Prépa CAPES
Mathématiques
Université de Cergy-Pontoise

RECUEIL D'EXERCICES D'ALGEBRE (I)

Groupes
Anneaux et corps
Arithmétique
Polynômes
Fractions rationnelles

Ceci est juste une compilation d'exercices d'algèbre destinés aux étudiants préparant le CAPES externe de mathématiques. Ont été particulièrement "pillés" :

S. Francinou, H. Gianella et S. Nicolas, Exercices de mathématiques, oraux des concours de Polytechnique et des Ecoles Normales Supérieures, Algèbre 1, Cassini

F. Liret et D. Martinais, Algèbre 1ere année, Cours de mathématiques DEUG MIAS, MASS et SM, Dunod

D. Prochasson, Algèbre 1ere année, Exercices corrigés, DEUG MIAS, MASS et SM, Algèbre 1ere année, Dunod

L. Schwartz, Algèbre, Mathématiques pour la licence, Dunod

J. M. Monier, Cours d'algèbre 1ere année MPSI-PCSI-PTSI, 2 tomes, Dunod

Table des matières

1. Groupes

Quelques rappels

Un ensemble G muni d'une loi $*$, ce que l'on note $(G, *)$, est un **groupe** si et seulement si sa loi $*$ est associative, admet un élément neutre et si tout élément admet un symétrique pour cette loi, soit :

$$\forall x, y, z \in G, x * (y * z) = (x * y) * z,$$
$$\exists e \in G, x * e = e * x = x,$$
$$\forall x \in G, \exists x' \in G, x * x' = x' * x = e.$$

Si de plus la loi est commutative, on dit que $(G, *)$ est un groupe commutatif ou abélien.

Un ensemble H est un **sous-groupe** de $(G, *)$ si et seulement si H est un sous-ensemble de G qui est un groupe muni de la même loi $*$. On appelle **sous-groupe engendré** par une partie A, un sous-ensemble de G, l'intersection de tous les sous-groupes de G contenant A ; on le note $\langle A \rangle$. On appelle **groupe monogène** un groupe engendré par un seul élément ; un groupe monogène fini est appelé **groupe cyclique**..

On appelle **ordre d'un groupe fini** le nombre de ses éléments. On appelle **ordre d'un élément** x, le plus petit entier (quand il existe) $n > 0$ tel que $x^n = e$, sinon on dit que x est d'ordre infini.

Théorème de Lagrange Si H est un sous-groupe d'un groupe fini, alors l'ordre de H divise l'ordre de G. En particulier, l'ordre d'un élément $g \in G$ divise l'ordre de G.

Un **morphisme de groupes** est une application Φ d'un groupe $(G, *)$ dans un groupe $(H, .)$ qui respecte les opérations :

$$\forall x, x' \in G, \Phi(x * x') = \Phi(x).\Phi(x').$$

S'il existe un morphisme bijectif entre deux groupes, on parle d'isomorphisme et de groupes isomorphes. Un isomorphisme d'un groupe dans lui-même s'appelle un automorphisme.

Un sous-groupe H d'un groupe $(G, *)$ est **distingué** dans G (et on note $H \lhd G$) si et seulement si

$$\forall x \in H, \forall y \in G, y * x * y^{-1} \in H.$$

Pour la notion de **groupes quotients**, voir l'exercice 18. La notion de **centre** d'un groupe est définie à l'exercice 9.

Vrai ou faux ?

1) Soit $(G, .)$ un groupe. Alors, pour tout $n \in \mathbb{N}$, tout $x \in G$, tout $y \in G$, $(x.y)^n = x^n.y^n$.

2) $\mathbb{Q} \setminus \{0\}$ muni de son addition usuelle est un groupe.

3) L'ensemble des nombres complexes de module 1 est un sous-groupe de $\mathbb{C} \setminus \{0\}$ muni de son produit usuel.

4) La fonction exp est un morphisme du groupe $(\mathbb{R}, +)$ dans le groupe $(\mathbb{R}^+ \setminus \{0\}, \times)$.

5) La fonction Ln est un isomorphisme du groupe $(\mathbb{R}^+ \setminus \{0\}, \times)$ sur le groupe $(\mathbb{R}, +)$.

6) L'ordre d'un élément g d'un groupe fini G est égal à l'ordre du groupe G.

7) Si G est un groupe abélien, alors tout sous-groupe de G est distingué.

8) $(\mathbb{R}, +)$ est un groupe monogène.

Quelques exercices

Exercice de cours

1a) Soient G un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de G. Montrer que $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

1b) Soient G un groupe et A un sous ensemble de G. Montrer que $\langle A \rangle$ est (au sens de l'inclusion) le plus petit sous-groupe contenant A.

2) Soit $f : (G, *) \to (H, .)$ un morphisme de groupe. On note e_h l'élément neutre de $(H, .)$.

2a) Montrer que $\mathrm{Ker}(f) = \{x \in G; f(x) = e_h\}$ est un sous-groupe de G.
2b) Montrer que $\mathrm{Im}(f) = \{y \in H, \exists x \in G, f(x) = y\}$ est un sous-groupe de H.
3) Soient G un groupe et A un sous-ensemble (non vide) de G. Alors, $\langle A \rangle$ est l'ensemble des composés multiples d'éléments de A et de symétriques d'éléments de A.
4a) Montrer que la composée de deux morphismes de groupe est un morphisme de groupe. Montrer que la bijection réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.
4b) Soit $(G, .)$ un groupe. Montrer que l'ensemble des automorphismes de G forme un groupe pour la loi de composition des applications. Pour $x \in G$, on définit $\phi_x(y) = x.y.x^{-1}$. Montrer que ϕ_x est un automorphisme (appelé **automorphisme intérieur** de G) de G. Montrer que l'ensemble des automorphismes intérieurs de G est un sous-groupe du groupe des automorphismes de G.

Exercice 1
Soit $G = \mathbb{R}^* \times \mathbb{R}$. Sur G, on définit la loi

$$(x, y) * (x', y') = (xx', xy' + y).$$

1) $(G, *)$ est-il un groupe commutatif ?
2) Montrer que $\mathbb{R}^{+*} \times \mathbb{R}$ est un sous-groupe de G.

Exercice 2
Soit $G = \{f_{a,b}, a \in \mathbb{R}^*, b \in \mathbb{R}\}$ où $f_{a,b} : \mathbb{R} \to \mathbb{R}$ est défini par $f_{a,b}(x) = ax + b$. Montrer que G muni de la loi de composition est un groupe. Est-il commutatif ?

Exercice 3
Soit $(G, .)$ un groupe et soient a et b des éléments de G tels que $a^5 = 1$ et $a^3.b = b.a^3$. Montrer que $a^6.b = b.a^6$. En déduire que a et b commutent.

Exercice 4
Soit Γ l'ensemble des matrices de $\mathcal{M}_3(\mathbb{Z}/3\mathbb{Z})$ de la forme

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

1) Montrer que Γ est un groupe pour la multiplication des matrices.
2) Montrer que $\forall M \in \Gamma \quad M^3 = \mathrm{Id}$.
3) Quel est le centre de M ?

Exercice 5
Soient $G = \mathbb{R}^* \times \mathbb{R}$. On définit sur G la loi

$$(x, y) * (x', y') = (xx', xy' + \frac{y}{x'}).$$

1) Montrer que $(G, *)$ est un groupe.
2) Quel est son centre ?
3) Montrer que $\mathbb{R}^* \times \{0\}$, $\{1\} \times \mathbb{R}$, $\mathbb{Q}^* \times \mathbb{Q}$ sont des sous-groupes de G.
4) Montrer que, pour tout $k \in \mathbb{R}$, l'ensemble

$$H_k = \left\{ \left(x, k \left(x - \frac{1}{x} \right) \right), x \in \mathbb{R}^+ \right\}$$

est un sous-groupe commutatif de G.

Exercice 6
Dans le plan euclidien , $ABCD$ est un carré de centre O et Ox est la médiatrice de AD. On note $r = \mathrm{Rot}(0, \frac{\pi}{2})$ et σ la symétrie par rapport Ox. D_4 est le groupe des isométries du plan laissant le carré globalement invariant.
1) Montrer que $D_4 = \{\mathrm{id}, \mathrm{r}, \mathrm{r}^2, \mathrm{r}^3, \sigma, \sigma\mathrm{r}, \sigma\mathrm{r}^2, \sigma\mathrm{r}^3\}$.
2) Quels sont les sous groupes de D_4 ? Lesquels sont distingués ?
3) Trouver $Z(D_4)$.

Exercice 7
Soit G un sous-groupe de $(\mathbb{C}, +)$ tel que, pour tout $x \in [0, 1]$, $x + ix^2 \in G$. Montrer que $G = \mathbb{C}$.

Exercice 8
Soit $(G, .)$ un groupe. On suppose que pour tout $x \in G$, $x^2 = 1$.
1) Montrer que l'on a $x = x^{-1}$ pour tout $x \in G$.
2) Montrer que le groupe $(G, .)$ est commutatif.

Exercice 9
Soit $(G, +)$ un groupe. On définit le centre de G par $Z(G) = \{x \in G; x + y = y + x, \forall y \in G\}$.
1) Montrer que $Z(G)$ est un sous-groupe de G.
2) Montrer que $Z(G)$ est un groupe abélien.
3) Montrer que $Z(G)$ est distingué dans G.

Exercice 10
Posons $w = \cos\dfrac{\pi}{3} + i\sin\dfrac{\pi}{3}$.
On pose $G = \{1, w, w^2, w^3, w^4, w^5\}$, $K = \{1, w^2, w^4\}$, et $L = \{1, w^3\}$.
1) Montrer que G est un sous-groupe de $(\mathbb{C} \setminus \{0\}, .)$. Quel est le symétrique de w ?
2) Montrer que K et L sont des sous-groupes de G.
3) Soit H un sous-groupe de G différent de $\{1\}$ et ne contenant ni w, ni w^5. Montrer que $H = K$ ou $H = L$.
4) Déterminer tous les sous-groupes de G.

Exercice 11
On note U l'ensemble des nombres complexes de module 1.
1) Montrer que l'application $f : \mathbb{C} \setminus \{0\} \to U$ défini par $f(z) = \dfrac{z}{|z|}$ est un morphisme surjectif.
2) Montrer que l'application $f : U \to U$ défini par $f(z) = z^2$ est un morphisme surjectif.

Exercice 12
Pour tout nombre x, $y \in \mathbb{R} \setminus \{1\}$, on pose $x * y = x + y - xy$.
1) Montrer que $(\mathbb{R} \setminus \{1\}, *)$ est un groupe commutatif.
2) On définit $f(x) = 1 - \dfrac{1}{x}$ pour $x \in \mathbb{R}^*$. Montrer que f est un isomorphisme de $(\mathbb{R}^*, \times)$ sur $(\mathbb{R} \setminus \{1\}, *)$.

Exercice 13
Soit G un groupe et e son élément neutre.
1) Montrer que si pour tout $x \in G$, $x^2 = e$, alors G est commutatif.

2) On suppose que G est fini et on pose

$$A = \{x \in G; x^2 = e\} \text{ et } B = \{x \in G; x^2 \neq e\}.$$

2a) Montrer que si un élément $x \in G$ appartient á B, alors $x^{-1} \in B$ et $x^{-1} \neq x$. En déduire que card(B) est pair.
2b) On suppose que card(G) est un entier pair. Montrer que card$(A) \geq 2$ et qu'il existe $x \in G$ tel que $x \neq e$ et $x^2 = e$.

