Algèbre – Devoir à la maison I

*Le devoir est à rendre au plus tard le **lundi 16 Octobre 2023**. Vous pouvez le rédiger en **français ou en anglais**. Le devoir est à rendre de l'une des façons suivantes : **directement lors d'une séance de TD** OU **à mon bureau** (2G20 au bâtiment 307) OU **dans mon casier** à l'entrée du bâtiment 307 OU **par mail en un UNIQUE fichier pdf avec votre nom** dans le nom du fichier à l'adresse kevin.destagnol@universite-paris-saclay.fr. Vous pouvez également bien sûr me contacter à cette adresse mail en cas de questions ou si vous repérez ce qui vous semble être une erreur d'énoncé.*

Problème 1 — C'est simple non ?!.

Soit n un entier et $k = \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ le corps fini à p éléments avec p un nombre premier. Soit E le k-espace vectoriel k^n. On note $\mathbf{P}(E)$ l'ensemble des droite vectorielles de K^n, *espace projectif de dimension* $n-1$. On notera également $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$ l'ensemble des matrices carrées de taille n à coefficients dans k de déterminant respecitvement non nul et 1.

1. Montrer que $Z(\mathrm{GL}_n(k)) = \{\lambda I_n \ : \ \lambda \in k^\times\} \cong k^\times$ et que $Z(\mathrm{SL}_n(k)) = \{\lambda I_n \ : \ \lambda \in k, \ \lambda^n = 1\}$.
On définit alors $\mathrm{PGL}_n(k) = \mathrm{GL}_n(k)/Z(\mathrm{GL}_n(k))$ et $\mathrm{PSL}_n(k) = \mathrm{SL}_n(k)/Z(\mathrm{SL}_n(k))$. Préciser les cardinaux des quatre groupes en jeu.
2. Montrer qu'il existe un morphisme injectif Φ de $\mathrm{PGL}_n(K)$ dans le groupe symétrique $\mathfrak{S}(\mathbf{P}(E))$.
3. Montrer que, si $n = 2$, $\mathbf{P}(E)$ est de cardinal $p+1$. On identifie Φ à un morphisme $\mathrm{PGL}_2(K) \longrightarrow \mathfrak{S}_{p+1}$.
4. On prend $p = 2$. Montrer que Φ induit des isomorphismes de $\mathrm{PGL}_2(\mathbf{F}_2)$ et $\mathrm{PSL}_2(\mathbf{F}_2)$ sur $\mathfrak{S}_3$.
5. On prend $p = 3$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}_2(\mathbf{F}_3)$ sur $\mathfrak{S}_4$ et de $\mathrm{PSL}_2(\mathbf{F}_3)$ sur $\mathfrak{A}_4$. Les groupes $\mathrm{PGL}_2(\mathbf{F}_3)$ et $\mathrm{SL}_2(\mathbf{F}_3)$ sont-ils isomorphes ?
6. On prend $p = 5$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}_2(\mathbf{F}_5)$ sur $\mathfrak{S}_5$ et de $\mathrm{PSL}_2(\mathbf{F}_5)$ sur $\mathfrak{A}_5$.
On pourra établir que tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$ pour $n \geqslant 5$.
7. On admettra dans un premier temps que $\mathrm{SL}_3(\mathbf{F}_2)$ est constitué de six classes de conjugaison : une de cardinal 1 consituée de I_3, une de cardinal 21 constituée d'éléments d'ordre 2, une de cardinal 56 constituée d'éléments d'ordre 3, deux de cardinal 24 constituée d'éléments d'ordre 7 et une de cardinal 42 constituée déléments d'ordre 4. Établir que $\mathrm{SL}_3(\mathbf{F}_2)$ est simple.
8. Dans toute cette question on supposera que G est un groupe non abélien.
   (a) Supposons que G est un groupe simple d'ordre $p^\alpha m$ avec $\alpha \geqslant 1$ et $p \nmid m$, p premier. On note n_p le nombre de p-Sylow de G. Montrer que $\#G$ divise $n_p!$.
   (b) Montrer que les seuls groupes simples non abéliens d'ordre $\leqslant 60$ sont d'ordre 48 ou 60.
   On pourra utiliser que tout entier $n \leqslant 60$, $n \notin \{48, 60\}$ est de la forme p^n, pq, pqr, p^2q, p^3q avec $p < q < r$ trois nombres premiers ou de la forme $p^m q^n$ avec $p < q$ premiers, $1 \leqslant m \leqslant 2$ et $n \geqslant 1$.
   (c) Montrer qu'un groupe d'ordre 48 n'est pas simple et exhiber un groupe simple d'ordre 60.

(Bonus)
   (a) Que dire d'une matrice de $\mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal $X+1$?
   (b) On suppose que $M \in \mathrm{SL}_3(\mathbf{F}_2)$ admet X^2+1 comme polynôme minimal. Montrer qu'une telle matrice est caractérisée par $\mathrm{Ker}(A+I_3)$ et $\mathrm{Ker}(A+I_3)$. Préciser les dimensions de ces espaces vectoriels et en déduire que les matrices de polynôme minimal X^2+1 forment une classe de conjugaison dont on spécifiera le cardinal et l'ordre des éléments.
   (c) Montrer qu'il n'existe aucune matrice $M \in \mathrm{SL}_3(\mathbf{F}_2)$ admettant X^2+X+1 comme polynôme minimal.
   (d) On suppose que $M \in \mathrm{SL}_3(\mathbf{F}_2)$ admet X^3+1 comme polynôme minimal. Établir que $\mathrm{Ker}(A+I_3)$ et $\mathrm{Ker}(A^2+A+I_3)$ sont supplémentaires. Préciser les dimensions de ces espaces vectoriels et en déduire que les matrices de polynôme minimal X^3+1 forment une classe de conjugaison dont on spécifiera le cardinal et l'ordre des éléments.
   Indication : On pourra remarquer qu'une matrice de $\mathrm{SL}_3(\mathbf{F}_2)$ de polynôme caractéristique X^2+X+1 est de la forme $\begin{pmatrix} a & 1 \\ 1 & 1-a \end{pmatrix}$ *avec $a \in \mathbf{F}_2$.*
   (e) Supposons que $M \in \mathrm{SL}_3(\mathbf{F}_2)$ admet un polynôme minimal irréductible de degré 3. Montrer qu'alors pour tout $x \in \mathbf{F}_2^3$, la famille (x, Ax, A^2x) est une base de $\mathbf{F}_2^3$. En déduire que les matrices de polynôme minimal X^3+X+1 (respectivement X^3+X^2+1) forment une classe de conjugaison dont on spécifiera le cardinal et l'ordre des éléments.
   (f) Supposons que $M \in \mathrm{SL}_3(\mathbf{F}_2)$ admet X^3+X^2+X+1 comme polynôme minimal. Montrer que $\mathrm{Ker}(A+I_3) \subseteq \mathrm{Ker}(A+I_3)^2$ et préciser les dimensions en jeu. Que dire de l'image par $A+I_3$ d'un vecteur de $\mathbf{F}_2^3 \smallsetminus \mathrm{Ker}(A+I_3)^2$? En déduire que les matrices de polynôme minimal X^3+X^2+X+1 forment une classe de conjugaison dont on spécifiera le cardinal et l'ordre des éléments.
   (g) En déduire que que $\mathrm{SL}_3(\mathbf{F}_2)$ est simple.

► **Compléments.** –On peut montrer[1] que les seuls groupes simples d'ordre $\leqslant 660$ sont d'ordre 60, 168, 360, 504 ou 660. On peut alors établir qie $\mathfrak{A}_5 \cong \mathrm{PSL}_2(\mathbf{F}_4) \cong \mathrm{PSL}_2(\mathbf{F}_5)$ est le seul groupe simple d'ordre 60 (à isomorphisme près) et que $\mathfrak{A}_6 \cong \mathrm{PSL}_2(\mathbf{F}_9)$ est le seul sous-groupe

1. Par des techniques similaires, certes un chouïa plus compliquées, mais tout à fait dans le cadre de ce cours ! Je vous renvoie pour cela au DM de l'an dernier et aux TDs des années précédentes !

