

Polycopié d'exercices.

MP2I - Lycée Faidherbe

Premier semestre - Algèbre - Chapitres 16 à 21.

Table des matières

16 Relations binaires sur un ensemble	2
16.1 $\mathbb{Z}/n\mathbb{Z}$	2
16.2 Relations d'ordre	4
16.3 Relations d'équivalence	13
16.4 Ensembles quotients	17
17 Dénombrement	19
17.1 Dénombrement pur et dur	19
17.2 Relations de récurrence	32
17.3 Problèmes ensemblistes	41
17.4 Principe des tiroirs de Dirichlet	43
17.5 Formule du crible	45
18 Structures algébriques usuelles	47
18.1 Lois de composition internes	47
18.2 Groupes	60
18.2.1 Exemples explicites	60
18.2.2 Calculs dans un groupe	63
18.2.3 Transport de structure	65
18.2.4 Morphismes	69
18.2.5 Groupes et combinatoire	73
18.2.6 Quelques groupes classiques	74
18.2.7 Sous-groupes de \mathbb{R}	76
18.2.8 Un problème de groupes complet (découpé en trois exercices)	79
18.3 Anneaux et corps	84
18.3.1 Anneaux et corps explicites	84
18.3.2 Anneaux ou corps obtenus par adjonction d'un élément	88
18.3.3 Anneau des fonctions à valeurs dans un anneau	90
18.3.4 Anneaux et corps génériques	92
18.4 Deuxième année : Lagrange, ordre et $\mathbb{Z}/n\mathbb{Z}$	96
19 Polynômes	99
19.1 Racines, rigidité	99
19.2 Factorisation	115
19.3 Divers	123
19.4 Arithmétique des polynômes	129
19.5 Relations coefficients-racines	133
19.6 Quantités polynomiales en quelque-chose	138
19.7 Polynômes à coefficients dans un corps quelconque (HP)	141
20 Fractions rationnelles	142
21 The Matrix has you...	155

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 $\mathbb{Z}/9\mathbb{Z}$.

Correction : Pour l'addition :

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

$\mathbb{Z}/7\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$

$\mathbb{Z}/8\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{8}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$

$\mathbb{Z}/9\mathbb{Z}$

Pour le produit :

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

$\mathbb{Z}/7\mathbb{Z}$

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\mathbb{Z}/8\mathbb{Z}$

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{3}$	$\bar{7}$	$\bar{2}$	$\bar{6}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{1}$	$\bar{6}$	$\bar{2}$	$\bar{7}$	$\bar{3}$	$\bar{8}$	$\bar{4}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\mathbb{Z}/9\mathbb{Z}$

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

Correction : Supposons que $x \wedge n = 1$. D'après le théorème de Bézout, il existe u et v tels que $xu + nv = 1$. Si on réduit modulo n , cela fait $xu \equiv 1[n]$ c'est-à-dire que, dans $\mathbb{Z}/n\mathbb{Z}$, $\bar{x} \times \bar{u} = \bar{1}$: \bar{x} est inversible.

Réciproquement, supposons \bar{x} inversible. Il existe alors $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{x} \times \bar{y} = \bar{1}$ ce qui signifie que $xy \equiv 1[n]$ donc qu'il existe $k \in \mathbb{Z}$ tel que $xy - kn = 1$: d'après le théorème de Bézout, cela signifie que $x \wedge n = 1$.

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

Correction : Supposons que \bar{x} soit un diviseur de 0. Dès lors, $\bar{x} \neq \bar{0}$ donc $x \not\equiv 0[n]$. De plus, il existe $\bar{y} \neq \bar{0}$ tel que $\bar{x} \times \bar{y} = \bar{0}$ donc $xy \equiv 0[n]$ c'est-à-dire que n divise xy . Si $x \wedge n = 1$ alors, d'après le théorème de Gauß, n divise y si bien que $\bar{y} = \bar{0}$ ce qui est absurde, donc $x \wedge n \neq 1$.

Réciproquement, supposons que $x \not\equiv 0[n]$ et $x \wedge n \neq 1$. Tout d'abord, n ne divise pas x donc $\bar{x} \neq \bar{0}$. Notons $d = x \wedge n \neq 1$ et posons $y = n/d$. Alors $y \in \llbracket 1; n-1 \rrbracket$ donc $\bar{y} \neq \bar{0}$ mais d divise x donc il existe k tel que $x = kd$ si bien que $xy = kn$ et donc $\bar{x} \times \bar{y} = \bar{0}$: \bar{x} est bien un diviseur de 0.

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

Correction : En termes de congruences, on cherche une CNS sur n pour qu'il existe x non divisible par n dont une puissance soit divisible par n . Montrons que ce n'est possible que lorsque n admet un facteur carré, c'est-à-dire s'il existe p premier tel que $v_p(n) \geq 2$, c'est-à-dire si n admet un facteur premier à une puissance différente de 1 dans sa décomposition en produit de facteurs premiers.

Supposons que ce soit le cas, c'est-à-dire que la décomposition de n en produit de facteurs premiers soit $n = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ avec l'un au moins des α_i qui soit supérieur ou égal à 2. Soit $x = p_1 \times \dots \times p_r$. Alors x n'est pas divisible par n mais, si on pose $k = \max(v_{p_1}(n), \dots, v_{p_r}(n))$, alors x^k est divisible par n donc $\bar{x}^k = \bar{0}$ mais $\bar{x} \neq \bar{0}$: $\mathbb{Z}/n\mathbb{Z}$ admet des éléments nilpotents non nuls.

Réciproquement, supposons que la décomposition en produit de facteurs premiers de n soit $n = p_1 \times \dots \times p_r$ avec les p_i premiers distincts. Soit $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ un élément nilpotent. Il existe $k \geq 1$ tel que $\bar{x}^k = \bar{0}$ donc tel que x^k soit divisible par n . En particulier, p_i divise x pour tout i et les p_i sont premiers entre eux deux à deux donc leur produit divise x i.e. n divise x c'est-à-dire que $\bar{x} = \bar{0}$: le seul élément nilpotent de $\mathbb{Z}/n\mathbb{Z}$ est $\bar{0}$.

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 $\mathcal{P}(\mathbb{R})$ 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 ?

Correction : L'ensemble $\{1\}$ (correspondant au cas $n = 1$) est le plus petit élément (donc la borne inférieure) car il est inclus dans tous les autres. Cependant, il n'y a pas de plus grand élément car la suite des ensembles $[1/n; n]$ est strictement croissante (au sens de l'inclusion évidemment). Cependant, \mathbb{R}_+^* est la borne supérieure. En effet, il contient tous les $[1/n; n]$ donc est un majorant de l'ensemble. Si on prend A un majorant, alors il contient tous les ensembles $[1/n; n]$. Si $x \in \mathbb{R}_+^*$, alors il existe $n_0 \geq 1$ tel que $1/n \leq x$ (car $1/n \xrightarrow{n \rightarrow +\infty} 0$) et n_1 tel que $x \leq n_1$ (car $n \xrightarrow{n \rightarrow +\infty} +\infty$). Soit $n = \max(n_0, n_1)$. Alors $1/n \leq x \leq n$ donc $x \in [1/n; n]$. En particulier, puisque $[1/n; n] \subset A$, $x \in A$ donc $\mathbb{R}_+^* \subset A$: \mathbb{R}_+^* est donc le plus petit de tous les majorants (au sens de l'inclusion) donc est bien la borne supérieure.

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

- Correction :**

1. Tout nombre $n \geq 2$ peut s'écrire sous la forme $n = 2^{v_2(n)} \times k$ avec k impair. Soient n_1 et n_2 deux entiers naturels non nuls.
 - Si n_2 est une puissance de 2 (y compris si $n_2 = 1 = 2^0$) et n_1 n'en est pas une, alors $n_1 \triangleleft n_2$.
 - Si n_1 et n_2 ne sont pas des puissances de 2 et $v_2(n_1) \leq v_2(n_2)$ (au sens de l'ordre usuel sur \mathbb{N}), alors $n_1 \triangleleft n_2$, et si $v_2(n_1) = v_2(n_2)$ et $n_1 \leq n_2$ (au sens de l'ordre usuel), alors $n_1 \triangleleft n_2$.
 - Enfin, si n_1 et n_2 sont des puissances de 2, $n_1 \triangleleft n_2$ si $n_2 \leq n_1$ (au sens de l'ordre usuel) i.e. \triangleleft est l'inverse de l'ordre usuel sur les puissances de 2.
2. Soit $n \in \mathbb{N}^*$. Dans tous les cas, que n soit une puissance de 2 ou non, d'après la question précédente, $n \triangleleft n$ donc \triangleleft est réflexive.

Soient n_1 et n_2 deux entiers naturels non nuls tels que $n_1 \triangleleft n_2$ et $n_2 \triangleleft n_1$. Si n_1 est une puissance de 2, alors n_2 en est une puisque $n_1 \triangleleft n_2$. Donc soit les deux sont des puissances de 2, soit aucun des deux n'est une puissance de 2. Si les deux sont des puissances de 2, alors $n_2 \leq n_1$ et $n_1 \leq n_2$ (au sens de l'ordre usuel) donc $n_1 = n_2$. Supposons que n_1 et n_2 ne soient pas des puissances de 2. Il n'est pas possible d'avoir $v_2(n_1) < v_2(n_2)$ et $v_2(n_2) < v_2(n_1)$ donc on a forcément $v_2(n_1) = v_2(n_2)$ et alors $n_1 \leq n_2$ et $n_2 \leq n_1$ donc on a égalité : la relation est antisymétrique.

Soient n_1, n_2, n_3 trois entiers naturels non nuls tels que $n_1 \triangleleft n_2$ et $n_2 \triangleleft n_3$. Il faut évaluer plusieurs cas :

- Si tous sont des puissances de 2, alors \triangleleft est l'inverse de l'ordre usuel : $n_3 \leq n_2$ et $n_2 \leq n_1$ donc $n_3 \leq n_1$ si bien que $n_1 \triangleleft n_3$.
- Il est impossible que n_1 soit une puissance de 2 et pas n_2 (car sinon $n_2 \triangleleft n_1$), tout comme il est impossible que n_2 soit une puissance de 2 et pas n_3 . Ainsi, si n_1 est une puissance de 2, alors n_2 et n_3 le sont aussi, et on a déjà traité ce cas. Supposons dans la suite que n_1 ne soit pas une puissance de 2.

4

- Si n_2 est une puissance de 2, n_3 en est forcément une donc $n_1 \triangleleft n_3$. On suppose dans la suite que n_2 n'est pas une puissance de 2.
- Si n_3 est une puissance de 2 alors $n_1 \triangleleft n_3$. On suppose dans la suite que n_3 n'en est pas une : n_1, n_2 et n_3 ne sont pas des puissances de 2. Par conséquent, $v_2(n_1) \leq v_2(n_2)$ et $v_2(n_2) \leq v_2(n_3)$.
- Si l'une des inégalités est stricte, alors $v_2(n_1) < v_2(n_3)$ donc $n_1 \triangleleft n_3$.
- Supposons enfin que $v_2(n_1) = v_2(n_2)$ et $v_2(n_2) = v_2(n_3)$ donc $v_2(n_1) = v_2(n_3)$, mais puisque $n_1 \triangleleft n_2$ alors $n_1 \leq n_2$ et de même $n_2 \leq n_3$ donc $n_1 \leq n_3$ donc $n_1 \triangleleft n_3$.

Dans tous les cas, $n_1 \triangleleft n_3$: \triangleleft est transitive. C'est donc une relation d'ordre : prouvons que c'est un ordre total. Soient donc n_1 et n_2 deux entiers naturels non nuls.

- Si n_1 n'est pas une puissance de 2 et n_2 en est une, $n_2 \triangleleft n_1$. Idem si n_2 n'est pas une puissance de 2 mais si n_1 en est une.
- Si n_1 et n_2 sont des puissances de 2, alors l'ordre est l'inverse de l'ordre usuel donc, dans tous les cas, l'un des deux est inférieur à l'autre (au sens de \triangleleft).
- Supposons que ni n_1 ni n_2 ne soient des puissances de 2. Si $v_2(n_1) < v_2(n_2)$ alors $n_1 \triangleleft n_2$. Si $v_2(n_2) < v_2(n_1)$, c'est le contraire. Enfin, si $v_2(n_1) = v_2(n_2)$, on a soit $n_1 \leq n_2$, soit $n_2 \leq n_1$, donc dans tous les cas, l'un est inférieur à l'autre (au sens de \triangleleft).

Dans tous les cas, $n_1 \triangleleft n_2$ ou le contraire : l'ordre est total.

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.

Correction :

1. Montrons que c'est une relation d'ordre.
 - Soit $x \in \mathbb{N}$. Alors $x = x^1$ donc il existe $n \in \mathbb{N}^*$ tel que $x = x^n$ si bien que $x \preccurlyeq x$: \preccurlyeq est réflexive.
 - Soit $(x, y) \in \mathbb{N}^2$ tel que $x \preccurlyeq y$ et $y \preccurlyeq x$. Alors il existe $n \in \mathbb{N}^*$ tel que $y = x^n$ et il existe k tel que $x = y^k$. Par conséquent, $x = (x^n)^k$ donc $x = x^{nk}$. En particulier, soit $x = 0$, et dans ce cas $y = 0 = x$, soit $y = 1$, et alors on a encore $y = 1 = x$, soit $nk = 1$, et alors $n = k = 1$ car ce sont des entiers positifs, si bien que $y = x$. Dans tous les cas, $x = y$: \preccurlyeq est antisymétrique.
 - Soit $(x, y, z) \in \mathbb{N}^3$ tel que $x \preccurlyeq y$ et $y \preccurlyeq z$: il existe $n \in \mathbb{N}^*$ tel que $y = x^n$ et il existe $k \in \mathbb{N}^*$ tel que $z = y^k$ si bien que $z = x^{nk}$ et $nk \in \mathbb{N}^*$: $x \preccurlyeq z$, et donc \preccurlyeq est transitive.

En conclusion, \preccurlyeq est bien une relation d'ordre, non totale car 2 et 3 sont incomparables : il n'existe pas d'entier n tel que $2^n = 3$ ni tel que $3^n = 2$.

2. On cherche les éléments y de \mathbb{N} tels qu'il n'existe pas de $x \neq y$ tel que $x \preccurlyeq y$ i.e. tels que y soit une puissance de x . Montrons que les éléments minimaux sont exactement 0, 1 et les entiers dont les puissances dans la décomposition en produit de facteurs premiers n'ont aucun diviseur commun distinct de 1.

Tout d'abord, 0 est un élément minimal. En effet, supposons que $x \preccurlyeq 0$: il existe n tel que $0 = x^n$ donc $x = 0$. 0 est bien un élément minimal. De plus, si $x \preccurlyeq 1$ alors il existe $n \in \mathbb{N}^*$ tel que $1 = x^n$ mais $n \geq 1$ donc $x = 1$: 1 est aussi un élément minimal.

