Devoir libre $n°1$
Correction

Exercice 1

1. Le polynôme $P(X) = X^4 + 3X^2 - 4$ se factorise dans $\mathbb{C}$: $P(X) = (X-1)(X+1)(X+2i)(X-2i)$ et sa dérivée $P'(X) = 4x^3 + 6X = 4X\left(X + i\sqrt{\frac{3}{2}}\right)\left(X - i\sqrt{\frac{3}{2}}\right)$. L'enveloppe convexe des racines de P est le rectangle de sommets $1, -1, 2i, -2i$ et les racines de P' sont 0, $i\sqrt{\frac{3}{2}}$ et $-i\sqrt{\frac{3}{2}}$, qui sont bien dans l'enveloppe convexe des racines de P.
Le polynôme $P(X) = X^3 - X^2 + X - 1 = (X-1)(X+i)(X-i)$ et sa dérivée $P'(X) = 3x^2 - 2X + 1 = 3\left(X - \frac{1+i\sqrt{2}}{3}\right)\left(X - \frac{1-i\sqrt{2}}{3}\right)$. L'enveloppe convexe des racines de P est le triangle de sommets $1, , i, -i$ et les racines de P' sont $\frac{1+i\sqrt{2}}{3}$ et $\frac{1-i\sqrt{2}}{3}$, qui sont bien dans l'enveloppe convexe.
Les racines de $P(X) = X^k - 1$ forme un polygone régulier à k cotés, 0 est l'unique racine de P' qui est le centre du polygone.
Il est facile de remarquer que si $P(x) = ax^2 + bx + c$ est un polynôme du second degré, le zéro de P est la demi-somme des zéros de P.

Remarque : Si un polynôme de degré n à coefficients réels admet n zéros réels distincts

$$x_1 < x_2 < ... < x_n,$$

on voit en utilisant le théorème de Rolle que les zéros du polynôme dérivé sont dans l'intervalle $[x_1, x_n]$.

2. Posons $P = a\prod_{k=1}^{n}(X - z_k)$ où les z_k sont les racines de P dans $\mathbb{C}$ non nécessairement deux à deux distinctes. On a

$$P' = \sum_{j=1}^{n}(X-z_1)...(X-z_j)'...(X-z_n) = \sum_{j=1}^{n}\prod_{k\neq j}^{n}(X-z_k) = \sum_{k=1}^{n}\frac{P}{X-z_j},$$

et donc

$$\frac{P'}{P} = \sum_{j=1}^{n}\frac{1}{z-z_j}.$$

En regroupant les fractions de même dénominateur, on obtient la décomposition en élément simple de $\frac{P'}{P}$ à savoir :

$$\frac{P'}{P} = \sum_{i=1}^{k}\frac{n_i}{z-\alpha_i}.$$

3. Si

$$P'(z) = 0 \quad \text{et} \quad P(z) \neq 0,$$

$$\sum_{i=1}^{r} \frac{n_i}{z - \alpha_i} = 0 \quad \text{ou encore} \quad \sum_{i=1}^{r} n_i \frac{\overline{z} - \overline{\alpha_i}}{|z - \alpha_i|^2} = 0,$$

ce qui s'écrit aussi

$$\left(\sum_{i=1}^{k} \frac{n_i}{|z - \alpha_i|^2} \right) \overline{z} = \sum_{i=1}^{k} \frac{n_i}{|z - \alpha_i|^2} \overline{\alpha_i}.$$

En prenant les conjugués, on obtient

$$\left(\sum_{i=1}^{k} \frac{n_i}{|z - a_i|^2} \right) z = \sum_{i=1}^{k} \frac{n_i}{|z - \alpha_i|^2} \alpha_i.$$

Le cas où z est aussi zéro de P est évident.

4. Soit z une racine de P' qui n'est pas une racine de P. On note $\lambda_i = \dfrac{\dfrac{n_i}{\overline{|z - \alpha_i|^2}}}{\left(\displaystyle\sum_{i=1}^{k} \frac{n_i}{|z - a_i|^2} \right)} \in [0, 1]$. On a donc $\displaystyle\sum_{i=1}^{k} \lambda_i = 1$, de plus $z = \displaystyle\sum_{i=1}^{k} \lambda_i \alpha_i$. On voit bien que z est un barycentre à coefficients positifs des α_i.

Exercice 2

Montrons d'abord le résultat préliminaire suivant :

Toute équation polynomiale de degré $n \in \mathbb{N}^*$ dans $\left(\mathbb{Z}/_{pZ} \right)$ admet au plus n solutions distinctes.

