Polycopié d'exercices.

MP2I - Lycée Faidherbe

Premier semestre - Algèbre - Chapitres 16 à 21.

Table des matières

Chapitre 16

Relations binaires sur un ensemble

« Ah, alors là, mon ami, si tu as été imprudent, c'est plus grave ! Les affaires tu sais c'est comme le livre de la ménagère : on ne va pas au marché sans savoir où prendre l'argent ! »

Les grandes familles

16.1 $\mathbb{Z}/n\mathbb{Z}$

On se donne dans cette partie un entier $n \geq 2$.

Exercice 1 : ✪ Donner les tables d'addition et de multiplication des ensembles $\mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$.

Exercice 2 : ✪✪ Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. On dit que $\overline{x}$ est inversible s'il existe $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{x} \times \overline{y} = \overline{1}$. Montrer que $\overline{x}$ est inversible si et seulement si $x \wedge n = 1$.

Exercice 3 : ✪✪ Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. On dit que $\overline{x}$ est un diviseur de 0 si $\overline{x} \neq \overline{0}$ et s'il existe $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ non nul tel que $\overline{x} \times \overline{y} = \overline{0}$. Montrer que $\overline{x}$ est un diviseur de 0 si et seulement si $x \not\equiv 0[n]$ et $x \wedge n \neq 1$.

Exercice 4 : ✪✪✪ Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. On dit que $\overline{x}$ est nilpotent s'il existe $k \geq 1$ tel que $\overline{x}^k = \overline{0}$. Donner une CNS sur n pour que $\mathbb{Z}/n\mathbb{Z}$ admette des éléments nilpotents non nuls.

16.2 Relations d'ordre

Exercice 5 : ✪ Soit E un ensemble non vide muni d'une relation R symétrique et transitive. Soit $x \in E$ et soit $y \in E$ tel que xRy. Alors yRx par symétrie donc xRx par transitivité. Ainsi, une relation symétrique et transitive est forcément réflexive, et donc la réflexivité ne sert à rien puisqu'elle est automatique. Où est la faute de raisonnement ?

Exercice 6 : ✪ On se place dans $\mathscr{P}(\mathbb{R})$ muni de l'inclusion. L'ensemble $\left\{ \left[\frac{1}{n} ; n \right] \mid n \in \mathbb{N}^* \right\}$ admet-il un plus grand élément ? une borne supérieure ? un plus petit élément ? une borne inférieure ?

Exercice 7 - Ordre de Charkovskii : ✪✪ On définit sur $\mathbb{N}^*$ la relation d'ordre total $\lhd$ suivante :

$$
\begin{array}{ccccccccccccccc}
 & 3 & \lhd & 5 & \lhd & 7 & \lhd & 9 & \lhd & 11 & \lhd & \cdots & \lhd & 2k+1 & \lhd & \cdots \\
\lhd & 2\times 3 & \lhd & 2\times 5 & \lhd & 2\times 7 & \lhd & 2\times 9 & \lhd & 2\times 11 & \lhd & \cdots & \lhd & 2\times(2k+1) & \lhd & \cdots \\
\lhd & 4\times 3 & \lhd & 4\times 5 & \lhd & 4\times 7 & \lhd & 4\times 9 & \lhd & 4\times 11 & \lhd & \cdots & \lhd & 4\times(2k+1) & \lhd & \cdots \\
\lhd & 8\times 3 & \lhd & 8\times 5 & \lhd & 8\times 7 & \lhd & 8\times 9 & \lhd & 8\times 11 & \lhd & \cdots & \lhd & 8\times(2k+1) & \lhd & \cdots \\
 & & & & & & & \vdots & & & & & & & & \\
\lhd & 2^n\times 3 & \lhd & 2^n\times 5 & \lhd & 2^n\times 7 & \lhd & 2^n\times 9 & \lhd & 2^n\times 11 & \lhd & \cdots & \lhd & 2^n\times(2k+1) & \lhd & \cdots \\
 & & & & & & & \vdots & & & & & & & & \\
 & \cdots & \lhd & 2^p & \lhd & \cdots & \lhd & 16 & \lhd & 8 & \lhd & 4 & \lhd & 2 & \lhd & 1
\end{array}
$$

1. Donner une définition de cette relation sans « petits points » [1]
2. Prouver que c'est un ordre total.

1. Bon... en s'arrangeant tout de même pour qu'elle soit réflexive et antisymétrique car on pourrait très bien définir une relation d'ordre strict ayant ce diagramme.

Exercice 8 : On définit sur $\mathbb{N}$ une relation $\preccurlyeq$ par : $x \preccurlyeq y \iff \exists n \in \mathbb{N}^*, y = x^n$.

1. ✪ Montrer que c'est une relation d'ordre. Est-ce un ordre total ?
2. ✪✪✪ Donner les éléments minimaux de cet ordre. Plus précisément, caractériser les éléments minimaux supérieurs ou égaux à 2 par leur décomposition en facteurs premiers.

Exercice 9 : ✪✪ Soit E un ensemble non vide. Soit $*$ une loi de composition interne commutative et associative sur E, c'est-à-dire :

- $\forall (x,y) \in E^2, x * y = y * x$.
- $\forall (x,y,z) \in E^3, x * (y * z) = (x * y) * z$.

On suppose de plus que tout élément de E est idempotent, i.e. : $\forall x \in E, x * x = x$. On définit sur E la relation $\preccurlyeq$ par :

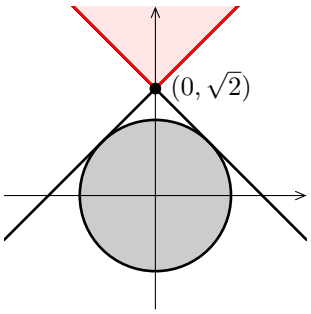
$$x \preccurlyeq y \iff x * y = x$$

1. Reconnaître $\preccurlyeq$ lorsque $*$ est l'intersection sur $\mathscr{P}(X)$.
2. Montrer que $\preccurlyeq$ est une relation d'ordre.
3. Montrer que, pour tout $(x,y) \in E^2$, $x * y = \inf(x,y)$ (au sens de la relation d'ordre $\preccurlyeq$).

Exercice 10 : ✪ On définit sur $\mathbb{R}^2$ une relation $\preccurlyeq$ par :

$$(x_1,y_1) \preccurlyeq (x_2,y_2) \iff |x_1 - x_2| \leq y_2 - y_1$$

1. Montrer que $\preccurlyeq$ est une relation d'ordre. Est-elle totale ?
2. ✪✪✪✪ Montrer que la borne supérieure du disque unité fermé est $(0, \sqrt{2})$.



Exercice 11 : ✪✪ Montrer qu'il n'existe pas de relation d'ordre totale $\preccurlyeq$ sur $\mathbb{C}$ qui soit compatible avec la structure de corps, c'est à dire qui vérifie :

$$\forall (x,y,z) \in \mathbb{C}^2, \begin{cases} x \preccurlyeq y & \Rightarrow \quad x + z \preccurlyeq y + z \\ (x \preccurlyeq y \text{ et } 0 \preccurlyeq z) & \Rightarrow \quad x \times z \preccurlyeq y \times z \end{cases}$$

Exercice 12 : ✪✪

1. Montrer que, dans un ensemble fini E non vide muni d'une relation d'ordre $\preccurlyeq$, il n'y a pas de suite infinie strictement monotone, c'est-à-dire de suite $(x_n)_{n\in\mathbb{N}}$ vérifiant : $(\forall n \in \mathbb{N}, (x_n \preccurlyeq x_{n+1} \text{ et } x_n \neq x_{n+1}))$ ou $(\forall n \in \mathbb{N}, (x_{n+1} \preccurlyeq x_n \text{ et } x_n \neq x_{n+1}))$. En déduire qu'un ensemble ordonné fini admet un élément minimal.
2. Que répondre à quelqu'un qui vous dit : « on trouve toujours plus bête que soi » ? Est-ce à dire qu'il existe un humain plus bête que tous les autres ?

Exercice 13 : ✪✪ Soit $(E, \preccurlyeq)$ un ensemble ordonné. On dit que c'est un bon ordre si toute partie non vide de E admet un plus petit élément.

1. Donner un exemple de bon ordre et un exemple de « mauvais ordre » total.
2. Montrer qu'un bon ordre est un ordre total.
3. Montrer que si $\preccurlyeq$ est un bon ordre, alors une suite décroissante d'éléments de E est stationnaire.
4. Soit $(E, \preccurlyeq)$ un ensemble totalement ordonné. On suppose qu'il existe une bijection f croissante de $\mathbb{N}$ dans E (c'est-à-dire telle que : $\forall (n,m) \in \mathbb{N}^2, n \leq m \Rightarrow f(n) \preccurlyeq f(m)$). Montrer que $\preccurlyeq$ est un bon ordre sur E.
5. Montrer qu'il n'existe pas de bijection croissante de $\mathbb{N}$ dans $\mathbb{Q}$ muni de l'ordre usuel.

Exercice 14 : ✪✪ Soit $(E, \leq)$ un ensemble ordonné. On suppose que toute partie non vide de E admet un maximum et un minimum. Montrer que E est un ensemble fini.

Exercice 15 : ✪✪ Dans cet exercice, pas si difficile mais assez abstrait (grrr), on montre que les relations d'ordre totales sont les meilleures relations d'ordre au sens d'un ordre sur l'ensemble des relations d'ordre.

Soit E un ensemble non vide. On note $O(E)$ l'ensemble des relations d'ordre sur E. Pour R_1 et R_2 appartenant à $O(E)$, on dit que R_2 est plus fine que R_1 si on a :

$$\forall (x,y) \in E^2, \qquad xR_1y \Rightarrow xR_2y$$

Autrement dit, si deux éléments sont comparables par R_1, ils le sont aussi par R_2 (et dans le même sens). On écrit alors $R_1 \preccurlyeq R_2$.

1. Montrer que $\preccurlyeq$ est une relation d'ordre sur $O(E)$.
2. Y a-t-il un plus petit élément pour $\preccurlyeq$ dans $O(E)$? Il n'est pas dur d'imaginer ce qui est la pire relation d'ordre possible...
3. Montrer qu'une relation d'ordre totale est un élément maximal de $O(E)$.
4. Soit $R \in O(E)$ non totale et soient a et b deux éléments de E non comparables par R. On définit la relation binaire S par :
$$xSy \iff [xRy \text{ ou } (xRa \text{ et } bRy)]$$
Que dire de S ? En déduire que les éléments maximaux de $O(E)$ pour $\preccurlyeq$ sont exactement les relations d'ordre totales.

Exercice 16 : ✪✪✪ On note E l'ensemble des couples (A, f) constitués d'une partie non vide A de $\mathbb{R}$ et d'une fonction $f : A \to \mathbb{R}$. On définit sur E une relation $\preccurlyeq$ par :

$$(A,f) \preccurlyeq (B,g) \iff A \subset B \qquad \text{et} \qquad g \text{ est un prolongement de } f : \forall x \in A, g(x) = f(x)$$

1. Montrer que $\preccurlyeq$ est une relation d'ordre. Est-ce un ordre total ?
2. L'ensemble des couples $\left([\,\varepsilon\,;+\infty\,[\,, \ln_{|[\,\varepsilon\,;+\infty\,[} \right)_{\varepsilon>0}$ admet-il un plus grand élément ? une borne supérieure ?

Exercice 17 - Ensembles inductifs : ✪✪✪ On dit qu'un ensemble ordonné $(E, \preccurlyeq)$ est inductif si toute partie non vide F de E totalement ordonnée admet un majorant (dans E).

1. Montrer qu'un ensemble fini est inductif.
2. $(\mathbb{Z}, \leq)$ est-il inductif ?
3. Soit E un ensemble non vide. Montrer que $(\mathscr{P}(E), \subset)$ est inductif.
4. On se replace dans le cadre de l'exercice 16. Montrer que $(E, \preccurlyeq)$ est un ensemble inductif.
5. On se replace dans le cadre de l'exercice 15. Montrer que $(O(E), \preccurlyeq)$ est un ensemble inductif.

Exercice 18 : ✪✪✪✪ Soit $(E, \preccurlyeq)$ un ensemble ordonné. On dit que c'est un ordre bien fondé s'il n'existe pas de suite infinie strictement décroissante.

1. Montrer qu'un bon ordre (voir l'exercice 13) est un ordre bien fondé.
2. Montrer que l'ordre produit et l'ordre lexicographique sur $\mathbb{N}^2$ sont bien fondés. En déduire qu'un ordre bien fondé n'est pas forcément un bon ordre.
3. Montrer qu'un ordre est un bon ordre si et seulement si c'est un ordre bien fondé et total.

Exercice 19 - Lemme de Spilrajn-Marczewski : ✪✪✪✪

1. Soit $(E, \leq_E)$ un ensemble ordonné fini de cardinal $n \geq 1$. Montrer qu'il existe une bijection croissante (i.e. vérifiant : $\forall (x,y) \in E^2, x \leq_E y \Rightarrow f(x) \leq f(y)$) de E dans $[\![\,1\,;\,n\,]\!]$.
2. En déduire qu'on peut munir E d'un ordre total $\preccurlyeq$ prolongeant $\leq_E$, c'est-à-dire tel que : $\forall (x,y) \in E^2, x \leq_E y \Rightarrow x \preccurlyeq y$. L'ordre $\preccurlyeq$ est appelé une extension linéaire de $\leq_E$.
3. Exhiber un ordre total sur $[\![\,1\,;\,10\,]\!]$ (différent de l'ordre $\leq$ usuel sur $\mathbb{Z}$) qui prolonge la relation de divisibilité, et représenter cet ordre sous la forme d'un diagramme linéaire.

16.3 Relations d'équivalence

Exercice 20 : ✪ On définit sur $E = (\mathbb{R}^*)^{\mathbb{N}}$, l'ensemble des suites ne s'annulant pas, la relation $\sim$ définie par :

$$(u_n)_{n\in\mathbb{N}} \sim (v_n)_{n\in\mathbb{N}} \iff \frac{u_n}{v_n} \xrightarrow[n\to+\infty]{} 1$$

1. Montrer que c'est une relation d'équivalence.
2. Montrer que deux suites équivalentes **convergentes** ont la même limite. Réciproque ?

Exercice 21 : ✪ Soit $n \in \mathbb{N}^*$. On définit sur $\mathbb{C}$ la relation R par : $z_1 R z_2 \iff {z_1}^n = {z_2}^n$. Montrer que c'est une relation d'équivalence et déterminer le cardinal des classes d'équivalence.

Exercice 22 - Germes de fonctions : ✪ On définit sur $\mathbb{R}^{\mathbb{R}}$ une relation $\sim$ par :

$$f \sim g \iff \exists \varepsilon > 0, \forall x \in [\,-\varepsilon\,;\varepsilon\,], f(x) = g(x)$$

Montrer que c'est une relation d'équivalence.

Exercice 23 : ✪ On définit sur $\mathbb{Z}$ une relation R par : $xRy \iff x+y$ est pair. Montrer que c'est une relation d'équivalence et donner les classes d'équivalence.

Exercice 24 : ✪ On définit sur $\mathbb{R}^{\mathbb{N}}$ une relation $\approx$ par : $(u_n)_{n\in\mathbb{N}} \approx (v_n)_{n\in\mathbb{N}} \iff \exists n_0 \in \mathbb{N}, \forall n \geq n_0, u_n = v_n$. Montrer que c'est une relation d'équivalence

Exercice 25 - Conjugaison : On note $S_{\mathbb{R}}$ l'ensemble des bijections de $\mathbb{R}$ dans $\mathbb{R}$. On définit sur $\mathbb{R}^{\mathbb{R}}$ une relation $\sim$ par :

$$f \sim g \iff \exists \varphi \in S_{\mathbb{R}}, f = \varphi^{-1} \circ g \circ \varphi$$

Montrer que c'est une relation d'équivalence.

Exercice 26 - Normes équivalentes : ✪ Soit E un ensemble non vide. On définit sur $\mathbb{R}^E$ une relation $\sim$ par :

$$f \sim g \iff \exists (\alpha,\beta) \in \left(\mathbb{R}_+^*\right)^2, \forall x \in E, \alpha g(x) \leq f(x) \leq \beta g(x)$$

Montrer que c'est une relation d'équivalence.

Exercice 27 : ✪✪

1. Que dire d'une relation d'équivalence $\sim$ sur $\mathbb{R}$ vérifiant : $\exists \varepsilon > 0, \forall (x,y) \in \mathbb{R}^2, |x-y| \leq \varepsilon \Rightarrow x \sim y$?
2. Même question avec une relation d'équivalence vérifiant : $\forall x \in \mathbb{R}, \exists \varepsilon > 0, \forall y \in \mathbb{R}, |x-y| \leq \varepsilon \Rightarrow x \sim y$.

Exercice 28 : ✪✪

1. On définit sur $\mathbb{R}$ une relation R par : $xRy \iff xe^y = ye^x$. Montrer que c'est une relation d'équivalence et donner le cardinal des classes d'équivalences.
2. **Remake :** On définit sur $\mathbb{R}_+^*$ une relation $\sim$ par : $x \sim y \iff \dfrac{\ln(x)}{y} = \dfrac{\ln(y)}{x}$. Montrer que c'est une relation d'équivalence et donner le cardinal des classes d'équivalences.

Exercice 29 : ✪✪✪ On définit sur $\mathbb{R}^{\mathbb{N}}$ une relation R par :

$$(u_n)_{n\in\mathbb{N}} R (v_n)_{n\in\mathbb{N}} \iff \forall n \in \mathbb{N}, \exists (p,q) \geq n, (u_p \leq v_n) \text{ et } (v_q \leq u_n)$$

1. R est-elle une relation d'ordre ? une relation d'équivalence ?
2. Notons c une suite constante. Déterminer les suites $(u_n)_{n\in\mathbb{N}}$ en relation avec c.

16.4 Ensembles quotients

Exercice 30 - Construction de $\mathbb{Z}$ à partir de $\mathbb{N}$: ✪✪✪

1. Montrer que la relation $\sim$ définie sur $\mathbb{N}^2$ par : « $(a,b) \sim (c,d) \iff a+d = b+c$ » est une relation d'équivalence.
2. Montrer que la fonction
$$\varphi : \begin{cases} \mathbb{N}^2/\sim & \to & \mathbb{Z} \\ \overline{(a,b)} & \mapsto & a-b \end{cases}$$
est bien définie et bijective. Ceci peut constituer une construction de $\mathbb{Z}$: les éléments de $\mathbb{Z}$ sont vus comme les différences de couples d'entiers.

Exercice 31 - Construction de $\mathbb{R}$ à partir de $\mathbb{Q}$: ✪✪✪✪
On note $\widetilde{\mathscr{P}}(\mathbb{Q})$ l'ensemble des parties de $\mathbb{Q}$ non vides et majorées. Soit la relation $\equiv$ définie sur $\widetilde{\mathscr{P}}(\mathbb{Q})$ par :

$$X \equiv Y \iff (\forall x \in X, \forall \varepsilon \in \mathbb{Q}_+^*, \exists y \in Y, x - \varepsilon \leq y) \text{ et } (\forall y \in Y, \forall \varepsilon \in \mathbb{Q}_+^*, \exists x \in X, y - \varepsilon \leq x)$$

1. Montrer que c'est une relation d'équivalence.
2. Soit $(X,Y) \in \widetilde{\mathscr{P}}(\mathbb{Q})^2$. Montrer que : $X \equiv Y \iff \sup_{\mathbb{R}}(X) = \sup_{\mathbb{R}}(Y)$.
3. En déduire une bijection entre $\widetilde{\mathscr{P}}(\mathbb{Q})/\equiv$ et $\mathbb{R}$. Ceci peut constituer une construction de $\mathbb{R}$: les éléments de $\mathbb{R}$ sont vus comme les bornes supérieures des sous-ensembles non vides majorés de $\mathbb{Q}$.

