

Exercice bonus 1.

Considérons l'anneau suivant pour un corps quelconque k :

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in k \right\}.$$

1. Démontrez que si $I \neq A$ est un idéal (bilatère/à gauche/à droite) de A , alors I est contenu dans un des sous-ensembles suivants de A :

$$A_1 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in k \right\}$$

et

$$A_2 = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \mid b, c \in k \right\}.$$

2. Montrez que A_1 et A_2 sont des idéaux bilatères. Montrez que A_1 et A_2 avec l'addition et la multiplication héritée de l'anneau A ne sont pas des anneaux.
3. Listez tous les idéaux (bilatères/à gauche/à droite) de A .

Solution. On note A^{op} l'anneau avec groupe additif $(A, +)$ avec la multiplication définie par

$$g_1 *_{op} g_2 = g_2 g_1.$$

Notez en premier lieu l'isomorphisme d'anneaux entre $\sigma : A \rightarrow A^{op}$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} c & b \\ 0 & a \end{pmatrix}.$$

On vérifie que c'est un isomorphisme. La bijectivité est claire, comme σ est son propre inverse au niveau ensembliste. De plus comme

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_1 \\ 0 & c_1 c_2 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} c_2 & b_2 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} c_1 & b_1 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} c_1 c_2 & a_1 b_2 + b_1 c_2 \\ 0 & a_1 a_2 \end{pmatrix},$$

on conclut que σ est un isomorphisme d'anneaux.

Cela va nous permettre d'effectuer des raisonnements par symétrie et de faire moins de calculs.

Barème. On enlèvera 10 points pour des affirmations de type "par symétrie" non motivées par des calculs ou l'isomorphisme évoqué ci-dessus. La symétrie ressentie dans la résolution de ce problème est incarnée par cet isomorphisme et il est important de pouvoir le détecter si on tient à formaliser de tels arguments.

1. On remarque si deux éléments d'une matrice dans la diagonale sont non-nuls, alors la matrice est inversible. Ainsi si I est un idéal (bilatère/à gauche/à droite) et $i \in I$ tel que les deux éléments de la diagonale sont non-nuls, comme i a dès lors un inverse (à gauche et à droite) alors $I = A$. Par contraposée, on conclut.

Barème. 10pts.

2. Notons que si

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

alors $A_1 = e_1 A$. Dès lors, A_1 est un idéal à droite. Maintenant pour $a, b, c \in k$ si

$$g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad g' = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix},$$

on a $ge_1 = e_1g'$. Ainsi on conclut que $e_1 A$ est également un idéal à gauche.

Comme $e_1^2 = e_1$, on voit que e_1 est un élément neutre à gauche dans A_1 . Si A_1 était un anneau avec la multiplication et l'addition héritée de A , celui-ci aurait un unique élément neutre 1_{A_1} et nécessairement $1_{A_1} = e_1$ car on aurait $e_1 = e_1 1_{A_1} = 1_{A_1}$. Mais si

$$e'_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

on voit $e'_1 e_1 = 0 \neq e'_1$. Ainsi, on conclut que A_1 ne peut être un anneau avec la multiplication et l'addition héritée de A .

Maintenant, A_1 est envoyé sur A_2 par l'isomorphisme σ . Dès lors, on conclut que A_2 est un idéal bilatère, et que A_2 ne peut être un anneau avec l'addition et la multiplication héritée de A .

Barème. 10 points pour montrer que A_1 et A_2 sont bilatères. 20 points pour montrer que ce ne sont pas des anneaux.

3. Traitons les idéaux non-nuls et non égaux à A . On commence par traiter les idéaux strictement contenus dans A_1 . On voit qu'un tel idéal I est forcément un k -espace vectoriel de dimension 1. Ainsi I est forcément de la forme, pour $a, b \in k$ fixés non tous les deux nuls

$$I = \left\{ \begin{pmatrix} \lambda a & \lambda b \\ 0 & 0 \end{pmatrix} \mid \lambda \in k \right\}.$$

Si $a = 0$, on note l'idéal

$$I_0 = \left\{ \begin{pmatrix} 0 & \lambda \\ 0 & 0 \end{pmatrix} \mid \lambda \in k \right\}.$$

Comme $I_0 = A_1 \cap A_2$, I_0 est un idéal bilatère.