Soit $y \geq 2$ donc les puissances dans la décomposition en produit de facteurs premiers n'ont aucun diviseur commun distinct de 1 (par exemple, les puissances ne sont pas toutes paires, comme dans $3^2 \times 5^4$). Soit $x \preccurlyeq y$: il existe $n \in \mathbb{N}^*$ tel que $x^n = y$ donc, pour tout p facteur premier de y , $v_p(y) = nv_p(x)$ donc n divise $v_p(y)$. Par conséquent, $n = 1$ car c'est le seul diviseur commun des $v_p(y)$ donc $x = y$: y est bien un élément minimal.

Enfin, soit y un entier qui n'est pas de cette forme et prouvons que ce n'est pas un élément minimal. Par hypothèse, les puissances des facteurs premiers de y ont un diviseur commun $n \geq 2$. Notons $y = p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$ avec les α_i divisibles par n , et posons $x = p_1^{\alpha_1/n} \times \dots \times p_k^{\alpha_k/n}$. On a bien $y = x^n$ donc $x \preccurlyeq y$ avec $x \neq y$: y n'est pas un élément minimal.

En conclusion, les éléments minimaux de \mathbb{N} sont 0, 1 et les nombres entiers dont les valuations p -adiques sont premières entre elles i.e. les puissances dans la décomposition en produit de facteurs premiers n'ont aucun diviseur commun distinct de 1 (par exemple $2^5 \times 3^2 \times 5^4$ est un élément minimal car 5, 2, 4 sont premiers entre eux dans leur ensemble).

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 $\mathcal{P}(X)$.
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).

Correction :

1. Si $*$ est l'intersection, alors \preccurlyeq est définie par :

$$\forall (A, B) \in \mathcal{P}(E)^2, A \preccurlyeq B \iff A \cap B = A$$

et on sait que $A \cap B = A$ si et seulement si $A \subset B$: \preccurlyeq est donc l'inclusion, qui est bien une relation d'ordre (cf. cours).

2. Montrons que \preccurlyeq est une relation d'ordre.
 - Soit $x \in E$. Puisque $x * x = x$ (x est idempotent), $x \preccurlyeq x$: \preccurlyeq est réflexive.
 - Soient x et y dans E tels que $x \preccurlyeq y$ et $y \preccurlyeq x$. Ainsi, $x * y = x$ et $y * x = y$. Or, la loi est commutative donc $x * y = y * x$ si bien que $x = y$: \preccurlyeq est antisymétrique.
 - Soit $(x, y, z) \in E^3$ tel que $x \preccurlyeq y$ et $y \preccurlyeq z$. Dès lors, $x * y = x$ et $y * z = z$. Ainsi, $x * z = (x * y) * z$. La loi étant associative, $x * z = x * (y * z) = x * y = x$ c'est-à-dire que $x \preccurlyeq z$: \preccurlyeq est transitive, c'est une relation d'ordre.
3. Soit $(x, y) \in E^2$. Il s'agit donc de prouver que $x * y$ est inférieur à x et à y et que tout minorant de x et de y est inférieur à $x * y$ (il est évident ici qu'on ne parle qu'au sens de la relation d'ordre \preccurlyeq). Tout d'abord, la loi étant commutative et associative :

$$\begin{aligned} (x * y) * x &= (y * x) * x \\ &= y * (x * x) \\ &= y * x \\ &= x * y \end{aligned}$$

c'est-à-dire que $x * y \preccurlyeq x$. On prouve de même (c'est même plus simple) que $x * y \preccurlyeq y$ donc $x * y$ est un minorant de x et de y . Soit à présent m un minorant de x et de y . Alors $m \preccurlyeq x$ donc $m * x = m$, et $m \preccurlyeq y$ donc $m * y = m$. Dès lors (on utilise encore l'associativité de la loi) :

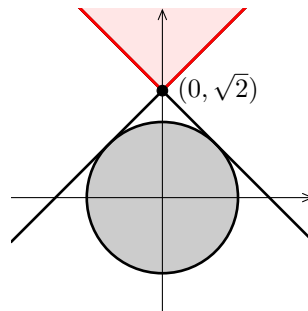
$$\begin{aligned} m * (x * y) &= (m * x) * y \\ &= m * y \\ &= m \end{aligned}$$

si bien que $m \preccurlyeq x * y$: on a bien le résultat voulu.

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 $(0, \sqrt{2})$.



Correction :

1. Montrons que c'est une relation d'ordre.
 - Soit $(x, y) \in \mathbb{R}^2$. Alors, d'une part, $|x - x| = 0$ et, d'autre part, $y - y = 0$ donc on a bien $|x - x| \leq y - y$: $(x, y) \preccurlyeq (x, y)$, \preccurlyeq est réflexive.

- Soient (x_1, y_1) et (x_2, y_2) deux éléments de \mathbb{R}^2 tels que $(x_1, y_1) \preccurlyeq (x_2, y_2)$ et $(x_2, y_2) \leq (x_1, y_1)$. Dès lors, $|x_1 - x_2| \leq y_2 - y_1$ donc $y_2 - y_1 \geq 0$. Par symétrie des rôles, $y_1 - y_2 \geq 0$ donc $y_1 = y_2$. Par conséquent, $x_1 = x_2$ puisque $|x_1 - x_2| \leq y_2 - y_1 = 0$. On en déduit que $(x_1, y_1) = (x_2, y_2)$: \preccurlyeq est antisymétrique.
- Soit $((x_1, y_1), (x_2, y_2), (x_3, y_3)) \in (\mathbb{R}^2)^3$ tel que $(x_1, y_1) \preccurlyeq (x_2, y_2)$ et $(x_2, y_2) \preccurlyeq (x_3, y_3)$. En d'autres termes :

$$|x_1 - x_2| \leq y_2 - y_1 \quad \text{et} \quad |x_2 - x_3| \leq y_3 - y_2$$

Par somme :

$$|x_1 - x_2| + |x_2 - x_3| \leq y_2 - y_1 + y_3 - y_2 = y_3 - y_1$$

Or, d'après l'inégalité triangulaire,

$$|x_1 - x_3| = |x_1 - x_2 + x_2 - x_3| \leq |x_1 - x_2| + |x_2 - x_3|$$

si bien que $|x_1 - x_3| \leq y_3 - y_1$: on a bien $(x_1, y_1) \preccurlyeq (x_3, y_3)$, \preccurlyeq est transitive, c'est bien une relation d'ordre.

Cependant, elle est pas totale car $(1, 0)$ et $(2, 0)$ sont incomparables : en effet, on n'a pas $|2 - 1| \leq 0 - 0$, ni $|1 - 2| \leq 0 - 0$.

2. Inspirons-nous du dessin ci-contre. Essayons de trouver géométriquement tous les majorants du disque unité, qu'on notera D . Soit $(x, y) \in \mathbb{R}^2$. Cherchons une CNS pour que (x, y) soit un majorant de D . Soit $(a, b) \in D$. Alors :

$$\begin{aligned} (a, b) \preccurlyeq (x, y) &\iff |a - x| \leq y - b \\ &\iff a - x \leq y - b \quad \text{et} \quad x - a \leq y - b \\ &\iff y \geq -x + b + a \quad \text{et} \quad y \geq x + b - a \end{aligned}$$

En termes géométriques : (x, y) est supérieur à (a, b) lorsque le point correspondant est au-dessus des deux droites d'équation $y = -x + (b + a)$ et $y = x + b - a$ i.e. des deux droites de pentes ± 1 d'ordonnée à l'origine $b + a$ ou $b - a$, i.e. dans l'intersection des deux domaines au-dessus des deux droites. (x, y) est donc un majorant de D lorsque ceci est vrai pour tout $(a, b) \in D$. Montrons donc que l'ensemble des majorants de D est la partie rouge ci-dessus, l'intersection des deux parties du plan au-dessus des deux droites d'équation $y = \pm x + \sqrt{2}$.

D'une part, soit (x, y) un majorant de D . D'après ce qui précède, $y \geq \pm x + b - a$ pour tout $(a, b) \in D$. C'est vrai en particulier pour $a = \sqrt{2}/2$ et $b = \sqrt{2}/2$ (car $(\sqrt{2}/2, \sqrt{2}/2)$ est bien un élément du disque) donc $y \geq -x + a + b = -x + \sqrt{2}$: le point est au-dessus de la droite d'équation $y = -x + \sqrt{2}$ (la droite qui descend sur le dessin ci-dessus). De même avec $a = -\sqrt{2}$ et $b = \sqrt{2}$ (cela correspond au cas où les droites sont les « plus hautes » i.e. tangentes au cercle unité), $y \geq x + b - a = x + \sqrt{2}$: on a bien les deux inégalités voulues.

D'autre part, soit (y, x) un élément de \mathbb{R}^2 tel que $y \geq \pm x + \sqrt{2}$, et montrons que c'est un majorant de D . Soit $(a, b) \in D$, montrons que $y \geq x + b - a$ et $y \geq -x + b + a$. Il suffit de prouver que $\sqrt{2} \geq b \pm a$. Or :

$$(b + a)^2 = a^2 + b^2 + 2ab \leq 1 + 2ab$$

puisque $a^2 + b^2 \leq 1$ car $(a, b) \in D$. De plus, $2ab \leq a^2 + b^2$ (inégalité remarquable) donc $(a + b)^2 \leq 1 + 1 = 2$ ce qui donne le résultat voulu. L'inégalité $b - a \leq \sqrt{2}$ se démontre de la même façon.

En conclusion, l'ensemble des majorants de D est l'ensemble rouge ci-dessus, l'intersection des deux parties du plan au-dessus des droites d'équation $y = \pm x + \sqrt{2}$, c'est-à-dire que (x, y) est un majorant si et seulement si $y \geq \pm x + \sqrt{2}$: $(0, \sqrt{2})$ est donc un majorant de D . Montrons finalement que c'est le plus petit. Soit (x, y) un majorant de D . Alors $y \geq \pm \sqrt{2}$ donc $y - \sqrt{2} \geq \pm x$ donc $|x - 0| \leq y - \sqrt{2}$: $(0, \sqrt{2}) \preccurlyeq (x, y)$, ce qui permet de conclure.

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 :

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

Correction : Raisonnons par l'absurde et supposons qu'il en existe une. Si $1 \preccurlyeq 0$, en ajoutant -1 , il vient $0 \preccurlyeq -1$. En multipliant par -1 , ce qui ne change pas le sens de l'inégalité puisque $0 \preccurlyeq -1$, on obtient que $0 \preccurlyeq 1$ donc $0 = 1$ par antisymétrie ce qui est absurde. On en déduit que $0 \not\preccurlyeq 1$: en effet, l'ordre est total donc, si ce n'est pas l'un, c'est l'autre.

Si $0 \not\preccurlyeq -1$, en ajoutant 1 des deux côtés, on trouve $1 \preccurlyeq 0$ ce qui est absurde. Ainsi, $-1 \preccurlyeq 0$ (idem, l'ordre est total).

Supposons que $0 \preccurlyeq i$. En multipliant par i , $0 \preccurlyeq -1$ ce qui est absurde. On en déduit que $i \preccurlyeq 0$. En ajoutant $-i$, il vient $0 \preccurlyeq -i$ et en multipliant par $-i$, $0 \preccurlyeq (-i)^2 = -1$. On ne peut pas avoir $0 \preccurlyeq i$ et $i \preccurlyeq 0$: un tel ordre n'existe pas.

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 $(\forall n \in \mathbb{N}, (x_{n+1} \preccurlyeq x_n \text{ et } x_{n+1} \neq x_n))$. 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 ?

Correction :

1. On montre comme en cours (récurrence sur p , à savoir faire) que, si une suite strictement croissante existe, alors, pour tous $n < p$, $u_n \preccurlyeq u_p$ et $u_n \neq u_p$, et idem (cf. cours) pour une suite strictement décroissante en particulier, la suite prend une infinité de valeurs différentes, ce qui est absurde car l'ensemble est fini.

S'il n'existe pas d'élément minimal, tout élément admet un autre élément qui lui est strictement inférieur (i.e. inférieur non égal) donc on peut construire une suite infinie strictement décroissante : on prend $x_0 \in E$ quelconque, puis on prend $x_1 \preccurlyeq x_0$ avec $x_1 \neq x_0$ et ainsi de suite, ce qui est absurde.

2. Il faut lui répondre : « non, l'humanité est un ensemble fini donc il y a au moins un élément minimal, c'est-à-dire une personne n'admettant personne de plus bête qu'elle ». Mais « être plus bête » n'étant pas un ordre total, il n'y a pas forcément de plus petit élément, il peut y avoir plusieurs éléments minimaux incomparables (il existe plusieurs types de bêtise).

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.

Correction :

1. L'ordre usuel sur \mathbb{N} est un bon ordre, mais pas l'ordre usuel sur \mathbb{Z} (ou \mathbb{Q} ou \mathbb{R}) : par exemple, \mathbb{Z} est non vide mais n'a pas de plus petit élément.
2. Soient a et b deux éléments de E (muni d'un bon ordre \preccurlyeq). Alors $\{a; b\}$ est non vide donc admet un plus petit élément : si c'est a , alors $a \preccurlyeq b$, si c'est b , alors $b \preccurlyeq a$. L'ordre est bien total.
3. Soit $E = \{u_n \mid n \in \mathbb{N}\}$ l'ensemble des termes de la suite. E étant non vide et l'ordre étant bon, E admet un plus petit élément u_{n_0} . Soit $n \geq n_0$. La suite étant décroissante, $u_n \leq u_{n_0}$. Or, u_{n_0} est le plus petit élément de E donc $u_n \geq u_{n_0}$ donc $u_n = u_{n_0}$: la suite est constante à partir du rang n_0 , la suite est stationnaire.
4. Soit B une partie non vide de E , montrons qu'elle admet un plus petit élément. Notons $A = f^{-1}(B)$ l'ensemble des antécédents des éléments de B : A est donc une partie de \mathbb{N} , non vide, donc admet un plus petit élément noté n_0 . En d'autres termes, pour tout $n \in A$, $n_0 \leq n$ (au sens de l'ordre usuel). Soit $a = f(n_0) \in B$ et soit $x \in B$. Puisque $x \in B$, alors, si on note n son antécédent par f (f est bijective), $n \in A$ donc $n_0 \leq n$ si bien que, par hypothèse sur f , $a = f(n_0) \leq f(n) = x$: a est le plus petit élément de B , l'ordre est un bon ordre.
5. D'après la question précédente, il suffit de prouver que l'ordre usuel n'est pas bon sur \mathbb{Q} , ce qui est immédiat (\mathbb{Q} n'admet pas de plus petit élément par exemple).

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.

Correction : Raisonnons par l'absurde et supposons que l'ensemble soit infini. Montrons qu'alors on peut construire une suite strictement monotone, ce qui sera absurde puisque l'ensemble des termes de la suite n'aura pas de maximum (si la suite est strictement croissante) ou pas de minimum (si elle est strictement décroissante).

