Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE PARCOURS 1

ALGEBRE ET GEOMETRIE

Examen terminal, le 5 janvier 2015, 9h00-12h00

CORRIGE ET BAREME

Question de cours. Soient $A, B \in K[X]$ avec $A \neq 0$. Il existe $Q, R \in K[X]$ tels que $B = QA + R$ et $\deg(R) < \deg(A)$ **(1 pt)**. De plus, Q et R sont uniquement déterminés par ces conditions **(1 pt)**.

Exercice 1. a. On montre que $g = h$. On doit donc montrer que $g(y) = h(y)$ quel que soit $y \in F$. Soit $y \in F$ quelconque. Comme $f\colon E \to F$ est surjective, il existe $x \in E$ tel que $f(x) = y$. Comme $g \circ f = h \circ f$, on a $(g \circ f)(x) = (h \circ f)(x)$. Or, le premier membre est égal à

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

Le second membre est égal à

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

On en déduit que $g(y) = h(y)$. Comme y était un élément quelconque F, on a $g = h$. **(1 pt)**

b. Soit $E = \emptyset$, $F = \{0\}$ et $G = \{0, 1\}$. Soient encore g et h les applications de F dans G définies par $g(0) = 0$ et $h(0) = 1$. On a bien $g \neq h$. L'application f de E dans F est l'unique application de l'ensemble vide dans F. Comme, de même, il n'existe qu'une seule application de $\emptyset$ dans G, on a obligatoirement $g \circ f = h \circ f$. **(1 pt)**

Exercice 2. a. La réflexivité de R est vérifiée car $a \leq a$ et $b \leq b$ pour tout $(a, b) \in \mathbb{N} \times \mathbb{N}$.

Quant à l'antisymétrie, supposons que $(a, b)\, R\, (a', b')$ et $(a', b')\, R\, (a, b)$. Cela veut dire que $a \leq a'$, $b \leq b'$, $a' \leq a$ et $b' \leq b$. On en déduit que $a = a'$ et $b = b'$, i.e., $(a, b) = (a', b')$, et R est antisymétrique.

Afin de montrer la transitivité, supposons que $(a, b)\, R\, (a', b')$ et $(a', b')\, R\, (a'', b'')$. On a donc $a \leq a'$, $b \leq b'$, $a' \leq a''$ et $b' \leq b''$. On en déduit que $a \leq a''$ et $b \leq b''$, i.e., $(a, b)\, R\, (a'', b'')$. D'où la transitivité de R.

Par conséquent, la relation R est une relation d'ordre sur $\mathbb{N} \times \mathbb{N}$. **(2 pt)**

b. Non, $(0, 1) \not R\, (1, 0)$ et $(1, 0) \not R\, (0, 1)$. **(0,5 pt)**

c. Non, le sous-ensemble non vide $\{(0, 1), (1, 0)\}$ de $\mathbb{N} \times \mathbb{N}$ ne contient pas de plus petit élément par rapport à la relation d'ordre R, comme on vient de voir dans le b. **(0,5 pt)**

Exercice 3. a. Comme a divise c, il existe $a' \in \mathbb{Z}$ tel que $aa' = c$. De même, il existe $b' \in \mathbb{Z}$ tel que $bb' = c$. Comme a et b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$ d'après Bézout. Multiplier cette équation par c et substituer $c = aa'$ et $c = bb'$ donne

$$c = (ua + vb)c = uac + vbc = uabb' + vbaa' = ab(ub' + va').$$

Comme $ub' + va' \in \mathbb{Z}$, on en déduit que ab divise c. (1,5 pt)

b. Prendre $a = b = c = 2$. On a $a|c$ et $b|c$ mais $ab = 4 \nmid c$. (0,5 pt)

Exercice 4. a. On déroule l'algorithme d'Euclide étendu :

$\mathbf{i}$	$\mathbf{r_{i\ 2}}$	$\mathbf{r_{i\ 1}}$	$\mathbf{q_i}$	$\mathbf{r_i}$	$\mathbf{u_i}$	$\mathbf{v_i}$
					1	0
					0	1
1	$X^4+6X^3+16X^2+21X+12$	X^3+4X^2+7X+5	$X+2$	X^2+2X+2	1	$-X-2$
2	X^3+4X^2+7X+5	X^2+2X+2	$X+2$	$X+1$	$-X-2$	X^2+4X+5
3	X^2+2X+2	$X+1$	$X+1$	1	X^2+3X+3	$-X^3-5X^2-10X-7$
4	$X+1$	1		0		