On traite maintenant le cas $a \neq 0$. On a les possibilités suivantes pour $\mu \in k$

$$I_1(\mu) = \left\{ \lambda \begin{pmatrix} 1 & \mu \\ 0 & 0 \end{pmatrix} \mid \lambda \in k \right\}.$$

Si $a, b, c \in k$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & \mu \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & a\mu \\ 0 & 0 \end{pmatrix}.$$

Ainsi $I_1(\mu)$ est un idéal à gauche. En revanche comme

$$\begin{pmatrix} 1 & \mu \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

on voit que $I_1(\mu)$ n'est pas un idéal à droite.

On a donc traité tous les idéaux non-nuls et stricts de A_1 . On sait de plus par le premier point que les idéaux non égaux à A sont forcément dans A_1 ou dans A_2 .

Notons

$$I_2(\mu) = \left\{ \lambda \begin{pmatrix} 0 & \mu \\ 0 & 1 \end{pmatrix} \mid \lambda \in k \right\}.$$

Par symétrie (l'isomorphisme entre A et A^{op} évoqué plus haut), on peut donc conclure que

$\{0\}, I_0, A_1, A_2, A$ sont les idéaux bilatères

que pour $\mu_1 \in k$

$I_1(\mu_1)$ sont les idéaux à gauche mais pas à droite

et que pour $\mu_2 \in k$

$I_2(\mu_2)$ sont les idéaux à droite mais pas à gauche.

Barème. 10 points pour montrer que I_0 est bilatère. 10 points pour montrer que les $I_1(\mu)$ sont des idéaux à gauche. 10 points pour montrer que les $I_1(\mu)$ ne sont des idéaux pas des idéaux à droite. 20 points pour traiter les $I_2(\mu)$ (donc que ce sont des idéaux à droite et pas à gauche). 10 points pour conclure avec la liste et argumenter que ce sont les seuls.

Si vous le souhaitez, vous pouvez rendre votre solution de l'exercice bonus sur la page Moodle du cours avant le mardi 30 mai, 18h.

Exercice bonus 6. Soit k un corps. On considère le corps des fonctions rationnelles $k(t)$. Soit $a, b, c, d \in k$ avec $ad - bc \neq 0$.

1. Soit $s \in k(t)$ non-constant. Montrer qu'il existe un unique k -morphisme $\phi_s : k(t) \rightarrow k(s)$ qui envoie t sur s .

Indication. Pour l'injectivité $k[t] \rightarrow k(s)$, montrer d'abord si $s = p(t)$ pour $p(t) \in k[t]$. Montrer ensuite pour $s = \frac{p(t)}{q(t)}$ en supposant que $(p(t), q(t)) = 1$. Remarquer que si un polynôme non-nul de degré n annule s , alors forcément $q(t) | p(t)^n$ dans $k[t]$.

2. Pour $s = \frac{at+b}{ct+d}$, montrez que ϕ_s définit un k -automorphisme de $k(t)$.

En utilisant le langage de la géométrie algébrique, on peut montrer que tout k -automorphisme de $k(t)$ est de cette forme. Ce fait n'est pas utile pour le reste de cet exercice.

3. Démontrez que l'association $\mathrm{GL}(2, k) \rightarrow \mathrm{Aut}_k(k(t))$ définie par

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto \phi_{\frac{at+b}{ct+d}}$$

donne un homomorphisme injectif des groupes

$$\alpha : \mathrm{PGL}(2, k) \hookrightarrow \mathrm{Aut}_k(k(t)).$$

4. Pour les éléments $g \in \mathrm{PGL}(2, k)$ suivants, si $G = \langle \alpha(g) \rangle$, calculer $d = [k(t) : k(t)^G]$.

- (a) Calculer ce degré avec

$$g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

- (b) Supposons que $\mathrm{char}(k) \neq 2$ et que k possède une racine primitive n -ième de l'unité (un élément d'ordre n dans le groupe multiplicatif $k^\times$) qu'on note ξ . Calculer ce degré avec

$$g = \begin{pmatrix} \xi + \frac{1}{\xi} & -\xi + \frac{1}{\xi} \\ -\xi + \frac{1}{\xi} & \xi + \frac{1}{\xi} \end{pmatrix}.$$

Exercice bonus 2.