Exercice 14
Soient $(G, *)$ et $(H, .)$ deux groupes et soit $f : G \to H$ un morphisme de groupes.
1) Montrer que pour tout sous-groupe G' de G, $f(G')$ est un sous-groupe de H.
2) Montrer que pour tout sous-groupe H' de H, $f^{-1}(H')$ est un sous-groupe de G.

Exercice 15
1) Montrer que les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}^{+*}, \times)$ ne sont pas isomorphes.
2) Montrer que les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ ne sont pas isomorphes.

Exercice 16
Soit $(G, .)$ un groupe tel que $f : G \to G$ défini par $f(x) = x^3$ soit un morphisme surjectif de groupe. Montrer que G est abélien.

Exercice 17
Soit G un groupe cyclique et soit a un générateur de G. On note e son élément neutre.
1) Montrer que G est commutatif.
2) Soit H un sous-groupe de G. On pose $A = \{m \in \mathbb{Z}, a^m \in H\}$. Montrer que, si $H \neq \{e\}$, alors A contient un élément positif. Soit m_0 le plus petit entier positif appartenant à A. Montrer que A est l'ensemble des multiples entiers de m_0.
3) Soit $\phi : G \to G$ un morphisme de groupe. Montrer que $\phi(H) \subset H$.

Exercice 18
1) Soient G un groupe et H un sous-groupe de G. On appelle relation à gauche (respectivement relation à droite) associée au sous-groupe H la relation définie par $x \sim y$ si et seulement si $x^{-1}y \in H$ (respectivement $x \sim' y$ si $yx^{-1} \in H$). 1a) Montrer que ces relations sont des relations d'équivalence.
1b) Déterminer les classes d'équivalence de $x \in H$ pour cette relation. Quel est leur cardinal ? On note G/H (respectivement H/G) l'ensemble des classe à gauche (respectivement à droite).
2) Démontrer le théorème de Lagrange.
3) Soit G un groupe fini. Montrer que l'ordre d'un élément $g \in G$ divise l'ordre du groupe (Ne pas oublier de montrer que g n'est pas d'ordre infini !). Montrer que l'ensemble des $m \in \mathbb{N} \setminus \{0\}$ tel que $g^m = e$ est l'ensemble des multiples (entiers positifs) de l'ordre de g.
4) Soit G un groupe d'ordre p où p est premier. Montrer que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
5) Dans un groupe fini à 24 éléments, peut-il exister un sous-groupe de 10 éléments ?
6) Soit G un groupe et H un sous-groupe distingué de G. Montrer que l'on peut munir G/H d'une structure de groupe (appelé **groupe quotient** de G par H) telle que l'application canonique $G \to G/H$ soit un morphisme de groupe. Montrer que le groupe $\mathbb{Z}/n\mathbb{Z}$ est le quotient du groupe $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.
7) Soit G un groupe. Montrer que si le groupe quotient $G/Z(G)$ (où $Z(G)$ est le centre de G) est cyclique, alors G est abélien.
8) Montrer que pour tout $n \geq \mathbb{N}^*$, il existe un unique sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ de cardinal

n.

Exercice 19
1) Soit G un groupe monogène.
1a) Montrer que si G est infini, alors G est isomorphe à $\mathbb{Z}$.
1b) Supposons que G soit cyclique d'ordre n. Montrer que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
1c) Que peut-on conclure de 1) et 2) ?
2) Montrer que l'ordre d'un élément est égal au cardinal du sous-groupe qu'il engendre.

Exercice 20
1a) Soit G un groupe dont tous les éléments (distincts de l'élément neutre) sont d'ordre 2. Montrer qu'il est commutatif.
1b) Montrer que si le groupe G est fini, son cardinal est une puissance de 2 (faire une récurrence sur l'ordre de G).
1c) Montrer que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.
2) Ecrire la table de tous les groupes à 4 et 6 éléments.
3) Soit p un nombre premier. Montrer que tout groupe d'ordre $2p$ contient un élément d'ordre p.

2. Le groupe S_n

Quelques rappels

On appelle S_n l'ensemble des bijections de $\{1, 2, .., n\}$ dans lui-même. Ses éléments sont appelés **permutations**. Muni de la loi de composition des applications, $(S_n, \circ)$ est un groupe : on le nomme groupe des permutations ou **groupe symétrique**. Pour toute permutation $\sigma \in S_n$, on appelle support de σ le complémentaire de l'ensemble des éléments invariants par σ (dans $\{1, 2, .., n\}$).

Soit s une permutation. On dit que s est une **transposition** s'il existe deux entiers i et j, différents et appartenant à $\{1, 2, ..n\}$, tels que

$$\begin{cases} s(i) = j \\ s(j) = i \\ s(k) = k \quad \text{pour tout } k \neq i, j. \end{cases}$$

On la note (ij). Toute permutation est produit de transpositions.

Soit p un entier tel que $2 \leq p \leq n$ et soit s une permutation. On dit que s est un **p-cycle** s'il existe p éléments $a_1, .., a_p$ de $\{1, ..., n\}$ deux à deux différents tels que

$$\begin{cases} s(a_i) = a_{i+1} \quad \text{pour tout entier } i < p \\ s(a_p) = a_1 \\ s(j) = j \qquad \text{pour tout } j \notin \{a_1, ..., a_p\}. \end{cases}$$

Cette permutation s se note $(a_1 a_2 ... a_p)$.

Toute permutation se décompose en produit de cycles de supports disjoints.

Soit $s \in S_n$. On dit que le couple $(s(i), s(j))$ est une **inversion** de s si et seulement si $i < j$ et $s(i) > s(j)$. On note $I(s)$ le nombre d'inversions de s et on appelle **signature** le nombre $\varepsilon(s) = (-1)^{I(s)}$.

La signature est un morphisme de S_n dans le groupe multiplicatif $(\{-1, 1\}, \times)$. On appelle groupe alterné l'ensemble des permutations de signature 1 (c'est le noyau du morphisme signature). On note le groupe alterné A_n, c'est un sous-groupe distingué de S_n qui est engendré par les 3-cycles.

Vrai ou faux ?

1) Le groupe S_n posséde $n!$ éléments.
2) Une transposition est un 2-cycle.
3) Soit $s \in S_4$ tel que $s(1) = 3$, $s(2) = 1$, $s(3) = 4$ et $s(4) = 2$. Alors, s est un 4-cycle et $s = (4, 2, 1, 3)$.
4) id est un cycle.

Quelques exercices

Exercice de cours

1) Montrer que si s est un p-cycle, $s^p = id$.
2) Montrer que si s et t sont deux cycles à supports disjoints, alors $st = ts$.
3) Montrer que tout élément de s_n différent de l'identité est produit de cycles à supports disjoints.
4) Montrer que tout élément de s_n est produit de transpositions.
5) Montrer que la signature est un morphisme de S_n dans le groupe multiplicatif $\{1, -1\}$.
6) Montrer que A_n est un sous-groupe distingué du groupe symétrique S_n et que son ordre est $\dfrac{n!}{2}$.

Exercice 1

Soit n un entier supérieur ou égal à 2. Soient $t = (i, j)$ une transposition de S_n et s un élément de S_n.
1) Montrer que $s(i) \neq s(j)$.
2) Montrer que $st(s^{-1})$ est la transposition de S_n qui échange $s(i)$ et $s(j)$.

Exercice 2

Notons s l'élément (1234) de S_4.
1) Décomposer s^2 et s^3 en produit de cycles à supports disjoints.
2) Montrer que les éléments id, s, s^2 et s^3 sont deux à deux différents.
3) Soit G la partie de S_4 définie par $G = \{id, s, s^2, s^3\}$. Montrer que G est un sous-groupe de S_4.

Exercice 3

Soient G et H les deux sous-groupes de S_4 définis par

$$H = \{id, (12)(34), (13)(24), (14)(23)\} \text{ et } G = \{id, (1234), (13)(24), (1432)\}.$$

1) Supposons que f est un morphisme de H dans G. Montrer que pour tout $s \in H$, $(f(s))^2 = id$.
2) Démontrer que les groupes G et H ne sont pas isomorphes.

Exercice 4
Posons $K = \{s \in S_4; s(3) = 3\}$.
1) Montrer que K est un sous-groupe de S_4.
2) Montrer que pour tout $s \in K$ et et tout $i \in \{1, 2, 4\}$, on a $s(i) \neq 3$. En déduire que les groupes K et $S(\{1, 2, 4\})$ sont isomorphes.
3) Montrer que les groupes K et S_3 sont isomorphes.

Exercice 5
Notons s l'élément de S_9 défini par

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 7 & 5 & 9 & 2 & 1 & 6 & 4 \end{pmatrix}$$

1) Décomposer s en produit de cycles à supports disjoints.
2) Trouver le plus petit entier positif n tel que $s^n = id$.

Exercice 6
Pour tout $n \in \mathbb{N}^*$, déterminer la signature de $s : \{1, 2, ...n\} \to \{1, 2, ...n\}$ définie par $s(i) = n + 1 - i$.

Exercice 7
Pour $n \in \mathbb{N}^*$, déterminer la signature de

$$\begin{pmatrix} 1 & 2 & 3 & ..... & n & n+1 & n+2 & .... & 2n \\ 2 & 4 & 6 & ..... & 2n & 1 & 3 & .... & 2n-1 \end{pmatrix}$$

Exercice 8
Soit s défini par

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & & & & & & & & \\ 7 & 1 & 5 & 12 & 6 & 3 & 9 & 4 & 2 & 11 \\ 8 & 10 & & & & & & & & \end{pmatrix}$$

1) Déterminer le nombre d'inversions et la parité de s.
2) Décomposer s (d'au moins une façon) en un produit de transpositions.
3) Décomposer s en un produit de cycles à supports disjoints. Retouver la valeur de la signature de s.

Exercice 9
On considére dans S_9 les permutations suivantes

$$u = (123)(456)(789), \quad v = (456), \quad w = (147)(258)(369).$$

1) Montrer que l'on a $u^3 = v^3 = w^3 = id$.
2) Calculer wvw^{-1} et $w^{-1}vw$. En déduire l'égalité $(wv)^2 w = u^2 v^{-1}$ et montrer que u est une puissance de wv.

Exercice 10
On considére dans S_6 les cycles $s_1 = (1356)$ et $s_2 = (24)$. On pose $s = s_1 s_2$.
1) Calculer s^n pour tout $n \in \mathbb{Z}$.
2) Montrer que l'ensemble $H = \{id, s, s^2, s^3\}$ est un sous-groupe de s_6.
3) Trouver une transposition t telle que chacune des permutations st et ts soit un 6-cycle.

Exercice 11
Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un morphisme injectif de S_n dans A_{n+2}.

Exercice 12
Etablir la table de tous les groupes à 6 éléments (voir exercice 20 de la feuille sur les groupes).

Exercice 13
Soit T un tétraèdre régulier de l'espace euclidien E de dimension 3, centré en l'origine.
1) Montrer que l'ensemble des isométries de E laissant T stable est un sous-groupe du groupe Isom$E$.
2) En considérant l'action sur les sommets montrer que ce groupe est isomorphe à S_4.

3. Anneaux et Corps

Quelques rappels

Soit A un ensemble muni de deux lois internes $+$ et $.$ (appelés respectivement somme et produit). On dit que $(A, +, .)$ est un **anneau** (unitaire) si
- $(A, +)$ est un groupe commutatif ;
- Pour tous x, y et z dans A, on a $(x.y).z = x.(y.z)$ (associativité du produit) ;
- Il existe $e \in A$ (élément neutre pour le produit) tel que $e.x = x.e = x$ pour tout $x \in A$. On notera dans la suite cet élément 1 ;
- Pour tous x, y et z dans A, on a $x.(y + z) = x.y + x.z$ et $(x + y).z = x.z + y.z$ (distributivité).

