Mathématiques spéciales

Corrigé de la feuille d'exercices n°6

Exercices obligatoires : 1 ; 2 ; 10 ; 13 ; 16 ; 22 ; 24 ; 30.

Exercices en groupes :

- exo n°5 Groupe 1 : Adrien ; Daniel ; Clément ; Maxime ;
- exo n°11 Groupe 2 : Raphaël ; Ernest ; Camil ; Constant ;
- exo n°21 Groupe 3 : Luca ; Michèle ; Tredy ; Malarvijy ;
- exo n°37 Groupe 4 : Lucas ; Augustin ; Ambroise ; Rayan ;
- exo n°39 Groupe 5 : Maxence ; Thibaut ; Ingrid ; Sébastien ;

1. Idéaux d'un anneau commutatif

a. Exercices basiques

Exercice 1.

Soit $(A, +, \times)$ un anneau commutatif et M une partie de A. On appelle annulateur de M l'ensemble des $x \in A$ tels que $xy = 0$ pour tout $y \in M$. Démontrer que l'annulateur de M est un idéal de $(A, +, \times)$.

Correction.

Notons I cet ensemble. Il suffit d'appliquer la définition. En effet, prenons $u, v \in I$ et $a \in A$. Alors, pour tout $y \in M$, on a

$$(u - v)y = uy - vy = 0$$

et

$$(au)y = a(uy) = 0.$$

Ainsi, $u - v$ et au sont dans I qui est un idéal.

Exercice 2.

On appelle nilradical d'un anneau commutatif $(A, +, \times)$ l'ensemble de ses éléments nilpotents, c'est-à-dire l'ensemble des $x \in A$ pour lesquels il existe $n \geq 1$ de sorte que $x^n = 0$. Démontrer que le nilradical de A est un idéal de A.

Correction.

Notons $N(A)$ le nilradical de A. D'abord $0 \in N(A)$ qui est donc non vide. Prenons ensuite $a \in A$, $x, y \in N(A)$, et m, n de sorte que $x^m = y^n = 0$. Remarquons d'abord que

$$(ax)^m = a^m x^m = 0$$

et donc $ax \in N(A)$. De plus, par la formule du binôme de Newton, on a

$$(x+y)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} x^k y^{n+m-1-k}.$$

Or, si $k \geq m$, alors $x^k = 0$ et si $k < m$, c'est-à-dire $k \leq m-1$, alors $n+m-1-k \geq n$ et $y^{n+m-1-k} = 0$. On a bien $(x+y)^{n+m-1} = 0$ et $x+y \in N(A)$. Il est très facile de vérifier que l'on a aussi $-x \in N(A)$. Finalement, on a bien prouvé que $N(A)$ est un idéal de A.

Exercice 3.

Soit A un anneau commutatif.

1. On suppose que A n'admet que les idéaux triviaux $\{0\}$ et A. Démontrer que A est un corps.
2. On suppose que A est intègre et qu'il n'admet qu'un nombre fini d'idéaux. Démontrer que A est un corps.

Correction.

1. Soit $x \in A \backslash \{0\}$. Alors l'idéal engendré par x ne peut pas être l'idéal $\{0\}$, donc c'est A tout entier. En particulier, il existe $y \in A$ tel que $yx = xy = 1_A$. C'est bien que A est un corps.
2. Prenons toujours $x \in A \backslash \{0\}$ et considérons les idéaux $I_n = x^n A$. Alors puisque A admet un nombre fini d'idéaux, il existe $n < p$ tel que $x^n A = x^p A$. En particulier, il existe $a \in A$ tel que $x^n = x^p a$. Ceci entraîne $x^n(1 - x^{p-n}a) = 0$. L'anneau étant intègre (et x étant non nul), ceci entraine que $x^{p-n}a = 1$. x est alors inversible, d'inverse $x^{p-n-1}a$.

Exercice 4.

Soit (I_n) une suite croissante d'idéaux de $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps. Démontrer que la suite (I_n) est stationnaire.

Correction.

Méthode 1 : Il existe un unique polynôme unitaire P_n tel que $I_n = (P_n)$. De plus, la condition $I_n \subset I_{n+1}$ entraîne que $P_{n+1} | P_n$. La suite $(\deg(P_n))$ est donc une suite d'entiers naturels décroissante : elle est stationnaire. Soit $p \in \mathbb{N}$ tel que, pour tout $p \geq n$, on a $\deg(P_n) = \deg(P_p)$. On a alors $P_n | P_p$, P_n et P_p sont unitaires et de même degré, donc ils sont égaux et $I_n = I_p$. La suite (I_n) est bien stationnaire. Méthode 2 : Posons $I = \bigcup_n I_n$. Puisque la suite (I_n) est croissante, il est facile de vérifier que I est un idéal. Il existe $P \in \mathbb{K}[X]$ tel que $I = (P)$. Mais alors, il existe $N \in \mathbb{N}$ tel que $P \in I_N$. On prouve alors que pour tout $n \geq N$, on a $I_n = (P)$. En effet, on a $I_n \subset I = (P)$,

et $P \in I_N \subset I_n \implies (P) \subset I_n$.

Exercice 5.

Soit $(\mathbb{D}, +, \times)$ l'anneau des nombres décimaux, c'est-à-dire l'ensemble des nombres de la forme $\frac{n}{10^k}$, avec $n \in \mathbb{Z}$ et $k \in \mathbb{N}$. Démontrer que cet anneau est principal.

Correction.

Soit I un idéal de $\mathbb{D}$. Alors $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, qui est un anneau principal. Il existe donc $a \in \mathbb{Z}$ tel que $I \cap \mathbb{Z} = a\mathbb{Z}$. On va prouver que $I = a\mathbb{D}$. Il est d'abord clair que $a\mathbb{D} \subset I$ puisque $a \in I$ et que I est un idéal. Réciproquement, soit $x = \frac{n}{10^k} \in I$. Alors $n = 10^k x \in I \cap \mathbb{Z}$ et donc $n = am$ pour un certain $m \in \mathbb{Z}$. Ainsi, $x = \frac{m}{10^k} a \in a\mathbb{D}$. Les idéaux de $\mathbb{D}$ sont donc les parties de $\mathbb{D}$ du type $a\mathbb{D}$, avec $a \in \mathbb{Z}$.

Exercice 6.

On souhaite étudier dans cet exercice les idéaux de $\mathbb{Z}^2$.

1. Soit I un idéal de $\mathbb{Z}^2$ et $I_1 = \{x \in \mathbb{Z};\ (x, 0) \in I\}$, $I_2 = \{y \in \mathbb{Z};\ (0, y) \in I\}$. Démontrer que I_1 et I_2 sont deux idéaux de $\mathbb{Z}$.
2. Démontrer que $I = I_1 \times I_2$.
3. Conclure.

Correction.

1. I_1 est non-vide car $(0, 0) \in I$. Soient $x, y \in I$ et $k \in \mathbb{Z}$. Alors $(x - y, 0) = (x, 0) - (y, 0) \in I$ et $(kx, 0) = (k, 2025) \times (x, 0) \in I$ d'où $x - y$ et $kx \in I_1$. I_1 est un idéal de $\mathbb{Z}^2$ et la preuve est similaire pour I_2.
2. Soit $(x, y) \in I_1 \times I_2$. Alors $(x, 0) \in I$, $(0, y) \in I$ d'où $(x, y) = (x, 0) + (0, y) \in I$. Ainsi, on a $I_1 \times I_2 \subset I$. Réciproquement, si $(x, y) \in I$, alors $(x, 0) = (1, 0) \times (x, y) \in I$ et donc $x \in I_1$. De même, $y \in I_2$ et donc $(x, y) \in I_1 \times I_2$.
3. $\mathbb{Z}$ étant principal, il existe des entiers a et b tels que $I_1 = a\mathbb{Z}$ et $I_2 = b\mathbb{Z}$. Alors d'après la question précédente, $I = a\mathbb{Z} \times b\mathbb{Z} = (a, b)\mathbb{Z}^2$.

b. Exercices d'entraînement

Exercice 7.

Soit $(A, +, \times)$ un anneau commutatif. Si I et J sont deux idéaux de A, on note

$$\begin{aligned} I + J &= \{i + j;\ i \in I,\ j \in J\} \\ I.J &= \{i_1 j_1 + \cdots + i_n j_n;\ n \geq 1,\ i_k \in I,\ j_k \in J\} \end{aligned}$$

On dit que deux idéaux I et J sont étrangers si $I + J = A$.

1. Montrer que $I+J$ et IJ sont encore des idéaux de A.
2. Montrer que $I.J \subset I \cap J$.
3. Montrer que $(I+J).(I \cap J) \subset I.J$.
4. Montrer que si I et J sont étrangers, alors $I.J = I \cap J$.

Correction.

1. Commençons par $I+J$. Il faut d'abord démontrer que c'est un sous-groupe de $(A,+)$. Mais $0 = 0+0 \in I+J$. D'autre part, si x et y sont éléments de $I+J$, on les écrit $x = i+j$, $y = i'+j'$, et on a
$$x - y = (i-i') + (j-j') \in I+J$$
puisque $i-i' \in I$ et $j-j' \in J$. D'autre part, pour $a \in A$, on a, par distributivité de $\times$ par rapport à $+$:
$$ax = ai + aj \in I+J$$
puisque, I et J étant deux idéaux, $ai \in I$ et $aj \in J$. Ceci prouve que $I+J$ est un idéal. Passons maintenant à $I.J$: $0 \times 0 = 0$ est élément de $I.J$. De plus, si $x = \sum_{k=1}^{n} i_k j_k$ et $y = \sum_{l=1}^{m} i'_l j'_l$, en posant $i_k = -i'_{k-n}$ et $j'_k = -j'_{k-n}$ pour k allant de $n+1$ à $n+m$, on a
$$x - y = \sum_{k=1}^{n+m} i_k j_k$$
ce qui prouve que $I.J$ est un sous-groupe de $(A,+)$. Enfin, pour tout a dans A, on a
$$ax = \sum_{k=1}^{n} (ai_k) j_k \in I.J$$
puisque chaque ai_k (resp. j_k) est élément de I (resp. de J).
2. Soit $x = \sum_{k=1}^{n} i_k j_k$ un élément de $I.J$. Pour chaque k, $i_k j_k$ est un élément de I puisque I est un idéal. Comme I est de plus stable par la somme, $I.J$ est bien contenu dans I. Par symétrie du rôle joué par I et J, $I.J$ est aussi contenu dans J et donc $I.J$ est contenu dans $I \cap J$.
3. Soit $x \in (I+J).(I \cap J)$. On écrit $x = \sum_{k=1}^{n} a_k b_k$ avec $a_k \in I+J$ et $b_k \in I \cap J$. Puisque $I.J$ est un idéal, il suffit de prouver que $a_k b_k \in I.J$. On écrit $a_k = i_k + j_k$, de sorte que
$$a_k b_k = i_k b_k + b_k j_k.$$
C'est un élément de $I.J$, car $i_k \in I$, $b_k \in J$ et $b_k \in I$, $j_k \in J$.
4. Il suffit de prouver que $I \cap J \subset I.J$. D'après la question précédente, on a $A.(I \cap J) \subset I.J$. Prenons $x \in I \cap J$. Alors $x = 1_A x \in A.(I \cap J) \subset I.J$ Ceci prouve l'inclusion restante.

Exercice 8.

Soit p un nombre premier. On note
$$\mathbb{Z}_p = \left\{ x = \frac{m}{n};\ (m,n) \in \mathbb{Z} \times \mathbb{N}^*,\ p \wedge n = 1 \right\}.$$

1. Vérifier que $\mathbb{Z}_p$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2. Soit $k \geq 0$. On note
$$J_{p^k} = \left\{ \frac{m}{n};\ (m,n) \in \mathbb{Z} \times \mathbb{N}^*,\ p \wedge n = 1,\ p^k | m \right\}.$$
Vérifier que J_{p^k} est un idéal de $\mathbb{Z}_p$.
3. Réciproquement, montrer que si I est un idéal de A, il existe $k \geq 1$ tel que $I = J_{p^k}$.