Tout d'abord, l'ordre est total : en effet, si a et b sont dans E , l'ensemble $\{a; b\}$ est non vide donc admet un minimum et un maximum. Si a est le minimum, alors $a \preccurlyeq b$, et si b est le maximum, alors $b \preccurlyeq a$: l'ordre est bien total (c'est même un

bon ordre, cf. exercice 13).

E admet un minimum par hypothèse, qu'on note x_0 . $E \setminus \{x_0\}$ est non vide (car E est infini) donc admet un minimum noté x_1 , et $x_0 \leq x_1$ puisque x_0 est le minimum de E , et $x_0 \neq x_1$. $E \setminus \{x_0; x_1\}$ est non vide (car E est infini) donc admet un minimum x_2 . On a $x_1 \leq x_2$ car x_1 est le minimum de $E \setminus \{x_0\}$ et $x_1 \neq x_2$ car $x_2 \neq E \setminus \{x_0; x_1\}$. Itérons le processus : soit $n \geq 2$, supposons x_0, \dots, x_n construits. E est infini donc $E \setminus \{x_0; \dots; x_n\}$ est non vide donc admet un minimum x_{n+1} , distinct de x_0, \dots, x_n et supérieur à x_n (car x_n était lui-même le minimum de $E \setminus \{x_0; \dots; x_{n-1}\}$). On a donc construit une suite strictement croissante d'éléments de E , ce qui est absurde puisque $A = \{x_n \mid n \in \mathbb{N}\}$ n'admet pas de maximum. En effet, s'il admet un maximum x_{n_0} , alors x_{n_0+1} est strictement plus grand que x_{n_0} qui est le maximum, ce qui est absurde : 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 :

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

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 $R_1 \preceq R_2$.

1. Montrer que \preceq est une relation d'ordre sur $O(E)$.
2. Y a-t-il un plus petit élément pour \preceq 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 \preceq sont exactement les relations d'ordre totales.

Correction :

1. Montrons que \preceq est une relation d'ordre sur $O(E)$.
 - Soit $R \in O(E)$. Soit $(x, y) \in E^2$ tel que xRy . Alors xRy . En d'autres termes, on a : $\forall (x, y) \in E^2, xRy \Rightarrow xRy$, c'est-à-dire que $R \preceq R$, R est réflexive.
 - Soient R_1 et R_2 dans $O(E)$ telles que $R_1 \preceq R_2$ et $R_2 \preceq R_1$. Soit $(x, y) \in E^2$. Si xR_1y alors xR_2y puisque $R_1 \preceq R_2$, et si xR_2y alors xR_1y puisque $R_2 \preceq R_1$. En d'autres termes : $xR_1y \iff xR_2y$, c'est-à-dire que R_1 et R_2 comparent les mêmes éléments, et dans le même sens. R_1 et R_2 sont donc la même relation d'ordre, $R_1 = R_2$, c'est-à-dire que \preceq est antisymétrique.
 - Soient R_1, R_2 et R_3 dans $O(E)$ telles que $R_1 \preceq R_2$ et $R_2 \preceq R_3$. Soit $(x, y) \in E^2$ tel que xR_1y . Alors xR_2y puisque $R_1 \preceq R_2$ et donc xR_3y puisque $R_2 \preceq R_3$. En d'autres termes, $R_1 \preceq R_3$: \preceq est transitive.

C'est donc bien une relation d'ordre.

2. Montrons que l'égalité est la « pire relation d'ordre possible » : elle ne compare des éléments égaux, donc n'est pas très utile! Montrons donc que c'est le plus petit élément de $(O(E), \preceq)$. Soit $R \in O(E)$, montrons que $= \preceq R$ (on a évidemment noté $=$ la relation égalité). Soit $(x, y) \in E^2$. Si $x = y$ alors x et y sont égaux donc $y = x$ si bien que xRy par réflexivité. Il en découle que R est plus fine que $=$ c'est-à-dire : $= \preceq R$, $=$ est bien le plus petit élément de $O(E)$.
3. Soit R_1 une relation d'ordre totale, et soit $R_2 \in O(E)$ telle que $R_1 \preceq R_2$: prouvons que $R_1 = R_2$. Soit $(x, y) \in E^2$. La relation étant totale, soit xR_1y , soit yR_1x . Supposons sans perte de généralité que xR_1y . Puisque $R_1 \preceq R_2$, alors xR_2y . En d'autres termes, pour tous x et y , x et y sont dans le même ordre pour R_1 et pour R_2 donc $R_1 = R_2$: R_1 est bien un élément maximal.
4. Montrons que S est une relation d'ordre sur E .
 - Soit $x \in E$. Alors xRx car R est une relation d'ordre donc réflexive donc xSx (rappelons que si xRy alors xSy) : S est réflexive.
 - Soit $(x, y) \in E^2$ tel que xSy et ySx . Il y a plusieurs cas de figure :
 - Si xRy et yRx alors, par antisymétrie de R , $x = y$.
 - Si $(xRa \text{ et } bRy)$ et $(yRa \text{ et } bRx)$: bRy et yRa donc, par transitivité de R , bRa ce qui est exclu car a et b sont incomparables, c'est-à-dire que ce cas de figure ne peut pas se produire.
 - Si xRy et $(yRa \text{ et } bRx)$: bRx et xRy donc bRy par transitivité, et puisque yRa , alors bRa ce qui est toujours impossible.

En résumé, seul le premier cas peut se produire, donc $x = y$: S est antisymétrique.

- Soient x, y, z trois éléments de E tels que xSy et ySz . Là aussi, plusieurs cas :
 - Si xRy et yRz alors, par transitivité de R , xRz donc xSz .
 - Si $(xRa$ et $bRy)$ et $(yRa$ et $bRz)$: bRy et yRa donc, par transitivité de R , bRa ce qui est exclu car a et b sont incomparables, c'est-à-dire que ce cas de figure ne peut pas se produire.
 - Si xRy et $(yRa$ et $bRz)$: puisque xRy et yRa , par transitivité de R , xRa et puisque bRz , on a bien xSz .

Dans tous les cas, xSz : S est transitive, S est bien une relation d'ordre, et $R \preceq S$ (en effet, si xRy , alors xSy). De plus, on a aRa et bRb car R est réflexive. En d'autres termes, aSb (définition de S avec $x = a$ et $y = b$) : S est plus fine que R et compare a et b qui sont incomparables par R , S est strictement plus fine que R , R n'est pas un élément maximal. En conclusion, si R est totale, alors R est un élément maximal, et si R n'est pas totale, alors R n'est pas un élément maximal : les éléments maximaux 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 $f : A \rightarrow \mathbb{R}$. On définit sur E une relation \preceq par :

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

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

Correction :

1. • Soit $(A, f) \in E$. Alors $A \subset A$ et f est un prolongement de f donc $(A, f) \preceq (A, f)$, \preceq est réflexive.
 • Soient (A, f) et (B, g) dans E tels que $(A, f) \preceq (B, g)$ et $(B, g) \preceq (A, f)$. Alors, $A \subset B$ et $B \subset A$ donc $A = B$, et g prolonge f (i.e. $\forall x \in A, f(x) = g(x)$) donc $f = g$ (car g est définie sur $B = A$). Finalement, $(A, f) = (B, g)$: \preceq est antisymétrique.
 • Soient (A, f) , (B, g) , (C, h) dans E tels que $(A, f) \preceq (B, g)$ et $(B, g) \preceq (C, h)$. Alors, $A \subset B$ et $B \subset C$ donc $A \subset C$, et g prolonge f et h prolonge g , c'est-à-dire que pour tout $x \in A$, $g(x) = f(x)$ et pour tout $x \in B$, $h(x) = g(x)$ mais $B \subset C$ donc pour tout $x \in A$, $h(x) = g(x) = f(x)$ si bien que h prolonge f . Finalement, $(A, f) \preceq (C, h)$: \preceq est transitive.

C'est bien une relation d'ordre mais elle n'est pas totale car l'inclusion n'est pas un ordre total : (\mathbb{R}_+, \exp) et (\mathbb{R}_-, \sin) sont incomparables car \mathbb{R}_+ n'est pas inclus dans \mathbb{R}_- et \mathbb{R}_- n'est pas inclus dans \mathbb{R}_+ .

2. Il n'y a aucun plus grand élément : en effet, si $([\varepsilon; +\infty[, \ln|_{[\varepsilon; +\infty[})$ est un tel couple, alors $([\varepsilon/2; +\infty[, \ln|_{[\varepsilon/2; +\infty[})$ lui est strictement supérieur. Cependant, (\mathbb{R}_+^*, \ln) est la borne supérieure. En effet, c'est évidemment un majorant (car \mathbb{R}_+^* contient tous les $[\varepsilon; +\infty[$ et \ln prolonge toutes les restrictions). De plus, si (A, f) est un majorant (c'est-à-dire que, pour tout $\varepsilon > 0$, $([\varepsilon; +\infty[, \ln|_{[\varepsilon; +\infty[}) \preceq (A, f)$), alors, pour tout $x \in \mathbb{R}_+^*$, il existe $\varepsilon > 0$ tel que $\varepsilon \leq x$ donc $x \in [\varepsilon; +\infty[$, mais $[\varepsilon; +\infty[\subset A$ donc $x \in A$, et f prolonge $\ln|_{[\varepsilon; +\infty[}$ donc $f(x) = \ln(x)$. Finalement, $\mathbb{R}_+^* \subset A$ et f prolonge la fonction \ln donc $(\mathbb{R}_+^*, \ln) \preceq (A, f)$, (\mathbb{R}_+^*, \ln) est le plus petit des majorants, c'est la borne supérieure.

Exercice 17 - Ensembles inductifs : ★★ On dit qu'un ensemble ordonné (E, \preceq) 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 $(\mathcal{P}(E), \subset)$ est inductif.
4. On se replace dans le cadre de l'exercice 16. Montrer que (E, \preceq) est un ensemble inductif.
5. On se replace dans le cadre de l'exercice 15. Montrer que $(O(E), \preceq)$ est un ensemble inductif.

Correction :

1. Soit F une partie de E totalement ordonnée (avec E un ensemble fini de cardinal n). Par récurrence sur le cardinal de F .
 • Si $k \in \llbracket 1; n \rrbracket$, notons H_k : « si F est de cardinal k alors F admet un majorant ».
 • Si $\text{card}(F) = 1$ alors F est un singleton : si x est l'unique élément de F alors $x \preceq x$: x est un majorant de F , H_1 est vraie.
 • Soit $k \in \llbracket 1; n-1 \rrbracket$. Supposons H_k vraie, supposons H_{k+1} vraie. Soit donc F de cardinal $k+1$. Soit $a \in F$. Si a est un majorant de F (i.e. si $a \geq b$ pour tout $b \in F$) alors F est majorée. Sinon, il existe $b \in F \setminus \{a\}$ tel que a ne soit pas supérieur à b donc tel que $a \preceq b$ (car l'ensemble est totalement ordonné). Or, $F \setminus \{a\}$ est de cardinal k donc, par HR, admet un majorant M . Par conséquent, pour tout $x \in F$, soit $x \neq a$ et alors $x \preceq M$, soit $x = a$ et alors $x \preceq b$ et $b \preceq M$ donc, par transitivité, $x \preceq M$: M est un majorant de F . Dans tous les cas, F admet un majorant donc H_{k+1} est vraie.

- D'après le principe de récurrence, H_k est vraie pour tout $k \in \llbracket 1; n \rrbracket$.

E est donc inductif.

2. $(\mathbb{Z}, +)$ n'est pas inductif car \mathbb{Z} est une partie totalement ordonnée de \mathbb{Z} mais n'a pas de majorant.
3. Soit F une partie de $\mathcal{P}(E)$ totalement ordonnée, c'est-à-dire que F est un ensemble de parties de E , totalement ordonnée pour l'inclusion. Notons

$$U = \bigcup_{X \in F} X$$

l'union de tous les éléments de F . Alors U est un majorant de F puisque tous les éléments de F sont inclus dans U : $(\mathcal{P}(E), \subset)$ est inductif.

4. Soit donc F une partie de $\mathcal{P}(E)$ totalement ordonnée : F est donc un ensemble de couples (A, f_A) avec $f : A \rightarrow \mathbb{R}$. Posons

$$U = \bigcup_{A \mid (A, f_A) \in F} A$$

l'union des ensembles A tels que $(A, f_A) \in F$. Alors $A \subset U$ pour tout $A \in F$. On définit de plus $f : U \rightarrow \mathbb{R}$ par : pour tout A tel que $x \in A$, $f(x) = f_A(x)$. Montrons que f est bien définie, c'est-à-dire que si $x \in A$ et $x \in B$, alors $f_A(x) = f_B(x)$, i.e. l'image de x ne dépend pas de l'ensemble choisi. F étant totalement ordonné, soit $(A, f_A) \preceq (B, f_B)$, et alors $f_B(x) = f_A(x)$ puisque f_B prolonge f_A , soit le contraire, et donc on a toujours $f_A(x) = f_B(x)$: l'image de x ne dépend pas de A , $f(x)$ est bien définie et f prolonge f_A , (U, f) est bien un majorant de F , E est inductif.

5. Soit F une partie de E totalement ordonnée. Notons S la relation définie par :

$$xSy \iff \exists R \in F, xRy$$

Alors S est une relation d'ordre :

- la réflexivité est évidente.
- Soient x et y tels que xSy . Alors il existe R_1 et R_2 dans F telles que xR_1y et yR_2x . Or, F est totalement ordonnée donc $R_1 \preceq R_2$ ou le contraire. Sans perte de généralité, supposons $R_1 \preceq R_2$ si bien que xR_2y et R_2 est antisymétrique donc $x = y$: S est antisymétrique.
- La démonstration de la transitivité est analogue.

S est donc une relation d'ordre qui prolonge tout élément de F donc un majorant de F : E est inductif.

Remarque : Le lemme de Zorn (équivalent à l'axiome du choix) stipule que tout ensemble inductif admet un élément maximal. Par exemple, dans l'exercice 15, $O(E)$ est inductif donc (d'après le lemme de Zorn donc d'après l'axiome du choix) admet un élément maximal : en d'autres termes, d'après le lemme de Zorn (donc d'après l'axiome du choix), tout ensemble peut être muni d'un ordre total.

Exercice 18 : ★★★★★ Soit (E, \preceq) 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.

Correction :

1. Découle de la question 3 de l'exercice 13.
2. Montrons que l'ordre produit est bien fondé. Soit $((x_n, y_n))_{n \in \mathbb{N}}$ une suite d'éléments de \mathbb{N}^2 . Un élément $(x, y) \in \mathbb{N}^2$ est strictement inférieur (au sens de l'ordre produit) à (x_0, y_0) si et seulement si $x \leq x_0$ et $y \leq y_0$, et si $x_0 \neq x$ ou $y_0 \neq y$. Il y a donc $(x_0 + 1)$ choix possibles pour x (les entiers de 0 à x_0) et $(y_0 + 1)$ choix possibles pour y , ce qui fait $(x_0 + 1) \times (y_0 + 1) - 1$ choix pour (x, y) (on enlève 1 car on enlève le couple (x, y)). En particulier, il n'existe qu'un nombre fini d'éléments de \mathbb{N}^2 inférieurs à (x_0, y_0) donc il n'est pas possible que la suite $((x_n, y_n))$ soit strictement décroissante.

