Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE PARCOURS 1

ALGEBRE ET GEOMETRIE

Examen terminal, le 9 janvier 2014, 13h30-16h30

CORRIGE ET BAREME

Question de cours. Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$. Il existe $q, r \in \mathbb{Z}$ tels que $b = qa + r$, où $0 \leq r < |a|$ **(1 pt)**. De plus, q et r sont uniquement déterminés par ces conditions **(1 pt)**.

Exercice 1. a. Non. Contre-exemple : soit $E = \{0, 1\}$ et soit f l'application de E dans lui-même définie par $f(0) = 1$ et $f(1) = 0$. On a bien $f \circ f = \mathrm{id}$, mais $f \neq \mathrm{id}$. **(0,5 pt)**

b. Non. Contre-exemple : soit $E = \{0, 1, 2\}$ et f définie par $f(0) = 1$, $f(1) = 2$, $f(2) = 0$. On a bien $f \circ f \circ f = \mathrm{id}$, mais $f \neq \mathrm{id}$. **(0,5 pt)**

c. Oui. Supposons que $f \circ f = \mathrm{id}$ et $f \circ f \circ f = \mathrm{id}$. On a alors

$$\mathrm{id} = f \circ f \circ f = (f \circ f) \circ f = \mathrm{id} \circ f = f,$$

car $f \circ f = \mathrm{id}$. D'où $f = \mathrm{id}$. **(0,5 pt)**

d. Supposons que $f \circ f$ est injective, et montrons que f l'est. Supposons que $x, y \in E$ sont tels que $f(x) = f(y)$. On montre que $x = y$. En appliquant f de deux côtés à l'égalité $f(x) = f(y)$, on obtient

$$(f \circ f)(x) = f(f(x)) = f(f(y)) = (f \circ f)(y).$$

Comme $f \circ f$ est injective, on en déduit que $x = y$, et f est injective. **(0,5 pt)**

e. Supposons que $f \circ f$ est surjective. Montrons que f l'est. Soit $y \in E$. Comme $f \circ f$ est surjective de E dans E, il existe $z \in E$ tel que $(f \circ f)(z) = y$, i.e., $f(f(z)) = y$. Posons $x = f(z)$. On a bien $x \in E$ et $f(x) = f(f(z)) = y$. Cela momtre que f est surjective. **(0,5 pt)**

f. Supposons que $f \circ f$ est bijective. Elle est donc injective et surjective. D'après les questions d et e ci-dessus, f est injective et surjective. Par conséquent, f est bijective. **(0,5 pt)**

Exercice 2. a. Montrons que la relation R est réflexive. Soit $f \in \mathcal{F}$. On a bien-sûr $f(x) \leq f(x)$ quel que soit $x \in \mathbb{R}$. D'ou $f\,R\,f$, et R est réflexive.

Montrons que la relation R est anti-symétrique. Soient $f, g \in \mathcal{F}$. Supposons que $f \leq g$ et que $g \leq f$. Cela veut dire que $f(x) \leq g(x)$ et $g(x) \leq f(x)$, quel que soit $x \in \mathbb{R}$. On a donc $f(x) = g(x)$ quel que soit $x \in \mathbb{R}$. On en déduit que $f = g$, et R est anti-symétrique.

Montrons la transitivité de R. Soient $f, g, h \in \mathcal{F}$. Supposons que $f \leq g$ et que $g \leq h$. Cela veut dire que $f(x) \leq g(x)$ et $g(x) \leq h(x)$, quel que soit $x \in \mathbb{R}$. On a donc $f(x) \leq h(x)$ quel que soit $x \in \mathbb{R}$, ce qui veut dire que $f\,R\,h$. La relation R est bien transitive.