Correction.

1. La preuve est facile et laissée au lecteur : le point clé est que si p est premier avec n et avec n', alors p est premier avec le produit nn'.
2. D'abord, on peut remarquer que $0 \in J_{p^k}$. Prenons ensuite $x = \frac{m}{n}$ et $y = \frac{m'}{n'}$ deux éléments de J_{p_k}. Alors
$$x - y = \frac{mn' - m'n}{nn'}$$
avec $p \wedge (nn') = 1$ (voir plus haut) et $p^k | m$, $p^k | m'$ et donc $p^k | mn' - m'n$. Ensuite, si $z = \frac{a}{b} \in \mathbb{Z}_p$, alors $xz = \frac{am}{bn}$ est tel que $p^k | am$ et $p \wedge (bn) = 1$, et donc $xz \in J_{p^k}$. J_{p^k} est bien un idéal de $\mathbb{Z}_p$.
3. Posons $k = \max\{l \geq 0;\ \forall x \in I,\ \exists (m,n) \in \mathbb{Z} \times \mathbb{N}^*, x = \frac{m}{n},\ p^l | m,\ p \wedge n = 1\}$ et prouvons que $I = J_{p^k}$. D'abord, il est clair que $I \subset J_{p^k}$. Réciproquement, soit $x \in J_{p^k}$, il faut prouver que $x \in I$. Par définition de k, on sait que l'on peut trouver $y = \frac{a}{b} \in I$ tel que $a = p^k a'$ avec $a' \wedge p = b \wedge p = 1$. Mais alors, $\frac{a'}{b}$ est inversible dans $\mathbb{Z}_p$, d'inverse $\frac{b}{a'}$. Puisque I est un idéal, ceci entraine que $p^k = y \times \frac{b}{a'} \in I$. Mais alors, puisque x s'écrit $x = p^k \frac{m'}{n}$ avec $p \wedge n = 1$, on en déduit que $x \in I$. On a bien démontré que tous les idéaux de $\mathbb{Z}_p$ sont de la forme J_{p^k}.

Exercice 9.

Soit $n \geq 2$. Démontrer que tous les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont principaux. A quelle condition $\mathbb{Z}/n\mathbb{Z}$ est-il principal ?

Correction.

Soit I un idéal de $\mathbb{Z}/n\mathbb{Z}$, et $J = \{m \in \mathbb{Z};\ \bar{m} \in I\}$. Alors J est un idéal de $\mathbb{Z}$. Il est non-vide car I est non-vide, et si $u, v \in J,\ k \in \mathbb{Z}$, alors
$$\overline{u+v} = \bar{u} + \bar{v} \in I \implies u + v \in J$$
$$\overline{ku} = \bar{k} \times \bar{u} \in I \implies ku \in J.$$
Ainsi, il existe $a \in \mathbb{Z}$ tel que $J = a\mathbb{Z}$. De plus, on peut aussi remarquer que, puisque $n\mathbb{Z} \subset J$, on doit avoir $a | n$. Démontrons alors que $I = \bar{a}\mathbb{Z}/n\mathbb{Z}$. Puisque $\bar{a} \in I$, il est clair que $\bar{a}\mathbb{Z}/n\mathbb{Z} \subset I$. Réciproquement, soit $\bar{u} \in \bar{a}\mathbb{Z}/n\mathbb{Z}$. Alors $\bar{u} = \bar{a} \times \bar{k} = \overline{ak}$ et donc $u \in a\mathbb{Z} + n\mathbb{Z} = a\mathbb{Z}$ puisque $a | n$. Ainsi, $\bar{u} \in I$, ce qui prouve l'inclusion réciproque. Ainsi, on a prouvé que tous les idéaux de $\mathbb{Z}/n\mathbb{Z}$

sont principaux. Pour que l'anneau lui-même soit principal, il faut encore qu'il soit intègre. Ceci n'est vrai que si n est premier.

Exercice 10.

Soit $\mathbb{Z}[i] = \{a + ib;\ a, b \in \mathbb{Z}^2\}$.

1. Démontrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
3. Soit $z \in \mathbb{C}$. Démontrer qu'il existe $\omega \in \mathbb{Z}[i]$ tel que $|z - \omega| < 1$.
4. Soient $u, v \in \mathbb{Z}[i]$ avec $v \neq 0$. Démontrer qu'il existe $q, r \in \mathbb{Z}[i]$ avec $u = qv + r$ et $|r| < |v|$. A-t-on unicité ?
5. Démontrer que $\mathbb{Z}[i]$ est principal.

Correction.

1. Il suffit de vérifier les propriétés... La preuve est laissée au lecteur !
2. Soit $a + ib$ un élément de $\mathbb{Z}[i]$ inversible. Son inverse est nécessairement le même que dans $\mathbb{C}$, c'est-à-dire
$$\frac{1}{a+ib} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}.$$
On ne peut pas avoir $(a, b) = (0, 0)$. Si $|a| \geq 2$, alors $\frac{a}{a^2+b^2}$ ne peut pas être un entier, et de même si $|b| \geq 2$, $\frac{b}{a^2+b^2}$ ne peut pas être un entier. On a donc $|a| \leq 1$ et $|b| \leq 1$. Mais le cas $(a, b) = (\pm 1, \pm 1)$ ne convient pas non plus. Donc les seules possibilités sont $(\pm 1, 0)$ et $(0, \pm 1)$ qui donnent effectivement des éléments inversibles. $\mathbb{Z}[i]$ possède donc 4 éléments inversibles : $1, -1, i, -i$.
3. Écrivons $z = x + iy$. On approche x et y par l'entier le plus proche : il existe $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. Mais alors, si on pose $\omega = a + ib$, on obtient
$$|z - \omega|^2 = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2} < 1.$$
4. D'après la question précédente, il existe $q \in \mathbb{Z}[i]$ tel que
$$\left|\frac{u}{v} - q\right| < 1.$$
Posons $r = v\left(\frac{u}{v} - q\right)$. Alors $|r| < |v|$ et on a bien $u = qv + r$. On n'a pas en général unicité de cette "division euclidienne" car on n'a pas unicité dans l'approximation de la question précédente. Prenons par exemple $u = 1 + i$ et $v = 2$, de sorte que u/v peut être approché par 0 ou 1 (ou aussi par i et $1 + i$). On peut alors écrire les deux divisions
$$1 + i = 0 \times 2 + (1 + i)$$
$$1 + i = 1 \times 2 + (-1 + i)$$
avec chaque fois le module du reste inférieur strict à 2.

5. Soit I un idéal de $\mathbb{Z}[i]$ non réduit à $\{0\}$. On considère $a \in I\backslash\{0\}$ tel que $|a|$ est minimal. Ceci a un sens, car $|z| \geq 1$ pour tout $z \in \mathbb{Z}[i]\backslash\{0\}$, et il y a seulement un nombre fini d'éléments de $\mathbb{Z}[i]$ de module inférieur à un réel donné. On va alors démontrer que I est l'idéal engendré par a. Pour cela, prenons $u \in I$ et effectuons la division euclidienne donnée par la question précédente :
$$u = qa + r \text{ avec } |r| < |a|.$$
Mais alors, $u \in I$, $qa \in I$ et donc $r \in I$. Par minimalité de $|a|$, on doit avoir $|r| = 0$, ce qui prouve que $u \in a\mathbb{Z}[i]$.

c. Exercices d'approfondissement

Exercice 11.

Soit A un anneau commutatif (unitaire). Si I est un idéal de A, on appelle radical de I l'ensemble $\sqrt{I} = \{x \in A;\ \exists n \geq 1,\ x^n \in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Soient I, J deux idéaux de A et $p \geq 1$. Montrer que
$$\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J},\ \sqrt{\sqrt{I}} = \sqrt{I} \text{ et } \sqrt{I^p} = \sqrt{I}.$$
3. Si $A = \mathbb{Z}$ et $I = k\mathbb{Z}$, $k \geq 1$, déterminer le radical de I.

Correction.

1. On commence par remarquer que si $x^n \in I$, alors pour tout $k \geq n$, $x^k = x^{k-n}x^n \in I$ (qui est un idéal). Montrons d'abord que $(\sqrt{I}, +)$ est un sous-groupe de $(A, +)$. En effet, $0 \in \sqrt{I}$ puisque $I \subset \sqrt{I}$ (prendre $n = 1$). De plus, si x est dans $\sqrt{I}$ alors $(-x)^n = (-1)^n x^n \in I$ puisque $x^n \in I$ et que I est un idéal. Prenons maintenant x, $y \in I$ et $n, m \in \mathbb{N}$ tels que $x^n \in I$, $y^m \in I$. Alors, par la formule du binôme que l'on peut appliquer dans l'anneau **commutatif** A, on a
$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$
Or, si $k \leq n$, alors $n + m - k \geq m$ et donc $y^{n+m-k} \in I$, ce qui entraine $x^k y^{n+m-k} \in I$. Si $k \geq n$, cette fois $x^k \in I$ et donc $x^k y^{n+m-k} \in I$. $(I, +)$ étant un sous-groupe de $(A, +)$, on en déduit que $(x+y)^{n+m} \in I$, c'est-à-dire $x + y \in \sqrt{I}$. Finalement, prouvons que pour $a \in A$ et $x \in \sqrt{I}$, alors $ax \in \sqrt{I}$. Soit $n \geq 0$ tel que $x^n \in I$. Alors $(ax)^n = a^n x^n \in I$, ce qui prouve le résultat.
2. <ul class="rien">
3. Soit $x \in \sqrt{I.J}$. Il existe $n \geq 1$ tel que $x^n \in I.J$, c'est-à-dire $x^n = \sum_k a_k b_k$ avec $a_k \in I$ et $b_k \in J$. Alors $x^n \in I$ puisque I est un idéal et $x^n = ab$, $a \in I$, et de même $x^n \in J$ (on utilise en fait que $I.J \subset I \cap J$). Ainsi, $x \in \sqrt{I \cap J}$. Soit maintenant $x \in \sqrt{I \cap J}$. Alors il existe $n \geq 1$ tel que $x^n \in I$ et $x^n \in J$. Donc $x \in \sqrt{I}$ et $x \in \sqrt{J}$, soit $x \in \sqrt{I} \cap \sqrt{J}$. Finalement, soit $x \in \sqrt{I} \cap \sqrt{J}$. Alors il existe $n, m \geq 1$ tels que $x^n \in I$ et $x^m \in J$. Alors $x^{n+m} = x^n x^m \in I.J$, et donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I.J}$.

4. On a $I \subset \sqrt{I}$ et donc $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Réciproquement, prenons $x \in \sqrt{\sqrt{I}}$. Il existe $n \geq 1$ tel que $x^n \in \sqrt{I}$. Posons $y = x^n \in \sqrt{I}$. Il existe $m \geq 1$ tel que $y^m \in I$. Alors, $x^{nm} = y^m \in I$ et donc $x \in \sqrt{I}$.
5. La dernière égalité se prouve de façon tout à fait identique !
6. Soit $x \in \mathbb{Z}$. x est dans $\sqrt{k\mathbb{Z}}$ si et seulement si il existe $n \geq 1$ tel que $x^n \in k\mathbb{Z}$. Autrement dit, $k|x^n$. Décomposons k en produits de facteurs premiers : $k = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. On obtient que $p_i|x^n \implies p_i|x$ pour tout $i = 1, \dots, r$ et donc $p_1 \dots p_r|x$, ce qui peut encore s'écrire $x \in (p_1 \dots p_r)\mathbb{Z}$. Réciproquement, si $x \in (p_1 \dots p_r)\mathbb{Z}$, alors, x s'écrit $x = p_1 \dots p_r m$. Notant $n = \max_{i \in \{1,\dots,r\}}(\alpha_i)$, on a $k|x^n$. Ainsi, on a prouvé que $\sqrt{I} = (p_1 \dots p_r)\mathbb{Z}$.