simple d'ordre 360 (à isomorphisme près). On peut par ailleurs montrer[2] que $\mathrm{PSL}_n(k)$ est simple pour tout $n \geqslant 2$ et k corps fini sauf pour $n = 2$ et $k = \mathbf{F}_2$ ou $\mathbf{F}_3$. Cela fournit un unique (à isomorphisme près) groupe simple d'ordre 168, à savoir $\mathrm{PSL}_2(\mathbf{F}_7) \cong \mathrm{PSL}_3(\mathbf{F}_2)$, un unique (à isomorphisme près) groupe simple d'ordre 504, à savoir $\mathrm{PSL}_2(\mathbf{F}_8)$ et un unique (à isomorphisme près) groupe simple d'ordre 660, à savoir $\mathrm{PSL}_2(\mathbf{F}_{11})$. Je rappelle que la classification (à isomorphisme près) des groupes finis simples est connue[3] et que les groupes simples se répartissent en quatre familles : les groupes abéliens d'ordre premier, les groupes alternés pour $n \geqslant 5$, les groupes de type Lie et les groupes sporadiques. On peut en réalité établir qu'à chaque fois, un groupe simple de cardinal n est unique à isomorphisme près (et alors on a ce que l'on appelle des isomorphismes exceptionnels entre deux groupes de deux familles différentes lorsque les cardinaux coïncident comme par exemple $\mathfrak{A}_5 \cong \mathrm{PSL}_2(\mathbf{F}_4) \cong \mathrm{PSL}_2(\mathbf{F}_5)$) sauf dans deux cas où on a deux classes d'isomorphismes : $\mathfrak{A}_8 \cong \mathrm{PSL}_4(\mathbf{F}_2) \ncong \mathrm{PSL}_3(\mathbf{F}_4)$ d'ordre[4] 20160 et les groupes $\mathrm{P}\Omega_{2n+1}(\mathbf{F}_q) \ncong \mathrm{PSp}_{2n}(\mathbf{F}_q)$ pour tout $n \geqslant 3$ et q puissance d'un nombre premier impair d'ordre[5]

$$q^{n^2} \prod_{i=1}^{n} \frac{q^{2i}-1}{2}.$$

Solution.

1. Cela résulte du fait plus général (sur un corps K quelconque) suivant : si un endomorphisme u de K^n commute avec tous les endomorphismes de déterminant 1, alors u est une homothétie. Il suffit pour cela de voir que tout vecteur $x \neq 0$ de K^n est vecteur propre pour u. Complétons x en une base $(x, e_1, \ldots, e_{n-1})$ de K^n ; soit M la matrice de u dans cette base, alors M commute avec la matrice de Jordan $J_n = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & (0) \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & (0) & & & 0 \end{pmatrix}$, ce qui implique qu'elle laisse stable le noyau de J_n, lequel est $K.x$. Ainsi x est bien vecteur propre pour u comme on voulait. Je vous renvoie au chapitre IV du Perrin pour plus de détails sur les groupes linéaires.

On a que le cardinal de $\mathrm{GL}_n(K)$ est

$$\#\mathrm{GL}_n(K) = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

En effet, on a $p^n - 1$ choix de première colonne non nulle, puis $p^n - p$ choix de seconde colonne non colinéaire à la première, etc... Comme par définition $\mathrm{SL}_n(K)$ est le noyau du morphisme de groupes surjectif $\det : \mathrm{GL}_n(K) \to K^\times$, son cardinal est celui de $\mathrm{GL}_n(K)$ divisé par $p-1$, soit

$$\#\mathrm{SL}_n(K) = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-2})p^{n-1}.$$

D'autre part, on a que $\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/Z(\mathrm{GL}_n(K))$ est ainsi le quotient de $\mathrm{GL}_n(K)$ par un groupe isomorphe à $K^\times$ (car le centre de $\mathrm{GL}_n(K)$ est constitué des matrices scalaires non nulles par la première question), donc $\#\mathrm{PGL}_n(K) = \#\mathrm{SL}_n(K)$. On obtient immédiatement par passage au quotient un morphisme injectif $\mathrm{PSL}_n(K) \to \mathrm{PGL}_n(K)$.

Enfin, le cardinal de $\mathrm{PSL_n}(K)$ dont on rappelle qu'il est défini par $\mathrm{PSL_n}(K) = \mathrm{SL}_n(K)/Z(\mathrm{SL}_n(K))$ et que $Z(\mathrm{SL}_n(K)) = Z(\mathrm{GL}_n(K)) \cap \mathrm{SL}_n(K) = \{\lambda I_n \ : \ \lambda^n = 1\}$. Or, il y a $\mathrm{pgcd}(n, p-1)$ racines n-ièmes de l'unité dans un corps K de cardinal p : en effet, on sait que $K^\times$ est un groupe cyclique d'ordre $p-1$, et on est donc ramené à compter le nombre de solutions x de $nx = 0$ dans $\mathbf{Z}/(p-1)\mathbf{Z}$, ce qui donne facilement le résultat puisque les solutions sont les éléments de $\mathbf{Z}/(p-1)\mathbf{Z}$ multiple de $\frac{p-1}{\mathrm{pgcd}(n,p-1)}$. Finalement,

$$\#\mathrm{PSL_n}(K) = \frac{(p^n - 1)(p^n - p)\cdots(p^n - p^{n-2})p^{n-1}}{\mathrm{pgcd}(n, p-1)}.$$

2. On fait opérer $\mathrm{PGL}_n(K)$ sur l'ensemble $\mathbf{P}(E)$ des droites vectorielles de E par $\bar{g}.D = g(D)$, où $g \in \mathrm{GL}_n(K)$ et $\bar{g}$ est son image dans $\mathrm{PGL}_n(K)$. Ceci est bien défini car si $\bar{g}_1 = \bar{g}_2$, alors g_1 et g_2 sont proportionnels donc $g_1(D) = g_2(D)$. L'opération est fidèle car les seuls $g \in \mathrm{GL}_n(K)$ qui stabilisent toutes les droites sont les homothéties. On obtient donc un morphisme injectif Φ de $\mathrm{PGL}_n(K)$ dans $\mathfrak{S}(\mathbf{P}(E))$.

3. item Les droites vectorielles de E sont données par une équation $x = ay$ dans le plan (avec $a \in K$) ou par l'équation $y = 0$. On obtient ainsi $q+1$ droites. On pouvait aussi raisonner en dénombrant le nombre de vecteurs non nuls de E, à savoir $p^2 - 1$ puis en remarquant qu'une droite (isomorphe à $\mathbf{F}_p$ contient $p-1$ tels vecteurs non nuls) si bien qu'on retrouve bien $\frac{p^2-1}{p-1} = p+1$ droites[6].

4. Les groupes $\mathrm{PGL}_2(\mathbf{F}_2)$ et $\mathrm{PSL}_2(\mathbf{F}_2)$ sont égaux et de cardinal 6 par **1.**, qui est aussi le cardinal de $\mathfrak{S}_3$. Ainsi, le morphisme injectif Φ est aussi surjectif, d'où le résultat.

2. Je vous renvoie par exemple au Perrin pour cela.
3. Mais difficile !
4. Vous pourrez en trouver une démonstration dans l'ouvrage *Histoires hédonistes des groupes* de Caldero et .
5. Voir ici pour des références.
6. Noter que ce raisonnement fournit que dans le cas général, on a $\frac{p^n-1}{p-1} = p^{n-1} + \cdots + 1$ droites dans $\mathbf{F}_p^n$.

5. Le cardinal de $\mathrm{PGL}_2(\mathbf{F}_3)$ est ici $(3^2-1).3 = 24$. Comme $\mathfrak{S}_4$ est aussi de cardinal 24, Φ est bien un isomorphisme. De plus $\mathrm{PSL}_2(\mathbf{F}_3)$ est un sous-groupe[7] d'indice 2 de $\mathrm{PGL}_2(\mathbf{F}_3)$, car $\mathrm{pgcd}(2, 3-1) = 2$. Comme le seul sous-groupe d'indice 2 de[8] $\mathfrak{S}_4$ est $\mathfrak{A}_4$, on en déduit que Φ induit un isomorphisme de $\mathrm{PSL}_2(\mathbf{F}_3)$ sur $\mathfrak{A}_4$.

Bien qu'ils aient même cardinal, les groupes $\mathrm{PGL}_2(\mathbf{F}_3)$ et $\mathrm{SL}_2(\mathbf{F}_3)$ ne sont pas isomorphes, par exemple parce que $\mathrm{SL}_2(\mathbf{F}_3)$ a un centre non trivial (de cardinal 2, égal à $\{\pm I_2\}$) alors que le centre de $\mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathfrak{S}_4$ est réduit au neutre. Noter du reste que la même preuve que pour calculer le centre de $\mathrm{GL}_n(K)$ et $\mathrm{SL}_n(K)$ (voir note de bas de page numéro 4) montre que les centres de $\mathrm{PGL}_n(K)$ et $\mathrm{PSL}_n(K)$ sont triviaux pour tout $n \geqslant 2$ (sur un corps quelconque).