La relation R étant réflexive, anti-symétrique et transitive, elle est un ordre partiel sur $\mathcal{F}$. **(0,5 pt)**

b. Non. Soit f la focntion définie par $f(x) = x$, et g la fonction définie par $g(x) = -x$. On n'a ni $f\,R\,g$ (car $f(1) > g(1)$), ni $g\,R\,f$ (car $g(-1) > f(-1)$). La relation R n'est donc pas totale. **(0,5 pt)**

Exercice 3. a. On montre que le reste dans la division euclidienne de a^n par 61 est égal à 1 pour tout $n \in \mathbb{N}^\star$. Pour $n = 1$ c'est vrai par hypothèse. Supposons que l'énoncé est vrai au rang n, pour un certain entier naturel non nul n, et montrons-le au rang $n + 1$. Plus explicitement, on suppose que le reste dans la division euclidienne de a^n par 61 est égal à 1, pour un certain entier naturel non nul n. On montre que le reste dans la division euclidienne de a^{n+1} par 61 est égal à 1. Or, comme le reste dans la division euclidienne de a^n par 61 est égal à 1, on a $a^n = q \times 61 + 1$, pour un certain entier relatif q. De plus, comme le reste dans la division euclidienne de a par 61 est égal à 1, on a aussi $a = q' \times 61 + 1$. Il s'ensuit que

$$a^{n+1} = a \times a^n = (q' \times 61 + 1) \times (q \times 61 + 1) = (qq' + q + q') \times 61 + 1.$$

Comme $qq' + q + q'$ est un entier relatif, et $0 \leq 1 < 61$, cette expression est la division euclidienne de a^{n+1} par 61.

On en déduit que le reste dans la division euclidienne de a^{n+1} par 61 est égal à 1. **(1 pt)**

b. Effectuons la division eulcidienne de 2014 par 61 : on obtient $2014 = 33 \times 61 + 1$. En particulier, le reste dans la division euclidienne de 2014 par 61 est égal à 1. D'après le a, le reste dans la division euclidienne de 2014^n par 61 est égal à 1 quel que soit $n \in \mathbb{N}^\star$. En particulier, le reste dans la division euclidienne de 2014^{2014} par 61 est égal à 1. **(1 pt)**

Exercice 4. a. Supposons que d est un diviseur commun de a et b. Comme d divise a, l'entier d divise $2a$. De même, comme d divise b, l'entier d divise $5b$. Du coup, d divise aussi la somme $2a + 5b$. De même, d divise $a + 3b$. Par conséquent, d est diviseur commun de $2a + 5b$ et $a + 3b$. **(0,5 pt)**

b. Supposons que d divise $2a + 5b$ et $a + 3b$. Il divise donc aussi $2 \times (a + 3b)$. Du coup, il divise la différence $2(a + 3b) - (2a + 5b) = b$, et aussi $(a + 3b) - 3b = a$. L'entier d est donc diviseur commun de a et b. **(1 pt)**

c. D'après ce qui précède, l'ensemble des diviseurs communs de a et b coïncide avec l'ensemble des diviseurs communs de $a + 2b$ et $a + 3b$. Du coup, ces deux ensembles ont le même plus grand élément, i.e., $\text{pgcd}(a, b) = \text{pgcd}(2a + 5b, a + 3b)$. **(0,5 pt)**

Exercice 5. a et b. On effectue l'algorithme d'Euclide étendu sur les polynômes A et B :

i	R_{i-2}	R_{i-1}	Q_i	R_i	U_i	V_i
-1					1	0
0					0	1
1	$2X^5 - 10X^4 + 21X^3 - 24X^2 + 12X$	$X^4 - 4X^3 + 7X^2 - 7X + 2$	$2X - 2$	$-X^3 + 4X^2 - 6X + 4$	1	$-2X + 2$
2	$X^4 - 4X^3 + 7X^2 - 7X + 2$	$-X^3 + 4X^2 - 6X + 4$	$-X$	$X^2 - 3X + 2$	X	$-2X^2 + 2X + 1$
3	$-X^3 + 4X^2 - 6X + 4$	$X^2 - 3X + 2$	$-X + 1$	$-X + 2$	$X^2 - X + 1$	$-2X^3 + 4X^2 - 3X + 1$
4	$X^2 - 3X + 2$	$-X + 2$		0		