Si on a de plus $x.y = y.x$ pour tous x, y dans A, alors A est un **anneau commutatif**.

Soit $(A, +; .)$ un anneau et soit B une partie de A. On dit que B est un **sous-anneau** de A si
- $(B, +)$ est un sous-groupe de $(A, +)$;
- $1 \in B$ (où 1 désigne l'élément neutre pour le produit sur A) et pour tous x et y dans B, $x.y \in B$.

Soient A et A' deux anneaux. On note 1_A et $1_{A'}$ leurs éléments neutres pour le produit. On dit qu'une application $f : A \to A'$ est un **morphisme d'anneau** si
- Pour tous x, y dans A, $f(x + y) = f(x) + f(y)$;
- Pour tous x, y dans A', $f(x.y) = f(x).f(y)$;
- $f(1_A) = 1_{A'}$.

Soit $(A, +, .)$ un anneau. On dit que $a \in A$ est un **diviseur de zéro à gauche** (respectivement **diviseur de zéro à droite**) dans A si $a \neq 0$ et il existe $b \in A$, $b \neq 0$ tel que $a.b = 0$ (respectivement $b.a = 0$). On dit que a est un **diviseur de zéro** si a est un diviseur de zéro à gauche et à droite. Un anneau $(A, +, .)$ (non réduit à 0) est **intègre** si A est commutatif et n'admet aucun diviseur de zéro. Un anneau $(A, +, .)$ est **principal** si A est intégre et tout idéal de A est de la forme $\{x.a; a \in A\}$ pour un certain $x \in A$.

Une partie I d'un anneau A est un **idéal bilatère** si $(I, +)$ est un sous-groupe de $(A, +)$ et pour tout $a \in A$ et tout $x \in I$, $x.a \in I$ et $a.x \in I$. On dit que cet idéal est un **idéal maximal** s'il n'existe pas d'idéal de A contenant I. Un idéal est dit **premier** si

pour tous x, y dans A tels que $x.y \in A$, alors soit $x \in I$, soit $y \in I$.

Soit $(K, +, .)$ un anneau. On dit que $(K, +, .)$ est un **corps** (commutatif) si $(K, +, .)$ est un anneau commutatif et si pour tout élement de K distinct de 0, il existe $x' \in K \setminus \{0\}$ tel que $x.x' = x'.x = 1$. Cet élément x' s'appelle l'inverse de x et se note x^{-1}. Soit L une partie de K. On dit que L est un **sous-corps** du corps K si L est un sous-anneau de K et si pour tout $x \in L \setminus \{0\}$, $x^{-1} \in L$. La **caractéristique** d'un corps K est le plus petit entier $k \in \mathbb{N}$ tel que $px = \overbrace{x.x.....x}^{p \text{ fois}} = 0$ pour tout $x \in K$ (voir exercice de cours, question 7).

Vrai ou faux ?

1) L'anneau $M_n(K)$ (où $K = \mathbb{R}$ ou $K = \mathbb{C}$) n'est pas commutatif.

2) $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{Z}[\sqrt{2}]$ (qui est l'ensemble des réels de la forme $a + b\sqrt{2}$ avec a, b dans $\mathbb{R}$) sont des sous-anneaux de $\mathbb{R}$.
3) $2\mathbb{Z} = \{2n, n \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Z}, +, .)$.
4) L'ensemble $\mathbb{Q}[i]$ des nombres complexes qui s'écrivent $a + ib$ avec a, b dans $\mathbb{Q}$ est un sous-corps de $\mathbb{C}$.

5) Les classes de 2, 3 et 4 sont des diviseurs de zéro dans $\mathbb{Z}/6\mathbb{Z}$.

6) Dans $M_2(\mathbb{R})$, la matrice $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ est un diviseur de zéro à gauche.

7) $\mathbb{Z}$ est un anneau intégre, mais pas $\mathbb{Z}/6\mathbb{Z}$.

8) Tout corps commutatif est un anneau intègre.

9) L'application $z \to \overline{z}$ est un automorphisme du corps $\mathbb{C}$.

10) La caractéristique du corps $\mathbb{Q}$ est 0, celle de $\mathbb{Z}/p\mathbb{Z}$ (p premier) est p.

Quelques exercices

Exercice de cours
On suit les mêmes notations que dans les rappels.

1) Soit A un anneau.
1a) Montrer que pour tout $x \in A$, $0.x = 0$.
1b) On suppose que A est commutatif. Montrer la formule du binôme pour $(x + y)^n$.
2) Soit B une partie d'un anneau A.
2a) Montrer que si B est un sous-anneau de $(A, +, .)$, alors $(B, +, .)$ est un anneau.
2b) Montrer que B est un sous-anneau de $(A, +, .)$ si et seulement si
- Pour tous x, y dans B, $x - y \in B$;
- Pour tous x, y dans B, $x.y \in B$;
- $1 \in B$.

2c) Reprendre 2a) et 2b) dans le cas d'un sous-corps.
3) Montrer que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.
4) Montrer qu'une intersection d'idéaux est un idéal. On appele idéal engendré par une partie d'un anneau A l'intersection de tous les idéaux contenant cette partie. Montrer que c'est le plus petit (au sens de l'inclusion) idéal contenant cette partie.
5) Soit $\phi : A \to A'$ un morphisme d'anneaux.
5a) Soit I' un idéal de A'. Montrer que $I = \phi^{-1}(I')$ est un idéal de A.
5b) Soit I un idéal de A. Montrer que si de plus ϕ est surjectif, alors $I' = \phi(I)$ est un idéal de A'.
6) Soit I un idéal (bilatère) d'un anneau A. Montrer que l'on peut définir le groupe quotient A/I. Pour tout $\overline{a}$, $\overline{b}$ dans A/I, on pose $\overline{a} + \overline{b} = a + b + I$ et $\overline{a} * \overline{b} = ab + I$. Montrer que ces lois sont bien définis sur A/I et que $(A/I, +, *)$ est un anneau (appelé anneau quotient de A par I). Montrer que l'application $\phi : A \to A/I$ défini par $\phi(a) = a + I$ est un morphisme d'anneau.

7) Soit K un corps. On définit $c : \mathbb{Z} \to K$ par $c(m) == \overbrace{1.1.....1}^{m \text{ fois}} = m.1$ pour $m \in \mathbb{N}$ et $c(m) = c(-m)$ si $m < 0$.
7a) Montrer que c est un morphisme d'anneau.
7b) Montrer que le noyau de c, noté I, est un idéal, puis que I est soit trivial (c'est à dire réduit à 0), soit premier.
7c) Si I est premier, montrer qu'il est maximal et constitué par les multiples d'un nombre premier p, appelé caractéristique de K.
Si I est trivial, on dit que K est de caractéristique 0.

7d) Soit K un corps de caractéristique p. Montrer que pour tout $x \in K$, $p.x = \overbrace{x.x.....x}^{p \text{ fois}} = 0$.
7e) Quelle est la caractéristique de $\mathbb{Q}$? de $\mathbb{Z}/p\mathbb{Z}$ (p premier) ?
8a) Montrer qu'un corps K contient toujours un plus petit sous-corps, qui est l'intersection de tous les sous-corps contenus dans K.
8b) Montrer que si K est de caractéristique 0, alors son plus petit sous-corps est isomorphe à $\mathbb{Q}$. Montrer que si K est de caractéristique p, son plus petit sous-corps est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exercice 1 (Anneau des entiers de Gauss)

Soit $\mathbb{Z}[i]$ l'ensemble des nombres complexes de la forme $a + ib$ où a, $b \in \mathbb{Z}$.
1) Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
2) Soit $z \in \mathbb{Z}[i]$. Montrer que $\overline{z} \in \mathbb{Z}[i]$ et que $|z|^2 \in \mathbb{N}$.
3) Soit $z \in \mathbb{Z}[i]$. Montrer que z appartient au groupe des éléments inversibles de l'anneau $\mathbb{Z}[i]$ si et seulement si $|z|^2 = 1$.
4) Expliciter le groupe des éléments inversibles de $\mathbb{Z}[i]$.
5) Montrer que pour tout $z \in \mathbb{C}$, il existe $z_0 \in \mathbb{Z}[i]$ tel que $|z - z_0| < 1$. En déduire que pour tout $z_0 \in \mathbb{Z}[i]$ et tout $z_1 \in \mathbb{Z}[i]$ non nul, il existe a_0, $a_1 \in \mathbb{Z}(i)$ tels que $z_0 = a_0 z_1 + a_1$ et $|a_1| < |z_1|$.
6) Montrer que $\mathbb{Z}[i]$ est un anneau principal.
Pour encore plus de propriétés de l'anneau de Gauss, voir "Algébre 1, ENS-X" de S. Francinou, H. Gianella, S. Nicolas aux éditions Cassini.

Exercice 2

Soit p un nombre premier. On appele $\mathbb{Z}_p$ l'ensemble des nombres rationnels que l'on peut écrire $\dfrac{m}{n}$ où m, n sont des entiers relatifs et n n'est pas divisible par p.
1) Montrer que $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}$.
2) Montrer que pour tout $x \in \mathbb{Q}$, $x \in \mathbb{Z}_p$ ou $x^{-1} \in \mathbb{Z}_p$.
3) L'objet de cette question est de montrer que les seuls sous-anneaux de $\mathbb{Q}$ qui contiennent $\mathbb{Z}_p$ sont $\mathbb{Z}_p$ et $\mathbb{Q}$.
3a) Soit A un sous-anneau de $\mathbb{Q}$ qui contient $\mathbb{Z}_p$ et tel qu'il existe un rationnel x appartenant à $A \setminus \mathbb{Z}_p$. On suppose que x s'écrive sous forme irréductible $x = \dfrac{m}{np^a}$ où $m \in \mathbb{Z}$, $n \in \mathbb{N}$ et $a \in \mathbb{N} \setminus \{0\}$. Montrer que pour tout entier b avec $0 \leq b \leq a$ on a $\dfrac{1}{p^b} \in A$.
3b) Montrer que pour tout $c \in \mathbb{N}$, on a $\dfrac{1}{p^c} \in A$, puis conclure.

Exercice 3

1) Soit A un anneau commutatif et soit I un idéal de A. On pose $I_1 = \{x \in A; \exists n \in \mathbb{N}, x^n \in I\}$. Montrer que I_1 est un idéal qui contient I.

2) On pose $A = \mathbb{Z}$ et soit I l'ensemble des multiples de 120. Montrer que I est un idéal. Déterminer I_1.

Exercice 4

Soit A un anneau tel que pour tout $x \in A$, $x^2 = x$.
1) Montrer que pour tout $x \in A$, $2x = 0$. En déduire que A est commutatif.
2) Montrer que pour tous x, y, z dans A,

$$(x+y)z = 0 \Longleftrightarrow (x(y+1)z = 0 \text{ et } (x+1)yz = 0).$$

Exercice 5

Soit A un anneau. Un élément $x \in A$ est dit nilpotent si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$.
1) Montrer que si x et y sont nilpotents et commutent, alors $x + y$ est nilpotent.
2) Montrer que si x est nilpotent et commute avec y, alors xy est nilpotent.
3) Soit x nilpotent dans A. Montre que $1 - x$ est inversible et calculer $(1 - x)^{-1}$.
4) Montrer que tout élément nilpotent appartient à tout idéal premier de A.
5) Soit A un anneau tel que $x^3 = x$ pour tout $x \in A$.
5a) Déterminer les éléments nilpotents de A.
5b) Soit $e \in A$ tel que $e^2 = e$, soit $a \in A$. On pose $b = ea(1-e)$. Calculer b^2 et en déduire que $ea = ae$. En déduire que pour tout $x \in A$, $x^2 \in Z(A)$ où $Z(A)$ désigne le centre de A.
5c) Montrer que A est commutatif.