On pourra donc prendre $U = X^2 + 3X + 3$ et $V = -X^3 - 5X^2 - 10X - 7$. (2 pts)

b. Comme $UA + VB = 1$ dans $\mathbb{Q}[X]$, on a aussi $U(10)A(10) + V(10)B(10) = 1$. Or, $b = B(10) = 10^3 + 4 \times 10^2 + 7 \times 10 + 5 = 1475$ et $a = A(10) = 10^4 + 6 \times 10^3 + 16 \times 10^2 + 21 \times 10 + 12 = 17822$. Du coup, $u = U(10) = 133$ et $v = V(10) = -1607$ conviennent, i.e., $133 \times 17822 - 1607 \times 1475 = 1$. (0,5 pt)

c. D'après Bézout, si $ua + vb = 1$ avec $u, v, a, b \in \mathbb{Z}$, alors a et b sont premiers entre eux. D'après le b, 17822 et 1475 sont premiers entre eux. (0,5 pt)

Exercice 5. a. Si $x \in \mathbb{R}$, on a $x^4 \geq 0$ et $3x^2 \geq 0$. Comme $1 > 0$, on a $x^4 + 3x^2 + 1 > 0$. En particulier, $x^4 + 3x^2 + 1 \neq 0$, i.e., le polynôme P n'a pas de racine dans $\mathbb{R}$. (0,5 pt)

b. Le Théorème fondamentale de l'algèbre dit que le nombre de racines d'un polynôme non nul dans $\mathbb{C}[X]$ est égal au degré du polynôme en question, lorsqu'on compte les racines avec leurs multiplicités. Comme $\deg(P) = 4$ ici, le polynôme P possède 4 racines dans $\mathbb{C}$. (0,5 pt)

c. Supposons que z est une racine de P dans $\mathbb{C}$. On a donc $z^4 + 3z^2 + 1 = 0$. Cela veut dire que z^2 est solution de l'équation $w^2 + 3w + 1 = 0$. Les solutions de cette dernière équation sont $w = (-3 \pm \sqrt{5})/2$. Remarquons que ces deux nombres réels sont tous les deux négatifs. C'est clair pour $(-3 - \sqrt{5})/2$. C'est donc vrai pour l'autre aussi car le produit des deux vaut 1, le coefficient constant dans $w^2 + 3w + 1$. Du coup, on a $z^2 = (-3 \pm \sqrt{5})/2 = -(3 \mp \sqrt{5})/2$, et comme ces deux nombres réels sont négatifs, on trouve

$$z = \pm i\sqrt{\tfrac{3}{2} \mp \tfrac{1}{2}\sqrt{5}}.$$

Ce sont donc les 4 racines de P dans C. **(1 pt)**

d. On déduit du c que

$$P = \left(X - i\sqrt{\tfrac{3}{2} + \tfrac{1}{2}\sqrt{5}}\right)\left(X - i\sqrt{\tfrac{3}{2} - \tfrac{1}{2}\sqrt{5}}\right)\left(X + i\sqrt{\tfrac{3}{2} - \tfrac{1}{2}\sqrt{5}}\right)\left(X + i\sqrt{\tfrac{3}{2} + \tfrac{1}{2}\sqrt{5}}\right).$$

Comme tout polynôme de degré 1 est irréductible, cette décomposition est la décomposition de P en facteurs irréductibles dans $\mathsf{C}[X]$. **(1 pt)**

e. Non, les seuls polynômes irréductibles dans $\mathsf{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 à discriminant strictement négatif. Comme P est de degré 4, le polynôme P n'est pas irréductible dans $\mathsf{R}[X]$. Sa décomposition en facteurs irréductibles dans $\mathsf{R}[X]$ s'obtient de celle dans $\mathsf{C}[X]$ du d en regroupant les facteurs complexes conjugués :

$$P = \left(X - i\sqrt{\tfrac{3}{2} + \tfrac{1}{2}\sqrt{5}}\right)\left(X + i\sqrt{\tfrac{3}{2} + \tfrac{1}{2}\sqrt{5}}\right)\left(X - i\sqrt{\tfrac{3}{2} - \tfrac{1}{2}\sqrt{5}}\right)\left(X + i\sqrt{\tfrac{3}{2} - \tfrac{1}{2}\sqrt{5}}\right) = (X^2 + \tfrac{3}{2} + \tfrac{1}{2}\sqrt{5})(X^2 + \tfrac{3}{2} - \tfrac{1}{2}\sqrt{5}).$$

Ces facteurs sont bien irréductibles dans $\mathsf{R}[X]$ car ils sont de discriminant strictement négatif. **(1 pt)**

Exercice 6. a. Si $a \in \mathsf{Z}$ est une racine de P, on a

$$(a^6 + 2a^5 - 5a^4 - 17a^3 - 26a^2 - 31a^1 - 20)a = a^7 + 2a^6 - 5a^5 - 17a^4 - 26a^3 - 31a^2 - 20a = 12.$$