Définition. Un anneau commutatif A est dit *connexe* si pour tout $a, b \in A$ tel que

$$a + b = 1 \quad \text{et} \quad ab = 0$$

alors soit $a = 0$ et $b = 1$, soit $a = 1$ et $b = 0$.

1. Montrer qu'un anneau commutatif est connexe si et seulement si les seuls idempotents de A sont 0 et 1.

On dit que $e \in A$ un idempotent est un *idempotent minimal* si eA est un anneau connexe non-nul avec l'addition et la multiplication venant de A avec e comme élément neutre. On pose

$$\pi_0(A) = \{e \in A \mid e \text{ est un idempotent minimal}\}$$

Remarquer que A est connexe si et seulement si $\pi_0(A) = \{1\}$.

2. Soit $(A_i)_{i=1}^n$ une collection finie d'anneaux connexes. Montrer que

$$|\pi_0(\prod_{i=1}^n A_i)| = n.$$

3. Montrer que

$$|\pi_0(\mathbb{Q}[\mathbb{Z}/4\mathbb{Z}])| = 3.$$

Solution.

1. Supposons tout d'abord que A est connexe. Soit $e \in A$ un idempotent. Alors $e + (1 - e) = 1$ et $e(1 - e) = 0$. Comme A est connexe, soit $e = 0$ ou $e = 1$. Réciproquement si les seuls idempotents sont 1 et 0, et $a, b \in A$ sont tels que $a + b = 1$ et $ab = 0$, alors $a = a(a + b) = a^2 + ab = a^2$. Ainsi a est idempotent et donc $a = 0$ ou $a = 1$, et par suite $b = 1$ ou $b = 0$.

Barème. 10 points pour chaque direction de l'équivalence.

2. Soit $(e_i) \in \prod_{i=1}^n A_i$ un idempotent minimal. Notons qu'alors e_i est un idempotent dans A_i . Ainsi, comme les A_i sont supposés connexes, soit $e_i = 0$ ou $e_i = 1$. Comme un produit $B \times C$ d'anneau non-nuls n'est jamais connexe car

$$(1_B, 0) + (0, 1_C) = 1_{B \times C} \quad (1_B, 0)(0, 1_C) = 0_{B \times C}$$

on voit qu'il existe un unique i_0 tel que $e_{i_0} = 1$. Dès lors il y a exactement n idempotents minimaux donnés par $f_i = (\delta_{ij})$ pour $1 \leq i \leq n$.

Barème. 10 points pour déterminer la forme des idempotents. 10 points pour identifier la forme des idempotents minimaux/un produit d'anneau non-nuls n'est jamais connexe. 10 points pour conclure/trouver les n idempotents minimaux.

3. Pour éviter toute confusion, on note $G = \mathbb{Z}/4\mathbb{Z}$, avec générateur x . On note que $\mathbb{Q}[G]$ est un $\mathbb{Q}$ -espace vectoriel de dimension 4, de base $1, x, x^2, x^4$ par définition d'anneau de groupe. On montre dans ce qui suit que le noyau de la surjection $\mathbb{Q}[t] \xrightarrow{\text{ev}_x} \mathbb{Q}[G]$ est $(t^4 - 1)$. Premièrement, comme $x^4 = 1$, il suit que cet idéal est inclus dans le noyau. Supposons qu'il existe un polynôme $p(t) = at^3 + bt^2 + ct + d \in \mathbb{Q}[t]$ de degré au plus 3 tel que $p(x) = 0$. Alors,

$$ax^3 + bx^2 + cx + d = 0.$$

Comme $1, x, x^2, x^3$ est une $\mathbb{Q}$ -base de $\mathbb{Q}[G]$, il suit que $a = b = c = d = 0$. Soit maintenant $f(t) \in \mathbb{Q}[t]$ tel que $f(x) = 0$ avec $\deg(f(t)) > 3$. Par division euclidienne il existe $q(t), r(t) \in \mathbb{Q}[t]$ avec $\deg(r(t)) \leq 3$ avec

$$f(t) = q(t)(t^4 - 1) + r(t).$$

Ainsi $r(x) = 0$ et par suite grâce à l'étape précédente $r(t) = 0$. Ainsi on conclut par double inclusion que $(t^4 - 1) = \ker(\text{ev}_x)$. On a dès lors,

$$\mathbb{Q}[G] \cong \mathbb{Q}[t]/(t^4 - 1).$$

Notons que $t^4 - 1 = (t^2 - 1)(t^2 + 1)$. On voit que la somme des idéaux $(t^2 - 1)$ et $(t^2 + 1)$ contient 1 car

$$\frac{t^2 + 1}{2} + \frac{1 - t^2}{2} = 1.$$

Ainsi, par le théorème des restes chinois, on a,

$$\mathbb{Q}[t]/(t^4 - 1) \cong \mathbb{Q}[t]/(t^2 - 1) \times \mathbb{Q}[t]/(t^2 + 1).$$