Chapitre 17

Dénombrement

« Je suis du FBI, tu sais ce que ça veut dire sale petit enfoiré ? Tu n'as aucun droit, ta vie dépend de moi, je pourrais te faire avaler tes dents et te les arracher par le trou de balle sans même violer tes droits civiques ! »

La Firme

Sauf indication contraire, n est un entier supérieur ou égal à 1.

17.1 Dénombrement pur et dur

Exercice 1 : ✪ À l'issue d'un concours, 160 candidats sont admis dont 70 garçons. Déterminer le nombre de classements possibles des 10 premiers admis qui contiennent autant de filles que de garçons.

Exercice 2 : ✪ On désire former un jury avec deux scientifiques et trois littéraires. On dispose pour cela de cinq scientifiques et de sept littéraires. Combien de jurys peut-on former dans les situations suivantes ?

1. Dans le cas général.
2. Un littéraire donné doit faire partie de tous les jurys.
3. Deux scientifiques ne s'entendent pas et ne peuvent pas faire partie du même jury.
4. Même question avec deux littéraires.

Exercice 3 : ✪ Soit A un ensemble fini non vide appelé *alphabet*. Les éléments de A sont appelés des *lettres*. Pour $n \in \mathbb{N}^*$, un *mot de longueur n sur l'alphabet A* est tout simplement un élément de A^n. Soit $p \geq 1$ le cardinal de A.

1. Combien y a-t-il de mots de longueur n ? Et de mots de longueur n formés de n lettres distinctes ?
2. Si $u = (u_1, \dots, u_n)$ on pose $\widetilde{u} = (u_n, \dots, u_1)$. u est appelé un *palindrome* si $u = \widetilde{u}$. Combien y a-t-il de palindromes de longueur n ?
3. Combien y a-t-il de mots de n lettres sans deux lettres consécutives identiques ?

Exercice 4 : ✪ En France, à tout véhicule est attribué un numéro d'immatriculation (SIV) formé de sept caractères alphanumériques : deux lettres, un tiret, trois chiffres, un tiret et deux lettres (par exemple « KZ-119-EP »). Les lettres interdites sont I, O et U (car elles sont trop ressemblantes avec 1, 0 et V respectivement). La série de chiffres 000 est interdite, ainsi que la série de lettres SS. Enfin la série WW est interdite pour le bloc de gauche (elle correspond aux immatriculations provisoires).

1. Combien y a-t-il d'immatriculations possibles ?
2. Combien y a-t-il d'immatriculations ne contenant aucune lettre ni chiffre dupliqué ?

Exercice 5 : ✪ Soit E l'ensemble des nombres à 6 chiffres ne contenant pas 0 dans leur écriture décimale.

1. Quel est le cardinal de E ?
2. Combien y a-t-il d'éléments de E composés de chiffres différents ?
3. Combien y a-t-il d'éléments impairs dans E ?
4. Combien y a-t-il d'éléments de E ne contenant que des 2 et des 3 ?
5. Soit $k \in [\![1 ; 6]\!]$. Combien y a-t-il d'éléments dont le premier 4 apparaît en k-ième position ?

Exercice 6 - Hirondelles et noix de coco : ✪ Quel est le nombre d'anagrammes (je précise que « anagramme » est un mot féminin !) du mot Ni ? Du mot knights ? Du mot shrubbery ? Et, en ne tenant pas compte des espaces ou des majuscules, du « mot » Ekke Ekke Ekke Ekke Ptang Zoo Boing ?

Exercice 7 : ✪ On suppose que $n \geq 2$ et que E est un ensemble à n éléments. Soient $a \neq b$ deux éléments de E.

1. Combien E admet-il de parties ne contenant ni a ni b ?
2. Combien E admet-il de parties ne contenant pas a ou ne contenant pas b ?

Exercice 8 : ✪ Donner le coefficient de $x^7y^3z^2$ dans $(x+2y+3z)^{12}$ à l'aide d'un raisonnement combinatoire.

Exercice 9 : ✪ Pierre le fermier a faim et veut commander une pizza chez Domino's. Il tombe sur cette publicité :

Il faut choisir la taille de la pizza (médium, large ou XL), la pâte (fine, classique, pan ou mozza crust), la base (sauce tomate, crème fraîche ou sauce barbecue) et enfin entre 3 et 11 ingrédients au choix parmi 35 ingrédients. Pierre le fermier peut-il attaquer Domino's pour publicité mensongère (et peut-être avoir une pizza gratuite) ?

Exercice 10 : ✪✪ Combien y a-t-il de diagonales dans un polygone convexe à n côtés ?

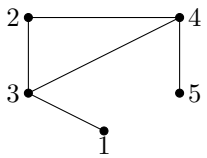
Exercice 11 : ✪✪ Dans un jeu de 52 cartes, combien y a-t-il de mains de 10 cartes avec exactement cinq trèfles ou exactement deux as ?

Exercice 12 : ✪✪ Soient n et p dans $\mathbb{N}^*$. Combien y a-t-il de familles strictement croissantes constituées de p éléments de l'ensemble $[\![1\,;n]\!]$?

Exercice 13 : ✪✪ Soit $n \geq 1$. Combien y a-t-il

1. de couples $(x,y) \in [\![1\,;n]\!]^2$ tels que $x < y$?
2. de couples $(x,y) \in [\![1\,;n]\!]^2$ tels que $x \leq y$?
3. de triplets $(x,y,z) \in [\![1\,;n]\!]^2$ tels que $x < y < z$?

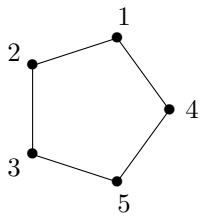
Exercice 14 - Graphes de Moore : ✪✪ Un graphe (simple, fini, sans boucle) est un couple (S,A), où S est un ensemble fini et où A est une partie de $\mathscr{P}_2(S)$, où $\mathscr{P}_2(S)$ est l'ensemble des parties de S à 2 éléments. Les éléments de S sont représentés par des points et les arêtes par des segments reliant les deux points qui les composent. Ci-dessous on a représenté le graphe (S,A) avec $S = [\![1\,;5]\!]$ et $A = \{\{1;3\};\{2;3\};\{2;4\};\{3;4\};\{4;5\}\}$:

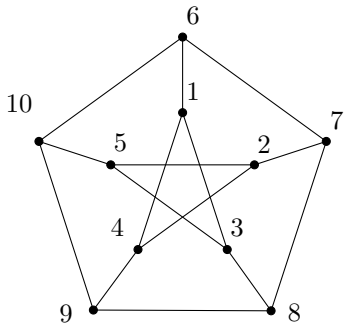


On appelle *degré* d'un sommet le nombre d'arêtes qui partent de ce sommet (c'est-à-dire plus simplement son nombre de voisins, par exemple, pour le graphe ci-dessus, le degré de 4 vaut 3, et celui de 5 vaut 1), et *distance* entre deux sommets la longueur du plus court chemin permettant d'aller de l'un à l'autre (par exemple, dans le graphe pentagonal ci-dessous, la distance entre 2 et 5 est égale à 2). Enfin, on dit qu'un graphe est de *diamètre* 2 si la plus grande distance entre deux sommets est 2. C'est par exemple le cas des deux graphes ci-dessous, tandis que le graphe ci-dessus est de diamètre 3 (car la distance entre 1 et 5 vaut 3).

Soit $d \geq 1$. Montrer qu'un graphe de diamètre 2 et dont tous les sommes ont un degré inférieur ou égal à d comporte au plus $n = d^2 + 1$ sommets.

Remarque : Lorsqu'il y a égalité, un tel graphe est appelé un graphe de Moore. Par exemple, les deux graphes ci-dessous sont des graphes de Moore (celui de droite est appelé graphe de Petersen) :



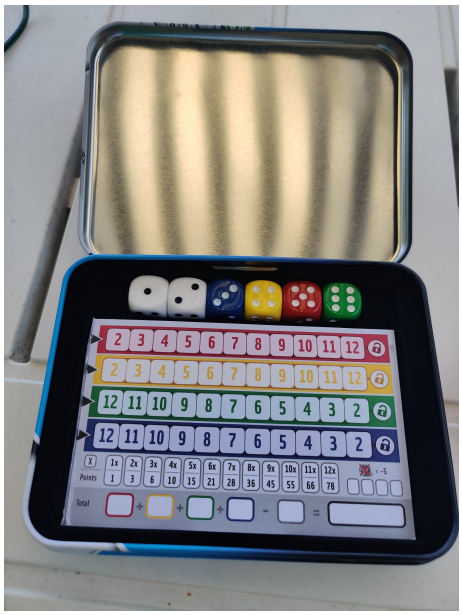


Le théorème de Hoffman et Singleton (que nous verrons peut-être en devoir cette année) dit que, si G est un graphe de Moore, alors $d = 1, 2, 3, 7$ ou 57... En particulier, il ne peut exister au plus que 5 graphes de Moore ! Lorsque $d = 1$, on a deux sommets reliés par une arête donc le graphe est de diamètre 1 (donc ce n'est pas un graphe de Moore), le graphe pentagonal ci-dessus est un graphe de Moore pour $d = 2$, le graphe de Petersen ci-dessus est un graphe de Moore pour $d = 3$, Hoffman et Singleton ont construit un graphe de Moore avec $d = 7$ (et donc 50 sommets : Wikipédia est votre ami pour savoir à quoi il ressemble). Par contre, on ne sait pas encore s'il existe un graphe de Moore de degré 57 à 3250 sommets...

Exercice 15 : ✪✪ Une urne contient 15 boules numérotées de 1 à 15. Les boules 1 à 5 sont blanches et les boules 6 à 15 sont noires. On tire successivement 5 boules de l'urne sans remise.

1. En tenant compte de l'ordre, combien y a-t-il de tirages possibles ?
2. En tenant compte de l'ordre, combien y a-t-il de tirages contenant deux boules blanches et trois boules noires ?

Exercice 16 : ✪✪ Pierre le fermier joue au jeu Qwixx (dont les règles n'ont aucune importance dans cet exercice). Ce jeu comporte six dés : deux dés blancs, un dé rouge, un dé vert, un dé bleu et un dé jaune. Après avoir joué, il décide de ranger les dés et, pour éviter la monotonie, il décide de les ranger à chaque fois dans une configuration différente, en prenant en compte les numéros et l'ordre des dés (ci-dessous deux configurations différentes).



Combien de parties peut-il effectuer ainsi ?

Exercice 17 : ✪✪ Un jeu de tarot est constitué de 78 cartes dont 22 atouts (21 numérotés de 1 à 21 et l'excuse ne portant pas de numéro). Combien y a-t-il de tirages de quinze cartes

1. en tout ?
2. contenant les trois bouts (le 1, le 21 et l'excuse) ?

3. contenant au moins un bout ?
4. contenant au moins une poignée (au moins 8 atouts) ?
5. une misère d'atouts (aucun atout) ?
6. contenant 5 atouts dont exactement un multiple de 3 et un multiple de 5 ?

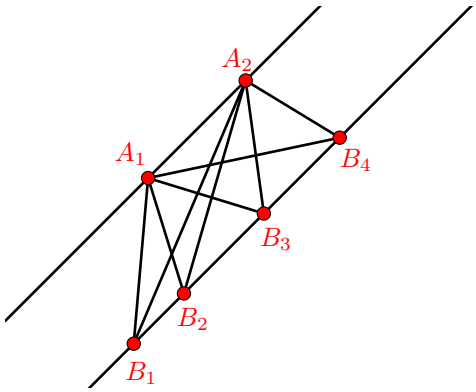
Exercice 18 : ✪✪

1. Soit $p \in [\![1\,;n]\!]$ et soit A une partie non vide de $[\![1\,;n]\!]$ de cardinal p. Montrer qu'il existe une unique application strictement croissante de $[\![1\,;p]\!]$ dans $[\![1\,;n]\!]$ dont l'image est A.
2. Soit $p \in \mathbb{N}^*$. Déterminer le nombre d'applications de $[\![1\,;p]\!]$ dans $[\![1\,;n]\!]$ strictement croissantes.
3. ✪✪✪ Soit $p \in \mathbb{N}^*$. À l'aide de l'exercice 26, déterminer le nombre d'applications croissantes de $[\![1\,;p]\!]$ dans $[\![1\,;n]\!]$.

Exercice 19 : ✪✪✪ Si A est une partie non vide de $[\![1\,;n]\!]$, on définit son diamètre par : $\mathrm{diam}(A) = \max(A) - \min(A)$.

1. Justifier que le diamètre est bien défini.
2. Soit $k \in \mathbb{N}$. Déterminer le nombre de parties de $[\![1\,;n]\!]$ de diamètre k.

Exercice 20 : ✪✪✪ On dispose de deux droites parallèles, dont l'une contient p points notés $A_1, \ldots, A_p$ et l'autre contient q points, notés $B_1, \ldots, B_q$. On suppose que trois des segments $[A_iB_j]$ ne sont jamais concourants.



Combien y a-t-il de points d'intersection entre les segments (si on ne compte pas les sommets) ?

Exercice 21 - Tu es comme le H de Hawaï : ✪✪✪ Le HUMUHUMUNUKUNUKUAPUA'A est un poisson multicolore et un emblème de l'état de Hawaï.

1. Démontrer que le nombre N d'anagrammes que l'on peut écrire avec 2 H, 2 M, 2 N, 2 K, 3 A et 1 P (c'est-à-dire sans prendre en compte le U) est donné par la formule (on ne demande pas de faire le calcul)

$$N = \frac{12!}{(2!)^4 3!}$$

   Dans les questions suivantes on pourra donner les résultats sous forme d'expressions pouvant contenir la lettre N. On ne demande pas de calculer numériquement ni de simplifier les résultats.
2. Combien y a-t-il d'anagrammes différentes de HUMUHUMUNUKUNUKUAPUAA ?
3. Une anagramme de HUMUHUMUNUKUNUKUAPUAA est dite *équilibrée* lorsqu'elle est sans U aux extrémités et sans U consécutifs, c'est-à-dire lorsqu'elle est de la forme

$$\bullet U \bullet U \bullet U \bullet U \bullet U \bullet U \bullet U \bullet U \bullet$$

   où chacun des 10 symboles $\bullet$ désigne une ou plusieurs lettres parmi les 12 suivantes : 2 H, 2 M, 2 N, 2 K, 3 A et 1 P.

   (a) Justifier qu'il n'est pas possible que l'un des symboles $\bullet$ représente 4 lettres ou plus.

   (b) Combien existe-t-il d'anagrammes équilibrées de HUMUHUMUNUKUNUKUAPUAA où l'on trouve trois lettres consécutives qui ne sont pas des U ?

   (c) Combien existe-t-il d'anagrammes équilibrées de HUMUHUMUNUKUNUKUAPUAA où l'on ne trouve pas trois lettres consécutives qui ne sont pas des U ?

   (d) Combien existe-t-il d'anagrammes équilibrées de HUMUHUMUNUKUNUKUAPUAA ?

Exercice 22 : ✪✪✪ Il y a $128 = 2^7$ participants au tournoi simple messieurs de Roland-Garros. Combien y a-t-il de façons d'organiser le premier tour, en considérant que l'ordre des parties n'a pas d'importance ?

Exercice 23 : ✪✪✪ Combien y a-t-il de mains de chaque sorte (quinte flush, carré, full, couleur, suite, brelan, double paire, paire, rien) au poker (5 cartes, dans un jeu de 52 cartes) ?

Exercice 24 - Formule d'inversion de Pascal : ✪✪✪

1. Montrer que $\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{n-k}$ pour tous $0 \leq j \leq k \leq n$. Interprétation combinatoire ?
2. Soient (a_n) et (b_n) deux suites de nombres réels telles que pour tout $n \in \mathbb{N}$ on ait

$$a_n = \sum_{k=0}^{n} \binom{n}{k} b_k$$

Montrer que pour tout $n \in \mathbb{N}$:

$$b_n = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} a_j$$

3. Soit $n \geq 1$. On appelle dérangement une permutation sans point fixe (on rappelle qu'une permutation d'un ensemble E peut être vue comme une bijection de E). Soit D_n le nombre de dérangements d'un ensemble à n éléments. Montrer que

$$D_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k!$$

Exercice 25 - Fonction de Möbius : ✪✪✪✪ On définit $\mu : \mathbb{N}^* \to \{0; 1; -1\}$ comme suit : $\mu(1) = 1; \mu(n) = 0$ si n contient un facteur carré ; $\mu(p_1 \dots p_r) = (-1)^r$ si les p_i sont des nombres premiers distincts.

1. Montrer que si n_1, n_2 sont deux éléments premiers entre eux de $\mathbb{N}^*$ alors $\mu(n_1)\mu(n_2) = \mu(n_1 n_2)$. Montrer que ce n'est plus vrai si les deux entiers ne sont pas supposés premiers entre eux.
2. Montrer que pour tout $n \in \mathbb{N}^*, n \neq 1$ on a $\sum_{d|n} \mu(d) = 0$ où la somme est prise sur les diviseurs de n.
3. Soit f une fonction de $\mathbb{N}^*$ dans $\mathbb{R}$ (note pour plus tard : on peut remplacer $\mathbb{R}$ par n'importe quel groupe abélien). On pose $g(n) = \sum_{d|n} f(d)$. Démontrer la formule d'inversion de Möbius :

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

Exercice 26 - Combinaisons avec répétitions : ✪✪✪✪ On appelle combinaison avec répétitions de k éléments parmi n un choix sans ordre de k éléments parmi n avec d'éventuelles répétitions. Par exemple, il y a 10 combinaisons avec répétitions de 3 éléments de l'ensemble $[\![1 ; 3]\!]$:

$$(1,2,3), (1,1,2), (1,1,3), (1,2,2), (2,2,3), (1,3,3), (2,3,3), (1,1,1), (2,2,2), (3,3,3)$$

1. On se donne $n + k - 1$ emplacements symbolisés par des étoiles :

$$\underbrace{* * \cdots *}_{n+k-1 \text{ emplacements}}$$

Montrer qu'on peut représenter une combinaison à k éléments dans un ensemble à n éléments par $n+k-1$ emplacements dont $k-1$ sont occupés par des barres verticales et les autres par des ronds :

$$\underbrace{\circ \circ \,||\, \circ \,|\, \cdots |\circ}_{n+k-1 \text{ emplacements}}$$

2. En déduire que le nombre de combinaisons avec répétitions de k éléments parmi n est $\binom{n+k-1}{k}$.

17.2 Relations de récurrence

Exercice 27 - Nombres de Bell : ✪✪ Pour tout $n \geq 0$, on note B_n le nombre de partitions d'un ensemble de cardinal n (l'ordre des ensembles formant la partition n'ayant pas d'importance) avec la convention $B_0 = 1$.

1. Calculer B_1, B_2 et B_3.
2. Montrer que, pour tout $n \in \mathbb{N}$:

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}$$

On pourra, dans un ensemble E de cardinal $n+1$, se donner un élément a de E et séparer les cas, selon le cardinal de la partie de E dans la partition qui contient a.

Exercice 28 - Nombre de surjections : ✪✪✪ Soient n et p appartenant à $\mathbb{N}^*$. On note $S(n,p)$ le nombre de surjections d'un ensemble à n éléments dans un ensemble à p éléments.

1. Calculer $S(n,p)$ lorsque $p > n$, ainsi que $S(n,n), S(n,1)$ et $S(n,2)$.
2. Calculer $S(n+1,n)$.
3. On suppose que $n \geq p+1$. Montrer que :

$$S(n,p) = \sum_{k=0}^{p} (-1)^{p-k} \binom{p}{k} k^n$$

On pourra utiliser l'exercice 24.

4. Montrer que pour tout $p \in [\![2\,;\, n-1]\!]$, $S(n,p) = p \times (S(n-1,p-1) + S(n-1,p))$. En déduire que :

$$S(n+2,n) = \frac{n(3n+1)(n+2)!}{24}$$

Exercice 29 : ✪✪✪ Pour tout ensemble E à n éléments, on note u_n le nombre d'involutions de E i.e. le nombre de fonctions $f : E \to E$ vérifiant $f \circ f = \mathrm{Id}_E$.