6. Le cardinal de $\mathrm{PGL}_2(\mathbf{F}_5)$ est $(5^2-1).5 = 120$, ce qui montre que Φ induit un isomorphisme de $\mathrm{PGL}_2(\mathbf{F}_5)$ sur un sous-groupe d'indice 6 de $\mathfrak{S}_6$, lequel est isomorphe à $\mathfrak{S}_5$ (voir l'exercice 1 de la feuille I). Comme $\mathrm{pgcd}(2, 5-1) = 2$, on a encore que $\mathrm{PSL}_2(\mathbf{F}_5)$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbf{F}_5) \simeq \mathfrak{S}_5$, et il est donc isomorphe via Φ à $\mathfrak{A}_5$.

On peut montrer que l'image de $\mathrm{PGL}_2(\mathbf{F}_5)$ par Φ, bien qu'isomorphe à $\mathfrak{S}_5$ n'est pas conjugué des sous-groupes de $\mathfrak{S}_6$ donnés par le stabilisateur d'un élément de $\{1, \ldots, 6\}$. Ce phénomène (existence d'un sous-groupe d'indice m non conjugué des stabilisateurs d'un point) ne se produit dans $\mathfrak{S}_m$ que pour $m = 6$, et explique la présence dans $\mathfrak{S}_6$ d'un automorphisme qui n'est pas intérieur. Voir les TDs des années précédentes pour plus de détails.

7. On admettra dans un premier temps que $\mathrm{SL}_3(\mathbf{F}_2)$ est constitué de six classes de conjugaison : une de cardinal 1 consituée de I_3, une de cardinal 21 constituée d'éléments d'ordre 2, une de cardinal 56 constituée d'éléments d'ordre 3, deux de cardinal 24 constituée d'éléments d'ordre 7 et une de cardinal 42 constituée déléments d'ordre 4. Établir que $\mathrm{SL}_3(\mathbf{F}_2)$ est simple.

8. Dans toute cette question on supposera que G est un groupe non abélien.

(a) On fait agir (transitivement) G sur l'ensemble S_p des ses n_p p-Sylow. Par simplicité, $n_p > 1$ et on a alors un morphisme non trivial $G \to \mathfrak{S}(S_p) \cong \mathfrak{S}_{n_p}$. Par simplicité de G, ce morphisme est injectif et donc par Lagrange $\#G \mid n_p!$.

(b) Si $m = 1$, alors comme dans la preuve du cas pq, on note n_q le nombre de q-Sylow. Par les théorèmes de Sylow, $n_q \mid p$ et n_q est congru à 1 modulo q^n. Comme $p < q$, on a nécessairement $n_q = 1$ et l'unique q-Sylow est distingué et G n'est pas simple[9].
Soit maintenant $m = 2$. Supposons G simple. On sait que n_q est congru à 1 modulo q et divise p^2. Ainsi par simplicité et car $p < q$, $n_q = p^2$ et $q \mid p^2 - 1 = (p+1)(p-1)$ donc par primalité de q, $q \leqslant p+1$ et comme $p < q$, on a $p = q+1$ si bien que $p = 2$ et $q = 3$. Ainsi $\#G = 4 \times 3^n$. Par **1.**, $4 \times 3^n \mid 4!$ donc $3^n \mid 6$ et donc $n = 1$ et G est de cardinal 12. On a alors par les théorèmes de Sylow et simplicité que $n_2 = 3$ et donc $\#G \mid 3!$, ce qui est absurde. Un tel groupe ne peut donc pas être simple. Supposons un tel G simple. Si $q < p$, alors on applique **2.** en inversant les rôles de p et de q pour traiter le cas p^2q et si $p < q$, on applique directement **2.** et de même inverser les rôles de p et de q permet de traiter le cas p^3q avec $q < p$. Il suffit de traiter le cas p^3q avec $p < q$. On a toujours n_q congru à 1 modulo q et $n_q \mid p^3$. Comme $p < q$, $n_q \in \{p^2, p^3\}$. Comptons alors les éléments d'ordre q dans G. On en a exactement $n_q(q-1)$. Si alors $n_q = p^3$, G contient au moins $p^3(q-1) = \#G - p^3$ éléments d'ordre q. le complémentaire de ces éléments est donc d'ordre p^3 et donc un p-Sylow, ce qui assure son unicité (car il ne contient aucun élément d'ordre q). Ainsi $n_p = 1$ ce qui contredit la simplicité de G. On peut donc supposer que $n_q = p^2$. Dans ce cas, la condition n_q congru à 1 fournit que $p \mid p^2 - 1$ et donc que $q = p+1$ et $p = 2$, $q = 3$ si bien que $\#G = 24$. On a alors nécessairement, $n_2 = 3$ (par simplicité et les théorèmes de Sylow) et $\#G$ devrait diviser $3!$, ce qui est absurde à nouveau. On en déduit donc bien qu'un tel groupe est non simple. On peut classifier à isomorphisme près les groupes d'ordre p^2q à l'aide du produit semi-direct.

(c) Soit G non commutatif de cardinal < 60. On peut éliminer tous les cardinaux une puissance de p car le centre d'un p-groupe est non trivial et distinct de G tout entier lorsque G est non abélien. cela fournit la non simplicité. Par les questions précédentes, on peut aussi enlever tous les groupes d'ordre pq, pq^n ou p^2q^n avec $p < q$ ainsi que ceux de la forme p^3q ou p^2q. En énumérant les entiers < 60, on voit que cela laisse uniquement les groupes d'ordre 48. Soit donc G d'ordre $48 = 2^4 \times 3$ que l'on suppose simple. On a alors $n_2 = 3$ et la question **1.** garantit alors que $48 \mid 3! = 6$, ce qui est absurde. Un tel groupe est donc non simple.

(Bonus) (a) Une matrice de $\mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal $X+1$ est nécessairement I_3, qui forme une classe de conjugaison.

(b) Soit $A \in \mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal $X^2+1 = (X+1)^2$. On a alors que $\mathrm{Im}(A+I_3) \subseteq \mathrm{Ker}(A+I_3)$ de dimension respective (en utilisant par exemple les résultats bien connus sur les matrices nilpotentes ou en trigonalisant sur une clôture algébrique) 1 et 2 et une telle matrice est caractérisée par la donnée de la droite $\mathrm{Im}(A+I_3)$ et du plan $\mathrm{Ker}(A+I_3)$. En effet, par exemple, en se fixant $P = \mathrm{Ker}(A+I_3)$, la matrice A est de la forme

$$A = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

7. Le fait qu'on obtienne un sous-groupe se voit grâce la composition de l'inclusion naturelle $i : \mathrm{SL}_n(\mathbf{F}_p) \to \mathrm{GL}_n(\mathbf{F}_p)$ avec la surjection canonique $\pi : \mathrm{GL}_n(\mathbf{F}_p) \to \mathrm{PGL}_n(\mathbf{F}_p)$. Il est facile de montrer que $\pi \circ i$ passe au quotient modulo $Z(\mathrm{SL}_n(\mathbf{F}_p))$ pour fournir un morphisme injectif $\mathrm{PSL}_n(\mathbf{F}_p) \to \mathrm{PGL}_n(\mathbf{F}_p)$ et ainsi on peut réaliser $\mathrm{PSL}_n(\mathbf{F}_p)$ comme un sous-groupe de $\mathrm{PGL}_n(\mathbf{F}_p)$.

8. Cela découle soit du fait que l'on connaît tous les sous-groupes de $\mathfrak{S}_n$ pour $n \leqslant 4$ et les sous-groupes distingués de $\mathfrak{S}_n$ pour $n \geqslant 5$ ou plus simplement du fait qu'un sous-groupe d'indice 2 donne lieu au quotient à un morphisme surjectif (donc non trivial) de $\mathfrak{S}_n \to \{\pm 1\}$. Or, le seul morphisme non trivial de $\mathfrak{S}_n$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature. Cela se voit en montrant qu'une transposition est nécessairement envoyée sur -1 et en utilisant le fait que les transpositions engendrent $\mathfrak{S}_n$. Il existe au moins une transposition envoyée sur -1 sinon pusiqu'elles engendrent $\mathfrak{S}_n$, le morphisme est trivial mais alors puisque toutes les transpositions sont conjuguées et que $\{\pm 1\}$ est abélien, toutes les transpositions ont la même image, à savoir -1, ce qui permet de conclure.

9. Le résultat pq^n pour la résolubilité (en fait un groupe simple est résoluble si, et seulement si, il est commutatif) est dû à Frobenius, le cas p^2q^n à Jordan et le cas général p^mq^n à Burnside en utilisant la théorie des représentations.

avec a ou b non nul et alors il est clair que a et b sont fixés par $D = \mathrm{Im}(A + I_3)$ car

$$A + I_3 = \begin{pmatrix} 0 & 0 & a \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix}.$$

On a alors 7 choix de droites D puis 3 choix de plans P qui la contienne [10], soit 21 éléments d'ordre 2 qui forment une classe de conjugaison.