Exercice 12.

Soit $\mathbb{Z}[i] = \{a + ib;\ a, b \in \mathbb{Z}^2\}$.

1. Démontrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
3. Soit $z \in \mathbb{C}$. Démontrer qu'il existe $\omega \in \mathbb{Z}[i]$ tel que $|z - \omega| < 1$.
4. Soient $u, v \in \mathbb{Z}[i]$ avec $v \neq 0$. Démontrer qu'il existe $q, r \in \mathbb{Z}[i]$ avec $u = qv + r$ et $|r| < |v|$. A-t-on unicité ?
5. Démontrer que $\mathbb{Z}[i]$ est principal.

Correction.

1. Il suffit de vérifier les propriétés... La preuve est laissée au lecteur !
2. Soit $a + ib$ un élément de $\mathbb{Z}[i]$ inversible. Son inverse est nécessairement le même que dans $\mathbb{C}$, c'est-à-dire
$$\frac{1}{a+ib} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}.$$
On ne peut pas avoir $(a, b) = (0, 0)$. Si $|a| \geq 2$, alors $\frac{a}{a^2+b^2}$ ne peut pas être un entier, et de même si $|b| \geq 2$, $\frac{b}{a^2+b^2}$ ne peut pas être un entier. On a donc $|a| \leq 1$ et $|b| \leq 1$. Mais le cas $(a, b) = (\pm 1, \pm 1)$ ne convient pas non plus. Donc les seules possibilités sont $(\pm 1, 0)$ et $(0, \pm 1)$ qui donnent effectivement des éléments inversibles. $\mathbb{Z}[i]$ possède donc 4 éléments inversibles : $1, -1, i, -i$.
3. Écrivons $z = x + iy$. On approche x et y par l'entier le plus proche : il existe $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. Mais alors, si on pose $\omega = a + ib$, on obtient
$$|z - \omega|^2 = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2} < 1.$$
4. D'après la question précédente, il existe $q \in \mathbb{Z}[i]$ tel que
$$\left|\frac{u}{v} - q\right| < 1.$$
Posons $r = v\left(\frac{u}{v} - q\right)$. Alors $|r| < |v|$ et on a bien $u = qv + r$. On n'a pas en général unicité de cette "division euclidienne" car on n'a pas unicité dans l'approximation de la question

précédente. Prenons par exemple $u = 1 + i$ et $v = 2$, de sorte que u/v peut être approché par 0 ou 1 (ou aussi par i et $1 + i$). On peut alors écrire les deux divisions

$$1 + i = 0 \times 2 + (1 + i)$$

$$1 + i = 1 \times 2 + (-1 + i)$$

avec chaque fois le module du reste inférieur strict à 2.

5. Soit I un idéal de $\mathbb{Z}[i]$ non réduit à $\{0\}$. On considère $a \in I\backslash\{0\}$ tel que $|a|$ est minimal. Ceci a un sens, car $|z| \geq 1$ pour tout $z \in \mathbb{Z}[i]\backslash\{0\}$, et il y a seulement un nombre fini d'éléments de $\mathbb{Z}[i]$ de module inférieur à un réel donné. On va alors démontrer que I est l'idéal engendré par a. Pour cela, prenons $u \in I$ et effectuons la division euclidienne donnée par la question précédente :
$$u = qa + r \text{ avec } |r| < |a|.$$
Mais alors, $u \in I$, $qa \in I$ et donc $r \in I$. Par minimalité de $|a|$, on doit avoir $|r| = 0$, ce qui prouve que $u \in a\mathbb{Z}[i]$.

2. Anneaux $\mathbb{Z}/n\mathbb{Z}$

Exercice 13.

1. Est-ce que $\overline{18}$ est inversible dans $\mathbb{Z}/49\mathbb{Z}$? Si oui, quel est son inverse ?
2. Est-ce que $\overline{42}$ est inversible dans $\mathbb{Z}/135\mathbb{Z}$? Si oui, quel est son inverse ?

Correction.

1. 18 et 49 sont premiers entre eux, et donc $\overline{18}$ est inversible dans $\mathbb{Z}/49\mathbb{Z}$. Pour trouver son inverse, il faut résoudre l'équation de Bezout $18u + 49v = 1$. Avec l'algorithme d'Euclide ou un logiciel, on trouve que $7 \times 49 - 19 \times 18 = 1$. Ainsi, l'inverse de $\overline{18}$ dans $\mathbb{Z}/49\mathbb{Z}$ est $\overline{-19} = \overline{30}$.
2. 3 divise à la fois 42 et 135. Ainsi, 3 n'est pas inversible dans $\mathbb{Z}/135\mathbb{Z}$.

Exercice 14.

Résoudre, dans $\mathbb{Z}/37\mathbb{Z}$, les équations ou systèmes d'équations suivants :

1. $\bar{7}y = \bar{2}$.
2. $\begin{cases} \bar{3}x + \bar{7}y &= \bar{3} \\ \bar{6}x - \bar{7}y &= \bar{0} \end{cases}$

Correction.

1. On cherche d'abord l'inverse de $\bar{7}$ dans $\mathbb{Z}/37\mathbb{Z}$. Cela revient a résoudre l'équation de Bezout $7u + 37v = 1$. En appliquant l'algorithme d'Euclide, on trouve qu'une solution particulière

est donnée par $16 \times 7 - 3 \times 37 = 1$. Ainsi, $\overline{16}$ est inverse de $\overline{7}$ dans $\mathbb{Z}/37\mathbb{Z}$. Il vient

$$\overline{7}y = \overline{2} \iff \overline{16} \times \overline{7}y = \overline{16} \times \overline{2} \iff y = \overline{32}.$$

2. Nous omettons dans ces questions les "barres" au dessus des entiers. On additionne la première et la deuxième ligne pour trouver $9x = 3$. Or, $1 = 37 - 4 \times 9$ et donc -4 est un inverse de 9 dans $\mathbb{Z}/37\mathbb{Z}$. On trouve donc

$$9x = 3 \iff x = -4 \times 3 = -12 = 25.$$

Si on reporte dans la première équation, on obtient

$$3 \times (-12) + 7y = 3 \iff 7y = 39 = 2.$$

Le résultat de la question précédente nous donne $y = 32$. La solution unique est donc le couple $(\overline{25}, \overline{32})$.

Exercice 15.

Déterminer les inversibles de $\mathbb{Z}/8\mathbb{Z}$. Le groupe des inversibles $(\mathbb{Z}/8\mathbb{Z})^*$ est-il cyclique ?

Correction.

D'après le cours, les éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont les classes d'entiers k tels que $k \wedge 8 = 1$. On a donc

$$(\mathbb{Z}/8\mathbb{Z})^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

On remarque que tous ces éléments sont d'ordre 1 ou 2 (par exemple, $\overline{3}^2 = \overline{9} = 1$, $\overline{7}^2 = \overline{49} = \overline{1}$). Ainsi, aucun n'engendre $(\mathbb{Z}/8\mathbb{Z})^*$ et ce groupe n'est pas cyclique.

Exercice 16.

Résoudre

1. $x^2 + x + \overline{7} = \overline{0}$ dans $\mathbb{Z}/13\mathbb{Z}$.
2. $x^2 - \overline{4}x + \overline{3} = \overline{0}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Correction.

L'idée est de procéder comme pour la résolution habituelle d'une équation du second degré. On applique donc la méthode qui conduit au discriminant, c'est-à-dire que l'on met le trinôme sous forme canonique.

1. On peut remarque pour cette question que $\overline{14} = \overline{1}$. Ainsi,

$$x^2 + x + \overline{7} = \overline{0} \iff x^2 + \overline{14}x + \overline{7} = 0 \iff (x + \overline{7})^2 - \overline{42} = \overline{0}$$

soit encore $(x + \overline{7})^2 = \overline{3}$. On remarque alors que $\overline{4}^2 = \overline{3}$. Ainsi, l'équation est équivalente à

$$(x + \overline{7})^2 - \overline{4}^2 = 0 \iff (x + \overline{7} + \overline{4})(x + \overline{7} - \overline{4}) = 0.$$

Puisque $\mathbb{Z}/13\mathbb{Z}$ est un corps, et donc en particulier est intègre, ceci est encore équivalent à $x + \overline{11} = \overline{0}$ ou $x + \overline{3} = \overline{0}$. L'ensemble des solutions est donc $\{\overline{2}, \overline{10}\}$.

2. On procède de la même façon. L'équation est équivalente à

$$(x - \overline{2})^2 - \overline{1} = 0.$$

On peut bien sûr factoriser encore et obtenir que l'équation est équivalente à

$$(x - \overline{2} - \overline{1})(x - \overline{2} + \overline{1}) = 0.$$

Mais cette fois, **on ne peut pas aller plus loin** car $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps. Il faut plutôt écrire $(x - \overline{2})^2 = \overline{1}$ et chercher les t dans $\mathbb{Z}/12\mathbb{Z}$ avec $t^2 = \overline{1}$. Pour cela on dresse le tableau :

t	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
t^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$-\overline{3}$	$\overline{4}$	$\overline{1}$	$\overline{0}$

(on a bien sûr $(-t)^2 = t^2$). Ainsi, l'équation est équivalente $x - \overline{2} \in \{-\overline{5}, -\overline{1}, \overline{1}, \overline{5}\}$. L'ensemble des solutions est donc $\{-\overline{3}, \overline{1}, \overline{3}, \overline{7}\}$. Il y a en particulier plus de deux solutions à cette équation polynomiale de degré 2 !

Exercice 17.

Les groupes $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ et $(\mathbb{Z}/2\mathbb{Z})^3$ sont-ils isomorphes ?

Correction.

Non, ces groupes ne sont pas isomorphes. En effet, si f est un isomorphisme de G sur H, et si g est un élément de G d'ordre n, alors $f(g)$ est aussi d'ordre n. Or, ici, $\mathbb{Z}/8\mathbb{Z}$ est le seul des 3 groupes à avoir un élément d'ordre 8, tandis que $(\mathbb{Z}/2\mathbb{Z})^3$ est le seul à ne pas avoir d'éléments d'ordre 4. Ces 3 groupes ne sont pas deux à deux isomorphes.

Exercice 18.

1. Soient n, m, a trois entiers tels que $n \wedge m = 1$. Montrer que l'équation $nx \equiv a\ [m]$ admet une unique solution modulo m.
2. Soient n, m, a, b quatre entiers avec $n \wedge m = 1$. Montrer que le système

$$\begin{cases} x & \equiv & a\ [n] \\ x & \equiv & b\ [m]. \end{cases}$$

admet une unique solution modulo nm.

3. Un phare émet un signal jaune toutes les 15 secondes et un signal rouge toutes les 28 secondes. On aperçoit le signal jaune 2 secondes après minuit et le rouge 8 secondes après minuit. A quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?
4. Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait alors trois pièces. Mais les pirates se querellent et six d'entre eux sont tués. Le

cuisinier recevrait alors quatre pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés et le partage laisserait cinq pièces d'or à ce dernier. Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

Correction.