1. Calculer u_1, u_2 et u_3.
2. Montrer que, pour tout $n \in \mathbb{N}$, $u_{n+2} = u_{n+1} + (n+1)u_n$.

Exercice 30 - Lemme de Kaplansky : ✪✪✪ Pour tout $n \geq 1$, on note u_n le nombre de parties (éventuellement vides) de $[\![1\,;\, n]\!]$ ne contenant pas deux entiers consécutifs.

1. Calculer u_1, u_2 et u_3.
2. Soit $n \geq 1$. Trouver une relation de récurrence entre u_{n+2}, u_{n+1} et u_n. En déduire la valeur de u_n.

Exercice 31 - Compositions : ✪✪✪ Dans tout l'exercice, si $k \geq 1$, on appelle composition de n à k éléments une k-liste (ordonnée, donc) $(\alpha_1, \ldots, \alpha_k)$ d'entiers strictement positifs dont la somme vaut n. On note $C(n,k)$ l'ensemble des compositions de n à k éléments.

1. Donner toutes les compositions à 3 éléments de l'entier 5.
2. Montrer que, si n et k sont supérieurs ou égaux à 2, alors l'application suivante

$$f : (\alpha_1, \ldots, \alpha_k) \mapsto \{\alpha_1; \alpha_1 + \alpha_2; \cdots; \alpha_1 + \cdots + \alpha_{k-1}\}$$

est une bijection de $C(n,k)$ dans l'ensemble des parties de $[\![1\,;\, n-1]\!]$ à $k-1$ éléments. En déduire le nombre de compositions de n à k éléments. Que se passe-t-il lorsque $k = 1$ ou $n = 1$?

3. (a) Donner le nombre de compositions de n (l'entier k étant quelconque) ne comportant que des 1 et des 2 (par exemple, $(2,1,1,2,2,1)$ convient pour 9, mais $(1,2,3,1,2)$ ne convient pas).

   (b) En déduire que la suite de Fibonacci vérifie la relation suivante :

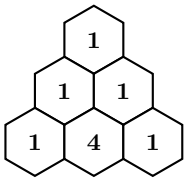
$$\forall n \geq 1, F_{n+1} = \sum_{i=0}^{+\infty} \binom{n-i}{i}$$

Exercice 32 - Nombres Eulériens : ✪✪✪✪ Pour tout $k \in [\![0\,;\, n-1]\!]$, on note $\left\langle {n \atop k} \right\rangle$ le nombre de permutations $w = (w_1, \ldots, w_n)$ de $[\![1\,;\, n]\!]$ contenant k descentes, c'est-à-dire k entiers $i \in [\![1\,;\, n-1]\!]$ (éventuellement aucun) vérifiant $w_i > w_{i+1}$. Par exemple, la permutation de $[\![1\,;\, 5]\!]$ notée $w = (1, 3, 2, 5, 4)$ contient 2 descentes, et la permutation $w = (1, 2, 3, 4, 5)$ n'en contient aucune.

1. Donner $\left\langle {1 \atop 0} \right\rangle, \left\langle {2 \atop 0} \right\rangle, \left\langle {2 \atop 1} \right\rangle, \left\langle {3 \atop 0} \right\rangle, \left\langle {3 \atop 1} \right\rangle, \left\langle {3 \atop 2} \right\rangle$.
2. Justifier que $\left\langle {n \atop 0} \right\rangle = \left\langle {n \atop n-1} \right\rangle = 1$ et $\left\langle {n \atop 1} \right\rangle = 2^n - n - 1$.
3. Montrer que :

$$\forall k \in [\![1\,;\, n-2]\!], \left\langle {n \atop k} \right\rangle = (n-k) \left\langle {n-1 \atop k-1} \right\rangle + (k+1) \left\langle {n-1 \atop k} \right\rangle$$

4. Construire les deux lignes suivantes dans le « triangle d'Euler » :

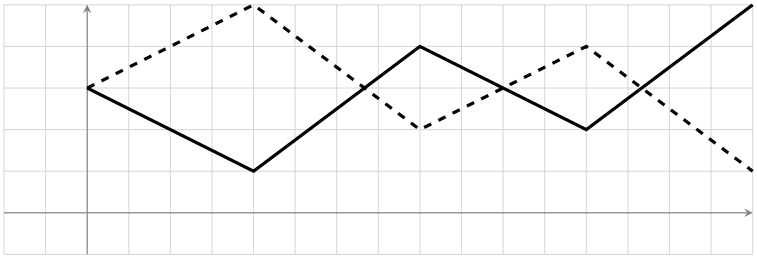


Exercice 33 - Permutations alternées : ✪✪✪✪ On dit qu'une permutation $w = (w_1, \ldots, w_n)$ de $[\![1\,;\, n]\!]$ est alternée si :

$$w_1 < w_2 > w_3 < w_4 > \cdots \qquad \text{ou} \qquad w_1 > w_2 < w_3 > w_4 < \cdots$$

Les permutations du premier type sont appelées permutations alternées haut/bas, et celles du second type sont appelées permutations alternées bas/haut.

1. Montrer qu'il y a autant de permutations alternées haut/bas que de permutations alternées bas/haut. On pourra s'inspirer du dessin suivant :



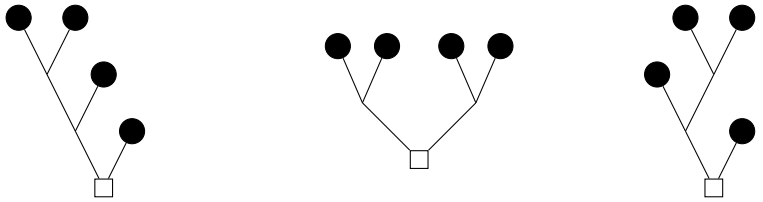
2. On note E_n le cardinal (commun, d'après la question précédente) de l'ensemble des permutations alternées bas/haut et de l'ensemble des permutations alternées haut/bas. Donner E_2, E_3, E_4.
3. En prenant la convention que $E_0 = E_1 = 1$, montrer que :

$$\forall n \geq 1, \qquad 2E_{n+1} = \sum_{k=0}^{n} \binom{n}{k} E_k E_{n-k}$$

Exercice 34 : ✪✪✪✪

1. Montrer que le nombre d'arbres à $n+1$ feuilles est C_n, le n-ième nombre de Catalan, si l'on convient que :
   - Par convention, il existe un seul arbre à 1 feuille.
   - À la base d'un arbre se trouve un « nœud racine ».
   - Chaque nœud possède une branche gauche et une branche droite (sauf pour un arbre ne contenant qu'une feuille).
   - Chaque branche mène à un nœud ou à une feuille.

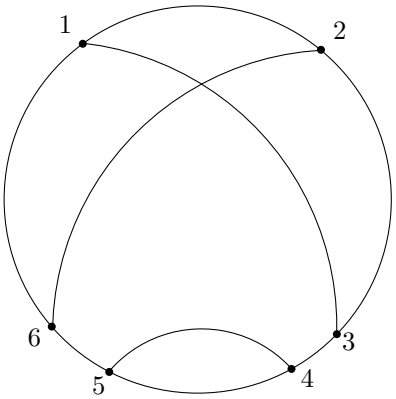
Voici trois exemples d'arbres à 4 feuilles (les disques noirs) :

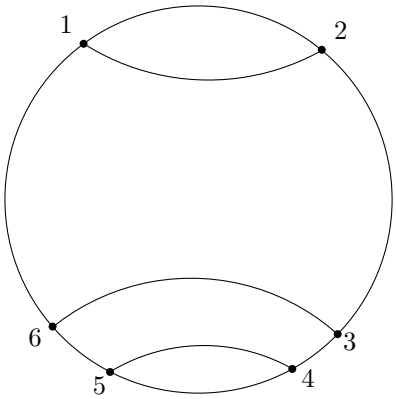


On rappelle que les nombres de Catalan sont définis par $C_0 = 1$ et :

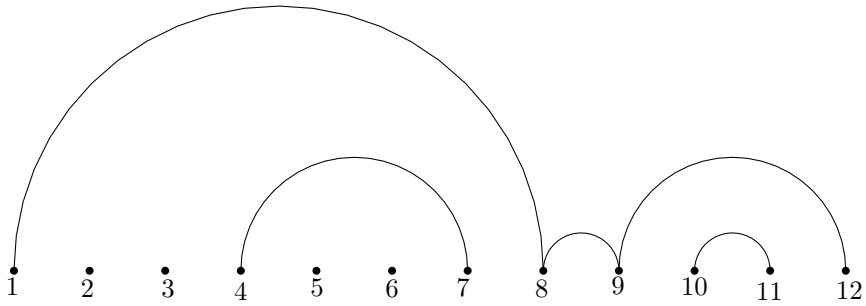
$$\forall n \geq 1, C_n = \sum_{k=0}^{n-1} C_k \times C_{n-1-k}$$

2. On dit qu'une partition de l'ensemble $[\![1\,;\, k]\!]$ est croisée s'il existe $1 \leq a < b < c < d \leq k$ tels que a, c appartiennent à une partie de la partition et b, d à une autre partie. Ci-dessous un dessin pour illustrer ce nom de partition croisée (et non croisée quand ce n'est pas le cas).





Exhiber une bijection entre les bons parenthésages à $2n$ parenthèses et les partitions non croisées de $[\![1\,;\, n]\!]$ (on rappelle qu'il peut y avoir des ensembles à un seul élément dans cette partition, comme dans l'autre dessin ci-dessous, qui donne une autre illustration du pourquoi du nom de ces partitions) :



3. On note, pour tout $n \geq 1$, γ_n le nombre de partitions de $[\![1\,;\, n]\!]$ non croisées (avec $\gamma_0 = 1$ par convention). Montrer d'une autre façon que, pour tout $n \geq 1$, $\gamma_n = C_n$. Plus précisément, montrer que la suite (γ_n) vérifie la même relation de récurrence que la suite (C_n).

17.3 Problèmes ensemblistes

Exercice 35 : ✪✪ Soit E un ensemble à n éléments. Montrer que $\sum_{X \subset E} \text{card}(X) = n2^{n-1}$.

Exercice 36 : ✪✪✪ Soit E un ensemble à n éléments. Combien y a-t-il de couples (A, B) de parties de E dont l'intersection soit un singleton ?

Exercice 37 : ✪✪✪ Soient n et p deux entiers strictement positifs, et soit E un ensemble à np éléments. Combien y a-t-il de partitions de E (en tenant compte de l'ordre puis sans en tenir compte) en n ensembles de cardinal p ?

Exercice 38 : ✪✪✪ Soit E un ensemble à n éléments.

1. Déterminer le nombre de couples $(X, Y) \in \mathscr{P}(E)^2$ tels que $X \subset Y$.
2. Déterminer le nombre de couples $(X, Y) \in \mathscr{P}(E)^2$ tels que $X \cap Y = \varnothing$.
3. Déterminer le nombre de triplets $(X, Y, Z) \in \mathscr{P}(E)^3$ tels que $X \subset Y \subset Z$.

Exercice 39 : ✪✪✪ Soit E un ensemble à n éléments.

1. Combien y a-t-il de partitions de E en deux ensembles (non vides) ?
2. Même question avec trois ensembles (non vides).

17.4 Principe des tiroirs de Dirichlet

Exercice 40 : ✪ Combien un village doit-il compter d'habitants pour que deux personnes au moins aient les mêmes initiales ?

Exercice 41 : ✪✪ Parmi 51 entiers distincts compris entre 1 et 100, montrer qu'il en existe toujours au moins deux consécutifs.

Exercice 42 : ✪✪ Montrer que, tous les matins, il existe deux élèves qui serrent le même nombre de mains (enfin, ça c'était avant le Covid...).

Exercice 43 : ✪✪ Soit $n \geq 1$.

1. Montrer qu'il existe n puissances de 10 distinctes ayant la même congruence modulo n.
2. En déduire qu'il existe un multiple de n qui ne s'écrit qu'avec des 1 et des 0 en écriture décimale.

Exercice 44 : ✪✪ Montrer que si on prend $n+1$ entiers distincts dans $[\![1\,;\, 2n]\!]$, alors il en existe un qui divise l'autre (on pourra s'intéresser à la valuation 2-adique de ces nombres). Montrer également qu'il en existe deux qui soient premiers entre eux.

Exercice 45 : ✪✪ Soient $a_1, \ldots, a_n$ des entiers (pas forcément distincts). Montrer qu'il existe $a_{k+1}, \ldots, a_l$ entiers consécutifs (éventuellement un seul) dont la somme est un multiple de n.

Exercice 46 : ✪✪✪ On dispose 1000 points distincts dans le plan. Montrer qu'il existe une droite séparant ces points en deux ensembles d'exactement 500 points.

Exercice 47 : ✪✪✪ Notons E_n l'ensemble des entiers à n chiffres ne s'écrivant qu'avec des 1 et des 2 (en écriture décimale). Quel est le cardinal de E_n ? Montrer que, parmi les éléments de E_n, un et un seul est divisible par 2^n.

17.5 Formule du crible

Exercice 48 : ✪ Combien y a-t-il d'entiers qui divisent au moins l'un des trois nombres 10^{60}, 20^{50} ou 30^{40} ?

Exercice 49 : ✪✪ Combien y a-t-il d'entiers entre 1 et 2024 divisibles par $2, 3$ ou 5 ?

Exercice 50 - Formule du crible de Poincaré : ✪✪✪✪ Montrer que si $E_1, \ldots, E_n$ sont des ensembles finis, alors :

$$\operatorname{card}\left(\bigcup_{k=1}^{n} E_k\right) = \sum_{k=1}^{n} \left((-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} \operatorname{card}\left(E_{i_1} \cap \cdots \cap E_{i_k}\right) \right)$$

Chapitre 18

Structures algébriques usuelles

« - Here. I wrote this when I was five.
- "A proof that algebraic topology can never have a non-self contradictory set of abelian groups." I'm just a blonde monkey to you, aren't I ?
- You said it, not me. »

The Big Bang Theory

Vrai ou Faux :

1. L'ensemble des racines complexes de -1 est un groupe pour la multiplication.
2. L'ensemble des fonctions $\mathscr{C}^\infty$ de $[\,0\,;1\,]$ dans $\mathbb{R}$ est un groupe pour l'addition.
3. L'ensemble vide est un sous-groupe de $\mathbb{Z}$.
4. Le seul sous-groupe de $\mathbb{Z}$ contenant 1 est $\mathbb{Z}$.
5. Le seul sous-groupe de $\mathbb{Z}$ contenant 4 est $4\mathbb{Z}$.
6. Un groupe fini est abélien.
7. La valeur absolue est un morphisme de groupes de $(\mathbb{R}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$.
8. La fonction $x \mapsto 2024\ln(x)$ est un morphisme de groupes de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.
9. L'image d'un morphisme de groupes est un sous-groupe du groupe d'arrivée.
10. L'image d'un groupe abélien par un morphisme de groupes est un groupe abélien.
11. L'image d'un groupe non abélien par un morphisme de groupes est un groupe non abélien.
12. L'image d'un groupe non abélien par un isomorphisme de groupes est un groupe non abélien.
13. Pour tout élément x d'un anneau A, $(-1_A) \times x$ est le symétrique de x pour l'addition.
14. Les éléments non nuls d'un anneau intègre sont inversibles.
15. La conjugaison est un morphisme de corps de $\mathbb{C}$ dans $\mathbb{C}$.
16. L'application partie réelle est un morphisme de corps de $\mathbb{C}$ dans $\mathbb{R}$.
17. L'application $x \mapsto -x$ est un morphisme de corps de $\mathbb{R}$ dans $\mathbb{R}$.

18.1 Lois de composition internes

Exercice 1 : ✪ Soit E muni d'une loi de composition associative et commutative notée multiplicativement. Soit $(x, y) \in E^2$. On suppose que xy est symétrisable. Montrer que x et y le sont aussi.

Exercice 2 : ✪ Soit E un ensemble non vide muni d'une loi de composition interne $*$. Un élément x de E est dit idempotent si $x * x = x$.

1. Montrer que si tout élément de E est régulier et si $*$ est distributive par rapport à elle-même, alors tout élément de E est idempotent.
2. Montrer que si tout élément de E est régulier et si $*$ est associative, alors E admet au plus un élément idempotent.

Exercice 3 : ✪ On munit l'ensemble $\mathbb{Q}^2$ d'une loi définie par $(x_1, y_1) \otimes (x_2, y_2) = (x_1x_2, y_1x_2 + y_2)$ pour tous couples (x_1, y_1) et (x_2, y_2) de $\mathbb{Q}^2$.

1. La loi $\otimes$ est-elle commutative ?

2. Montrer que $\otimes$ est associative et admet un élément neutre.
3. Étudier l'existence de symétriques.

Exercice 4 : ✪

1. Soit $\mathbb{N}$ muni des deux lois internes $*$ et $\circ$ définies par $a * b = a + 2b, a \circ b = 2ab$. Sont-elles commutatives, associatives, distributives l'une par rapport à l'autre ?
2. Même question avec $a * b = a + b$ et $a \circ b = ab^2$.
3. Même question avec $a * b = a^2 + b^2$ et $a \circ b = a^2b^2$.

Exercice 5 : ✪ Pour tous réels x et y, on pose $x \star y = x + y + xy^2$.

1. La loi $\star$ est-elle commutative ? associative ?
2. Montrer que $\star$ admet un élément neutre.
3. Montrer qu'aucun élément de $\mathbb{R}^*$ n'admet d'inverse pour $\star$.
4. Résoudre l'équation $x \star x = 3$.

Exercice 6 : ✪✪ Soit E un ensemble muni d'une loi $*$ associative. On suppose que E admet un élément neutre à gauche (i.e. : $\forall a \in E, e * a = a$) et que pour tout $a \in E$, il existe $b \in E$ tel que $b * a = e$.

1. Soit $a \in E$ tel que $a * a = a$. Montrer que $a = e$.
2. Soient $a \in E$ et $b \in E$ tel que $b * a = e$. Montrer que $a * b = e$.
3. Montrer que e est aussi élément neutre à droite (i.e. : $\forall a \in E, a * e = a$). E est alors muni d'une structure de groupe.

Exercice 7 : ✪✪ Soit $*$ la loi de composition interne sur $\mathbb{Q}$ définie par $a * b = a + b + ab$.

1. Associativité, commutativité, élément neutre de $*$?
2. $*$ est-elle distributive par rapport à l'addition et la multiplication dans $\mathbb{Q}$?
3. Quels sont les éléments inversibles, réguliers, idempotents (i.e. les éléments x tels que $x * x = x$) ?
4. Résoudre les équations $7 * x = 3$, $x * (-5) = -1$, $x * x = 2$, $x * x = 3$.
5. ✪✪✪ Calculer, pour a inversible et $n \in \mathbb{Z}$, a^n (il s'agit des puissances au sens de la loi $*$).

Exercice 8 - L'addition parallèle : ✪✪ Il est bien connu (demandez à votre professeur de physique préféré) en électricité que si on met deux résistances R_1 et R_2 en parallèle, la résistance équivalente obtenue est $\dfrac{R_1R_2}{R_1+R_2}$. On se propose dans cet exercice d'étudier quelques aspects de cette loi de composition interne.

On note // la loi de composition interne définie sur $\mathbb{R}_+^*$ par :

$$a//b = \frac{ab}{a+b}$$

1. Montrer que c'est bien une loi de composition interne.
2. Montrer qu'elle est associative et commutative.
3. Montrer que // n'a pas d'élément neutre.
4. Soient a et b strictement positifs. Soit $x > 0$. Montrer que

$$\inf_{\substack{(y,z)\in\mathbb{R}^2 \\ y+z=x}} \left(ay^2 + bz^2\right) = (a//b)x^2$$

   Cette borne inférieure est-elle atteinte ? Si oui, en quel(s) (y, z) ?
5. ✪✪✪ Soient $n \geq 1$, $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n)$ deux n-uplets de réels strictement positifs. Montrer que :

$$\sum_{i=1}^{n}(a_i//b_i) \leq \left(\sum_{i=1}^{n} a_i\right) // \left(\sum_{i=1}^{n} b_i\right)$$

   On pourra raisonner par récurrence prouver le résultat pour $n = 1$ et $n = 2$ (et s'armer de patience...).
6. Question bonus : donner une interprétation physique des résultats prouvés dans cet exercice.