On trouve $D = -X + 2$ **(2 pts)**, $U = X^2 - X + 1$ et $V = -2X^3 + 4X^2 - 3X + 1$ **(2 pts)**.

c. Le nombre réel 2 est racine du polynôme D. Comme D divise A et B, le nombre réel 2 est racine de A et B. **(0,5 pt)**

d. Supposons que $a \in \mathbb{R}$ est racine commune de A et B. On a donc $X - a$ divise A et B. Du coup, $X - a$ divise D. Or, $\deg(D) = 1$. Donc $D = \lambda(X - a)$ avec $\lambda \in \mathbb{R}$. Comme $D = -X + 2$, on obtient $\lambda = -1$ et $a = 2$. Cela montre que A et B ont au plus une racine en commun dans $\mathbb{R}$, à savoir 2. **(0,5 pt)**

Exercice 6. a. Soit $x \in \mathbb{R}$. L'évaluation de A en x est $A(x) = x^4 + 6x^2 + 25$ et est strictement positif car $x^4 \geq 0$, $6x^2 \geq 0$ et $25 > 0$. Le polynôme A n'a donc pas de racine dans $\mathbb{R}$. **(0,5 pt)**

b. Oui. Le Théorème fondamental de l'algèbre implique que tout polynôme complexe de degré $d \geq 0$ possède exactement d racines dans $\mathbb{C}$ lorsqu'on les compte avec multiplicités. **(0,5 pt)**

c. Soit $z \in \mathbb{C}$ tel que $A(z) = 0$. On a donc $z^4 + 6z^2 + 25 = 0$. En posant $w = z^2$, le nombre complexe w satisfait $w^2 + 6w + 25 = 0$. Le discriminant de cette dernière expression est $\Delta = 6^2 - 4 \times 25 = 36 - 100 = -64$. Une racine carrée de Δ est $8i$, et on obtient que $w = \frac{1}{2}(-6 \pm 8i) = -3 \pm 4i$. **(1 pt)**

Comme z est racine carrée de w, déterminons les racines carrées de $-3+4i$; les racines carrées de $-3-4i$ seront les conjugués. Ecrire $z = x + iy$, avec $x, y \in \mathbb{R}$. On a $x^2 - y^2 = -3$, $2xy = 4$ et $x^2 + y^2 = 5$. On en déduit que $x^2 = 1$, i.e., $x = \pm 1$ et $y = \pm 2$ (signes couplés). Les racines carrées de $-3+4i$ sont donc $\pm(1+2i)$, et celles de $-3-4i$ sont $\pm(1-2i)$. Les racines de A dans $\mathbb{C}$ sont donc $\pm 1 \pm 2i$. **(1 pt)**

d. D'après le c, on a

$$A = (X - (1+2i))\,(X + (1+2i))\,(X - (1-2i))\,(X + (1-2i))$$

dans $\mathbb{C}[X]$, ce qui est bien la décomposition en facteurs irréductibles de A dans $\mathbb{C}[X]$ car tous les facteurs sont de degré 1. **(1 pt)**

e. Non, les polynômes irréductibles dans $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 sans racine réelle. Or, A est de degré 4. Donc il n'est pas irréductible. En fait, en regroupant les facteurs complexes de A ci-dessus en pairs complexes conjugués, on obtient

$$A = (X - (1+2i))\,(X - (1-2i))\,(X + (1+2i))\,(X + (1-2i)) = (X^2 - 2X + 5)(X^2 + 2X + 5)$$

dans $\mathbb{C}[X]$. On a donc $A = (X^2 - 2X + 5)(X^2 + 2X + 5)$ dans $\mathbb{R}[X]$. Comme ces deux facteurs sont de degré 2 et sont à discriminant strictement négatif, ils sont irréductibles dans $\mathbb{R}[X]$. Cette décomposition de A dans $\mathbb{R}[X]$ est donc la décomposition en facteurs irréductibles de A. **(1 pt)**