1. Puisque $n \wedge m = 1$, le théorème de Bezout nous donne l'existence de $u, v \in \mathbb{Z}$ tel que $un + vm = 1$. L'équation $nx \equiv a\ [m]$ implique $unx \equiv ua\ [m]$. Or, $un \equiv 1[m]$ et donc l'équation devient $x \equiv ua[m]$. Réciproquement, si $x \equiv ua\ [m]$, alors $nx \equiv nua \equiv a[m]$. Ainsi, l'ensemble des solutions de l'équation est $\{ua + mk;\ k \in \mathbb{Z}\}$.
2. On a l' équivalence suivante :

$$\begin{cases} x & \equiv & a\ [n] \\ x & \equiv & b\ [m] \end{cases} \iff \begin{cases} \exists k \in \mathbb{Z},\ x = a + nk \\ nk \equiv b - a\ [m]. \end{cases}$$

On applique alors le résultat de la question précédente pour obtenir les valeurs possibles de k. Soit $(u, v) \in \mathbb{Z}^2$ tels que $un + vm = 1$.

$$\begin{cases} x & \equiv & a\ [n] \\ x & \equiv & b\ [m] \end{cases} \iff \begin{cases} \exists k \in \mathbb{Z},\ x = a + nk \\ k \equiv u(b - a)\ [m] \end{cases}$$
$$\iff \begin{cases} \exists k \in \mathbb{Z},\ x = a + nk \\ \exists l \in \mathbb{Z},\ k = u(b - a) + ml. \end{cases}$$

On remplace alors k par sa valeur dans la première équation, et on trouve que x est solution si et seulement si il existe $l \in \mathbb{Z}$ tel que $x = a+nu(b-a)+nml$. On obtient bien des solutions qui sont uniques modulo nm.
3. On commence par mettre en équation le problème. Soit x les temps, en secondes depuis minuit, où les deux phares sont allumés au même moment. Les données du problème nous disent que x est solution du système :

$$\begin{cases} x & \equiv & 2\ [15] \\ x & \equiv & 8\ [28]. \end{cases}$$

On cherche le plus petit entier naturel x solution de ce système. Comme $15 \wedge 28 = 1$, on peut appliquer les résultats de la question précédente. Il suffit de chercher (u, v) tels que $15u + 28v = 1$. On applique l'algorithme d'Euclide :

$$\begin{aligned} 28 &= 15 \times 1 + 13 \\ 15 &= 13 \times 1 + 2 \\ 13 &= 6 \times 2 + 1 \end{aligned}$$

soit, en remontant les calculs

$$\begin{aligned} 1 &= -6 \times 2 + 1 \times 13 \\ &= -6 \times (15 - 13) + 13 = 7 \times 13 - 6 \times 15 \\ &= 7 \times (28 - 15) - 6 \times 15 \\ &= 7 \times 28 - 13 \times 15. \end{aligned}$$

x est donc le plus petit entier naturel de

$$\{2 + 15 \times (-13) \times (8 - 2) + 28 \times 15 \times k;\ k \in \mathbb{Z}\} = \{-1168 + 420k;\ k \in \mathbb{Z}\}.$$

Le plus petit entier naturel de cet ensemble est obtenu pour $k = 3$, et on trouve $x = 92$: les deux phares seront allumés au même moment pour la première fois 1 minute et 32 secondes après minuit.

4. Là encore, il faut traduire ceci en termes de congruences. On a :

$$\begin{cases} x & \equiv & 3\ [17] \\ x & \equiv & 4\ [11] \\ x & \equiv & 5\ [6] \end{cases}$$

Ce problème se traite exactement de la même façon. On peut aussi résoudre d'abord les deux premières équations ensembles, puis introduire dans la troisième. Ici, tout est facilité si on remarque que 37 est tel que $37 \equiv 3\ [17]$ et $37 \equiv 4\ [11]$. Puisque $17 \wedge 11 = 1$, on sait d'après la deuxième question que

$$\begin{cases} x & \equiv & 3\ [17] \\ x & \equiv & 4\ [11] \end{cases} \iff x \equiv 37[187].$$

On doit donc résoudre le système

$$\begin{cases} x & \equiv & 37\ [187] \\ x & \equiv & 5\ [6]. \end{cases}$$

Or, $1 = 1 \times 187 - 6 \times 37$. L'ensemble des solutions de ce système est donc :

$$\{37 + 187 \times 1 \times (5 - 37) + 1122k;\ k \in \mathbb{Z}\} = \{-5947 + 1122k;\ k \in \mathbb{Z}\}.$$

Le plus petit entier positif est obtenu pour $k = 6$ et donne 785. Le cuisinier est sûr d'obtenir au moins 785 pièces d'or.

Exercice 19.

1. Donner la liste des éléments de $\mathbb{Z}/7\mathbb{Z}$ qui sont des carrés. Combien y en a-t-il ?
2. Soit a un élément $\mathbb{Z}/7\mathbb{Z}$. Quel est le cardinal de l'ensemble $\{-x^2 + a : x \in \mathbb{Z}/7\mathbb{Z}\}$?
3. En déduire que, pour un a donné dans $\mathbb{Z}/7\mathbb{Z}$, l'équation $x^2 + y^2 = a$ a toujours une solution, où x, y sont dans $\mathbb{Z}/7\mathbb{Z}$.
4. Donner une solution explicite de l'équation $u^2 + v^2 \equiv -1 \pmod 7$, avec $u, v \in \mathbb{Z}$.

Correction.

1. On calcule les carrés de chacun des éléments :

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
x^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$

Les carrés de $\mathbb{Z}/7\mathbb{Z}$ sont donc $\bar{0}$, $\bar{1}$, $\bar{2}$ et $\bar{4}$.

2. Considérons l'application $\phi : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ définie par $\phi(y) = a - y$. Alors ϕ est injective : si $\phi(y) = \phi(y')$, on a $y = y'$. Puisque $\mathbb{Z}/7\mathbb{Z}$ est finie, elle est bijective. De plus, si on pose $C = \{x^2 : \ x \in \mathbb{Z}/7\mathbb{Z}\}$ et $D = \{a - x^2 : \ x \in \mathbb{Z}/7\mathbb{Z}\}$, alors $\phi(C) = D$. Ainsi, D a même cardinal que C, c'est-à-dire 4.
3. Reprenons les deux ensembles C et D de la question précédente. Ils possèdent tous les deux 4 éléments. Donc $\mathbb{Z}/7\mathbb{Z}$ possède 7 éléments, ils ne peuvent pas être disjoints. Ils possèdent donc un élement commun. Soit $z \in C \cap D$. Alors il existe x et y dans $\mathbb{Z}/7\mathbb{Z}$ tels que $z = x^2$ et $z = a - y^2$. En particulier, $x^2 + y^2 = a$.
4. Reprenons le tableau de la première question, en le complétant par le calcul de $-1 - x^2$:

$$\begin{array}{c|c|c|c|c|c|c|c} x & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ x^2 & \bar{0} & \bar{1} & \bar{4} & \bar{2} & \bar{2} & \bar{4} & \bar{1} \\ -1-x^2 & \bar{6} & \bar{5} & \bar{2} & \bar{4} & \bar{4} & \bar{2} & \bar{5} \end{array}$$

On remarque ainsi que si $x = \bar{2}$ et $y = \bar{3}$, alors $x^2 = -1 - y^2$, c'est-à-dire $x^2 + y^2 = -1$. Ainsi, si on pose $u = 2$ et $v = 3$, on a bien $u^2 + v^2 \equiv -1 \pmod 7$.

Exercice 20.

Soit $n \geq 3$ un entier.

1. Soit a un entier impair. Montrer que $a^{2^{n-2}} \equiv 1 \ [2^n]$.
2. Le groupe $\left(\mathbb{Z}/(2^n\mathbb{Z})\right)^*$ est-il cyclique ?

Correction.

1. On procède par récurrence sur n et on écrit $a = 2k + 1$. Pour $n = 3$, on a $(2k+1)^2 = 4k^2 + 4k + 1 = 1 + 4k(k+1)$. Or, $k(k+1)$ est un nombre pair car ou bien k, ou bien $k+1$ est pair. Ainsi, $4k(k+1)$ est divisible par 8 et $a^2 \equiv 1 \ [8]$. Supposons maintenant le résultat établi au rang n, c'est-à-dire que $a^{2^{n-2}} = 1 + u2^n$. On met tout au carré et on trouve :

$$\begin{aligned} a^{2^{(n+1)-2}} &= (1 + u2^n)^2 \\ &= 1 + 2u2^n + u^2 2^{2n} \\ &= 1 + 2^{n+1}(u + u^2 2^{n-1}) \end{aligned}$$

ce qui prouve bien le résultat au rang $n + 1$.

2. Soit $G = \left(\mathbb{Z}/(2^n\mathbb{Z})\right)^*$. Un élément $\overline{x}$ de $\mathbb{Z}/(2^n\mathbb{Z})$ est élément de G si et seulement si $x \wedge 2^n = 1$, si et seulement si $x \wedge 2 = 1$. Ainsi, on peut décrire G comme

$$G = \{\overline{x};\ 1 \leq x \leq 2^n,\ x \wedge 2 = 1\}.$$

Mais dans $\{1, \ldots, 2^n\}$, il y a exactement 2^{n-1} éléments impairs. Le cardinal de G est donc égal à 2^{n-1}. Or, pour $g = \overline{a} \in G$, la question précédente nous dit que

$$\{g^k; k \geq 0\} = \{g^k;\ 0 \leq k < 2^{n-2}\}.$$

Ce dernier ensemble comporte au plus 2^{n-2} éléments, et g n'est pas un élément cyclique de G. G n'est donc pas cyclique.

Exercice 21.

Le but de cet exercice est de montrer qu'il n'existe pas d'entier $n \geq 2$ tel que n divise $2^n - 1$. On raisonne par l'absurde et on supposons qu'un tel entier n existe. On note p le plus petit diviseur premier de n.

1. Montrer que $p > 2$.
2. On note m l'ordre de la classe de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$.
   (a) Montrer que $m|p-1$.
   (b) Montrer que $m|n$.
   (c) Conclure.

Correction.

1. Si $2|n$, alors $2|2^n - 1$ et donc $2^n - 1$ est pair, ce qui n'est pas le cas.
2. (a) Puisque p est premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe de cardinal $p-1$. D'après le théorème de Lagrange, l'ordre de tout élément divise $p-1$. Donc $m|p-1$.
   (b) Par hypothèse, $2^n \equiv 1\ [n]$ ce qui entraîne $2^n \equiv 1\ [p]$, ou encore $2^n = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. n est donc un multiple de l'ordre de 2, ou encore $m|n$.
   (c) Puisque p est le plus petit facteur premier de n, on a $n \wedge (p-1) = 1$. Ainsi, $m|\text{pgcd}(p-1, n) = 1$, et donc $m = 1$. C'est absurde puisque $2 \neq 1$ dans $\mathbb{Z}/p\mathbb{Z}$, $p \geq 3$. Il est donc impossible que n divise $2^n - 1$.

3. Arithmétique des polynômes

a. Exercices basiques

Exercice 22.

Résoudre les équations suivantes, où l'inconnue est un polynôme P de $\mathbb{R}[X]$:

1. $P(X^2) = (X^2+1)P(X)$ **2.** $P'^2 = 4P$
3. $P \circ P = P$.

Correction.

1. Le polynôme nul est évidemment solution. Sinon, si P est solution, alors on a

$$2\deg(P) = \deg(P) + 2$$

ce qui prouve que $\deg(P)$ doit être égal à 2. Maintenant, si $P(X) = aX^2 + bX + c$, alors

$$\begin{aligned} P(X^2) &= aX^4 + bX^2 + c \\ (X^2+1)P(X) &= aX^4 + bX^3 + (a+c)X^2 + bX + c. \end{aligned}$$

On en déduit que $b = 0$, puis que $a + c = 0$. Les solutions sont donc les polynômes qui s'écrivent $P(X) = a(X^2 - 1)$, $a \in \mathbb{R}$.

2. Là encore, le polynôme nul est solution, et c'est la seule solution constante. Par ailleurs, si P est une solution non constante, alors son degré vérifie l'équation

$$2(\deg(P)-1)=\deg(P)$$

ce qui entraîne que $\deg(P)=2$. Maintenant, si $P(X)=aX^2+bX+c$, alors

$$\begin{aligned} P'^2 &= (2aX+b)^2 = 4a^2X^2+4abX+b^2 \\ 4P &= 4aX^2+4bX+4c. \end{aligned}$$

Ceci entraîne $a^2=a$, donc $a=1$ (le polynôme est de degré 2, $a\neq 0$), puis $c=b^2/4$. Les polynômes solutions sont donc le polynôme nul et les polynômes $P(X)=X^2+bX+b^2/4$, avec $b\in\mathbb{R}$.