Exercice 9 : ✪✪ Soient E et F deux ensembles non vides. Soit $f : E \to F$.

1. On suppose dans cette question que E n'est pas un singleton. Montrer que si f est injective mais non surjective, alors f admet plusieurs symétriques à gauche (pour la composition). Admet-elle un symétrique à droite ?
2. Montrer que si f est surjective mais non injective, alors f admet plusieurs symétriques à droite. Admet-elle un symétrique à gauche ?

Exercice 10 : Soit E un ensemble à n éléments.

1. ✪ Dénombrer les lois de composition internes sur E.
2. ✪✪ Dénombrer les lois de composition internes commutatives sur E.
3. ✪✪✪ Dénombrer les lois de composition internes commutatives sur E admettant un élément neutre.

Exercice 11 : ✪✪✪ Soit E un ensemble fini muni d'une loi de composition interne associative notée multiplicativement. Montrer qu'il existe $x \in E$ tel que $x^2 = x$.

18.2 Groupes

18.2.1 Exemples explicites

Exercice 12 : ✪ Soit n un entier naturel impair. On définit sur $\mathbb{R}$ la loi $*$ par :

$$\forall (x, y) \in \mathbb{R}^2, x * y = \sqrt[n]{x^n + y^n}$$

1. Montrer que $(\mathbb{R}, *)$ est un groupe abélien.
2. Soit $\varphi : x \mapsto x^n$. Montrer que φ est un isomorphisme de groupes de $(\mathbb{R}, *)$ dans $(\mathbb{R}, +)$.

Exercice 13 : ✪✪ Montrer que $\bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$. Est-il égal à $\mathbb{U}$?

Exercice 14 : ✪✪ Les ensembles suivants sont-ils des groupes ?

1. L'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ de la forme $x \mapsto ax + b$ avec $(a, b) \in \mathbb{R}^* \times \mathbb{R}$ muni de la composition.
2. $]-1\,;1[$ muni de la loi $\oplus$ définie par $x \oplus y = \dfrac{x + y}{1 + xy}$.
3. $\mathbb{R}^2$ muni de la loi $\star$ définie par $(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 e^{x_2} + y_2 e^{x_1})$.

Exercice 15 : ✪✪ Soit G l'ensemble suivant :

$$G = \left\{ x + y\sqrt{3} \,|\, x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1 \right\}$$

Montrer que G est un sous-groupe de $\mathbb{R}^{+*}$.

18.2.2 Calculs dans un groupe

Exercice 16 : ✪ Soit G un groupe. Soient $(a, b) \in G^2$ et $n \in \mathbb{N}^*$ tels que $(ab)^n = e$. Montrer que $(ba)^n = e$.

Exercice 17 : ✪ Soit G un groupe (pas nécessairement abélien) de neutre e et soient a et b deux éléments de G.

1. Montrer que si $ab = b^2a$ et $b^5 = e$ alors $ab^3 = ba$ et $a^2b^2 = b^3a^2$.
2. Montrer que si $a^5 = e$ et $ab = ba^3$ alors $a^2b = ba$ et $ab^3 = b^3a^2$.

Exercice 18 : ✪✪ Soit G un groupe tel que pour tout $(x, y) \in G^2, (xy)^2 = x^2y^2$. Montrer que G est commutatif.

Exercice 19 : ✪✪ Soit G un groupe dont tous les éléments x vérifient $x^2 = e$. Montrer que G est abélien.

18.2.3 Transport de structure

Exercice 20 : ✪✪ Soient G_1, G_2, H_1, H_2 quatre groupes. On suppose que G_1 et G_2 sont isomorphes, ainsi que H_1 et H_2. Montrer que les groupes $G_1 \times H_1$ et $G_2 \times H_2$ sont isomorphes.

Exercice 21 : ✪✪ Soient $(G, \times)$ un groupe, E un ensemble (pas forcément un groupe) et $f : G \to E$ une bijection. On définit une loi de composition interne $*$ sur E par :

$$\forall (x, y) \in E^2, x * y = f\left(f^{-1}(x) \times f^{-1}(y)\right)$$

Montrer que $(E, \times)$ est un groupe isomorphe à $(G, \times)$.

Exercice 22 : ✪✪ Soit $(E, \top)$ un groupe. Soit F un ensemble non vide muni d'une loi interne $\perp$. On suppose qu'il existe une bijection $f : E \to F$ telle que :

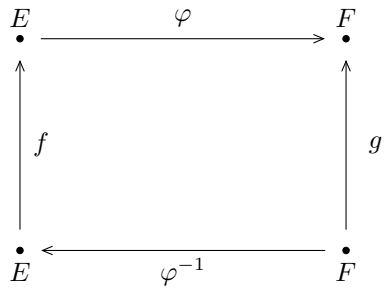
$$\forall (x, y) \in E^2, f(x \top y) = f(x) \perp f(y)$$

Montrer que $(F, \perp)$ est un groupe isomorphe à $(E, \top)$.

Exercice 23 : ✪✪ Soient $(G, .)$ un groupe et $a \in G$. On définit une nouvelle loi $*$ sur G par $x * y = xay$. Montrer que $(G, *)$ est un groupe isomorphe à $(G, .)$.

Exercice 24 : ✪✪✪ Les deux questions sont indépendantes.

1. Montrer que si E et F sont deux ensembles équipotents (i.e. s'il existe une bijection de E dans F) alors S_E et S_F sont isomorphes. On pourra s'inspirer du dessin ci-contre.
2. Montrer que si un ensemble contient au moins 3 éléments, alors $Z(S_E) = \{\mathrm{Id}_E\}$, c'est-à-dire que Id_E est le seul élément qui commute avec tout le monde.



18.2.4 Morphismes

Exercice 25 : ✪ Soit $n \geq 1$. Montrer que $z \mapsto z^n$ réalise un endomorphisme de groupe de $(\mathbb{C}^*, \times)$ (i.e. un morphisme de groupes de $(\mathbb{C}^*, \times)$ dans lui-même). Donner son image et son noyau.

Exercice 26 : ✪✪

1. Donner tous les morphismes de groupe de $\mathbb{Z}$ dans lui-même. En déduire le groupe des automorphismes de $\mathbb{Z}$ (i.e. des morphismes bijectifs de $\mathbb{Z}$ dans lui-même).
2. Donner tous les morphismes de groupe de $\mathbb{Q}$ dans lui-même.

Exercice 27 : ✪✪ Donner tous les morphismes de groupe de $\mathbb{Q}$ dans $\mathbb{Z}$.

Exercice 28 - Isomorphismes : ✪✪ Les groupes suivants sont-ils isomorphes ?

1. $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$.
2. $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$.
3. $(\mathbb{Q}, +)$ et $(\mathbb{Z}, +)$.
4. $(\mathbb{Q}_+^*, \times)$ et $(\mathbb{R}_+^*, \times)$.
5. $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$.

Exercice 29 - Autour de l'inverse : ✪✪✪

1. Montrer par récurrence que, pour tout n, une involution sur un ensemble à $2n + 1$ éléments admet au moins un point fixe.
2. Soit G un groupe. Montrer que $x \mapsto x^{-1}$ est un automorphisme de G (i.e. un morphisme bijectif de G dans lui-même) si et seulement si G est abélien.
3. On suppose dans cette question que G est un groupe fini et que f est un automorphisme de G involutif sans point fixe non trivial, c'est-à-dire : $\forall x \in G, f(x) = x \Rightarrow x = e$.
   (a) Montrer que $x \mapsto f(x)x^{-1}$ est une bijection de G dans G.
   (b) Montrer que pour tout $x \in G, f(x) = x^{-1}$.
   (c) En déduire que G est abélien et de cardinal impair.

18.2.5 Groupes et combinatoire

Exercice 30 : ✪✪ Soit G un groupe fini et soient A, B deux parties de G telles que $\text{card}(A) + \text{card}(B) > \text{card}(G)$. Enfin, notons $AB = \{ab \,|\, a \in A, b \in B\}$.

1. Montrer que, pour tout $g \in G$, $A \cap \{gb^{-1} \,|\, b \in B\}$ est non vide.
2. Montrer que $G = AB$.

Exercice 31 : ✪✪✪ Soit G un groupe et soient H et K deux sous-groupes de G. On pose $HK = \{hk \,|\, (h,k) \in H \times K\}$: c'est donc l'ensemble des produits d'un élément de H par un élément de K (dans cet ordre).

1. Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$, KH étant défini de façon analogue.
2. (a) Soient h_1 et h_2 deux éléments de H et k_1 et k_2 deux éléments de K. Montrer que $h_1k_1 = h_2k_2$ si et seulement s'il existe $x \in H \cap K$ tel que $h_2 = h_1x$ et $k_2 = x^{-1}k_1$.
   (b) On suppose que G est fini. Montrer que $\text{card}(HK) \times \text{card}(H \cap K) = \text{card}(H) \times \text{card}(K)$.

Exercice 32 : ✪✪✪ Soient G un groupe fini, H un groupe (pas forcément fini) et $f : G \to H$ un morphisme de groupes. Montrer que $\text{card}(G) = \text{card}(\ker(f)) \times \text{card}(\text{Im}(f))$.

18.2.6 Quelques groupes classiques

Exercice 33 - Centre d'un groupe : ✪✪ Soit G un groupe. On rappelle que le centre de G est l'ensemble $Z(G) = \{x \in G \,|\, \forall y \in G, xy = yx\}$ c'est-à-dire l'ensemble des éléments qui commutent avec tout le monde.

1. Montrer que si $f : G \to G$ est un automorphisme, alors $f(Z(G)) = Z(G)$.
2. Soit H un sous-groupe de G. Y a-t-il une inclusion entre $Z(H)$ et $Z(G) \cap H$? Montrer, à l'aide de l'exercice 24, qu'il n'y a pas forcément égalité.

Exercice 34 - Sous-groupes distingués : ✪✪✪ Soit G un groupe et soit H un sous-groupe de G. Si $x \in G$, on note $xH = \{xh \,|\, h \in H\}$, et on définit de façon analogue Hx et xHx^{-1}.

1. Montrer que les trois conditions suivantes sont équivalentes :

   - $\forall x \in G, xH = Hx$.
   - $\forall x \in G, xHx^{-1} = H$.
   - $\forall x \in G, \forall h \in H, xhx^{-1} \in H$.

   On dit qu'un sous-groupe de G vérifiant ces conditions est un sous-groupe distingué de G.
2. Montrer que si G est commutatif, tout sous-groupe de G est distingué dans G.
3. Soit $f : G_1 \to G_2$ un morphisme de groupes. Montrer que $\ker(f)$ est distingué dans G_1.
4. Montrer que $Z(G)$, le centre de G, est distingué dans G.
5. On suppose dans cette question que G est fini et que H est un sous-groupe d'indice 2 de G, c'est-à-dire que $\text{card}(H) = \text{card}(G)/2$. Montrer que H est distingué dans G. On pourra commencer par prouver que si $x \notin H$, G est l'union disjointe de H et de xH.

Exercice 35 - Théorème de Cayley : ✪✪✪ Soit G un groupe. En considérant la fonction φ_g de G dans lui-même définie par $\varphi_g : x \mapsto gx$, montrer que G est isomorphe à un sous-groupe de S_G. En déduire que si G est un groupe à n éléments, alors G est isomorphe à un sous-groupe de S_n. On pourra utiliser l'exercice 24.

18.2.7 Sous-groupes de $\mathbb{R}$

Exercice 36 : ✪✪

1. Montrer que $G = \{n + 2\pi p \,|\, (n,p) \in \mathbb{Z}^2\}$ est dense dans $\mathbb{R}$. On pourra utiliser sans démonstration le fait que π est irrationnel.
2. En déduire que l'ensemble $\{\cos(n) \,|\, n \in \mathbb{N}\}$ est dense dans $[-1\,;1]$.

Exercice 37 : ✪✪✪

1. Soit $(a,b) \in \mathbb{R}^2$. Montrer que $a\mathbb{Z} + b\mathbb{Z} = \{an + bk \,|\, (n,k) \in \mathbb{Z}^2\}$ est un sous-groupe de $\mathbb{R}$, et qu'il est dense si et seulement si a et b sont non nuls et a/b est irrationnel.
2. On se donne dans cette question un réel α et on note $H = \alpha\mathbb{N} + \mathbb{Z}$ (défini de manière analogue à l'ensemble de la question précédente).
   (a) Montrer que H un sous-groupe de $\mathbb{R}$ si et seulement si α est rationnel. On suppose dans la suite que α est irrationnel et on cherche à prouver que H est dense dans $\mathbb{R}$.

(b) Soient $a < b$ deux réels. Montrer, à l'aide de la question 1, qu'il existe $z \in \alpha\mathbb{N} + \mathbb{Z}$ tel que $0 < |z| < b - a$.

(c) Conclure (on pourra distinguer les cas selon le signe de z, et s'inspirer de la preuve de la densité de $\mathbb{Q}$ dans $\mathbb{R}$).

Exercice 38 : ✪✪✪ Montrer qu'il existe une puissance de 2 (positive ou négative) qui commence par votre date de naissance. Pour les puissances négatives, on dit qu'elles commencent au premier chiffre non nul (par exemple $1/4 = 0.25$ commence par un 2).

18.2.8 Un problème de groupes complet (découpé en trois exercices)

Exercice 39 - Produit semi-direct : ✪✪✪✪

1. Si G est un groupe, on note $\mathrm{Aut}(G)$ l'ensemble de ses automorphismes. Montrer que $(\mathrm{Aut}(G), \circ)$ est un groupe.
2. Soient H et K deux groupes et $\varphi : K \to \mathrm{Aut}(H)$ un morphisme de groupe. On munit $H \times K$ de la loi interne $*$ définie par :

$$(h_1, k_1) * (h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2)$$

Montrer que $(H \times K, *)$ est un groupe. Ce groupe est appelé produit semi-direct de H et K relativement à φ et est noté $H \rtimes_\varphi K$ ou $H \rtimes K$ s'il n'y a aucune ambiguïté sur φ.

3. Expliquer pourquoi le produit semi-direct est une généralisation du produit direct.

Exercice 40 - Un critère bien pratique : ✪✪✪✪ Soit G un groupe. On suppose que G admet deux sous-groupes H et K vérifiant les conditions suivantes :

- H est distingué dans K (cf. exercice 34)
- $H \cap K = \{e\}$.
- $G = HK$ (cf. exercice 31).

1. Montrer que pour tout $k_1 \in K$, $f_{k_1} : h \mapsto k_1hk_1{}^{-1}$ est un automorphisme de H. On note cet automorphisme morphisme $\varphi(k_1)$.
2. Montrer que G est isomorphe au produit semi-direct $H \rtimes_\varphi K$ où φ est définie par :

$$\varphi : \begin{cases} K & \longrightarrow & \mathrm{Aut}(H) \\ k_1 & \longmapsto & \varphi(k_1) \end{cases}$$

On vérifiera bien que φ est un morphisme de groupes.

Exercice 41 - Application à un certain type de groupes d'ordre 8 : ✪✪✪✪ On se donne dans cet exercice un groupe G à 8 éléments. On suppose qu'il existe $a \in G$ d'ordre 4 et $b \in G \backslash \mathrm{gr}(a)$ d'ordre 2. On pose enfin $H = \mathrm{gr}(a)$ et $K = \mathrm{gr}(b)$.

1. Montrer que H et K vérifient les conditions de l'exercice précédent. On pourra utiliser les exercices 31 et 34.
2. Rappeler pourquoi H est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ et K à $\mathbb{Z}/2\mathbb{Z}$. Dans la suite, quitte à raisonner comme dans l'exercice 20, on supposera donc que $H = \mathbb{Z}/4\mathbb{Z}$ et $K = \mathbb{Z}/2\mathbb{Z}$. On en déduit qu'il existe $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ tel que G soit isomorphe à $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.
3. En déduire qu'il existe exactement deux groupes non isomorphes vérifiant cette condition et donner leurs tables (on pourra utiliser l'exercice 69).

Remarque : Ici s'achève (presque) la recherche des groupes à 8 éléments (à isomorphisme près) : cf. corrigé.

18.3 Anneaux et corps

18.3.1 Anneaux et corps explicites

Exercice 42 : ✪ Montrer que l'ensemble des fonctions continues de $[\,0\,;1\,]$ dans $\mathbb{R}$ est un anneau (muni de l'addition et du produit des fonctions). Est-il intègre ?

Exercice 43 : ✪ On considère l'anneau $A = \mathbb{R}^{[\,0\,;2\,]}$ muni de l'addition et du produit des fonctions (il n'est pas demandé de prouver que c'est effectivement un anneau). On note A_1 l'ensemble des éléments de A nuls sur $]\,1\,;2\,]$. Montrer que $(A_1, +, \times)$ est un anneau inclus dans A. Est-ce un sous-anneau de A ?

Exercice 44 : ✪ On note $\mathbb{Q}_i$ l'ensemble des rationnels dont le dénominateur (dans l'écriture irréductible) est impair. Montrer que $\mathbb{Q}_i$ est un anneau et donner ses éléments inversibles.

Exercice 45 : ✪ Soit $k \in \mathbb{R}$. On munit $\mathbb{R}$ des deux lois de composition internes suivantes :

$$\forall (a,b) \in \mathbb{R}^2, a\$b = a+b-k \qquad \text{et} \qquad a \top b = ab - k(a+b) + k(k+1)$$

Étudier la structure de $(\mathbb{R}, \$, \top)$.

Exercice 46 : ✪ Montrer que $\mathbb{D}$ (l'ensemble des nombres décimaux) est un anneau. Est-ce un corps ? Mêmes question avec l'ensemble des nombres dyadiques.

Exercice 47 : ✪✪ Soit E un ensemble non vide quelconque.

1. Montrer que $(\mathscr{P}(E), \Delta)$ est un groupe abélien.
2. Montrer que $(\mathscr{P}(E), \Delta, \cap)$ est un anneau commutatif.
3. Est-ce que $(\mathscr{P}(E), \Delta, \cup)$ est un anneau ?
4. Soit F une partie de E. $\mathscr{P}(F)$ est-il un sous-anneau de $\mathscr{P}(E)$?
5. **Remake :** Ces résultats sont-ils encore vrais avec $\mathscr{P}_f(E)$, l'ensemble des parties finies de E, à la place de $\mathscr{P}(E)$?

Exercice 48 - L'anneau $\mathbb{Z}^2$: ✪✪✪✪ On munit $\mathbb{Z}^2$ de sa structure d'anneau produit comme dans l'exercice 61.

1. Quels sont les diviseurs de 0, les éléments inversibles de $\mathbb{Z}^2$?
2. Trouver tous les morphismes d'anneaux de $\mathbb{Z}^2$ dans $\mathbb{Z}$. On pourra s'intéresser aux images de $e_1 = (1,0)$ et $e_2 = (0,1)$ par un tel morphisme.
3. Déterminer les sous-anneaux de $\mathbb{Z}^2$.

18.3.2 Anneaux ou corps obtenus par adjonction d'un élément

Exercice 49 : ✪✪

1. Montrer que $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \,|\, (a,b) \in \mathbb{Z}^2\right\}$ est un anneau intègre.
2. On définit sur $\mathbb{Z}\left[\sqrt{2}\right]$ une application N par $N(a+b\sqrt{2}) = a^2 - 2b^2$. Montrer que N est une application multiplicative i.e. vérifie $N(xy) = N(x)N(y)$ pour tous x et y.
3. En déduire que les éléments inversibles de $\mathbb{Z}\left[\sqrt{2}\right]$ sont exactement les éléments de la forme $a+b\sqrt{2}$ avec $a^2-2b^2 = \pm 1$. D'après l'exercice 13 du chapitre 1, il y a donc une infinité d'inversibles.

Exercice 50 : ✪✪

1. Montrer que le seul morphisme de corps de $\mathbb{Q}$ dans $\mathbb{Q}$ est l'identité.
2. Déterminer tous les automorphismes de corps de $\mathbb{Q}\left[\sqrt{2}\right]$.