Exercice 6

Soit A un anneau et $E = \mathbb{Z} \times A$. Sur E, on pose :

$$(m,a) + (p,b) = (m+p, a+b),$$
$$(m,a).(p,b) = (mp, mb + pa + ab).$$

1) Montrer que $(E, +, .)$ est un anneau. L'anneau E a-t-il un élément unité ?
2) Montrer que

$$\begin{aligned} \Phi : \quad & A \to E \\ & a \mapsto (0,a) \end{aligned}$$

est un morphisme d'anneaux. Est-ce un morphisme d'anneaux unitaires ?
3) Etudier si A commutatif (resp. intègre) $\Rightarrow$ E commutatif (resp. intègre).

Exercice 7

Soit $A = C^0([0,1], \mathbb{R})$.
1) Vérifier que A est un anneau unitaire.
2) Soit $x \in [0,1]$. Montrer que $M(x) = \{f \in A; f(x) = 0\}$ est un idéal. $M(x)$ est-il premier, maximal ?
3) Soit I un idéal de A tel que $E_I = \cap_{f \in I} f^{-1}\{0\}$ soit vide. Montrer que I contient une fonction ne s'annulant jamais. En déduire que $I = A$.
4) Déduire de la question précédente que les idéaux maximaux de A sont de la forme $M(x)$.

Exercice 8

Soit A un anneau commutatif.
1) Montrer qu'un idéal I est premier ssi A/I est intègre.
2) Montrer qu'un idéal I est maximal ssi A/I est un corps.

Exercice 9

1) Quels sont les idéaux d'un corps ?

2) Soit A un anneau commutatif unitaire qui ne possède que des idéaux premiers. Montrer que A est un corps.

Exercice 10

Montrer qu'il existe une structure d'anneau et une seule sur un ensemble à 2 éléments, respectivement 3 éléments. Etudier le cas d'un ensemble à 4 éléments. Dire lesquels sont des corps.

Exercice 11

Soit $\mathbb{D}$ l'anneau des nombres décimaux. Montrer que $\mathbb{D}$ est principal.

Exercice 12

Un idéal I est dit primaire si la condition $xy \in I$ implique qu'il existe un entier n tel que $x^n \in I$ ou $y^n \in I$.

1) Quels sont les idéaux primaires de $\mathbb{Z}$.

2) Etant donné un idéal I, on appele radical de I et on note $\sqrt{I}$ l'idéal engendré par les éléments x tels qu'il existe un entier n tel que $x^n \in I$. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.

3) Montrer que le radical d'un idéal primaire est premier.

Exercice 13

Pour tout nombre premier p, on note $\mathbb{Q}(\sqrt{p})$ l'ensemble des nombres réels de la forme $a + \sqrt{p}b$ où a, b sont des nombres rationnels.

1) Soit p un nombre premier. Montrer que $\mathbb{Q}(\sqrt{p})$ est un $\mathbb{Q}$-espace vectoriel de dimension 2. Montrer que $\mathbb{Q}(\sqrt{p})$ est un sous-corps de $\mathbb{R}$.

2) Montrer que $\sqrt{2}$ n'appartient pas à $\mathbb{Q}(\sqrt{3})$.

3) Montrer que l'on a $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.

4) Déterminer tous les automorphismes de $\mathbb{Q}(\sqrt{2})$.

Exercice 14

1) Montrer que $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$. On désigne par α une de ses racines complexes et on pose

$$A = \{a + b\alpha + c\alpha^2, (a, b, c) \in \mathbb{Q}^3\}.$$

2) Montrer que A est un sous-corps de $\mathbb{C}$.

Exercice 15

1) Soient a et b deux éléments d'un corps K de caractéristique p. Montrer que pour tout entier n,

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

2) Applications : Montrer les résultats classiques suivants.

Petit théorème de Fermat. Soit p un nombre premier et soit n un entier naturel. Montrer que n^p est congru à n modulo p.

Théorème de Wilson. Soit p un nombre premier. Le produit $(p-1)!$ est congru à -1 modulo p.

Quelques rappels

4.1. Division euclidienne.

Théorème 4.1. *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $0 \leq r < |b|$ et $a = bq + r$. Trouver le couple (q, r) s'appelle effectuer la* **division euclidienne** *de a par b, q s'appelle le quotient de cette division et r le reste.*

On en déduit que l'anneau $\mathbb{Z}$ est euclidien, et donc principal (voir la feuille sur anneaux et corps).

Corollaire 4.2. *Tous les sous-groupes de $\mathbb{Z}$ sont de la forme $k\mathbb{Z}$ avec $k \in \mathbb{N}$.*

4.2. PGCD de deux entiers.

4.2.1. *Première approche.*

Définition 4.1. *Soient a et b deux entiers naturels non-nuls. L'ensemble des diviseurs communs à a et b est un ensemble non-vide fini qui admet un plus grand élément. On l'appelle le* **plus grand diviseur commun** *à a et b, et on le note $PGCD(a, b)$.*

Proposition 4.2. *Supposons que b ne divise pas a. Si on note r le reste de la division euclidienne de a par b, alors les diviseurs communs à a et b sont les mêmes que les diviseurs communs à b et r. Par conséquent $PGCD(a, b) = PGCD(b, r)$.*

Une conséquence de cette proposition est la mise en oeuvre de **l'algorithme d'Euclide**. L'algorithme se terminant par b divise a, on peut en déduire que les diviseurs communs à deux entiers naturels divisent leur PGCD.

4.2.2. *Deuxième approche.*

Définition 4.3. *Soient a et b deux entiers. $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, il existe donc un unique entier naturel noté $a \wedge b$ tel que $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.*

Proposition 4.4. *Si a et b sont deux entiers naturels non-nuls, alors $a \wedge b = PGCD(a, b)$.*

Preuve Par définition $a \wedge b$ divise a et b. Si d est un diviseur commun à a et b alors $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$ donc d divise $a \wedge b$. $a \wedge b$ est donc le plus grand diviseur commun pour la relation d'ordre divisibilité dans $\mathbb{N}$, c'est donc le plus grand pour la relation d'ordre classique.

Définition 4.5. *On dit que deux entiers sont* **premiers entre eux** *si et seulement si leur $PGCD$ est égal à 1.*

Théorème 4.6. *(***Théorème de Bezout***)*
Soient a et b deux entiers, alors $a \wedge b = 1$ si et seulement si il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $au + bv = 1$.

Preuve Si $a \wedge b = p$ alors $p \in a\mathbb{Z} + b\mathbb{Z}$, donc il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $p = au + bv$. La réciproque est immédiate pour $p = 1$.

Théorème 4.7. *(***Théorème de Gauss***)*
Si $a \wedge b = 1$ et si a divise bc alors a divise c.

Preuve Puisque $a \wedge b = 1$ par Bezout, il existe (u, v) tel que $au + bv = 1$ en multipliant par c on en déduit $c = au + bcv$ et donc a divise c.

4.3. **PPCM de deux entiers.**

Définition 4.1. *On appelle* **plus petit multiple commun** *à deux entiers naturels non nuls a et b, l'entier naturel $PPCM(a,b)$ qui minimise l'ensemble des multiples strictement positifs communs à a et b.*

Définition 4.2. *Soient a et b deux entiers. $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, il existe donc un unique entier naturel noté $a \vee b$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.*

Proposition 4.3. *Soient a et b deux entiers naturels, alors $a \vee b = PPCM(a,b)$.*

Proposition 4.4. *Soient a et b deux entiers, alors $(ka \vee kb) = k.(a \vee b)$ pour tout $k \in \mathbb{N}$.*

Proposition 4.5. *Soient a et b deux entiers naturels, alors $(a \vee b).(a \wedge b) = ab$.*

Preuve On montre par Gauss que si $a \wedge b = 1$ alors $(a \vee b) = ab$. On en déduit que si a et b sont différents de 0 alors $\left(\frac{a}{a \wedge b} \vee \frac{b}{a \wedge b}\right) = \frac{ab}{(a \wedge b)^2}$.

4.4. **Nombres premiers.**

Définition 4.1. *On appelle* **nombre premier** *(ou irréductible) tout entier naturel différent de 0 et 1 qui n'est divisible que par lui-même et 1.*

Proposition 4.2. *Soient p un entier irréductible et a un entier alors $p \wedge a \in \{1, p\}$.*

Ce résultat est évident puisque $p \wedge a$ doit diviser p. On peut traduire cette proposition par le fait que si p ne divise pas a alors $a \wedge p = 1$. On en déduit par Gauss que si p divise un produit de termes ab et si p ne divise pas a alors p divise b. Ceci peut encore se traduire par la proposition suivante.

Proposition 4.3. *Si p est un entier irréductible alors $p\mathbb{Z}$ est un idéal premier.*

Remarque : Réciproquement pour p un entier naturel, si $p\mathbb{Z}$ est un idéal premier alors p est bien un entier irréductible.

Théorème fondamental de l'arithmétique *Tout entier naturel différents de 0 et 1, peut se décomposer de manière unique à l'ordre près des facteurs comme produit d'entiers irreductibles. C'est à dire que pour tout $n \in \mathbb{N} \setminus \{0,1\}$ il existe k couples $(p_i, \alpha_i)_{1 \leq i \leq k}$ où les p_i sont des nombres premiers distincts et n_i des entiers naturels non nuls tels que $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.*

On peut utiliser la décompostion en nombres premiers des entiers pour calculer les PGCD ou les PPCM.

4.5. **L'anneau $\mathbb{Z}/n\mathbb{Z}$.** Soit n un entier naturel naturel non nul et soient a et b des entiers relatifs. On dit que a est **congru** à b modulo n (que l'on note $a \equiv b\ [n]$) si et seulement si n divise $a - b$. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de ses classes d'équivalence. L'ensemble $\mathbb{Z}/nZ$ peut être muni naturellement d'une addition et d'un produit qui en fait un anneau commutatif (en fait, $\mathbb{Z}/n\mathbb{Z}$ est l'anneau quotient de $\mathbb{Z}$ par $n\mathbb{Z}$).

Vrai ou faux ?

1) l'entier 908070605040302010 est divisible par 9.

2) L'entier 12 est le reste de la division euclidienne de -45 par 19.

3) Le PGCD de 585 et 247 est 13.

4) L'entier 9123 est premier.

4bis) L'entier $2^{13} - 1$ est premier.

5) Pour tout $n \in \mathbb{N}$ sans facteur carré, $\sqrt{n}$ est irrationnel.

6) On a $2^{18} \equiv -1$ [37].

Quelques exercices

Exercice de cours

1) Soient a et b des entiers (relatifs). On dit que a divise b (ou encore que a est un diviseur de b) (ou encore que b est un multiple de a) s'il existe $q \in \mathbb{Z}$ tel que $b = aq$.
1a) Montrer que si a divise b, il existe un unique $q \in \mathbb{Z}$ tel que $b = aq$.
1b) Soit n un entier positif et d un diviseur de n. Montrer que $-n \leq d \leq n$.
1c) Soient a, b, c des entiers. Montrer que
- Si a divise b et b divise c, alors a divise c ;
- Si a divise b et b divise a, alors $|a| = |b|$;
- Si a divise b et c, alors a divise $b + c$.