(c) Soit $A \in \mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal X^2+X+1. Alors nécessairement, le polynôme caractéristique est $X^3+1 = (X+1)(X^2+X+1)$ et 1 est valeur propre de A mais 1 n'est pas racine de X^2+X+1. On a donc une contradiction et X^2+X+1 ne peut pas apparaître comme polynôme minimal [11].

(d) Soit $A \in \mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal $X^3+1 = (X+1)(X^2+X+1)$. Cela se produit lorsque la droite $\mathrm{Ker}(A+I_3)$ et le plan $\mathrm{Ker}(A^2+A+I_3)$ sont supplémentaires dans $\mathbf{F}_2^3$. Une telle matrice est donc entièrement caractérisée par la donnée d'une droite et d'un plan supplémentaire ainsi que d'une matrice de $\mathrm{SL}_2(\mathbf{F}_2)$ de polynôme caractéristique X^2+X+1. On a 7 choix de droites puis 4 choix de plan (en effet, on a 6 choix d'un vecteur non nul non colinéaire au vecteur de la droite choisie et alors on peut choisir tout vecteur différent de la somme du vecteur directeur de la droite choisie et du vecteur choisi. Ce faisant, on obtient 12 plans mais chacun étant compté trois fois) puis on voit qu'une matrice $\mathrm{SL}_2(\mathbf{F}_2)$ de polynôme caractéristique X^2+X+1 est de la forme $\begin{pmatrix} a & 1 \\ 1 & 1-a \end{pmatrix}$ avec $a \in \mathbf{F}_2$ et on a ainsi 2 possibilités, soit finalement 56 telles matrices, toutes d'ordre 3.

(e) Soit $A \in \mathrm{SL}_3(\mathbf{F}_2)$. Le polynôme minimal de A est irréductible de degré 3 si, et seulement si [12], pour tout $x \in \mathbf{F}_2^3$ non nul, la famille (x, Ax, A^2x) est une base de $\mathbf{F}_2^3$. Pour x non nul, on a donc 6 choix pour Ax et 4 choix pour A^2x (A^3x étant fixé par le polynôme minimal), ce qui fournit 24 matrices dans chacun des cas, d'ordre 7 car $X^7+1 = (1+X)(X^3+X+1)(X^3+X^2+1)$. Noter que si A a pour polynôme minimal X^3+X+1 alors A^{-1} a pour polynôme minimal X^3+X^2+1 et inversement.

(f) Soit finalement $A \in \mathrm{SL}_3(\mathbf{F}_2)$ de polynôme minimal $X^3+X^2+X+1 = (X+1)^3$. Cela arrive si, et seulement si, $\mathrm{Ker}(A+I_3)$ est une droite contenue dans le plan $\mathrm{Ker}(A+I_3)^2$ et tout vecteur hors de ce plan a une image dans le plan mais pas dans la droite. Ainsi, une telle matrice est déterminée par le choix d'une droite contenue dans un plan et de l'image par $A+I_3$ d'un vecteur hors de ce plan dans le plan mais pas dans la droite. On a ainsi $7 \times 3 \times 2 = 42$ telles matrices d'ordre 4 car $X^4+1 = (X+1)^4$.

(g) On a donc bien obtenu 168 éléments répartis en 6 classes de conjugaison. Soit à présent $H \neq \{I_3\} \lhd \mathrm{SL}_3(\mathbf{F}_2)$. Supposons que H ne contienne ni élément d'ordre 3 ni élément d'ordre 7. Alors le cardinal de H divise $168/21 = 8$ donc H contient un élément d'ordre 2 donc les 21 éléments conjugués d'ordre 2 et H contient au moins 22 éléments, absurde. On sait donc que H contient un élément d'ordre 3 ou un élément d'ordre 7. Dans le premier cas, H contient 56 éléments d'ordre 7 donc $\#H \geqslant 57$ et $\#H \in \{84, 168\}$ donc H contient les 21 éléments d'ordre 2 et 24 éléments d'ordre 7 conjugués et $\#H \geqslant 57+24+21 = 102$ donc $\#H = 168$. Dans le second cas, H contient 24 éléments d'ordre 7 et en fait les 48 car les classes de conjugaison sont échangées par inversion donc $\#H \geqslant 49$ et $\#H \in \{56, 84, 168\}$ donc H a un élément d'ordre 7 et on conclut de nouveau que $\#H = 168$, ce qui conclut la preuve.

On pouvait plus simplement ici faire appel aux invariants de similitudes.

Problème 2 — Artin vs Nœther. Fight!. Soit A un anneau commutatif. On dit que A satisfait la propriété $(*)$ si toute suite décroissante d'idéaux de A est stationnaire, *i.e.* pour toute suite $(I_n)_{i \in \mathbf{N}}$ telle que $I_{n+1} \subseteq I_n$ pour tout $n \geqslant 0$, il existe $n_0 \in \mathbf{N}$ tel que $I_n = I_{n_0}$ pour tout $n \geqslant n_0$. On définit également le *spectre* d'un anneau A comme étant l'ensemble de ses idéaux premiers et on le notera $\mathrm{Spec}(A)$. L'objectif de ce problème est d'étudier quelques propriétés de cette classe d'anneaux.

1. Préciser parmi les anneaux suivants lesquels satisfont la propriété $(*)$ et lesquels sont nœthériens :

$$A \text{ fini}, \quad \mathbf{Z}, \quad k[X]/(X^n) \text{ pour } k \text{ corps et } n \in \mathbf{N}.$$

2. Montrer qu'un anneau qui satisfait la propriété $(*)$ et intègre est un corps et que, plus généralement, tout idéal premier d'un anneau de satisfaisant la propriété $(*)$ est maximal.
On pourra considérer des idéaux de la forme (a^n) pour $a \in A$ et $n \in \mathbf{N}$.

3. Soient deux idéaux I et J d'un anneau A. Rappeler pourquoi $\{ij \ : \ (i,j) \in I \times J\}$ n'est pas en général un idéal. On définit donc l'idéal IJ comme l'idéal *engendré* par les ij pour $i \in I$ et $j \in J$. Justifier que $IJ \subseteq I \cap J$ et donner un exemple où l'inclusion est stricte.

4. Montrer que $\mathrm{Spec}(A)$ est fini si A satisfait la propriété $(*)$.
On pourra considérer une suite d'idéaux de la forme $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_r$ pour $\mathfrak{m}_i$ des idéaux maximaux.

5. On définit le *nilradical* de A comme étant $\mathcal{N}(A) = \{x \in A \ : \ \exists n \in \mathbf{N}, \text{ tel que } x^n = 0\}$.

10. Bien remarquer que tout plan de $\mathbf{F}_2^3$ contient 3 des 7 droites de $\mathbf{F}_2^3$ et est de cardinal 4.

11. On aurait aussi pu voir qu'on obtenait 168 éléments avec les autres polynômes minimaux.

12. Polynôme minimal pas irréductible implique par le lemme des noyaux le fait qu'il existe un x qui ne vérifie pas l'hypothèse. Pour la réciproque, on voit que l'espace engendré par la famille (x, Ax, A^2x) est stable par A et si son supplémentaire est non réduit à 0, alors la matrice A dans une base de cet espace et de son supplémentaire est diagonale par blocs ce qui contredit l'irréductiblité du polynôme caractéristique.

a) Justifier que $\mathcal{N}(A)$ est un idéal de A.

b) On note J l'intersection de tous les idéaux premiers de A. Montrer que $\mathcal{N}(A) \subseteq J$.

c) Réciproquement, soit $a \in A \setminus \mathcal{N}(A)$ et $\mathcal{E}$ la collection de tous les idéaux ne contenant aucune puissance de a. Établir que $\mathcal{E}$ possède un élément maximal qui est un idéal premier de A et en déduire que $\mathcal{N}(A) = J$.
On pensera au lemme de Zorn.

d) On suppose dans la suite de cette question **5.** que l'anneau A satisfait la propriété $(*)$. On suppose par ailleurs disposer d'un entier n tel que pour tout $k \geqslant n$, $\mathcal{N}(A)^n = \mathcal{N}(A)^k$. On pose alors $\mathfrak{a} = \mathcal{N}(A)^n$ et on suppose que $\mathfrak{a} \neq (0)$. Soit alors $\mathcal{B}$ la collection des idéaux $\mathfrak{b}$ tels que $\mathfrak{ab} \neq (0)$. Justifier qu'il existe un idéal $\mathfrak{c}$ qui soit un élément minimal de $\mathcal{B}$.

e) Montrer que $\mathfrak{c}$ est principal. On notera c un générateur.

f) Montrer que $\mathfrak{ca} = \mathfrak{c}$.

g) En déduire que si A satisfait la propriété $(*)$, alors il existe $n_0 \in \mathbf{N}$ tel que $\mathcal{N}(A)^{n_0} = (0)$ et des idéaux maximaux $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ (non nécessairement distincts) de A tels que $\mathfrak{m}_1 \cdots \mathfrak{m}_r = (0)$.

