UNIVERSITÉ GRENOBLE-ALPES Prépa Agreg

Enseignant : Rémi Molinier
remi.molinier@univ-grenoble-alpes.fr

Exercices sur les anneaux

Merci beaucoup à Vincent Beck pour presque l'entièreté des exercices de cette longue liste.

1 La structure d'anneau.

Exercice 1 – Anneau de fonction
Soit A un anneau et I un ensemble.

1) Montrer que l'ensemble $\mathscr{F}(I,A)$ des fonctions de I dans A est un anneau (commutatif si A l'est). Quel est l'élément neutre pour l'addition, la multiplication ?

2) On suppose que I est un espace métrique et $A=\mathbb{R}$. Montrer que les fonctions continues sur I forment un sous-anneau de $\mathscr{F}(I,A)$.

3) Pour $x\in I$, montrer que l'application

$$\begin{aligned}\mathrm{ev}_x\colon \mathscr{F}(I,A) &\longrightarrow A\\ f &\longmapsto f(x)\end{aligned}$$

est un morphisme d'anneaux appelé *morphisme d'évaluation en x.*

4) Déterminer les diviseurs de 0 dans $\mathscr{C}(\mathbb{R},\mathbb{R})$.

5) Déterminer les éléments inversibles de $\mathscr{F}(I,A)$? de $\mathscr{C}(\mathbb{R},\mathbb{R})$?

6) Soit $x_0\in\mathbb{R}$. Montrer que l'ensemble $\{f\in\mathscr{C}(\mathbb{R},\mathbb{R}) \mid f(x_0)=0\}$ est un idéal maximal de $\mathscr{C}(\mathbb{R},\mathbb{R})$. Est-il principal ? Que se passe-t-il si on remplace $\mathscr{C}(\mathbb{R},\mathbb{R})$ par $\mathbb{R}[X]$, $\mathscr{C}^\infty(\mathbb{R},\mathbb{R})$, $\mathscr{F}(\mathbb{R},\mathbb{R})$?

7) Existe-t-il des éléments nilpotents non nuls dans $\mathscr{C}(\mathbb{R},\mathbb{R})$?

8) Soit U un ouvert de $\mathbb{C}$ et $\mathcal{H}$ l'anneau des fonctions holomorphes sur U. Montrer que $\mathcal{H}$ est intègre si et seulement si U est connexe.

Exercice 2 – Diviseurs de 0

1) Déterminer les diviseurs de 0 dans $\mathbb{Z},\mathbb{D},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{R}[X]$.

2) Déterminer les diviseurs de 0 dans $\mathbb{Z}/4\mathbb{Z}$.

3) Déterminer les diviseurs de 0 dans $\mathbb{Z}/n\mathbb{Z}$.

4) Dans un anneau commutatif, montrer que le produit ab est un non-diviseur de 0 si et seulement si a et b le sont.

5) Montrer qu'un sous-anneau d'un anneau intègre est intègre.

6) Un produit d'anneaux est-il intègre ? un corps ?

7) Soit k un corps et $P\in k[X]$. Déterminer les diviseurs de 0 dans $k[X]/(P)$.

Exercice 3 – Éléments inversibles
Soit A un anneau.

1) Montrer que l'ensemble $A^\times$ des éléments inversibles de A est un groupe pour la multiplication.

2) Déterminer les éléments inversibles de $\mathbb{Z},\mathbb{D},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{R}[X]$.

3) Comparer les groupes $\mathbb{F}_3(X)^\times$ et $\mathbb{Q}(X)^\times$.

4) Déterminer les éléments inversibles de $\mathbb{Z}/4\mathbb{Z}$.

5) Déterminer les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

6) Montrer que si u est inversible et x nilpotent et $ux = xu$ alors $u+x$ est inversible. En particulier, montrer que $1+x$ est inversible. Quel est l'inverse ?

7) Montrer que si $f : A \to B$ est un morphisme d'anneaux alors f induit par restriction un morphisme de groupes de $A^\times$ dans $B^\times$. On suppose que f est surjectif, le morphisme de $A^\times$ dans $B^\times$ induit est-il surjectif ?

8) Montrer que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

9) Soit k un corps et $P \in k[X]$. Déterminer les éléments inversibles de $k[X]/(P)$. En déduire que $k[X]/(P)$ est un corps si et seulement si P est irréductible.

Exercice 4 – Éléments nilpotents et radical

1) Déterminer les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$.

2) Soit k un corps et $P \in k[X]$. Déterminer les éléments nilpotents de $k[X]/(P)$.

3) On suppose que A est un anneau commutatif. Montrer que l'ensemble des éléments nilpotents de A est un idéal de A ? Le résultat s'étend-il à un anneau non commutatif ?

4) On suppose encore que A est commutatif. On considère un idéal I de A. Montrer que l'ensemble

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N},\ x^n \in I\}$$

est un idéal contenant I. Que vaut $\sqrt{0}$? Calculer $\sqrt{\sqrt{I}}$?

5) Décrire l'idéal de A/I correspondant à $\sqrt{I}$.

6) Montrer que l'intersection des idéaux premiers de A contenant I est $\sqrt{I}$ (c'est une question difficile : on pourra montrer que si $x \notin \sqrt{I}$, l'ensemble des idéaux contenant I ne rencontrant pas l'ensemble $\{x^n \mid n \in \mathbb{N}\}$ est non vide et admet un élément maximal qui est un idéal premier de A).

7) Montrer que $A/\sqrt{0}$ est un anneau réduit (i.e. n'a pas d'élément nilpotent non nul).

L'exercice suivant est **FONDAMENTAL**.

Exercice 5 – Caractéristique

1) Propriété universelle de l'anneau $\mathbb{Z}$. Soit A un anneau unitaire. Montrer qu'il existe un unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to A$. Vérifier qu'il est donné par $f(k) = k1_A$.

Le noyau de l'unique morphisme $f : \mathbb{Z} \to A$ est de la forme $n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$. Cet entier n est appelé la *caractéristique de l'anneau* A. C'est le plus petit entier non nul (s'il existe) tel que $n1_A = 0$. Il vérifie aussi $na = 0$ pour tout $a \in A$ (pourquoi ?).

2) Montrer que le sous-anneau premier de A est isomorphe à $\mathbb{Z}/\mathrm{car}(A)\mathbb{Z}$.

3) Montrer que si A est un sous-anneau de B alors $\mathrm{car}(A) = \mathrm{car}(B)$.

4) Soit $g : A \to B$ un morphisme d'anneau. Comparer la caractéristique de A et celle de B. En déduire que si $\mathrm{car}(A)$ et $\mathrm{car}(B)$ sont premiers entre eux alors il n'y a pas de morphisme d'anneaux entre A et B.

5) Quelle est la caractéristique de $\mathbb{Z}/n\mathbb{Z}$, de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}[X]$?

6) Quelle est la caractéristique de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$? et celle de $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

7) Quelle est la caractéristique de $\prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$?

8) Quelle peut être la caractéristique d'un anneau intègre ? d'un corps ?

9) Montrer qu'il n'existe pas de morphisme de corps entre deux corps n'ayant pas la même caractéristique.

10) Montrer qu'un anneau de caractéristique p (premier) peut être muni d'une structure d'espace vectoriel sur le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

11) Montrer que si A et B sont deux anneaux de caractéristique p et $f : A \to B$ un morphisme d'anneaux alors f est $\mathbb{F}_p$ linéaire pour la structure définie dans la question précédente.

12) Montrer qu'il n'existe aucun morphisme d'anneaux unitaires de $\mathbb{Q}$ (resp. $\mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ avec $n \geq 1$) dans $\mathbb{Z}$.

13) Montrer que l'unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to \mathbb{Q}$ vérifie que pour tous morphismes d'anneaux unitaires $g, h : \mathbb{Q} \to A$ tel que $g \circ f = h \circ f$, on a $h = g$.

Exercice 6 – Anneau quotient

Soit A un anneau, I un idéal de A. On définit la relation d'équivalence sur I $\mathscr{R}_I$ par

$$x \mathscr{R}_I y \iff x - y \in I\,.$$

L'ensemble quotient se note A/I (c'est bien entendu cohérent avec la notation usuelle puisque I est un sous-groupe du groupe additif A et $\mathscr{R}_I$ la relation habituelle).

1) Soit $\mathscr{R}$ une relation d'équivalence sur un anneau A. Montrer qu'il existe sur $A/\mathscr{R}$ une structure de groupe telle que la surjection canonique π soit un morphisme d'anneaux (cette structure étant alors unique) si et seulement si $\mathscr{R}$ est compatible avec les deux lois de A. De plus, montrer que si ces conditions sont vérifiées, il existe un idéal I de A tel que $\mathscr{R} = \mathscr{R}_I$ (remarquer que I est nécessairement la class de 0).

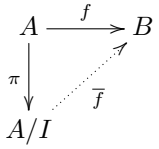
2) Décrire la classe de x pour $\mathscr{R}_I$.

3) Montrer que la relation $\mathscr{R}_I$ est compatible avec les lois de A. En déduire qu'il existe une unique structure d'anneau sur A telle que la surjection canonique soit un morphisme d'anneaux.

4) Montrer que tout idéal de A est le noyau d'un morphisme (qu'on peut supposer surjectif) d'anneaux.

5) **Propriété universelle du quotient.** Soient A un anneau, I un idéal de A et $\pi : A \to A/I$ la surjection canonique. On considère un anneau B et $f : A \to B$ un morphisme d'anneaux. Montrer l'équivalence des trois propriétés suivantes

(i) Il existe une application $\overline{f} : A/I \to B$ telle que $f = \overline{f} \circ \pi$ i.e. telle que le diagramme suivant soit commutatif



(ii) $I \subset \ker f$

(iii) $f(I) = \{0_A\}$.

Montrer que lorsque ces conditions sont vérifiées, l'application $\overline{f}$ est uniquement définie et que c'est un morphisme de d'anneaux. Vérifier que $\operatorname{Im} \overline{f} = \operatorname{Im} f$ et $\ker \overline{f} = \ker f/H$ et que $\overline{f}$ est donnée par $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in A$ (où $\overline{x} = \pi(x)$ désigne la classe de x dans A/I).

Morale (à retenir) : *se donner un morphisme d'anneaux issu d'un quotient, c'est la même chose que de se donner un morphisme trivial sur l'idéal par lequel on veut quotienter. C'est donc très facile de construire des morphismes issus de quotients.*

6) Montrer que l'application

$$\begin{aligned} \operatorname{Hom}_{\text{ann.}} A/IB &\longrightarrow \operatorname{Hom}_{\text{gr.}} AB \\ \varphi &\longmapsto \varphi \circ \pi \end{aligned}$$

est une application injective dont on déterminera l'image. Pour un élément de l'image, on décrira l'unique antécédent.

7) Premier théorème d'isomorphisme. Soit $f : A \to B$ un morphisme d'anneaux. Montrer que f induit un isomorphisme de groupes $\varphi : A/\ker f \to \operatorname{Im} f$ donné par $\varphi(x + \ker f) = f(x)$ pour tout $x \in A$. Qu'obtient-on lorsque f est surjectif ?