1d) Démontrer le théorème 1.1, puis le corollaire 1.2.
1e) Montrer que $\mathbb{Z}$ est un anneau principal.
1f) Montrer que $\mathbb{Z}$ est un anneau intègre.
2a) Soient a et b des entiers naturels. Montrer qu'il existe des entiers (relatifs) u et v tels que $PGCD(a, b) = au + bv$ (Théorème de Bezout). En déduire une preuve du théorème 2.6. Ecrire la relation de Bezout pour $a = 585$ et $b = 247$.
2b) Soient $n \in \mathbb{N}^*$, $(a_1, ..., a_n) \in \mathbb{Z}^{*n}$. Montrer que a_1, ...,a_n sont premiers dans leur ensemble (c'est à dire $PGCD(a_1, ..a_n) = 1$) si et seulement s'il existe $(u_1, ..u_n) \in \mathbb{Z}^n$ tel que $\sum_{i=1}^{n} x_i u_i = 1$.
2c) Soient a et b des entiers positifs. Montrer que tout diviseur de a et b divise $PGCD(a, b)$, et que, pour tout $n \in \mathbb{N}$, $PGCD(na, nb) = nPGCD(a, b)$.
2d) Démontrer le théorème de Gauss (Théorème 2.7).
3a) Montrer que l'ensemble des nombres premiers est infini.
3b) Soit $n \geq 2$. Montrer que si n n'est pas premier, alors il existe un facteur premier p de n (c'est à dire un nombre premier p qui divise n) tel que $p \leq \sqrt{n}$. En déduire l'ensemble des nombres premiers inférieurs à 121.
3c) Soient a et b des entiers naturels et soit p un nombre premier. Montrer que si p divise ab, alors p divise a ou p divise b (Lemme d'Euclide).
3d) Soit p un nombre premier. Montrer que si k est un entier tel que $0 < k < p$, alors p divise le coefficient binomial C_k^p.
3e) Démontrer le théorème fondamental de l'arithmétique.
4) Soit $n \in \mathbb{N}$.
4a) Trouver tous les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

4b) Pour quelles valeurs de n, $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre ? un corps (commutatif) ?
4c) Montrer que si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a + c \equiv b + d\ [n]$ et $ac \equiv bd\ [n]$.
4d) Montrer que, si a est un entier, le reste de la division euclidienne de a par n est l'unique entier x tel que $a \equiv x\ [n]$ et $0 \leq x < n$.
4e) Retrouver les critéres de divisibilité par 2, 3, 5, 9 et 11.

Exercice 1
1) Trouver tous les entiers x et y tels que $637x+595y = 91$. Même question avec l'équation $637x + 595y = 143$.
2) Résoudre dans $\mathbb{N}^*$, $PGCD(x, y) = 18$ et $PPCM(x, y) = 540$.
3a) Vérifier que 442 et 495 sont premiers entre eux.
3b) Trouver tous les $(u, v) \in \mathbb{Z}^2$ tels que $442u + 495v = 1$.
3c) Résoudre $\overline{442}x = \overline{314}$ d'inconnue $x \in \mathbb{Z}/495\mathbb{Z}$ ($\overline{y}$ désigne la classe de y dans $\mathbb{Z}/495\mathbb{Z}$).

Exercice 2
On rappelle qu'un nombre entier est composé s'il n'est pas premier. Montrer que les nombres suivants sont composés.
1a) $n^4 - n^2 + 16$ où $n \in \mathbb{Z}$;
1b) $4n^3 + 6n^2 + 4n + 1$ où $n \in \mathbb{N}^*$;
1c) $2^{4n+2} + 1$ où $n \in \mathbb{N}^*$.
2) Quels sont les nombres premiers qui sont somme de deux nombres composés.

Exercice 3
Résoudre les équations diophantiennes suivantes dans l'ensemble indiqué.
1) $xy = 2x + 3y$ dans $\mathbb{Z}^2$.
2) $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{5}$ dans $\mathbb{Z}^{*2}$.
3) $x^3 + xy + y^3 = 209$ dans $\mathbb{N}^2$.
4) $3^x = 8 + y^2$ dans $\mathbb{N}^2$.
5) $x^2 + 5y^2 = 3$ dans $\mathbb{Z}^2$.

Exercice 4
Soit $(a, b) \in \mathbb{N}^2$ tel que $\dfrac{1}{2}(a^3 + b^3)$ soit un nombre premier. Montrer que $a = b = 1$.

Exercice 5
1) Soient x et y des entiers. On suppose que $3x + 7y$ est multiple de 11. Montrer que $4x - 9y$ est multiple de 1.
2) Si a et b sont des entiers, quelle est la congruence de $a^2 + b^2$ modulo 4 ? En déduire que si p est un nombre premier différent de 2 et s'il existe des entiers a et b tels que $p = a^2 + b^2$, alors $p - 1$ est multiple de 4.
3) Montrer que pour tout entier x non divisible par 3, x^3 est congru à 1 ou à -1 modulo 9. En déduire qu'il n'existe pas d'entiers a, b, c, tous non divisibles par 3, tels que $a^3+b^3 = c^3$.

Exercice 6
1) Soit a un entier positif. Montrer qu'il existe un entier u tel que $au \equiv 1\ [n]$ si et seulement si a et n sont premiers entre eux.
2) Soit $b \in \mathbb{Z}$. Trouver tous les entiers x tels que $24x \equiv b\ [182]$.

Exercice 7
1) Soient n et k des entiers supérieurs ou égaux à 2 et premiers entre eux. Montrer que

pour tout entier a et b, il existe un entier x tel que $x \equiv a\ [n]$ et $x \equiv b\ [k]$ (Théorème chinois des restes).
2) Soient $n \in \mathbb{N}^*$, a_1,...,$a_n \in \mathbb{N}^*$ des entiers premiers entre eux deux à deux. On pose $a = \Pi_{i=1}^n a_i$. Montrer que pour tout $(b_1, ..b_n) \in \mathbb{Z}^n$, il existe $\beta \in \mathbb{Z}$ tel que

$$\forall x \in \mathbb{Z}, ((\forall i \in \{1, ..n\}, x \equiv b_i\ [a_i]) \Longleftrightarrow (x \equiv \beta\ [a])).$$

3) Trouver tous les entiers $x \in \mathbb{Z}$ tels que $x \equiv 3\ [17]$ et $x \equiv 5\ [19]$.
4) Trouver tous les entiers $x \in \mathbb{Z}$ tels que $x \equiv 2\ [18]$ et $x \equiv 11\ [45]$.
5) Trouver tous les entiers $x \in \mathbb{Z}$ tels que $x \equiv 4\ [5]$, $x \equiv 3\ [6]$ et $x \equiv 2\ [7]$.

Exercice 8
1) Montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les $k\mathbb{Z}$ où $k \in \mathbb{N}$.
2) Déterminer les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$.

Exercice 9
1) Soit p un nombre premier. Montrer que si x est un entier, $x^p \equiv x\ [p]$ (Petit théorème de Fermat).
2) Soit p un nombre premier. Montrer que si l'entier x n'est pas un multiple de p, alors $x^{p-1} \equiv 1\ [p]$.
3) Calculer 7^{1998} modulo 13.
4) Montrer que pour tout $n \in \mathbb{Z}$, 42 divise $n^7 - n$.
5) Soient p premier, $(a, b) \in \mathbb{Z}^2$ tel que $a^p \equiv b^p\ [p]$. Montrer que $a^p \equiv b^p\ [p^2]$.

Exercice 10
1) Soit p un nombre premier et a un entier naturel qui n'est pas un multiple de p.
1a) Montrer qu'il existe un plus petit entier k tel que $a^k \equiv 1\ [p]$.
1b) Soit $n \in \mathbb{N}$. Montrer que l'on a $a^n \equiv 1\ [p]$ si et seulement si n est multiple de k.
2a) Démontrer que $5^8 \equiv -1\ [17]$.
2b) En déduire que 16 est le plus petit entier naturel k tel que $5^k \equiv 1\ [17]$.
2c) Soit a un entier tel que $1 \leq a \leq 16$. Montrer qu'il existe $n \in \mathbb{N}$ tel que $5^n \equiv a\ [17]$.
2d) Trouver tous les entiers naturels n tels que $5^n \equiv 3\ [17]$.
3a) Soient a et r deux entiers relatifs premiers entre eux. Montrer qu'il existe $k \in \mathbb{N}^*$ tel que $a^k \equiv 1\ [r]$.
3b) Soient a et r deux entiers avec $a > r \geq 2$. Montrer que la suite arithmétique de premier terme a et de raison r contient une infinité de termes ayant tous les mêmes diviseurs premiers.

Exercice 11
1) Montrer que $10^6 \equiv 1\ [7]$. Montrer aussi que pour tout entier $n \geq 1$, $10^n \equiv 4\ [6]$.
2) En déduire que pour tout entier $n \geq 1$, $10^{10^n} \equiv 4\ [7]$.

Exercice 12
Le but est de résoudre l'équation (E) $x^2 + 1 \equiv 0\ [65]$.
1) Montrer qu'un entier vérifie cette équation si et seulement si l'on ($x \equiv 5\ [5]$ ou $x \equiv 8\ [13]$) et ($x \equiv 2\ [5]$ ou $x \equiv 3\ [5]$).
2) Soient m et n deux entiers tels que l'on ait $5m + 13n = 0$. Montrer que 13 divise m et 5 divise n.
3) Trouver des entiers u et v tels que l'on ait $13u + 5v = 1$.
4) Trouver toutes les solutions entières de l'équation (E).

Exercice 13
1) Résoudre dans $\mathbb{Z}$ l'équation $6x^2 + 5x + 1 = 0$.
2) Montrer que pour tout p premier, il existe $n \in \mathbb{N}$ tel que $6n^2 + 5n + 1 \equiv 0\ [p]$.
3) Montrer que ce résultat subsiste dans le cas où p est un entier naturel non nul quelconque (pour cela, montrer que p peut s'écrire $p = 2^k(2m + 1)$ avec k, m dans $\mathbb{Z}$).

Exercice 14
Montrer qu'il existe un multiple de 1996 dont l'écriture décimale ne comporte que le chiffre 4.

Exercice 15
1) Soit $p \in \mathbb{N}$ avec $p \geq 2$. Montrer que p est premier si et seulement si $(p-1)! \equiv -1\ [p]$ (Théorème de Wilson).
2) Soit $n \in \mathbb{N}$ avec $n \geq 5$. Montrer que si $n + 2$ est premier, alors $n! - 1$ est composé (c'est à dire, n'est pas premier).
3) Soit p un nombre premier impair. Montrer que $2((p-3)!) \equiv -1\ [p]$.
4) Soit p premier. Montrer que pour tout $n \in \mathbb{Z}$, p divise $n^p + n(p-1)!$.

Exercice 16
1) Déterminer une condition nécessaire sur $m \in \mathbb{N}$ pour que 2^m soit premier.
On pose pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$; F_n est le n-ième nombre de Fermat.
2) Vérifier que F_0, F_1, F_2, F_3 et F_4 sont des nombres premiers. Montrer que F_5 est divisible par 641 (on pourra observer que $641 = 5^4 + 2^4 = 1 + 5 \times 2^7$).
3) Prouver que si $n \neq m$ alors F_n et F_m sont premiers entre eux. Retrouver le théorème d'Euclide : il existe une infinité de nombres premiers.
4) Si p est un diviseur de F_p, montrer que $p \equiv 1\ [2^{n+1}]$. Expliquer pourquoi on en vient naturellement à essayer 641 comme diviseur de F_5.

Exercice 17
Montrer que l'ensemble des nombres premiers congrus à 3 modulo 4 est infini.