Exercice 51 : ✪

1. Montrer que $A = \{a + b\sqrt{3} \,|\, (a,b) \in \mathbb{Q}^2\}$ est un corps. Est-ce le cas de $B = \{a + b\sqrt{2} + c\sqrt{3} \,|\, (a,b,c) \in \mathbb{Q}^3\}$?
2. Montrer que A et $\mathbb{Q}\left[\sqrt{2}\right]$ ne sont pas isomorphes.

Exercice 52 : ✪✪

1. Montrer que $\mathbb{Q}[i] = \{a + ib \,|\, (a,b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{C}$.
2. On définit de même $\mathbb{Q}[j]$ où $j = e^{2i\pi/3}$. Montrer que $\mathbb{Q}[j]$ est un corps non isomorphe à $\mathbb{Q}[i]$.

Exercice 53 - Anneau d'Eisenstein : ✪✪✪ On définit $\mathbb{Z}[j]$ de façon analogue à ci-dessus.

1. Vérifier que $\mathbb{Z}[j]$ est un anneau.
2. Soit $u \in \mathbb{Z}[j]$. Vérifier que u est inversible dans $\mathbb{Z}[j]$ si et seulement si $|u| = 1$.
3. En déduire tous les inversibles de $\mathbb{Z}[j]$.

18.3.3 Anneau des fonctions à valeurs dans un anneau

Les quatre exercices suivants utilisent le fait (cf. cours) que si A est un anneau et I un ensemble non vide, alors A^I est muni d'une structure d'anneau quand on le munit de la somme et du produit de fonctions.

Exercice 54 : ✪ Si K est un corps, l'ensemble K^I est-il muni d'une structure de corps pour ces mêmes lois ? d'une structure d'anneau intègre ?

Exercice 55 : ✪ Soit E un ensemble non vide. Donner les diviseurs de zéro et les inversibles de $\mathbb{Z}^E$.

Exercice 56 : ✪✪ Soit A un anneau et soit I un ensemble non vide. Montrer que $U\left(A^I\right) = U(A)^I$.

Exercice 57 : ✪✪✪ On note S_t l'ensemble des suites stationnaires à valeurs dans $\mathbb{Z}$.

1. Vérifier que S_t est un sous-anneau de $\mathbb{Z}^{\mathbb{N}}$.
2. On souhaite déterminer tous les morphismes d'anneaux de S_t dans $\mathbb{Z}$.
   (a) Si $i \in \mathbb{N}$, on note v_i l'application évaluation en i c'est-à-dire que pour toute suite $u \in S_t$, on a $v_i(u) = u_i$. Montrer que v_i est un morphisme d'anneaux de S_t dans $\mathbb{Z}$.
   (b) Notons v_∞ l'application limite c'est-à-dire la fonction qui à toute suite $u \in S_t$ associe sa limite. Prouver que v_∞ est bien définie puis que c'est un morphisme d'anneaux.

   On souhaite montrer que ce sont les seuls morphismes d'anneaux de S_t dans $\mathbb{Z}$. On se donne dans la suite φ un morphisme d'anneaux de S_t dans $\mathbb{Z}$. De plus, si $i \in \mathbb{N}$, on note e_i la suite dont tous les termes valent 0 sauf celui d'indice i qui vaut 1 et, enfin, on note $\tilde{1}$ la suite constante égale à 1

   (c) Montrer qu'il existe au plus un $i \in \mathbb{N}$ tel que $\varphi(e_i) \neq 0$.
   (d) Supposons qu'il existe $i_0 \in \mathbb{N}$ tel que $\varphi(e_{i_0}) \neq 0$. Montrer que $(\varphi - v_{i_0})(e_i) = 0$ pour tout $i \in \mathbb{N}$ et que $(\varphi - v_{i_0})\left(\tilde{1}\right) = 0$. En déduire que $\varphi = v_{i_0}$.
   (e) Montrer de même que si $\varphi(e_i) = 0$ pour tout $i \in \mathbb{N}$, alors $\varphi = v_\infty$.

18.3.4 Anneaux et corps génériques

Exercice 58 : ✪ Soient A_1 et A_2 deux anneaux et $f : A_1 \to A_2$ un morphisme d'anneaux. Montrer que si A_2 a au moins deux éléments, $\ker(f)$ n'est pas un sous-anneau de A_1.

Exercice 59 : ✪ Montrer que le centre d'un anneau A est un sous-anneau de A.

Exercice 60 : ✪ Soit A un anneau (pas forcément commutatif) et soient a et b deux éléments de A tels que ab soit nilpotent. Montrer que ba est nilpotent.

Exercice 61 - Anneau produit : ✪ Soient $(A_1, +_1, \times_1)$ et $(A_2, +_2, \times_2)$ deux anneaux. S'inspirer du cours pour munir $A_1 \times A_2$ d'une structure d'anneau. Donner les inversibles de $A_1 \times A_2$ en fonction de ceux de A_1 et de ceux de A_2.

Exercice 62 : ✪✪ Soit A un anneau. On suppose que pour tout $(x, y) \in A^2, xy = yx$ ou $-yx$.

1. On pose $Z(A) = \{x \in A \,|\, \forall y \in A, xy = yx\}$ (Z est donc le centre de A) et $Y(A) = \{x \in A \,|\, \forall y \in A, xy = -yx\}$. Montrer que $Z(A)$ et $Y(A)$ sont des sous-groupes de A.
2. Montrer par l'absurde que $A = Z(A) \cup Y(A)$.
3. En déduire que A est commutatif.

Exercice 63 - Anneaux de Boole : ✪✪✪ Un anneau de Boole est un anneau dans lequel tout élément vérifie $x^2 = x$.

1. Donner un exemple d'anneau de Boole non réduit à un élément.
2. Montrer que, dans un anneau de Boole, tout élément x vérifie $x = -x$.
3. Montrer qu'un anneau de Boole est commutatif.
4. Déterminer (à isomorphisme près) le seul anneau de Boole intègre.
5. On définit une relation binaire $\preccurlyeq$ sur A par : $x \preccurlyeq y \iff yx = x$. Montrer que $\preccurlyeq$ est une relation d'ordre.

Exercice 64 - Idéaux : ✪✪✪ Si A est un anneau et si I est une partie de A, on dit que I est un idéal de A si I est un sous-groupe de $(A, +)$ absorbant pour la loi $\times$, i.e. :

$$\forall (a, i) \in A \times I, \qquad a \times i \in I \qquad \text{et} \qquad i \times a \in I$$

1. Donner les idéaux de $\mathbb{Z}$.
2. Soit $f : A_1 \to A_2$ un morphisme d'anneaux. Montrer que $\ker(f)$ est un idéal de A_1.
3. Soit I un idéal d'un anneau A. Montrer que I contient un élément inversible de A si et seulement si $I = A$.
4. Soit K un corps. Montrer que $\{0\}$ et K sont les seuls idéaux de K. En déduire qu'un morphisme de corps est forcément injectif.
5. Réciproquement, supposons que A soit un anneau commutatif dont les seuls idéaux sont $\{0\}$ et A. Montrer que A est un corps. On pourra s'intéresser, pour $x \in A$ non nul, à l'ensemble $xA = \{xa \,|\, a \in A\}$.
6. Supposons que A soit commutatif et que les tous les idéaux I de A vérifient :

$$\forall (x, y) \in A^2, xy \in I \Rightarrow x \in I \text{ ou } y \in I$$

   Montrer que A est intègre puis que $x \in x^2 A$ pour tout $x \in A$. En déduire que A est un corps.
7. Soit I un idéal d'un anneau commutatif A. On appelle radical de I l'ensemble noté $\sqrt{I}$ défini par :

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

   Montrer que $\sqrt{I}$ est un idéal de A. Expliciter $\sqrt{12\mathbb{Z}}$.

Exercice 65 - Un théorème de Kaplansky : ✪✪✪ On se donne dans cet exercice un anneau A commutatif et intègre, et on suppose que pour tout $a \in A$, il existe $b \in A$ tel que $a + b - ba = 0$.

1. Montrer que la loi $*$ définit par $a * b = a + b - ba$ est une loi de composition interne sur $A\backslash\{1\}$ qui en fait un groupe.
2. En déduire que A est un corps.

Exercice 66 : ✪✪✪ Soit $\mathbb{K}$ un corps. Le but de cet exercice est de prouver que les groupes $(\mathbb{K}, +)$ et $(\mathbb{K}^*, \times)$ ne sont pas isomorphes.

1. Démontrer ce résultat lorsque $\mathbb{K}$ est fini. On suppose dans la suite que $\mathbb{K}$ est infini.
2. Soit $\varphi : \mathbb{Z} \to K$ définie par $\varphi(n) = \underbrace{1_\mathbb{K} + \cdots + 1_\mathbb{K}}_{n \text{ fois}}$ si $n \geq 0$, et $\varphi(n) = \underbrace{-1_\mathbb{K} - \cdots - 1_\mathbb{K}}_{-n \text{ fois}}$ sinon. On rappelle (cf cours) que φ est un morphisme d'anneaux.
   (a) Justifier qu'il existe $p \in \mathbb{N}$ tel que $\ker(\varphi) = p\mathbb{Z}$: p est appelé la caractéristique de $\mathbb{K}$.
   (b) Montrer que p est nulle ou est un nombre premier.
3. Prouver que $(\mathbb{K}, +)$ et $(\mathbb{K}^*, \times)$ ne sont pas isomorphes. On s'intéressera à l'équation $x^2 = 1_\mathbb{K}$.

18.4 Deuxième année : Lagrange, ordre et $\mathbb{Z}/n\mathbb{Z}$

Exercice 67 : ✪ Soit $n \geq 2$. Donner les diviseurs de zéro éventuels de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 68 : ✪✪ Soit $n \geq 2$. Donner une CNS sur n pour que $\mathbb{Z}/n\mathbb{Z}$ admette des éléments nilpotents non nuls.

Exercice 69 : ✪✪ Expliciter tous les automorphismes de groupes de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.

Exercice 70 : ✪✪ Soit $n \geq 2$. Montrer que tous les diviseurs de zéro de $\mathbb{Z}/n\mathbb{Z}$ sont nilpotents si et seulement s'il existe p premier et $\alpha \geq 1$ tel que $n = p^\alpha$.

Exercice 71 : ✪✪ Soit G un groupe. Montrer que G n'admet aucun sous-groupe différent de $\{e\}$ et de lui-même si et seulement si G est fini et $\text{card}(G)$ est un nombre premier. Que dire alors de G ?

Exercice 72 : ✪✪✪ Montrer qu'un sous-groupe d'un groupe cyclique est cyclique.

Exercice 73 : ✪✪✪

1. Soit $n \geq 1$. Donner les sous-groupes de $\mathbb{U}_n$. On rappelle (cf. chapitre 7) que $\mathbb{U}_d \subset \mathbb{U}_n$ si et seulement si d divise n.
2. Montrer que les seuls sous-groupes finis de $\mathbb{C}^*$ sont de la forme $\mathbb{U}_n$.

Exercice 74 : ✪✪✪✪ Soit G un groupe fini non abélien. On pose $A = \{(a, b) \in G^2 \,|\, ab = ba\}$. Montrer que :

$$\text{card}(A) \leq \frac{5}{8} \times \text{card}(G)^2$$

Remarque : Il en découle que, dans un groupe fini non abélien, la probabilité que deux éléments commutent est inférieure ou égale à 5/8.

Chapitre 19

Polynômes

« Que je voudrais bien tenir un de ces puissants de quatre jours, si légers sur le mal qu'ils ordonnent, quand une bonne disgrâce a cuvé son orgueil ! Je lui dirais... que les sottises imprimées n'ont d'importance qu'aux lieux où l'on en gêne le cours ; que, sans la liberté de blâmer, il n'est point d'éloge flatteur ; et qu'il n'y a que les petits hommes qui redoutent les petits écrits. »

Beaumarchais, Le mariage de Figaro

Si rien n'est précisé, les polynômes sont supposés à coefficients dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et on pourra si besoin identifier polynômes et fonctions polynomiales.

Vrai ou Faux ?

1. Soit $P \in \mathbb{R}[X]$. Si P est de degré 2 alors $P + X^2$ aussi.
2. $x^2 + x + 1 \in \mathbb{R}_2[X]$.
3. $x^2 + x + 1 \in \mathbb{R}_3[X]$.
4. $x \mapsto x^2 + x + 1 \in \mathbb{R}_3[X]$.
5. $X^2 + X + 1 \in \mathbb{R}_3[X]$.
6. PQ' et QP' ont même degré.
7. Si P' est scindé alors P est scindé.
8. $2X$ est un diviseur de X.
9. Un polynôme constant est de degré nul.
10. $X - 2$ divise $X^5 - 3X^4 - 2X^3 + 3X^2 + 7X + 6$.
11. Si les seules racines complexes de P sont 0 et 1 alors $P = X(X - 1)$.
12. Si P et Q sont dans $\mathbb{C}[X]$, si $\deg P \leq \deg Q$ et si toutes les racines de P sont racines de Q alors P divise Q.
13. $-j$ est racine de $X^2 - X + 1$.
14. Si j est racine de $P \in \mathbb{R}[X]$ alors j^2 est aussi racine de P.

19.1 Racines, rigidité

Exercice 1 : ✪ Montrer qu'il existe un unique $P \in \mathbb{R}_n[X]$ tel que pour tout $k \in [\![0 ; n]\!], P(k) = k^n$.

Exercice 2 : ✪ Soient P, Q deux polynômes tels que pour tout réel $x, P(x)\sin(x) + Q(x)\cos(x) = 0$. Montrer que P et Q sont nuls.

Exercice 3 : ✪ Soient P et Q deux polynômes tels que pour tout $n \in \mathbb{N}, P\left(n^2\right) = Q\left(n^2\right)$. Montrer que $P = Q$.

Exercice 4 : ✪

1. Soit $n \geq 2$. Donner la multiplicité de la racine $a \neq 0$ de $P = (X - a)^n - (X^n - a^n)$.
2. **Remake :** Donner la multiplicité de 1 en tant que racine de $P = X^{10} - 25X^6 + 48X^5 - 25X^4 + 1$.
3. Soit $n \geq 1$. Trouver les complexes a et b tels que $(X - 1)^2$ divise $aX^{n+1} + bX^n + 1$.

Exercice 5 : ✪ Soit $P \in \mathbb{R}[X]$ de degré n et soit $a \in \mathbb{R}$ tel que $P(a), P'(a), \ldots, P^{(n)}(a)$ soient strictement positifs. Montrer que P ne s'annule pas sur $[\,a\,;+\infty\,[$.

Exercice 6 : ✪

1. Soient $(m,n,p) \in \mathbb{N}^3$. Montrer que X^2+X+1 divise $X^{3m+2}+X^{3n+1}+X^{3p}$.
2. **Remake :** Soit $n \in \mathbb{N}$ et soit $P_n \in \mathbb{C}[X]$ défini par $P_n = X^n+1$. Pour quelles valeurs de n P_n est-il divisible par X^2+1 ?

Exercice 7 : ✪ Soit $P \in \mathbb{R}[X]$. Montrer que P est monotone à partir d'une certaine valeur réelle.

Exercice 8 : ✪ Montrer qu'il n'existe pas de polynôme $P \in \mathbb{Z}[X]$ non constant tel que, pour tout $n \in \mathbb{Z}$, $P(n)$ soit un nombre premier.

Exercice 9 : ✪ Soit $(P,Q,R) \in \mathbb{R}[X]^3$ tel que $Q \circ P = R \circ P$. Montrer que si P n'est pas constant alors $Q = R$.

Exercice 10 : ✪ Soit $P \in \mathbb{C}[X]$ tel que $P\left(X^2\right) = P(X)P(X+1)$.

1. Donner la valeur de P si P est constant. On suppose dans la suite que ce n'est pas le cas.
2. Montrer que P admet au moins une racine complexe a.
3. Montrer que a^2 est aussi racine de P.
4. En déduire que $a = 0$ ou que a est une racine de l'unité.

Exercice 11 - Polynômes mystères : ✪

1. Le polynôme P est de degré 4 et vérifie $P(1) = P(2) = P'(2) = 0$, $P(0) = 4$ et $P(3) = 1$. Qui est-il ?
2. Même question avec le polynôme Q de degré 2024, qui admet -3 pour racine d'ordre de multiplicité 796, 3 pour racine d'ordre de multiplicité 1227, 1 pour racine simple et dont le coefficient constant est 6^{2023}.

Exercice 12 : ✪ Soient P et Q deux polynômes réels distincts. Montrer que :

$$(\exists A \in \mathbb{R}, \forall t \geq A, P(t) < Q(t)) \qquad \text{ou} \qquad (\exists A \in \mathbb{R}, \forall t \geq A, Q(t) < P(t))$$

Exercice 13 : ✪✪ Soient $P \in \mathbb{C}[X]$ et $n \in \mathbb{N}^*$. Montrer que si $P(X^n)$ est divisible par $X-1$ alors il l'est aussi par X^n-1.

Exercice 14 : ✪✪ Soient p et q deux entiers supérieurs ou égaux à 2 premiers entre eux. Montrer que $(X^p-1)(X^q-1)$ divise $(X-1)(X^{pq}-1)$.

Exercice 15 : ✪✪ Montrer qu'il n'existe pas de polynôme $P \in \mathbb{R}[X]$ tel que, pour tout $k \in \mathbb{N}^*$:

- $P(k) = 1/k$
- $P(k) = \sqrt{k^2+1}$
- $P(k) = 2^k$

Exercice 16 : ✪✪ Montrer de deux façons différentes qu'un polynôme réel de degré impair admet au moins une racine (réelle).

Exercice 17 : ✪✪ Montrer qu'il n'existe pas de polynôme $P \in \mathbb{C}[X]$ tel que pour tout $z \in \mathbb{C}, P(z) = \overline{z}$.

Exercice 18 : ✪✪

1. Montrer qu'un polynôme $P \in \mathbb{C}[X]$ non constant est surjectif.
2. On cherche à présent tous les polynômes injectifs. Soit $P \in \mathbb{C}[X]$ injectif.
   (a) P peut-il être constant ?
   (b) Montrer que P a une unique racine complexe (éventuellement de multiplicité supérieure à 1) qu'on notera α. En déduire une expression de P sous forme factorisée.
   (c) Montrer que si $\deg(P) \geq 2$, le coefficient dominant de P admet au moins deux antécédents.
   (d) En déduire tous les polynômes injectifs.

Exercice 19 - Un classique : ✪✪ Soit $P \in \mathbb{R}[X]$ scindé.

1. On suppose que les racines de P sont simples. Montrer que P' est aussi scindé à racines simples.
2. ✪✪✪ Montrer que P' est scindé dans le cas général.

3. On vient donc de montrer que le polynôme dérivé d'un polynôme scindé (sur $\mathbb{R}$) est lui aussi scindé. Ce résultat est un grand classique. Voici trois exercices qui l'utilisent.
   (a) Soit $P \in \mathbb{R}[X]$ scindé. Montrer que si α est une racine multiple de P' alors α est racine de P.
   (b) Soit $\lambda \in \mathbb{R}^*$ et soit $P \in \mathbb{R}[X]$ scindé. Montrer que les racines (complexes) de $P^2 + \lambda^2$ sont simples.
   (c) Montrer que X^3+1 n'est pas scindé à racines simples sur $\mathbb{R}$. S'inspirer de cet exemple pour montrer qu'un polynôme réel scindé à racines simples ne peut pas avoir deux coefficients consécutifs nuls.

Exercice 20 : ✪✪

1. (a) Soit f dérivable n fois sur $\mathbb{R}$. On suppose qu'il existe $a_1 < a_2 < \cdots < a_{n+1}$ tels que $f(a_1) = f(a_2) = \cdots = f(a_{n+1})$. Montrer qu'il existe $\alpha \in]\, a_1\,;a_{n+1}\,[$ tel que $f^{(n)}(\alpha) = 0$.
   (b) Soit $P \in \mathbb{R}[X]$ de degré n. Montrer que l'équation $P(x) = e^x$ admet au plus $n+1$ solutions.
2. ✪✪✪✪ Soit $P \in \mathbb{R}[X]$ non constant. Montrer que l'équation $P(x) = \sin(x)$ admet un nombre fini de solutions.