8) Applications. En utilisant l'exercice 5, montrer que $\operatorname{Hom}_{\text{ann.}} \mathbb{Z}/n\mathbb{Z}A$ a au plus un élément. à quelle condition $\operatorname{Hom}_{\text{ann.}} \mathbb{Z}/n\mathbb{Z}A \neq \emptyset$? En déduire $\operatorname{Hom}_{\text{ann.}} \mathbb{Z}/n\mathbb{Z}\mathbb{Z}/m\mathbb{Z}$. Comparer avec $\operatorname{Hom}_{\text{gr.}} \mathbb{Z}/n\mathbb{Z}\mathbb{Z}/m\mathbb{Z}$.

Exercice 7 – Théorème de correspondance

Soient A et B deux anneaux et $f : A \to B$ un morphisme **surjectif** d'anneaux. On note $K = \ker f$, $\mathscr{A}$ (resp. $\mathscr{A}_K$) l'ensemble des idéaux de $\mathscr{A}$ (resp. contenant K), $\mathscr{B}$ l'ensemble des idéaux de B.

1) Montrer que l'application

$$\begin{aligned} \alpha \colon \mathscr{A} &\longrightarrow \mathscr{B} \\ I &\longmapsto f(I) \end{aligned}$$

est bien définie. (On remarquera aussi que cette application n'est pas bien définie si f n'est pas surjectif : $f(I)$ n'est pas un idéal).

2) Montrer que l'application

$$\begin{aligned} \beta \colon \mathscr{B} &\longrightarrow \mathscr{A} \\ J &\longmapsto f^{-1}(J) \end{aligned}$$

est bien définie et à valeurs dans $\mathscr{A}_K$.

3) Pour $J \in \mathscr{H}$ et $I \in \mathscr{G}$, calculer $\alpha \circ \beta(J)$ et $\beta \circ \alpha(I)$. En déduire que β est injective, α est surjective et β et α sont des bijections réciproques l'une de l'autre entre $\mathscr{A}_K$ et $\mathscr{B}$.

4) Montrer que ces bijections induites par α et β conservent les inclusions, les intersections (attention, ce n'est pas purement formel), les idéaux premiers, les idéaux maximaux, les radicaux.

5) Deuxième théorème d'isomorphisme. Soit J (resp. I) un idéal de B (resp. A contenant K). Construire un isomorphisme de groupes entre $A/\beta(J)$ et B/J (resp. entre A/I et $B/\alpha(I)$).

6) Application. On considère un anneau A, K un idéal de A et $f : A \to A/K$ la surjection canonique. Décrire des bijections respectant les inclusions, les intersections, les idéaux premiers et maximaux et les sous-groupes de A/K. Déduire de la question précédente, l'isomorphisme de groupe $A/I \cong (A/K)/(I/K)$ pour tout idéal I de A contenant K.

7) Application. Voir l'exercice 20.

8) Application. Soit k un corps et $0 \neq P \in k[X]$. Montrer que l'anneau $k[X]/P$ n'a qu'un nombre fini d'idéaux.

9) Complément. On considère à présent A et B deux anneaux et $f : A \to B$ un morphisme d'anneau qu'on ne suppose plus surjectif. Donner un exemple d'idéal de A tel que $f(I)$ ne soit pas un idéal de B. Montrer que l'image réciproque d'un idéal (resp. premier) est un idéal (resp. premier). Est-ce le cas pour un idéal maximal ?

Exercice 8 – Morphismes d'anneaux

Soit $f : \mathbb{R} \to \mathbb{R}$ un endomorphisme d'anneau.

1) Calculer $f(n)$ pour $n \in \mathbb{Z}$ puis pour $f \in \mathbb{Q}$.

2) Montrer que $f(x) \geq 0$ si $x \geq 0$ (on caractérisera la positivité d'un réel en terme algébrique).

3) En déduire que f est croissante.

4) En déduire que $f = \mathrm{Id}_{\mathbb{R}}$.

5) Soit $f : \mathbb{C} \to \mathbb{C}$ un endomorphisme d'anneau. Montrer l'équivalence

(i) f est l'identité ou la conjugaison ;

(ii) f est continu ;

(iii) $f(\mathbb{R}) \subset \mathbb{R}$;

(iv) $f(x) = x$ pour tout $x \in \mathbb{R}$.

Exercice 9 – Matrice triangulaire
Soit k un corps. On considère le sous-anneau de $\mathrm{Mat}_2(k)$

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

1) Déterminer les éléments nilpotents de A ?

2) Déterminer les inversibles de A ?

3) Déterminer les éléments réguliers à droite, à gauche ?

4) Déterminer les idéaux de A et les quotients correspondants.

Exercice 10 – Anneau produit et idéaux
On considère l'anneau produit $A = A_1 \times \cdots \times A_n$.

1) Soit I un idéal bilatère de A. Montrer que $I = I_1 \times \cdots \times I_n$ où I_j est un idéal bilatère de A_j. Quel est le quotient ?

2) On suppose que tous les A_i sont non nuls et commutatifs. Décrire les idéaux premiers de A ? les idéaux maximaux de A ?

3) On suppose que les A_j sont des corps. Combien A admet-il d'éléments maximaux ? En déduire qu'un produit de deux corps n'est jamais isomorphe à un produit de trois corps.

Exercice 11 – Opérations sur les idéaux
Soit A un anneau.

1) Soit I et J deux idéaux à gauche (resp. à droite, bilatère). Montrer que $I + J = \{i + j \mid i \in I, j \in J\}$ est un idéal à gauche (resp. à droite, bilatère).

2) Soit I et J deux idéaux à gauche (resp. à droite, bilatère). Montrer que

$$IJ = \left\{ \sum_{k=0}^{n} i_k j_k \mid n \in \mathbb{N}, i_k \in I, j_k \in J \right\}$$

est un idéal à gauche (resp. à droite, bilatère).

3) Montrer que $(I + J) + K = I + (J + K)$, $(IJ)K = I(JK)$, $(I + J)K = IK + JK$ et $I(J + K) = IJ + IK$. Montrer $0 + I = I + 0 = I$ et $AI = I$ (si I est un idéal à gauche). A-t-on $IA = I$?

Exercice 12 – Anneaux finis

1) Montrer qu'un anneau intègre fini est un corps.

2) Donner des exemples d'anneaux non intègres et finis.

3) Déterminer les anneaux à 2,3 et 4 éléments.

Exercice 13 – Anneaux d'idempotents
Soit A un anneau tel que $a^2 = a$ pour tout $a \in A$.

1) Montrer que A est commutatif.

2) Dans cette question (et dans cette question seulement), on suppose que A est intègre. Montrer que A est un corps et que A a deux éléments.

3) Montrer que tout idéal premier de A est maximal.

Exercice 14 – Manipulations algébriques
Soit A un anneau tel que $a^3 = a$ pour tout $a \in A$.

1) Déterminer les éléments nilpotents de A.

2) Soit $e \in A$ tel que $e^2 = e$ et $a \in A$ et $b = ea(1-e)$. Calculer b^2 et en déduire que $ea = ae$.

3) En déduire que pour tout $x \in A$ alors $x^2 \in ZA$.

4) Montrer que $2x \in ZA$ pour tout $x \in A$.

5) Montrer que $3x^2 + 3x = 0$. En déduire que $3x \in ZA$.

6) Montrer que A est commutatif.

Exercice 15 – Anneaux de fonctions continues sur un compact
Soit A l'anneau des fonctions continues de $[0, 1]$ dans $\mathbb{R}$.

1) Soit $x \in [0, 1]$. Montrer que $I_x = \{f \in A \mid f(x) = 0\}$ est un idéal maximal de A. Quel est le quotient A/I_x ?

2) Tous les idéaux de A sont-ils maximaux ? premiers ?

3) I_x est-il principal ?

4) Montrer que $(I_x)^2 = I_x$.

5) Montrer que tout idéal maximal de A est de la forme I_x.

Definition 1 (Idéal premier)**.** Soit I un idéal de A un anneau commutatif. On dit que I est un idéal premier si les propriétés équivalentes suivantes sont vérifiées

(i) A/I est intègre ;

(ii) $I \neq A$ et $xy \in I \Longleftrightarrow x \in I$ ou $y \in I$.

(iii) $A \setminus I$ est une partie multiplicative de A.

Definition 2 (Idéal maximal)**.** Soit I un idéal de A un anneau commutatif. On dit que I est un idéal maximal si les propriétés équivalentes suivantes sont vérifiées

(i) A/I est un corps ;

(ii) $I \neq A$ et si J est un idéal tel que $I \subset J$ alors $J = A$ ou $J = I$;

(iii) I est un élément maximal (pour l'inclusion) parmi les idéaux distincts de A.

Exercice 16 – Idéaux premiers, idéaux maximaux

1) Soit A un anneau intègre. Montrer que si A contient un nombre fini d'idéaux alors A est un corps (on pourra considérer les idéaux de la forme (a^n)).

2) Soit A un anneau commutatif. Montrer qui si A contient un nombre fini d'idéaux alors tout idéal premier est maximal.

3) Soit A un anneau tel que tout idéal est premier. Montrer que A est un corps (on pourra considérer les idéaux de la forme (x^2)).

Exercice 17 – Lemme de Zorn et anneaux
Soit A un anneau commutatif.

1) On suppose que $A \neq \{0\}$. Montrer que A admet un idéal maximal.

2) Soit $I \neq A$ un idéal de A. Montrer qu'il existe un idéal maximal de A contenant I (on pourra appliquer la question précédente à A/I).

3) Soit $f \in A$. On note $S = \{f^n \mid n \in \mathbb{N}\}$. à quelle condition l'ensemble des idéaux ne rencontrant pas S admet un élément maximal. Montrer qu'un tel idéal maximal est premier. En déduire que l'intersection des idéaux premiers de A est formée des éléments nilpotents de A.

2 Congruences et nombres premiers.

2.1 Congruences.

Exercice 18 – Congruences

1) Calculer le dernier chiffre de l'écriture décimale de 7^{7^7}.

2) Déterminer le plus petit multiple de 19 dont l'écriture en base 10 ne comporte que des 1.

3) Soient $m, n \in \mathbb{N}^*$ premiers entre eux. Expliciter l'application inverse de l'isomorphisme du lemme chinois

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

4) Soient $m, n \in \mathbb{N}^*$. Montrer que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est cyclique si et seulement si m et n sont premiers entre eux.

5) Soient $m, n \in \mathbb{N}^*$. Montrer que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à un groupe de la forme $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ avec $b \mid a$. Donner une expression pour a et b en fonction de m et n.

6) Soient m, n deux entiers naturels non nuls et soit d leur pgcd. Montrer que $\text{pgcd}(2^m - 1, 2^n - 1) = 2^d - 1$.

7) Soit $(F_n)_{n \geqslant 0}$ la suite de Fibonacci ($F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geqslant 0$).

(i) Montrer que F_m et F_{m+1} sont premiers entre eux.

(ii) Montrer que $F_n = F_{m+1}F_{n-m} + F_mF_{n-m-1}$ pour $m < n$.

(iii) Soient m, n deux entiers naturels non nuls et soit d leur pgcd. Montrer que $\text{pgcd}(F_m, F_n) = F_d$.

Exercice 19 – Morphisme

1) Soient m, n deux entiers supérieurs ou égaux à 1. Combien y a-t-il de morphismes d'anneaux de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?

2) Combien y a-t-il de morphismes de groupes de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?

3) Combien y a-t-il de morphismes de groupes, d'anneaux de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{C}$?

Exercice 20 – Un exemple
Soit $A = \mathbb{Z}/3^4 5^2 7\mathbb{Z}$.