Pour l'ordre lexicographique à présent. Soit $((x_n, y_n))_{n \in \mathbb{N}}$ une suite d'éléments de \mathbb{N}^2 . Un élément $(x, y) \in \mathbb{N}^2$ est strictement inférieur (au sens de l'ordre lexicographique) à (x_0, y_0) si et seulement si $x < x_0$ ou $x = x_0$ et $y \leq y_0$. Le problème est qu'il y a un nombre infini de termes strictement inférieurs à (x_0, y_0) (par exemple tous les $(x_0 - 1, y)$ avec $y \in \mathbb{N}$). L'idée est qu'il n'y a qu'un nombre fini de termes avec le même x_0 , ensuite on prend un x strictement inférieur avec un y donné, puis il n'y a qu'un nombre fini de termes avec le même x , puis on prend un autre x strictement

inférieur etc. Il y a au plus $y_0 - 1$ termes strictement inférieurs à (x_0, y_0) de la forme (x_0, y) (i.e. avec le même x_0). Il existe forcément un terme (x_{n_1}, y_{n_1}) avec $x_{n_1} < x_{n_0}$. De même, il existe un terme (x_{n_2}, y_{n_2}) avec $x_{n_2} < x_{n_1}$ et ainsi de suite : pour tout élément de la suite (x_n, y_n) , il existe un couple (x_k, y_k) avec $x_k < x_n$: on peut donc extraire une suite (x_{n_p}, y_{n_p}) avec (x_{n_p}) strictement décroissante ce qui est absurde car c'est une suite d'entiers.

Finalement, l'ordre produit sur \mathbb{N}^2 n'étant pas total, ce n'est pas un bon ordre alors qu'il est bien fondé : un ordre bien fondé n'est pas forcément un bon ordre.

- On sait déjà qu'un bon ordre est bien fondé et total. Réciproquement, supposons qu'un ordre \preccurlyeq soit bien fondé et total, et prouvons que c'est un bon ordre. Soit A une partie non vide de E , et supposons que A n'admette pas de plus petit élément. Soit $x_0 \in A$. Puisque A n'admet pas de plus petit élément, il existe $x_1 \in A$ différent de x_0 tel que x_0 ne soit pas inférieur à x_1 donc, puisque l'ordre est total, on a forcément $x_1 \preccurlyeq x_0$. De même, il existe $x_2 \preccurlyeq x_1$ avec $x_2 \neq x_1$, et on itère le procédé : on construit une suite infinie strictement décroissante, ce qui est absurde puisque l'ordre est bien fondé.

Exercice 19 - Lemme de Spilrajn-Marczewski : ★★☆☆

- 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 $\llbracket 1; n \rrbracket$.
- 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 .
- Exhiber un ordre total sur $\llbracket 1; 10 \rrbracket$ (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.

Correction :

- Le problème est que l'ordre n'est pas forcément total, on ne peut pas écrire $x_1 \leq \dots \leq x_n$. Raisonnons par récurrence sur n .

- Si $n \geq 1$, notons H_n : « si E est un ensemble fini de cardinal n , il existe une bijection croissante de E dans $\llbracket 1; n \rrbracket$. »
- H_1 est évidemment vraie : si $E = \{x\}$ est un singleton, la fonction f qui envoie x sur 1 est une bijection croissante.
- Soit $n \geq 1$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. On suppose donc que E est un ensemble fini de cardinal $n + 1$. Le problème est que E n'a pas forcément de minimum ou de maximum. Cependant, puisque c'est un ensemble fini, alors il admet un élément maximal (on le montre comme dans exercice 12) : notons-le a . Dès lors, $E \setminus \{a\}$ est de cardinal n : par hypothèse de récurrence, il existe une bijection croissante $g : E \setminus \{a\} \rightarrow \llbracket 1; n \rrbracket$. Montrons que la fonction définie sur E par $f(a) = n + 1$ (on envoie a , un élément maximal, sur $n + 1$), et $f(x) = g(x)$ si $x \neq a$.

f est injective : en effet, soient $x \neq y$ deux éléments de E . Si x et y sont distincts de a , alors $f(x) = g(x)$ et $f(y) = g(y)$ mais g est injective donc $f(x) \neq f(y)$. Si l'un des deux vaut a , alors son image est égale à $n + 1$ et l'autre appartient à $\llbracket 1; n \rrbracket$ donc on a quand même $f(x) \neq f(y)$: f est injective.

f est surjective : en effet, $n + 1$ est atteint par a , et tout élément de $\llbracket 1; n \rrbracket$ est atteint par un élément de $E \setminus \{a\}$ car g est surjective.

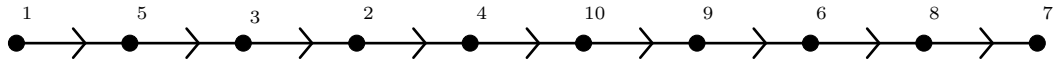
Montrons enfin que f est croissante : soient $x \leq_E y$. Supposons que x et y soient distincts de a . Puisque g est croissante sur $E \setminus \{a\}$, $g(x) \leq g(y)$, et puisque $g(x) = f(x)$ et $g(y) = f(y)$, cela donne le résultat voulu. Si $y = a$ alors $f(y) = n + 1$ donc on a forcément $f(x) \leq f(y)$. Enfin, si $x = a$ alors $y = a$ car a est un élément maximal donc on a bien $f(x) = f(y)$ (puisque $x = y$) : f est bien une bijection croissante, ce qui clôt la récurrence.

- Notons \preccurlyeq la relation : $x \preccurlyeq y \iff f(x) \leq f(y)$ (l'ordre \leq étant l'ordre usuel sur $\llbracket 1; n \rrbracket$). Si $x \leq_E y$ alors (f est croissante) $f(x) \leq f(y)$ donc $x \preccurlyeq y$: \preccurlyeq prolonge \leq_E . Il suffit pour conclure de montrer que c'est une relation d'ordre total sur E .

- Soit $x \in E$. Alors $f(x) \leq f(x)$ donc $x \preccurlyeq x$: \preccurlyeq est réflexive.
- Soient x et y dans E tels que $x \preccurlyeq y$ et $y \preccurlyeq x$: par définition, il en découle que $f(x) \leq f(y)$ et $f(y) \leq f(x)$ donc $f(x) = f(y)$: f étant injective, $x = y$, \preccurlyeq est antisymétrique.
- Soient x, y, z dans E tels que $x \preccurlyeq y$ et $y \preccurlyeq z$: il en découle que $f(x) \leq f(y)$ et $f(y) \leq f(z)$ donc, par transitivité de l'ordre usuel, $f(x) \leq f(z)$ donc $x \preccurlyeq z$: \preccurlyeq est transitive.

\preccurlyeq est une relation d'ordre. Enfin, si x et y sont dans E , l'ordre usuel étant total, soit $f(x) \leq f(y)$, et alors $x \preccurlyeq y$, soit $f(y) \leq f(x)$, et alors $y \preccurlyeq x$: \preccurlyeq est total.

- Il suffit de construire la bijection strictement croissante, ensuite on prend le même ordre que les images. Suivons la marche à suivre de l'hérédité : on envoie un élément maximal sur $n + 1$ (ici, 10), et on itère le procédé. 7 est un élément maximal donc on met 7 « à la fin ». 8 est un élément maximal de ce qui reste (i.e. en enlevant 7) donc on met 8 avant 7. 6 est ensuite un élément maximal de ce qui reste etc. On en déduit un ordre total sur $\llbracket 1; 10 \rrbracket$ qui prolonge la divisibilité mais différent de l'ordre usuel :



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 :

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

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

Correction :

1. Montrons que c'est une relation d'équivalence.

- Soit $(u_n) \in E$. Alors, pour tout n , $u_n \neq 0$ donc $u_n/u_n = 1 \xrightarrow{n \rightarrow +\infty} 1 : (u_n) \sim (u_n)$, \sim est réflexive.
- Soient (u_n) et (v_n) dans E telles que $(u_n) \sim (v_n)$. Alors $u_n/v_n \xrightarrow{n \rightarrow +\infty} 1$ si bien que $v_n/u_n \xrightarrow{n \rightarrow +\infty} 1/1 = 1 : (v_n) \sim (u_n)$, \sim est symétrique.
- Soient $(u_n), (v_n)$ et (w_n) dans E telles que $(u_n) \sim (v_n)$ et $(v_n) \sim (w_n)$. Dès lors, $u_n/v_n \xrightarrow{n \rightarrow +\infty} 1$ et $v_n/w_n \xrightarrow{n \rightarrow +\infty} 1$ si bien que

$$\frac{u_n}{w_n} = \frac{u_n}{v_n} \times \frac{v_n}{w_n} \xrightarrow{n \rightarrow +\infty} 1$$

i.e. $(u_n) \sim (w_n) : \sim$ est transitive.

C'est donc bien une relation d'équivalence.

2. Soient donc (u_n) et (v_n) deux suites équivalentes convergentes. Notons L la limite de (u_n) . Alors $v_n/u_n \xrightarrow{n \rightarrow +\infty} 1$ donc

$$v_n = \frac{v_n}{u_n} \times u_n \xrightarrow{n \rightarrow +\infty} 1 \times L = L$$

donc (v_n) a la même limite que (u_n) . Cependant, la réciproque est fautive : la suite (u_n) de terme général $1/n$ et la suite (v_n) de terme général $1/n^2$ ont la même limite, 0, mais ne sont pas équivalentes car le quotient ne tend pas vers 1.

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.

Correction : Montrons que c'est une relation d'équivalence.

- Soit $z \in \mathbb{C}$. Alors $z^n = z^n$ donc $z R z : R$ est transitive.
- Soit $(z_1, z_2) \in \mathbb{C}^2$ tel que $z_1 R z_2$. Alors $z_1^n = z_2^n$ donc $z_2^n = z_1^n$ si bien que $z_2 R z_1 : R$ est symétrique.
- Soit $(z_1, z_2, z_3) \in \mathbb{C}^3$ tel que $z_1 R z_2$ et $z_2 R z_3$. En d'autres termes, $z_1^n = z_2^n$ et $z_2^n = z_3^n$ donc $z_1^n = z_3^n$ c'est-à-dire que $z_1 R z_3 : R$ est transitive.

En d'autres termes, R est bien une relation d'équivalences. Soit $z \in \mathbb{C}$, soit $\alpha = z^n$. On cherche le nombre de complexes y tels que $y^n = \alpha$, c'est-à-dire le nombre de racines n -ièmes de $\alpha = z^n$. D'après le chapitre 7, si $\alpha = 0$, α n'admet qu'une seule racine n -ième : lui-même, et si $\alpha \neq 0$, α admet n racines n -ièmes. En conclusion, si $z = 0$, alors z est tout seul dans sa classe d'équivalence, sinon la classe d'équivalence de z contient n éléments.

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.

Correction : Montrons que c'est une relation d'équivalence.

- Soit $f \in \mathbb{R}^{\mathbb{R}}$. Alors, si on pose $\varepsilon = 1 > 0$, pour tout $x \in [-\varepsilon; \varepsilon]$, $f(x) = f(x) : f \sim f$, \sim est réflexive.
- Soient f et g dans $\mathbb{R}^{\mathbb{R}}$ telles que $f \sim g$. Alors il existe $\varepsilon > 0$ tel que, pour tout $x \in [-\varepsilon; \varepsilon]$, $f(x) = g(x)$ donc $g(x) = f(x)$, si bien que $g \sim f : \sim$ est symétrique.

- Soient f, g et h dans $\mathbb{R}^{\mathbb{R}}$ telles que $f \sim g$ et $g \sim h$. Dès lors, il existe $\varepsilon_1 > 0$ tel que, pour tout $x \in [-\varepsilon_1; \varepsilon_1]$, $f(x) = g(x)$ et il existe $\varepsilon_2 > 0$ tel que, pour tout $x \in [-\varepsilon_2; \varepsilon_2]$, $g(h) = h(x)$. Posons $\varepsilon = \min(\varepsilon_1, \varepsilon_2) > 0$. Pour tout $x \in [-\varepsilon; \varepsilon]$, $f(x) = g(x)$ et $g(x) = h(x)$ donc $f(x) = h(x)$: $f \sim g$, \sim est transitive. C'est donc bien 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.

Correction : Montrons que c'est une relation d'équivalence.

- Soit $x \in \mathbb{Z}$. Alors $x + x = 2x$ est pair donc xRx : R est réflexive.
- Soient x et y dans \mathbb{Z} tels que xRy . Alors $x + y$ est pair donc $y + x$ est pair, c'est-à-dire que yRx : R est symétrique.
- Soient x, y, z tels que xRy et yRz : alors $x + y$ et $y + z$ sont pairs. Dès lors, x et y ont la même parité, et y et z ont la même parité, si bien que x et z ont la même parité donc $x + z$ est pair : xRz , R est transitive.

C'est donc bien une relation d'équivalence. Soit $x \in \mathbb{Z}$. Soit $y \in \mathbb{Z}$. Alors xRy si et seulement si $x + y$ est pair, si et seulement si x et y ont la même parité. En d'autres termes, la classe d'équivalence de x est l'ensemble des entiers de même parité que x . En conclusion, il y a deux classes d'équivalence : l'ensemble des nombres pairs, et l'ensemble des nombres impairs.

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

Correction : En d'autres termes, deux suites sont en relation si et seulement si elles sont égales à partir d'un certain rang. Prouvons que c'est une relation d'équivalence.

- Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$. Alors $n_0 = 0$ convient : pour tout $n \geq 0$, $u_n = u_n$: $(u_n) \approx (u_n)$, \approx est réflexive.
- Soient (u_n) et (v_n) deux suites telles que $(u_n) \approx (v_n)$. Il existe alors n_0 tel que pour tout $n \geq n_0$, $u_n = v_n$. Ainsi, pour tout $n \geq n_0$, $v_n = u_n$ donc $(v_n) \approx (u_n)$: \approx est symétrique.
- Soient (u_n) , (v_n) et (w_n) trois suites telles que $(u_n) \approx (v_n)$ et $(v_n) \approx (w_n)$. Il existe donc n_0 tel que, pour tout $n \geq n_0$, $u_n = v_n$ et il existe n_1 tel que, pour tout $n \geq n_1$, $v_n = w_n$. Soit $n_2 = \max(n_0, n_1)$. Pour tout $n \geq n_2$, $u_n = v_n$ et $v_n = w_n$ donc $u_n = w_n$ si bien que $(u_n) \approx (w_n)$: \approx est transitive, 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.

