Devoir Surveillé n°5 - Sujet groupes B et C

Préliminaires

1. (Question de cours) Définition du produit matriciel, démonstration de l'associativité.
2. (Question de cours) Lemme de Riemann-Lebesgue (démonstration dans le cas $\mathscr{C}^1$).
3. Montrer que l'ensemble des rationnels qui peuvent s'écrire comme quotient de deux entiers impairs est un sous-groupe de $\mathbb{R}^*$.
4. Factoriser sur $\mathbb{R}$ et sur $\mathbb{C}$ le polynôme $P = X^4 + 3X^3 + 5X^2 + 3X$.
5. Le nom du groupe Imagine Dragons provient d'une anagramme de « Imagine Dragons », uniquement connue des membres du groupe [1]. Donner le nombre de possibilités (sans tenir compte des espaces ou des majuscules).

Problème - Polynômes cyclotomiques

Si n est un entier naturel non nul :

- on note comme en cours $\mathbb{U}_n = \left\{e^{2ik\pi/n} \,|\, k \in [\![\, 0\,;\, n-1 \,]\!]\right\}$ l'ensemble des racines n-ièmes de l'unité, c'est-à-dire l'ensemble des complexes ω vérifiant $\omega^n = 1$.
- on dit qu'un complexe ω est une racine **primitive** n-ième de l'unité si $\omega^n = 1$ et si, pour tout $q \in [\![\, 1\,;\, n-1 \,]\!], \omega^q \neq 1$. En d'autres termes, une racine primitive n-ième de l'unité est une racine n-ième de l'unité pour laquelle n est la plus petite puissance q (non nulle) telle que $\omega^q = 1$.
- on note P_n l'ensemble des racines primitives n-ièmes de l'unité.

Partie I - Caractérisation des racines primitives n-ièmes de l'unité

On se donne dans cette partie un entier $n \geq 1$.

1. Expliciter sans démonstration les ensembles P_1, P_2, P_3 et P_4.
2. Donner une CNS sur $n \geq 1$ pour que $(P_n, \times)$ soit un groupe.
3. (a) Soit $k \in [\![\, 0\,;\, n-1 \,]\!]$ tel que $k \wedge n \neq 1$. Montrer que $e^{2ik\pi/n} \notin P_n$.
   (b) Réciproquement, soit $k \in [\![\, 0\,;\, n-1 \,]\!]$ tel que $k \wedge n = 1$. En raisonnant par l'absurde, justifier que $e^{2ik\pi/n}$ est une racine primitive n-ième de l'unité. On a donc prouvé que $P_n = \left\{e^{2ik\pi/n} \,|\, k \in [\![\, 0\,;\, n-1 \,]\!], k \wedge n = 1\right\}$. En particulier, par exemple, $e^{2i\pi/n}$ est une racine primitive n-ième de l'unité.
   (c) Soient z_1 et z_2 deux racines primitives n-ièmes de l'unité. Montrer qu'il existe u premier avec n tel que ${z_1}^u = z_2$ (on pourra utiliser le théorème de Bézout).

Partie II - Définition et premières propriétés des polynômes cyclotomiques

Dans la suite de ce problème, pour tout $n \geq 1$, on définit le n-ième polynôme cyclotomique par :

$$\Phi_n = \prod_{\omega \in P_n} (X - \omega) = \prod_{\substack{k=0 \\ k \wedge n = 1}}^{n} (X - e^{2ik\pi/n})$$

1. (Question de cours) Soit $n \geq 1$. Factoriser sur $\mathbb{C}$ le polynôme $X^n - 1$.
2. Écrire sous forme développée Φ_2, Φ_3, Φ_4. Vérifier en particulier que ces polynômes sont à coefficients entiers.
3. (a) Justifier que $\Phi_5 = \dfrac{X^5 - 1}{X - 1}$. En déduire Φ_5 sous forme développée.
   (b) Plus généralement, si $p \geq 2$ est un nombre premier, calculer Φ_p (on exprimera Φ_p sous forme de somme).
4. Soit $n \geq 1$.
   (a) Si d est un diviseur (positif) de n, on note $E_d = \{k \in [\![\, 0\,;\, n-1 \,]\!] \,|\, k \wedge n = d\}$. Justifier rapidement que $[\![\, 0\,;\, n-1 \,]\!] = \bigcup_{d|n} E_d$.

1. True story !

(b) Soit d un diviseur de n. On note $F_d = \left\{k \in [\![0\,;\, \frac{n}{d} - 1]\!] \,|\, k \wedge \frac{n}{d} = 1\right\}$. Justifier que E_d et F_d sont en bijection.