6. Soit A un anneau nœthérien.

a) Soit I un idéal de A. Montrer qu'il existe des idéaux premiers $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ contenant I tels que $\mathfrak{P}_1 \cdots \mathfrak{P}_n \subseteq I$.
On pourra raisonner par l'absurde et considérer la collection des idéaux contenant I et ne contenant aucun produit fini d'idéaux premiers contenant I et montrer qu'elle admet un élément maximal $\mathfrak{m}$ qui n'est pas premier. Conclure alors en considérant pour $ab \in \mathfrak{m}$ avec $a, b \notin \mathfrak{m}$ les idéaux $\mathfrak{m} + aA$ et $\mathfrak{m} + bA$.

b) En déduire qu'un anneau noethérien dont tout idéal premier est maximal admet un nombre fini d'idéaux maximaux.
On pourra commencer par établir que si $IJ \subseteq \mathfrak{Q}$ avec $\mathfrak{Q}$ un idéal premier de A et I, J deux idéaux quelconques de A, alors $I \subseteq \mathfrak{Q}$ ou $J \subseteq \mathfrak{Q}$.

7. Montrer que si A est nœthérien, alors il existe un entier n_0 tel que $\mathcal{N}(A)^{n_0} = (0)$.

(Bonus) On cherche dans cette question à comprendre le lien entre anneau satisfaisant la propriété $(*)$ et anneau nœthérien.

a) Soit I un idéal d'un anneau A et J un idéal de A contenu dans I. On dispose alors de la suite exacte courte de groupes abéliens $0 \to J \xrightarrow{i} I \xrightarrow{p} I/J \to 0$. Montrer que toute suite décroissante (*resp.* croissante) d'idéaux de A contenus dans J est stationnaire et que toute suite décroissante (*resp.* croissante) d'idéaux de A/J contenus dans I/J est stationnaire, si, et seulement s'il en est de même pour toute suite décroissante (*resp.* croissante) d'idéaux de A contenus dans I.
On pourra, à partir d'une suite d'idéaux $(I_n)_{n\in\mathbf{N}}$ inclus dans I, considérer les suites $(p(I_n))_{n\in\mathbf{N}}$ et $(i^{-1}(I_n))_{n\in\mathbf{N}}$ et établir que si $p(I_n) = p(I_m)$ et $i^{-1}(I_n) = i^{-1}(I_m)$, alors $I_n = I_m$.

b) Soit k un corps et E un k-espace vectoriel. Montrer que toute suite croissante de sous-espaces vectoriels est stationnaire si, et seulement si, toute suite décroissante de sous-espaces vectoriels est stationnaire si, et seulement si, E est de dimension finie.

c) On suppose que l'on dispose d'idéaux maximaux $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ d'idéaux maximaux de A tels que $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_r = (0)$. Montrer alors que A est nœthérien si, et seulement s'il satisfait la propriété $(*)$.
On pourra raisonner par récurrence descendante sur k et montrer que $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_k$ vérifie que toute suite décroissante d'idéaux contenu dans $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_k$ est stationnaire. On considérera alors la suite exacte

$$0 \to \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_k \to \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_{k-1} \to \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_{k-1}/\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_k \to 0$$

et on remarquera que $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_{k-1}/\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_k$ est un $A/\mathfrak{m}_k$-espace vectoriel.

d) Montrer que tout anneau satisfaisant la propriété $(*)$ est nœthérien. Réciproquement, montrer qu'un anneau nœthérien dans lequel tout idéal premier est maximal satisfait la propriété $(*)$.

Solution. Un tel anneau est en réalité un *anneau artinien*. Ces anneaux jouent un rôle important en géométrie algébrique et plus particulièrement en théorie de la déformation.

1. (sur 1,5 points) Soit A un anneau fini. Le résultat est alors clair car on a un nombre fini d'idéaux donc A est noethérien et artinien.
Il est clair que dans $\mathbf{Z}$, on dispose de la suite strictement décroissante d'idéaux

$$\mathbf{Z} \supseteq p\mathbf{Z} \supseteq p^2\mathbf{Z} \supseteq p^3\mathbf{Z} \supseteq \cdots$$

pour p premier. Ainsi $\mathbf{Z}$ n'est pas artinien mais $\mathbf{Z}$ étant principal, il est noethérien.
Enfin, $k[X]/(X^n)$ est un quotient de $k[X]$ avec $k[X]$ noethérien donc $k[X]$ est noethérien[13]. Enfin, notons que $k[X]/(X^n)$ est un k-espace vectoriel de dimension finie[14] et qu'un idéal de $k[X]/(X^n)$ est en particulier un sous-espace vectoriel. À toute suite décroissante d'idéaux $(I_n)_{n\in\mathbf{N}}$, correspond donc une suite strictement décroissante d'entiers

$$\dim(I_0) \geqslant \dim(I_1) \geqslant \dim(I_2) \geqslant \cdots \geqslant 0$$

13. On rappelle que tout quotient d'un anneau noethérien l'est et que si A est noethérien, $A[X]$ l'est par le théorème de transfert de Hilbert. En revanche, le résultat ne vaut pas pour un sous-anneau.

14. De base $\left(1, \overline{X}, \dots, \overline{X}^{n-1}\right)$ où $\overline{X}$ désigne la classe de X dans $k[X]/(X^n)$, donc de dimension n. On montre en effet facilement qu'il s'agit d'une famille libre et génératrice.

qui est nécessairement stationnaire. Comme on a une inclusion entre deux idéaux, consécutifs, cela implique immédiatement que $(I_n)_{n\in\mathbf{N}}$ est stationnaire et que $k[X]/(X^n)$ est artinien [15]. On pouvait aussi dire que les idéaux de $k[X]/(X^n)$ sont en correspondance avec les idéaux de $k[X]$ contenant (X^n). Comme $k[X]$ est principal, ces idéaux sont de la forme (P) avec $P \mid X^n$ et on voit qu'on a donc un nombre fini d'idéaux de la forme $\pi((X^k))$ pour $0 \leqslant k \leqslant n-1$.

2. **(sur 1,5 points)** Soient A un anneau artinien intègre et $a \in A \setminus \{0\}$. On considère alors la suite décroissante d'idéaux

$$A \supseteq aA \supseteq a^2A \supseteq a^3A \supseteq \cdots$$

Puisque A est artinien, il existe un entier n_0 tel que pour tout $n \geqslant n_0$, $a^{n_0}A = a^nA$. En particulier, $a^{n_0} \in a^{n_0+1}A$ et il existe $b \in A$ tel que $a^{n_0} = a^{n_0+1}b$ ce qui équivaut à $a^{n_0}(1-ab) = 0$. Par intégrité et puisque $a \neq 0$, il vient $1 = ab$ et a est inversible. On en déduit que A est un corps.

Soit à présent A un anneau artinien et $\mathfrak{P}$ un idéal premier. En particulier, $A/\mathfrak{P}$ est intègre. On constate [16] que tout quotient d'un anneau artinien est artinien et donc $A/\mathfrak{P}$ est un anneau artinien intègre, donc un corps d'après ce qui précède [17].

3. **(sur 1 point)** On n'a en général pas stabilité par somme dans l'ensemble [18] $\{ij \ : \ (i,j) \in I \times J\}$. Il est alors clair que tout élément de IJ s'écrit comme une somme finie de termes de la forme ij avec $i \in I$ et $j \in J$. Puisque I et J sont des idéaux, il est clair que $ij \in I \cap J$ et on a clairement le résultat. Dans $\mathbf{Z}$, on vérifie que si $I = n\mathbf{Z}$ et $J = m\mathbf{Z}$, alors $IJ = nm\mathbf{Z}$ et $I \cap J = \mathrm{ppcm}(n,m)\mathbf{Z}$. On obtient en particulier égalité si n et m sont premiers entre eux et une inclusion stricte sinon.