- Soit $f \in \mathbb{R}^{\mathbb{R}}$. Alors, si on pose $\varphi = \text{Id}_{\mathbb{R}}$ qui est bien une bijection de \mathbb{R} dans \mathbb{R} , on a $f = \varphi^{-1} \circ f \circ \varphi$ c'est-à-dire que $f \sim f$: \sim est réflexive.
- Soient f et g dans $\mathbb{R}^{\mathbb{R}}$ telles que $f \sim g$. Alors il existe $\varphi \in S_{\mathbb{R}}$ telle que $f = \varphi^{-1} \circ g \circ \varphi$. En composant à gauche par φ et à droite par φ^{-1} , on obtient $(\varphi \circ \varphi^{-1}) = \varphi^{-1} \circ \varphi$ car φ est bijective) : $g = \varphi \circ f \circ \varphi^{-1}$. Or, $\varphi = (\varphi^{-1})^{-1}$, si bien qu'en posant $\psi = \varphi^{-1}$, on a bien $\psi \in S_{\mathbb{R}}$ et $g = \psi^{-1} \circ f \circ \psi$ donc $g \sim f$: \sim est symétrique.
- Soient f, g et h dans $\mathbb{R}^{\mathbb{R}}$ telles que $f \sim g$ et $g \sim h$. Dès lors, il existe $\varphi \in S_{\mathbb{R}}$ et $\psi \in S_{\mathbb{R}}$ telles que $g = \varphi^{-1} \circ f \circ \varphi$ et $h = \psi^{-1} \circ g \circ \psi$ si bien que

$$h = \psi^{-1} \circ \varphi^{-1} \circ f \circ \varphi \circ \psi$$

Or (cf. chapitre 3), $\psi^{-1} \circ \varphi^{-1} = (\varphi \circ \psi)^{-1}$ (voir l'anecdote du trésor) si bien que

$$h = (\varphi \circ \psi)^{-1} \circ f \circ \varphi \circ \psi$$

Or, ψ et φ sont des bijections donc, par composition, $\varphi \circ \psi$ est aussi une bijection de \mathbb{R} dans \mathbb{R} donc appartient à $S_{\mathbb{R}}$. Finalement, $f \sim h$, h est transitive.

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

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

Montrer que c'est une relation d'équivalence.

Correction :

- Soit $f \in \mathbb{R}^E$. Alors, si on pose $\alpha = \beta = 1$ qui sont bien strictement positifs, on a bien : $\forall x \in E, \alpha f(x) \leq f(x) \leq \beta f(x)$, c'est-à-dire que $f \sim f$: \sim est réflexive.

- Soient f et g dans \mathbb{R}^E telles que $f \sim g$. Alors il existe α et β strictement positifs tels que, pour tout $x \in E$, $\alpha g(x) \leq f(x) \leq \beta g(x)$. Il en découle (α et β étant strictement positifs) que $g(x) \leq \frac{1}{\alpha} \times f(x)$ et $\frac{1}{\beta} \times f(x) \leq g(x)$, c'est-à-dire que :

$$\forall x \in E, \frac{1}{\beta(x)} \times f(x) \leq g(x) \leq \frac{1}{\alpha} \times f(x)$$

$1/\alpha$ et $1/\beta$ étant strictement positifs, on en déduit que $g \sim f : \sim$ est symétrique.

- Soient f, g et h dans \mathbb{R}^E telles que $f \sim g$ et $g \sim h$. Dès lors, il existe $\alpha_1, \beta_1, \alpha_2, \beta_2$ strictement positifs tels que :

$$\forall x \in E, \alpha_1 g(x) \leq f(x) \leq \beta_1 g(x) \quad \text{et} \quad \alpha_2 h(x) \leq g(x) \leq \beta_2 h(x)$$

Soit $x \in E$. $\alpha_2 h(x) \leq g(x)$ donc $\alpha_1 \alpha_2 h(x) \leq \alpha_1 g(x) \leq f(x)$, et $g(x) \leq \beta_2 h(x)$ donc $f(x) \leq \beta_1 g(x) \leq \beta_1 \beta_2 h(x)$ donc

$$\alpha_1 \alpha_2 h(x) \leq f(x) \leq \beta_1 \beta_2 h(x)$$

$\alpha_1 \alpha_2$ et $\beta_1 \beta_2$ étant strictement positifs, cela signifie que $f \sim h : \sim$ est transitive, 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 : $\forall x \in \mathbb{R}, \exists \varepsilon > 0, \forall y \in \mathbb{R}, |x - y| \leq \varepsilon \Rightarrow x \sim y$.

Correction :

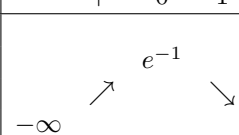
1. Montrons que tous les réels sont équivalents. Soit $(x, y) \in \mathbb{R}^2$. Sans perte de généralité, supposons $x \leq y$. Par hypothèse, $x \sim x + \varepsilon$, $x + \varepsilon \sim x + 2\varepsilon$ et pour tout n , $x + n\varepsilon \sim x + (n+1)\varepsilon$ (même pas besoin de récurrence : on applique la propriété de l'énoncé avec $x + n\varepsilon$ à la place de x et $x + (n+1)\varepsilon$ à la place de y). Par transitivité, tous les $x + n\varepsilon$ sont équivalents à x . Soit n tel que $x + n\varepsilon \leq y < x + (n+1)\varepsilon$ (de façon explicite, $n = \lfloor (y - x)/\varepsilon \rfloor$ mais ce n'est pas indispensable). Alors $x + n\varepsilon \sim y$ et par transitivité, $x \sim y$. Ainsi, tous les réels sont équivalents, il n'y a qu'une classe d'équivalence : \mathbb{R} tout entier.
2. On prouve que le résultat est encore valable avec une borne supérieure comme dans l'exercice 67 du chapitre 13 : soient x et y deux réels, avec $x \leq y$. Notons $A = \{t \in [x; y] \mid xRt\}$. Alors A est non vide car contient x (par réflexivité de R) et est majoré par y donc admet une borne supérieure α . Par hypothèse, il existe $\varepsilon > 0$ tel que, pour tout $t \in \mathbb{R}$: $|t - \alpha| \leq \varepsilon \Rightarrow tR\alpha$. Par caractérisation de la borne supérieure (pas par caractérisation séquentielle!), il existe $t \in A$ tel que $|t - \alpha| \leq \varepsilon$ si bien que $tR\alpha$. Or, $t \in A$ donc xRt donc, par transitivité, $xR\alpha$. Si $\alpha = y$ alors xRy , sinon il existe $t \in]\alpha; y]$ tel que $|t - \alpha| \leq \varepsilon$ si bien que αRt et, par transitivité, xRt ce qui contredit la définition de α : on en déduit que $\alpha = y$ donc xRy ce qui permet de conclure.

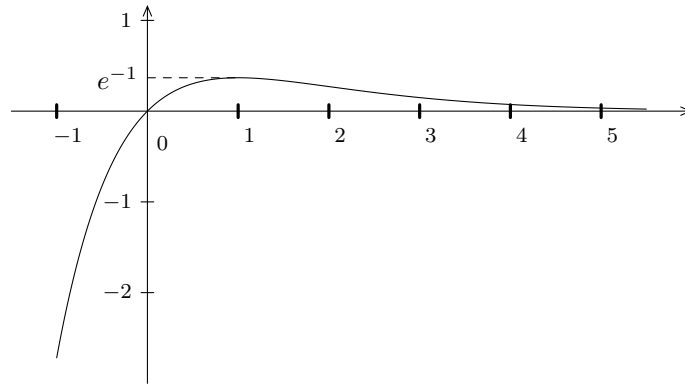
Exercice 28 : ★★

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 : $x \sim y \iff \frac{\ln(x)}{y} = \frac{\ln(y)}{x}$. Montrer que c'est une relation d'équivalence et donner le cardinal des classes d'équivalences.

Correction :

1. Tout d'abord : $xRy \iff f(x) = f(y)$ où $f : t \mapsto xe^{-x}$, et le fait que R soit une relation d'équivalence est immédiat. On peut généraliser à toute fonction $f : E \rightarrow F$, on appelle alors R la relation d'équivalence associée à f (cf. cours). Soit $x \in \mathbb{R}$. On cherche le cardinal de $\text{cl}(x) = \{y \in \mathbb{R} \mid f(y) = f(x)\}$. Par définition, $\text{cl}(x)$ est l'ensemble des réels y dont l'image vaut $f(x)$, c'est-à-dire l'ensemble des antécédents de $f(x)$ par f . On cherche donc le nombre d'antécédents de $f(x)$ (cf. cours pour un dessin, avec l'exemple du cosinus) : donnons le tableau de variations de f .

	$-\infty$	1	$+\infty$
$g'(x)$	+	0	1
g			



- Si $x \leq 0$ alors $f(x) \leq 0$. Notons $y = f(x) \leq 0$. $f(t) \xrightarrow{t \rightarrow -\infty} -\infty$ et $f(0) = 0$, f est continue et strictement croissante sur \mathbb{R}_- : d'après le théorème de la bijection, $y = f(x)$ a un unique antécédent (x) sur \mathbb{R}_- , et puisque f est strictement positive sur \mathbb{R}_+^* , $y = f(x)$ n'a aucun antécédent sur \mathbb{R}_+^* (pas besoin de TVI ici !!). Dès lors, $f(x)$ a un unique antécédent (égal à x) : si $x \leq 0$, $\text{cl}(x)$ est de cardinal 1.
 - Si $x = 1$, $f(x) = e^{-1}$ et on sait que e^{-1} est atteint une seule fois sur \mathbb{R} . Si $x = 1$, $\text{cl}(x)$ est de cardinal 1.
 - Si $x \in]0; 1[\cup]1; +\infty[$ alors $f(x) \in]0; e^{-1}[$. De même que ci-dessus, $y = f(x)$ est atteint deux fois sur \mathbb{R} donc il existe deux réels t (l'un d'entre eux étant égal à x) tels que $f(t) = f(x)$: $\text{cl}(x)$ est de cardinal 2.
2. Il suffit d'écrire que xRy si et seulement si $x \ln(x) = y \ln(y)$. Le fait que ce soit une relation d'équivalence est alors immédiat. On étudie alors la fonction définie sur \mathbb{R}_+^* par $f(t) = t \ln(t)$. On prouve alors que si $x = 1/e$, $\text{cl}(x)$ est de cardinal 1, si $x \in]0; 1/e[\cup]1/e; 1[$, $\text{cl}(x)$ est de cardinal 2, et si $x \geq 1$, $\text{cl}(x)$ est de cardinal 1.

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 .

Correction : Deux suites sont en relation si, pour tout n , un terme de v finit par être plus petit que u_n et un terme de u finit par passer sous v_n , c'est-à-dire qu'on ne peut pas avoir un terme d'une suite strictement supérieur à tous les termes de l'autre suite.

1. Montrons que c'est une relation d'équivalence mais pas une relation d'ordre.
 - Soit (u_n) une suite. Soit $n \in \mathbb{N}$ et soit $p = q = n$. Alors $(u_p \leq u_n)$ et $(u_q \leq u_n)$ donc $(u_n)R(u_n)$: (u_n) est réflexive.
 - Soient (u_n) et (v_n) deux suites telles que $(u_n) \leq (v_n)$. Soit $n \in \mathbb{N}$. Il existe donc p et q supérieurs à n tels que $(u_p \leq v_n)$ et $(v_q \leq u_n)$ donc il existe q et p supérieurs à n tels que $(v_q \leq u_n)$ et $(u_p \leq v_n)$, c'est-à-dire que $(v_n)R(u_n)$: R est symétrique.
 - Cependant, si (u_n) est la suite de terme général $(-1)^n$ et si (v_n) est la suite de terme général $(-1)^{n+1}$ alors, pour tout n , en posant $p = n + 1$, on a $u_p = (-1)^n \leq v_n = (-1)^{n+1}$, et si on pose $q = n + 1$, on a $v_q = (-1)^{n+2} = (-1)^n \leq u_n = (-1)^n$. Il en découle que $(u_n)R(v_n)$ donc, par symétrie, $(v_n)R(u_n)$ mais les deux suites ne sont pas égales : R n'est pas antisymétrique, ce n'est pas une relation d'ordre.
 - Soient (u_n) , (v_n) et (w_n) trois suites telles que $(u_n)R(v_n)$ et $(v_n)R(w_n)$. Soit $n \in \mathbb{N}$. Il existe p et q supérieurs à n tels que $u_p \leq v_n$ et $v_q \leq w_n$. Or, $(v_n)R(w_n)$ donc :

$$\forall \text{truc} \in \mathbb{N}, \exists r, s \geq \text{truc}, (v_r \leq w_{\text{truc}}) \text{ et } (w_s \leq v_{\text{truc}})$$

En prenant $\text{truc} = q$: il existe $s \geq q \geq n$ tel que $w_s \leq v_q \leq u_n$. Or (toujours car $(v_n)R(w_n)$), il existe $k \geq n$ tel que $v_k \leq w_n$ et puisque $(u_n)R(v_n)$, il existe $r \geq k \geq n$ tel que $u_r \leq v_k \leq w_n$ si bien que $(u_n)R(w_n)$, d'où la transitivité, c'est bien une relation d'équivalence.

2. Soit donc (u_n) une suite constante égale à $\lambda \in \mathbb{R}$. Soit (v_n) une suite.

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

En d'autres termes, (v_n) est en relation avec (u_n) si et seulement si tous les termes de (v_n) sont supérieurs à λ et si, pour tout n , il existe $q \geq n$ tel que $v_q \leq \lambda$. Encore en d'autres termes : (v_n) est en relation avec (u_n) si et seulement si tous les termes de la suite (v_n) sont supérieurs à λ et s'il existe une infinité de termes inférieurs donc égaux (car ils sont supérieurs) à λ . En conclusion : les suites équivalentes à (u_n) , suite constante égale à λ sont les suites supérieurs à (u_n) admettant une infinité de termes égaux à λ .

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

$$\varphi : \begin{cases} \mathbb{N}^2 / \sim & \rightarrow & \mathbb{Z} \\ \overline{(a, b)} & \mapsto & a - b \end{cases}$$

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.

Correction :

1. Montrons que c'est une relation d'équivalence.
 - Soit $(a, b) \in \mathbb{N}^2$. Alors $a + b = b + a$ donc $(a, b) \sim (a, b)$, \sim est réflexive.
 - Soient (a, b) et (c, d) tels que $(a, b) \sim (c, d)$. Alors $a + d = b + c$ donc $b + c = a + d$ si bien que $(c, d) \sim (a, b)$: \sim est symétrique.
 - Soient (a, b) , (c, d) , (e, f) dans \mathbb{N}^2 tels que $(a, b) \sim (c, d)$ et $(c, d) \sim (e, f)$. Alors $a + d = b + c$ donc $a - b = c - d$ et $c + f = d + e$ donc $c - d = e - f$ donc $a - b = e - f$ donc $a + f = e + b$ c'est-à-dire que $(a, b) \sim (e, f)$: \sim est transitive.