Exercice 21 : ✪✪ Soit $P \in \mathbb{R}[X]$ de degré n. Montrer que le nombre de réels ε tels que $P + \varepsilon$ admette des racines multiples est inférieur ou égal à $n-1$. Illustrer par un dessin. En déduire qu'il existe $\alpha > 0$ tel que pour tout $\varepsilon \in]\, 0\,;\alpha\,[$, $P + \varepsilon$ n'admette que des racines simples.

Exercice 22 : ✪✪ Soit $P \in \mathbb{C}[X]$ tel que pour tout x appartenant à $\mathbb{R}$, $P(x)$ soit réel. Montrer que $P \in \mathbb{R}[X]$.

Exercice 23 : ✪✪✪ Soit $P \in \mathbb{C}[X]$ de degré n tel qu'il existe $a_1, \ldots, a_{n+1}$ rationnels tels que $P(a_i) \in \mathbb{Q}$ pour tout $i \in [\![\, 1\,;\, n+1\,]\!]$. Montrer que $P \in \mathbb{Q}[X]$. On pourra utiliser les polynômes de Lagrange.

Exercice 24 - Parce qu'il ne faut quand même pas rêver : ✪ Donner un polynôme $P \notin \mathbb{Z}[X]$ tel que $P(n) \in \mathbb{Z}$ pour tout $n \in \mathbb{Z}$.

Remarque : Dans l'exercice 55 du chapitre 30, nous donnerons tous les polynômes $P \in \mathbb{C}[X]$ vérifiant : $\forall n \in \mathbb{Z}, P(n) \in \mathbb{Z}$.

Exercice 25 : ✪✪

1. Donner tous les polynômes $P \in \mathbb{R}[X]$ vérifiant
$$\forall k \in \mathbb{N}, \quad \int_k^{k+1} P(t)\,\mathrm{d}t = k$$
2. Donner tous les polynômes $P \in \mathbb{R}[X]$ vérifiant
$$\forall k \in \mathbb{N}^*, \quad \int_k^{k+1} P(t)\,\mathrm{d}t = \frac{1}{k}$$

Exercice 26 : ✪✪ On se donne dans cet exercice un polynôme $P \in \mathbb{Z}[X]$.

1. Montrer que si $P(0)$ et $P(1)$ sont impairs, alors P n'a aucune racine dans $\mathbb{Z}$.
2. On suppose que P est unitaire et que P admet une racine $r \in \mathbb{Q}$. Montrer que $r \in \mathbb{Z}$.
3. Généraliser le résultat précédent au cas où P n'est pas unitaire.
4. Montrer que $P = X^{2023} + X + 1$ a une unique racine réelle, et que cette racine est irrationnelle.
5. Montrer que si $k \geq 2$ et si $d \in \mathbb{N}$ n'est pas la puissance k-ième d'un entier, alors $\sqrt[k]{d}$ est un irrationnel.

Exercice 27 : ✪✪ Trouver tous les polynômes $P \in \mathbb{C}[X]$ tels que :
$$\forall (x,y) \in \mathbb{C}^2, P(xy) = P(x) \times P(y)$$

Exercice 28 : ✪✪ Montrer que le nombre de racines distinctes de $P \in \mathbb{C}[X]$ (non nul) est $\deg(P) - \deg(P \wedge P')$.

Exercice 29 : ✪✪ Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire à coefficients complexes. Soit $z \in \mathbb{C}$ une racine de P. Montrer que
$$|z| \leq \max\left(1, \sum_{i=0}^{n-1} |a_i|\right)$$

Exercice 30 - Un cas particulier du théorème d'Eneström-Kakeya : ✪✪ Soit

$$P = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$$

et on suppose que $a_0 \geq a_1 \geq \cdots \geq a_n > 0$. Montrer que les racines complexes de P sont de module supérieur ou égal à 1 (on pourra s'intéresser à $(1-X) \times P$).

Exercice 31 : ✪✪ Soient $(a_1, a_2, a_3, b_1, b_2, b_3) \in \mathbb{K}^6$ distincts. On se donne le tableau suivant :

$a_1 + b_1$	$a_1 + b_2$	$a_1 + b_3$
$a_2 + b_1$	$a_2 + b_2$	$a_2 + b_3$
$a_3 + b_1$	$a_3 + b_2$	$a_3 + b_3$

On suppose que le produit des termes de chaque colonne vaut 2024. Donner le produit des termes de chaque ligne. On s'intéressera au polynôme $(X + a_1)(X + a_2)(X + a_3)$.

Exercice 32 : ✪✪✪ Soit $P \in \mathbb{K}[X]$. Montrer que $P - X$ divise $P \circ P - X$ (on commencera par montrer qu'il divise $P \circ P - P$).

Exercice 33 - Polynômes « exponentiels » : ✪✪✪

Pour tout $n \in \mathbb{N}$, on définit le polynôme $P_n \in \mathbb{R}[X]$ par $P_n = \sum_{k=0}^{n} \frac{X^k}{k!}$.

1. Montrer que les racines complexes de P_n sont toutes simples.
2. Montrer que pour tout $n \in \mathbb{N}$, P_{2n} n'a pas de racine réelle, que P_{2n+1} a une unique racine réelle qu'on note a_n, et que $a_n \neq 0$.
3. Donner le tableau de variation de P_{2n+1} et de P_{2n+3}, ainsi que leurs tableaux de signes.
4. Montrer que $a_n < 0$ pour tout n.
5. Soit $n \geq 0$.
   (a) Soit $p \leq n$. Donner le signe de
   $$\frac{(2n+3)^{2p}}{(2p)!} - \frac{(2n+3)^{2p+1}}{(2p+1)!}$$
   (b) Donner le signe de $P_{2n+1}(-2n-3)$. Comparer a_n et $-2n-3$.
   (c) En calculant le signe de $P_{2n+3}(a_n)$, montrer que la suite (a_n) est décroissante.
6. On admet le résultat suivant (qu'on montrera au chapitre 23) :
   $$\forall x \in \mathbb{R} \qquad \sum_{k=0}^{n} \frac{x^k}{k!} \xrightarrow[n \to +\infty]{} e^x$$
   Montrer que $a_n \xrightarrow[n \to +\infty]{} -\infty$.

Exercice 34 - Polynômes stabilisant le cercle unité : ✪✪✪ On note $E = \{P \in \mathbb{C}[X] \mid P(\mathbb{U}) \subset \mathbb{U}\}$ l'ensemble des polynômes complexes stabilisant le cercle unité.

1. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ avec $a_n \neq 0$. On pose $\widehat{P} = \sum_{k=0}^{n} \overline{a_{n-k}} X^k$.
   (a) Dans le cas particulier où $P = (3+i)X^4 + 2X^3 + (1+i)X^2 - 2024$, expliciter $\widehat{P}$.
   (b) On revient au cas général. Montrer que pour tout $z \in \mathbb{U}, \widehat{P}(z) = z^n \overline{P(z)}$.
2. Si $P \in E$, que vaut $P\widehat{P}$? En déduire le degré de $\widehat{P}$.
3. Déterminer l'ensemble E.

Exercice 35 : ✪✪✪ Soient P et Q deux polynômes de degré $n \geq 1$ de $\mathbb{C}[X]$ tels que P et Q aient le même ensemble de racines, ainsi que $P - 1$ et $Q - 1$. Le but de l'exercice est de prouver que $P = Q$. On pose pour cela $R = P - Q$.

1. Justifier que $P \wedge P'$ et $(P-1) \wedge P'$ sont premiers entre eux.
2. À l'aide de l'exercice 28, prouver que R admet au moins $n+1$ racines distinctes et conclure.

Exercice 36 : ✪✪✪ Soit $P \in \mathbb{C}[X]$ non constant et soit E un sous-ensemble fini de $\mathbb{C}$. Montrer que :

$$\operatorname{card}(P^{-1}(E)) \geq (\operatorname{card}(E) - 1)\deg(P) + 1$$

On pourra utiliser l'exercice 28.

19.2 Factorisation

Exercice 37 - Une factorisation : ✪ Soit $P = (X^2-1)^2 - 3X(X^2+1)$.

1. Montrer que j est racine de P. Donner une autre racine complexe de P.
2. En déduire toutes les racines de P et sa factorisation sur $\mathbb{R}[X]$.

Exercice 38 : ✪ Soit $n \geq 1$. Factoriser le polynôme

$$P_n = 1 - X + \frac{X(X-1)}{2!} + \cdots + \frac{(-1)^n X(X-1)\cdots(X-n+1)}{n!}$$

Exercice 39 : ✪ Soit $P = (X+1)^7 - X^7 - 1$. Montrer que j est racine de P et factoriser P sur $\mathbb{R}$.

Exercice 40 : ✪✪ Factoriser sur $\mathbb{R}$ et sur $\mathbb{C}$ les polynômes $X^8 + X^4 + 1$ et $X^{12} + 1$.

Exercice 41 : ✪✪ Soit $n \in \mathbb{N}^*$.

1. Décomposer $P_n = \sum_{k=0}^{n} X^k$ en produit de facteurs irréductibles dans $\mathbb{C}[X]$.
2. En déduire la valeur de $\prod_{k=1}^{n} \sin\left(\frac{k\pi}{n+1}\right)$.

Exercice 42 : ✪✪ Soit $n \geq 1$. Calculer le produit

$$P = \prod_{k=1}^{n-1} \left(1 - e^{2ik\pi/n}\right)$$

Exercice 43 : ✪✪ Soit p un entier supérieur ou égal à 1.

1. Donner la factorisation du polynôme $X^{2p} - 1$ dans $\mathbb{R}[X]$ (indice : c'est dans le cours).
2. Donner la factorisation sur $\mathbb{R}$ de $1 + X + \cdots + X^{2p-1}$. En déduire que

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

Exercice 44 : ✪✪ Soit $P \in \mathbb{R}[X]$ unitaire de degré $n \geq 1$. Montrer que P est scindé sur $\mathbb{R}$ si et seulement si $|P(z)| \geq |\mathrm{Im}(z)|^n$ pour tout $z \in \mathbb{C}$.

Exercice 45 : ✪✪

1. Soit P un polynôme unitaire de degré n tel que pour tout k appartenant à $[\![1\,;\, n+1]\!]$ on ait $P(k) = \frac{1}{k^2}$. Donner $P(n+2)$. On s'intéressera au polynôme $Q = X^2P - 1$.
2. **Remake :** Soit P de degré n tel que pour tout $k \in [\![0\,;\, n]\!], P(k) = \frac{k}{k+1}$. Donner $P(n+1)$.

Exercice 46 : ✪✪ Factoriser sur $\mathbb{C}$ le polynôme $8X^3 - 12X^2 - 2X + 3$ sachant que ses racines sont en progression arithmétique.

Exercice 47 : ✪✪✪ On se place dans cet exercice sur $\mathbb{R}[X]$.

1. Montrer que si A et B sont deux polynômes qui sont sommes de deux carrés (de polynômes), il en est de même pour AB.
2. Montrer qu'un polynôme P est somme de deux carrés si et seulement s'il est positif, c'est-à-dire si et seulement si $P(x) \geq 0$ pour tout $x \in \mathbb{R}$.
3. **Remake :** Montrer qu'un polynôme P est positif sur $\mathbb{R}_+$ si et seulement s'il existe $(C, D) \in \mathbb{R}[X]^2$ tel que $P = C^2 + XD^2$.

Exercice 48 : ✪✪✪ Soient $a_1, \ldots, a_n$ deux entiers deux à deux distincts. Montrer que

$$P = \prod_{k=1}^{n} (X - a_k)^2 + 1$$

est irréductible sur $\mathbb{Z}$ (i.e. si $P = AB$ avec A et B dans $\mathbb{Z}[X]$ alors A ou B est constant égal à ± 1).

19.3 Divers

Exercice 49 : ✪ Soit $n \geq 1$. Soit P un polynôme de degré n. Déterminer le degré des polynômes $Q = X^2P'$ et $R = XP' + P$.

Exercice 50 : ✪ Déterminer tous les polynômes P tels que $P(2) = 6$, $P'(2) = 1$, $P''(2) = 4$ et $P^{(n)}(2) = 0$ pour tout $n \geq 3$.

Exercice 51 : ✪ Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Montrer que

$$Q = \sum_{k=0}^{n} (-1)^k \times \frac{P^{(k)}(X) \times X^{k+1}}{(k+1)!}$$

est l'unique polynôme s'annulant en 0 dont la dérivée vaut P.

Exercice 52 - Polynômes à coefficients alternés : ✪ On dit qu'un polynôme $P \in \mathbb{R}[X]$ est à coefficients alternés s'il peut s'écrire sous la forme

$$P = \sum_{n=0}^{+\infty} (-1)^n a_n X^n$$

où $(a_n)_{n\in\mathbb{N}}$ est une suite presque nulle de réels positifs. Montrer que le produit de deux polynômes à coefficients alternés est encore à coefficients alternés.

Exercice 53 : ✪ Soit $n \in \mathbb{N}^*$. Donner le degré et le coefficient dominant de

$$P = \prod_{\ell=1}^{n} \left(64X^6 + 2024X^4 + \ell\right)^{\ell^2}$$

Exercice 54 - Un peu de cryptographie : ✪

Pierre le fermier, Jules le métalleux et Jean le musicien décident d'acheter un coffre-fort pour entreposer l'argent du loyer. Comme ils ne se font pas confiance, il doit être impossible à l'un d'entre eux d'ouvrir le coffre seul, ou à deux d'entre eux d'ouvrir le coffre sans le troisième. Par contre, ils doivent quand même pouvoir l'ouvrir une fois par mois pour sortir l'argent du loyer, ou n'importe quand, par exemple pour payer l'électricité, à la condition qu'ils soient tous les trois réunis. Bien sûr, quand ils l'ont ouvert, ils connaissent le code, donc celui-ci doit changer à chaque ouverture. Ils demandent conseil à Antoine le professeur, qui est honnête et en qui tous les trois ont confiance. Dans sa grande sagesse, il leur propose le protocole suivant :

- Antoine le professeur choisit un polynôme $P \in \mathbb{R}_2[X]$, qu'il garde secret.
- Il choisit trois réels distincts a_1, a_2 et a_3, et calcule $b_1 = P(a_1), b_2 = P(a_2)$ et $b_3 = P(a_3)$. Tout cela est gardé secret.
- Il donne à Pierre le fermier le couple (a_1, b_1), à Jules le métalleux le couple (a_2, b_2) et à Jean le musicien le couple (a_3, b_3). Chacun des colocataires connaît son couple, mais pas celui des autres.
- Les colocataires savent que le code du coffre est la valeur en 42 du polynôme d'interpolation de Lagrange passant par les trois points $(a_1, b_1), (a_2, b_2)$ et (a_3, b_3). Ainsi, s'ils veulent ouvrir le coffre, il leur suffit de mettre leurs couples (qu'on appelle leurs clefs privées) en commun, de calculer le polynôme en question (n'oublions pas qu'ils ont fait une classe prépa !) et de trouver le code.
- Une fois le coffre ouvert, ils rappellent Antoine le professeur pour qu'il choisisse un nouveau polynôme et leur donne de nouvelles clefs (c'est-à-dire de nouveaux couples de réels).

1. On rappelle que le polynôme d'interpolation de Lagrange L passant par les trois points est l'unique polynôme de degré ≤ 2 passant par ces trois points (il n'est pas demandé de le montrer). Montrer que $L = P$.
2. La clef de Pierre est $(1, 5)$, celle de Jules est $(2, 3)$ et celle de Jean est $(-1, 36)$. Donner le code du coffre.
3. Pierre et Jules veulent voler l'argent de Jean : Pierre pour s'acheter une trayeuse, et Jules pour aller au Hellfest. Ils mettent donc leurs clefs en commun. Puisqu'ils ne connaissent pas celle de Jean, ils vont essayer de deviner le code. Peut-être qu'après tout ils peuvent déterminer P rien qu'avec leurs deux clefs, ou au moins réduire les possibilités.
   (a) Soit $\alpha \in \mathbb{R}$. Exhiber un polynôme $Q \in \mathbb{R}_2[X]$ vérifiant $Q(1) = 5, Q(2) = 3$ et $Q(42) = \alpha$.
   (b) Pierre et Jules peuvent-ils ouvrir le coffre sans Jean ?

Exercice 55 : ✪✪ Soient P et Q deux polynômes réels distincts de degré $n \geq 0$. Montrer que $\deg\left(P^3 - Q^3\right) \geq 2n$. Le résultat est-il encore valable sur $\mathbb{C}$?

Exercice 56 : ✪✪ Montrer que pour tout $P \in \mathbb{K}[X]$,

$$P(X+1) = \sum_{n=1}^{+\infty} \frac{P^{(n)}(X)}{n!}$$

cette somme étant en fait finie.

Exercice 57 : ✪✪ Résoudre une équation dont l'inconnue est un polynôme se fait toujours par analyse/synthèse. De façon générale, on s'intéresse à une caractéristique du polynôme P, ce qui réduit considérablement le choix, et ensuite on passe à la synthèse. Il y a en gros trois façons de faire, chacune étudiée dans un exemple ci-dessous.

1. Trouver tous les polynômes P vérifiant $P(2X) = P'(X)P''(X)$ (s'intéresser au degré).
2. Trouver tous les polynômes P vérifiant $(X+4)P(X) = XP(X+1)$ (s'intéresser aux racines de P).
3. Trouver tous les polynômes P vérifiant $(X^2+1)P'' = 6P$ (s'intéresser au coefficient dominant).
4. Trouver tous les polynômes P vérifiant $P\left(X^2\right) = (X^2+1)P(X)$ (débrouillez-vous !).

Exercice 58 - Polynômes de Legendre : ✪✪✪ Pour tout $n \in \mathbb{N}$, on pose $P_n = \left(X^2-1\right)^n$ et

$$L_n = \frac{1}{2^n \times n!} \times {P_n}^{(n)}$$

1. Déterminer le degré et le coefficient dominant de L_n.
2. Calculer $L_n(1)$ et $L_n(-1)$.

Remarque : Les polynômes de Legendre sont un cas particulier de polynômes orthogonaux. Nous en reparlerons dans l'exercice 44 du chapitre 34.

Exercice 59 - Lemme de Gauß : ✪✪✪ Si $P \in \mathbb{Z}[X]$ est non nul, on appelle contenu de P, noté $c(P)$, le PGCD des coefficients de P, et un polynôme est dit primitif lorsque son contenu vaut 1.

1. On se donne dans cette question uniquement deux polynômes primitifs $P = a_n X^n + \cdots + a_0$ et $Q = b_m X^m + \cdots + b_0$. Soit p premier.
   (a) Justifier l'existence de $i_0 = \min\{i \in \mathbb{N} \,|\, p \nmid a_i\}$ et $j_0 = \min\{j \in \mathbb{N} \,|\, p \nmid b_j\}$.
   (b) À l'aide du coefficient d'indice $i_0 + j_0$ de PQ, montrer que PQ est primitif.
2. Montrer que pour tous P et Q non nuls (pas forcément primitifs), $c(PQ) = c(P)c(Q)$.

Exercice 60 : ✪✪✪✪ Donner tous les polynômes $P \in \mathbb{Q}[X]$ tels que $P(\mathbb{R}\backslash\mathbb{Q}) \subset \mathbb{R}\backslash\mathbb{Q}$. On pourra utiliser l'exercice 26.

19.4 Arithmétique des polynômes

Exercice 61 : ✪ Effectuer à chaque fois la division euclidienne de A par B.

1. $A = 6X^6 - 3X^5 - 5X^2 + 10X - 6, B = 4X^3 + X - 1$.
2. $A = 7X^7 - 5X^5 + 3X^3 - X, B = 6X^6 - 4X^4 + 2X^2$.

