A– Soit p un nombre premier. Soit A un anneau fini de caractéristique n et de cardinal une puissance de p.

1. Montrer qu'on a un homomorphisme injectif d'anneaux $\mathbb{Z}/n\mathbb{Z} \to A$.
2. Montrer que n divise le cardinal de A ?
3. Montrer que si A est de cardinal p^2, il est isomorphe à $\mathbb{Z}/p^2\mathbb{Z} \to A$, à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ou à un corps fini à p^2 éléments. En particulier, montrer que A est commutatif.
4. Donner un exemple d'un anneau non commutatif de cardinal p^4 (de cardinal p^3 ?).

B– Nilradical d'un anneau commutatif. Soit A un anneau commutatif. On dit qu'un élément non nul x de A est *nilpotent* s'il existe un entier $n > 0$ tel que $x^n = 0$.

1. Montrer que l'ensemble des éléments nilpotents de A est un idéal, que l'on note $Nil(A)$ et qu'on appelle *nilradical* de A.
2. Quel est le nilradical d'un anneau intègre, de $\mathbb{Z}/2007\mathbb{Z}$?
3. Montrer qu'un élément nilpotent appartient à tout idéal premier de A.
4. Montrer que $A/Nil(A)$ n'a pas d'élément nilpotent non nul.
5. Soit $x \in A$. Posons $S = \{x^n / n \geq 0\}$. Si x n'est pas nilpotent, montrer que l'on peut considérer l'anneau localisé $S^{-1}A$. Considérons l'homomorphisme canonique d'anneaux $i : A \to S^{-1}A$. Montrer que $i(x)$ est inversible, puis que l'image réciproque par i d'un idéal maximal I de $S^{-1}A$ est un idéal premier ne contenant pas x.
6. Montrer que $Nil(A)$ coïncide avec l'intersection des idéaux premiers de A.
7. Soit I un idéal de A. On appelle *radical* de I l'ensemble constitué des $x \in A$ tels que $x^n \in I$ pour au moins un entier $n > 0$. (Le nilradical est donc le radical de $\{0\}$.) Montrer que le radical de I est l'image réciproque dans A du nilradical de A/I.

C– Soit $\mathbb{K}$ un corps. Soit n un entier > 0.

1. Montrer qu'une matrice de $M(n, \mathbb{K})$ est inversible à gauche si, et seulement si, elle est inversible à droite. En déduire que si les matrices A et B vérifient $AB = A + B$, alors $BA = B + A$.
2. Montrer le polynôme caractéristique de AB est égal à celui de BA. En déduire que $I_n - AB$ est inversible si, et seulement si, $I_n - BA$ l'est.
3. Soit R un anneau. Soient a et $b \in R$. Montrer que si $1 - ba$ est inversible à gauche, il en est de même de $1 - ab$. (On notera que l'hypothèse implique que b appartient à l'idéal à gauche $R(1 - ab)$, et donc 1 également. Une variante plus astucieuse consiste à remarquer que si $x(1 - ba) = 1$, alors $(1 + axb))(1 - ab) = 1$.)
4. Énoncer une propriété analogue pour l'inversibilité à droite.

D– Le radical de jacobson d'un anneau (non commutatif).

1. Soit a un élément d'un anneau A vérifiant la condition $\forall x, y \in A,\ 1 - xay \in A^\star$. Montrer que a appartient à tout idéal à gauche maximal de A, ainsi qu'à tout idéal à droite maximal de A.

   Indication.– Si I est un idéal à gauche maximal et $a \notin I$, alors $Aa + I = A$. Écrire $1 = xa + m$ pour aboutir à une contradiction.

2. On suppose maintenant que a appartient à tout idéal à gauche maximal. Montrer a vérifie alors la condition précédente. (Commencer par établir que $1 - xa$ est inversible à gauche pour tout x. On introduirait (lemme de Zorn) si ce n'était pas le cas un idéal à gauche maximal contenant $1 - xa$. On dispose donc pour tout x d'un élément x' tel que $x'(1 - xa) = 1$, soit $x' = 1 - (-x'x)a$, et donc d'un x'' tel que $1 = x''x' = x'' + x''x'xa = x'' + xa$, et $1 - xa$ serait inversible à droite, tout comme $1 - ax$.)