\sim est donc une relation d'équivalence.
2. Montrons que cette fonction est bien définie, c'est-à-dire que si $(a, b) \sim (c, d)$, l'image est la même, l'image est la même peu importe le représentant de la classe d'équivalence choisi. Or, si $(a, b) \sim (c, d)$, alors $a + d = c + b$ donc $a - b = c - d$ donc la différence est la même, peu importe le représentant choisi dans la classe d'équivalence, la différence est la même, donc $f(\overline{(a, b)}) = f(\overline{(c, d)})$: f est bien définie. Montrons qu'elle est bijective.

Soit $n \in \mathbb{Z}$. Alors $n = f(\overline{(n, 0)})$ donc f est surjective. Soient $\overline{(a, b)}$ et $\overline{(c, d)}$ deux classes d'équivalence distinctes, c'est-à-dire que $a + d \neq c + b$ i.e. $a - b \neq c - d$. Alors $f(\overline{(a, b)}) = a - b \neq c - d = f(\overline{(c, d)})$: f est injective donc bijective.

Exercice 31 - Construction de \mathbb{R} à partir de \mathbb{Q} : ★★★★★

On note $\widetilde{\mathcal{P}}(\mathbb{Q})$ l'ensemble des parties de \mathbb{Q} non vides et majorées. Soit la relation \equiv définie sur $\widetilde{\mathcal{P}}(\mathbb{Q})$ 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 $(X, Y) \in \widetilde{\mathcal{P}}(\mathbb{Q})^2$. Montrer que : $X \equiv Y \iff \sup_{\mathbb{R}}(X) = \sup_{\mathbb{R}}(Y)$.
3. En déduire une bijection entre $\widetilde{\mathcal{P}}(\mathbb{Q}) / \equiv$ 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} .

Correction :

1. • Soit X une partie non vide majorée de \mathbb{Q} . Soit $x \in X$ et soit $\varepsilon \in \mathbb{Q}_+^*$. Alors $x - \varepsilon \leq x$ donc il existe $y \in X$, $x - \varepsilon \leq y$ (en prenant $x = y$). Idem pour l'autre (en prenant $y = x$). Ainsi :

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

c'est-à-dire que $X \equiv X$: \equiv est réflexive.

- Soient X et Y deux parties non vides majorées de \mathbb{Q} telles que $X \equiv Y$. Alors :

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

Ainsi :

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

c'est-à-dire que $Y \equiv X$: \equiv est symétrique.

- Soient X, Y, Z trois parties non vides majorées de \mathbb{Q} telles que $X \equiv Y$ et $Y \equiv Z$. Alors :

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

et

$$(\forall y \in Y, \forall \varepsilon \in \mathbb{Q}_+^*, \exists z \in Z, y - \varepsilon \leq z) \text{ et } (\forall z \in Z, \forall \varepsilon \in \mathbb{Q}_+^*, \exists y \in Y, z - \varepsilon \leq y)$$

Soient donc $x \in X$ et $\varepsilon \in \mathbb{Q}_+^*$. Il existe $y \in Y$ tel que $x - \varepsilon/2 \leq y$ (le résultat étant vrai pour tout $\varepsilon > 0$, il est vrai pour $\varepsilon/2$). De plus, il existe $z \in Z$ tel que $y - \varepsilon/2 \leq z$ si bien que $x - \varepsilon \leq z$. On montre de même que, pour tout $z \in Z$, pour tout $\varepsilon > 0$, il existe $x \in X$ tel que $z - \varepsilon \leq x$ si bien que $X \equiv Z : \equiv$ est transitive, c'est une relation d'équivalence.

2. Soit $(X, Y) \in \widetilde{\mathcal{P}}(\mathbb{Q})^2$. Supposons que $X \equiv Y$. Les sup en question existent bien car on a des parties non vides majorées. Notons s_x et s_y respectivement la borne supérieure de x et la borne supérieure de y . Soit $\varepsilon > 0$. Tout d'abord, puisque $X \equiv Y$, alors pour tout $x \in X$ et tout $\varepsilon > 0$, il existe $y \in Y$ tel que $x - \varepsilon \leq y$. ε étant quelconque strictement positif, on en déduit que $x \leq y$ donc y est un majorant de x donc $\sup(X) \leq y$. Ceci étant vrai pour tout y , il vient : $\sup(X) \leq \sup(Y)$, et par symétrie des rôles on en déduit que $\sup(Y) \leq \sup(X)$, d'où l'égalité.

Réciproquement, supposons que $\sup(X) = \sup(Y)$. Soit $x \in X$ et soit $\varepsilon > 0$. Par caractérisation séquentielle de la borne supérieure, il existe $y \in Y$ tel que $\sup(Y) - \varepsilon < y \leq \sup(Y)$. Or, $\sup(Y) = \sup(X)$ donc $x \leq \sup(X)$. Finalement, $x - \varepsilon \leq \sup(X) - \varepsilon < y$. On a donc montré :

$$\forall x \in X, \forall \varepsilon \in \mathbb{Q}_+^*, \exists y \in Y, x - \varepsilon \leq y$$

L'autre assertion se démontre par symétrie des rôles, c'est-à-dire que $X \equiv Y$. D'où l'équivalence.

3. Soit f la fonction qui à $\text{cl}(X)$ associe $\sup(X)$. La question précédente prouve que f est bien définie (deux parties équivalentes ont même borne supérieure, l'image ne dépend pas du représentant choisi). De plus, toujours d'après la question précédente, f est injective : à deux classes d'équivalence différentes correspondent deux bornes supérieures différentes. Enfin, soit $x \in \mathbb{R}$. Par caractérisation séquentielle de la densité, il existe une suite (x_n) dans \mathbb{Q} qui converge vers x , et on peut même s'arranger pour prendre $x_n \leq x$ pour tout n (prendre $x_n = \lfloor 10^n x \rfloor / 10^n$). En prenant $E = \{x_n \mid n \in \mathbb{N}\}$, on a bien $\sup(E) = x$ donc $f(\overline{E}) = x : f$ est surjective.

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 tes 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.

Correction : Un tel classement est totalement déterminé par :

- Le choix des 5 garçons : $\binom{70}{5}$ choix possibles (on ne peut pas prendre plusieurs fois le même, et l'ordre ne compte pas encore).
- Le choix des 5 filles : $\binom{90}{5}$ choix possibles.
- Le classement de ces 10 élèves : $10!$ choix possibles.

D'après le principe multiplicatif, il y a donc $10! \times \binom{70}{5} \times \binom{90}{5}$ tels classements possibles.

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.

Correction :

1. Un tel jury est totalement déterminé par :

- Le choix du littéraire : $\binom{7}{3}$ (l'ordre ne compte pas et on ne peut pas prendre plusieurs fois le même).
- Le choix du scientifique : $\binom{5}{2}$ (l'ordre ne compte pas et on ne peut pas prendre plusieurs fois le même).

D'après le principe multiplicatif, il y a donc $\binom{7}{3} \times \binom{5}{2}$ choix possibles.

2. Rien ne change pour les scientifiques, mais il n'y a plus que deux places disponibles pour les littéraires, si bien qu'il y a $\binom{6}{2}$ choix possibles pour les littéraires. Le nombre de jurys est donc $\binom{6}{2} \times \binom{5}{2}$.

3. Rien ne change pour les littéraires. Pour les scientifiques, la seule option impossible est que les deux scientifiques soient ensembles : il suffit donc de la retirer, c'est-à-dire qu'il y a $\binom{5}{2} - 1$ choix possibles pour les scientifiques, si bien que le nombre de jurys est $\binom{7}{3} \times \left(\binom{5}{2} - 1 \right)$.
4. Rien ne change pour les scientifiques. Pour les littéraires, là c'est un peu plus compliqué puisqu'il y a plusieurs configurations impossibles : celles avec les deux littéraires et un troisième larron. Ce choix de littéraire est totalement déterminé par le choix du troisième littéraire, il y a 5 (ou, ce qui revient au même, $\binom{5}{1}$) choix possibles pour ce troisième littéraire. Finalement, il y a $\binom{7}{3} - 5$ choix possibles pour les littéraires, si bien qu'il y a $\binom{5}{2} \times \left(\binom{7}{3} - 5 \right)$ jurys possibles.

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 $\tilde{u} = (u_n, \dots, u_1)$. u est appelé un *palindrome* si $u = \tilde{u}$. 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 ?

Correction :

1. D'après le cours, A^n est de cardinal p^n donc il y a p^n mots de longueur n . Toujours d'après le cours, il y a $\frac{p!}{(p-n)!} = p(p-1) \cdots (p-n+1)$ mots de longueur n formés de n lettres distinctes.
2. Tout dépend de si n est pair ou impair. Si n est pair, un palindrome est entièrement déterminé par $u_1, \dots, u_{n/2}$, on connaîtra ensuite les autres lettres (on aura $u_n = u_1, u_{n-1} = u_2$ etc.) et il y a p choix possibles pour chaque lettre donc il y a $p^{n/2}$ palindromes de longueur n . Si n est impair, il ne faut pas oublier la lettre centrale : un palindrome de longueur n est entièrement déterminé par $u_1, \dots, u_{\frac{n+1}{2}}$ donc il y a $p^{\frac{n+1}{2}}$ palindromes de longueur n .
3. Un tel mot est entièrement déterminé par :
 - la première lettre : p choix possibles.
 - la deuxième lettre : $p-1$ choix possibles (toutes sauf la première).
 - la troisième lettre : $p-1$ choix possibles (toutes sauf la deuxième, mais on peut reprendre la première).
 - et ainsi de suite, il y a $p-1$ choix pour toutes les lettres sauf la première.
 Finalement, il y a $p \times (p-1)^{n-1}$ mots de longueur n 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 ?

Correction :

1. Pour choisir une immatriculation, on peut :
 - choisir les lettres du bloc de gauche : sans les deux séries et les lettres interdites, il y a 23 choix pour la première puis (indépendamment du choix de la première lettre) il y a 23 choix pour la deuxième. Par principe multiplicatif, il y a donc 23^2 choix pour les deux premières lettres. Il y a donc $23^2 - 2$ choix pour le bloc de gauche.
 - puis (indépendamment du bloc de gauche choisi) choisir les chiffres : cela consiste à choisir un nombre entre 001 et 999. Il y a 999 possibilités.
 - puis (indépendamment du bloc et des chiffres choisis) choisir les lettres du bloc de droite : il y a $23^2 - 1$ choix pour le bloc de gauche (les 23^2 couples possibles moins la série SS).
 Par principe multiplicatif, il y a donc $(23^2 - 2) \times 999 \times (23^2 - 1) = 277977744$ plaques d'immatriculation possibles.
2. Pour choisir une telle immatriculation :
 - Le choix de la première lettre, 23 choix possibles, et de la deuxième, 22 (différente de la première) : il y a 23×22 choix possibles pour le bloc de gauche (plus besoin de retirer SS et WW car les lettres sont distinctes).
 - Il y a $10 \times 9 \times 8$ possibilités pour le bloc de chiffres.

- Il y a 21 choix pour la première lettre de droite (on retire les lettres de gauche) et 20 pour la suivante. Encore une fois, impossible d'avoir *SS* donc 21×20 choix pour le membre de droite.
- Finalement, il y a $23 \times 22 \times 10 \times 9 \times 8 \times 21 \times 20$ telles immatriculations.

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 $k \in \llbracket 1 ; 6 \rrbracket$. Combien y a-t-il d'éléments dont le premier 4 apparaît en k -ième position ?

Correction :

1. Un tel entier peut être assimilé à un 6-uplet (a, b, c, d, e, f) d'éléments de $\llbracket 1 ; 9 \rrbracket$ donc E peut être assimilé à $\llbracket 1 ; 9 \rrbracket^6$ si bien que $\text{card}(E) = 9^6$.
2. Comme dans l'exercice 3 : $\frac{9!}{3!} = 9 \times 8 \times 7 \times 6 \times 5 \times 4$.
3. Un élément est impair si et seulement s'il se termine par 1, 3, 5, 7, 9 donc il y a 5 choix pour le dernier chiffre : il y a donc $9^5 \times 5$ éléments impairs dans E .
4. 2 choix possibles pour chaque chiffre (2 ou 3) donc il y a 2^6 tels nombres.
5. Il y a 8 choix possibles pour les chiffres en position $1, \dots, k-1$ et 9 pour les entiers en position $k+1, \dots, 6$ (et l'entier en position k est un 4) donc il y a $8^{k-1} \times 9^{6-k}$ entiers de cette forme.

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 ?

Correction : Il y a 2 anagrammes du mot Ni et $7!$ anagrammes du mot knights car toutes les lettres sont distinctes. Pour shrubbery, il y a 2 b et 2 r. On peut faire comme en classe : il y a $9!$ façons de permuter les 9 lettres, mais plusieurs donnent le même mot : puisqu'il y a deux b, il y a $2! = 2$ façons de permuter les b au sein d'un même mot, donc pour chaque mot, il y a 2 permutations des e qui donnent ce mot, donc il y a 2 permutations qui donnent le même mot, qui ne comptent que pour un mot. Pour avoir le nombre total d'anagrammes, il faut donc diviser par 2, et idem pour le r, si bien qu'il y a $\frac{9}{2 \times 2}$ anagrammes du mot shrubbery. On peut aussi raisonner de la façon suivante : donner une anagramme est comme jouer au pendu, il faut mettre les 9 lettres sur les 9 emplacements ci-dessous :

— — — — — — — — —

Il y a $\binom{9}{2}$ choix pour placer les deux b (l'ordre ne compte pas car, si on place un b à un endroit et un b à un autre, on peut intervertir les deux b et cela ne changera rien) :

— — $\frac{b}{-}$ — — — $\frac{b}{-}$ — —

Il reste 7 emplacements pour les r : $\binom{7}{2}$ choix possibles :

— — $\frac{b}{-}$ — $\frac{r}{-}$ — $\frac{b}{-}$ $\frac{r}{-}$ —

et ainsi de suite jusqu'à avoir rempli les emplacements : $\binom{5}{1}$ choix pour le s, $\binom{4}{1}$ choix pour le h, $\binom{3}{1}$ choix pour le y, $\binom{2}{1}$ choix pour le e, et $\binom{1}{1}$ choix pour le u puisqu'il ne reste qu'un emplacement. Par principe multiplicatif, le nombre d'anagrammes de shrubbery est :

$$\binom{9}{2} \times \binom{7}{2} \times \binom{5}{1} \times \binom{4}{1} \times \binom{3}{1} \times \binom{2}{1}$$

et en donnant la valeur des coefficients binomiaux avec des factorielles et en simplifiant, on retrouve évidemment le même résultat. Enfin, pour Ekke Ekke Ekke Ekke Ptang Zoo Boing : il y a :

- 29 lettres.
- 8 e.
- 8 k.
- 3 o.
- 2 g.