1) Déterminer les éléments inversibles, nilpotents, diviseurs de 0 dans A.

2) Déterminer les idéaux de A.

3) Quels sont les idéaux premiers de A, les idéaux maximaux ?

4) Donnez les inclusions des idéaux les uns dans les autres.

Exercice 21 – Parce que savoir faire l'algorithme d'Euclide est INDISPENSABLE

1) Calculer le pgcd de $P = 2X^4 - 3X^2 + 1$ et $Q = X^3 + X^2 - X - 1$ dans $\mathbb{Q}[X]$ et $U, V \in \mathbb{Q}[X]$ tel que $\text{pgcd}(P, Q) = UP + VQ$. Même question dans $\mathbb{R}[X]$.

2) Calculer l'inverse de $X^3 - X + 1$ dans $\mathbb{Q}[X]/(X^2 + X + 1)$.

3) Calculer $\text{pgcd}(X^n - 1, X^m - 1)$.

4) Montrer que $\text{pgcd}(m, n) = 1$ si et seulement si m est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 22 – Les carrés dans un corps fini

1) On suppose dans cette question que k est un corps fini de caractéristique 2. Montrer que tout élément de k est un carré.

On suppose pour le reste de l'exercice que k est un corps fini de caractéristique $p \neq 2$. On note $q = p^d = |k|$. Pour les questions c et e, proposer deux méthodes : l'une élémentaire (avec le théorème de Lagrange et le fait que dans un corps, un polynôme de degré d a au plus d racines), l'autre reposant sur la cyclicité de $k^\times$.

2) Déterminer les solutions de l'équation $x^2 = 1$ dans k.

3) Montrer que, dans k, il y a exactement $(q+1)/2$ carrés (indication pour la méthode élémentaire : étudier le morphisme de groupes $x \in k^\times \mapsto x^2 \in k^\times$).

4) Montrer que $x^{(q-1)/2} \in \{\pm 1\}$ pour tout $x \in k^\times$.

5) Montrer que $x \in k^\times$ est un carré dans k si et seulement si $x^{(q-1)/2} = 1$.

6) Montrer que -1 est un carré dans k si et seulement si $q = 1[4]$. En déduire que -1 est un carré modulo p si et seulement si $p = 1[4]$.

7) Application (voir [Tau92, théorème 5.3 p.368]) : un premier pas vers le théorème des 2 carrés. On suppose que $p = 1[4]$ et on fixe $u \in \mathbb{Z}$ tel que $-1 = u^2[p]$. Soit $\Gamma \subseteq \mathbb{Z}^2$ le sous-ensemble

$$\Gamma = \left\{(a, b) \in \mathbb{Z}^2 \mid a = ub[p]\right\}$$

Montrer que Γ est un sous-groupe de $\mathbb{Z}^2$. Déterminer le groupe quotient $\mathbb{Z}^2/\Gamma$. **Remarque :** *Ici le fait que $u^2 = -1[p]$ n'a aucune importance. Cette propriété de u sert en fait dans la suite de la démonstration du théorème des deux carrés.*

2.2 Quelques critères élémentaires de primalité.

Les exercices suivants (exercices 23 et 27) sont extrêmement classiques.

Exercice 23 – Théorème de Fermat-Euler

[Dem97, Proposition 2.11, exercices 2.23 et 2.24] Il s'agit ici d'étudier quelques conséquences élémentaires du théorème de Lagrange (l'ordre d'un élément divise l'ordre du groupe) dans la théorie des $\mathbb{Z}/n\mathbb{Z}$.

1) Montrer que si a et n sont deux entiers premiers entre eux alors $a^{\varphi(n)} = 1\ [n]$. Que se passe-t-il si n est premier ?

2) Soient $a \in \mathbb{N}^*$ et $n \geq 2$ tels que $a^{n-1} = 1\ [n]$ et $a^x \neq 1\ [n]$ pour tout diviseur strict x de $n - 1$. Montrer que n est premier.

3) Soient a et n deux entiers naturels non nuls. Montrer que $n \mid \varphi(a^n - 1)$.

4) Soient a, n et m trois entiers naturels. On suppose que m est premier et que $n \mid a^m - 1$. Montrer que $n \mid a - 1$ ou $m \mid \varphi(n)$. En déduire que tout facteur premier du nombre de Mersenne $2^m - 1$ où $m > 2$ est congru à 1 modulo $2m$.

Exercice 24 – Théorème de Wilson

[Dem97, exercices 2.16 à 2.19] Soit $n \geq 2$. Montrer que n est premier si et seulement si $(n-1)! = -1\ [n]$. Lorsque n n'est pas premier, calculer $(n-1)!\ [n]$. Pour quelques compléments autour du théorème de Wilson : `http://www.math.jussieu.fr/~beck/pdf/cplt-wilson.pdf`.

Exercice 25 – Nombres de Mersenne
[Dem97, 3.2.4 et exercice 6.32]

1) Soient $m \geq 2$ et $n \geq 1$ des entiers. Montrer que si $m^n - 1$ est premier, alors $m = 2$ et n est premier.

Un nombre de la forme $2^n - 1$ est appelé **nombre de Mersenne**.

2) Soit p un entier premier et soit q un diviseur premier de $2^p - 1$. Montrer que p divise $q - 1$.

Exercice 26 – Nombres de Fermat
[Dem97, 3.2.3, exercices 5.14 et 6.32]

1) Soient $m \geq 2$ et $n \geq 1$ un entier. Monter que si $m^n + 1$ est premier, alors n est une puissance de 2 et m est pair.

Le nombre $x_n = 2^{2^n} + 1$ est appelé **le $n^{\text{ième}}$ nombre de Fermat**. Les nombres $x_0 = 3, x_1 = 5, x_2 = 17, x_3 = 257, x_4 = 65537$ sont premiers. Mais $x_5 = 641 \times 6700417$ ne l'est pas.

2) Montrer que si $n \neq m$ sont non nuls alors x_n et x_m sont premiers entre eux (on pourra considérer un diviseur premier commun à x_m que x_n ou alors, comme dans la question d, factoriser $x_n - 2 = 2^{2^n} - 1$). En déduire qu'il existe une infinité de nombres premiers.

3) Montrer que $x_{n+1} = (x_n - 1)^2 + 1$ pour $n \geq 0$.

4) En déduire que, pour $n \geq 1$,

$$x_n - 2 = \prod_{k=0}^{n-1} x_k \,.$$

En particulier, on obtient que $x_m \mid x_n - 2$ si $m < n$. Retrouver le résultat de la question b à savoir x_m et x_n sont premiers entre eux pour $n \neq m$ non nuls.

Dans les questions e et f , on considère $n \geq 1$ et p un diviseur premier de x_n. On suppose que $p \neq x_n$.

5) Montrer que $p = 2^{n+1}m + 1$ où m admet un diviseur premier impair.

6) Montrer que 2 est un carré modulo p. En déduire que $p = 2^{n+2}m + 1$. On pourra utiliser le calcul du symbole de Legendre

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \qquad et \qquad \left(\frac{2}{p}\right) = 2^{(p-1)/2}[p] \,.$$

Exercice 27 – Nombres de Carmichael
[Dem97, Propositions 3.25 et 3.27] On utilisera librement le fait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. Un entier n non premier est dit de Carmichael si $a^{n-1} = 1\ [n]$ pour tout entier a premier à n.

1) Montrer qu'un nombre de Carmichael est sans facteur carré (regarder n modulo p^{k-1} si $n = p^k m$ avec $\text{pgcd}(m, p) = 1$) et produit d'au moins trois nombres premiers impairs.

2) Soit n un entier naturel supérieur strictement à 1. Montrer l'équivalence des propositions suivantes :

(i) n est de Carmichael

(ii) Pour tout entier a, on a $a^n = a\,[n]$.

(iii) n n'est pas premier, n est sans facteur carré et $p - 1$ divise $n - 1$ pour tout diviseur premier p de n.

3) Montrer que 561 est de Carmichael (c'est le plus petit nombre de Carmichael).

3 Propriétés arithmétiques des anneaux.

3.1 Divisibilité.

Exercice 28 – Divisibilité
Soient A un anneau commutatif (on ne suppose pas A intègre) et $a, b \in A$.

1) Montrer que les propriétés suivantes sont équivalentes

(i) il existe $c \in A$ tel que $ca = b$;

(ii) $b \in (a)$;

(iii) $(b) \subset (a)$;

Si ces conditions sont vérifiées, on dit que a *divise* b et on écrit $a \mid b$. On dit que a et b sont *associés* si $a \mid b$ et $b \mid a$

2) Montrer que a et b sont associés si et seulement si $(a) = (b)$. Montrer que être associés est une relation d'équivalence sur A.

On dit que a et b sont *fortement associés* s'il existe $u \in A^\times$ tel que $b = ua$.

3) Montrer que être fortement associés est une relation d'équivalence.

4) Montrer que des éléments fortement associés sont associés.

5) Montrer que dans un anneau intègre des éléments associés sont fortement associés.

6) Donner un exemple d'éléments associés qui ne sont pas fortement associés (on pourra considérer l'anneau $\mathbb{Q}[X, Y, Z, T]/(X - YZ, Y - TX)$).

Exercice 29 – Élement premier, élément irréductible
Soit A un anneau commutatif.

1) Soit $p \in A$. Montrer l'équivalence des deux propriétés suivantes

(i) p est non nul non inversible et si $p \mid ab$ alors $p \mid a$ ou $p \mid b$;

(ii) (p) est un idéal premier non nul.

Un élément vérifiant ces propriétés est appelé *élément premier de* A.

2) Soit $p \in A$. On suppose que A est **intègre**. Montrer l'équivalence des deux propriétés suivantes

(i) p est non inversible et si $p = ab$ alors a est inversible ou b est inversible ;

(ii) (p) est non nul et maximal parmi les idéaux de A qui sont principaux et distincts de A.

Un élément vérifiant ces propriétés est appelé *élément irréductible de* A.

3) Déterminer les éléments premiers (resp. irréductible) d'un corps, de $\mathbb{Z}$, $k[T]$.

4) Montrer que T est un élément premier de $A[T]$ si et seulement si A est intègre.

5) Montrer qu'un élément premier est toujours irréductible (si A est intègre).

6) Montrer que dans un anneau principal, un élément irréductible est premier.

Exercice 30 – PPCM et PGCD
[Dem97, Chapitre VII] Soit A un anneau commutatif. On ne suppose pas pour l'instant A intègre.

1) Soient $a_1, \ldots, a_m \in A$. On dit que $d \in A$ est un ppcm de $a_1, \ldots, a_m$ si d vérifie les deux conditions suivantes

(i) $a_i \mid d$ pour tout $i \in \{1, 2, \ldots, m\}$ (i.e. d est un multiple commun des a_i) ;

(ii) pour tout $d' \in A$ vérifiant $a_i \mid d'$, on a $d \mid d'$ (i.e. d est "le" plus petit multiple commun).

2) Soient $a_1, \ldots, a_m \in A$. On dit que $d \in A$ est un pgcd de $a_1, \ldots, a_m$ si d vérifie les deux conditions suivantes

(i) $d \mid a_i$ pour tout $i \in \{1, 2, \ldots, m\}$ (i.e. d est un diviseur commun des a_i) ;

(ii) pour tout $d' \in A$ vérifiant $d' \mid a_i$, on a $d' \mid d$ (i.e. d est "le" plus grand diviseur commun).

