Corrigé du contrôle continu d'algèbre 1 du 10 décembre 2007

Exercice 1 a) $1 + j = 1 + \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = e^{i\pi/3}$.

b) Notons $cl(j)$ la classe d'équivalence de j. Soit $z \in \mathbb{C}$. On a $(1+j)^3 = (e^{i\pi/3})^3 = e^{i\pi} = -1$. Donc $z \in cl(j)\mathbb{C}$ ssi $(1+z)^3 = e^{i\pi}$ ssi il existe k dans $\{0,1,2\}$ tel que $1 + z = e^{i(\pi+2k\pi)/3}$ ssi il existe k dans $\{0,1,2\}$ tel que $z = e^{i(\pi+2k\pi)/3} - 1$. On a donc :

$$cl(j) = \{e^{i\pi/3} - 1, e^{i\pi} - 1, e^{i5\pi/3} - 1\} = \{j, -2, \bar{j}\}$$

Exercice 2 On vérifie tout d'abord que $P(1) = 0$, donc 1 est racine de P. Calculons $P'(1)$. On a $P' = 4X^3 + 3iX^2 - 6X + (2 - 3i)$. On a donc $P'(1) = 4 + 3i - 6 + 2 - 3i = 0$. Calculons $P"(1)$. On a $P" = 12X^2 + 6iX - 6$ donc $P"(1) = 6 + 6i \neq 0$. Donc 1 est racine double de P : $m = 2$.

Puisque 1 est racine double de P, on a $(X-1)^2|P$, donc le reste dans la division euclidienne de P par $(X-1)^2$ est nul. De ce fait, le quotient est l'unique polynôme Q tel que $Q(X-1)^2 = P$.Pour trouver le quotient, on peut soit poser la division euclidienne, soit procéder par identification. Le quotient est l'unique polynôme Q tel que $Q(X-1)^2 = P$. Comme P est de degré 4, Q est de degré 2. Donc il existe des complexes a, b, c tels que $Q = aX^2 + bX + c$. Ces complexes sont tels que $(aX^2 + bX + c)(X^2 - 2X + 1) = P$. En développant le membre de gauche et en utilisant que deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients, on obtient $a = 1$ (terme de plus haut degré), $c = 2i$ (terme constant), puis $-2a + b = i$ (terme de degré 3) donc $b = 2 + i$. Donc $Q = X^2 + (2+i)X + 2i$.

Exercice 3 Soit P un polynôme solution. Il existe un nombre infini de réels x tels que $\cos x = -1$ donc tels que $1 + \cos x = 0$, donc P a une infinité de racines. Or un polynôme qui a une infinité de racines est nul, donc $P = 0$. Mais $P = 0$ n'est pas solution car pour $x = 0$, $1 + \cos x = 2 \neq 0$. Il n'y a donc aucun polynôme solution.

Exercice 4

a) L'application n'est pas injective car $f(2) = f(1/2)$. En revanche, elle est surjective. En effet, soit $z_0 \in \mathbb{C}$. Pour un complexe z non nul, $f(z) = z_0$ ssi $z + \frac{1}{z} = z_0$ ssi

$$z^2 - z_0 z + 1 = 0$$

Cette équation est une équation du second degré a coefficients complexes. Elle a donc au moins une solution $z' \in \mathbb{C}$. De plus, $z' \neq 0$ car 0 n'est pas solution de l'équation. Donc $z' \in \mathbb{C}^*$ et $f(z') = z_0$. Donc z_0 a au moins un antécédent par f. Comme ceci est vrai pour tout z_0 dans $\mathbb{C}$, l'application f est surjective.

b) Soit $z = a + ib \in \mathbb{C}^*$, avec a et b réels. On a

$$\frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{a^2+b^2} = \frac{a-ib}{|z|^2}$$

La partie imaginaire de $f(z)$ est donc

$$b\left(1 - 1/|z|^2\right)$$

Elle est nulle si et seulement si $b = 0$ ou $|z| = 1$. On a donc

$$f^{-1}(\mathbb{R}) = \mathbb{R} \cup \{z \in \mathbb{C}, |z| = 1\}$$

c) Soit $z \in \mathbb{C}^*$. On a $f(z) = i \Leftrightarrow z + \frac{1}{z} = i \Leftrightarrow z^2 - iz + 1 = 0$. Le discriminant est $\Delta = i^2 - 4 = -5 = (i\sqrt{5})^2$. Les solutions de l'équation du second degré précédentes sont donc $z_1 = i\left(1 + \frac{\sqrt{5}}{2}\right)$ et $z_2 = i\left(1 - \frac{\sqrt{5}}{2}\right)$. Ces solutions sont bien dans $\mathbb{C}^*$. On a donc

$$\{z \in \mathbb{C}^*, f(z) = i\} = \left\{ i\left(1 + \frac{\sqrt{5}}{2}\right), i\left(1 - \frac{\sqrt{5}}{2}\right) \right\}$$

Exercice 5

1) Supposons par l'absurde que pour tout $k \in \mathbb{N}$, $R_k \neq 0$. Il s'ensuit que pour tout $k \in \mathbb{N}$, R_{k+2} est le reste de la division euclidienne de R_k par R_{k+1} donc $deg(R_{k+2}) \leq deg(R_{k+1}) - 1$ donc par une récurrence évidente $\deg(R_k) \leq deg(R_0) - k$. Pour $k > deg(R_0)$ on a donc que le degré de R_k est un entier strictement négatif, ce qui est impossible. Il existe donc bien un entier naturel k tel que $R_k = 0$.