Comme $t^2 - 1 = (t - 1)(t + 1)$ et que la somme des idéaux $(t - 1)$ et $(t + 1)$ contient 1 car

$$\frac{t + 1}{2} + \frac{1 - t}{2} = 1$$

on peut encore appliquer le théorème des restes chinois pour obtenir,

$$\mathbb{Q}[t]/(t^4 - 1) \cong \mathbb{Q}[t]/(t - 1) \times \mathbb{Q}[t]/(t + 1) \times \mathbb{Q}[t]/(t^2 + 1).$$

Avant de conclure, on montre que le noyau de la surjection $\mathbb{Q}[t] \xrightarrow{\text{ev}_i} \mathbb{Q}[i]$ est $(t^2 + 1)$. Comme $\mathbb{Q}[i]$ est un $\mathbb{Q}$ -espace vectoriel de dimension 2, il suit que si $f(t) \in \ker(\text{ev}_i)$ avec $\deg(f(t)) \leq 2$, alors $f(t) = 0$. Pour un élément quelconque du noyau, on se ramène à ce cas par division euclidienne, comme plus haut.

Ainsi, on conclut que

$$\mathbb{Q}[G] \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}[i].$$

Comme un anneau intègre est connexe (car si $a, b \in A$ un anneau intègre tel que $ab = 0$, alors a ou $b = 0$.) On conclut ainsi que

$$|\pi_0(\mathbb{Q}[\mathbb{Z}/4\mathbb{Z}])| = 3.$$

Barème. 20 points pour monter $\mathbb{Q}[G] \cong \mathbb{Q}[t]/(t^4 - 1)$. 10+10 points pour utiliser deux fois le théorème des restes chinois. 10 points pour montrer que $\mathbb{Q}[i] \cong \mathbb{Q}[t]/(t^2 + 1)$. 10 points pour conclure.

Remarque. Les idempotents minimaux de $\mathbb{Q}[G]$ sont :

$$\frac{x^3 + x^2 + x + 1}{4}, \quad \frac{1 - x + x^2 - x^3}{4}, \quad \frac{1 - x^2}{2}.$$

Remarque. Pour montrer que $\mathbb{Q}[G]$ est isomorphe à $\mathbb{Q}[t]/(t^4 - 1)$ on peut utiliser l'adjonction $\mathbb{Q}[G] \dashv (-)^\times$ entre les $\mathbb{Q}$ -algèbres et les groupes abéliens pour conclure que ces deux anneaux co-représentent tous deux le foncteur $\xi_4 : \mathbb{Q}\text{-Alg} \rightarrow \text{Set}$

$$A \mapsto \{a \in A \mid a^4 = 1\}.$$

Exercice bonus 3. Soit p un nombre premier. On dit qu'un anneau commutatif est de *caractéristique* p si le morphisme $\mathbb{Z} \rightarrow A$ envoie p sur zéro et donc factorise par $\mathbb{F}_p \rightarrow A$. **Dans cet exercice, on travaille uniquement avec des anneaux non-nuls commutatifs de caractéristique p .** On note $F : A \rightarrow A$ le *morphisme de Frobenius* $a \mapsto a^p$. Voir *Série 3, exercice 4.3*.

1. Montrer que le morphisme $\mathbb{F}_p \rightarrow A$ est injectif.
2. Montrer que $A^F := \{a \in A \mid F(a) = a\}$ est un sous-anneau.
3. Montrer que si A est intègre et $A = A^F$, alors $\mathbb{F}_p \rightarrow A$ est un isomorphisme.
4. Montrer que si $A = A^F$, alors tout idéal premier est maximal.
5. Montrer que $\pi_0(A) = \pi_0(A^F)$. (Voir *exercice bonus 2*.)

Solution.