Des éléments $a_1, \ldots, a_m$ dont le pgcd est 1 sont dit premiers entre eux.
Attention ppcm **et** pgcd **n'existent pas forcément (voir l'exercice 38).**

3) Montrer que $a_1, \dots, a_m \in A$ admet un ppcm si et seulement si l'idéal $(a_1) \cap \dots \cap (a_m)$ est principal (on a ainsi un condition simple d'existence des ppcm : ce n'est pas le cas pour les pgcd).

4) On suppose que l'idéal $(a_1, \dots, a_m)$ est principal. Montrer que $a_1, \dots, a_m$ admettent un pgcd et qu'on a une relation de Bézout. Montrer que dans $k[X, Y]$, X et Y ont 1 comme pgcd mais que l'idéal (X, Y) n'est pas principal.

5) Montrer que $a_1, \dots, a_m$ admettent un pgcd si et seulement si l'ensemble des idéaux **principaux** contenant $(a_1, \dots, a_m)$ admet un élément plus petit élément.

6) Montrer que dans un anneau principal ppcm et pgcd existent toujours et qu'on dispose de relation de Bézout pour le pgcd.

Dans toute la suite de l'exercice A est un anneau commutatif **intègre**.

7) Soit $a \neq 0$. Montrer que la famille $(a_1, \dots, a_n)$ admet un ppcm si et seulement si la famille $(aa_1, \dots, aa_n)$ en admet un. Donner le lien entre les deux ppcm.

8) Montrer que le résultat précédent n'est pas vrai pour les pgcd. Cependant, montrer qu'on a le résultat suivant : si le pgcd de la famille $(aa_1, \dots, aa_n)$ existe, montrer que celui de la famille $(a_1, \dots, a_n)$ existe et qu'on a la relation $\operatorname{pgcd}(aa_1, \dots, aa_n) = a \operatorname{pgcd}(a_1, \dots, a_n)$.

9) On suppose que x et y ont un ppcm. Montrer que $m \mid xy$. On écrit alors $xy = md$. Montrer que d est un pgcd pour x et y et que, pour tout $a \in A \setminus \{0\}$, $\operatorname{pgcd}(ax, ay)$ existe et vaut ad (avoir un ppcm implique avoir un pgcd).

10) Montrer que si x, y et d sont tel que ad soit un pgcd de ax et ay pour tout $a \in A \setminus \{0\}$ alors on peut définir m tel que $md = xy$ et m est un ppcm de x et y. En déduire que (avoir un pgcd n'implique pas avoir un ppcm).

11) Montrer que si l'idéal (x, y) est principal alors $(x) \cap (y)$ l'est.

12) On dit que x et y sont *fortement premiers entre eux* si x et y ont un ppcm qui est xy. Montrer que des éléments qui sont fortement premiers entre eux sont premiers entre eux mais que la réciproque n'est pas vraie.

13) Montrer que si x et y sont fortement premiers entre eux et si $x \mid yz$ alors $x \mid z$ (le lemme d'Euclide ou de Gauss est vrai dans un anneau intègre sous l'hypothèse fortement premier entre eux).

14) Montrer que dans un anneau factoriel, des éléments sont fortement premiers entre eux si et seulement si ils sont premiers entre eux. En déduire que des éléments fortement premier entre eux ne sont pas forcément étrangers.

15) Soit A un anneau intègre. Montrer l'équivalence des propriétés suivantes

(i) L'intersection de deux idéaux principaux de A est un idéal principal.

(ii) Tout couple d'éléments de A admet un ppcm.

(iii) Tout couple d'éléments de A admet un pgcd.

Si les conditions précédentes sont vérifiées alors les produits xy et $\operatorname{pgcd}(x, y) \operatorname{ppcm}(x, y)$ sont associés ; deux éléments sont premiers entre eux si et seulement si ils sont fortement premiers entre eux. Tout élément irréductible est premier.

16) Montrer qu'un anneau intègre est factoriel si et seulement si tout élément irréductible est premier et il n'existe pas de suite infinie $(x_i)_{i \in \mathbb{N}}$ telle que pour tout $i > 0$ on a $x_i \mid x_{i-1}$ et x_i n'est pas associé à x_{i-1}.

17) Montrer qu'un anneau intègre est factoriel si et seulement si toute suite croissante d'idéaux principaux est stationnaire et l'intersection de deux idéaux principaux est principal.

18) Montrer qu'un élément p est irréductible si et seulement si $\operatorname{pgcd}(a, p)$ existe et vaut 1 ou p pour tout $a \in A$.

19) Montrer qu'un élément irréductible p est premier si et seulement si $\operatorname{ppcm}(a, p)$ existe, pour tout $a \in A$.

3.2 Les différents types d'anneaux.

Definition 3 (Anneau factoriel)**.** Soit A un anneau. On dit que A est *factoriel* si

(i) A est intègre ;

(ii) **(Existence de la décomposition en irréductibles)** Tout élément non nul peut s'écrit comme un produit d'irréductible : si $a \neq 0$ il existe des éléments $(q_1, \dots, q_s)$ irréductibles dans A tel que $a = q_1 \cdots q_s$.

(iii) **(Unicité de la décomposition en irréductibles)** La décomposition d'un élément non nul et non inversible en facteurs irréductibles est unique à l'ordre près et à la multiplication par des inversibles près : si $q_1 \cdots q_m = q'_1 \cdots q'_s$ avec les q_i et q'_i irréductibles alors $s = m$ et il existe $\sigma \in \mathfrak{S}_m$ et des éléments $u_i \in A^\times$ tels que $q'_i = u_i q_{\sigma(i)}$.

Exercice 31 – Anneaux factoriels
Soit A un anneau intègre.

1) Démontrer l'équivalence des propositions suivantes

(i) A est factoriel ;

(ii) Tout élément non nul et non inversible possède une décomposition en produit d'irréductibles. Tout élément irréductible est premier ;

(iii) Tout élément non nul et non inversible est produit d'éléments premiers.

(iv) Tout élément non nul et non inversible possède une décomposition en produit d'irréductibles. L'anneau A vérifie le lemme de Gauss : si $a \mid bc$ et a premier avec b alors $a \mid c$.

Dans un anneau intègre, on appelle système de représentants des éléments premiers un ensemble $\mathcal{S}$ d'éléments premiers de A tel que tout élément premier à A soit associé à un élément et un seul.

2) Donner des systèmes de représentants des éléments premiers de $\mathbb{Z}$ et $k[X]$.

3) Soit A un anneau factoriel et $\mathcal{S}$ un système de représentants des éléments premiers de A. Montrer que tout élément $a \in A$ **non nul** s'écrit de manière unique sous la forme

$$a = u_a \prod_{p \in \mathcal{S}} p^{\nu_p}(a)$$

où $u_a \in A^\times$, $\nu_p(a) \in \mathbb{N}$ et $\nu_p(a) = 0$ sauf pour un nombre fini d'éléments $p \in \mathcal{S}$. De plus $\nu_p(a)$ ne dépend pas du choix de p et de a dans leur classe pour la relation "être associé". L'entier $\nu_p(a)$ s'appelle la *multiplicité de p dans a.*

4) Soit A un anneau factoriel et $\mathcal{S}$ un système de représentants des éléments premiers de A et $K = \mathrm{Frac}(A)$. Montrer que tout élément $x \in K$ **non nul** s'écrit de manière unique sous la forme

$$x = u_a \prod p \in \mathcal{S} p^{\nu_p}(a)$$

où $u_a \in A^\times$, $\nu_p(a) \in \mathbb{Z}$ et $\nu_p(a) = 0$ sauf pour un nombre fini d'éléments $p \in \mathcal{S}$. En déduire que $K^\times \cong_{gr.} A^\times \times \mathbb{Z}^{(\mathcal{S})}$. En déduire que $\mathbb{F}_3(X)^\times$ et $\mathbb{Q}^\times$ sont isomorphes.

5) Soit A un anneau factoriel et $a, b, c \in A$ non nuls avec a et b premiers entre eux. Montrer que si $a \mid c$ et $b \mid c$ alors $ab \mid c$.

6) Soit A un anneau factoriel, $\mathcal{S}$ un système de représentant des éléments premiers de A et $a, b \in A$ non nuls. Montrer que

(i) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$;

(ii) $a \mid b \quad \iff \quad \forall p \in \mathcal{S}, \quad \nu_p(a) \leq \nu_p(b)$;

(iii) $\prod p \in \mathcal{S} p^{\min(\nu_p(a), \nu_p(b))}$ est un pgcd de a et b ;

(iv) $\prod p \in \mathcal{S} p^{\max(\nu_p(a),\nu_p(b))}$ est un ppcm de a et b.

Exercice 32 – Anneaux principaux
Soit A un anneau. Un anneau *intègre* est un anneau **commutatif** non réduit à 0 tel que $xy \neq 0$ implique $x \neq 0$ ou $y \neq 0$. Un anneau *p*rincipal est un anneau **intègre** tel que tout idéal est principal.

1) Montrer que dans un anneau principal, tout idéal premier **non nul** est maximal.

2) Montrer que dans un anneau principal, ppcm et pgcd existent toujours.

3) Montrer qu'un anneau principal est factoriel.

Exercice 33 – Anneaux euclidiens
Soit A un anneau euclidien est un *intègre* tel qu'il existe une fonction appelée stathme $\varphi : A \setminus \{0\} \to \mathbb{N}$ telle que pour tout $a, b \in A \times A \setminus \{0\}$, il existe $q, r \in A$ tel que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$

1) Dans un anneau euclidien, écrire un algorithme d'Euclide étendu permettant le calcul d'une relation de Bézout.

2) Montrer qu'un anneau euclidien est principal.

3) Montrer que $k[X]$ et $\mathbb{Z}$ sont euclidiens.

Exercice 34 – Quelques idéaux non principaux

1) Montrer que 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$ mais que 1 n'est pas dans l'idéal $(2, X)$.

2) Montrer que $(2, X)$ n'est pas un idéal principal de $\mathbb{Z}[X]$.

3) Montrer que (X, Y) n'est pas un idéal principal de $A[X, Y]$.

4) Montrer que (X) est un idéal premier de $K[X, Y]$. Quel est le quotient ?

5) Parmi les idéaux $(2X)$, (X, Y) et $(2, X, Y)$ de $\mathbb{Z}[X, Y]$, lesquels sont premiers ? maximaux ?

6) Soit $a \in A$. Montrer que $A[X]/(X - a)$ est isomorphe à A.

Exercice 35 – Corps et propriétés arithmétiques
Soit k un corps.

1) Montrer que k est un anneau euclidien. Déterminer un stathme et la division euclidienne.

2) Montrer que k est un anneau principal.

3) Montrer que k est un anneau factoriel. Quels sont les éléments irréductibles de k ?

Exercice 36 – Anneau factoriel VS anneau principal
[Per81, Chapitre II Exercices 3.6 et 5.2, Corollaire 3.21]

1) Soit A un anneau principal. Montrer que A est factoriel.

2) Soit A un anneau factoriel tel que tout idéal de type fini est principal. Montrer que A est principal.

3) Soit A un anneau intègre et noethérien tel que tout idéal maximal est principal. Montrer que A est principal (on pourra d'abord montrer que A est factoriel).