Comme $a^6 + 2a^5 - 5a^4 - 17a^3 - 26a^2 - 31a^1 - 20 \in \mathsf{Z}$, on a $a \mid 12$. **(1 pt)**

b. D'après le a, les seules racines possibles de P dans Z sont les diviseurs de 12 i.e. $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. Or,

$$P(1) = 1 + 2 - 5 - 17 - 26 - 31 - 20 - 12 = -2 - 17 - 26 - 31 - 20 - 12 < 0$$

et

$$P(-1) = -1 + 2 + 5 - 17 + 26 - 31 + 20 - 12 = -8 \neq 0$$

donc P n'a pas de racine en ± 1. Puis,

$$P(2) = ((((((2+2)2 - 5)2 - 17)2 - 26)2 - 31)2 - 20)2 - 12 = (((((-3) \times 2 - 17)2 - 26)2 - 31)2 - 20)2 - 12 < 0$$

donc 2 n'est pas racine non plus. Par contre,

$$P(-2) = ((((((-2+2)(-2) - 5)(-2) - 17)(-2) - 26)(-2) - 31)(-2) - 20)(-2) - 12 = 0.$$

Donc -2 est une racine de P. Pour simplifier les calculs dans la suite, on effectue la division longue de P par $X+2$ et on obtient

$$P = (X^6 - 5X^4 - 7X^3 - 12X^2 - 7X - 6)(X+2).$$

Soit donc $Q = X^6 - 5X^4 - 7X^3 - 12X^2 - 7X - 6$. On a $P = Q(X+2)$ dans $\mathbb{Q}[X]$. Si l'un des diviseurs restant de 12, à savoir $\pm 3, \pm 4, \pm 6, \pm 12$ est racine de P, il est forcément racine de Q. On vérifie donc si $\pm 3, \pm 4, \pm 6, \pm 12$ sont racines de Q. Or,

$$Q(3) = ((((3^2 - 5)3 - 7)3 - 12)3 - 7)3 - 6 = 0.$$

Donc 3 est racine de Q et donc racine de P. On divise Q par $X-3$ et on ontient

$$Q = (X^5 + 3X^4 + 4X^3 + 5X^2 + 3X + 2)(X-3).$$

Posons $R = X^5 + 3X^4 + 4X^3 + 5X^2 + 3X + 2$. On a donc $Q = R(X-3)$ dans $\mathbb{Q}[X]$. Si l'un des diviseurs restants de 12 est racine de P, il l'est forcément de R. On vérifie donc si $-3, \pm 4, \pm 6, \pm 12$ sont racines de R. Or, R est à coefficients strictement positifs, donc $4, 6, 12$ ne sont pas racines de R et non plus de P. Quant à $-3, -4, -6$, on peut vérifier qu'ils ne sont pas racines de R. L'alternative est d'évoquer un même argument que dans le a, et de dire qu'une racine a de R dans $\mathbb{Z}$ divise forcément le coefficient constant 2 de R. Comme -3, -4 et -6 ne divisent pas 2, ils ne sont ni racine de R ni racine de P. (1 pt)

c. Si $a \in \mathbb{Z}$ est racine double de P, le polynôme $(X-a)^2$ divise P dans $\mathbb{Q}[X]$. Il existe donc $Q \in \mathbb{Q}[X]$ tel que $(X-a)^2 Q = P$. On peut écrire $Q = X^5 + bX^4 + cX^3 + dX^2 + eX + f$ avec $b, c, d, e, f \in \mathbb{Q}$. Comme $(X^2 - 2aX + a^2)Q = P$, on a

$$X^7 + (b-2a)X^6 + (c - 2ab + a^2)X^5 + (d - 2ac + a^2 b)X^4 + (e - 2ad + a^2 c)X^3 + (f - 2ae + a^2 d)X^2 + (-2af + a^2 e)X + a^2 f = \\ X^7 + 2X^6 - 5X^5 - 17X^4 - 26X^3 - 31X^2 - 20X - 12.$$

Du coup, $b - 2a = 2$, et donc $b \in \mathbb{Z}$ car $a \in \mathbb{Z}$. Puis, $c = 2ab - a^2 - 5 \in \mathbb{Z}$ car $a, b \in \mathbb{Z}$, et de même $d, e, f \in \mathbb{Z}$. Comme $a^2 f = -12$ et $f \in \mathbb{Z}$, on a $a^2 | -12$, ou mieux, $a^2 | 12$ dans $\mathbb{Z}$. (1 pt)

d. On a vu dans le b que les seules racines de P dans $\mathbb{Z}$ sont -2 et 3. D'après le c, seul -2 peut être racine double de P car $3^2 = 9 \nmid 12$. Vérifions que -2 est effectivement racine double de P. Rappelons qu'on avait déjà décomposé P dans $\mathbb{Q}[X]$ comme

$$P = (X+2)(X-3)R$$

où $R = X^5 + 3X^4 + 4X^3 + 5X^2 + 3X + 2$. Afin de montrer que -2 est racine double de P, il suffit de vérifier que -2 est racine simple de R. Or,

$$R(-2) = ((((-2+3)(-2)+4)(-2)+5)(-2)+3)(-2)+2 = 0.$$

D'où -2 est bien racine simple de R. Cela montre que -2 est racine double (au moins) de P. (1 pt)