Exercice 62 : ✪ Calculer, pour $n \geq 2$, les restes des divisions euclidiennes de $P = (X-3)^{2n} + (X-2)^n - 2$ par, respectivement, $(X-3)(X-2)$ et $(X-2)^2$. Pour la deuxième, on pourra dériver l'expression obtenue en écrivant la division euclidienne. Recommencer en donnant le reste de la division euclidienne de $(X^n+1)^2$ par $(X+1)^2$, puis en donnant le reste de la division euclidienne de X^n par $(X-1)^3$.

Exercice 63 : ✪ Montrer que $X^5 - 1$ et $X^2 + X + 1$ sont premiers entre eux. Déterminer une relation de Bézout entre ces polynômes.

Exercice 64 : ✪✪ Soit $(n,p) \in (\mathbb{N}^*)^2$. S'inspirer de l'exercice 59 du chapitre 6 pour prouver que $(X^n-1) \wedge (X^p-1) = X^{n \wedge p} - 1$.

Exercice 65 : ✪✪ Trouver les réels a tels que $X^2 - aX + 1$ divise $X^4 - X + a$ dans $\mathbb{R}[X]$.

Exercice 66 - Introduction au résultant : ✪✪ Soient n, m deux entiers naturels non nuls et P et Q deux éléments de $\mathbb{K}[X]$ de degrés respectifs n et m. Montrer que P et Q ne sont pas premiers entre eux si et seulement s'il existe deux polynômes A et B non nuls de $\mathbb{K}[X]$ de degrés $\deg A < m$ et $\deg B < n$ tels que $AP = BQ$.

Exercice 67 - Pour tous les âges : ✪✪

Pierre le fermier et Jules le métalleux discutent :

« Devine l'âge de mon fils sachant qu'il est racine d'un polynôme P à coefficients entiers relatifs.
- Je crois qu'il a 7 ans.
- Ah non, $P(7) = 77$, il est plus vieux.
- Dans ce cas il a le même âge que mon chien.
- Non plus ! Si y est l'âge de ton chien, $P(y) = 85$. Il est encore plus vieux.
- C'est bon, j'ai trouvé. »

Le but de l'exercice est de faire comme Jules le métalleux et de trouver l'âge du fils... ainsi que l'âge du chien ! On reprend les notations du dialogue et on appelle $\alpha \in \mathbb{N}$ l'âge du fils.

1. Montrer que le théorème de la division euclidienne est encore valable sur $\mathbb{Z}$ si B est unitaire.
2. Quel âge a le fils ? et le chien ?

Exercice 68 : ✪✪✪ Soit $n \geq 2$ un entier. Déterminer les polynômes de degré n, divisibles par $X + 1$ et dont les restes dans la division euclidienne par $X + 2, \ldots, X + n + 1$ sont égaux.

Exercice 69 : ✪✪✪ Soient P et Q appartenant à $\mathbb{Z}[X]$ n'ayant aucune racine complexe commune.

1. Montrer qu'il existe A et B appartenant à $\mathbb{Z}[X]$ et $d \in \mathbb{N}^*$ tels que $AP + BQ = d$.
2. Montrer que pour tout $n \in \mathbb{N}$, $P(n + d) - P(n)$ est divisible par d.
3. En déduire que la suite de terme général $u_n = P(n) \wedge Q(n)$ est d-périodique.

19.5 Relations coefficients-racines

Exercice 70 : ✪ Donner la somme et le produit des racines complexes (comptées avec multiplicité) de $P = 2X^5 + 3X^4 + 2X^3 + X^2 + X + 2024$.

Exercice 71 : ✪✪ Soit $P \in \mathbb{C}[X]$ de degré $n \geq 2$. On note

$$\mu(P) = \frac{1}{n} \sum_{P(z)=0} z$$

la moyenne arithmétique des racines de P comptées avec multiplicité. Montrer que $\mu(P) = \mu(P')$ et donner leur valeur commune.

Exercice 72 : ✪✪ Soit $n \geq 1$. Montrer qu'il n'y a qu'un nombre fini de polynômes unitaires de degré n à coefficients dans $\mathbb{Z}$ dont toutes les racines complexes ont un module inférieur ou égal à 1.

Exercice 73 : ✪✪ Résoudre le système suivant :

$$\begin{cases} x + y + z = 1 \\ x^2 + y^2 + z^2 = 9 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1 \end{cases}$$

Exercice 74 : ✪✪ Soit $(p, q) \in \mathbb{C}^2$. Soit $P = X^3 + pX + q$. Soient x, y, z les trois racines complexes de P comptées avec multiplicité.

1. Montrer que $P'(x)P'(y)P'(z) = 4p^3 + 27q^2$.
2. En déduire une CNS pour que P admette une racine multiple.

Exercice 75 : ✪✪ Soit $P \neq 0$ et soit $n = \deg(P)$. Montrer que les sommes des racines de $P, P', \ldots, P^{(n-1)}$ forment une progression arithmétique.

Exercice 76 : ✪✪✪ Soit $n \geq 1$ et soit $f : \mathbb{C}^n \to \mathbb{C}^n$ qui à $(z_1, \ldots, z_n)$ associe $(\sigma_1, \ldots, \sigma_n)$ où σ_k désigne la k-ième fonction symétrique élémentaire des z_i.

1. L'application f est-elle surjective ?
2. Montrer que f n'est pas injective.

3. Montrer cependant que si $(z_1, \dots, z_n)$ et $(a_1, \dots, a_n)$ sont deux éléments de $\mathbb{C}^n$ qu'on ne peut pas déduire l'un de l'autre par permutation des coordonnées, alors $f(z_1, \dots, z_n) \neq f(a_1, \dots, a_n)$.

Exercice 77 : ✪✪✪✪ Montrer que l'ensemble des réels x tels que $\sum_{k=1}^{100} \frac{k}{x-k} \geq 1$ est une réunion finie d'intervalles. Calculer la somme de leurs longueurs.

19.6 Quantités polynomiales en quelque-chose

Exercice 78 : ✪

1. Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique $P_n \in \mathbb{N}[X]$ (dont la définition est évidente) tel que $\tan^{(n)} = P_n(\tan)$. En déduire que, pour tout $n \in \mathbb{N}$ et tout $x \in \left[0\,;\frac{\pi}{2}\right[$, $\tan^{(n)}(x) \geq 0$.
2. **Remake :** Soit $f : x \mapsto e^{e^x}$. Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique $P_n \in \mathbb{R}[X]$ tel que, pour tout $x \in \mathbb{R}$, $f^{(n)}(x) = P_n\left(e^x\right) \times e^{e^x}$.

Exercice 79 : ✪✪

1. Soit $n \in \mathbb{N}$ et soit $x \neq 0$. Développer $\left(x^n + \frac{1}{x^n}\right) \times \left(x + \frac{1}{x}\right)$.
2. Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique polynôme P_n tel que, pour tout $x \neq 0$, $P_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$.

Exercice 80 - Polynômes de Tchebychev de seconde espèce : ✪✪✪ Soit $n \geq 1$. S'inspirer du cours pour montrer l'existence d'un unique polynôme Q_n vérifiant, pour tout $\theta \in \mathbb{R}$, $\sin(\theta)Q_n(\cos(\theta)) = \sin((n+1)\theta)$.

19.7 Polynômes à coefficients dans un corps quelconque (HP)

Exercice 81 : ✪ On dit qu'un corps $\mathbb{K}$ est algébriquement clos si tout polynôme non constant à coefficients dans $\mathbb{K}$ admet une racine dans $\mathbb{K}$. Montrer qu'un corps algébriquement clos est infini. Réciproque ?

Exercice 82 : ✪✪ Soit $\mathbb{K}$ un corps fini et soit $f : \mathbb{K} \to \mathbb{K}$. Montrer que f est polynomiale i.e. qu'il existe $P \in \mathbb{K}[X]$ tel que pour tout $x \in \mathbb{K}$, $f(x) = P(x)$.

Exercice 83 - Théorème de Wilson (le retour) : ✪✪✪ Cet exercice fait appel au théorème de Lagrange et à la notion d'ordre dans un groupe (cf. chapitre 18). Soit p un nombre premier.

1. Sur $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, montrer que
$$X^{p-1} - 1 = \prod_{k=1}^{p-1}(X - k)$$
2. En déduire que $(p-1)! \equiv -1[p]$.

Exercice 84 : ✪✪✪ Cet exercice fait appel au théorème de Lagrange et à la notion d'ordre dans un groupe (cf. chapitre 18). Soit p un nombre premier et soit $x \in \mathbb{Z}/p\mathbb{Z}$. Montrer que $x \neq 0$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.

Chapitre 20

Fractions rationnelles

« Le djembé est à la musique ce que le couteau est à la purée. »

Les Fatals Picards, Djembé man

Si rien n'est précisé, les fractions rationnelles sont supposées à coefficients dans $\mathbb{C}$.

Exercice 1 : ✪ Décomposer en éléments simples dans $\mathbb{C}(X)$ les fractions suivantes :

1. $\dfrac{X^4+1}{X^4-1}$ 2. $\dfrac{X^2+1}{(X-1)(X-2)(X-3)}$ 3. $\dfrac{X^2+1}{X^2(X-1)^2}$ 4. $\dfrac{X^{16}+1}{X^4+1}$

Exercice 2 : ✪ Donner la limite de la suite de terme général $u_n = \displaystyle\sum_{k=1}^{n} \frac{1}{1+2+\cdots+k}$.

Exercice 3 : ✪ Montrer qu'il n'existe pas de fraction rationnelle F telle que $F^2 = X$.

Exercice 4 : ✪ Quelle est la partie entière de $\dfrac{X^4-2X^3+X+1}{(X-1)(X-2)}$?

Exercice 5 : ✪ Soient F et G deux fractions rationnelles qui coïncident en une infinité de points (pour les grincheux : telles que les fonctions rationnelles associées coïncident en une infinité de points). Montrer que $F = G$.

Exercice 6 : ✪ Soit $n \geq 1$. Décomposer en éléments simples sur $\mathbb{C}$ les fractions rationnelles $\dfrac{X}{X^n-1}$ et $\dfrac{X^{n-1}}{X^n-1}$.

Exercice 7 : ✪ Soit $A = \{R \in \mathbb{C}(X) \mid \deg(R) \leq 0\}$.

1. Montrer que A est un anneau.
2. L'ensemble $\left\{ \dfrac{1}{P} \;\middle|\; P \in \mathbb{K}[X]^* \right\} \cup \{0\}$ est-il un sous-anneau de A ?

Exercice 8 : ✪✪ Décomposer en éléments simples sur $\mathbb{C}$ la fraction rationnelle $F = \dfrac{1}{(X^3-1)^2}$. On pourra comparer $F(X)$ et $F(jX)$.

Exercice 9 : ✪ Soit $P \in \mathbb{C}[X]$ non nul. Donner une CNS pour que P' divise P.

Exercice 10 : ✪✪ On se place dans cet exercice sur $\mathbb{R}[X]$. On suppose que P est scindé à racines simples. Soit $\alpha \in \mathbb{R}$. Enfin, on pose $Q_\alpha = P + \alpha P'$.

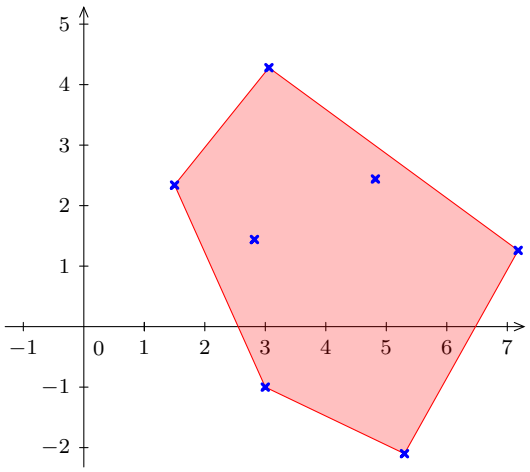
1. Donner les variations de Q_α/P (pour les grincheux : de la fonction rationnelle associée).
2. En déduire que Q_α est scindé à racines simples.

Exercice 11 : ✪✪ On se place dans cet exercice sur $\mathbb{R}(X)$. Soit $n \geq 1$. Posons $G = \dfrac{X^n}{(X+1)^n}$.

1. Donner la décomposition en éléments simples de $G(X-1)$. En déduire celle de G.
2. Donner la décomposition en éléments simples de $\dfrac{X^{2n}}{(X^2+1)^n}$.

Exercice 12 - Théorème de Gauß-Lucas : ✪✪ Soit $P \in \mathbb{C}[X]$ à racines simples. Soit $\alpha \in \mathbb{C}$ une racine de P'. Montrer que α peut s'écrire comme une combinaison linéaire à coefficients positifs (donc réels) de somme 1 des racines de P. On pourra utiliser le fait que $\overline{0} = 0$...

Interprétation géométrique : Les racines de P' sont dans l'enveloppe convexe des racines de P, où l'enveloppe convexe d'une famille de points est le plus petit convexe qui les contient. De façon imagée, c'est le polygone que formera un élastique qui contiendra tous les points (cf. cours de l'année prochaine). Par exemple, sur le dessin ci-dessous, si les racines de P sont les croix, alors les racines de P' sont dans la zone coloriée :



Exercice 13 : ✪ Soit $P \in \mathbb{C}[X]$ de degré $n \geq 1$. On suppose que P admet n racines simples notées $z_1, \ldots, z_n$.

1. Montrer que si les z_k sont tous non nuls, $\displaystyle\sum_{k=1}^{n} \frac{1}{z_k P'(z_k)} = \frac{-1}{P(0)}$.
2. ✪✪✪ Donner la valeur de $\displaystyle\sum_{k=1}^{n} \frac{1}{P'(z_k)}$. On séparera les cas $n = 1$ et $n \geq 2$.

Exercice 14 : ✪✪ Soit $n \geq 1$. Soit $P \in \mathbb{R}[X]$ unitaire de degré n et soit $R = X(X-1)\ldots(X-n)$. Donner la valeur de $\displaystyle\sum_{k=0}^{n} \frac{P(k)}{R'(k)}$ et en déduire que parmi $|P(0)|, \ldots, |P(n)|$, l'un au moins est supérieur ou égal à $\dfrac{n!}{2^n}$.

Exercice 15 : ✪✪✪ Soit $n \geq 1$. Décomposer en éléments simples $1/T_n$, où T_n est le n-ième polynôme de Tchebychev.

Exercice 16 : ✪✪✪ On se donne dans cet exercice deux entiers naturels $n < m$. On note $\omega = e^{i\pi/2m}$.

1. Soit $z = x + iy \in \mathbb{C}\backslash\mathbb{R}$. Soit $x \in \mathbb{R}$. Montrer que l'intégrale $\displaystyle\int_{-x}^{x} \frac{\mathrm{d}t}{t-z}$ est bien définie puis que
$$\int_{-A}^{A} \frac{\mathrm{d}t}{t-z} \xrightarrow[A\to+\infty]{} \mathrm{sgn}(y) \times i\pi$$
où $\mathrm{sgn}(a)$ est le signe du réel a, c'est-à-dire 1 si a est strictement positif, et -1 si a est strictement négatif (on justifiera donc pourquoi y est non nulle)
2. Montrer que la décomposition en éléments simples (sur $\mathbb{C}$) de $\dfrac{X^{2n}}{1+X^{2m}}$ est :
$$\frac{X^{2n}}{1+X^{2m}} = \sum_{k=0}^{2m-1} \frac{\alpha_k}{X - \omega^{2k+1}}$$
où, pour tout $k \in [\![0\,;\, 2m-1]\!]$, $\alpha_k = \dfrac{-\omega^{(2k+1)(2n+1)}}{2m}$.
3. Montrer que $\displaystyle\sum_{k=m}^{2m-1} \alpha_k = -\sum_{k=0}^{m-1} \alpha_k$.
4. Donner le signe de $\mathrm{Im}\left(\omega^{2k+1}\right)$ selon la valeur de $k \in [\![0\,;\, 2m-1]\!]$.
5. Montrer que
$$\int_{-x}^{x} \frac{t^{2n}}{1+t^{2m}}\,\mathrm{d}t \xrightarrow[x\to+\infty]{} \frac{\pi}{m \sin\left(\dfrac{2n+1}{2m}\pi\right)}$$
On pourra poser $\beta = \omega^{2n+1}$ pour simplifier les calculs.

Chapitre 21

The Matrix has you...

« There's a difference between knowing the path and walking the path. »

Matrix

Comme dans le cours, si rien n'est précisé, $\mathbb{K}$ est un corps, $n, p, \ldots$ sont des entiers naturels supérieurs ou égaux à 1 et les matrices considérées appartiennent à $\mathscr{M}_n(\mathbb{K})$.

Vrai ou Faux ?

1. L'ensemble des matrices inversibles est stable par somme.
2. L'ensemble des matrices non inversibles est stable par somme.
3. L'ensemble des matrices de la forme $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$, pour $x \in \mathbb{K}$, est un sous-groupe de $\mathscr{M}_n(\mathbb{K})$.
4. L'ensemble des matrices de la forme $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$, pour $x \in \mathbb{K}$, est un sous-anneau de $\mathscr{M}_n(\mathbb{K})$.
5. L'ensemble des matrices triangulaires supérieures avec des 1 sur la diagonale est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$.
6. $\mathscr{M}_n(\mathbb{N})$ est stable par produit.
7. Si $M \in \mathscr{M}_n(\mathbb{Z})$ est inversible alors $M^{-1} \in \mathscr{M}_n(\mathbb{Z})$.
8. $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 5 & 6 \\ 0 & 0 & 7 & 8 \\ 0 & 0 & 0 & 9 \end{pmatrix}$ est inversible.
9. Si $A^2 = 0$ alors $A = 0$.
10. Si $A^2 = 0$ alors A n'est pas inversible.
11. Si tous les coefficients diagonaux de M sont non nuls alors M est inversible.
12. Si tous les coefficients de M sont non nuls alors M est inversible.
13. Si M est inversible alors $M \times M^\top$ est inversible et symétrique.
14. Une matrice et sa transposée commutent.
15. Si le système $AX = B$ admet des solutions alors A est inversible.
16. Si un système linéaire n'a pas de solution, alors le système homogène associé n'a pas de solution.
17. Si un système linéaire n'a pas de solution, alors le système homogène associé a une unique solution.
18. Si un système linéaire a une unique solution, alors le système homogène associé a une unique solution.

Exercice 1 : ✪ Calculer les produits suivants :

1. $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
3. $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$
4. $\begin{pmatrix} 0 & 4 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix}$
5. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix}$
6. $\begin{pmatrix} 3 & 6 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -2 & 2 \\ 1 & -1 \end{pmatrix}$
7. $\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$

Exercice 2 : ✪ Soient les matrices suivantes :

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 0 & 7 & 8 \\ 9 & 1 & 0 & 0 \\ -1 & 2 & 1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 5 & 2 \\ 2 & -1 & 1 \\ 3 & 0 & 1 \\ 4 & 1 & 0 \end{pmatrix} \qquad C = \begin{pmatrix} -1 & 2 & 0 & 1 \\ 1 & 5 & -2 & 3 \\ 4 & 1 & 0 & 8 \end{pmatrix} \qquad D = \begin{pmatrix} 1 \\ -2 \\ 3 \end{pmatrix}$$
$$E = \begin{pmatrix} 5 & 2 & -4 \end{pmatrix}$$

Parmi tous les produits possibles de ces matrices ($A^2, AB, BA, CE \dots$), dire lesquels sont bien définis et les calculer.

Exercice 3 : ✪ Donner les transposées des 5 matrices de l'exercice précédent.

Exercice 4 : ✪ On considère dans $\mathscr{M}_n(\mathbb{R})$ les matrices A et B définies par :

$$\forall (i,j) \in [\![1\,;n]\!]^2, \qquad A_{i,j} = i + j \qquad \text{et} \qquad B_{i,j} = i - j$$

Calculer le terme général des matrices $C = A - B$ et $D = AB$.

Exercice 5 : ✪ Soient A, B symétriques. Montrer que AB est symétrique si et seulement si A et B commutent.