- 2 n.
- 1 z.
- 1 b.
- 1 i.
- 1 p.
- 1 t.
- 1 a.

On peut soit raisonner comme dans le cours : $29!$ permutations des lettres, mais plusieurs donnent le même mot. Les 8 e ne comptent que pour 1 donc il faut diviser par $8!$, et idem pour tous les autres, si bien que le nombre d'anagrammes recherché est

$$\frac{29!}{8!8!3!2!2!}$$

ou on joue au pendu : le nombre recherché est

$$\binom{29}{8} \times \binom{21}{8} \times \binom{13}{3} \times \binom{10}{2} \times \binom{8}{2} \times \binom{6}{1} \times \binom{5}{1} \times \binom{4}{1} \times \binom{3}{1} \times \binom{2}{1} \times 1$$

et en écrivant les coefficients binomiaux avec des factorielles on trouve évidemment la même chose.

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 ?

Correction :

1. On cherche le nombre de parties de $E \setminus \{a; b\}$, ensemble à $n - 2$ éléments : il y a donc 2^{n-2} telles parties.
2. Si on note P_a l'ensemble des parties ne contenant pas a et P_b l'ensemble des parties ne contenant pas b , alors

$$\text{card}(P_a \cup P_b) = \text{card}(P_a) + \text{card}(P_b) - \text{card}(P_a \cap P_b)$$

si bien que le nombre voulu est $2^{n-1} + 2^{n-1} - 2^{n-2} = 2^n - 2^{n-2}$.

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

Correction : Il faut piocher 7 x dans les 12 parenthèses : $\binom{12}{7}$ choix possibles. Il faut aussi piocher 3 fois le terme $2y$ dans les 5 termes restants : $\binom{5}{3}$ choix possibles. Ensuite, il n'y a plus qu'un choix pour les $3z$. Cependant, il ne faut pas oublier qu'on choisit $2y$ et $3z$: le 2 est aussi à la puissance 3 et le z à la puissance 2. Finalement, le coefficient cherché est $\binom{12}{7} \times \binom{5}{3} \times 2^3 \times 3^2$.

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) ?

Correction : Soit $k \in \llbracket 3; 11 \rrbracket$ le nombre d'ingrédients choisis. Une pizza à k ingrédients est entièrement déterminée par :

- la taille : 3 choix possibles.
- la pâte : 4 choix possibles.

- la base : 3 choix possibles.
- les ingrédients : $\binom{35}{k}$ choix possibles.

Par principe multiplicatif, cela fait $3 \times 4 \times 3 \times \binom{35}{k} = 36 \times \binom{35}{k}$ choix possibles. Par principe additif (les pizzas avec 3, 4, ..., 11 ingrédients sont deux à deux incompatibles, si on veut), le nombre total de pizzas est

$$\sum_{k=3}^{11} 36 \times \binom{35}{k}$$

Avec une calculatrice, on trouve que le nombre total de pizzas est 25 332 472 548 : Domino's aurait même pu dire qu'il y a plus d'un milliard de possibilités ! Mais les ingrédients proposés sont peut-être moins nombreux dans certaines pizzerias... ou ils n'ont peut-être tout simplement pas voulu se casser la tête !

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

Correction : Chaque sommet est une extrémité de $n-3$ diagonales (on exclut les segments reliant un sommet à lui-même et à ses deux voisins immédiats, ceux-là sont des côtés du polygone, pas des diagonales). Puisqu'il y a n sommets, par principe additif, cela devrait faire $n(n-3)$ diagonales... sauf que celles-ci sont comptées deux fois, une pour la première extrémité, et une pour la deuxième, si bien que le nombre de diagonales est finalement $\frac{n(n-3)}{2}$. Par exemple, dans un pentagone, cela fait $5 \times 2/2 = 5$ diagonales (tracez-les). Remarquons que $n(n-3)/2$ est toujours entier car n et $n-3$ sont de parités différentes donc l'un des deux est pair.

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 ?

Correction : Notons A l'ensemble des mains de 10 cartes avec exactement 5 trèfles et T l'ensemble des mains de 10 cartes avec exactement 2 as. On a donc :

$$\text{card}(A \cup T) = \text{card}(A) + \text{card}(T) - \text{card}(A \cap T)$$

- Par principe multiplicatif, $\text{card}(A) = \binom{13}{5} \binom{39}{5}$ puisqu'il y a $\binom{13}{5}$ façons de choisir 5 cartes parmi les trèfles et $\binom{39}{5}$ façons de choisir les 5 autres cartes parmi les 39 non trèfles
- Par principe multiplicatif, $\text{card}(T) = \binom{4}{2} \binom{48}{8}$ puisqu'il y a $\binom{4}{2}$ façons de choisir 2 cartes parmi les as et $\binom{48}{8}$ façons de choisir les 8 autres cartes parmi les 48 non as.
- Pour compter $\text{card}(A \cap T)$, remarquons qu'il y a deux possibilités disjointes (selon qu'on prend ou non l'as de trèfle) :
 - Ou bien on choisit l'as de trèfle puis les 4 autres trèfles parmi les 12 trèfles restants (il y a $\binom{12}{4}$ possibilités), l'autre as parmi les 3 as restants (il y a $\binom{3}{1}$ possibilités) et les 4 autres cartes parmi celles qui ne sont ni trèfle ni as (il y a $\binom{36}{4}$ possibilités).
 - Ou bien on choisit 5 trèfles parmi les 12 trèfles n'étant pas un as (il y a $\binom{12}{5}$ possibilités), deux as parmi les 3 as n'étant pas trèfle (il y a $\binom{3}{2}$ possibilités) et les 3 autres cartes parmi celles qui ne sont ni trèfle ni as (il y a $\binom{36}{3}$ possibilités).

Par principes multiplicatif et additif, on en déduit que

$$\text{card}(A \cap T) = \binom{12}{4} \binom{3}{1} \binom{36}{4} + \binom{12}{5} \binom{3}{2} \binom{36}{3}$$

Finalement

$$\text{card}(A \cup T) = \binom{13}{5} \binom{39}{5} + \binom{4}{2} \binom{48}{8} - \binom{12}{4} \binom{3}{1} \binom{36}{4} - \binom{12}{5} \binom{3}{2} \binom{36}{3}.$$

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 $\llbracket 1; n \rrbracket$?

Correction : Une telle famille est entièrement déterminée par ses éléments, l'ordre est automatiquement l'ordre croissant. Il y a donc $\binom{n}{p}$ telles familles.

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

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

Correction :

1. Pour tout entier $x \in \llbracket 1; n-1 \rrbracket$, il y a $n-x$ valeurs possibles de y (tous les entiers de $x+1$ à n), et aucune valeur pour $x = n$. Par principe additif, le nombre de tels couples est :

$$\sum_{k=1}^{n-1} (n-k) = n(n-1) - \frac{n(n-1)}{2} = \frac{n(n-1)}{2}$$

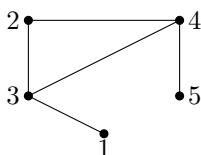
2. Pour tout entier $x \in \llbracket 1; n \rrbracket$, il y a $n-x+1$ valeurs possibles de y (tous les entiers de x à n). Par principe additif (les différents cas de figure sont incompatibles), le nombre de tels couples est (on fait ensuite le changement d'indice $j = n+1-k$ qui revient à compter les entiers en sens inverse)

$$\sum_{k=1}^n (n+1-k) = \sum_{j=1}^n j = \frac{n(n+1)}{2}$$

On pouvait aussi dire que c'est le nombre de couples de la partie précédente $+n$ car on ajoute les couples où $x = y$.

3. De même que dans l'exercice précédent, il y a $\binom{n}{3} = \frac{n(n-1)(n-2)}{6}$ tels triplets.

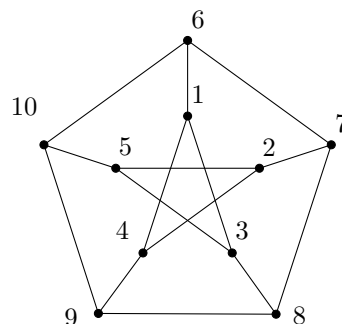
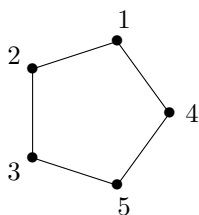
Exercice 14 - Graphes de Moore : ♣♣ Un graphe (simple, fini, sans boucle) est un couple (S, A) , où S est un ensemble fini et où A est une partie de $\mathcal{P}_2(S)$, où $\mathcal{P}_2(S)$ est l'ensemble des parties de S à 2 éléments. Les éléments de S sont représentés par des points et les arêtes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

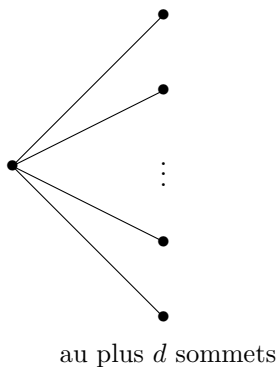
Soit $d \geq 1$. Montrer qu'un graphe de diamètre 2 et dont tous les sommets ont un degré inférieur ou égal à d comporte au plus $n = d^2 + 1$ sommets.

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) :

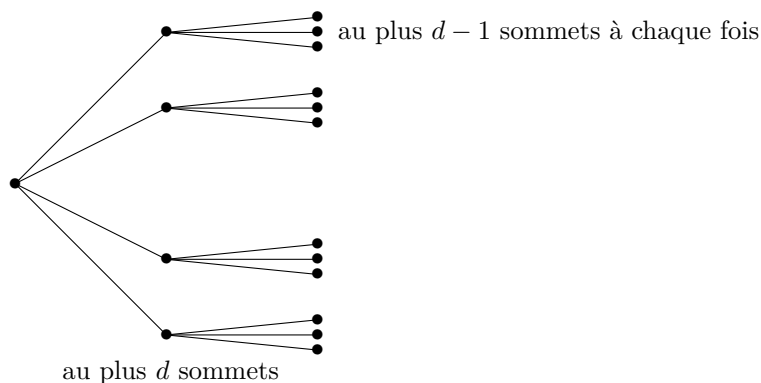


Le théorème de Hoffman et Singleton (que nous verrons peut-être en devoir cette année) dit que, si G est un graphe de Moore, alors $d = 1, 2, 3, 7$ ou $57...$ En particulier, il ne peut exister au plus que 5 graphes de Moore! Lorsque $d = 1$, on a deux sommets reliés par une arête donc le graphe est 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...

Correction : Prenons le premier sommet, qui a au plus d voisins (car les sommets sont tous de degré inférieur ou égal à d) :



Chacun de ces d nouveaux sommets a au plus $d - 1$ nouveaux voisins (en plus du sommet original). Certains, évidemment, peuvent être des sommets communs !



Et comme le diamètre est 2, on s'arrête là! Dans le meilleur (ou pire?) des cas, tous les sommets sont différents, la première rangée compte un sommet, la deuxième d et la troisième, par principe multiplicatif, $d(d - 1)$ (chacun des sommets de la première rangée, et il y en a au plus d , a au plus $d - 1$ voisins). Par principe additif (s'ils sont tous distincts), cela donne au plus $1 + d + d(d - 1) = d^2 + 1$ 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 ?

Correction :

1. Comme d'habitude : $\frac{15!}{10!} = 15 \times 14 \times 13 \times 12 \times 11$.
2. Un tel tirage est entièrement déterminé par les numéros des boules blanches ($\binom{5}{2}$ choix possibles) et par les numéros des boules noires ($\binom{10}{3}$ choix possibles) ainsi que par l'ordre des cinq boules ($5!$ choix possibles). Le nombre voulu est donc $\binom{5}{2} \times \binom{10}{3} \times 5!$.

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 ?

Correction : Un rangement des dés est entièrement déterminé par :

- La position des dés blancs : $\binom{6}{2}$ choix possibles. En effet, il y a 6 emplacements, et l'ordre dans lequel on met les deux dés blancs ne compte pas (on peut les intervertir, cela ne change pas la place des dés blancs).
- La position des autres dés : ceux-ci étant distincts, il y a $4!$ façons de les ordonner.
- La valeur des 6 dés : 6^6 .

Par principe multiplicatif, il y a $\binom{6}{2} \times 4! \times 6^6 = 16\,796\,160$ possibilités. En faisant 100 parties par jour, Pierre mettra 460 ans à épuiser toutes les possibilités !

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 ?

Correction :

1. $\binom{78}{15}$.
2. Il y a $\binom{75}{12}$ choix : on choisit les 12 cartes restantes.
3. S'il y a un seul bout, il y a trois choix pour le bout et $\binom{75}{14}$ choix pour les autres cartes (on pioche parmi les 75 cartes qui ne sont pas des bouts) ce qui fait, par principe multiplicatif, $3 \times \binom{75}{14}$ tirages possibles. S'il y a deux bouts, on a $\binom{3}{2} = 3$ choix pour les deux bouts, et $\binom{75}{13}$ choix pour les autres ce qui donne $3 \times \binom{75}{13}$, et le cas des trois bouts a été réglé à la question précédente. Par principe additif (les trois cas sont incompatibles) :

$$3 \times \binom{75}{14} + 3 \times \binom{75}{13} + \binom{75}{12}$$

4. Si ce tirage contient k atouts, il est entièrement déterminé par le choix des atouts, $\binom{22}{k}$ choix possibles, et par le choix des autres cartes, $\binom{56}{15-k}$ (on prend les cartes restantes parmi les cartes qui ne sont pas des atouts). Par principe multiplicatif, il y a $\binom{22}{k} \times \binom{56}{15-k}$ tirages possibles avec k atouts. Par principe additif, le nombre de tirages avec une poignée est :

$$\sum_{k=8}^{15} \binom{22}{k} \times \binom{56}{15-k}$$

5. Toutes les cartes sont prises dans les 56 cartes qui ne sont pas des atouts donc il y a $\binom{56}{15}$ tirages possibles.
6. Il y a deux cas de figure : soit le tirage contient 15, et alors il n'y a plus d'autre multiple de 3 ni de 5, soit les multiples de 3 et de 5 sont distincts et distincts de 15. Dans le premier cas, il y a $\binom{12}{4}$ choix pour les atouts (quatre atouts qui ne sont pas des multiples de 3 ou de 5 c'est-à-dire pas 3, 5, 6, 9, 10, 12, 15, 18, 20, 21) et $\binom{56}{10}$ pour les cartes qui ne sont pas des atouts, si bien qu'on a $\binom{12}{4} \times \binom{56}{10}$ choix tirages possibles lorsqu'il y a le chiffre 15. Dans le deuxième cas, il y a 6 choix possibles pour le multiple de 3 (on enlève 15) et 3 choix pour le multiple de 15 puis $\binom{12}{3}$ pour les 3 atouts restants puis toujours $\binom{56}{10}$ pour les cartes restantes, et donc il y a $6 \times 3 \times \binom{12}{3} \times \binom{56}{10}$ tels tirages. Enfin, par principe additif, le nombre cherché est :

$$\binom{12}{4} \times \binom{56}{10} + 6 \times 3 \times \binom{12}{3} \times \binom{56}{10}$$

Exercice 18 : ★★

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

Correction :

1. Notons les éléments de A $x_1 < \dots < x_p$ qu'on ordonne de façon strictement croissante. La seule fonction bijective strictement croissante est la fonction f qui envoie 1 sur x_1 , 2 sur x_2 etc. En effet, si $f(1) > 1$, si on note i l'antécédent de 1 (1 est atteint car f est surjective) alors $1 < i$ et $f(i) < f(1)$ ce qui est absurde car f est strictement croissante. De même on prouve que $f(2) = 2$ etc.
2. Une application strictement croissante est injective donc son image a p éléments. Une telle application est entièrement déterminée par son image d'après la fonction précédente (car il y a unicité). Par conséquent, il y a autant de fonctions strictement croissantes que de parties de $\llbracket 1; n \rrbracket$ de cardinal p , c'est-à-dire $\binom{n}{p}$ (on remarque, ce qui est évident, que le nombre recherché vaut 0 si $p > n$).
3. Ici, p peut être inférieur ou supérieur à n (par exemple, une application constante est croissante donc on peut avoir $p = 2024$ et $n = 1$). Une telle application croissante est entièrement déterminée par les images des p éléments (comptées avec répétitions) : il y en a $\binom{n+p-1}{p}$ d'après l'exercice 26. L'ordre, comme ci-dessus, est déterminé de façon unique : les plus petits éléments sont envoyés sur les plus petites images, et ainsi de suite.