1. Comme A est non-nul, et que les seuls idéaux de $\mathbb{F}_p$ sont l'idéal nul et $\mathbb{F}_p$, il suit que $A \rightarrow \mathbb{F}_p$ est injectif. En effet, si le noyau est égal à $\mathbb{F}_p$ cela implique que 1 est envoyé sur 0 et donc que l'anneau d'arrivée est nul, ce qui est exclu par hypothèse.

Barème. 10 points.

2. Cela suit du fait que F est un morphisme d'anneau. En effet, $0, 1 \in A^F$ et si $a, b \in A^F$ alors $F(a + b) = F(a) + F(b) = a + b$ et $F(ab) = F(a)F(b) = ab$. On conclut donc que A^F est un sous-ensemble de A qui contient 0 et 1, et stable par addition et multiplication, donc un sous-anneau.

Barème. 10 points.

3. Si $a \in A$ est nilpotent, alors il existe n tel que $a^n = 0$. Soit alors N suffisamment grand tel que $p^N \geq n$. On obtient alors $a = a^{p^N} = 0$. On conclut donc que $\text{nil}(A) = 0$.

Barème. 10 points.

4. On sait déjà par le premier point que $\mathbb{F}_p \rightarrow A$ est injectif. Notons que $A = A^F$ signifie que $a^p = a$ pour tout $a \in A$.

Par l'absurde on suppose que $|A| \geq p + 1$. Notons dès lors $a_1, \dots, a_{p+1}$ des éléments distincts de A . On mène la division euclidienne de $t^p - t$ par $t - a_1$ pour obtenir un $f_1(t) \in A[t]$ tel que

$$t^p - t = (t - a_1)f(t) + a$$

pour $a \in A$. En évaluant en a_1 , on obtient que $a = 0$. *Maintenant, on utilise de manière cruciale que A est intègre* pour voir que pour $i \geq 2$ on a $f(a_i) = 0$. En effet en évaluant en a_i on a

$$0 = (a_i - a_1)f(a_i),$$

et donc comme $a_1 \neq a_i$ et que A est intègre, on voit que $f(a_i) = 0$. Ainsi, on peut continuer par récurrence sur $2 \leq i \leq p + 1$ obtenir par le même procédé que

$$t^p - t = (t - a_1) \cdots (t - a_{p+1})g(t)$$

pour un $g(t) \in A[t]$. Ainsi par la formule du degré (notons qu'ici intègre n'est *pas* utilisé car tous les polynômes en jeu sont moniques) on voit que

$$p = \deg(t^p - t) \geq p + 1,$$

une contradiction.

Barème. 10 points pour avoir l'idée de diviser le polynôme $t^p - t$. 10 points pour utiliser l'hypothèse d'intégrité. 10 points si la preuve est correcte.

5. Soit $\mathfrak{p}$ premier de A . Alors $A/\mathfrak{p}$ est encore fixé par le Frobenius. On conclut alors avec le point précédent. En effet, il suit que le morphisme

$$\mathbb{F}_p \rightarrow A \rightarrow A/\mathfrak{p}$$

est un isomorphisme. Dès lors comme $A/\mathfrak{p}$ est un corps, il suit que $\mathfrak{p}$ est maximal.

Barème. 10 points pour se réduire au cas intègre. 10 points pour utiliser le point précédent et conclure.

6. On commence par montrer que A est connexe si et seulement si A^F est connexe. Tout d'abord, notons que tout les idempotents de A sont dans A^F et donc les idempotents de A et de A^F sont en bijection. Comme un anneau non-nul est connexe si et seulement si les seuls idempotents sont 0 et 1, notre assertion suit.

Notons désormais que $\pi_0(A) = \pi_0(A^F)$ suivrait de, si $e \in A$ est un idempotent

$$(eA)^F = eA^F.$$

On montre alors cette dernière égalité. Notons que $eA^F \subset (eA)^F$. Pour l'inclusion inverse, il suffit simplement de noter que si $(ea)^p = ea$, alors $ea = e(ea) \in eA^F$.

Barème. Si on a procédé comme au-dessus, 10 points pour montrer que A est connexe si et seulement si A^F est connexe, puis 10 points pour conclure.