Exercice 6 - Calcul de l'inverse grâce à un polynôme annulateur : ✪ Soit

$$A = \begin{pmatrix} -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$

Calculer $A^2 + 5A$ et en déduire que A est inversible et donner son inverse. Plus généralement, soit $A \in \mathscr{M}_n(\mathbb{K})$ telle que

$$A^{2024} + \sum_{k=0}^{2023} \lambda_k A^k = 0$$

où $(\lambda_0, \dots, \lambda_{2023})$ sont des éléments de $\mathbb{K}$. On suppose que $\lambda_0 \neq 0$. Montrer que $A \in \mathrm{GL}_n(\mathbb{K})$.

Exercice 7 : ✪ Soient A, B, C non nulles telles que $ABC = 0$. Montrer que deux au moins sont non inversibles.

Exercice 8 : ✪ Inverser les matrices suivantes :

1. $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$
2. $\begin{pmatrix} 0 & 1 & 0 \\ 2 & 3 & -2 \\ 4 & -1 & -2 \end{pmatrix}$
3. $\begin{pmatrix} 1 & 2 & -1 \\ 2 & -1 & -1 \\ -1 & 2 & 0 \end{pmatrix}$

Exercice 9 : ✪ Montrer qu'il existe deux uniques suites $(\alpha_n)_{n\geq 1}$ et $(\beta_n)_{n\geq 1}$ que l'on explicitera telles que pour tout $n \geq 1, A^n = \alpha_n A + \beta_n A^2$, où

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

Exercice 10 - Inverse d'une matrice d'ordre 2 : ✪ Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

1. Montrer que $A^2 - (a+d)A + (ad - bc)I = 0$.
2. Donner une CNS pour que A soit inversible.
3. Donner alors A^{-1}.

Exercice 11 : ✪ On suppose $n \geq 2$ et on pose

$$J = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ \vdots & & \ddots & & \vdots \\ 1 & 1 & \dots & 0 & 1 \\ 1 & 1 & \dots & 1 & 0 \end{pmatrix} \in \mathscr{M}_n(\mathbb{C})$$

Calculer J^2. En déduire que J est inversible et donner son inverse.

Exercice : 12 : ✪ Soit A la matrice de $\mathscr{M}_{2n+1}(\mathbb{R})$ dont tous les coefficients sont nuls sauf ceux en ligne et colonne n qui valent 1. Calculer A^2.

Exercice 13 - Un problème de racine carrée : ✪ On pose

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

Le but de cet exercice est de montrer qu'il n'existe pas de matrice $B \in \mathscr{M}_3(\mathbb{C})$ telle que $B^2 = A$ (alors que tous les coefficients de A sont positifs : ce n'est pas aussi simple !). On fait un raisonnement par l'absurde et on suppose donc qu'une telle matrice B existe.

1. Montrer que A et B commutent. En déduire que B est triangulaire supérieure.
2. Conclure.

Exercice 14 : ✪ Soit $(A, B) \in \mathscr{M}_n(\mathbb{K})$ tel que $AB = A + I_n$.

1. Montrer que A est inversible et déterminer son inverse.
2. En déduire que $AB = BA$.

Exercice 15 : ✪✪

1. Soit $A \in \mathscr{M}_{n,p}(\mathbb{R})$ tel que $A \times A^\top = 0$. Montrer que $A = 0$ (regarder les coefficients diagonaux du produit). Au fait, de quels 0 parle-t-on ?
2. Le résultat est-il encore valable si $A \in \mathscr{M}_{n,p}(\mathbb{C})$? Recommencer l'exercice en supposant cette fois que $A \times \left(\overline{A}\right)^\top = 0$.

Exercice 16 : ✪✪ Soit $\omega = e^{2i\pi/n}$. On pose $\Omega = \left(\omega^{(k-1)(\ell-1)}\right)_{1 \leq k,\ell \leq n} \in \mathscr{M}_n(\mathbb{C})$.

1. Calculer $\Omega \times \overline{\Omega}$.
2. En déduire que Ω est inversible et calculer son inverse.

Exercice 17 - Entraînement à l'écrit (mais pas que) : ✪✪

1. Soit $(a, b, c) \in \mathbb{R}^3$. Calculer les puissances de $A = \begin{pmatrix} \pi & a & b \\ 0 & \pi & c \\ 0 & 0 & \pi \end{pmatrix}$.
2. Calculer les puissances de $A = \begin{pmatrix} 1 & -2 & -6 \\ -3 & 2 & 9 \\ 2 & 0 & -3 \end{pmatrix} \in \mathscr{M}_3(\mathbb{K})$. On commencera par calculer A^3. A est-elle inversible ?
3. Soient $A = \begin{pmatrix} -1 & 1 \\ -6 & 4 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$.
   (a) Calculer $P^{-1}AP$. En déduire A^n pour tout n.
   (b) Expliciter les suites (u_n) et (v_n) définies par $u_0 = 1, v_0 = 3$ et pour tout n

$$\begin{cases} u_{n+1} &= & -u_n &+ & v_n \\ v_{n+1} &= & -6u_n &+ & 4v_n \end{cases}$$

4. Soit $a \in \mathbb{R}^*$. On pose

$$A = \begin{pmatrix} 0 & a & a^2 \\ 1/a & 0 & a \\ 1/a^2 & 1/a & 0 \end{pmatrix}$$

   (a) Calculer A^2.
   (b) Trouver deux vecteurs non colinéaires (en particuliers non nuls) X et Y dans $\mathbb{R}^3$ tels que $AX = -X$ et $AY = -Y$.
   (c) Trouver un vecteur non nul $Z \in \mathbb{R}^3$ tel que $AZ = 2Z$.
   (d) Soit P dont les vecteurs colonnes sont X, Y et Z dans cet ordre. Inverser P.
   (e) Calculer $D = P^{-1}AP$. En déduire que A est inversible. Calculer D^n pour tout $n \in \mathbb{N}^*$. En déduire A^n pour tout $n \in \mathbb{N}^*$.

Exercice 18 : ✪✪ Montrer que la permutation de deux lignes (ou deux colonnes) peut s'obtenir au moyen des deux autres opérations élémentaires.

Exercice 19 : ✪✪ On suppose que $n \geq 2$. Soit $A \in \mathrm{GL}_n(\mathbb{R})$.

1. Soit B la matrice obtenue en échangeant les colonnes i et j de A. Justifier que la matrice B est inversible. Comment calculer B^{-1} à partir de A^{-1} ?
2. Soit C la matrice obtenue en ajoutant deux fois la i-ème colonne à la j-ème colonne. Justifier que la matrice C est inversible. Comment calculer C^{-1} à partir de A^{-1} ?

Exercice 20 - Une autre construction de $\mathbb{C}$: ✪ On pose

$$C = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid (a,b) \in \mathbb{R}^2 \right\}$$

1. Montrer que C est un sous-anneau commutatif de $\mathscr{M}_n(\mathbb{R})$.
2. Montrer que C est un corps.
3. Montrer que l'application

$$\begin{cases} \mathbb{C} & \to & C \\ a+ib & \mapsto & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{cases}$$

est un isomorphisme de corps. On aurait donc pu construire $\mathbb{C}$ de cette manière ! Vérifier qu'il existe bien une matrice $J \in C$ telle que $J^2 = -I_2$.

Exercice 21 - Le corps des quaternions : ✪✪ Le corps des quaternions, construit par Hamilton en 1843, est un surcorps de $\mathbb{C}$ non commutatif [1]. Il admet une base $(1,i,j,k)$ avec les propriétés $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i$ et $ki = -ik = j$ (et l'ensemble $\{\pm 1; \pm i; \pm j; \pm k\}$ est alors un groupe à 8 éléments noté $\mathbb{H}_8$ [2], cf. chapitre 17). Une manière simple de construire ce corps et qui évite les vérifications fastidieuses (par exemple de l'associativité du produit) consiste à utiliser les matrices.

On considère le sous-ensemble $\mathbb{H}$ de $\mathscr{M}_2(\mathbb{C})$ constitué des matrices h de la forme $\begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix}$ avec $z_1, z_2 \in \mathbb{C}^2$: on dit que $\mathbb{H}$ est l'ensemble des quaternions. On considère les quatre éléments suivants de $\mathbb{H}$:

$$e_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad e_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad e_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

1. Montrer que $\mathbb{H}$ est un sous-anneau de $\mathscr{M}_2(\mathbb{C})$ stable par multiplication par un réel. Est-il stable par multiplication par un complexe ?
2. Montrer que tout élément de $\mathbb{H}$ est combinaison linéaire (à coefficients réels) de (e_0, e_1, e_2, e_3).
3. Dresser un tableau de tous les produits $e_i e_j$. $\mathbb{H}$ est-il commutatif ?
4. Pour $h \in \mathbb{H}$ de la forme ci-dessus on pose $\overline{h} = \begin{pmatrix} \overline{z_1} & \overline{z_2} \\ -z_2 & z_1 \end{pmatrix}$. Montrer que l'application qui à h associe $\overline{h}$ est un isomorphisme d'anneaux involutif de $\mathbb{H}$.
5. Calculer $h\overline{h}$ et en déduire que tout élément non nul de $\mathbb{H}$ est inversible dans $\mathbb{H}$. Que peut-on en déduire ?
6. Montrer que $\mathbb{H}$ contient un corps isomorphe à $\mathbb{C}$.

Remarque : Intuitivement, on se dit que $\mathbb{C}$ est un surcorps de $\mathbb{R}$ de dimension 2 et que $\mathbb{H}$ est de dimension 4. Nous verrons une façon rigoureuse de le faire au chapitre 30. Frobenius a prouvé en 1877 qu'il était n'existe pas de surcorps de $\mathbb{R}$ de dimension 3.

Exercice 22 : ✪✪ Montrer sans calcul de résolution (mais en utilisant l'exercice 10) que $L_1 = L_2 = 0$ sont les seules solutions du système linéaire suivant :

$$\begin{cases} \cos(1) \times L_1 & + & \sin(1) \times L_2 & = & L_1 \\ -\sin(1) \times L_1 & + & \cos(1) \times L_2 & = & L_2 \end{cases}$$

Exercice 23 : ✪✪ On pose $\mathcal{A} = \{aJ_n + bI_n \mid (a,b) \in \mathbb{C}^2\}$ $(n \geq 2)$ où, comme en cours, $J_n \in \mathscr{M}_n(\mathbb{C})$ est la matrice dont tous les coefficients sont égaux à 1.

1. Montrer que $\mathcal{A}$ est un sous-anneau de $\mathscr{M}_n(\mathbb{C})$. Montrer de deux façons différentes que J_n n'est pas inversible.

1. Bon, les corps étant commutatifs par définition, il faudrait plutôt parler d'une « algèbre à division » ou d'un « corps gauche ».
2. Personnellement c'est mon groupe préféré...

2. Donner toutes les matrices $M \in \mathcal{A}$ telles que $M^n = I_n$.
3. ✪✪✪ Soit $M = aJ_n + bI_n \in \mathcal{A}$. Montrer que M admet un inverse dans $\mathcal{A}$ si et seulement si $b(b+na) \neq 0$ et donner alors l'inverse de M.

Exercice 24 - Matrice d'un projecteur : ✪✪ Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$. Soit

$$P = \frac{1}{\mathrm{card(G)}} \sum_{g \in G} g$$

Montrer que $P^2 = P$.

Exercice 25 - « Ce que l'on conçoit bien s'énonce clairement... » : ✪✪ Les deux questions sont indépendantes.

1. On dit qu'une matrice $M \in \mathscr{M}_n(\mathbb{K})$ est en damier si $M_{i,j} = 0$ dès que $i - j$ est impair. Montrer que l'ensemble des matrices en damier est un sous-anneau de $\mathscr{M}_n(\mathbb{K})$.
2. Même question avec l'ensemble des matrices centrosymétriques : on dit que $M \in \mathscr{M}_n(\mathbb{K})$ est centrosymétrique si $M_{i,j} = M_{n+1-i,n+1-j}$ pour tout $(i,j) \in [\![1\,;\, n]\!]^2$.

Exercice 26 : ✪✪ Soit A telle que $A \times A^\top \times A = I_n$. Montrer que $A^3 = I_n$.

Exercice 27 : ✪✪ On définit sur $\mathscr{M}_n(\mathbb{C})$ les deux applications N et N' par

$$N(A) = \max_{1 \leq i \leq n} \left(\sum_{j=1}^{n} |A_{i,j}| \right) \qquad \text{et} \qquad N'(A) = \max_{1 \leq j \leq n} \left(\sum_{i=1}^{n} |A_{ij}| \right)$$

Les trois questions sont indépendantes.

1. Montrer que N est une norme, c'est-à-dire :
   - $\forall A \in \mathscr{M}_n(\mathbb{C}), N(A) = 0 \iff A = 0$.
   - $\forall (A,B) \in \mathscr{M}_n(\mathbb{C})^2, N(A+B) \leq N(A) + N(B)$.
   - $\forall (A,\lambda) \in \mathscr{M}_n(\mathbb{C}) \times \mathbb{C}, N(\lambda A) = |\lambda| A$.
2. (a) Montrer que :

$$\forall A \in \mathscr{M}_n(\mathbb{C}), \qquad \frac{1}{n} N'(A) \leq N(A) \leq n N'(A)$$

   (b) Montrer que les constantes $1/n$ et n sont les meilleures possibles.
3. Montrer que : $\forall (A,B) \in \mathscr{M}_n(\mathbb{C})^2, N(A \times B) \leq N(A) \times N(B)$.

Exercice 28 : ✪✪ Soit $M \in \mathscr{M}_n(\mathbb{Z})$. On suppose qu'il existe $P \in \mathrm{GL}_n(\mathbb{C})$ et $D \in \mathscr{M}_n(\mathbb{C})$ diagonale telles que $M = PDP^{-1}$. On suppose enfin que les termes diagonaux de D appartiennent à $\mathbb{U}$.

1. Montrer que M est inversible.
2. Montrer qu'il existe $A \in \mathbb{R}$ tel que pour tout $q \geq 1$, les coefficients de M^q soient bornés par A. En déduire qu'il n'existe qu'un nombre fini de puissances distinctes de M.
3. Montrer qu'il existe $p \geq 1$ tel que $M^p = I_n$ et en déduire que les coefficients diagonaux de D sont des racines de l'unité.

Exercice 29 - Générateur automatique de matrices orthogonales : ✪✪ Soit $A \in A_n(\mathbb{R})$. On admet que $I_n + A$ est inversible et on pose $\Omega = (I_n - A) \times (I_n + A)^{-1}$. Montrer que $\Omega^\top \times \Omega = I_n$.

Exercice 30 : ✪✪ On note $O_n(\mathbb{Z})$ l'ensemble des matrices de taille n dont chaque ligne et chaque colonne comporte un et un seul coefficient égal à ± 1, les autres étant nuls. Donner le cardinal de $O_n(\mathbb{Z})$.

Exercice 31 - Centre de $\mathscr{M}_n(\mathbb{K})$: ✪✪✪

1. Soit $A \in \mathscr{M}_n(\mathbb{K})$. On appelle commutant de A l'ensemble $C(A) = \{M \in \mathscr{M}_n(\mathbb{K}) \mid AM = MA\}$. Montrer que $C(A)$ est un sous-anneau de $\mathscr{M}_n(\mathbb{K})$.
2. Soit $(k,l) \in [\![1\,;\, n]\!]^2$. A quelle condition une matrice M est-elle dans $C(E_{k,l})$?
3. Le centre de $\mathscr{M}_n(\mathbb{K})$, noté $Z(\mathscr{M}_n(K))$, est l'ensemble des matrices qui commutent avec toutes les autres. Montrer que

$$Z(\mathscr{M}_n(K)) = \bigcap_{1 \leq i,j \leq n} C(E_{i,j})$$

puis préciser cette intersection.

4. Donner l'ensemble des matrices qui commutent avec toutes les matrices diagonales.

Exercice 32 : ✪✪✪ Soit $A \in \mathrm{GL}_n(\mathbb{R})$ telle que $A + A^{-1} = I_n$. Exprimer $A^k + A^{-k}$ pour tout $k \in \mathbb{N}$.

Exercice 33 - Début de X MP 2014 : ✪✪✪ On considère l'ensemble des matrices carrées de taille 3 triangulaires supérieures strictes à coefficients réels :

$$L = \{M_{p,q,r} \,|\, (p,q,r) \in \mathbb{R}^3\} \qquad \text{où} \qquad M_{p,q,r} = \begin{pmatrix} 0 & p & r \\ 0 & 0 & q \\ 0 & 0 & 0 \end{pmatrix}$$

On définit $H = \{I_3 + M \,|\, M \in L\}$. Si A et B appartiennent à $\mathscr{M}_3(\mathbb{R})$, on appelle commutateur de A et B la matrice $[A,B] = AB - BA$. Enfin, si $M \in L$, on appelle exponentielle de M et on note $\exp(M)$ la matrice $I_3 + M + \frac{1}{2}.M^2$.

1. Calculer l'exponentielle de $M_{p,q,r}$.
2. Montrer que l'on définit une loi de groupe $*$ sur L en posant pour $M, N \in L$:

$$M * N = M + N + \frac{1}{2}[M,N]$$

   On explicitera l'inverse de $M_{p,q,r}$.
3. Déterminer les matrices $M_{p,q,r} \in L$ qui commutent avec tous les éléments de L pour la loi $*$. $(L,*)$ est-il commutatif ?
4. Montrer que pour toutes matrices $M, N \in L$, on a :

$$(\exp M) \times (\exp N) = \exp(M * N)$$

5. Soient M et N deux éléments de L. Montrer que :

$$\exp([M,N]) = \exp(M)\exp(N)\exp(-M)\exp(-N)$$

6. Montrer que H muni du produit usuel des matrices est un sous-groupe de $\mathrm{GL}_3(\mathbb{R})$ et que

$$\exp : (L,*) \to (H,\times)$$

   est un isomorphisme de groupes.

Exercice 34 : ✪✪✪

1. Soit $A \in \mathrm{GL}_n(\mathbb{R})$ telle que A et A^{-1} soient à coefficients positifs ou nuls. Montrer que chaque ligne et chaque colonne de A comporte un et un seul coefficient non nul.
2. Montrer que la réciproque est vraie, c'est-à-dire que si $A \in \mathrm{GL}_n(\mathbb{R})$ est à coefficients positifs ou nuls et si chaque ligne et chaque colonne de A comporte un et un seul coefficient non nul, alors A^{-1} est aussi à coefficients positifs ou nuls.

Exercice 35 - Matrices de permutation, cas général : ✪✪✪ On note S_n l'ensemble des permutations de $[\![1\,;n]\!]$ i.e. des bijections de $[\![1\,;n]\!]$ dans lui-même. Si $\sigma \in S_n$, on pose $M_\sigma = \left(\delta_{i,\sigma(i)}\right)_{1\leq i,j\leq n} \in \mathscr{M}_n(\mathbb{K})$.

1. Soit $\sigma \in S_n$. Décrire plus précisément M_σ.
2. Montrer que $G = \{M_\sigma \,|\, \sigma \in S_n\}$, l'ensemble des matrices de permutation, est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ isomorphe à S_n.
3. Soit $A \in \mathscr{M}_n(\mathbb{K})$ et soit $\sigma \in S_n$. Calculer $A \times M_\sigma$ et $M_\sigma \times A$.
4. Expliquer pourquoi cet exercice généralise le résultat du cours concernant les matrices de permutation.

Exercice 36 - Décomposition LU (Lower-Upper) : ✪✪✪✪ Soit $A = (a_{i,j})_{1\leq i,j\leq n}$. On suppose que pour tout $k \in [\![1\,;n]\!]$, la sous-matrice $(a_{i,j})_{1\leq i,j\leq k}$ est inversible.

1. À l'aide du pivot de Gauß, montrer qu'il existe L triangulaire inférieure avec des 1 sur la diagonale et U triangulaire supérieure inversible telle que $A = LU$.
2. Prouver que cette décomposition est unique.