Exercice 18
On note $\sigma(n)$ la somme des diviseurs de $n \in \mathbb{N}^*$. Montrer que $\sigma(n) \leq n + n\ln n$.

5. Polynômes

Quelques rappels

Dans la suite, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

Un **polynôme** P à coefficients dans $\mathbb{K}$ est une suite (a_n) d'éléments de $\mathbb{K}$ telle qu'il existe $p \in \mathbb{N}$ vérifiant $a_n = 0$ pour tout $n > p$.

Soit P le polynôme (a_n), soit Q le polynôme (b_n) et soit $\lambda \in \mathbb{K}$. Les polynômes $P + Q$, $\lambda\ P$ et PQ sont respectivement définis comme étant les polynômes $(a_n + b_n)$, (λa_n) et (c_n) où $c_0 = a_0 b_0$ et pour tout $n \in \mathbb{N}^*$, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Soit $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. Alors, $\mathbb{K}[X]$ muni des opérations définis précédemment est une

algèbre. En particulier, $\mathbb{K}[X]$ est un anneau commutatif.

Notons X le polynôme $(0,1,0,0,...)$. On pose $P^0 = 1$ et, pour tout $n \in \mathbb{N}^*$, on note P^n le polynôme $\overbrace{P.P.....P}^{n \text{ fois}}$. Alors, tout polynôme P de $K[X]$ s'écrit de manière unique sous la forme $P = a_n X^n + ... + a_1 X + a_0$ où a_0, a_1,...,a_n sont dans $\mathbb{K}$ et $a_n \neq 0$. L'entier n s'appelle le **degré** de P et on le note $\deg P$. Le coefficient a_n s'appelle le **coefficient dominant** de P et $a_n X^n$ s'appelle le **monôme de plus haut degré** de P. Si $a_n = 1$, on dit que le polynôme P est **unitaire**.

Soient P et Q deux polynômes dans $\mathbb{K}[X]$. On dit que P **divise** Q (ou que P est un **diviseur** de Q, ou encore que Q est un **multiple** de P) s'il existe $R \in \mathbb{K}[X]$ tel que $Q = P\ R$. L'anneau $\mathbb{K}[X]$ est intègre.

Soient A et B des polynômes dans $\mathbb{K}[X]$ (avec $B \neq 0$). Alors, il existe des polynômes Q et R uniques tels que $A = BQ + R$ et $R = 0$ ou $\deg R < \deg B$. Le polynôme Q s'appelle le quotient et le polynôme R s'appelle le reste de la **division euclidienne** de A par B. Ceci implique que l'anneau $\mathbb{K}[X]$ est euclidien, donc principal (voir la feuille sur anneaux et corps).

Si P et Q sont deux polynômes non nuls, alors il existe un unique polynôme unitaire de plus grand degré qui divise P et Q. Ce polynôme s'appelle le **plus grand commun diviseur** de P et Q, et se note $PGCD(P,Q)$. Notons que si R est le reste de la division euclidienne de P par Q, alors $PGCD(P,Q) = PGCD(Q,R)$, ceci permet d'élaborer un algorithme de calcul du PGCD : l'**algorithme d'Euclide**. On dit que les polynômes P et Q sont **premiers entre eux** si $PGCD(P,Q) = 1$.

Théorème de Bezout. Soient P et Q deux polynômes non nuls. Si $D = PGCD(P,Q)$, alors il existe des polynômes U et V tels que $D = UP + VQ$.
En particulier, P et Q sont premiers entre eux si et seulement s'il existe des polynômes U et V tels que $UP + VQ = 1$.

Théorème de Gauss. Soient P, Q, R des polynômes non nuls. Si P divise QR et si P et Q sont premiers entre eux, alors P divise R.

Si P et Q sont deux polynômes non nuls, alors il existe un unique polynôme unitaire de plus bas degré qui est un multiple de P et Q. Ce polynôme s'appelle le **plus petit commun diviseur** et se note $PPCM(P,Q)$.

Un polynôme P est dit **irréductible** (ou **premier**) si $\deg P > 1$ et P n'admet comme diviseur que les polynômes de la forme α ($\alpha \in \mathbb{K} \setminus \{0\}$) et βP ($\beta \in \mathbb{K} \setminus \{0\}$). Tout polynôme P de degré au moins 1 admet une décomposition unique (à l'ordre près des facteurs et à des constantes de $\mathbb{K} \setminus \{0\}$ près) en produit de polynômes irréductibles.

Soit P le polynôme $P(X) = a_n X^n + ... + a_1 X + a_0$ (avec a_n) et soit $a \in \mathbb{K}$. On pose $P(a) = a_n x^n + ... + a_1 a + a_0$. La fonction de K dans K qui à tout élèment $x \in \mathbb{K}$ associe $P(x)$ s'appelle la **fonction polynôme** associée à P.
L'équation $P(x) = 0$ d'inconnue $x \in \mathbb{K}$ et où $P \in \mathbb{K}[X]$ s'appelle **équation algébrique**.
Soit P un polynôme et soit $a \in \mathbb{K}$. On dit que a est une **racine** de P si $P(a) = 0$. Dans ce cas, le plus grand entier positif r tel que $(X-a)^r$ divise P s'appelle l'**ordre de**

multiplicité de a dans P. Si $r = 1$, on dit que la racine est **simple**. Si $r \geq 2$, on dit que la racine est **multiple**. Un polynôme P est dit **scindé** s'il existe $\lambda \in \mathbb{K}$, $n \in \mathbb{N}^*$, x_1,.....,x_n tels que $P = \lambda \Pi_{i=1}^{n}(X - x_i)$ (où les x_i ne sont pas nécessairement distincts).

Soient $n \in \mathbb{N}^*$, x_1, ..., $x_n \in \mathbb{K}$. On appelle **fonctions symétriques élémentaires** de x_1, ..., x_n les σ_i, $i = 1, .., n$, donnés par

$$\begin{aligned}
\sigma_1 &= \sum_{j=1}^{n} x_j \\
\sigma_2 &= \sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2} \\
&\vdots \quad \vdots \\
\sigma_k &= \sum_{1 \leq i_1 < i_2 < \ldots < i_n \leq n} x_{i_1} x_{i_2} \ldots\ldots x_{i_k} \\
&\vdots \quad \vdots \\
\sigma_n &= x_1 x_2 \ldots\ldots\ldots x_n
\end{aligned}$$

Soient $n \in \mathbb{N}^*$, a_0, a_1, ..., $a_n \in \mathbb{K}$, tel que $a_n \neq 0$ et $P = \sum_{i=0}^{n} a_i X^i$. Supposons P scindé sur K, et notons x_1, ..., x_n les zéros de P. Alors, si on note σ_1,...., σ_n leurs fonctions symétriques élémentaires, on a

$$\begin{aligned}
\sigma_1 &= -\frac{a_{n-1}}{a_n} \\
&\vdots \quad \vdots \\
\sigma_k &= (-1)^k \frac{a_{n_k}}{a_n} \\
&\vdots \quad \vdots \\
\sigma_n &= (-1)^n \frac{a_0}{a_n}.
\end{aligned}$$

Soit le polynôme $P = \sum_{n=0}^{N} a_n X^n$. On appelle **polynôme dérivé** de P le polynôme noté P' défini par

$$P' = \sum_{n=1}^{N} n a_n X^{n-1}.$$

On pose $P^{(0)} = P$, $P^{(1)} = P$ et pour tout $k \in \mathbb{N}^*$, $P^{k+1} = (P^{(k)})'$. La **formule de Taylor** s'écrit $P(X) = \sum_{k=0}^{N} \frac{P^k(a)}{k!}(X - a)^k$.

Théorème de d'Alembert-Gauss. Tout polynôme non constant de $\mathbb{C}[X]$ a une racine dans $\mathbb{C}$.

Les polynômes irréductibles de $\mathbb{C}(X]$ sont les polynômes de degré 1 (donc tout polynôme de $\mathbb{C}[X]$ peut s'écrire comme un produit de polynôme de degré 1). Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans

racine réelle (donc tout polynôme de $\mathbb{R}[X]$ peut s'écrire comme produit de polynômes de degré 1 et de polynômes de degré 2 sans racine réelle).

Vrai ou faux ?

1) Le reste de la division euclidienne de $X^5 + X^2 + 1$ par $X^2 + X + 1$ est $2X - 1$.

2) Le reste de la division euclidienne de P par $X - a$ (où $a \in \mathbb{K}$) est $P(a)$.

3) Le PGCD de $X^4 + 4X^3 + X^2 - 16$ et de $X^3 + 3X^2 - 3X + 4$ est $X + 4$.

4) Le polynôme $X^3 - 2$ est un polynôme irréductible de $\mathbb{Q}[X]$.

5) Le polynôme $X^4 + 4X^3 + 10X^2 + 12X + 9$ n'a pas de racine multiple dans $\mathbb{C}$.

6) Les polynômes $X^5 + 3X^3 + 2X^2 - 4X + 8$ et $X^4 + X^3 + 6X^2 + 4X + 8$ ont une racine commune dans $\mathbb{C}$.

7) Soient Q un polynôme non nul et soit P un polynôme irréductible. Alors, ou bien P divise Q, ou bien P et Q sont premiers entre eux.

8) Soit $P \in \mathbb{R}[X]$. Pour tout $z \in \mathbb{C}$, $P(\overline{z}) = \overline{P(z)}$. (Variante : Les racines dans $\mathbb{C}$ de $P \in \mathbb{R}[X]$ de degré 2 sont des nombres complexes conjugués).

Quelques exercices

Exercice de cours

1) Démontrer que $\mathbb{K}[X]$ est un anneau commutatif, puis que $\mathbb{K}[X]$ est une algèbre.
2) Soient P, Q, R des polynômes dans $\mathbb{K}[X]$. Montrer que
- Si P divise Q, alors $\deg P \leq \deg Q$.
- Si P divise Q et si Q divise R, alors P divise R.
- Si P divise Q et si Q divise P, alors il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $P = \lambda Q$.
- Si P divise Q et R, alors P divise $Q + R$.

3) Montrer que l'anneau $\mathbb{K}[X]$ est intègre.
4) Montrer la proposition sur la division euclidienne, puis que $\mathbb{K}[X]$ est un anneau principal.
5a) Soient P et Q deux polynômes non nuls. Montrer que, si R est le reste de la division euclidienne de P par Q, alors $PGCD(P, Q) = PGCD(Q, R)$.
5b) Soient P et Q deux polynômes non nuls. Montrer que les quotients de P et Q par $PGCD(P, Q)$ sont des polynômes premiers entre eux.
6) Soient P et Q deux polynômes non nuls.
6a) Montrer que tout diviseur de P et Q divise $PGCD(P, Q)$.
6b) Montrer que pour polynôme unitaire R, $PGCD\ (RP, RQ) = R\ PGCD\ (P, Q)$.
7) Soient P un polynôme et a un élément de $\mathbb{K}$.
7a) Montrer que le reste de la division de P par $X - a$ est $P(a)$.
7b) Montrer que a est racine de P si et seulement si le polynôme $X - a$ divise P.
7c) Montrer que si P est de degré n ($n \in \mathbb{N}$), alors P a au plus n racine.
7d) Montrer que a est racine multiple de P si et seulement si $P(a) = P'(a) = 0$.
8) Soit P un polynôme de degré 2 ou 3. Montrer que P est irréductible si et seulement si

P n'a pas de racine dans $\mathbb{K}$.