4. **(sur 1,5 points)** Raisonnons par l'absurde en supposant qu'il existe une infinité d'idéaux premiers (et donc maximaux par **2.**) $(\mathfrak{m}_n)_{n\in\mathbf{N}^*}$. Établissons alors que pour tout $r \in \mathbf{N}^*$, $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{r+1} \subset \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_r$ strictement. L'inclusion est claire et supposons par l'absurde que l'on ait égalité. Comme les $\mathfrak{m}_i$ sont maximaux et distincts, il existe pour tout $i \in \{1,\dots,r\}$, $m_i \in \mathfrak{m}_i \setminus \mathfrak{m}_{r+1}$. On a donc $m_1m_2\cdots m_r \in \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_r = \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_r\mathfrak{m}_{r+1} \subseteq \mathfrak{m}_{r+1}$. Un idéal maximal étant en particulier premier, cela impliquerait qu'il existe un $i_0 \in \{1,\dots,r\}$ tel que $m_{i_0} \in \mathfrak{m}_{r+1}$, ce qui est une contradiction. On a donc une suite infinie strictement décroissante d'idéaux, ce qui contredit le fait que A soit artinien. En conclusion, le spectre de A est bien fini.

5. a) **(sur 1 point)** Soient $x, y \in \mathcal{N}(A)$. On a alors n et m entiers naturels non nuls tels que $x^n = y^m = 0$. On a alors puisque l'anneau est commutatif

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

Si alors $k \geqslant n$, $x^k = 0$ donc $x^k y^{n+m-k} = 0$ et si $k < n$ alors $n+m-k > m$ donc $y^{n+m-k} = 0$ et $x^k y^{n+m-k} = 0$. On a donc par stabilité par somme que $(x+y)^{n+m} = 0$ et $x+y \in \mathcal{N}(A)$. Pour x dans $\mathcal{N}(A)$ tel que $x^n = 0$ et $a \in A$, on a alors par commutativité que $(ax)^n = a^n x^n = 0$ si bien que $ax \in \mathcal{N}(A)$, qui est donc bien un idéal.

b) **(sur 0,5 point)** Si $a \in \mathcal{N}(A)$ et un entier n tel que $a^n = 0$. On a donc $a^n \in \mathfrak{P}$ pour tout idéal premier $\mathfrak{P}$ de A. Cela implique immédiatement que $a \in \mathfrak{P}$ et donc que $a \in J$.

c) **(sur 2 points)** Soit $a \in J \setminus \mathcal{N}(A)$. Notons $\mathcal{E}$ l'ensemble des idéaux de A ne contenant aucune puissance de a. Cet ensemble est non vide car contenant [19] (0) et ordonné par l'inclusion. Il est par ailleurs inductif car pour une famille (I_i) totalement ordonnée de $\mathcal{E}$, alors $\bigcup I_i$ est un majorant [20] dans $\mathcal{E}$. Par le lemme de Zorn, on en déduit l'existence un élément maximal $\mathfrak{P}$ dont on va montrer qu'il est premier. Soient x et y non dans $\mathfrak{P}$ et montrons que xy n'est pas dans $\mathfrak{P}$. On a que $\mathfrak{P} + Ax$ est un idéal contenant $\mathfrak{P}$ strictement et par maximalité de $\mathfrak{P}$, il ne peut pas être dans $\mathcal{E}$ si bien qu'il contient une puissance de a. On a donc qu'il existe un entier naturel k non nul ainsi que $p \in \mathfrak{P}$ et $b \in A$ tels que $a^k = p + bx$ et de même qu'il existe un entier naturel ℓ non nul ainsi que $q \in \mathfrak{P}$ et $c \in A$ tels que $a^\ell = q + cy$. Ainsi $a^{k+\ell} = (p+bx)(q+cy) = pq + (bx)q + (cy)p + (bc)(xy)$ n'est pas dans $\mathfrak{P}$ par définition de $\mathfrak{P}$ donc $(bc)(xy)$ n'est pas dans $\mathfrak{P}$ et $xy \notin \mathfrak{P}$. On en déduit donc bien que $\mathfrak{P}$ est un idéal premier mais par définition de $\mathfrak{P}$, $a \notin \mathfrak{P}$ si bien que $a \notin J$. On a donc $J \subseteq \mathcal{N}(A)$ et finalement en combinant avec la question précédente que $\mathcal{N}(A) = J$.

Remarque : Vous trouverez en question 3 de l'exercice 8 du TD 3 sur les anneaux une démonstration différente utilisant une partie multiplicative S et le localisé $S^{-1}A$ qui semble ne pas recourir au lemme de Zorn. Mais une lecture attentive montre qu'on utilise le fait que tout idéal propre est contenu dans un idéal maximal, fait dont la démonstration repose justement sur le lemme de Zorn ! Vous trouverez également dans le DM 1 de l'an dernier, une généralisation du nilradical, à savoir le radical d'un idéal I de A (le nilradical correspondant au cas $I = (0)$).

15. De manière générale, si A est un anneau noethérien, $\mathfrak{m}$ un idéal maximal et $n \in \mathbf{N}^*$, alors $A/\mathfrak{m}^n$ est artinien.
16. De manière identique au cas noethérien en utilisant la correspondance entre idéaux de $A/\mathfrak{P}$ et idéaux de A contenant $\mathfrak{P}$.
17. On pouvait bien sûr redémontrer cela à la main !
18. Par exemple dans $k[X,Y]$ avec k un corps, $I = (X,Y)$ et $J = (X^2,Y)$, on a que

$$X \times X^2 + Y \times Y = X^3 + Y^2$$

n'est pas de la forme $(PX+QY)(RX^2+SY)$ car X^3+Y^2 est irréductible (par exemple car il l'est sur $k(X)[Y]$ sur lequel il est de degré 2 sans racine).
19. En effet, si (0) contient une puissance de a, alors on a $a \in \mathcal{N}(A)$.
20. Il s'agit d'un idéal car l'ensemble est totalement ordonné. Par exemple, si $x, y \in \bigcup I_i$, il existe i_x et i_y tels que $x \in I_{i_x}$ et $y \in I_{i_y}$. Comme la famille des (I_i) est totalement ordonnée, on a soit $I_{i_x} \subseteq I_{i_y}$ soit $I_{i_y} \subseteq I_{i_x}$. Supposons sans perte de généralité que $I_{i_x} \subseteq I_{i_y}$, alors $x, y \in I_{i_y}$ et $x+y \in I_{i_y}$ qui est un idéal et finalement $x+y \in \bigcup I_i$. Je rappelle que sinon, en général, une union d'idéaux n'est pas un idéal !

d) **(sur 0,5 point)** On obtient de manière identique au cas noethérien [21] que dans un anneau artinien toute collection non vide d'idéaux de A admet un élément minimal pour l'inclusion. On peut donc considérer $\mathfrak{c}$ un élément minimal pour $\mathcal{B}$ car $\mathcal{B}$ est non vide puisque $\mathfrak{a} \in \mathcal{B}$ car $\mathfrak{a}^2 = \mathfrak{a} \neq (0)$.

e) **(sur 0,5 point)** On obtient du fait que $\mathfrak{ac} \neq (0)$ l'existence d'un $c \in \mathfrak{c}$ tel que $c\mathfrak{a} \neq 0$ et donc $cA \in \mathcal{B}$ et $cA \subseteq \mathfrak{c}$. La minimalité de $\mathfrak{c}$ garantit par conséquent que $\mathfrak{c} = cA$ est principal.

f) **(sur 1 point)** On a

$$(\mathfrak{ca})\mathfrak{a} = \mathfrak{ca}^2 = \mathfrak{ca}$$

car $\mathfrak{a}^2 = \mathcal{N}(A)^{2n} = \mathcal{N}(A)^n = \mathfrak{a}$. Ainsi, on a $(\mathfrak{ca})\mathfrak{a} \neq (0)$ et $\mathfrak{ca} \in \mathcal{B}$. Comme $\mathfrak{ca} \subseteq \mathfrak{c}$, par minimalité, il vient $\mathfrak{ca} = \mathfrak{c}$.

g) **(sur 1,5 points)** On déduit de la question précédente qu'il existe $g \in \mathfrak{a}$ tel que $c = cg$. On a donc $cg^2 = (cg)g = cg = c$ et de proche en proche pour tout entier ℓ, $cg^\ell = c$. Mais par définition, $g \in \mathfrak{a} \subseteq \mathcal{N}(A)$ et donc il existe n_0 tel que $g^{n_0} = 0$, ce qui entraîne que $c = 0$ et donc $\mathfrak{c} = (0)$, ce qui est une contradiction car on a $\mathfrak{ac} \neq (0)$. On en déduit donc que $\mathfrak{a} = 0$, ce qui établit que $\mathcal{N}(A)^n = (0)$. On a alors que si A est artinien, on a par définition un entier n tel que pour tout $k \geqslant n$, $\mathcal{N}(A)^n = \mathcal{N}(A)^k$ et on obtient donc qu'il existe un entier n_0 tel que $\mathcal{N}(A)^{n_0} = (0)$. On a alors que A possède un nombre fini d'idéaux maximaux $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ et on a alors clairement que

$$\mathfrak{m}_1 \cdots \mathfrak{m}_s \subseteq \bigcap_{i=1}^{s} \mathfrak{m}_i = \mathcal{N}(A)$$

et finalement $(\mathfrak{m}_1 \cdots \mathfrak{m}_s)^n = (0)$, ce qui fournit la conclusion désirée avec n copies de chaque idéal maximal de A.