3. Montrer que l'ensemble des éléments $a \in A$ vérifiant la condition ci-dessus est stable par addition, et que c'est donc clairement un idéal bilatère de A.

4. Vérifier que cet idéal bilatère, que l'on notera $rad(A)$ et que l'on appellera le radical (de Jacobson) de A coïncide avec l'intersection des idéaux à gauche maximaux de A, tout comme avec l'intersection des idéaux à droite maximaux de A.

5. Quel est le radical de $A/rad(A)$?

6. Quel est le radical des anneaux commutatifs $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{K}[A]$?

7. Quel est le radical de Jacobson de l'anneau $\mathbb{Z}$, ainsi que celui de l'anneau $M(2, \mathbb{Z})$?

8. Montrer que $rad(A)$ est le plus grand des idéaux à gauche I de A vérifiant $1 + I \subset A^\star$.

9. Montrer que si un idéal bilatère J est contenu dans $rad(A)$, alors le radical de A/J est $rad(A)/J$.

10. Montrer qu'un idéal à gauche (ou à droite) formé d'éléments nilpotents est nécessairement contenu dans $rad(A)$. Montrer que le radical de l'anneau des matrices triangulaire supérieures à coefficients dans $\mathbb{K}$ est l'idéal (bilatère) des matrices triangulaires supérieures strictes.

11. Rappelons que le nilradical d'un anneau *commutatif* est l'ensemble $Nil(A)$ de ses éléments nilpotentset que c'en est un idéal. Déterminer le nilradical et le radical de Jacobson de l'anneau $\mathbb{K}[J_n]$, où J_n est le bloc de Jordan plein. En déduire que l'inclusion $Nil(A) \subset rad(A)$ peut être stricte.

12. Étendre aux $\mathbb{K}$-algèbres (unitaires), où K est un corps commutatif, la notion de radical de Jacobson. Montrer que le radical de Jacobson d'une algèbre A de dimension finie est nilpotent. (Invoquer un argument de type Nakayama : considérer à cet effet une famille génératrice minimale de l'idéal – à gauche – $rad(A)^m$ vérifiant pour un m bien choisi, du fait de la décroissance stationnaire de la suite des puissances de $rad(A)$, $rad(A) \cdot rad(A)^m = rad(A)^m$, et montrer par l'absurde que $rad(A)^m$ est en fait nul.) Retrouver le résultat de la question 10.

E– Corps et anneaux de quaternions.

1. Soit $\mathbb{H}$ l'algèbre associative de dimension 4 sur $\mathbb{R}$, ayant pour base les éléments $1, i, j, k$ et dont la table de multiplication est générée par les règles $i^2 = j^2 = -1$ et $ij = -ji = k$. Montrer que cette algèbre

existe bien et qu'elle est isomorphe à l'algèbre réelle $\mathbb{H}'$ des matrices complexes $\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}$.

2. Montrer que l'algèbre $\mathbb{H}$ est un corps (non commutatif). (On interprètera à cette occasion dans $\mathbb{H}$ le déterminant sur $\mathbb{H}'$.)

3. Déterminer le groupe des éléments inversibles de l'anneau $R_{\mathbb{Z}}$ engendré par i et j.

4. On considère le sous-groupe du groupe additif $(\mathbb{H}, +)$ engendré par les éléments $(1 + i + j + k)/2$, i, j et k. Montrer que ce groupe est isomorphe à $\mathbb{Z}^4$, qu'il contient le groupe $(R_{\mathbb{Z}}, +)$ comme sous-groupe d'indice deux, qu'il contient 1 et, enfin, qu'il est stable par multiplication. On notera l'anneau correspondant par $R_{\mathbb{H}}$, et on le désignera comme l'anneau des quaternions d'Hurwitz.

5. Déterminer le groupe des unités de l'anneau $R_{\mathbb{H}}$. On montrera qu'il a un seul 2-Sylow, isomorphe à $\mathbb{H}_8$, et qu'il est donc isomorphe au groupe $SL(2, \mathbb{F}_3)$. Dessiner le graphe du treillis de ses sous-groupes.

F– Idempotents

On dit que $e \in A$ est idempotent si $e^2 = e$.

1. Caractériser de diverses manières les idempotents de l'algèbre $M(n, \mathbb{K})$. Déterminer les composantes connexes de l'ensemble des idenmpotents de $M(n, \mathbb{C})$.