4) Montrer que $\mathbb{Z}[X]$ et $k[X, Y]$ sont factoriels mais non principaux. Donner un exemple d'anneau factoriel non noethérien (et donc non principal).

Exercice 37 – Anneaux principaux et intégrité

1) Montrer que tout idéal de $\mathbb{Z}/n\mathbb{Z}$ est principal et que si n n'est pas premier alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal.

2) Généraliser au cas d'un quotient d'un anneau principal quelconque.

3) Montrer que tout idéal de $\mathbb{Z}^2$ est principal et mais $\mathbb{Z}^2$ n'est pas principal.

4) Généraliser à un produit d'anneaux principaux.

Exercice 38 – Un anneau intègre non factoriel
[Per81, Chapitre II Exercice 3.4] [Dem97, Exercice 6.20] Soit $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}, \quad a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

1) Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un sous-anneau de $\mathbb{C}$. Montrer qu'il est intègre (et noethérien).

2) Déterminer le groupe des éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{5}]$. On pourra introduire l'application

$$N : z = a + ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}] \longmapsto z\overline{z} = a^2 + 5b^2 \in \mathbb{Z}\,.$$

3) Montrer que $p = 2 + i\sqrt{5}$ est irréductible et que (p) n'est pas premier. En déduire que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

4) Montrer que 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm et que 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd dans $\mathbb{Z}[i\sqrt{5}]$.

Exercice 39 – Un autre exemple d'anneau intègre non factoriel
Soit k un corps.

1) Montrer que l'ensemble $A = \{P \in k[T], P'(0) = 0\}$ est un sous-anneau de $k[T]$.

2) Montrer que $A = k[T^2, T^3]$ et que $A = k[X, Y]/X^3 - Y^2$. En déduire que A est noethérien.

3) Montrer que T^2 et T^3 sont irréductibles dans A. Sont-ils premiers dans A ? En déduire que A n'est pas factoriel.

4) Donner deux factorisations en irréductibles de T^6 dans A. Retrouver le fait que A n'est pas factoriel.

5) Exhiber un idéal non principal de A.

Exercice 40 – Éléments associés et intégrité
On considère l'anneau $A = \mathbb{Z}[X, Y, Z, T]/(X - ZY, Y - XT)$. On note x, y les classes de X et Y dans A. Montrer que x et y sont associés mais qu'il n'existe pas d'élément inversible u tel que $xu = y$ (voir un autre exemple dans [Per81, Remarque II.3.7]).

Exercice 41 – Arithmétique des anneaux de polynômes
[FGN01, Exercice 3.9] Soit A un anneau commutatif unitaire.

1) Montrer l'équivalence des trois propriétés suivantes

(i) A est un corps ;

(ii) $A[X]$ est un anneau euclidien ;

(iii) $A[X]$ est un anneau intègre.

2) On suppose que A est un anneau euclidien qui n'est pas un corps vérifiant pour tout $(a, b) \in A \times A \setminus \{0\}$ il existe un **unique** couple (q, r) tel que $a = bq + r$ et $r = 0$ ou $\nu(r) < \nu(b)$ (unicité de la division euclidienne). Montrer qu'il existe un corps k tel que $A = k[X]$.

Exercice 42 – Le théorème des deux carrés
[Per81, Chapitre II.6] Soit $\mathbb{Z}[i] = \{a + ib, \quad a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

1) Montrer que c'est un sous-anneau de $\mathbb{C}$ appelé l'*anneau des entiers de Gauss*.

2) On définit l'application norme

$$\begin{aligned} N\colon \mathbb{Z}[i] &\longrightarrow \mathbb{N} \\ z &\longmapsto z\overline{z}\,. \end{aligned}$$

Montrer que N est une fonction multiplicative puis déterminer les inversibles de l'anneau $\mathbb{Z}[i]$.

3) Montrer que $\mathbb{Z}[i]$ est euclidien.

4) Montrer si m et n sont tous deux sommes de deux carrés d'entiers, alors mn est somme de deux carrés également.

5) Soit p un entier premier. Montrer que p est une somme de deux carrés si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

6) à SAVOIR FAIRE ABSOLUMENT. Soit p un entier premier. Montrer que les anneaux $\mathbb{Z}[i]/(p)$ et $\mathbb{F}_p[X]/(X^2+1)$ sont isomorphes. En déduire que p est irréductible dans dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

7) Soit p un entier premier. Déduire de ce qui précède que p est une somme de deux carrés si et seulement si $p = 1$ ou 2 [4].

8) Démontrer le théorème des deux carrés : soit n un entier naturel et

$$n = \prod_p p^{v_p(n)}$$

sa décomposition en facteurs premiers. Alors n est somme de deux carrés d'entiers si et seulement si $v_p(n)$ est pair pour tout entier premier p tel que $p = 3$ [4].

Exercice 43 – L'anneau $\mathbb{Z}[\sqrt{n}]$

Soit $n \in \mathbb{Z}$ un entier qui n'est pas un carré. On note $x \in \mathbb{C}$ une racine du polynôme $X^2 - n$.

1) Montrer que $\mathbb{Q}[x] := \{a + bx \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$ de dimension 2 sur $\mathbb{Q}$ et isomorphe à $\mathbb{Q}[X]/X^2 - n$ via le morphisme d'évaluation en x. En déduire que l'écrire sous la forme $a + bx$ détermine a et b.

2) On définit l'application

$$\begin{aligned} \sigma : \quad \mathbb{Q}[x] &\longrightarrow \mathbb{Q}[x] \\ a + bx &\longmapsto a - bx. \end{aligned}$$

Montrer que l'application σ est un automorphisme de $\mathbb{Q}$-algèbre. Calculer son inverse.

3) On désigne par $\mathbb{Z}[x] := \{a + bx, a, b \in \mathbb{Z}\}$. Montrer que $\mathbb{Z}[x]$ est un sous-anneau de $\mathbb{Q}[x]$ et que σ induit par restriction un isomorphisme de $\mathbb{Z}[x]$.

4) Pour $z = a + bx \in \mathbb{Q}[x]$, on pose $N(z) = z\sigma(z) = a^2 - b^2 n$. Montrer que $N(zz') = N(z)N(z')$ pour tous $z, z' \in \mathbb{Q}[x]$.

5) Montrer que $N(z) = 0$ si et seulement si $z = 0$.

6) Montrer que si $z \in \mathbb{Z}[x]$ alors $N(z) \in \mathbb{Z}$.

7) Montrer que si $z \in \mathbb{Z}[x]$ alors z est inversible dans $\mathbb{Z}[x]$ si et seulement si $N(z) \in \{-1, 1\}$.

8) Montrer qu'il existe une décomposition en irréductible dans $\mathbb{Z}[x]$.

9) Dans le cas où $n = -5$, montrer que $\mathbb{Z}[x]$ n'est pas factoriel : on pourra considérer $6 = 2 \cdot 3 = (1-x)(1+x)$. Déterminer les inversibles de $\mathbb{Z}[x]$. Trouver un idéal non principal de $\mathbb{Z}[x]$.

10) Dans le cas où $n = -1$, montrer que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien pour la fonction N (pour effectuer la division euclidienne de a par b dans $\mathbb{Z}[i]$, on pourra considérer le quotient ab^{-1} dans $\mathbb{Q}[i]$ et choisir l'élément de $\mathbb{Z}[i]$ le plus proche : on fera un dessin). Déterminer les inversibles de $\mathbb{Z}[i]$.

11) Montrer que le résultat de la question précédente s'étend au cas où $n = -2$, $n = 2$ et $n = 3$.

Exercice 44 – Irréductibilité de polynômes

Soit A un anneau intègre.

1) Montrer que a et b n'ont pas de diviseur commun alors $aX + b$ est irréductible dans $A[X]$.

2) Montrer que si les éléments a, b, c n'ont pas de diviseur commun et si $b^2 - 4ac$ n'est pas un carré dans R alors le polynôme $aX^2 + bX + c$ est irréductible dans $A[X]$.

3) Montrer que la réciproque à la question précédente est vrai si A est factoriel et 2 est inversible dans R.

4) Soit K un corps. On note $M = (X_{ij}) \in \mathrm{Mat}_n(K[X_{ij}, i, j])$ la matrice de taille $n \times n$ dont les coefficients sont des indéterminées. Montrer que $\det M$ est un élément irréductible de $K[X_{ij}, i, j]$.

5) Montrer que χ_M est un élément irréductible de $\mathbb{Z}[X, X_{ij}, i, j]$.

6) On écrit $P = P_0 + \cdots + P_d \in A[X_1, \ldots, X_n]$ où les P_i sont les composantes homogènes de P (où A est factoriel). Monter que si P_d est irréductible alors P l'est. Montrer que si $P = P_{d-1} + P_d$ avec P_d et P_{d-1} sont non nuls et sans facteurs communs alors P est irréductible. On suppose que $P = P_{d-2} + P_d$ avec P_d et P_{d-2} sont non nuls et sans facteurs communs et d est impair alors P est irréductible. Trouver un contre-exemple si d est pair.

L'exercice suivant est un critère préparatoire à l'exercice 46.

Exercice 45 – Une condition nécessaire sur un anneau pour qu'il soit euclidien
[Per81, Proposition II.5.1] Soit A un anneau euclidien. Montrer qu'il existe $x \in A \setminus A^\times$ tel que la restriction de la surjection naturelle $\pi : A \to A/(x)$ à $A^\times \cup \{0\}$ est surjective. Montrer qu'alors $A/(x)$ est un corps.

Exercice 46 – Un exemple d'anneau principal non euclidien
[Per81, Chapitre II.5] On considère le sous-anneau A de $\mathbb{C}$ engendré par $\alpha := (1 + i\sqrt{19})/2$:

$$A = \mathbb{Z}[\alpha] = \{P(\alpha), \quad P \in \mathbb{Z}[X]\}.$$

Le but de cet exercice est de démontrer que A n'est pas euclidien, puis de démontrer que A est principal en utilisant une "division euclidienne affaiblie".

1) Vérifier que $\alpha^2 - \alpha + 5 = 0$. Montrer que $A = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$.

2) Montrer que A est stable par conjugaison. On définit $N(z) = z\overline{z}$ pour $z \in A$. à l'aide de N, décrire $A^\times$.

3) Montrer que A n'est pas euclidien (utiliser le critère de l'exercice 45).

4) Soient $z, z' \in A$ non nuls. Montrer qu'il existe $q, r \in A$ vérifiant les deux conditions suivantes :

(i) $N(r) < N(z')$,

(ii) $z = z'q + r$ ou $2z = z'q + r$.

(on pourra écrire $z/z' = u + v\alpha$ avec $u, v \in \mathbb{Q}$, soit $n = E(v)$ et discuter selon que $v \in \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$ ou pas).

5) Montrer que (2) est un idéal maximal de A (on pourra vérifier que $A \cong_{ann.} \mathbb{Z}[X]/(X^2 - X + 5)$).

6) Montrer que A est principal.

Exercice 47 – Séries formelles
soit k un corps. Montrer que $k[[X]]$ est un anneau euclidien.

Exercice 48 – Critère d'Eisenstein
Soit A un anneau factoriel, $P \in A[X]$ avec $P = a_nX^n + \cdots + a_0$ $(a_n \neq 0)$ et $p \in A$ un irréductible. On suppose que $p \nmid a_n$, $p \mid a_i$ pour tout $i \in \{0, 1, \ldots, n-1\}$ et $p^2 \nmid a_0$. L'objectif est de montrer que P est irréductible sur $\mathrm{Frac}(A)[X]$.

