q = TU$ dans $\mathbb{R}[Z]$. Comme R et S sont de degré 1, les polynômes T et U seraient de degré au plus 1. Comme Q_i est de degré 2, ils seraient tous les deux de degré égal à 1. Cela contredirait le fait que Q_i est irréductible dans $\mathbb{R}[Z]$. **(2 pt)**

c. L'anneau $\mathbb{R}[X,Y]$ étant factoriel, l'unicité de cette écriture est l'unicité de la décomposition d'un polynôme non nul de $\mathbb{R}[X,Y]$ en facteurs irréductibles. Explicitement, cela veut dire que, si de plus

$$H = v \cdot Q_1 \cdots Q_{r'} \cdot Q_{r'+1} \cdots Q_{r'+s'},$$

où $v \in \mathbb{R}^\star$, $Q_1, \ldots, Q_{r'+s'} \in \mathbb{R}[X,Y]$ sont homogènes et irréductibles, avec $Q_1, \ldots, Q_{r'}$ de degré 1 et $Q_{r'+1}, \ldots, Q_{r'+s'}$ de degré 2, et $r', s' \in \mathbb{N}$, alors $r' = r$, $s' = s$, et il existe des permutations σ de l'ensemble $\{1, \ldots, r\}$ et τ de l'ensemble $\{r+1, \ldots, r+s\}$ telles que Q_i soit associé à $P_{\sigma(i)}$ dans $\mathbb{R}[X,Y]$ pour $i = 1, \ldots, r$, et Q_i soit associé à $P_{\tau(i)}$ pour $i = r+1, \ldots, r+s$. **(2 pt)**

d. Ecrivons

$$F = \frac{H}{(X^2+Y^2)^d}$$

où d est un entier naturel et $H \in \mathbb{R}[X,Y]$ est un polynôme homogène de degré $2d$. On peut supposer que H et X^2+Y^2 sont premiers entre eux. (D'ailleurs, comme $\frac{X^2+Y^2}{Y^2} = (\frac{X}{Y})^2+1$ est le polynôme irréductible Z^2+1 évalué en $\frac{X}{Y}$, le polynôme X^2+Y^2 est irréductible dans $\mathbb{R}[X,Y]$ comme on a vu ci-dessus. La condition que H et X^2+Y^2 sont premiers entre eux revient donc à dire que X^2+Y^2 ne divise pas H.) D'après le b, il existe $u, P_1, \ldots, P_{r+s}$ comme au c tels que

$$F = u \cdot \frac{P_1 \cdots P_r \cdot P_{r+1} \cdots P_{r+s}}{(X^2+Y^2)^d}.$$

Comme l'irréductible X^2+Y^2 ne divise pas le numérateur, aucun des P_i n'est associé à X^2+Y^2. **(2 pt)**

e. L'unicité de la décomposition en irréductibles d'une fraction non nulle de $\mathbb{R}(X,Y)$ implique que la décomposition du d est unique dans le sens suivant. Supposons que

$$F = v \cdot \frac{Q_1 \cdots Q_{r'} \cdot Q_{r'+1} \cdots Q_{r'+s'}}{(X^2+Y^2)^e}$$

est une autre décomposition comme au d. Alors, $r' = r$, $s' = s$, $e = d$, et il existe des permutations σ de l'ensemble $\{1,\dots,r\}$ et τ de l'ensemble $\{r+1,\dots,r+s\}$ telles que Q_i soit associé à $P_{\sigma(i)}$ pour $i = 1,\dots,r$, et que Q_i soit associé à $P_{\tau(i)}$ pour $i = r+1,\dots,r+s$. **(2 pt)**

f. D'après ce qui précède, les diviseurs dans A, à association près, de

$$F = u \cdot \frac{P_1 \cdots P_r \cdot P_{r+1} \cdots P_{r+s}}{(X^2+Y^2)^d}$$

dans sa décomposition établie au d, sont les fractions

$$D_\varepsilon = \frac{P_1^{\varepsilon_1} \cdots P_r^{\varepsilon_r} \cdot P_{r+1}^{\varepsilon_{r+1}} \cdots P_{r+s}^{\varepsilon_{r+s}}}{(X^2+Y^2)^{|\varepsilon|}},$$

où $\varepsilon = (\varepsilon_1,\dots,\varepsilon_{r+s}) \in \{0,1\}^{r+s}$ tel que $\varepsilon_1 + \cdots + \varepsilon_r$ est pair, et où

$$|\varepsilon| = \tfrac{1}{2}\varepsilon_1 + \cdots + \tfrac{1}{2}\varepsilon_r + \varepsilon_{r+1} \cdots + \varepsilon_{r+s}.$$