3. Si P est une solution qui n'est pas le polynôme nul, alors le degré de $P\circ P$ vaut $\deg(P)^2$, et donc on a l'équation

$$\deg(P)^2=\deg(P).$$

et donc $\deg(P)=1$ ou $\deg(P)=0$. Maintenant, si $P(X)=aX+b$, alors

$$\begin{aligned} P\circ P(X) &= a(aX+b)+b = a^2X+(ab+b) \\ P(X) &= aX+b. \end{aligned}$$

On doit donc avoir $a^2=a$, soit $a=1$ ou $a=0$, et $ab=0$. Si $a=1$, alors $b=0$ et si $a=0$, alors b peut être quelconque dans $\mathbb{R}$. Finalement, on trouve que les solutions sont les polynômes constants et le polynôme $P(X)=X$.

Exercice 23.

Calculer le quotient et le reste de la division euclidienne de

1. $X^4+5X^3+12X^2+19X-7$ par X^2+3X-1 ;
2. $X^4-4X^3-9X^2+27X+38$ par X^2-X-7 ;
3. X^5-X^2+2 par X^2+1.

Correction.

On trouve les résultats suivants :

1. Le quotient est X^2+2X+7, le reste est nul ;
2. Le quotient est X^2-3X-5, le reste est $X+3$;
3. Le quotient est X^3-X-1, le reste est $X+3$.

Exercice 24.

Soit $P\in\mathbb{K}[X]$, soit $a\in\mathbb{K}$ et soit R le reste de la division euclidienne de P par $(X-a)^2$. Exprimer R en fonction de $P(a)$ et de $P'(a)$.

Correction.

R est de degré au plus 1 et s'écrit donc $R(X) = \alpha X + \beta$. Évaluons la relation

$$P(X) = (X-a)^2 Q(X) + \alpha X + \beta$$

au point a. On trouve $P(a) = a\alpha + \beta$. Dérivons maintenant la relation précédente :

$$P'(X) = 2(X-a)Q(X) + (X-a)^2 Q'(X) + \alpha.$$

On évalue à nouveau en a et on trouve que

$$\alpha = P'(a).$$

En revenant à la première équation, on en déduit que $\beta = P(a) - aP'(a)$.

Exercice 25.

Soit $P \in \mathbb{R}[X]$, $a, b \in \mathbb{R}$, $a \neq b$. Sachant que le reste de la division euclidienne de P par $(X-a)$ vaut 1 et que le reste de la division euclidienne de P par $X-b$ vaut -1, que vaut le reste de la division euclidienne de P par $(X-a)(X-b)$?

Correction.

On sait que $P(X) = (X-a)Q_1(x) + 1$, et donc $P(a) = 1$. De même, on a $P(b) = -1$. La division euclidienne de P par $(X-a)(X-b)$ s'écrit

$$P(X) = (X-a)(X-b)Q(x) + \alpha x + \beta.$$

On évalue cette relation en a et en b, et on trouve le système

$$\begin{cases} \alpha a + \beta &= 1 \\ \alpha b + \beta &= -1. \end{cases}$$

La résolution de ce système ne pose pas de difficultés et donne comme unique solution

$$\alpha = \frac{2}{a-b} \text{ et } \beta = \frac{-a-b}{a-b}.$$

Le reste recherché est donc

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

Exercice 26.

Donner une condition nécessaire et suffisante sur $(\lambda, \mu) \in \mathbb{C}^2$ pour que X^2+2 divise $X^4 + X^3 + \lambda X^2 + \mu X + 2$.

Correction.

On réalise la division euclidienne de $X^4+X^3+\lambda X^2+\mu X+2$ par X^2+2, et on trouve :

$$X^4+X^3+\lambda X^2+\mu X+2=(X^2+2)(X^2+X+(\lambda-2))+(\mu-2)X+6-2\lambda.$$

Le polynôme X^2+2 divise donc $X^4+X^3+\lambda X^2+\mu X+2$ si et seulement si le reste est nul, donc si et seulement si $\mu=2$ et $\lambda=3$. Une autre possibilité est de remarquer que les racines de X^2+2 sont $\sqrt{2}i$ et $-\sqrt{2}i$, et donc que la décomposition en produits d'irréductibles de X^2+2 est $(X-\sqrt{2}i)(X+\sqrt{2}i)$. Pour que $X^4+X^3+\lambda X^2+\mu X+2$ soit divisible par X^2+2, il faut et il suffit que $\sqrt{2}i$ et $-\sqrt{2}i$ soient racines de $X^4+X^3+\lambda X^2+\mu X+2$. On évalue ce polynôme en $\sqrt{2}i$ et $-\sqrt{2}i$ et on trouve un système linéaire que doit vérifier le couple (λ,μ). On trouve bien sûr la même solution.

Exercice 27.

Déterminer les pgcd suivants :

1. $P(X)=X^4-3X^3+X^2+4$ et $Q(X)=X^3-3X^2+3X-2$;
2. $P(X)=X^5-X^4+2X^3-2X^2+2X-1$ et $Q(X)=X^5-X^4+2X^2-2X+1$;
3. $P(X)=X^n-1$ et $Q(X)=(X-1)^n$, $n\geq 1$.

Correction.

1. On applique l'algorithme d'Euclide. Le dernier reste non-nul donne un pgcd des deux polynômes. On a successivement :

$$\begin{aligned}
X^4-3X^3+X^2+4 &= (X^3-3X^2+3X-2)X+(-2X^2+2X+4)\\
X^3-3X^2+3X-2 &= (-2X^2+2X+4)\left(\frac{-X}{2}+1\right)+3X-6\\
(-2X^2+2X+4) &= (3X-6)\times\left(\frac{-2X}{3}-\frac{2}{3}\right).
\end{aligned}$$

   Un pgcd est donc $3X-6$ (ou $X-2$).

2. On répète le même procédé :

$$\begin{aligned}
X^5-X^4+2X^3-2X^2+2X-1 &= (X^5-X^4+2X^2-2X+1)1+2X^3-4X^2+4X-2\\
X^5-X^4+2X^2-2X+1 &= (2X^3-4X^2+4X-2)((X^2)/2+X/2)+X^2-X+1\\
2X^3-4X^2+4X-2 &= (X^2-X+1)(2X-2)+0
\end{aligned}$$

   Un pgcd des deux polynômes est donc X^2-X+1.

3. Les diviseurs non-constants de Q sont les polynômes du type $c(X-1)^p$, avec $1\leq p\leq n$. Parmi ces diviseurs, seuls ceux de la forme $c(X-1)$ divisent aussi P (par exemple, car 1 est racine simple et non double de P, ou bien parce qu'on sait comment décomposer P en produits d'irréductibles...). Ainsi, $P\wedge Q=X-1$.

Exercice 28.

Trouver deux polynômes U et V de $\mathbb{R}[X]$ tels que $AU + BV = 1$, où $A(X) = X^7 - X - 1$ et $B(X) = X^5 - 1$.

Correction.

On utilise l'algorithme d'Euclide. On a

$$\begin{aligned} X^7 - X - 1 &= (X^5 - 1)X^2 + X^2 - X - 1 \\ X^5 - 1 &= (X^2 - X - 1)(X^3 + X^2 + 2X + 3) + 5X + 2 \\ X^2 - X - 1 &= (5X + 2)(X/5 - 7/25) - 11/25. \end{aligned}$$

On remonte ensuite les calculs. On va partir plutôt de

$$11 = -25(X^2 - X - 1) + (5X - 7)(5X + 2)$$

pour éviter de trainer des fractions. On trouve alors successivement :

$$\begin{aligned} 11 &= -25(X^2 - X - 1) + (5X - 7)\big((X^5 - 1) - (X^2 - X - 1)(X^3 + X^2 + 2X + 3)\big) \\ &= (-5X^4 + 2X^3 - 3X^2 - X - 4)(X^2 - X - 1) + (5X - 7)(X^5 - 1) \\ &= (-5X^4 + 2X^3 - 3X^2 - X - 4)(X^7 - X - 1) + (5X^6 - 2X^5 + 3X^4 + X^3 + 4X^2 + 5X - 7)(X^5 - 1). \end{aligned}$$

Il suffit de diviser par 11 pour obtenir les polynômes U et V.

Exercice 29.

Soient P et Q des polynômes de $\mathbb{C}[X]$ non constants. Montrer que P et Q ont un facteur commun si, et seulement si, il existe $A, B \in \mathbb{C}[X]$, $A \neq 0$, $B \neq 0$, tels que $AP = BQ$ et $\deg(A) < \deg(Q)$, $\deg(B) < \deg(P)$.

Correction.

Supposons que P et Q ont un facteur commun D. On factorise $P = DB$ et $Q = DA$, A et B vérifient les conditions voulues. Réciproquement, si $P \wedge Q = 1$ et $AP = BQ$, alors $P|BQ$ et par le théorème de Gauss $P|B$. Ceci contredit les contraintes imposées à B.

Exercice 30.

Décomposer le polynôme suivant en produit d'irréductibles de $\mathbb{R}[X]$:

$$P(X) = 2X^4 + X^2 - 3.$$

Correction.

Le polynôme est un polynôme "bicarré" : il s'écrit $P(X) = Q(X^2)$ où $Q(X) = 2X^2 + X - 3$. On

commence par factoriser ce polynôme. Ses racines sont 1 et $-3/2$. Donc Q se factorise en

$$Q(X) = 2(X-1)\left(X + \frac{3}{2}\right).$$

On en déduit que

$$P(X) = 2(X^2-1)\left(X^2 + \frac{3}{2}\right) = 2(X-1)(X+1)\left(X^2 + \frac{3}{2}\right).$$

Comme $X^2 + \frac{3}{2}$ est un polynôme de degré 2 sans racines réelles, on a bien obtenu la décomposition de P en produit d'irréductibles.

Exercice 31.

Soit P le polynôme $X^4 - 6X^3 + 9X^2 + 9$.

1. Décomposer $X^4 - 6X^3 + 9X^2$ en produit de facteurs irréductibles dans $\mathbb{R}[X]$.
2. En déduire une décomposition de P en produit de facteurs irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.

Correction.

1. On écrit simplement

$$X^4 - 6X^3 + 9X^2 = X^2(X^2 - 6X + 9) = X^2(X-3)^2.$$

2. L'astuce(?) est d'écrire $9 = -(3i)^2$, et de reconnaitre une différence de deux carrés. Donc on a :

$$\begin{aligned} X^4 - 6X^3 + 9X^2 + 9 &= \big(X(X-3)\big)^2 - (3i)^2 \\ &= \big(X(X-3) - 3i\big)\big(X(X-3) + 3i\big) \\ &= (X^2 - 3X - 3i)(X^2 - 3X + 3i). \end{aligned}$$

On factorise chacun de ces deux polynômes. Le discriminant du premier est $9 + 12i = (\sqrt{3}(2+i))^2$. Ses racines sont $\alpha_1 = \frac{3}{2} + \sqrt{3} + \frac{i\sqrt{3}}{2}$ et $\alpha_2 = \frac{3}{2} - \sqrt{3} - \frac{i\sqrt{3}}{2}$. Le discriminant du second est $9 - 12i = (\sqrt{3}(2-i))^2$, et ses racines sont $\beta_1 = \frac{3}{2} + \sqrt{3} - \frac{i\sqrt{3}}{2}$ et $\beta_2 = \frac{3}{2} - \sqrt{3} + \frac{i\sqrt{3}}{2}$. La décomposition de P en produit d'irréductibles de $\mathbb{C}[X]$ est donc

$$(X-\alpha_1)(X-\alpha_2)(X-\beta_1)(X-\beta_2).$$

Pour obtenir la décomposition en produit d'irréductibles de $\mathbb{R}[X]$, on regroupe les racines complexes conjuguées, à savoir α_1 et β_1 d'une part et α_2 et β_2 d'autre part. On trouve

$$P = \big(X^2 - (2\sqrt{3}+3)X + 3\sqrt{3} + 6\big)\big(X^2 + (2\sqrt{3}-3)X - 3\sqrt{3} + 6\big).$$

b. Exercices d'entraînement

Exercice 32.