Exercice bonus 4. Soit $A = \mathbb{Z}[i\sqrt{d}]$ pour un $d \geq 1$. Pour un $a + bi\sqrt{d} \in \mathbb{Z}[i\sqrt{d}]$ on pose la norme $N(a + bi\sqrt{d}) = a^2 + db^2$

1. Soit $x \in A$ non-nul. Montrer que

$$|A/(x)| = N(x).$$

(C'est à dire que la cardinalité du quotient est égale à la norme de x .)

Remarquer que A est un groupe abélien libre de rang 2 et que le quotient $A/(x)$ est égal au quotient de A par l'image de l'application linéaire $\cdot x : A \rightarrow A$, et utiliser la forme normale de Smith pour conclure.

Dans le point 2. on considère (B, σ) un anneau euclidien quelconque qui n'est pas un corps.

2. Montrer qu'il existe un $b \in B$ non-nul et non inversible tel que

$$|B/(b)| \leq |B^\times| + 1.$$

3. Montrer que si $d > 3$, alors A n'est pas Euclidien. (Il ne s'agit pas de montrer que N n'est pas une fonction Euclidienne pour A , mais qu'il n'en existe aucune.)

Solution.

1. Prenons $x = a + bi\sqrt{d} \in A$ non-nul. On prend $(1, i\sqrt{d})$ comme $\mathbb{Z}$ -base de A . Dès-lors il suit que la matrice de $\cdot x$ dans cette base est

$$\begin{pmatrix} a & -db \\ b & a \end{pmatrix}.$$

Le déterminant de cette matrice qui est égal $a^2 + bd^2 = N(x)$. Par la forme normale de Smith, il existe des automorphismes de groupes abéliens $f, g : A \rightarrow A$ tel que $f \circ (\cdot x) \circ g$ est sous forme diagonale dans la base $(1, i\sqrt{d})$. Soit donc $\alpha_1, \alpha_2 \in \mathbb{Z}$ tel que la matrice soit de forme,

$$\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}.$$

avec donc $|\alpha_1\alpha_2| = N(x)$. Ainsi on peut identifier $A/(x)$ en tant que groupe abélien à

$$\mathbb{Z}/\alpha_1\mathbb{Z} \oplus \mathbb{Z}/\alpha_2\mathbb{Z}$$

ce qui conclut. (Noter que comme le déterminant est non nul α_1 et α_2 sont aussi non-nuls, et donc ces groupes sont finis, de cardinal $|\alpha_1\alpha_2|$.)

Barème. 10 points pour identifier la norme d'un élément non-nul x avec le déterminant de l'application $\cdot x$. 20 points pour utiliser la forme normale de Smith et pour exprimer $A/(x)$ comme une somme de groupe abélien finis. 10 points pour conclure.

2. Soit $b \in B$ non-nul et non-inversible (B n'est pas un corps) tel que $\sigma(b)$ soit minimal parmi les éléments non-nuls et non-inversibles. Soit $b' \in B$ quelconque. Comme b est non-nul, par division Euclidienne, il existe $q, r \in B$ tel que

$$b' = bq + r,$$

avec $\sigma(r) < \sigma(b)$ ou $r = 0$, en particulier r est nul ou inversible. Dès lors, il suit que

$$|B/(b)| \leq |B^\times| + 1.$$

Barème. 20 points pour l'idée de prendre b non-nul et non inversible avec $\sigma(b)$ minimal. 10 points pour conclure avec la division euclidienne.

3. Supposons par l'absurde que A soit Euclidien. Soit dès lors un élément $x = a + bi\sqrt{d} \in A$ comme au point précédent. Avec la norme multiplicative $N : A \rightarrow \mathbb{N}$, on voit que les seuls inversibles de A sont 1 et -1 . Dès lors, une combinaison deux deux points précédents donne,

$$1 < a^2 + b^2d \leq 3.$$

Comme $d > 3$ on voit que $b = 0$. Comme 2 et 3 ne sont pas des carrés d'entiers, on aboutit à une contradiction.

Barème. 10 points pour identifier les inversibles de A à $\{1, -1\}$. 20 points pour utiliser les deux points précédents et conclure.