Il suffit de montrer que toute suite croissante d'idéaux principaux non nuls de A est stationnaire. Soit (I_n) une telle suite. Soit F un générateur de I_0. Comme $I_0 \subseteq I_n$, l'idéal I_n est engendré par une diviseur de F de la forme D_{ε_n}, pour unique $\varepsilon_n \in \{0,1\}^{r+s}$. Comme $I_n \subseteq I_{n+1}$, on a $\varepsilon_{n+1} \leq \varepsilon_n$ pour l'ordre partiel produit sur $\{0,1\}^{r+s}$. Comme ce dernier ensemble est fini, la suite (ε_n) est stationnaire, et donc aussi la suite (I_n). **(6 pt)**

g. Les diviseurs de $\frac{P_1P_2}{X^2+Y^2}$ dans A, à association près, sont

$$D_\varepsilon = \frac{P_1^{\varepsilon_1} P_2^{\varepsilon_2}}{(X^2+Y^2)^{|\varepsilon|}},$$

où $\varepsilon = (\varepsilon_1,\varepsilon_2) \in \{0,1\}^2$ avec $\varepsilon_1 + \varepsilon_2$ pair. Du coup, les seuls diviseurs de $\frac{P_1P_2}{X^2+Y^2}$ dans A, à association près, sont

$$1 \quad \text{et} \quad \frac{P_1P_2}{X^2+Y_2}.$$

Il s'ensuit que $\frac{P_1P_2}{X^2+Y^2}$ est irréductible dans A. **(2 pt)**

Le cas de l'irréductibilité de $\frac{P}{X^2+Y^2}$ est plus facile : ses diviseurs dans A, à association près, sont

$$D_\varepsilon = \frac{P^\varepsilon}{(X^2+Y^2)^\varepsilon},$$

où $\varepsilon = 0$ ou 1. Cela implique de suite que $\frac{P}{X^2+Y^2}$ est irréductible dans A. **(2 pt)**

h. On a les deux décompositions en irréductibles distinctes suivantes du même élément non nul de A :

$$\frac{X^2}{X^2+Y^2} \cdot \frac{Y^2}{X^2+Y^2} = \frac{XY}{X^2+Y^2} \cdot \frac{XY}{X^2+Y^2}. \quad \textbf{(4 pt)}$$

i. D'après ce qu'on a vu ci-dessus, les seuls diviseurs communs de U et V dans A sont les fractions constantes. Si I était donc principal, on aurait eu $I = A$, ce qui est absurde compte tenu de la question suivante. **(4 pt)**

j. Soit $f\colon A \to \mathbb{R}$ le morphisme d'évaluation en $(1,-1)$. Le morphisme f étant surjectif et $\mathbb{R}$ étant un corps, $\ker(f)$ est un idéal maximal de A. Comme $U, V \in \ker(f)$, on a $I \subseteq \ker(f)$. **(2 pt)**

On montre l'inclusion réciproque. Soit $F \in \ker(f)$. Comme $F(1,-1) = 0$, on a $r \neq 0$ dans l'écriture du d. Comme r est pair, $r \geq 2$. Il s'ensuit que F est divisible dans A par un élément de la forme

$$\frac{(X+Y)(aX+bY)}{X^2+Y^2},$$

pour certains $a, b \in \mathbb{R}$. Comme les formes lineaires $X+Y$ et $X-Y$ engendrent l'espace vectoriel réel des formes linéaires en X et Y, il existe $\lambda, \mu \in \mathbb{R}$ tel que

$$aX + bY = \lambda(X+Y) + \mu(X-Y).$$

Il s'ensuit que

$$\frac{(X+Y)(aX+bY)}{X^2+Y^2} = \frac{(X+Y)(\lambda(X+Y)+\mu(X-Y))}{X^2+Y^2} = \\ \lambda \cdot \frac{(X+Y)^2}{X^2+Y^2} + \mu \cdot \frac{X^2-Y^2}{X^2+Y^2} = \lambda U + \mu V \in I.$$