2) Puisque $R_{n+1} \neq 0$, il existe un polynome Q tel que $R_n = QR_{n+1} + R_{n+2}$. Supposons que $P|R_n$ et $P|R_{n+1}$. Il existe donc des polynôme A et B tels que $R_n = PA$ et $R_{n+1} = PB$. On a donc $R_{n+2} = R_n - QR_{n+1} = PA - QPB = P(A - QB)$ donc $P|R_{n+2}$, or $P|R_{n+1}$ par hypothèse, donc $P|R_{n+1}$ et $P|R_{n+2}$. Réciproquement, supposons que $P|R_{n+1}$ et $P|R_{n+2}$. Il existe donc des polynômes B et C tels que $R_{n+1} = PB$ et $R_{n+2} = PC$. On a donc $R_n = QR_{n+1} + R_{n+2} = QPB + PC = P(QB + C)$ donc $P|R_n$, donc $P|R_n$ et $P|R_{n+1}$.

3) Pour tout entier naturel n, notons H_n la propriété : $n > m$ ou $(P|R_0$ et $P|R_1) \Leftrightarrow (P|R_n$ et $P|R_{n+1})$. Montrons par récurrence que H_n est vraie pour tout $n \leq m$.

Initialisation : H_0 est trivialement vraie.

Hérédité : supposons H_n vraie. Si $n + 1 > m$, H_{n+1} est trivialement vraie. Sinon, on a $R_{n+1} \neq 0$ donc d'après 2), $(P|R_n$ et $P|R_{n+1}) \Leftrightarrow (P|R_{n+1}$ et $P|R_{n+2})$. Or par hypothèse de récurrence, compte tenu de $n \leq n + 1 \leq m$, on a : $(P|R_0$ et $P|R_1) \Leftrightarrow (P|R_n$ et $P|R_{n+1})$. Donc $(P|R_0$ et $P|R_1) \Leftrightarrow (P|R_{n+1}$ et $P|R_{n+2})$, donc H_{n+1} est vraie.

Donc H_n est vraie pour tout entier naturel n. Donc, pour $n = m$, on a : $(P|R_0$ et $P|R_1) \Leftrightarrow (P|R_m$ et $P|R_{m+1})$. Mais $R_{m+1} = 0$ donc tout polynôme divise R_{m+1}, donc $(P|R_m$ et $P|R_{m+1}) \Leftrightarrow P|R_m$, d'où le résultat.

4) On pose les divisions euclidiennes successives. On obtient d'abord $X^5 + X^3 - X + 1 = (X^2 - 1)(X^3 + 2X) + (X + 1)$ donc $R_2 = X + 1$, puis $X^2 - 1 = (X + 1)(X - 1) + 0$ donc $R_3 = 0$, ce qui implique que pour $n \geq 3$, $R_n = 0$. On est donc dans le cas $m = 2$ et $R_m = X + 1$. D'après la question 3), les polynômes qui divisent à la fois $X^5 + X^3 - X + 1$ et $X^2 - 1$ sont donc les polynômes qui divisent $X + 1$, à savoir les polynômes constant non nuls et les polynômes de la forme $a(X + 1)$ où a est un réel non nul.

Petites explications sur cet exercice : ceux qui ont fait spécialité mathématiques en terminale devraient connaître l'algorithme d'Euclide pour le calcul du PGCD de deux entiers r_0 et r_1. Cet algorithme consiste à d'abord calculer le reste r_2 dans la division euclidienne de r_0 par r_1, puis le reste r_3 dans la division euclidienne de r_1 par r_2, etc. Le dernier reste non nul est le PGCD de r_0 et r_1.

L'arithmétique dans $K[X]$ se fait essentiellement de la même manière que l'arithmétique dans $\mathbb{Z}$, ceci parce que $\mathbb{K}[X]$ et $\mathbb{Z}$ partagent de nombreuses caractéristiques communes (on dit que ce sont des “anneaux principaux", mais je n'ai malheureusement pas le temps de vous expliquer ce que cela veut dire). En particulier, on peut définir le PGCD de deux polynômes et pour calculer ce PGCD on utilise l'algorithme d'Euclide, comme dans $\mathbb{Z}$. L'exercice 5 explique cet algorithme.

Pour être tout à fait complet, notons que le PGCD de deux polynômes (une notion hors programme) est l'unique polynôme unitaire de degré maximal qui divise à la fois ces deux polynômes. On demande que le PGCD soit unitaire parce que sinon il serait défini à une constante multiplicative près (de la même manière, dans $\mathbb{Z}$, on demande au PGCD d'être positif). Pour déterminer le PGCD de deux polynômes, on procède comme dans l'exercice sauf qu'à la fin on multiplie le dernier reste non nul par l'inverse de son coefficient dominant. Ceci pour obtenir un polynôme unitaire.