Aix–Marseille Université 2018-2019

Mathématiques – M1

DEVOIR SURVEILLÉ N°2– ALGÈBRE ET GÉOMÉTRIE

correction

Exercice 1 Commençons par déterminer des polynômes minimaux pour $\sqrt{3}$ et $\sqrt[3]{2}$. Très clairement, on a $P(\sqrt{3}) = Q(\sqrt[3]{2}) = 0$ avec $P(X) = X^2 - 3$ et $Q(X) = X^3 - 2$. Ils sont également irréductibles sur $\mathbb{Q}[X]$, on peut argumenter cela de différentes manières :

- d'après le critère d'Eisenstein appliqués respectivement en $p = 3$ et $p = 2$;
- comme ils sont unitaires, être irréductible dans $\mathbb{Q}[X]$, c'est équivalent à être irréductible dans $\mathbb{Z}[X]$, et comme ils sont de degré inférieur à trois, être non irréductible dans $\mathbb{Z}[X]$ revient à avoir une racine α dans $\mathbb{Z}$. Mais dans ce dernier cas, on aurait alors, respectivement, $\alpha^2 = 3$ ou $\alpha^3 = 2$ et tout facteur premier de α serait de multiplicité au moins deux dans la décomposition 2 ou 3, ce qui est impossible.

Les polynômes P et Q sont donc minimaux pour $\sqrt{3}$ et $\sqrt[3]{2}$. Il suffit maintenant de calculer le résultant, en Y, de $Q(Y) = Y^3 - 2$ et $P(X - Y) = (X - Y)^2 - 3 = Y^2 - 2XY + X^2 - 3$. Cela donne

$$\begin{vmatrix} 1 & 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 & -2 \\ 1 & -2X & X^2-3 & 0 & 0 \\ 0 & 1 & -2X & X^2-3 & 0 \\ 0 & 0 & 1 & -2X & X^2-3 \end{vmatrix}$$

$$\overset{\substack{C4 \leftarrow C4 + 2.C1 \\ C5 \leftarrow C5 + 2.C2}}{=} \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & -2X & X^2-3 & 2 & -4X \\ 0 & 1 & -2X & X^2-3 & 2 \\ 0 & 0 & 1 & -2X & X^2-3 \end{vmatrix}$$

$$\overset{\substack{\text{développe } L1 \\ \text{développe } L2}}{=} \begin{vmatrix} X^2-3 & 2 & -4X \\ -2X & X^2-3 & 2 \\ 1 & -2X & X^2-3 \end{vmatrix}$$

$$\overset{\substack{C2 \leftarrow C2 + 2X.C1 \\ C3 \leftarrow C3 + (3 - X^2).C1}}{=} \begin{vmatrix} X^2-3 & 2X^3-6X+2 & -X^4+2X-9 \\ -2X & -3X^2-3 & 2X^3-6X+2 \\ 1 & 0 & 0 \end{vmatrix}$$

$$\overset{\text{développe } L3}{=} \begin{vmatrix} 2X^3-6X+2 & -X^4+6X^2-4X-9 \\ -3X^2-3 & 2X^3-6X+2 \end{vmatrix}$$

$$= (2X^3 - 6X + 2)^2 - (X^4 - 6X^2 + 4X + 9)(3X^2 + 3)$$

$$= X^6 - 9X^4 - 4X^3 + 27X^2 - 36X - 23.$$

On en déduit que $X^6 - 9X^4 - 4X^3 + 27X^2 - 36X - 23$ est un polynôme annulateur de $\sqrt{3} + \sqrt[3]{2}$.

Exercice 2

Le groupe des inversibles de $\mathbb{Z}/10\mathbb{Z}$ est cyclique. Cela peut s'argumenter de plusieurs manières :

- car le groupe des inversibles d'un corps fini est toujours cyclique ;
- car c'est un groupe de cardinal $10 = 2.5$ et que tout groupe de cardinal pq, avec p et q premiers distincts est cyclique. Là aussi, cela peut s'argumenter de plusieurs manières :
  - car d'après le théorème de Cauchy ou d'après le théorème de Sylow, il existe des éléments d'ordre 2 et 5 et, la multiplication dans $\mathbb{Z}/11\mathbb{Z}$ étant commutative, leur produit est d'ordre 10 ;

- car, d'après le théorème de Lagrange, tout élémet x non trivial est d'ordre 2, 5 ou 10, et si x est d'ordre 2 (resp. 5), alors le quotient par $< x >$ est d'ordre 5 (resp. 2) donc cyclique et qu'un relevé d'un générateur est d'ordre 5 (resp. 2) ou 10. Dans les deux cas, son produit avec x est d'ordre 10.