Quel est le reste de la division euclidienne de $(X+1)^n - X^n - 1$ par

1. $X^2 - 3X + 2$ **2**. $X^2 + X + 1$ **3**. $X^2 - 2X + 1$?

Correction.

1. La méthode pour ce type d'exercice est toujours la même. On commence par écrire *a priori* le résultat de la division euclidienne, par exemple pour le premier polynôme :

$$(X+1)^n - X^n - 1 = Q(X)(X^2 - 3X + 2) + aX + b,$$

où a et b sont deux réels. On évalue ensuite la relation en les racines du diviseur, qui sont ici 1 et 2. On trouve alors

$$\begin{cases} 2^n - 2 &= a + b \\ 3^n - 2^n - 1 &= 2a + b. \end{cases}$$

Et finalement on résoud le système pour trouver a et b, qui sont ici égaux à :

$$\begin{cases} a &= 3^n - 2^{n+1} + 1 \\ b &= -3^n + 2^{n+1} + 2^n - 3. \end{cases}$$

2. On écrit la même chose,

$$(X+1)^n - X^n - 1 = Q(X)(X^2 + X + 1) + aX + b,$$

et on utilise cette fois que les racines de $X^2 + X + 1$ sont j et j^2. Il suffit ici en réalité d'utiliser l'évaluation en j, sachant que tout nombre complexe s'écrit de façon unique sous la forme $x + jy$, avec $x, y \in \mathbb{R}$. On trouve :

$$(1+j)^n - j^n - 1 = Q(j) \times 0 + aj + b.$$

On distingue ensuite suivant la valeur de n modulo 3, utilisant que

$$(1+j)^n - j^n - 1 = (-1)^n j^{2n} - j^n - 1.$$

— Si $n \equiv 0\ [3]$, alors $j^{2n} = j^n = 1$, et donc on a

$$(-1)^n - 2 = aj + b$$

de sorte que le reste est $(-1)^n - 2$.

— Si $n \equiv 1\ [3]$, alors $j^n = j$ et donc $j^{2n} = j^2 = -1 - j$, $j^n = j$, ce qui donne

$$\big((-1)^{n+1} - 1\big)j + \big((-1)^{n+1} - 1\big) = aj + b.$$

Le reste est donc $\big((-1)^{n+1} - 1\big)(X+1)$.

— Si $n \equiv 2\ [3]$, alors $j^{2n} = j$ et $j^n = j^2 = -1 - j$. On trouve

$$\big((-1)^n + 1\big)j = aj + b.$$

Le reste est alors $\big((-1)^n + 1\big)X$.

3. On recommence en écrivant

$$(X+1)^n - X^n - 1 = Q(X)(X^2 - 2X + 1) + aX + b,$$

et en remarquant que $X^2 - 2X + 1$ a pour racine double 1. Si on évalue en 1, on obtient une seule relation, à savoir

$$2^n - 2 = a + b.$$

Pour obtenir une seconde relation, il faut dériver la relation issue de la division euclidienne et l'évaluer à nouveau en 1 (c'est toujours cette méthode qui fonctionne pour une racine double). On trouve :

$$n(X+1)^{n-1} - nX^{n-1} = Q'(X)(X^2 - 2X + 1) + 2Q(X)(X-1) + a,$$

ce qui donne la relation

$$n2^{n-1} - n = a.$$

On retrouve alors sans problèmes b, qui est égal à :

$$b = (2-n)2^{n-1} + n - 2.$$

Exercice 33.

Démontrer que

1. $X^{n+1}\cos\big((n-1)\theta\big) - X^n\cos(n\theta) - X\cos\theta + 1$ est divisible par $X^2 - 2X\cos\theta + 1$;
2. $nX^{n+1} - (n+1)X^n + 1$ est divisible par $(X-1)^2$.

Correction.

1. Pour prouver que $X^2 - 2X\cos\theta + 1$ divise $X^{n+1}\cos\big((n-1)\theta\big) - X^n\cos(n\theta) - X\cos\theta + 1$, il suffit de prouver que ce dernier polynôme s'annule en les deux racines (complexes) de $X^2 - 2X\cos\theta + 1$, à savoir $e^{i\theta}$ et $e^{-i\theta}$. Il suffit de prouver le résultat pour $e^{i\theta}$ car, le polynôme étant réel, si z est racine, son conjugué $\bar{z}$ est racine. On trouve

$$\begin{gathered} e^{i(n+1)\theta}\cos\big((n-1)\theta\big) - e^{in\theta}\cos(n\theta) - e^{i\theta}\cos\theta + 1 = \\ \Big(\cos\big((n+1)\theta\big)\cos\big((n-1)\theta\big) - \cos^2(n\theta) - \cos^2\theta + 1\Big) + \\ i\Big(\sin\big((n+1)\theta\big)\cos\big((n-1)\theta\big) - \sin(n\theta)\cos(n\theta) - \sin\theta\cos\theta\Big). \end{gathered}$$

Le reste n'est plus qu'une affaire de formules de trigonométrie :

$$\begin{aligned}
\cos\big((n+1)\theta\big)\cos\big((n-1)\theta\big) &= \frac{1}{2}\Big(\cos(2n\theta)+\cos(2\theta)\Big)\\
\cos^2(n\theta) &= \frac{1}{2}\Big(\cos(2n\theta)+1\Big)\\
\cos^2\theta &= \frac{1}{2}\Big(\cos(2\theta)+1\Big)\\
\sin\big((n+1)\theta\big)\cos\big((n-1)\theta\big) &= \frac{1}{2}\Big(\sin(2n\theta)+\sin(2\theta)\Big)\\
\sin(n\theta)\cos(n\theta) &= \frac{1}{2}\sin(2n\theta)\\
\sin\theta\cos\theta &= \frac{1}{2}\sin(2\theta).
\end{aligned}$$

En faisant les bonnes sommes et différences des relations précédentes, on trouve bien que

$$e^{i(n+1)\theta}\cos\big((n-1)\theta\big) - e^{in\theta}\cos(n\theta) - e^{i\theta}\cos\theta + 1 = 0.$$

2. C'est fois, on a affaire à une racine d'ordre 2, et il suffit de prouver que 1 est racine de $P(X) = nX^{n+1} - (n+1)X^n + 1$ et de $P'(X) = n(n+1)X^n - n(n+1)X^{n-1}$, ce qui est évident... Pour justifier cela, on peut faire appel à la partie du cours consacrée aux racines, ou partir de la division euclidienne

$$nX^{n+1} - (n+1)X^n + 1 = Q(X)(X-1)^2 + aX + b.$$

Faire $X = 1$ dans la relation précédente donne $a + b = 0$. De plus, si on dérive la relation précédente et qu'on fait à nouveau $X = 1$, on obtient $a = 0$.

Exercice 34.

Soient $A, B, P \in \mathbb{K}[X]$ avec P non-constant. On suppose que $A \circ P | B \circ P$. Démontrer que $A|B$.

Correction.

On écrit la division euclidienne de B par A, $B = AQ + R$ avec $\deg(R) < \deg(A)$. On compose alors par P, et on obtient $B \circ P = (A \circ P) \times (Q \circ P) + R \circ P$. Or, le polynôme $A \circ P$ a pour degré $\deg(A) \times \deg(P)$. Le polynôme $R \circ P$ a pour degré $\deg(R) \times \deg(P)$. On en déduit que $\deg(R \circ P) < \deg(A \circ P)$ et donc que $B \circ P = (A \circ P) \times (Q \circ P) + R \circ P$ est la division euclidienne de $B \circ P$ par $A \circ P$. Mais on sait que $A \circ P | B \circ P$ et donc on en déduit que $R \circ P$ est égal à 0. Ceci n'est possible que si $R = 0$, et donc $A|B$.

Exercice 35.

Le but de cet exercice est de déterminer

$$E = \{P \in \mathbb{R}[X];\ P(X^2) = (X^3+1)P(X)\}.$$

1. Démontrer que le polynôme nul ainsi que le polynôme $X^3 - 1$ sont solutions du problème.

2. Analyse du problème. Soit $P \in E$ non nul.
   (a) Montrer que P est de degré 3.
   (b) Démontrer que $P(1) = 0$, puis que $P'(0) = P''(0) = 0$ (on pourra penser à dériver la relation $P(X^2) = (X^3 + 1)P(X)$).
   (c) En effectuant la division euclidienne de P par $X^3 - 1$, démontrer qu'il existe $\lambda \in \mathbb{R}$ tel que $P(X) = \lambda(X^3 - 1)$.
3. Synthèse du problème : en déduire l'ensemble E.

Correction.

1. Il est clair que $0 = (X^3 + 1)0$ et donc le polynôme nul est solution. Pour $P(X) = X^3 - 1$, on a $P(X^2) = X^6 - 1$ et $(X^3 + 1)P(X) = (X^3 + 1)(X^3 - 1) = X^6 - 1$. Ce polynôme est aussi solution.
2. (a) Notons n le degré de P. Alors $P(X^2)$ est de degré $2n$ et $(X^3 + 1)P(X)$ est de degré $n + 3$. Le degré n vérifie donc l'équation $2n = n + 3$, soit $n = 3$.
   (b) En évaluant la relation en $X = 1$, on a $P(1^2) = P(1) = 0$. Dérivons maintenant l'équation $P(X^2) = (X^3 + 1)P(X)$. On trouve
   $$2XP'(X^2) = 3X^2P(X) + (X^3 + 1)P'(X).$$
   Si on évalue en $X = 0$, on trouve $P'(0) = 0$. Dérivons une second fois cette équation. On trouve
   $$2P'(X^2) + 4X^2P''(X^2) = 6XP(X) + 6X^2P'(X) + (X^3 + 1)P''(X).$$
   On évalue cette équation en $X = 0$ et on trouve, tenant compte du fait que l'on sait déjà que $P'(0) = 0$, $P''(0) = 0$.
   (c) Effectuons la division euclidienne de P par $X^3 - 1$. On peut écrire
   $$P(X) = Q(X)(X^3 - 1) + R(X)$$
   où $\deg(R) \leq 2$ et donc $R(X)$ s'écrit $R(X) = aX^2 + bX + c$. De plus, en considérant le degré, Q ne peut être qu'un polynôme constant, et donc $Q(X) = \lambda$ avec $\lambda \in \mathbb{R}$. Il reste à montrer que $a = b = c = 0$. Puisque $P(1) = 0$, on a $a + b + c = 0$. De plus, dérivons $P(X) = \lambda(X^3 - 1) + (aX^2 + bX + c)$. On obtient
   $$P'(X) = 3\lambda X^2 + (2aX + b).$$
   Puisque $P'(0) = 0$, on a $b = 0$. On dérive une seconde fois la relation, on obtient
   $$P''(X) = 6\lambda X + 2a$$
   et puisque $P''(0) = 0$, on a $a = 0$ et finalement également $c = 0$.
3. La question précédente nous dit que si $P \in E$, alors ou bien P est nul ou bien $P(X) = \lambda(X^3 - 1)$ pour un certain $\lambda \in \mathbb{R}^*$. Réciproquement, d'après la première question, le polynôme nul et les polynômes $\lambda(X^3 - 1)$, $\lambda \in \mathbb{R}^*$ sont éléments de E. Finalement, on peut conclure que $E = \{\lambda(X^3 - 1);\ \lambda \in \mathbb{R}\}$.

Exercice 36.