Exercice 1

1) Trouver une CNS sur $(\lambda, \mu) \in \mathbb{R}^2$ pour que $X^4 + \lambda X^3 + \mu X^2 + 12X + 4$ soit le carré d'un polynôme de $\mathbb{R}[X]$.

2) Soit $n \in \mathbb{N}^*$. En utilisant $(1+X)^{2n}(1-X)^{2n} = (1-X^2)^{2n}$, montrer que

$$\sum_{k=0}^{2n} (-1)^k \left(C_{2n}^k\right)^2 = (-1)^n C_{2n}^n.$$

3) Soit $n \in \mathbb{N}^*$. Pour $k = 0, ..., n$, on note $P_k = (X+k)^k$. Montrer que $(P_k)_{0 \leq k \leq n}$ est une base de l'espace vectoriel des polynômes de $\mathbb{R}[X]$ de degré au plus n.

4) Soient $(\alpha, \beta)^2 \in \mathbb{C}^2$ tel que $\alpha \neq \beta$ et soit $A \in \mathbb{C}[X]$. Montrer qu'il existe un unique polynôme $P \in \mathbb{C}[X]$ tel que $P(X-\alpha) + P(X-\beta) = A$.

Exercice 2

1) Résoudre dans $\mathbb{R}[X]$ l'équation $X(X+1)P'' + (X+2)P' - P = 0$.

2) Résoudre dans $\mathbb{C}[X]$ l'équation $P(2X) = P'(X)P''(X)$.

3) Montrer que pour tout $n \in \mathbb{N}$, il existe un unique $P_n \in \mathbb{Q}[X]$ tel que $P_n - P_n' = X^n$, puis calculer P_n.

Exercice 3

1) Trouver tous les $a \in \mathbb{R}$ tels que $X^2 - aX + 1$ divise $X^4 - X + a$ dans $\mathbb{R}[X]$.

2a) Quel est, pour $n \in \mathbb{N}^*$ et $\theta \in \mathbb{R}$ fixés, le reste noté R de la division euclidienne de $P = (X \sin\theta + \cos\theta)^n$ par X^2+1 dans $\mathbb{C}[X]$?

2b) Montrer que les reste de la division de P par $(X^2+1)^2$ est de la forme $(X^2+1)(cX+d) + R(X)$ où c et d sont des nombres réels.

2c) Calculer c et d (on pourra dériver l'égalité exprimant la division de P par $(X^2+1)^2$).

3) Soient a un nombre complexe non nul et n, k des entiers positifs tels que $n > k$.

3a) Notons q le quotient et r le reste de la division euclidienne de n par k. Montrer que le reste de la division euclidienne de $X^n - a^n$ par $X^k - a^k$ est $a^{kq}(X^r - a^r)$.

3b) Notons d le PGCD de n et k. Montrer que le plus grand diviseur de $X^n - a^n$ et $X^k - a^k$ est $X^d - a^d$.

4) Soit $n \in \mathbb{N}$. Trouver le reste de la division euclidienne de $X^{2n+1} + (X+1)^{n+2}$ par $X^2 + X + 1$ dans $\mathbb{C}[X]$.

5) Soient $n \in \mathbb{N}^*$, $(a, b) \in \mathbb{C}^2$ avec $a \neq b$, $A = (X-a)^{2n} + (X-b)^{2n}$ et $B = (X-a)^2(X-b)^2$. Déterminer le reste de la division euclidienne de A par B.

Exercice 4

1a) Trouver tous les $P, Q \in \mathbb{Q}[X]$ tels que $(X^6-1)P + (X^{10}-1)Q = X^2+1$.

1b) Trouver tous les $P, Q \in \mathbb{Q}[X]$ tels que $(X^6-1)P + (X^{10}-1)Q = X^3 + X^2 - X - 1$.

2a) Les polynômes $X^5+3X^3+2X^2-4X+8$ et $X^4+X^3+6X^2+4X+8$ ont-ils une racine commune dans $\mathbb{C}$? En déduire toutes les racines complexes de $X^4+X^3+6X^2+4X+8$.

2b) Le polynôme $X^4 + 4X^3 + 10X^2 + 12X + 9$ a-t-il une racine multiple dans $\mathbb{C}$? En déduire toutes les racines complexes de $X^4 + 4X^3 + 10X^2 + 12X + 9$.

3a) Montrer que les polynômes X^4+1 et X^3+1 sont premiers entre eux.

3b) Trouver tous les polynômes U et V de $\mathbb{Q}[X]$ tels que $(X^4+1)U - (X^3+1)V = 2$.

3c) Trouver tous les polynômes $P \in \mathbb{Q}[X]$ tels que X^4+1 divise P et X^3+1 divise $P-2$.

4) Calculer le PPCM de $X^3 - 7X - 6$, $X^3 - 3X + 2$ et $X^3 - 4X^2 + 3X$.

Exercice 5

1a) Trouver la décomposition de X^4+1 en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$.
1b) Quels sont les polynômes unitaires de degré 2 de $\mathbb{R}[X]$ qui divisent X^4+1 ?
1c) Montrer que X^4+1 est un polynôme irréductible de $\mathbb{Q}[X]$.
2a) Trouver la décomposition de X^4-2 en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$.
2b) Quels sont les polynômes unitaires de degré 2 de $\mathbb{R}[X]$ qui divisent X^4-2 ?
2c) Montrer que X^4-2 n'a pas de racine dans $\mathbb{Q}$.
2d) Montrer que X^4-2 est un polynôme irréductible de $\mathbb{Q}[X]$.

Exercice 6

1) Soit $n \in \mathbb{N}$ avec $n \geq 2$. On pose $P = 1 + X + \dfrac{X^2}{2!} + .. + \dfrac{X^n}{n!}$. Montrer que toutes les racines complexes de P sont simples.
2) Soit $P \in \mathbb{R}[X]$ défini par $P = X^4 + X^3 + X^2 + 3$. Montrer que P n'a pas de racine réelle. Est-il irréductible dans $\mathbb{R}[X]$?
3) Soit P le polynôme dans $\mathbb{Q}[X]$ défini par $P = X^3 - X^2 - 2$.
3a) Soient $p \in \mathbb{Z}$ et $q \in \mathbb{N}$ tels que $PGCD(p,q) = 1$. Montrer que si $\dfrac{p}{q}$ est racine de P, alors $q = 1$.
3b) Montrer que P n'a pas de racine rationnelle. Est-il irréductible dans $\mathbb{Q}[X]$?

Exercice 7

Soient $n \in \mathbb{N}^*$, $(a,b) \in \mathbb{K}^2$ (avec $\mathbb{K}$ sous-corps de $\mathbb{C}$), $A = 1 - abX^2$, $B = 1 - (a+b)X + abX^2$. Former le reste et le quotient de la division suivant les puissances croissantes de A par B jusqu'à l'ordre n.

Exercice 8

1) Résoudre dans $\mathbb{C}$ le système suivant

$$\begin{cases} x + y + z = 3 \\ xy + yz + zx = 2 \\ x^3 + y^3 + z^3 = 9 \end{cases}$$

2) Trouver une CNS sur $\lambda \in \mathbb{C}$ pour que deux des zéros z_1, z_2, z_3 de $z^3 + 5z^2 - 8z + \lambda = 0$ vérifient $z_1 + z_2 = -1$. Dans ce cas, résoudre l'équation.

Exercice 9

1) Soit $n \in \mathbb{N}^*$. Former la décomposition en polynômes irréductibles de $\mathbb{C}[X]$ de $P = \sum_{k=0}^{n} X^k$. En déduire la valeur de $\Pi_{k=1}^{n} \sin\left(\dfrac{k\pi}{n+1}\right)$.
2) On considère le polynôme $P = X^5 + X + 1$.
2a) Montrer que P n'a pas de racine dans $\mathbb{Q}$.
2b) Montrer que $P(j) = 0$ où $j = e^{\frac{2i\pi}{3}}$.
2c) Quelle est la décomposition de P en produit de pôlynomes irréductibles dans $\mathbb{Q}[X]$?
3) On considère le polynôme $P = X^5 - 1$.
3a) Factoriser P en polynômes unitaires irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.
3b) Calculer $\cos\frac{2\pi}{5}$ et $\sin\frac{2\pi}{5}$.
4) Soit $P = X^5 + 7X^4 + 17X^3 + 17X^2 + 7X + 1$.
4a) Vérifier que -1 est racine de P.
4b) Montrer que P a deux racines multiples que l'on précisera.

4c) Factoriser P en produit de polynômes irréductibles dans $\mathbb{Q}[X]$, puis dans $\mathbb{R}[X]$.

Exercice 10

1) Montrer que $P = X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$. On désigne par α une de ses racines complexes et on pose $A = \{a + b\alpha + c\alpha^2, a, b, c \in \mathbb{Q}\}$.
2) En étudiant $\phi : \mathbb{Q}[X] \to \mathbb{C}$ défini par $\phi(S) = S(\alpha)$, montrer que A est un sous-anneau de $\mathbb{C}$. Montrer que A est un sous-corps de $\mathbb{C}$.
(Voir aussi l'exercice 14 dans la feuille sur anneaux et corps)

Exercice 11

1) Dans quels corps a-t-on $X^4 - X^2 + 1 = (X^2 - 5X + 1)(X^2 + 5X + 1)$?
1) Dans l'anneau $\mathbb{Z}/15\mathbb{Z}[X]$, effectuer la division euclidienne de $P(X) = 5X^3 + X + 8$ par $Q(X) = 8X^2 + 4X + 1$.
3) Soit K un corps de caractéristique différente de 2. Dans $K[X]$, montrer que $Q(X) = X^3 + X^2 + X + 1$ divise $P(X) = X^n(X^3 + 2X^2 + 2X + 2)^n + X^{4n} - X^4 - 1$ si et seulement si n est pair.
4)Soit $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$.
4a) Faire la liste de tous les polynômes de degré 1,2,3 de $\mathbb{K}[X]$. Préciser pour chacun s'il est scindé, irréductible.
4b) Dans $\mathbb{K}[X]$, le polynôme $X^4 + X^2 + 1$ admet-il des racines ? Est-il irréductible ?
4c) Dans $\mathbb{K}[X]$, le polynôme $X^4 + 1$ admet-il des racines ? Est-il irréductible ? Même question dans $\mathbb{Z}[X]$.
4d) Montrer que si un polynôme est irréductible dans $\mathbb{K}[X]$, alors il est irréductible dans $\mathbb{Z}[X]$.
4e) Montrer que $X^4 + X + 1$ est irréductible dans $\mathbb{K}[X]$ et donc dans $\mathbb{Z}[X]$.

6. Fractions rationnelles

Quelques rappels

Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. Sur $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$, on définit la relation d'équivalence $(A_1, B_1)\mathcal{R}(A_2, B_2) \Leftrightarrow A_1B_2 = A_2B_1$. L'ensemble des classes d'équivalence est noté $\mathbb{K}(X)$ et ses éléments s'appellent les **fractions rationnelles à une indéterminée et à coefficients dans** $\mathbb{K}$. On définit sur $\mathbb{K}(X)$ une loi d'addition par $(A, B) + (C, D) = (AD + BC, BD)$ et une loi de multiplication par $(A, B)(C, D) = (AB, CD)$. Alors $(K(X), +.)$ est un corps commutatif. On définit aussi une loi externe par $\alpha(A, B) = (\alpha A, B)$. Alors $K(X)$ est une algèbre associative, commutative et unitaire et $K[X]$ est la sous-algèbre des polynômes.
On note dorénavant $\dfrac{A}{B}$ la classe de (A, B).