• car dans $\mathbb{Z}/11\mathbb{Z}$, $2^5(= 32) = -1$ donc 2 n'est d'ordre ni 2 ni 5, il est donc d'ordre 10 et engendre de fait cycliquement tout les inversibles.

Cette dernière méthode donne notamment un élément d'ordre maximal. Les autres sont ses puissances inférieures à 10, premières avec 10, à savoir $2^3 = 8$, $2^7 = 2^5.2^2(= -4) = 7$ et $2^9 = 2^7.2^2 = 7.4(= 28) = 6$. Les éléments d'ordre maximal parmi les inversibles de $\mathbb{Z}/11\mathbb{Z}$ sont donc 2, 6, 7 et 8.

Exercice 3

1. (a) Il suffit de montrer que Z est non vide et stable par addition, multiplication, prise d'opposé et prise d'inverse. Il est non vide car il contient 0 et 1, ce qui montre par ailleurs que son cardinal est au moins deux [1]. Soit $x_1, x_2 \in Z$, alors pour tout $y \in \mathbb{F}$ on a
   - $(x_1 + x_2)y = x_1y + x_2y = yx_1 + yx_2 = y(x_1 + x_2)$;
   - $x_1x_2y = x_1yx_2 = yx_1x_2$;
   - $(-x_1)y = -(x_1y) = -(yx_1) = y(-x_1)$ [2] ;
   - $x_1^{-1}y = x_1^{-1}yx_1x_1^{-1} = x_1^{-1}x_1yx_1^{-1} = yx_1^{-1}$.

   Donc $x_1 + x_2, x_1x_2, -x_1, x_1^{-1} \in Z$.

   (b) Par définition, $(\mathbb{F}, +)$ est un groupe abélien. Pour tout $\lambda \in Z$ et $x \in \mathbb{F}$, on définit $\lambda.x$ comme le produit λx dans $\mathbb{F}$. On a alors bien, pour tout $\lambda_1, \lambda_2 \in Z$ et $x_1, x_2 \in \mathbb{F}$
   - $\lambda_1.(x_1 + x_2) = \lambda_1(x_1 + x_2) = \lambda_1x_1 + \lambda_1x_2 = \lambda_1.x_1 + \lambda_1.x_2$;
   - $(\lambda_1 + \lambda_1).x_1 = (\lambda_1 + \lambda_1)x_1 = \lambda_1x_1 + \lambda_2x_1 = \lambda_1.x_1 + \lambda_2.x_1$;
   - $\lambda_1.(\lambda_2.x_1) = \lambda_1\lambda_2x_1 = (\lambda_1\lambda_2).x_1$;
   - $1.x_1 = 1x_1 = x_1$.

   Cela définit donc bien une structure de Z–espace vectoriel sur $\mathbb{F}$.

   (c) En tant que Z–espace vectoriel, $\mathbb{F}$ est nécessairement de dimension finie car sinon $\mathbb{F}$ posséderait une infinité d'éléments indépendants et donc une infinité d'éléments. Il existe donc $n \in \mathbb{N}$ tel que $\mathbb{F} \cong Z^n$ et on a $|\mathbb{F}| = |Z^n| = |Z|^n = q^n$. Mais $|\mathbb{F}| \geq 2$ donc $n \neq 0$ et on a supposé que $Z \neq \mathbb{F}$ donc $n \neq 1$.

2. (a) i. Un élément commutant avec tout le monde commute notamment avec x. On en déduit que $Z \subset Z(x)$. Mais, pour les même raisons que Z dans la question 1.(a), $Z(x)$ est par ailleurs stable par addition, multiplication, prise d'opposé et prise d'inverse ; on en déduit comme à la question 1.(b) que $Z(x)$ est un Z–espace vectoriel et donc, comme à la question 1.(c), que $|Z(x)| = q^{d_x}$ avec $d_x \in \mathbb{N}^*$.

   ii. Un élément de Stab(x) est un élément $y \in \mathbb{F}^*$ vérifiant $y^{-1}xy = x$, c'est-à-dire $xy = yx$. Un élément non nul de $\mathbb{F}$ est donc dans Stab(x) si et seulement si il est dans $Z(x)$. Par ailleurs, 0 est le seul élément nul, et il est dans Z, donc dans $Z(x)$. On en déduit que Stab$(x) \cup \{0\} = Z(x)$.

   iii. D'après la question précédente, Stab$(x) = Z(x) \cap \mathbb{F}^*$, or on a déjà vu que $Z(x)$ était stable par produit et prise d'inverse. Par intersection de groupes, c'est donc un sous-groupe de $\mathbb{F}^*$ et, d'après le théorème de Lagrange, $|\text{Stab}(x)| = q^{d_x} - 1$ divise $|\mathbb{F}^*| = q^n - 1$.