1) On suppose que P n'est pas irréductible sur $\mathrm{Frac}(A)[X]$. Montrer qu'on peut écrire $P = QR$ avec $\deg Q < \deg P$ et $\deg R < \deg P$ et $QR \in A[X]$.

2) Montrer que Q et R ont tous leurs coefficients sauf le coefficient dominant qui sont divisibles par p (on pourra réduire modulo p l'égalité $P = QR$).

3) Obtenir une contraction en considérant le coefficient de plus bas degré de P.

4) En déduire que si P est primitif alors P est irréductible sur $A[X]$.

5) Donner un exemple où P n'est pas primitif. En déduire que le critère d'Eisenstein ne donne pas l'irréductibilité dans $A[X]$.

Exercice 49 – Application du critère d'Eisenstein

1) Soit P un nombre premier. Montrer que $P(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ est irréductible sur $\mathbb{Q}$ (considérer $P(X+1)$)

2) Montrer que $X^n - 2$ est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

3) Soit A un anneau factoriel de caractéristique différentes de 2, $n \in \mathbb{N}$ et $n \geq 2$. Montrer que ${X_1}^2 + \cdots + {X_n}^2 - 1$ est irréductible dans $A[X_1, \ldots, X_n]$. Que se passe-t-il en caractéristique 2 ?

4 Le théorème chinois.

Definition 4 (Idéaux étrangers)**.** Soit A un anneau commutatif unitaire. Pour deux idéaux I et J de A, on dit que I et J sont *étrangers* si $I + J = A$ où $I + J = \{i + j \in A, \quad i \in I, j \in J\}$. Autrement dit I et J sont étrangers si et seulement si il existe $i \in I$ et $j \in J$ tel que $i + j = 1$.

Exercice 50 – Idéaux étrangers
Soit A un anneau commutatif unitaire et $I_1, \ldots, I_k$ des idéaux de A.

1) On suppose que les idéaux I_i pour $1 \leq i \leq k$ sont deux à deux étrangers. Montrer que I_1 est étranger avec $I_2 \cdots I_k$.

2) Montrer que pour tout $m, n \in \mathbb{N}$, les idéaux ${I_1}^m$ et ${I_2}^n$ sont étrangers (au fait c'est quoi ${I_1}^m$?).

3) Soit $\mathfrak{m}$ et $\mathfrak{m}'$ deux idéaux maximaux **distincts** de A. Montrer qu'ils sont étrangers. En déduire que $\mathfrak{m}^m$ et $\mathfrak{m}'^n$ sont étrangers pour tous $m, n \in \mathbb{N}$.

Exercice 51 – Théorème chinois
Soient A un anneau commutatif unitaire et I et J deux idéaux de A. On note $\pi_I : A \to A/I$ et $\pi_J : A \to A/J$ les surjections canoniques. On définit l'application

$$\begin{aligned} \varphi \colon A &\longrightarrow A/I \times A/J \\ x &\longmapsto (\pi_I(x), \pi_J(x)) \end{aligned}$$

1) Vérifier que φ est un morphisme d'anneaux.

2) Calculer $\ker \varphi$.

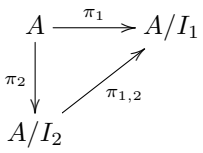
3) Montrer que φ est surjectif si seulement si I et J sont étrangers. Construire explicitement un antécédent de $(a, b) = (\pi_I(x), \pi_J(y)) \in A/I \times A/J$.

4) On définit $IJ := \{\sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N}, i_k \in I, j_k \in J\}$. Montrer que $IJ \subset I \cap J$. Donner un exemple où $IJ \subsetneq I \cap J$.

5) On suppose que I et J sont étrangers. Montrer que $I \cap J = IJ$.

6) Conclure que si I et J sont étrangers alors φ induit un isomorphisme entre A/IJ et $A/I \times A/J$ donné par $\overline{x} \mapsto (\pi_I(x), \pi_J(x))$ où $\overline{x}$ désigne la classe de $x \in A$ modulo IJ.

7) Soit $I_2 \subset I_1$ deux idéaux d'un anneaux commutatif unitaire. Pour $i \in \{1,2\}$, on note $\pi_i : A \to A_{I_i}$ les surjections canoniques. Montrer que l'application π_1 passe au quotient par π_2 i.e. construire un morphisme $\pi_{1,2} : A/I_2 \to A/I_1$ tel que le diagramme suivant commute :



La commutativité du diagramme s'écrit aussi : à la classe de x modulo I_2, on associe la classe de x modulo I_1. Par exemple, comme $4\mathbb{Z} \subset 2\mathbb{Z}$, on peut parler de la classe modulo 2 d'un élément de $\mathbb{Z}/4\mathbb{Z}$.

8) Réécriture du théorème chinois. Vérifier que le lemme chinois s'écrit $y \in A/IJ \mapsto (\pi_{I,IJ}(y), \pi_{J,IJ}(y))$ est un isomorphisme.

Exercice 52 – Lorsqu'il a plusieurs idéaux
Soient A un anneau commutatif unitaire et $I_1, \dots, I_k$ des idéaux de A deux à deux étrangers. Montrer que l'application

$$\begin{aligned} \varphi\colon A &\longrightarrow A/I_1 \times \cdots \times A/I_k \\ x &\longmapsto (\pi_1(x), \dots, \pi_k(x)) \end{aligned}$$

est surjective de noyau $I_1 \cdots I_k$ et induit un isomorphisme entre $A/I_1 \cdots I_k$ et $A/I_1 \times \cdots \times A/I_k$.

Remarque : *La démonstration se fait évidemment par récurrence sur k. Cela donne ainsi une méthode pour la résolution de système de congruence (pour des idéaux étrangers) à plus de deux équations : en appliquant la question c de l'exercice 51, on remplace les deux premières équations par une équation de congruence modulo le produit des idéaux. On réduit ainsi le nombre d'équations. La question a de l'exercice 53 propose un exemple concret d'application de cette méthode.*

Exercice 53 – Théorème chinois
Résoudre dans $\mathbb{Z}$ le système d'équation

1) $\begin{cases} x = 1\,[3] \\ x = 4\,[5] \\ x = 0\,[7] \end{cases}$

2) $\begin{cases} x = 4\,[15] \\ x = 8\,[21] \end{cases}$

3) $\begin{cases} x = 11\,[15] \\ x = 8\,[21] \end{cases}$

4) Trouver dans $\mathbb{Z}/7\mathbb{Z}[X]$ les polynômes tel que $f(0) = 3$, $f(1) = 0$ et $f(2) = 6$.

5) Interpréter les problèmes d'interpolations de Lagrange et d'Hermite comme des problèmes de congruence. En déduire l'existence et l'unicité de leur solution.

6) Un algorithme de recherche de solutions d'un système de congruence dans un anneau euclidien. On considère le système d'équation

$$\begin{cases} x = b_1 \mod (a_1) \\ \quad \vdots \\ x = b_n \mod (a_n) \end{cases}$$

où les a_i sont premiers entre eux deux à deux. Décrire un algorithme de construction de solutions sous la forme

$$x = \gamma_1 + \gamma_2 a_1 + \cdots + \gamma_k a_1 a_2 \cdots a_{k-1}$$

où les γ_i sont à calculer. Expliquer pour l'intérêt de cette méthode est de permettre d'ajouter une équation au système de congruence sans qu'on ait besoin de faire tous les calculs. Pour les analystes numériciens, comment s'appelle cette méthode dans le cas de l'interpolation de Lagrange ? Est-ce que ça marche dans un anneau principal ?

Exercice 54 – Lemme chinois et algèbre linéaire
Soient k un corps, E un k-espace vectoriel de dimension finie et u un endomorphisme de E dont le polynôme caractéristique est scindé.

1) **Décomposition de Dunford.** Montrer qu'il existe des endomorphismes d et n de E avec d diagonalisable, n nilpotent, $u = d + n$ et $dn = nd$. Montrer que d et n sont des polynômes en u et qu'un tel couple est unique. On pourra considérer P un solution du système

$$\begin{cases} P = \lambda_1 & \mod (X - \lambda_1)^n \\ \quad \vdots & \\ P = \lambda_r & \mod (X - \lambda)^n \end{cases}$$

où les λ_i sont les valeurs propres distinctes de u.

2) Montrer que les projecteurs sur un sous-espace caractéristique de u parallèlement aux autres sous-espaces caractéristiques de u sont des polynômes en u. On pourra considérer P un solution du système

$$\begin{cases} P = 1 & \mod (X - \lambda_1)^n \\ P = 0 & \mod (X - \lambda_2)^n \\ \quad \vdots & \\ P = 0 & \mod (X - \lambda_r)^n \end{cases}$$

où les λ_i sont les valeurs propres distinctes de u.

Exercice 55 – Algèbre de dimension finie
Soit k un corps et A une k-algèbre commutative de dimension finie.

1) Montrer que A est intègre si et seulement si A est un corps (comparer avec le fait qu'un anneau commutatif fini est intègre si et seulement si un corps).

2) En déduire que tout idéal premier de A est un idéal maximal.

3) Montrer que A a un nombre fini d'idéaux maximaux (vérifier que si les $\mathfrak{m}_i$ sont des idéaux maximaux distincts, la suite d'idéaux $\prod j \leq i \mathfrak{m}_j$ est strictement décroissante). On note pour la suite $\mathcal{M} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ l'ensemble des idéaux maximaux de A.

4) Montrer que $J := \mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. En déduire que $x \in J$ si et seulement si $1 - ax$ est inversible pour $a \in A$.

5) Soit I un idéal de A. Montrer que $IJ = I$ implique $I = 0$ (on pourra considérer une partie génératrice minimale de l'idéal I).

6) En déduire qu'il existe $n \in \mathbb{N}$ tel que $J^n = 0$.

7) En déduire que A est isomorphe à un produit d'algèbre locale (i.e. avec un unique idéal maximal) de dimension finie.

8) Soit B un anneau commutatif unitaire quelconque. Montrer que tout élément nilpotent est dans tout idéal premier. Soit $f \in B$, à quelle condition l'ensemble des idéaux de B qui ne rencontre pas l'ensemble des puissances de f admet un élément maximal ? Montrer qu'un tel idéal est un idéal premier de B. En déduire que l'intersection des idéaux premiers de B est l'ensemble des éléments nilpotents de B.

9) En déduire que J est l'ensemble des éléments nilpotents de A. Retrouver le fait que $J^n = 0$ (attention au piège !).

10) Montrer que A est réduite (i.e. que le seul élément nilpotent de A est 0) si et seulement si A est un produit de corps.

5 Équations diophantiennes.

Exercice 56 – Equations linéaires
Trouver toutes les solutions entières de chacune des équations suivantes :

1) $19x + 11y = 3$,

2) $18x + 24y = 12$,

3) $37x + 17y = 5$,

4) $21x + 14y = 7$,

5) $1995x + 2793y = 1596$

Exercice 57 – Systèmes d'équations linéaires
Résoudre les systèmes linéaires diophantiens suivants :

1)
$$\begin{cases} 4x - 2y - z = 5 \\ x + 3y - 4z = 7 \end{cases}$$

2)
$$\begin{cases} 3x + 2y - 5z = 2 \\ 2x + 6y - 10z = 4 \\ x + 2y - 3z = 2 \end{cases}$$

3)
$$\begin{cases} 2x - y + 2z = 1 \\ 5x - 3y + 3z = 2 \\ -x - 2z = 3 \end{cases}$$

Exercice 58 – Exemples d'équations diophantiennes non linéaires

1) Trouver toutes les solutions entières de l'équation $x^2 - y^2 = 459$.