Pour toute fraction rationnelle $F \in \mathbb{K}(X)$, il existe une représentation $F = \dfrac{A}{B}$ tel que A et B soient des polynômes premiers entre eux. Ce représentant est appelé **forme irréductible** de F.
On appelle **degré** de la fraction rationnelle $F = \dfrac{A}{B}$ l'entier $\deg\left(\dfrac{A}{B}\right) = \deg A$ - $\deg B$.
Soient F une fraction rationnelle et $\dfrac{A}{B}$ un représentant irrductible de F. Toute racine de multiplicité k de B est dite **pôle d'ordre k** de F et toute racine de multiplicité k de A

est dite **racine d'ordre k** de F.

Soient F une fraction rationnelle et $\frac{A}{B}$ un représentant irréductible de F. On définit la **fonction rationnelle** $\tilde{F} : \Delta_F \to K \quad x \to \tilde{F}(x) = \frac{\tilde{A}(x)}{\tilde{B}(x)}$ où Δ_F est le complémentaire dans $\mathbb{K}$ de l'ensemble des pôles de F.

A toute fraction rationnelle $F \in K(X)$, on peut associer un et un seul polynôme E tel que le degré de la fraction $F - E$ soit strictement négatif. Alors, E est la **partie entière** de F. Pratiquement, on effectue la division euclidienne de A par B (où $\frac{A}{B}$ est la forme irréductible de F) : $A = BE + R$ et donc

$$\frac{A}{B} = E + \frac{R}{B}.$$

Décomposition en éléments simples dans $\mathbb{C}$

Soit $F = \frac{A}{B}$ sous forme irréductible. Si on note E sa partie entière, on a alors

$$F = E + \sum_{i=n}^{n} \left(\sum_{j=1}^{k_i} \frac{\alpha_{i,j}}{(X - a_i)^j} \right)$$

où $a_1, \cdots, a_n$ sont les racines complexes distinctes de B et $k_1, \cdots, k_n$ leur multiplicité, et où les $\alpha_{i,j} \in \mathbb{C}$.

On appelle **partie polaire** associée au pôle a_i de multiplicité k_i la somme $\sum_{j=1}^{k_i} \frac{\alpha_{i,j}}{(X - a_i)^j}$.

On détermine cette partie polaire de la façon suivante : si a est un pôle d'ordre k, on écrit la fraction rationnelle sous la forme : $\frac{A(X)}{(X-a)^k} C(X)$ et on pose : $A(Y + a) = P(Y)$ et $C(Y + a) = Q(Y)$. On calcule ensuite le quotient $a_0 + a_1 Y + \cdots + a_{k-1} Y^{k-1}$ de la division de $P(Y)$ par $Q(Y)$ suivant les puissances croissantes de Y et à l'ordre $k - 1$. Alors la partie polaire relative au pôle a est

$$\frac{a_0}{(X-a)^k} + \frac{a_1}{(X-a)^{k-1}} + \cdots + \frac{a_{k-1}}{(X-a)}$$

Si $\frac{A}{B}$ est une fraction irréductible de $K(X)$ présentant un pôle simple en a, la partie polaire est donné par $\frac{A(a)}{B'(a)(X-a)}$.

Décomposition en éléments simples dans $\mathbb{R}$

Soit $F = \frac{A}{B}$ irréductible avec $\deg B \geq 1$ et soit E sa partie entière. On peut alors écrire

$$B = b \prod_{i=1}^{n} (X - a_i)^{k_i} \prod_{j=1}^{m} (X^2 + p_j X + q_j)^{l_j}$$

où $a_1, \cdots, a_n$ sont les racines réelles distinctes de B et $k_1, \cdots, k_n$ leur multiplicité, et où les $p_j,\ q_j \in \mathbb{R}$.

D'où, $F = E + \sum_{i=1}^{n} \left(\sum_{r=1}^{k_i} \frac{\alpha_{i,r}}{(X - a_i)^r} \right) + \sum_{j=1}^{m} \left(\sum_{s=1}^{l_j} \frac{\beta_{j,s} X + \gamma_{j,s}}{(X^2 + p_j X + q_j)^s} \right)$ avec $\alpha_{i,j},\ \beta_{i,j},\ \gamma_{i,j}$

dans $\mathbb{R}$.

Quelques éléments pour le calcul pratique des coefficients

(1) Calcul de la partie entière : division euclidienne

(2) Décomposition de B pour déterminer les pôles et leurs ordres

(3) Cas d'un pôle simple : Si a est un pôle simple, le coefficient de $\frac{1}{X-a}$ est donné par $\frac{A(a)}{B'(a)}$ si la fraction est écrite sous la forme $\frac{A(X)}{B(X)}$ et par $\frac{A(a)}{C(a)}$ si F est donnée par $\frac{A(X)}{(X-a)C(X)}$

(4) Cas d'un pôle multiple

(a) Pour un ordre élévé, on utilise la division suivant les puissances croissantes.

(b) Pour une multiplicité de 2 ou 3, on peut parfois utiliser des points particuliers.

(c) Pour le calcul de β_{j,l_j} et γ_{j,l_j}, on peut procéder de la façon suivante : on multiplie par $(X^2+p_jX+q_j)^{l_j}$ puis on prend pour valeurs de X les deux racines complexes du polynômes. Ensuite, on itère le procédé à partir de la fraction rationnelle $\frac{A}{B} - \frac{\beta_{j,l_j}X+\gamma_{j,l_j}}{(X^2+p_jX+q_j)^{l_j}}$

(d) Si $E=0$, on peut multiplier par une même puissance de X et égaler les parties entiéres obtenues.

(e) On peut utiliser la parité de la fonction.

(f) On peut aussi utiliser les limites l'infini ...

Vrai ou faux ?

1) La décomposition en éléments simples dans $\mathbb{R}$ de $\frac{3}{X^3+1}$ est de la forme

$$\frac{a}{X+1}+\frac{b}{X^2-X+1}.$$

2) La décomposition en éléments simples dans $\mathbb{R}$ de $\frac{X^4+1}{(X-1)^3(X-2)}$ est de la forme

$$1+\frac{a}{(X-1)^3}+\frac{b}{(X-1)^2}+\frac{c}{X-1}+\frac{d}{X-2}.$$

3) La décomposition en éléments simples dans $\mathbb{C}$ de $\frac{X^4+1}{(X+i)(X^2-2i)}$ est de la forme

$$aX+b+\frac{c}{X+i}+\frac{d}{X+1+i}+\frac{e}{X-1-i}.$$

4) La décomposition en éléments simples dans $\mathbb{C}$ de $\frac{1}{(X-i)^3}$ est $\frac{1}{(X-i)^3}$.

Quelques exercices

Exercice de cours

1) Montrer que $(\mathbb{K}(X), +, .)$ est un corps commutatif.

2) Montrer que la définition du degré d'une fraction rationnelle ne dépend pas du représentant choisi.

3) Montrer l'existence et l'unicité de la forme irréductible d'une fraction rationnelle.

4) Montrer l'existence et l'unicité de la décomposition en éléments simples dans $\mathbb{R}$ et $\mathbb{C}$.

Exercice 1

1) Montrer qu'il n'existe pas de $F \in \mathbb{K}(X)$ (où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$) tel que $F^2 = X$.

2) Soit $P \in \mathbb{R}[X]$ de degré $n \in \mathbb{N}$ tel que $P(-1) \neq 0$ et $-\dfrac{P'(-1)}{P(-1)} \leq \dfrac{n}{2}$. Démontrer que P admet au moins un zéro dans $\mathbb{C}$ de module ≥ 1.

Exercice 2

Décomposer en éléments simples sur $\mathbb{R}$ les fractions rationnelles suivantes.

1) $\dfrac{X^3+1}{(X-1)^4}$;

2) $\dfrac{3}{X^3+1}$;

3) $\dfrac{X^4+1}{(X-1)^2(X^2+1)}$;

4) $\dfrac{X^4+1}{(X-1)^3(X-2)}$;

5) $\dfrac{2X^3+1}{(X+1)(X^2-3X+2)}$;

6) $\dfrac{2X}{X^4+X^2+1}$;

7) $\dfrac{X^5+1}{X^3(X-2)}$;

8) $\dfrac{1}{(X-1)^4(X+2)^3}$;

9) $\dfrac{2X^2+5}{(X^2-1)^3}$;

10) $\dfrac{X}{(X-1)^2(X-2)}$;

11) $\dfrac{X^{2n}}{(X^2+1)^n}$ $(n \in \mathbb{N}^*)$;

12) $\dfrac{X^8-X^4+2}{(X^2+X+1)^3}$;

13) $\dfrac{X}{(X-1)^2(X^2+1)^2}$.

Exercice 3

Décomposer en éléments simples sur $\mathbb{C}$ les fractions rationnelles suivantes.

1) $\dfrac{X^4+1}{(X-i)(X^2-2i)}$;

2) $\dfrac{X^2-1}{(X^2+1)^2}$;

3) $\dfrac{(X^2+1)^2}{(X+1)^2(3X^2-2X+1)}$;

4) $\dfrac{1}{X^n-1}$ $(n \in \mathbb{N}^*)$;

5) $\dfrac{X^4+1}{X(X^2-1)^2}$;

6) $\dfrac{X^6}{(X-1)^4(X^2+1)}$.

Exercice 4

1) Soit α une racine complexe du polynôme X^2+X+1.

1a) Montrer que $(1,\alpha)$ est une base de $\mathbb{C}$. Calculer les coordonnées de α^3 et de $(1+\alpha)^2$.

1b) Décomposer en éléments simples dans $\mathbb{R}$ la fraction rationnelle $\dfrac{X^4+1}{(X+1)^2(X^2+X+1)}$.

2) Décomposer en éléments simples dans $\mathbb{R}$ la fraction rationnelle $\dfrac{X}{(X-1)^2(X^2+1)^2}$.

3) Même question avec $\dfrac{X^2+2}{(X^2+1)^3(X^2+X+1)}$.

Exercice 5

Soit $P \in \mathbb{C}[X]$. On note α_1,...., α_p les racines de P, et k_1,...., k_p leur ordre de multiplicité.

1) Montrer que la décomposition de la fraction rationnelle $\dfrac{P'}{P}$ est

$$\frac{P'}{P} = \frac{k_1}{X-\alpha_1} + ... \frac{k_p}{X-\alpha_p}.$$

2) On suppose que la partie réelle de chacun des α_j $(j=1,..,p)$ est positive ou nulle. Montrer que les racines de P' sont de partie réelle positive ou nulle.

Exercice 6

Soeint P et Q des éléments de $\mathbb{C}[X]$. On pose $A = \dfrac{P}{Q}$.

1) On suppose que α est une racine simple de Q. Montrer que dans la décomposition de A en éléments simples dans $\mathbb{C}(X)$, l'élément simple dont le dénominateur est $X-\alpha$ est $\dfrac{a}{X-\alpha}$ où $a = \dfrac{P(\alpha)}{Q'(\alpha)}$.

2) En utilisant 1), décomposer en éléments simples dans $\mathbb{C}[X]$ les fractions rationnelles $\dfrac{nX^{n-1}}{X^n-1}$ et $\dfrac{1}{X^n-1}$ (on notera ω_1,..,ω_n les racines n-ièmes de l'unité dans $\mathbb{C}$).

3) Soit $P \in \mathbb{C}[X]$ n'admettant que des racines simples non nulles x_1,..,x_n. Montrer (en utilisant la question 1) que $\displaystyle\sum_{i=1}^{n} \frac{1}{x_i P'(x_i)} = -\frac{1}{P(0)}$. Que vaut $\displaystyle\sum_{i=1}^{n} \frac{1}{P'(x_i)}$?