6. a) **(sur 1,5 points)** On raisonne par l'absurde et on suppose que I ne contient aucun produit d'un nombre fini d'idéaux premiers contenant I. On considère alors la collection C d'idéaux contenant I et satisfaisant cette propriété (qui donc par hypothèse est non vide car contenant I). Une telle collection possède un élément maximal car A est noethérien, que l'on notera $\mathfrak{m}$. On a que $\mathfrak{m}$ n'est pas premier (car sinon il contient un produit d'un idéal premier, à savoir lui-même) et $\mathfrak{m} \neq A$ car sinon tout idéal propre de A contenant I ne contient de produit fini d'idéaux premiers contenant I mais on sait par le théorème de Krull, que I est contenu dans un idéal maximal. Comme $\mathfrak{m}$ n'est pas premier, on dispose de $a, b \in A$ tels que $ab \in \mathfrak{m}$ et $a, b \notin \mathfrak{m}$. Les idéaux $I_a = \mathfrak{m} + aA$ et $I_b = \mathfrak{m} + bA$ vérifient $I_a I_b \subseteq \mathfrak{m}$ avec $\mathfrak{m}$ strictement inclus dans I_a et dans I_b. Par maximalité de $\mathfrak{m}$, I_a et I_b contiennent tous les deux un produit fini d'idéaux premiers et donc $I_a I_b$ aussi. Ainsi $\mathfrak{m}$ aussi, ce qui est une contradiction. On a donc le résultat.

b) **(sur 1,5 points)** On applique ce qui précède à l'idéal (0) et on obtient l'existence d'un nombre fini d'idéaux premiers (donc maximaux) $\mathfrak{P}_1 \cdots \mathfrak{P}_n = (0)$. Soit à présent un idéal maximal $\mathfrak{m}$ de A. On a donc

$$\mathfrak{P}_1 \cdots \mathfrak{P}_n = (0) \subseteq \mathfrak{m}.$$

Cela implique qu'il existe $i_0 \in \{1, \ldots, n\}$ tel que $\mathfrak{P}_i \subseteq \mathfrak{m}$. En effet, sinon il existe pour tout $i \in \{1, \ldots, n\}$, $x_i \in \mathfrak{P}_i \setminus \mathfrak{m}$. On aurait alors $x_1 \cdots x_n \in \mathfrak{P}_1 \cdots \mathfrak{P}_n \subseteq \mathfrak{m}$ avec aucun des x_i dans $\mathfrak{m}$, ce qui est absurde car $\mathfrak{m}$ est en particulier premier. On a donc qu'il existe $i_0 \in \{1, \ldots, n\}$ tel que $\mathfrak{P}_i \subseteq \mathfrak{m}$ et comme $\mathfrak{P}_i$ est premier (donc maximal), on en déduit que $\mathfrak{m} = \mathfrak{P}_i$, ce qui établit le résultat souhaité.

7. **(sur 1 point)** On utilise le fait que puisque A est noethérien, $\mathcal{N}(A) = \langle a_1, \ldots, a_r \rangle$ est de type fini. Il existe donc n_i tel que $a_i^{n_i} = 0$ et on vérifie aisément que $\mathcal{N}(A)^{n_1+\cdots+n_r} = (0)$ car on vérifie que tout élément de $\mathcal{N}(A)^{n_1+\cdots+n_r}$ s'écrit comme un polynôme à coefficients dans A homogène en les a_i de degré $n_1 + \cdots + n_r$. On a ainsi des combinaisons linéaires de monômes

$$a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r} \quad \text{avec} \quad k_1 + \cdots + k_r = n_1 + \cdots + n_r.$$

On a donc nécessairement un $k_i \geqslant n_i$ et donc $a_i^{k_i} = 0$ et

$$a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r} = 0.$$

On pouvait aussi raisonner en disant que

$$\mathcal{N}(A) = \bigcap_{\mathfrak{m} \in \mathrm{Spec}(A)} \mathfrak{m}.$$

On a alors un nombre fini d'idéaux maximaux $\mathfrak{m}_1, \cdots, \mathfrak{m}_s$ tels que

$$\mathfrak{m}_1 \cdots \mathfrak{m}_s = (0).$$

On a donc puisque pour tout i, $\mathcal{N}(A) \subseteq \mathfrak{m}_i$ que

$$\mathcal{N}(A)^s \subseteq \mathfrak{m}_1 \cdots \mathfrak{m}_s = (0)$$

soit $\mathcal{N}(A)^s = (0)$.

21. Qui est dans le cours.

(Bonus sur 4 points)

a) On prouve que le caractère artinien passe au quotient et de la même façon que dans le cas noethérien et le cas d'un idéal est clair si bien que seule la réciproque nécessite quelques détails. On suppose donc que l'on dispose d'une suite exacte $0 \longrightarrow J \xrightarrow{i} I \xrightarrow{p} I/J \longrightarrow 0$ où I/J est l'idéal de A/J correspondant à I via la correspondance entre idéaux de A/J et idéaux A contenant J. On suppose[22] que toute suite décroissante d'idéaux de I/J et de I est stationnaire et on considère une suite décroissante d'idéaux $(I_n)_{n\in\mathbf{N}}$ de I. La suite $(p(I_n))_{n\in\mathbf{N}}$ est alors une suite d'idéaux de A/I contenu dans J/I. On en déduit qu'il existe $n_0 \in \mathbf{N}$ tel que pour tout $k \geqslant n_0$, $p(I_k) = p(I_{n_0})$. De même, on considère $(i^{-1}(I_n) = J \cap I_n)_{n\in\mathbf{N}}$ qui est une suite décroissante d'idéaux de A contenu dans J et il existe $n_1 \in \mathbf{N}$ tel que pour tout $k \geqslant n_1$, $i^{-1}(I_k) = i^{-1}(I_{n_1})$. On considère alors $N = \max(n_0, n_1)$ et pour tout $k \geqslant N$, $p(I_k) = p(I_N)$ et $i^{-1}(I_k) = i^{-1}(I_N)$. Montrons alors que cela implique que $I_k = I_N$, ce qui fournira le résultat souhaité. Par décroissance, on a $I_N \subseteq I_k$ et soit $x \in I_k$. On a alors $p(x) \in p(I_k) = p(I_N)$ de sorte qu'il existe $y \in I_N$ tel que $x - y \in \mathrm{Ker}(p) = \mathrm{Im}(i)$. Ainsi, $x - y \in i(J)$ et $x - y \in I_k$. Ainsi, $x - y = i(j)$ pour $j \in J$ et $j \in i^{-1}(I_k) = i^{-1}(I_N)$. D'où, $i(j) \in I_N$ et comme $y \in I_N$, on a bien $x \in I_N$ et $I_k = I_N$.

b) Il est clair que si E est de dimension finie, alors toute suite décroissante de sous-espaces vectoriels stationne en utilisant le même argument qu'en question **1.** Réciproquement, raisonnons par contraposition et supposons que E est de dimension infinie et choisissons[23] $(e_i)_{i\in I}$ une base de E dont on peut extraire une suite $e_{i_1}, e_{i_2}, \ldots$ d'éléments deux à deux distincts. Posant W_n le sous-espace vectoriel engendré par les e_{i_m} pour tout $m \geqslant n$, on obtient une suite strictement décroissante de sous-espaces vectoriels $W_1 \supseteq W_2 \supseteq \cdots$. On a alors l'équivalence E de dimension finie si, et seulement si, toute suite décroissante de sous-espaces vectoriels est stationnaire. On peut établir de la même façon le cas croissant[24].