(c) Montrer que :

$$\prod_{k \in E_d} (X - e^{2ik\pi/n}) = \Phi_{n/d}$$

(d) En déduire que :

$$X^n - 1 = \prod_{d|n} \Phi_d$$

5. Le but de cette question est de montrer par récurrence que, pour tout $n \geq 1$, $\Phi_n \in \mathbb{Z}[X]$.

(a) Prouver l'initialisation. Dans la suite, on se donne un entier $n \geq 2$, on suppose le résultat vrai jusqu'au rang $n-1$ et on cherche à prouver qu'il est encore vrai au rang n.

(b) (Question de cours) Énoncer (sans démonstration) le théorème de division euclidienne (sur $\mathbb{K}[X]$).

(c) On admet [2] que le théorème de division euclidienne est encore valable sur $\mathbb{Z}[X]$ si B est unitaire. Comparer la division euclidienne (on justifiera bien qu'on peut appliquer ce théorème, et on précisera bien où on utilise l'hypothèse de récurrence) de $X^n - 1$ par

$$B = \prod_{\substack{d|n \\ d \neq n}} \Phi_d$$

avec la question 4.(d), et conclure.

Partie III - Théorème de Wedderburn

Dans cette partie, nous prenons une certaine liberté avec le programme [3] et nous nous autoriserons à parler de corps non commutatif. On se donne dans cette partie un corps (pas forcément commutatif, donc) fini K (dont les lois sont notées de façon usuelle, et les neutres [4] également, c'est-à-dire 0 et 1) et le but de cette partie est de prouver que K est commutatif.

1. (Question de cours) Donner la définition d'un anneau.
2. Soit $Z(K)$ le centre de K, c'est-à-dire : $Z(K) = \{x \in K \,|\, \forall y \in K, xy = yx\}$. Montrer que $Z(K)$ est un sous-corps de K. Dans la suite, on note q le cardinal de $Z(K)$.

On admet (nous le montrerons dans le chapitre 30) qu'il existe $n \geq 1$ tel que card$(K) = q^n$.

3. On raisonne par l'absurde et on suppose dans la suite de cette partie que K n'est pas commutatif. Justifier que $n > 1$.
4. On se donne dans les questions $4, 5, 6$ un élément $a \in K \backslash Z(K)$. On note $Z_a = \{y \in K \,|\, ay = ya\}$. On prouverait de même qu'à la question 2 (et donc on l'admettra) que Z_a est un sous-corps de K. Justifier rapidement que $Z(K)$ est inclus strictement dans Z_a. De même, nous admettons qu'il existe $d > 1$ tel que $\text{card}(Z_a) = q^d$.
5. On note p (qui n'est pas forcément un nombre premier) le quotient de la division euclidienne de n par d et r le reste.

(a) Développer la quantité $q^r \left(q^{pd} - 1\right) + (q^r - 1)$.

(b) Donner la valeur de la somme $1 + q^d + q^{2d} + \cdots + q^{(p-1)d}$.

(c) En déduire que $q^r - 1$ est le reste de la division euclidienne de $q^n - 1$ par $q^d - 1$.

(d) On rappelle le théorème de Lagrange : si G est un groupe fini et si H est un sous-groupe de G, alors le cardinal de H divise le cardinal de G. Justifier que $q^d - 1$ divise $q^n - 1$ et en déduire que d divise n.

6. (a) Justifier, à l'aide de la partie précédente, que :

$$\frac{X^n - 1}{X^d - 1} = \prod_{\substack{m|n \\ m \nmid d}} \Phi_m$$

(b) En déduire que, si $d \neq n$, alors $\Phi_n(q)$ divise (on parle ici de divisibilité dans $\mathbb{Z}$) $\dfrac{q^n - 1}{q^d - 1}$.

7. (a) On définit sur K^* la relation $\sim$ par : $x \sim y \iff \exists g \in K^*, gxg^{-1} = y$. Justifier que $\sim$ est une relation d'équivalence.

(b) Comme dans le DM n° 14, si $x \in K^* \backslash Z(K)^*$, on note $\text{Stab}(x) = \{g \in K^* \,|\, gxg^{-1} = x\}$. Justifier que $\text{Stab}(x) = {Z_x}^*$.

2. cf. l'exercice 67 du chapitre 19 : il suffit de remplacer b_p par 1 dans la preuve du cours.

3. Pour gagner en lisibilité : sinon, nous sommes obligés de parler de corps gauche ou d'algèbre à division, et de prendre des précautions oratoires extraordinaires pour éviter de parler de corps (car, par définition, un corps est commutatif), ce qui compliquerait considérablement les choses.