2. Décompositions de l'unité. idempotent primitif, idempotent central.

3. Montrer que les décompositions de l'anneau $A = I_1 + \cdots + I_m$ en sommes directes de m idéaux à gauche sont en correspondances bijective avce les décompositions de l'unité $1 = e_1 + \cdots + e_m$ en somme (orthogonale) de m idempotents. Montrer que dans ce cas, on a $I_k = Ae_k$. Noter que l'idéal à gauche Ae_k est indécomposable si, et seulement si, e_k est un idempotant primitif.

4. Énoncer un analogue pour les idéaux à droite.

5. Montrer que les décompositions de A en somme directes d'idéaux bilatères sont en correspondance bijective avec les décompositions de l'unité en somme d'idempotents centraux. Montrer que dans ce cas, chaque idéal bilatère A_k de la décomposition $A = A_1 \oplus \cdots \oplus A_m$ est un anneau pour-lui même ayant e_k comme unité. Montrer que l'anneau A est alors isomorphe à l'anneau produit $A_1 \times \cdots \times A_k$, et que tout isomorphisme de A avec un produit fini d'anneaux est de la sorte.

6. Examiner le cas important de l'algèbre $\mathbb{C}[A]$. En déduire la décomposition de l'espace vectoriel $\mathbb{C}^n$ ne somme des sous-espaces caractéristiques de la matrice A.

7. On dit que A est connexe s'il ne peut s'écrire comme produit de deux anneaux non triviaux. Montrer que cela veut dire que les seul idempotents centraux sont 0 et 1. Montrer que l'algèbre des matrices triangulaires inférieures 3×3 telles que $t_{21} = 0$ est connexe, mais s'écrit comme la somme de trois idéaux à gauche indécomposables.

8. Soit e un idempotent dans A. Montrer que eAe est un anneau admettant e comme l'élément unité. Montrer que l'idéam à gauche Ae a une structure naturelle de eAe-module à droite, et que l'idéal à droite eA a une structure de eAe-module à gauche. Montrer que l'anneau eAe est canoniqument isomorphe

à l'anneau des endomorphismes du AeA-module à droite Ae (ou à l'anneau des ensomorphismes du eAe-module à gauche eA).

9. Montrer que les idempotents de l'anneau $A/rad(A)$ se relèvent en des idempotents de A.

G– Anneaux locaux, algèbres locales

On dit que l'anneau A est local s'il admet un seul idéal à gauche maximal.

1. Montrer que l'anneau $\mathbb{K}[X^2, X^3]$ est local.
2. Quand est-ce que l'algèbre $\mathbb{K}[A]$ est locale ?
3. Montrer que l'ensemble des éléments non inversibles d'un anneau local A est un idéal bilatère. Réciproque.
4. Montrer que dans un anneau local un élément quelconque a vérifie a ou $1-a$ est inversible. Réciproque.
5. Montrer que les seuls idempotents d'un algèbre locale de dimension finie sont 0 et 1. Réciproque. Examiner aussi le cas $A = \mathbb{K}[X]$.
6. Montrer que si A est une $\mathbb{K}$-algèbre locale, alors la $\mathbb{K}$-algèbre $A/rad(A)$ est isomorphe à $\mathbb{K}$.
7. Montrer que si l'anneau A admet un seul idéal à droite maximal, alors il est local.
8. Montrer que l'idempotent e est primitif si, et seulement si, l'anneau $eAe \simeq End(Ae)$ est un anneau local. Moralité : localité=indécomposabilité. Traiter l'exemple du $\mathbb{K}[X]$-module indécomposable $\mathbb{C}^n$, où X agit par la matrice de Jordan pleine J_n.

H– Théorème des deux carrés

1. Montrer que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est isomorphe à l'anneau quotient $\mathbb{Z}[X]/(X^2+1)$.
2. Soit p un nombre premier. En déduire que l'idéal engendré par p dans $\mathbb{Z}[i]$ est premier si et seulement si le polynôme X^2+1 admet des racines dans un corps à p éléments, puis que cette dernière condition est équivalente à $p \equiv 1 \pmod 4$.
3. Montrer qu'un nombre entier est somme de deux carrés si et seulement si chacun de ses facteurs premiers est somme de deux carrés. En déduire quels sont les nombres entiers qui sont sommes de deux carrés.