c) On utilise la suite exacte $0 \longrightarrow \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k \longrightarrow \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1} \longrightarrow \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1}/\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k \longrightarrow 0$ pour $k \in \{0, \ldots, n\}$ et on raisonne par récurrence descendante pour établir que $\prod_{i=0}^{k} \mathfrak{m}_i$ avec $\mathfrak{m}_0 = A$ vérifie que toute suite d'idéaux décroissantes contenus dans $\prod_{i=0}^{k} \mathfrak{m}_i$ est stationnaire si, et seulement si, toute suite croissante l'est. Le cas $k = 0$ fournira le résultat. L'initialisation $k = n$ est claire puisqu'on obtient l'idéal nul. Supposons à présent le résultat valable pour k. Ainsi toute suite décroissante d'idéaux de A contenus dans $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k$ est stationnaire si, et seulement si, toute suite croissante l'est. Par ailleurs, on constate que $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1}/\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k$ est un $A/\mathfrak{m}_k$-espace vectoriel[25]. En effet, on a un idéal de $A/\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k$ donc la stabilité par somme et soit $\overline{a}$ la classe de a dans $A/\mathfrak{m}_k$. On pose alors, pour $\pi(x)$ et $\pi : \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1} \longrightarrow \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1}/\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k$, $\overline{a}\pi(x) = \pi(ax)$. Cette définition fait bien de $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1}/\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k$ un espace vectoriel et ne dépend pas du choix du représentant car si $a - b \in \mathfrak{m}_k$, alors $ax - bx \in \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k$. On a de plus que tout idéal admet une structure de sous-espace vectoriel. On déduit des questions précédentes que toute suite décroissante d'idéaux de $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1}/\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k$ est stationnaire si, et seulement si, toute suite croissante l'est[26]. Par a), on en déduit que c'est le cas pour $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1}$, ce qui permet d'achever notre récurrence descendante et d'en déduire le résultat.

d) Il suffit de voir que si A est artinien, la question **5.** g) garantit qu'on est en mesure d'appliquer la question d). Ainsi un anneau artinien est noethérien. Réciproquement, soit A est noethérien dans lequel tout idéal premier est maximal. Il suffit pour conclure de trouver un nombre fini d'idéaux premiers dont le produit est nul. Une fois que l'on sait[27] qu'on a un nombre fini d'idéaux maximaux et que $\mathcal{N}(A)$ est nilpotent, on peut donc à nouveau appliquer c) et en déduire que A est artinien. On a donc bien l'équivalence souhaitée.

► **Compléments.–** On commence par montrer que $f_{\mathfrak{m}} : A \longrightarrow A_{\mathfrak{m}}$ est un morphisme surjectif de noyau $\mathfrak{m}^k$, ce qui établira la première partie de la question via le théorème d'isomorphisme. Commençons par remarquer que la correspondance entre idéaux de A et ceux de $A/\mathfrak{m}^k$ fournit qu'un idéal de $A/\mathfrak{m}^k$ correspond à un idéal I de A tel que $\mathfrak{m}^k \subseteq I$ et ainsi un idéal maximal de $A/\mathfrak{m}^k$ correspond à un idéal de A maximal contenant $\mathfrak{m}^k$. On voit qu'il s'agit nécessairement de $\mathfrak{m}$ car sinon pour tout $m \in \mathfrak{m}$, $m^k \in \mathfrak{m}'$ pour $\mathfrak{m}'$ un autre idéal maximal et comme un tel idéal est en particulier premier, $m \in \mathfrak{m}'$ et $\mathfrak{m} \subseteq \mathfrak{m}'$ et $\mathfrak{m} = \mathfrak{m}'$ par maximalité. On en déduit que $A/\mathfrak{m}^k$ possède un unique idéal maximal $\mathfrak{m}/\mathfrak{m}^k$. Il s'agit donc d'un anneau local et on a vu en TD 4 exercice 3 que cela implique que les inversibles de $A/\mathfrak{m}^k$ sont précisément les éléments en dehors de $\mathfrak{m}/\mathfrak{m}^k$. Soit alors $a \in \mathrm{Ker}(f_{\mathfrak{m}})$. On a donc $\frac{a}{1} = \frac{0}{1}$ et par définition $s \notin \mathfrak{m}$ tel que $sa = 0$. On a donc en particulier $\overline{sa}$ dans le quotient $A/\mathfrak{m}^k$ et $\overline{s}$ est inversible donc $\overline{a} = 0$ et $a \in \mathfrak{m}^k$. Réciproquement, si $b \in \mathfrak{m}^k$, alors il existe $s \notin \mathfrak{m}$ tel que $sb = 0$. En effet, on peut choisir $b_i \in \mathfrak{n}_i \setminus \mathfrak{m}$ pour tout idéal maximal $\mathfrak{n}_1, \ldots, \mathfrak{n}_r$ distinct de $\mathfrak{m}$. Alors $s = b_1^k \cdots b_r^k$ convient car $s \notin \mathfrak{m}$ par propriété des idéaux premiers et $sb \in (\mathfrak{n}_1 \cdots \mathfrak{n}_r\mathfrak{m})^k = (0)$. On a donc bien que $\mathrm{Ker}(f_{\mathfrak{m}}) = \mathfrak{m}$. Reste à obtenir la surjectivité. Soit $\frac{a}{s}$ avec $a \in A$ et $s \notin \mathfrak{m}$ et on cherche $x \in A$ tel que $\frac{x}{1} = \frac{a}{s}$. Si l'idéal engendré dans $A/\mathfrak{m}^k$ par la classe de s est propre, alors il est contenu dans un idéal maximal, donc

22. On verra plus tard que le vocabulaire des modules permettrait de simplifier un peu l'exposition ici.

23. Noter que cela utilise en général le lemme de Zorn.

24. On pouvait aussi être tenté.e d'utiliser un supplémentaire mais attention qu'il est incorrect pour $(F_n)_{n\in\mathbf{N}}$ est une suite croissante d'espaces vectoriels, que tout choix de supplémentaire $(G_n)_{n\in\mathbf{N}}$ fournit une suite décroissante. On peut en revanche s'arranger pour que ce soit le cas. On fixe un supplémentaire G_0 de F_0 et supposons $F_0, \ldots, F_k$ construits. On a alors $E = F_k \oplus G_k$ et $F_{k+1} \subseteq F_k$. On peut donc écrire $F_k = F_{k+1} \oplus G'_k$ de sorte que $E = F_k \oplus (G'_k \oplus G_k)$ et on peut poser $G_{k+1} = G'_k \oplus G_k$ qui contient bien G_k.

25. Noter que puisqu'on a un idéal maximal, $A/\mathfrak{m}_k$ est bien un corps.

26. Par exemple, si on prend I un tel idéal du quotient, il correspond à $I = \pi(I')$ pour I' un idéal de A vérifiant $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k \subseteq I' \subseteq \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{k-1}$. On a alors clairement stabilité par somme et $\overline{a}\pi(x) = \pi(ax)$ avec $x \in I'$ donc $ax \in I'$ et on a stabilité par multiplication par un scalaire.

27. En fait, la question **6.** a) appliquée à $I = (0)$ suffit à être en mesure d'appliquer c).

nécessairement dans $\mathfrak{m}/\mathfrak{m}^k$, ce qui impliquerait que $s \in \mathfrak{m}$. On en déduit que cet idéal est égal à $A/\mathfrak{m}^k$ et en particulier il existe $u \in A$ tel que $\overline{su} = \overline{1}$, ce qui implique que $us - 1 \in \mathfrak{m}^k$. On déduit de ce qui précède qu'il existe $t \notin \mathfrak{m}$ tel que $t(us-1) = 0$ et donc $\frac{1}{s} = \frac{u}{1}$ dans $A_{\mathfrak{m}}$. Il s'ensuit que $f(au) = f(a)f(u) = \frac{a}{1} \cdot \frac{u}{1} = \frac{a}{1} \cdot \frac{1}{s} = \frac{a}{s}$ par définition de la structure d'anneau sur $A_{\mathfrak{m}}$. On a donc le résultat. Pour conclure, on utilise le fait que $\prod_{i=1}^{n} \mathfrak{m}_i^k = (0)$ de sorte que

$$A \cong A/(0) = A/\prod_{i=1}^{n} \mathfrak{m}_i^n \cong \prod_{i=1}^{n} A/\mathfrak{m}_i^k \cong \prod_{i=1}^{n} A_{\mathfrak{m}_i}$$

par le théorème chinois.

►**Remarque.–** Noter qu'en général, le morphisme naturel f donné par

$$a \longmapsto \left(\frac{a}{1}, \ldots, \frac{a}{1}\right)$$

est toujours injectif. En effet, si $a \in \mathrm{Ker}(f)$, alors $\frac{a}{1} = \frac{0}{1}$ dans chaque $A_{\mathfrak{m}_i}$ et donc il existe $u_i \notin \mathfrak{m}_i$ tel que $u_i a = 0$ par définition du localisé. En particulier, si on considère

$$\mathrm{Ann}(a) = \{x \in A \ : \ xa = 0\}$$

alors on obtient un idéal de A qui n'est contenu dans aucun des $\mathfrak{m}_i$, ce qui implique (par Krull) que $\mathrm{Ann}(a) = A$ et en particulier pour $x = 1$, $a = 0$ et par un raisonnement similaire montrer que le morphisme naturel $A \to \prod_{i=1}^{n} A_{\mathfrak{m}_i}$ est surjectif et donc un isomorphisme.