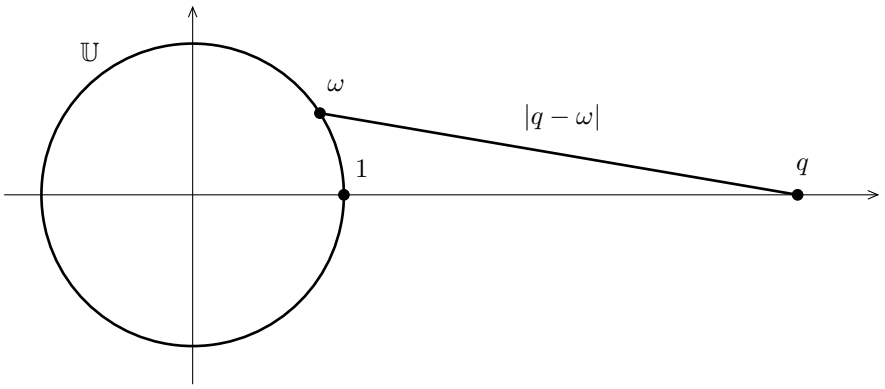
4. Qu'on suppose distincts : on suppose que K n'est pas un singleton.

8. On rappelle le résultat suivant, vu dans le DM n° 14 (c'est l'équation aux classes, couplée avec l'égalité $\text{card}(K^*) = \text{card}(\text{cl}(x)) \times \text{card}(\text{Stab}(x))$:

$$\text{card}(K^*) = \text{card}(Z(K)^*) + \sum_{\text{cl}(x)\,|\,x\notin Z(K)^*} \frac{\text{card}(K^*)}{\text{card}(\text{Stab}(x))}$$

Déduire de la question 6.(b) que $\Phi_n(q)$ divise $q-1$ (là encore, on parle de divisibilité dans $\mathbb{Z}$).

9. Si ω est une racine primitive n-ième de l'unité, justifier que $|q-\omega| > q-1$ et conclure à une absurdité.



On a donc prouvé le théorème de Wedderburn [5] :

Théorème de Wedderburn : tout corps fini est commutatif.

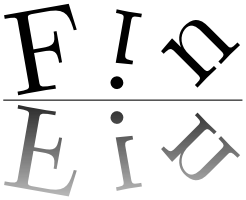
Partie IV - Irréductibilité des polynômes cyclotomiques

On se donne dans cette partie un entier $n \geq 1$ et on souhaite prouver que Φ_n est irréductible sur $\mathbb{Q}$, c'est-à-dire qu'on ne peut pas écrire Φ_n comme un produit de deux polynômes non constants. On se donne dans toute cette partie une racine primitive n-ième de l'unité notée ω.

1. On note $I = \{A \in \mathbb{Q}[X] \,|\, A(\omega) = 0\}$.
   (a) Montrer que I est un sous-groupe de $(\mathbb{Q}[X], +)$ et qu'il est absorbant pour le produit [6], c'est-à-dire :
   $$\forall P \in \mathbb{Q}[X], \forall A \in I, P \times A \in I$$
   (b) Montrer que $E = \{\deg(A) \,|\, A \in I \text{ non constant}\}$ admet un plus petit élément qu'on notera d.
   (c) Justifier que I contient un polynôme unitaire de degré d qu'on notera M dans la suite.
   (d) Montrer que tous les éléments de I sont divisibles par M. On pourra utiliser le théorème de division euclidienne [7].
2. On admet [8] le résultat suivant, que l'on appelle le lemme-clef :

   Lemme-clef : Si $z \in P_n$ est racine de M et si p est un nombre premier qui ne divise pas n, alors $M(z^p) = 0$.

   On souhaite prouver que Φ_n est irréductible sur $\mathbb{Q}$: on se donne donc deux polynômes A et $B \in \mathbb{Q}[X]$ tels que $\Phi_n = AB$ et on souhaite prouver que A ou B est constant.
   (a) Justifier que ω est racine de A ou B. Sans perte de généralité, on suppose que $A(\omega) = 0$.
   (b) Justifier qu'il existe $P \in \mathbb{Q}[X]$ tel que $\Phi_n = M \times P \times B$.
   (c) À l'aide de la partie I et du lemme-clef, montrer que toutes les racines primitives n-ièmes de l'unité sont racines de M.
   (d) En déduire que B est constant.



5. Prouvé par Leonard Wedderburn (de trois façons différentes) en 1905 mais la preuve donnée ici a été trouvée par Ernst Witt en 1931.
6. On dit que I est un idéal de $\mathbb{Q}[X]$, cf. exercice 64 du chapitre 18.
7. $\mathbb{Q}$ étant un corps, le théorème de division euclidienne du cours est encore valable sur $\mathbb{Q}[X]$ (sans avoir besoin de supposer B unitaire).
8. Pour le prouver, il faut travailler sur $\mathbb{Z}/p\mathbb{Z}$.