2) L'équation $x^3 - y^2 = 2$:

(i) Montrer que $\mathbb{Z}[i\sqrt{2}]$ est euclidien.

(ii) Montrer que si (x, y) est une solution entière de l'équation $x^3 - y^2 = 2$, alors il existe $a, b \in \mathbb{Z}$ tels que $y + i\sqrt{2} = \left(a + ib\sqrt{2}\right)^3$. En déduire toutes les solutions entières de l'équation $x^3 - y^2 = 2$.

3) Sur les équations de Fermat. [Sam67]

(i) Trouver toutes les solutions entières de l'équation $x^2 + y^2 = z^2$. (Indication : on pourra d'abord se ramener au cas où $x > 0$, $y > 0$, $z > 0$, $\text{pgcd}(x, y) = 1$ et x est pair).

(ii) Soient x, y, z des entiers tels que $xyz \neq 0$ et $x^4 + y^4 = z^2$. à l'aide de la question précédente montrer qu'il existe x', y', z' des entiers tels que $x'y'z' \neq 0$, $|z'| < |z|$ et $x'^4 + y'^4 = z'^2$. En déduire qu'il n'existe pas d'entiers x, y, z tels que $xyz \neq 0$ et $x^4 + y^4 = z^4$.

Exercice 59 – Le théorème de la base adaptée : sous-module donné par une partie génératrice
Dans chacun des cas suivants, déterminer les facteurs invariants, une paire de base adaptées ainsi que des équations du sous-module de $\mathbb{Z}^n$ engendré par les vecteurs e_i :

1) $n = 5$, $e_1 = \begin{bmatrix} -1 \\ -4 \\ 1 \\ 2 \\ -4 \end{bmatrix}$, $e_2 = \begin{bmatrix} -2 \\ 3 \\ 1 \\ 5 \\ -3 \end{bmatrix}$, $e_3 = \begin{bmatrix} -5 \\ 3 \\ 5 \\ -3 \\ 3 \end{bmatrix}$.

2) $n=5$, $e_1=\begin{bmatrix}-5\\4\\-6\\-6\\-3\end{bmatrix}$, $e_2=\begin{bmatrix}-6\\6\\-12\\-6\\-6\end{bmatrix}$, $e_3=\begin{bmatrix}-3\\3\\-6\\-3\\-3\end{bmatrix}$.

3) $n=4$, $e_1=\begin{bmatrix}-3\\5\\-2\\0\end{bmatrix}$, $e_2=\begin{bmatrix}0\\-2\\0\\-2\end{bmatrix}$, $e_3=\begin{bmatrix}3\\11\\0\\8\end{bmatrix}$.

4) $n=4$, $e_1=\begin{bmatrix}-1\\0\\0\\1\end{bmatrix}$, $e_2=\begin{bmatrix}-7\\12\\-9\\7\end{bmatrix}$, $e_3=\begin{bmatrix}10\\-9\\9\\-10\end{bmatrix}$, $e_4=\begin{bmatrix}-6\\12\\-9\\6\end{bmatrix}$.

Exercice 60 – Théorème de la base adaptée : sous-module donné par des équations
Résoudre les systèmes linéaires suivants. Dans chaque cas, donner une base adaptée pour l'espace des solutions.

1)
$$\begin{cases}-4x+2y+3z+3t+4u=0\\5x-y-3z-3t+7u=0\\-4x+2z+2t-7u=0\\-x+y+z+t+6u=0\end{cases}$$

2)
$$\begin{cases}x+3y-2z+3t=0\\x+3y-8z+9t=0\\2y+4z-4t=0\end{cases}$$

3)
$$\begin{cases}-3x-4y+3z=0\,[6]\\-9y+9z=0\,[6]\\3x+12y-12z=0\,[6]\end{cases}$$

en notant $S\subset\mathbb{Z}^3$ l'espace des solutions, montrer que $\mathbb{Z}^3/S$ est fini et calculer son cardinal.

4)
$$\begin{cases}-5x-7y-2z+5t=0\,[6]\\-21x+19y-10z+7t=0\,[6]\\-13x+3y-6z+7t=0\,[6]\end{cases}$$

6 Polynômes.

Proposition 1 (Propriété universelle des polynômes)**.** *Soit (B,ρ) une A-algèbre commutative et $b_1,\dots,b_n\in B$. Il existe un unique morphisme φ de A-algèbres de $A[X_1,\dots,X_n]$ dans B tel que $\varphi(X_i)=b_i$.*
Il est donné par

$$\varphi\left(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n}a_{i_1,\dots,i_n}{X_1}^{i_1}\cdots{X_n}^{i_n}\right)=\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n}a_{i_1,\dots,i_n}{b_1}^{i_1}\cdots{b_n}^{i_n}$$

φ est appelé le morphisme d'évaluation en les b_i.

Exercice 61 – Fonctorialité
Soit A, B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneau.

1) Montrer que f s'étend en un morphisme de A-algèbres de $A[[X]]$ sur $B[[X]]$ envoyant X sur X.

2) Montrer de même que f s'étend de façon unique en un morphisme de A-algèbres de $A[X_1, \ldots, X_n]$ sur $B[X_1, \ldots, X_n]$ envoyant X_i sur X_i.

3) En déduire que si I est un idéal de A, on a un morphisme surjectif de $A[X]$ dans $(A/I)[X]$. Quel est le noyau (le comparer à l'idéal engendré par I dans $A[X]$) ?

Exercice 62

1) Montrer que $1 + X$ est inversible dans $A[[X]]$.

2) Montrer que $1 + X$ est un carré dans $\mathbb{Q}[[X]]$.

3) Soit k un corps. Déterminer les idéaux de $k[[X]]$.

Exercice 63
Déterminer le nombre de monômes de $A[X_1, \ldots, X_n]$ de degré total m.

Exercice 64
Soit K un corps. À quelle condition sur la famille a_i l'endomorphisme de A-algèbre de $K[X_1, \ldots, X_n]$donné par $X_1 \mapsto a_1 X_1$ et $X_i \mapsto X_i + a_i X_1$ est-il un automorphisme ?

Peut-on remplacer K par un anneau commutatif quelconque ?

Exercice 65
Soit $a = (a_1, \ldots, a_n) \in A^n$. Montrer que l'ensemble des polynômes $P \in A[X_1, \ldots, X_n]$ tel que $P(a) = 0$ est l'idéal engendré par les $X_i - a_i$.

Exercice 66
Montrer que $A[X, Y]/\langle Y^3 - X^2 \rangle$ est isomorphe à la sous-A-algèbre de $A[T]$ formé des polynômes dont le coefficient en T est 0 (on pourra montrer que cette dernière algèbre est engendré par T^2 et T^3).

Exercice 67 – Racines d'un polynôme

1) On considère le corps (ou plutôt l'anneau à division) des quaternions $\mathbb{H}$. Montrer que le polynôme $X^2 + 1$ a au moins trois racines (et même une infinité).

2) On considère l'anneau commutatif non intègre $A = k[X]/X^2$ où k est un corps infini. Montrer que le polynôme T^2 de $A[T]$ admet une infinité de racines.

Exercice 68
Trouver $P \in \mathbb{Z}[U, V, W]$ tel que

$$P(X + Y + Z, XY + YZ + XZ, XYZ) = X^2Y^2 + X^2Z^2 + Y^2Z^2 + X^2YZ + Y^2XZ + Z^2XY.$$

Exercice 69 – Division euclidienne et polynômes
Soit A un anneau commutatif unitaire et $P, Q \in A[X]$ où Q est un polynôme à coefficient dominant inversible.

1) Montrer que la restriction de la surjection canonique induit une bijection ("A-linéaire") entre l'ensemble des polynômes de degré inférieur ou égal à n et $A[X]/(Q)$.

2) On suppose que $A = k$ est un corps. En déduire que $k[X]/(Q)$ est un espace vectoriel de dimension $\deg Q$ et de base $(\pi(1), \pi(X), \ldots, \pi(X^{\deg Q - 1}))$ où $\pi : k[X] \to k[X]/(Q)$ est la surjection canonique.

Exercice 70

1) Soit A un anneau commutatif. Déterminer les morphismes d'anneaux de $\mathbb{Z}[X]$ dans A.

2) Soit $f : A \to B$ un morphisme d'anneaux commutatifs vérifiant la propriété $\mathscr{P}$: si $g, h : B \to C$ sont des morphismes d'anneaux commutatifs vérifiant $f \circ g = f \circ h$ alors $g = h$. Montrer que f est injectif.

3) Montrer qu'un morphisme injectif vérifie la propriété $\mathscr{P}$.

4) Déterminer les automorphismes de $\mathbb{Z}[X]$.

Exercice 71

1) Montrer que $\mathbb{Z}[X]/(2, X)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

2) Soit $p \in \mathbb{Z}$ un nombre premier. Montrer que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_p[X]/(X^2 + 1)$.

3) En déduire que p est un élément premier de $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{F}_p$ si et seulement si $p = 3\,[4]$.

Exercice 72
Soit k un corps. Montrer que dans $k[X]$, il y a une infinité d'éléments irréductibles. L'argument marche-t-il pour $k[[X]]$?

Exercice 73 – Anneaux de polynômes
Soit A un anneau commutatif unitaire. Un élément de A est dit nilpotent s'il existe $n \geq 0$ tel que $x^n = 0$.

1) Montrer que l'ensemble $\mathfrak{n}$ des éléments nilpotents de A est un idéal de A et que $A/\mathfrak{n}$ n'a pas d'éléments nilpotents non nuls.

2) Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$. Montrer que P est un élément nilpotent de $A[X]$ si et seulement si tous les a_i sont des éléments nilpotents de A.

3) Soit x un élément nilpotent de A. Montrer que $1 + x$ est inversible dans A (on pourra chercher l'inverse sous forme de somme de puissance de x).

4) Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$. Montrer que P est inversible si et seulement si a_0 est inversible et a_i est nilpotent pour tout $i \geq 1$. Indication, on pourra montrer que ${a_n}^{r+1} b_{m-r} = 0$ pour tout r où les b_i sont les coefficients d'un inverse de P.

5) Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$. Montrer que P est un diviseur de 0 si et seulement si il existe $a \neq 0$ tel que $aP = 0$ (on pourra considérer Q non nul de degré minimal tel que $PQ = 0$ et montrer par récurrence décroissante que $a_i Q = 0$).

6) Montrer qu'un élément nilpotent est dans tous les idéaux premiers de A.

7) Montrer que $x \in A$ appartient à tous les idéaux maximaux de A si et seulement si, pour tout $a \in A$, l'élément $1 - ax$ est inversible dans A.

8) Montrer que l'intersection des idéaux maximaux de $A[X]$ est formée des éléments nilpotents de $A[X]$.

Exercice 74
Soit A un anneau factoriel et $P = a_n X^n + \cdots + a_0 \in A[X]$ avec $a_n \neq 0$. On note K le corps de fraction de A.