Déterminer tous les polynômes $P \in \mathbb{R}[X]$ vérifiant $P(0) = 0$ et $P(X^2+1) = \big(P(X)\big)^2 + 1$

Correction.

Pour tout $x \in \mathbb{R}$, on a $P(x^2+1) = \big(P(x)\big)^2 + 1$. Pour $x = 0$, on trouve $P(1) = 1$. Pour $x = 1$, on trouve $P(2) = 2$. Pour $x = 2$, on trouve $P(5) = 5$. Pour $x = 5$, on trouve $P(5^2+1) = 5^2+1$. Ceci nous incite à considérer la suite définie par $u_{n+1} = u_n^2 + 1$ et $u_0 = 0$. Il est aisé de prouver que cette suite est strictement croissante. De plus, on prouve par récurrence sur n que $P(u_n) = u_n$. En effet, la propriété est vraie pour $n = 0, 1, 2, 3$. Si elle est vraie au rang n, alors on a

$$P(u_{n+1}) = P(u_n^2+1) = \big(P(u_n)\big)^2 + 1 = u_n^2 + 1 = u_{n+1}$$

ce qui prouve l'hérédité. Posons alors $Q(X) = P(X) - X$. Q est un polynôme qui s'annule en chaque u_n. Comme les u_n sont tous différents, Q admet une infinité de racines. Donc Q est identiquement nulle et on a $P(X) = X$. Réciproquement, X convient.

Exercice 37.

1. Rappeler la décomposition en produits d'irréductibles de $X^n - 1$.
2. En déduire la décomposition en produits d'irréductibles de $1 + X + \cdots + X^{n-1}$.
3. Calculer $\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right)$.
4. Pour $\theta \in \mathbb{R}$, calculer $\prod_{k=0}^{n-1} \sin\left(\frac{k\pi}{n} + \theta\right)$.

Correction.

1. Les racines de ce polynôme sont les racines n-ièmes de l'unité. On en déduit que
$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right).$$
2. On a $(1 + X + \cdots + X^{n-1})(X-1) = X^n - 1$. On en déduit que
$$1 + X + \cdots + X^{n-1} = \prod_{k=1}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right).$$
3. On va évaluer la factorisation précédente en 1. On trouve
$$n = \prod_{k=1}^{n-1} \left(1 - e^{\frac{2ik\pi}{n}}\right).$$
Or,
$$1 - e^{\frac{2ik\pi}{n}} = -2ie^{\frac{ik\pi}{n}} \sin\left(\frac{k\pi}{n}\right) = 2(-1)e^{\frac{i\pi}{2}} e^{\frac{ik\pi}{n}} \sin\left(\frac{k\pi}{n}\right).$$

On effectue le produit et on trouve :

$$\begin{aligned}\prod_{k=1}^{n-1}\left(1-e^{\frac{2ik\pi}{n}}\right) &= 2^{n-1}(-1)^{n-1}e^{\frac{i(n-1)\pi}{2}}e^{\frac{i\pi}{n}\times\frac{n(n-1)}{2}}\prod_{k=1}^{n-1}\sin\left(\frac{k\pi}{n}\right)\\ &= 2^{n-1}\prod_{k=1}^{n-1}\sin\left(\frac{k\pi}{n}\right)\end{aligned}$$

On en déduit que

$$\prod_{k=1}^{n-1}\sin\left(\frac{k\pi}{n}\right)=\frac{n}{2^{n-1}}.$$

4. La méthode est parfaitement similaire, mais cette fois on part de la factorisation de X^n-1 que l'on évalue en $\exp(-2i\theta)$. On trouve d'une part

$$e^{-2ni\theta}-1=(-2i)e^{-in\theta}\sin(n\theta)$$

et d'autre part

$$\begin{aligned}\prod_{k=0}^{n-1}\left(e^{-2i\theta}-e^{\frac{2ik\pi}{n}}\right) &= \prod_{k=0}^{n-1}(-2i)e^{\frac{ik\pi}{n}-\theta}\sin\left(\frac{k\pi}{n}+\theta\right)\\ &= (-2i)2^{n-1}\prod_{k=0}^{n-1}\sin\left(\frac{k\pi}{n}+\theta\right).\end{aligned}$$

On conclut finalement que

$$\prod_{k=0}^{n-1}\sin\left(\frac{k\pi}{n}+\theta\right)=\frac{\sin(n\theta)}{2^{n-1}}.$$

Exercice 38.

On dit qu'un polynôme $P\in\mathbb{C}[X]$ de degré n est réciproque s'il s'écrit $P=a_nX^n+\cdots+a_0$ avec $a_k=a_{n-k}$ pour tout k dans $\{0,\dots,n\}$.

1. Soit $P\in\mathbb{C}[X]$ de degré n. Démontrer que P est réciproque si et seulement si $P(X)=X^nP\left(\frac{1}{X}\right)$.
2. Montrer qu'un produit de polynômes réciproques est réciproque.
3. On suppose que P et Q sont réciproques et que $Q|P$. Démontrer que $\frac{P}{Q}$ est réciproque.
4. Soit $P\in\mathbb{C}[X]$ un polynôme réciproque.
   (a) Démontrer que si α est une racine de P, alors $\alpha\neq 0$ et α^{-1} est une racine de P.
   (b) Démontrer que si 1 est une racine de P, alors sa multiplicité est supérieure ou égale à 2.
   (c) Démontrer que si le degré de P est impair, alors -1 est racine de P.
   (d) Démontrer que si P est de degré pair et si -1 est une racine de P, alors sa multiplicité est supérieure ou égale à 2.

5. Démontrer que tout polynôme réciproque de $\mathbb{C}[X]$ de degré $2n$ se factorise en

$$P = a_{2n}(X^2 + b_1X + 1)\dots(X^2 + b_nX + 1).$$

Que peut-on dire si le degré de P est impair ?

Correction.

1. Soit $P = a_nX^n + \dots + a_0$, alors

$$X^nP\left(\frac{1}{X}\right) = a_0X^n + \dots + a_n.$$

Ainsi, si P est réciproque, on a bien $X^nP(1/X) = P(X)$. Réciproquement, si $X^nP(1/X) = P(X)$, alors on a nécessairement $a_0 = a_n$, $a_1 = a_{n-1}$, etc... Donc P est réciproque.

2. Soient P et Q réciproques, de degrés respectifs n et m. Alors

$$X^nP(1/X) = P(X) \text{ et } X^mQ(1/X) = Q(X).$$

On en déduit que

$$X^{n+m}(PQ)(1/X) = X^nP(1/X)X^mQ(1/X) = P(X)Q(X) = (PQ)(X).$$

Ainsi, d'après la question précédente, PQ est réciproque.

3. Le raisonnement est complètement identique, en utilisant le quotient au lieu du produit !

4. (a) Puisque P est réciproque, $a_0 = a_n \neq 0$ et donc $P(0) = a_0 \neq 0$. D'autre part, si α est racine de P, alors la relation $P(\alpha) = \alpha^nP(\alpha^{-1})$ prouve que α^{-1} est aussi racine de P.

   (b) Dérivons la relation de la première question. On trouve, pour tout $x \neq 0$,

$$P'(x) = nx^{n-1}P(1/x) - x^{n-2}P'(1/x).$$

   On évalue en 1, et on trouve

$$P'(1) = -P'(1)$$

   et donc $P'(1) = 0$. On en déduit que 1 est racine au moins double.

   (c) On utilise encore le résultat de la première question, et on remarque que $P(-1) = -P(-1)$ puisque le degré de P est impair. Donc $P(-1) = 0$.

   (d) On raisonne exactement comme deux questions plus haut.

5. On va procéder par récurrence sur n, le cas $n = 1$ étant trivial. Supposons donc que le résultat a été démontré pour tout polynôme réciproque de degré $2n$, et prouvons-le pour un polynôme réciproque P de degré $2n + 2$. Soit α une racine de P. Alors, on sait que $\alpha \neq 0$ et que α^{-1} est aussi racine de P. Si $\alpha \neq 1, -1$, $\alpha^{-1} \neq \alpha$ et on peut factoriser P par $(X-\alpha)(X-\alpha^{-1})$. Or, il est facile de vérifier que $(X-\alpha)(X-\alpha^{-1})$ s'écrit $(X^2+b_{n+1}X+1)$. D'autre part, si $\alpha = 1$ ou $\alpha = -1$, alors α est racine de multiplicité au moins deux, et on peut factoriser par $(X-\alpha)^2$. Un tel polynôme s'écrit encore $(X^2 + b_{n+1}X + 1)$. Donc, dans tous les cas, en notant $Q = X^2 + b_{n+1}X + 1$, on a $Q|P$ et P, Q réciproques. On en déduit que $\frac{P}{Q}$ est réciproque, de degré $2n$, donc par l'hypothèse de récurrence s'écrit

$$\frac{P}{Q} = a_{2n+2}(X^2 + b_1X + 1)\dots(X^2 + b_nX + 1).$$

On remultiplie par Q, et on a bien prouvé que le résultat est vrai au rang $n+1$. Si maintenant P est réciproque de degré impair $2n+1$, alors -1 est racine de P et P se factorise par le polynôme réciproque $Q = X+1$. Donc $\frac{P}{Q}$ est réciproque de degré pair $2n$, donc s'écrit $a_{2n+1}(X^2+b_1X+1)\dots(X^2+b_nX+1)$. Ainsi, tout polynôme réciproque de degré impair $2n+1$ se factorise en

$$P = a_{2n+1}(X+1)(X^2+b_1X+1)\dots(X^2+b_nX+1).$$

c. Exercices d'approfondissement

Exercice 39.

Déterminer les polynômes P de degré supérieur ou égal à 1 et tels que $P'|P$.

Correction.

Puisque $P'|P$, $P = QP'$, et les considérations de degré font que Q est de degré 1. On peut donc écrire :

$$P = \lambda(X-\alpha)P'.$$

On applique ensuite la formule de Taylor à P en α :

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k,$$

$$P'(X) = \sum_{k=1}^{n} \frac{kP^{(k)}(\alpha)}{k!}(X-\alpha)^{k-1},$$

$$\lambda(X-\alpha)P'(X) = \sum_{k=1}^{n} \frac{\lambda kP^{(k)}(\alpha)}{k!}(X-\alpha)^k.$$

Par identification, on obtient, pour tout k dans $\{0,\dots,n\}$:

$$\frac{P^{(k)}(\alpha)}{k!}(\lambda k-1) = 0.$$

Maintenant, $P^{(n)}(\alpha) \neq 0$, et donc $\lambda = 1/n$. Ceci entraîne par suite que, pour tout k dans $\{0,\dots,n-1\}$, on a :

$$P^{(k)}(\alpha) = 0.$$

Ainsi,

$$P(X) = \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n,$$

ce qui prouve que $P(X) = K(X-\alpha)^n$, où K est une constante. La réciproque se vérifie aisément.

Exercice 40.

Déterminer les couples (A, B) de polynômes non nuls de $\mathbb{R}[X]$ tels que le quotient et le reste dans la division euclidienne de A par B et dans la division euclidienne de B par A soient identiques.

Correction.

Procédons par analyse-synthèse. Supposons donc que la propriété est vraie. Il existe alors un polynôme Q et un polynôme R avec $\deg(R) < \min(\deg(A), \deg(B))$ tel que $A = BQ + R$ et $B = AQ + R$. Mais alors, on a aussi

$$\begin{aligned} A = (AQ+R)Q + R = AQ^2 + RQ + R &\iff A(1-Q^2) - R(1+Q) = 0 \\ &\iff A(Q+1)(1-Q) - R(1+Q) = 0 \\ &\iff (Q+1)\big(A(1-Q) - R\big) = 0. \end{aligned}$$

Si le produit de deux polynômes est nul, c'est que l'un de ces deux polynômes est nul. Ainsi, on a ou bien $1 + Q = 0$ ou bien $A(1 - Q) - R = 0$. On distingue donc deux cas

— Si $Q = -1$, alors $A = -B + R$ et $B = -A + R$. Autrement dit, il existe deux polynômes $P, R \in \mathbb{R}[X]$ avec $\deg(R) < \deg(P)$ tels que $A = P + R$ et $B = -P + R$.