Exercice bonus 5. Soit $n \geq 1$ un entier. On dit qu'une racine n -ième de l'unité ξ est primitive si n est le plus petit entier tel que $\xi^n = 1$. On pose,

$$\Phi_n(t) = \prod_{\substack{\xi \text{ racine} \\ \text{primitive} \\ n\text{-ième} \\ \text{de l'unité}}} (t - \xi) \in \mathbb{C}[t].$$

1. Montrer que $t^n - 1 = \prod_{d|n} \Phi_d(t)$ et que $\Phi_n(t) \in \mathbb{Z}[t]$.
2. Soit p un nombre premier et $n \geq 1$. En utilisant le critère d'Eisenstein et le changement de variable $t \mapsto t + 1$, montrer que $\Phi_{p^n}(t)$ est irréductible. (c.f. exemple 3.9.4.(2))
3. Soit $n \geq 1$ un entier et p un premier qui est premier avec n . On note ξ_n une racine primitive n -ième de l'unité. Soit $m(t) \in \mathbb{Q}[t]$ le polynôme minimal de ξ_n . Montrer que $m(t) \in \mathbb{Z}[t]$. Montrer que si ξ est une racine de $m(t)$, alors ξ^p est une racine de $m(t)$. En déduire que $m(t) = \Phi_n(t)$.

Indication: on pourra montrer par l'absurde que si ξ^p n'est pas une racine de $m(t)$ alors $t^n - 1$ a une racine double modulo p , ce qui est absurde comme $(n, p) = 1$ (Voir Proposition 4.4.10).

4. Montrer qu'il existe une infinité de premiers p tel que $\Phi_n(t)$ a une racine dans $\mathbb{F}_p[t]$. En déduire qu'il existe une infinité de premiers p tel que $p \equiv 1 \pmod n$.

Indication: pour tout m suffisamment grand si un nombre premier p divise $\Phi_n(m!)$ alors $p > m$.

Solution.

1. Notons que comme le produit de toutes les racines n -ièmes de l'unité sont égales au produit des racines primitives d -ièmes pour $d \mid n$, on a

$$t^n - 1 = \prod_{d|n} \Phi_d(t).$$

On montre par récurrence sur n que $\Phi_n(t)$ a coefficients entiers. Pour $n = 1$, on a $\Phi_1(t) = (t - 1)$. Pour $n > 1$ notons que $\Phi_n(t)$ est le résultat de la division euclidienne dans $\mathbb{Z}[t]$ de $t^n - 1$ par $\prod_{d|n, d \neq n} \Phi_d(t)$ et ce dernier polynôme est bel et bien à coefficients entiers par récurrence.

Barème. 10 pts pour $t^n - 1 = \prod_{d|n} \Phi_d(t)$, et 10 pts pour montrer que les coefficients du polynôme sont entiers.

2. Notons tout d'abord que

$$t^p - 1 = (t - 1)\Phi_p(t),$$

et donc que $\Phi_p(t) = t^{p-1} + t^{p-2} + \dots + 1$. Notons également que

$$t^{p^n} - 1 = (t^{p^{n-1}} - 1)\Phi_{p^n}(t),$$

et donc que $\Phi_{p^n}(t) = \Phi_p(t^{p^{n-1}})$. Notons que $\Phi_{p^n}(t+1) \equiv (\Phi_p(t+1))^{p^{n-1}} = t^{p^{n-1}} \pmod p$ par le raisonnement de l'exemple 3.9.4.(2). Comme de plus le coefficient constant de $\Phi_{p^n}(t+1)$ est égal à p , le critère d'Eisenstein permet de conclure à l'irréductibilité de $\Phi_{p^n}(t)$.

Barème. 10 pts pour montrer que $\Phi_{p^n}(t) = \Phi_p(t^{p^{n-1}})$. 10 pts pour conclure avec Eisenstein.

3. Écrivons $t^n - 1 = m(t)g(t)$ avec $g(t) \in \mathbb{Q}$. Comme $m(t)$ et $t^n - 1$ ont coefficients dominant 1, g aussi. Dès lors pour $c, d \in \mathbb{Z}$, on a

$$t^n - 1 = \frac{1}{c}(cm(t))\frac{1}{d}(dg(t))$$

pour $cm(t), dg(t) \in \mathbb{Z}[t]$ primitifs. Par le lemme de Gauss (version II), on a $\frac{1}{cd} \in \mathbb{Z}^\times$. Donc $\frac{1}{d} = \pm c \in \mathbb{Z}$ et donc $c, d = \pm 1$. Ainsi $m(t) \in \mathbb{Z}[t]$.