   iv. Par division euclidienne ou factorisations successives dans $\mathbb{Z}[X]$, on a

$$X^n - 1 = (X^{d_x} - 1)(X^{n-d_x} + X^{n-2d_x} + \cdots + X^r) + X^r - 1$$

1. c'est en réalité un fait général, un sous-corps contient toujours 0 et 1 et est donc toujours de cardinal au moins deux
2. la première et la dernière égalité découlant de $x_1y + (-x_1)y = (x_1 - x_1)y = 0$ et $yx_1 + y(-x_1) = y(x_1 - x_1) = 0$

avec r le reste de la division euclidienne dans $\mathbb{Z}$ de n par d_x. Evalué en $X = q$, et étant donné que $q^{d_x} - 1$ divise $q^n - 1$ d'après le point précédent, on en déduit que $q^{d_x} - 1$ divise $q^r - 1$. Or $r < d_x$ et $q \geq 2$, donc $0 \leq q^r - 1 < q^{d_x} - 1$. On en déduit que $q^r - 1 = 0$ et donc, encore car $q \geq 1$, que $r = 0$. Autrement dit, d_x divise n.

Par un argument de cardinalité, on a par ailleurs $n = d_x$ si et seulement si $Z(x) = \mathbb{F}$, c'est-à-dire si et seulement si tout le monde commute avec x, autrement dit si et seulement si $x \in Z$ et donc si et seulement si $x \in Z^*$ puisque x est supposé non nul.

v. D'après la formule des classes, on a

$$|\omega(x)| = \frac{|\mathbb{F}^*|}{|\text{Stab}(x)|} = \frac{q^n - 1}{q^{d_x} - 1} = \frac{\prod\limits_{d \text{ divise } n} \phi_d(q)}{\prod\limits_{d \text{ divise } d_x} \phi_d(q)} = \prod_{\substack{d \text{ divise } n \\ d \text{ ne divise pas } d_x}} \phi_d(q).$$

(b) i. Les orbites de l'action de $\mathbb{F}^*$ sur lui-même par conjugaison fournit une partition de $\mathbb{F}^*$. Une orbite est par ailleurs réduite à un singleton $\{x\}$ si et seulement si $\text{Stab}(x) = \mathbb{F}^*$ et donc, d'après la question 2.(a).iv., si et seulement si $x \in Z^*$. On en déduit que

$$|\mathbb{F}^*| = \sum_{\omega \text{ orbite}} |\omega| = \sum_{\substack{\omega \text{ orbite} \\ |\omega|=1}} 1 + \sum_{\substack{\omega \text{ orbite} \\ |\omega|>1}} |\omega| = \sum_{x \in Z^*} 1 + \sum_{\substack{\omega \text{ orbite} \\ |\omega|>1}} |\omega| = |Z^*| + \sum_{\substack{\omega \text{ orbite} \\ |\omega|>1}} |\omega|.$$

ii. On sait que $\phi_n(q)$ divise $q^n - 1 = |\mathbb{F}^*|$. De plus, pour tout $x \in \mathbb{F}^*$ telle que $|\omega(x)| > 1$, on a $d_x < n$ et $\phi_n(q)$ divise donc également $\prod\limits_{\substack{d \text{ divise } n \\ d \text{ ne divise pas } d_x}} \phi_d(q) = \phi_n(q) \times \prod\limits_{\substack{d \text{ divise } n, d \neq n \\ d \text{ ne divise pas } d_x}} \phi_d(q)$, qui est égal d'après la question 2.(a).v., à $|\omega(x)|$. On en déduit que $\phi_n(q)$ divise $|\mathbb{F}^*| - \sum\limits_{\substack{\omega \text{ orbite} \\ |\omega|>1}} |\omega| = |Z^*| = q - 1$.

3. (a) On a $z = a + ib$ avec $a \in [-1, 1[$ et donc $|q - z| = |q - a - ib| = \sqrt{(q-a)^2 + b^2} \geq |q - a| = q - a$ car $q \geq 2$ et $a < 1$, et pour les mêmes raisons $q - a > q - 1 \geq 1$.

(b) Comme $n > 1$, 1 n'est pas racine $n^{\text{ième}}$ primitive, on peut alors déduire de la question précédente que $|\phi_n(q)| \geq \prod\limits_{\substack{\zeta \in \mathbb{C} \text{ racine } n^{\text{ème}} \\ \text{primitive de l'unité}}} |q - \zeta| > (q-1)^{\varphi(n)} \geq q - 1$, où $\varphi(n) \geq 1$ est le degré [3] de ϕ_n, ce qui contredit le point précédent et, de fait, l'hypothèse que $\mathbb{F}$ est non commutatif. On déduit donc que $\mathbb{F}$ est commutatif.

3. ϕ_n est de degré au moins 1 car $e^{\frac{2i\pi}{n}}$ fournit déjà une racine $n^{\text{ième}}$ primitive de l'unité