1) Montrer que tout élément non nul de K peut s'écrire $x = a/b$ avec $\mathrm{pgcd}(a, b) = 1$.

2) On suppose que $x = a/b = a'/b'$ avec $\text{pgcd}(a,b) = 1 = \text{pgcd}(a',b')$. Montrer qu'il existe $u \in A^\times$ tel que $ua = a'$ et $ub = b'$.

3) On suppose que $x = a/b \in K^\times$ avec $\text{pgcd}(a,b) = 1$ est racine de P. Montrer que $a \mid a_0$ et $b \mid a_n$.

4) En déduire que si $x \in K^\times$ est racine d'un polynôme unitaire à coefficient dans A alors $x \in A$.

Exercice 75 – Une application de la propriété universelle des polynômes
Montrer qu'il n'existe pas d'éléments U, V, W de l'anneau $\mathbb{Z}[X_1, X_2, X_3, Y_1, Y_2, Y_3]$ vérifiant

$$U^2 + V^2 + W^2 = ({X_1}^2 + {X_2}^2 + {X_3}^2)({Y_1}^2 + {Y_2}^2 + {Y_3}^2)$$

Exercice 76 – Un mécanisme classique
Soit A un anneau commutatif et $U, V \in \text{Mat}_n(A)$. Montrer que $\det(UV) = \det(U)\det(V)$ et aussi $\text{com}(U)\text{com}(V) = \text{com}(UV)$ et encore $\chi_U(U) = 0$.

Exercice 77 – Multiplicité et dérivée
Soit A un anneau commutatif et $P \in A[X]$.

1) Montrer que a est une racine multiple de P si et seulement si $P(a) = P'(a) = 0$

2) La multiplicité d'une racine a correspond-elle toujours à l'ordre d'annulation des dérivées de P ?

Exercice 78 – Fonction polynomiale
Soit A un anneau intègre.

1) Soit $P \in A[X]$ de degré $n \geq 0$. Montrer que P a au plus n racines dans A.

2) Soit $P \in A[X_1, \dots X_n]$. On suppose que pour $i \in \{1, 2, \dots, n\}$, il existe des sous-ensembles A_i de A tel que $P(a_1, \dots, a_n) = 0$ pour tout $(a_1, \dots, a_n) \in A_1 \times \cdots \times A_n$. On suppose de plus que pour tout i, on a $|A_i| > \deg_{X_i} P$. En déduire que $P = 0$.

3) On suppose que A est un anneau intègre infini. Montrer que le morphisme de A-algèbres

$$\begin{aligned} A[X_1, \dots, X_n] &\longrightarrow \mathscr{F}(A^n, A) \\ P &\longmapsto ((a_1, \dots, a_n) \mapsto P(a_1, \dots, a_n)) \end{aligned}$$

est injectif.

4) Montrer qu'un anneau intègre fini est un corps. Montrer que si $A = k$ est un corps fini alors le morphisme de k-algèbres

$$\begin{aligned} k[X_1, \dots, X_n] &\longrightarrow \mathscr{F}(k^n, k) \\ P &\longmapsto ((a_1, \dots, a_n) \mapsto P(a_1, \dots, a_n)) \end{aligned}$$

est surjectif. Déterminer son noyau.

Definition 5 (Graduation)**.** Soit $n \geq 1$. Dans $\mathbb{C}[X_1, \dots, X_n]$, le monôme $X_1^{i_1} \cdots X_n^{i_n}$ est dit de *degré* $\sum_{j=1}^{n} i_j$.
Un polynôme $P \in \mathbb{C}[X_1, \dots, X_n]$ est dit *homogène (de degré d)* s'il est combinaison linéaire de monômes de même degré (d). On remarquera que

(i) tout $P \in CC[X_1, \dots, X_n]$ est, de manière unique, somme $P = P_1 + \cdots + P_\ell$ d'éléments non nuls et homogènes de degrés $d_1, \dots, d_\ell$ deux à deux distincts (on dit que P_i est la *composante homogène de degré* d_i *de* P) ;

(ii) le polynôme 1 est homogène de degré 0 ;

(iii) le produit de deux éléments homogènes de degrés respectifs d et d' est homogène de degré $d + d'$.

Ces trois conditions font de $\mathbb{C}[X_1, \dots, X_n]$ un *anneau gradué* (par définition), on dit aussi que $\mathbb{C}[X_1, \dots, X_n]$ est muni d'une *graduation*.

Exercice 79 – Idéaux homogènes
Soient A un anneau gradué et I un idéal de A. Montrer que les conditions suivantes sont équivalentes

(i) I est engendré par un ensemble d'éléments homogènes.

(ii) I est engendré par l'ensemble de ses éléments homogènes.

(iii) étant donné $P \in A$, on a $P \in I$ si et seulement si chaque composante homogène de P est dans I.

(iv) Il existe une graduation de A/I telle que la projection canonique $\pi\colon A \twoheadrightarrow A/I$ soit homogène (c'est-à-dire, $\pi(P)$ est homogène de degré d dès que P l'est).

Sous l'une des conditions équivalents ci-dessus, on dira que I est un *idéal homogène*.

Dans la suite, on pose $A = \mathbb{C}[X_1, \ldots, X_n]$ et on suppose que G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$. Si $g \in G$ et $v \in \mathbb{C}^n$, on notera ${}^g v$ pour le produit matriciel gv.

Exercice 80 – L'action de G sur A
On admet que l'application qui à un polynôme $P \in A$ associe sa fonction polynomiale $f_P\colon \mathbb{C}^n \to \mathbb{C}$ est un morphisme injectif d'algèbres.

1) Soient $f\colon \mathbb{C}^n \to \mathbb{C}$ une application et $g \in G$. On pose ${}^g f$ l'application $v \mapsto f({}^{g^{-1}} v)$. Montrer que ceci définit une action par automorphismes de $\mathbb{C}$-algèbre de G sur la $\mathbb{C}$-algèbre des fonctions $\mathbb{C}^n \to \mathbb{C}$.

2) Montrer qu'il existe une et une seule action $(g, P) \mapsto {}^g P$ de G sur A par automorphisme de $\mathbb{C}$-algèbre telle que $f_{{}^g P} = {}^g f_P$ pour tout $P \in A$.

3) Soient $i \in \{1, \ldots, n\}$ et $g \in G$. Expliciter ${}^g X_i$ en fonction des coefficients de g^{-1}.

4) Soit $P \in A$ homogène, que peut-on dire de ${}^g P$ pour $g \in G$?

Exercice 81 – L'anneau A^G des invariants
On note $A^G = \{P \in A, \quad \forall g \in G,\ {}^g P = P\}$.

1) Démontrer que A^G est une sous-algèbre de A.

2) Soit $P \in A$. Montrer que $P \in A^G$ si et seulement si chaque composante homogène de P est dans A^G.

3) Caractériser les éléments de A^G en termes fonctions polynomiales.

4) Soit $p\colon A \to A$ l'application définie par

$$p(P) = \frac{1}{|G|} \sum_{g \in G} {}^g P.$$

Montrer que p est un projecteur d'image A^G.

Exercice 82 – A^G est un anneau de type fini
Soit I l'idéal de A engendré par l'ensemble des éléments de $P \in A^G$ dont le terme constant est nul.

1) Montrer que I est un idéal homogène de A.

2) Montrer qu'il existe $P_1, \ldots, P_m \in A^G$ homogènes de degrés tous non nuls tels que $I = (P_1, \ldots, P_m)$.

3) Montrer que la $\mathbb{C}$-algèbre A^G est engendrée par $P_1, \ldots, P_m$. En particulier, elle est de type fini.

Exercice 83 – Le cas des polynômes symétriques
Soit A un anneau commutatif et $n \geq 1$.

1) Montrer qu'il existe une unique action $(\sigma, P) \mapsto \sigma P$ de $\mathfrak{S}_n$ sur $A[X_1, \ldots, X_n]$ par automorphismes de A-algèbre telle que $\sigma X_i = X_{\sigma^{-1}(i)}$ pour $i \in \{1, \ldots, n\}$ et $\sigma \in \mathfrak{S}_n$.

2) Montrer que $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est une sous-A-algèbre de $A[X_1 \ldots, X_n]$.

Cette algèbre est appelée *l'algèbre des polynômes symétriques en n indéterminées à coefficients dans A.*

3) Montrer qu'un polynôme $P \in A[X_1, \ldots, X_n]$ est symétrique si et seulement si chacune de ses composantes homogène l'est.

Definition 6 (Polynômes symétriques élémentaires)**.** Soit $k \in \{1, \ldots, n\}$. On définit le polynôme $\Sigma_k \in A[X_1, \ldots, X_n]$ par

$$\Sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}$$

Le polynôme Σ_k est appelé *le k-ème polynôme symétrique élémentaire en $X_1, \ldots, X_n$.*

Exercice 84 – Théorème de structure

1) Que valent Σ_1 et Σ_n ?

2) Montrer que Σ_k est un polynôme homogène de degré k.

Soit $\varphi_n \colon A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ le morphisme d'algèbres tel que $\varphi_n(X_i) = \Sigma_i$ pour tout $i \in \{1, \ldots, n\}$. Par commodité, on note $P(\Sigma_1, \ldots, \Sigma_n)$ pour $\varphi_n(P)$.
Soit $\pi \colon A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_{n-1}]$ l'unique morphisme de A-algèbres tel que $\pi(X_i) = X_i$ pour $1 \leq i \leq n-1$ et $\pi(X_n) = 0$. L'image $\pi(P)$ d'un polynôme P est dite *obtenue à partir de P en substituant 0 à X_n.*

3) Soit $\sigma \in \mathfrak{S}_{n-1} \subset \mathfrak{S}_n$ et $P \in A[X_1, \ldots, X_n]$. Montrer que $\pi(\sigma P) = \sigma\pi(P)$.

4) Si $n \geq 2$ quelle est l'image par π des polynômes symétriques élémentaires $\Sigma_1, \ldots, \Sigma_n$?
Si $P \in A[X_1, \ldots, X_n]$, que peut-on dire de $\pi(P(\Sigma_1, \ldots, \Sigma_n))$?

5) Montrer que φ_n est injectif (indication : étant donné Q tel que $Q(\Sigma_1, \ldots, \Sigma_n) = 0$, on pourra considérer le polynôme obtenu à partir de $Q(\Sigma_1, \ldots, \Sigma_n)$ en substituant 0 à X_n).

6) Montrer que φ_n est surjectif (indication : étant donné P un polynôme symétrique, on pourra vérifier que Σ_n divise P si et seulement si $\pi(P) = 0$, puis raisonner par récurrence en écrivant $\pi(P)$ comme un polynôme en les polynômes symétriques élémentaires en $X_1, \ldots, X_{n-1}$).

7) En déduire que les algèbres $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ et $A[X_1, \ldots, X_n]$ sont isomorphes.

Références

[Dem97] Michel Demazure. *Cours d'algèbre. Primalité. Divisibilité. Codes.* Cassini, 1997.

[FGN01] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Exercices de mathématiques - Oraux X-ENS - Algèbre - Volume 1.* Cassini, 2001.

[Per81] Daniel Perrin. *Cours d'algèbre.* école normale supérieure de jeunes filles, 1981.

[Sam67] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, collection Méthodes, 1967.

[Tau92] Patrice Tauvel. *Mathématiques générales pour l'agrégation.* Elsevier-Masson, 1992.