— Si $Q \neq -1$, alors $A(1 - Q) - R = 0$. Pour des considérations de degré (rappelons que $\deg(R) < \deg(A)$), ceci n'est possible que si $Q = 1$ et $R = 0$. On obtient alors le cas trivial $A = B$.

Passons à la synthèse. Supposons que $A = B$ ou qu'il existe un couple de polynômes (P, R) de $\mathbb{R}[X]$ avec $\deg(R) < \deg(P)$ tels que $A = P + R$ et $B = -P + R$. Alors les divisions euclidiennes de A par B et de B par A ont bien même quotient et même reste. On a donc démontré que l'ensemble des couples solutions est

$$\mathcal{S} = \{(P, P);\ P \in \mathbb{R}[X]\} \cup \{(P + R, -P + R);\ P, R \in \mathbb{R}[X],\ \deg(R) < \deg(P)\}.$$

Exercice 41.

Soient n, p deux entiers naturels non nuls et soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbb{C}[X]$. Pour chaque $k \in \{0, \dots, n\}$, on note r_k le reste de la division euclidienne de k par p. Démontrer que le reste de la division euclidienne de P par $X^p - 1$ est le polynôme $R(X) = \sum_{k=0}^{n} a_k X^{r_k}$.

Correction.

On va démontrer que $X^p - 1$ divise $P - R$. En effet, le degré de R est inférieur strict à p, et R sera bien le reste dans la division euclidienne de P par $X^p - 1$. On écrit alors que

$$P - R = \sum_{k=0}^{n} a_k (X^k - X^{r_k}),$$

et il suffit de prouver que $X^p - 1$ divise chaque $X^k - X^{r_k}$. Écrivons alors $k = mp + r_k$, d'où l'on tire

$$X^k - X^{r_k} = X^{r_k}(X^{mp} - 1) = X^{r_k}(X^p - 1)(1 + X^p + \cdots + X^{(m-1)p}).$$

$X^p - 1$ divise bien $P - R$!

Exercice 42.

1. Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{C}) \subset \mathbb{R}$.
2. Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{R}) \subset \mathbb{R}$.
3. Soit $P \in \mathbb{C}[X]$. Démontrer que $P(\mathbb{Q}) \subset \mathbb{Q}$ si et seulement si $P \in \mathbb{Q}[X]$.

Correction.

1. Il est clair que si $P(X) = a$, avec $a \in \mathbb{R}$, alors P est solution. Si P n'est pas constant, alors le polynôme $Q(X) = P(X) - i$ n'est pas constant lui aussi. D'après le théorème de d'Alembert-Gauss, il s'annule. En particulier, il existe $z \in \mathbb{C}$ tel que $P(z) = i$, et donc on n'a pas $P(\mathbb{C}) \subset \mathbb{R}$. Ainsi, les polynômes solutions sont les polynômes constants, avec une constante réelle.
2. Les polynômes à coefficients réels sont bien entendu solutions. De plus, si $x \in \mathbb{R}$, alors puisque $P(x) \in \mathbb{R}$, on a
$$P(x) = \overline{P(x)} = \overline{P}(x).$$
Ainsi, le polynôme $P - \overline{P}$ admet une infinité de racine. Ce ne peut être que le polynôme nul. Mais les coefficients de $P - \overline{P}$ sont ($2i$-fois) les parties imaginaires des coefficients de P. Ainsi, tous les coefficients de P ont une partie imaginaire nulle. C'est bien que P est un élément de $\mathbb{R}[X]$.
3. Il est clair que si $P \in \mathbb{Q}[X]$, alors $P(\mathbb{Q}) \subset \mathbb{Q}$. Réciproquement soit $P \in \mathbb{C}[X]$ tel que $P(\mathbb{Q}) \subset \mathbb{Q}$. Soit d le degré de P et soit $(L_0, \dots, L_d)$ la famille des polynômes de Lagrange associée aux entiers $(0, \dots, d)$. Alors la formule donnant ces polynômes nous dit qu'ils sont à coefficients dans $\mathbb{Q}$. De plus, on a
$$P(X) = \sum_{k=0}^{d} P(k) L_k(X).$$
P est bien à coefficients dans $\mathbb{Q}$.

Exercice 43.

On note
$$\mathcal{S} = \{P \in \mathbb{R}[X];\ \exists P_1, P_2 \in \mathbb{R}[X];\ P = P_1^2 + P_2^2\}.$$

1. Montrer que $\mathcal{S}$ est stable par produit. On pourra considérer l'application $\phi : \mathbb{C}[X] \to \mathbb{R}[X]$, $P \mapsto P\bar{P}$.
2. Soit $P \in \mathbb{R}[X]$ tel que $P(x) \geq 0$ pour tout $x \in \mathbb{R}$. Montrer qu'il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + B^2$.

Correction.

1. Cela suit directement de l'identité suivante, très simple à vérifier (mais moins à trouver !) :
$$(P_1^2 + P_2^2)(Q_1^2 + Q_2^2) = (P_1Q_2 + P_2Q_2)^2 + (P_1Q_1 - P_2Q_1)^2.$$
On peut la retrouver grâce à l'indication. En effet, si $P = P_1 + iP_2$ et $Q = Q_1 + iQ_2$, alors
$$\phi(P)\phi(Q) = \phi(PQ)$$

et les deux membres de l'égalité correspondent à l'égalité écrite ci-dessus.

2. Décomposons P en produits de facteurs irréductibles :

$$P(X) = \lambda \prod_{i=1}^{m} (X - a_i)^{m_i} \prod_{j=1}^{p} (X^2 + \alpha_j X + \beta_j)$$

où chaque polynôme $X^2 + \alpha_j X + \beta_j$ est de discriminant négatif. Puis P est toujours positif, il est clair que $\lambda \geq 0$ et que chaque m_i est pair (sinon P changerait de signe au voisinage de a_i et donc ne pourrait pas être positif partout). D'après la question précédente, il suffit de vérifier que chaque terme intervenant dans la décomposition précédente est une somme de deux carrés. Écrivant $\lambda = \mu^2$, on obtient $\lambda = \mu^2 + 0^2$. D'autre part, posons $m_i = 2n_i$ et $A_i = (X - a_i)^{n_i}$. Alors $(X - a_i)^{m_i} = A_i^2 + 0^2$. Reste à traiter les polynômes du type $X^2 - \alpha X + \beta$, de discriminant négatif. L'idée est d'utiliser la forme canonique de ces polynômes. En effet, on a

$$X^2 + \alpha X + \beta = \left(X + \frac{\alpha}{2}\right)^2 + \frac{4\beta - \alpha^2}{4}.$$

Puisque le discriminant est négatif, on peut poser

$$\gamma = \sqrt{\frac{4\beta - \alpha^2}{4}}$$

et on a alors

$$X^2 + \alpha X + \beta = \left(X + \frac{\alpha}{2}\right)^2 + \gamma^2.$$

Ce terme est aussi somme de deux carrés.

Exercice 44.

Si $P \in \mathbb{Z}[X]$, on appelle contenu de P, et on note $c(P)$, le pgcd des coefficients de P.

1. Soit $P, Q \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que p divise tous les coefficients de PQ. Montrer que p divise tous les coefficients de P ou tous les coefficients de Q.
2. Soit $P, Q \in \mathbb{Z}[X]$ et $R(X) = \frac{PQ}{c(P)c(Q)} \in \mathbb{Z}[X]$. Démontrer que $c(R) = 1$. En déduire que l'on a $c(PQ) = c(P)c(Q)$.
3. Soit Q un polynôme de $\mathbb{Z}[X]$. On suppose que Q n'est pas irréductible dans $\mathbb{Q}[X]$. Démontrer qu'il existe deux polynômes A et B de $\mathbb{Z}[X]$ tels que $Q = AB$, avec $\deg(A) < \deg(Q)$ et $\deg(B) < \deg(Q)$.
4. Soit $A(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que
$$p | a_k, \text{ pour tout } 0 \leq k \leq n-1, \ p \not| a_n, \ p^2 \not| a_0.$$
Démontrer que A est irréductible dans $\mathbb{Q}[X]$.
5. Démontrer qu'il existe dans $\mathbb{Q}[X]$ des polynômes irréductibles de tout degré $n \geq 1$.

Correction.

1. Il est possible de faire une preuve directe par l'absurde. Le plus simple, néanmoins est de raisonner dans $\mathbb{Z}/p\mathbb{Z}[X]$. Pour $R \in \mathbb{Z}[X]$, notons en effet $\bar{R}$ son projeté dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Alors, on a $\overline{PQ} = \bar{P}\bar{Q}$. De plus, puisque p divise tous les coefficients de PQ, on a $\overline{PQ} = 0$. Puisque $\mathbb{Z}/p\mathbb{Z}$ est intègre, ceci implique que $\bar{P} = 0$ ou $\bar{Q} = 0$. La première éventualité signifie que p divise tous les coefficients de P, la seconde que p divise tous les coefficients de Q.

2. Si $c(R) \neq 1$, il existe un nombre premier p qui divise tous les coefficients de R. Notons $P_1 = P/c(P)$ et $Q_1 = Q/c(Q)$. Alors $R = P_1Q_1$ et donc d'après la première question, p divise tous les coefficients de P_1 ou tous les coefficients de Q_1. Ceci contredit la définition du contenu. Puisque $1 = c(R) = \frac{c(PQ)}{c(P)c(Q)}$, on obtient bien que $c(PQ) = c(P)c(Q)$.

3. Remarquons d'abord qu'on peut se ramener à $c(Q) = 1$ (quitte ensuite à multiplier par $c(Q)$). Factorisons $Q = CD$ dans $\mathbb{Q}[X]$. Soit α et β de sorte que $C_1 = \alpha C$ et $D_1 = \beta D$ soit éléments de $\mathbb{Z}[X]$. Alors $\alpha\beta Q = C_1D_1$. Utilisant le résultat de la question précédente, on a donc $\alpha\beta = c(C_1)c(D_1)$. Mais alors

$$Q = \frac{C_1D_1}{\alpha\beta} = \frac{C_1D_1}{c(C_1)c(D_1)} = \frac{C_1}{c(C_1)} \times \frac{D_1}{c(D_1)}.$$

   On a le résultat voulu en posant $A = \frac{C_1}{c(C_1)}$ et $B = \frac{D_1}{c(D_1)}$.

4. Supposons que A n'est pas irréductible dans $\mathbb{Q}[X]$. Alors d'après la question précédente, A s'écrit BC, avec $1 < \deg(B) < \deg(A) = n$. Projetons l'égalité $A = BC$ dans $\mathbb{Z}/p\mathbb{Z}$. Il vient

$$\overline{a_n}X^n = \overline{B} \times \overline{C}.$$

   De plus, puisque $\deg(B) + \deg(C) = \deg(A)$, que $\deg(\bar{B}) \leq \deg(B)$, $\deg(\bar{C}) \leq \deg(C)$ et $\overline{a_n} \neq \bar{0}$, $\deg(\bar{B}) = \deg(B)$ et $\deg(\bar{C}) = \deg(C)$. Par unicité de la réduction en produits d'irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a $\bar{B} = \overline{b_k}X^k$ et $\bar{C} = \overline{c_l}X^l$. En particulier, $\overline{b_0} = \overline{c_0} = 0$, c'est-à-dire $p|b_0$ et $p|c_0$. Puisque $a_0 = b_0c_0$, on a $p^2|a_0$, une contradiction.

5. Les polynômes de degré 1 sont irréductibles. Pour les polynômes de degré $n \geq 2$, il suffit de considérer par exemple $X^n - 2$, auquel on peut très facilement appliquer le critère d'Eisenstein.