Par conséquent, $F \in I$ également. **(6 pt)**

Exercice 4. On a

$$\sigma_1^4 = (X_1+X_2+X_3)^4 = (X_1+X_2+X_3)^3(X_1+X_2+X_3) = \\ (X_1^3+X_2^3+X_3^3)(X_1+X_2+X_3) = X_1^4 + X_1^3X_2 + \text{permutés}.$$

Du coup,

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

On a

$$\sigma_1^2\sigma_2 = (X_1+X_2+X_3)^2(X_1X_2+X_1X_3+X_2X_3) = \\ (X_1^2+X_2^2+X_3^2+2X_1X_2+2X_1X_3+2X_2X_3)(X_1X_2+X_1X_3+X_2X_3) = \\ X_1^3X_2 + 5X_1^2X_2X_3 + 2X_1^2X_2^2 + \text{permutés}.$$

Du coup,

$$X_1^4+X_2^4+X_3^4 = \sigma_1^4 - \sigma_1^2\sigma_2 + 2X_1^2X_2^2 + 2X_1^2X_2X_3 + \text{permutés}. \quad \textbf{(5 pt)}$$

On a

$$\sigma_2^2 = (X_1X_2+X_1X_3+X_2X_3)^2 = X_1^2X_2^2 + 2X_1^2X_2X_3 + \text{permutés}.$$

Du coup,

$$X_1^4+X_2^4+X_3^4 = \sigma_1^4 - \sigma_1^2\sigma_2 + 2\sigma_2^2 + X_1^2X_2X_3 + \text{permutés}. \quad \textbf{(5 pt)}$$

On a

$$\sigma_1\sigma_3 = (X_1+X_2+X_3)X_1X_2X_3 = X_1^2X_2X_3 + \text{permutés}.$$

Du coup,

$$X_1^4+X_2^4+X_3^4 = \sigma_1^4 - \sigma_1^2\sigma_2 + 2\sigma_2^2 + \sigma_1\sigma_3. \quad \textbf{(5 pt)}$$

On prend donc

$$g = Y_1^4 + 2Y_1^2Y_2 + 2Y_2^2 + Y_1Y_3.$$

Exercice 5. a. On montre que $\text{Rés}(X^6-1, X^4-2) = 0$ dans $\mathbb{F}_7$ pour les polynômes X^6-1 et X^4-2 dans $\mathbb{F}_7[X]$ **(2 pt)** en montrant qu'ils ont une racine commune dans $\mathbb{F}_7$ même **(2 pt)**. D'après le petit théorème de Fermat, l'ensemble des racines de X^6-1 dans $\mathbb{F}_7$ est $\mathbb{F}_7^\star$. Il suffit donc de montrer que 2 possède une racine 4-ième dans $\mathbb{F}_7^\star = \mathbb{F}_7^\times$. Comme $\mathbb{F}_7^\times$ est cyclique d'ordre 6, l'ensemble des puissances 4-ièmes dans $\mathbb{F}_7^\times$ coïncide avec l'ensemble des carrés dans $\mathbb{F}_7^\times$. Il suffit donc de vérifier que 2 est un carré dans $\mathbb{F}_7^\times$. Comme

$$2^{\frac{7-1}{2}} = 2^3 = 1$$

dans $\mathbb{F}_7$, l'élément 2 est bien un carré dans $\mathbb{F}_7^\times$. Cela montre que X^6-1 et X^4-2 ont une racine commune dans $\mathbb{F}_7$. **(3 pt)**

b. On a

$$\text{Rés}(X^6-1, X^4-2) = ((\sqrt[4]{2})^6-1)((-\sqrt[4]{2})^6-1)((i\sqrt[4]{2})^6-1)((-i\sqrt[4]{2})^6-1) = \\ ((\sqrt{2})^3-1)^2(-(\sqrt{2})^3-1)^2 = (1-2^3)^2 = 49. \quad \textbf{(6 pt)}$$