Soit ξ une racine quelconque de $m(t)$ et par l'absurde supposons que ξ^p ne soit pas une racine de $m(t)$. Alors si $t^n - 1 = m(t)f(t)$ on a que ξ^p est une racine de $f(t)$. Comme $m(t)$ est irréductible dans $\mathbb{Q}[t]$, notons que c'est aussi le polynôme minimal de ξ . Dès lors $m(t) | f(t^p)$ dans $\mathbb{Q}[t]$ et donc dans $\mathbb{Z}[t]$ comme ces polynômes sont primitifs. En réduisant modulo p (ce qu'on dénote par $\overline{(-)}$ dans la suite), on voit alors que $\overline{m(t)} | \overline{f(t^p)} = (\overline{f(t)})^p$. Dès lors, $\overline{m(t)}$ et $\overline{f(t)}$ ont une racine commune, car les racines (sans compter les multiplicités) de $\overline{f(t)}$ et $(\overline{f(t)})^p$ sont les mêmes. Mais comme $\overline{t^n - 1} = \overline{m(t)f(t)}$ n'a pas de racine multiple comme $(n, p) = 1$, on obtient une contradiction.

Notons que toute racine primitive n -ième de l'unité est de la forme $\xi_n^{p_1 \cdots p_r}$ avec $(p_i, n) = 1$. On obtient par récurrence sur r que toute racine primitive n -ième de l'unité est une racine de $m(t)$ et donc que $\Phi_n(t) = m(t)$.

Barème. 10 pts pour montrer que $m(t)$ est à coefficients entiers. 20 pts pour montrer si ξ est une racine de $m(t)$ alors, ξ^p aussi. 5 pts pour $\Phi_n(t) = m(t)$.

4. Soit m suffisamment grand pour que $\Phi_n(m!) \neq 0, 1, -1$. Soit alors p premier tel que $p \mid \Phi_n(m!)$. Alors $p \mid (m!)^n - 1$. Si $p \leq m$, on aurait $p \mid 1$, ce qui est absurde. Ainsi, il suit qu'il existe une infinité de premiers tel que $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p$. En effet, on peut prendre un $m' \geq p$ puis appliquer à nouveau l'argument pour m' pour trouver un premier $p' > m' \geq p$ et ainsi de suite pour construire une suite infinie croissante de premiers où $\overline{\Phi_n(t)}$ s'annule.

Notons que n est fixé et donc sans perte de généralité $(p, n) = 1$. Notons k le corps de décomposition de $\overline{t^n - 1} \in \mathbb{F}_p[t]$. On montre par récurrence croissante sur les diviseurs d de n que les racines de $\overline{\Phi_d(t)}$ dans k sont exactement les racines primitives d -ième de l'unité. Pour $d = 1$, l'assertion est vérifiée car $\overline{\Phi_1(t)} = \overline{t - 1}$. Traitons le pas d'induction. Comme $(p, d) = 1$ le polynôme $\overline{t^d - 1} \in \mathbb{F}_p[t]$ n'a pas de racines multiples. Ainsi le sous-groupe multiplicatif des racines d -ième de l'unité est de cardinal d . Comme tous les éléments de ce sous-groupe multiplicatif sont des racines de $t^e - 1$ pour e l'exposant du groupe, on a forcément $d = e$ sinon $t^e - 1$ aurait trop de racines. Dès lors ce sous-groupe est cyclique d'ordre d . Grâce à la récurrence les racines de $\overline{\Phi_{d'}(t)}$ pour tout diviseur $d' \neq d$ de d sont les racines primitives d' -ième de l'unité, c'est à dire les éléments multiplicatifs d'ordre d' . Par suite, en utilisant la formule du point 1., les racines de $\overline{\Phi_d(t)}$ sont forcément les éléments restants du groupe cyclique formé par les racines de $t^d - 1$, c'est à dire les éléments d'ordre d .

Dès lors si $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p$, cela implique qu'il existe une racine primitive n -ième de l'unité dans $\mathbb{F}_p$. En particulier, par Lagrange, $n \mid p - 1$, et donc que $p \equiv 1 \pmod{n}$.

Barème. 10 pts pour montrer qu'il y a une infinité de premiers tel que $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p$. 10 pts pour montrer que les racines de $\overline{\Phi_n(t)}$ sont des racines primitives de l'unité (noter que l'hypothèse $(p, n) = 1$ est importante pour cela.) 5 pts pour conclure avec Lagrange.