D'abord montrons qu'un polynôme P à coefficients dans $Z/_{pZ}$ admettant x pour racine est divisible par $(X - x)$. En effet, par récurrence forte sur le degré, si P est de coefficient dominant α, de degré n, et admet x pour racine, alors $P - \alpha X^{n-1}(X - x)$ est de degré inférieur à celui de P, on peut lui appliquer l'hypothèse de récurrence.
Montrons ensuite par récurrence qu'un polynôme de degré n dans $Z/_{pZ}$ admet au plus n racines distinctes.
Il n'y a rien à prouver pour $n = 1$. Supposons la propriété vérifiée pour $n > 0$ fixé, montrons la pour $n + 1$.
Soit donc P un polynôme de degré $n + 1$. Si P n'admet pas de racine, le résultat est évident. Si x est une racine de P, alors on peut écrire $P = (X - x)Q$, où Q est de degré $n - 1$, et l'hypothèse de récurrence permet alors de conclure.

1. On trouve les ensembles suivants : $C_3 = \{\overline{1}\}$, $C_5 = \{\overline{1}, \overline{4}\}$, $C_7 = \{\overline{1, 2, 4}\}$, $C_{11} = \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$.

2. Il est clair que C_p est stable par multiplication et par passage à l'inverse. Donc C_p est un sous-groupe de $\left(\mathbb{Z}/_{p\mathbb{Z}} \right)^*$.

3. On a, pour tout x et y de C_p, $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$, donc f est un morphisme de groupes.

4. On a $x^2 = y^2$ si et seulement si $(x-y)(x+y) = 0$. Comme p est premier, $Z/_{pZ}$ est un corps, c'est un anneau intègre, et donc $f(x) = f(y)$ si et seulement si $x = y$ ou $x = -y$.

5. Soit $a \in C_p$, donc il existe $y \in \left(\mathbb{Z}/_{pZ}\right)^*$ tel que $a = y^2$. On alors aussi $a = (-y)^2$, or $y \neq -y$ puisque p est impair, donc a est le carré d'au moins deux éléments de $\left(\mathbb{Z}/_{pZ}\right)^*$. En fait, c'est le carré d'exactement deux éléments, car le polynôme $X^2 - a$ est de degré 2, donc admet au plus deux racines dans $\left(\mathbb{Z}/_{pZ}\right)$ (d'après le résultat préliminaire). Puisque $\left(\mathbb{Z}/_{pZ}\right)^*$ possède $p-1$ éléments, et puisque chaque éléments de C_p est le carré d'execatement deux des ces éléments, on en déduit qu'il y a exactement $\dfrac{p-1}{2}$ carrés.

Exercice 3

1. Soit $x = \dfrac{p}{q}$ une racine rationnelle écrite sous forme de fraction irréductible ($p \wedge p = 1$) de $P = a_n X^n + ... + a_0$, on a alors

$$0 = P\left(\frac{p}{q}\right) = a\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + ... + a_0 = \frac{a_n p^n + a_{n-1}p^{n-1}q + ... + a_1 pq^{n-1} + a_0 q^n}{q^n}$$

Donc :

$$p(a_n p^{n-1} + a_{n-1}p^{n-1}q + ... + a_1 q^{n-1}) = -a_0 q^n$$

et p divise donc $a_0 q^n$. Comme $\dfrac{p}{q}$ est irréductible, cela entraine que p divise a_0. De même q divise a_n.

2. Il suffit donc de tester quelles sont les racines de P parmi toutes les fractions irréductibles de la forme un diviseur de a_0 sur un diviseur de a_n (attention à ne pas oublier les diviseurs négatifs !).

• Si $\dfrac{p}{q}$ est une racine rationnelle de $P(X) = X^5 - X^2 + 1$, alors p divise 1, donc $p \in \{-1, 1\}$, de même q divise 1, donc $q \in \{-1, 1\}$. On obtient donc deux possibilités 1 et -1, mais 1 et -1 ne sont pas des racines, donc P n'admet pas des racines dans $\mathbb{Q}$.

• Soit $\dfrac{p}{q}$ une racine rationnelle de $P(X) = 2X^4 - X^3 + X^2 - X + 2$. On a p divise 2 donc vaut ± 1 ou ± 2, de même q divise 2 donc vaut ± 1 ou ± 2. On teste donc $1, -1, 2, -2, \dfrac{1}{2}, \dfrac{-1}{2}$. La vérification permet de conclure que le polynôme P n'a pas de racines rationnelles.

• Les diviseurs du coefficient dominant du polynôme $X^3 - 6X^2 - 4X - 21$ sont -1 et 1. Ceux du coefficient constant sont $1, -1, 3, -3, 7, -7, 21$ et -21. Par conséquent, les seuls rationnels susceptibles d'être des racines sont

$$\pm 1, \pm 3, \pm 7 \text{ et } \pm 21.$$

En remplaçant x successivement par chacune de ces valeurs, on trouve que la seule qui vérifie l'équation polynomiale est 7.

• • • • • • • • • •