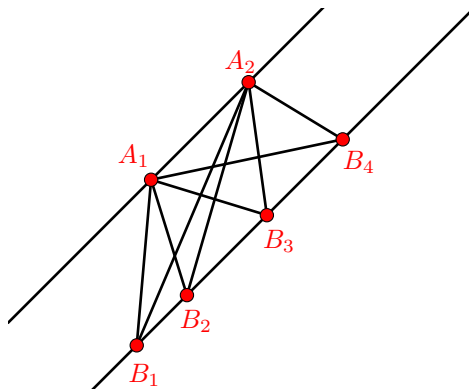
Exercice 19 : ★★★ Si A est une partie non vide de $\llbracket 1; n \rrbracket$, on définit son diamètre par : $\text{diam}(A) = \max(A) - \min(A)$.

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

Correction :

1. Un ensemble fini admet toujours un maximum et un minimum.
2. Tout d'abord, le diamètre est inférieur ou égal à n donc il n'y a aucune partie de $\llbracket 1; n \rrbracket$ de diamètre k si $k > n$. Supposons à présent que $k \in \llbracket 0; n \rrbracket$. Si $k = 0$ alors A est un singleton : n choix possibles. Si $k = 1$ alors le max et le min sont consécutifs si bien que A est de la forme $\{m; m+1\}$ avec $m \in \llbracket 1; n-1 \rrbracket$: $n-1$ choix possibles. Supposons à présent $k \geq 2$. Si le minimum est connu, le maximum aussi puisqu'il suffit de lui ajouter k . Un ensemble de diamètre k est donc entièrement déterminé par :
 - le minimum : $n-k$ choix possibles (tous les entiers de 1 à $n-k$: il faut garder de la place pour le maximum).
 - les entiers entre le minimum et le maximum. Entre m et $m+k$, il y a $k-1$ entiers, qui peuvent appartenir ou non à A . Pour chaque entier, deux possibilités : appartenir ou non, donc il y a 2^{k-1} choix possibles.
 Finalement, si $k \geq 2$, il y a $(n-k) \times 2^{k-1}$ parties de diamètre k .

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



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

Correction : Sur l'exemple ci-dessus, il y a 6 points d'intersection. Si on prend quatre points A_i, A_k, B_j, B_l , alors les segments $[A_i B_j]$ et $[A_k B_l]$ ont un point d'intersection si et seulement si $i < k$ et $j > l$. En effet, si $i = j$ alors les segments ont un sommet commun donc n'ont pas d'autre point d'intersection, et idem si $k = l$. Si $i < j$ et $k < l$, les segments ne sont pas parallèles mais « vont dans la même direction » donc ne s'intersectent pas (on pourrait le prouver rigoureusement en introduisant un repère mais ce n'est pas l'esprit de l'exercice). Dès lors, la seule possibilité est d'avoir $i < k$ et $j > l$ (les segments se croisent). En d'autres termes, quand on prend deux points parmi les A et deux points parmi les B , il n'y a qu'une possibilité pour avoir un point d'intersection, et ce point d'intersection est différent pour chaque choix de points car trois segments ne sont pas concourants. En conclusion, il y a autant de points d'intersection que de façon de choisir deux points parmi les A et de façons de choisir deux points parmi les B , c'est-à-dire (par principe multiplicatif)

$$\binom{p}{2} \times \binom{q}{2} = \frac{p(p-1)}{2} \times \frac{q(q-1)}{2}$$

On constate que pour $p = 2$ et $q = 4$ on trouve bien 6 points d'intersection.

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

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

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 ?

Correction :

1. Idem que dans l'exercice 6.
2. Idem, on obtient

$$\frac{21!}{9!(2!)^4 3!}$$

On peut aussi dire qu'une telle anagramme est obtenue en plaçant les U ($\binom{9}{21}$ choix possibles) puis en plaçant les autres lettres, et on se retrouve dans le cas de figure de la question précédente, il y a N choix possibles, si bien que le nombre recherché est $\binom{21}{9} \times N$ et on trouve évidemment la même chose.

3. (a) Il y a 10 points : si l'un d'eux représente 4 lettres ou plus, il reste au plus 8 lettres à mettre sur les 9 points restants, un point sera donc vide et il y aura deux U consécutifs ce qui est exclu.
- (b) Si trois lettres consécutives ne sont pas des U , cela signifie qu'un point représente trois lettres. Il reste donc 9 lettres à mettre en 9 points donc une lettre par points. Une telle anagramme est donc entièrement déterminée par le choix du point contenant 3 lettres (10 choix possibles), les autres points accueilleront forcément une seule lettre, et l'ordre des autres lettres N choix possibles. Par principe multiplicatif, il y a $10N$ telles anagrammes.
- (c) Si un point représente deux lettres au plus, alors il y a deux points qui représentent deux lettres, les autres en représentent une seule. Une telle anagramme est totalement déterminée par le choix des deux points ($\binom{10}{2}$ choix possibles) et par le choix des autres lettres (N choix possibles). Il y a donc $\binom{10}{2}N$ choix possibles.
- (d) Les deux cas précédents étant incompatibles, par principe additif, il y a

$$10N + \binom{10}{2}N$$

anagrammes équilibrées.

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 ?

Correction : Posons $n = 2^7$. Un tel premier tour est entièrement déterminé par l'ordre des joueurs, c'est-à-dire qu'il y a $n!$ permutations. Mais parmi ces permutations, par exemple, si on échange les deux premiers joueurs, cela donne le même premier tour. On peut faire pareil pour tous les matches, et il y en a $n/2 = 2^6$. Par conséquent, il faut diviser par $2^{n/2}$. Finalement, on divise aussi par $(n/2)!$ car on peut permuer les $n/2$ matches sans changer le premier tour. Finalement, si on pose $n = 2^7 = 128$, il y a

$$\frac{n!}{2^{n/2} \times (n/2)!} = \frac{128!}{2^{64} \times 64!}$$

façons d'organiser le premier tour.

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) ?

Correction :

- Une quinte flush est entièrement déterminée par sa couleur, 4 choix possibles, et par sa plus petite carte (inutile de connaître les autres, c'est automatique). En effet, si sa plus petite carte est un 5 alors les cartes sont 5, 6, 7, 8, 9. Il y a 10 choix possibles pour la première carte : As, 2, ..., 10. Le valet et les autres ne conviennent pas car Valet - Dame - Roi - As - 2 ne marche pas (mais As - 2 - 3 - 4 - 5 convient). Il y a donc 40 quinte flush.
- Un carré est entièrement déterminé par la valeur du carré (disons carré de dames), 13 choix possibles, et par le choix de la cinquième carte, 48 choix possibles. Il y a donc 13×48 choix possibles.
- Un full est entièrement déterminé par la valeur de la carte du brelan (disons, brelan de rois), 13 choix possibles, puis par leur couleur, $\binom{4}{3}$ choix possibles, puis par la valeur de la paire, disons paire de dames, 12 choix possibles (toutes sauf la valeur du brelan) et par les couleurs de la paire, $\binom{4}{2}$ choix possibles. Par conséquent, il y a $13 \times \binom{4}{3} \times 12 \times \binom{4}{2}$ fulls possibles.
- Une couleur est entièrement déterminée par sa couleur, 4 choix possibles, et par ses cinq cartes, $\binom{13}{5}$ choix possibles, il y a donc $4 \times \binom{13}{5}$ choix possibles auxquels il faut soustraire 40 car, si les cinq cartes se suivent, on a une quinte flush.
- Une suite est entièrement déterminée par ses cinq cartes : il y a $\binom{52}{5}$ choix possibles, auxquels il faut soustraire le nombre de quinte flush, le nombre de carrés, le nombre de fulls et le nombre de couleurs.
- Un brelan est entièrement déterminé par la valeur du brelan, 13 choix possibles (disons brelan de rois), puis par la couleur des cartes, $\binom{4}{3}$ choix possibles, puis par les deux autres cartes, $\binom{48}{2}$ (on prend les deux cartes restantes parmi les cartes qui ne sont pas des rois si on a pris un brelan de rois). Cela ne peut pas être un carré car on ne tire pas le quatrième roi, mais on peut avoir un full si, par exemple, on tire deux dames. On ne peut pas avoir de couleur, de suite, de quinte flush. Finalement, il y a $13 \times \binom{4}{3} \times \binom{48}{2}$, moins le nombre de fulls, mains possibles avec un brelan.
- Il y a $\binom{13}{2}$ choix possibles pour les valeurs des paires (attention de ne pas prendre 13 choix possibles pour la première paire et 12 pour la seconde, car en faisant comme ça on introduit une notion d'ordre entre les paires) puis $\binom{4}{2}$ choix pour les couleurs de la première paire, puis $\binom{4}{2}$ choix pour les couleurs de la seconde paire. Puis, si on enlève les 8 cartes correspondant à ces deux valeurs (par exemple, si on a une paire de rois et une paire de dames, on enlève les rois et les dames) et on pioche là-dedans une cinquième carte, ce qui fait 44 choix possibles. Il est impossible d'avoir quoi que ce soit d'autre qu'une double paire par construction donc il n'y a rien à enlever, ce qui fait $\binom{13}{2} \times \binom{4}{2}^2 \times 44$ choix pour une double paire.
- Pour la paire, 13 choix pour la valeur, $\binom{4}{2}$ pour les couleurs, $\binom{48}{3}$ pour piocher les trois cartes restantes dans ce qui reste (on a aussi enlevé les cartes de la même valeur que celles dans la paire, même celles qui ne sont pas dans la

paire, pour ne pas risquer d'avoir un brelan ou un carré). Cependant, il faut soustraire le full et la double paire, si bien qu'on a $13 \times \binom{4}{2} \times \binom{48}{3}$ moins le nombre de fulls moins le nombre de doubles paires.

- C'est le nombre total de tirages, $\binom{52}{5}$, moins tout le reste.

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

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

Correction : Les deux premières questions ont été prouvées dans le chapitre 4. L'interprétation combinatoire de la première question est la suivante : si on choisit k objets parmi n (une équipe) puis j personnes parmi ces k (les chefs), cela revient au même que de choisir les chefs d'abord puis de choisir les $n-k$ membres restants de l'équipe parmi les $n-j$ objets suivants. Répondons à présent à la question 3. L'ensemble des permutations de E , de cardinal $n!$, est l'union disjointe des ensembles des permutations à k points fixes, pour k allant de 0 à n . Or, si $k \in \llbracket 0; n \rrbracket$, une permutation à k points fixes est entièrement déterminée par le choix des points fixes, $\binom{n}{k}$ choix possibles, puis par l'image des autres, dont aucun n'est un point fixe : on a donc un dérangement pour les autres éléments, au nombre de $n-k$, si bien qu'il y a D_{n-k} possibilités. Par principe multiplicatif, il y a $\binom{n}{k} \times D_{n-k}$ permutations avec k points fixes, et par principe additif :

$$n! = \sum_{k=0}^n \binom{n}{k} D_{n-k}$$

En faisant un changement d'indice :

$$n! = \sum_{j=0}^n \binom{n}{n-j} D_j = \sum_{k=0}^n \binom{n}{n-k} D_k$$

car l'indice est muet, et puisque $\binom{n}{k} = \binom{n}{n-k}$, on a

$$n! = \sum_{k=0}^n \binom{n}{k} D_k$$

On conclut en appliquant la question 2.

Exercice 25 - Fonction de Möbius : ★★☆☆ On définit $\mu : \mathbb{N}^* \rightarrow \{0; 1; -1\}$ 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 :

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

Correction :

- Soient n_1 et n_2 deux entiers naturels non nuls premiers entre eux. Il y a deux cas :
 - Supposons que $n_1 n_2$ admette un facteur carré d^2 avec $d \geq 2$. Alors d admet un facteur premier p si bien que p^2 divise $n_1 n_2$: p^2 apparaît dans la décomposition de $n_1 n_2$ en produit de facteurs premiers. Or, n_1 et n_2 sont premiers entre eux donc ne peuvent pas contenir p tous les deux : il en découle que p^2 apparaît dans celle de n_1 ou dans celle de n_2 . En particulier, n_1 ou n_2 a un facteur carré donc $\mu(n_1) = 0$ ou $\mu(n_2) = 0$ si bien que $\mu(n_1)\mu(n_2) = 0$ et $\mu(n_1 n_2) = 0$ car $n_1 n_2$ admet un facteur carré.
 - Supposons que $n_1 n_2$ n'ait aucun facteur carré. Alors n_1 et n_2 n'ont aucun facteur carré. Notons s le nombre de facteurs premiers de n_1 et s celui de n_2 , si bien que $n_1 = p_1 \cdots p_r$ et $n_2 = q_1 \cdots q_s$ où les p_i et q_j sont premiers distincts deux à deux (les puissances sont égales à 1 car n_1 et n_2 sont sans facteur carré). Il en découle que $\mu(n_1) = (-1)^r$ et $\mu(n_2) = (-1)^s$ et $n_1 n_2 = p_1 \cdots p_r q_1 \cdots q_s$: les p_i et q_j étant distincts puisque n_1 et n_2 sont premiers entre eux donc n'ont aucun facteur carré commun $n_1 n_2$ est le produit de $r + s$ facteurs premiers distincts si bien que $\mu(n_1 n_2) = (-1)^{r+s} = (-1)^r \times (-1)^s = \mu(n_1)\mu(n_2)$.
- Soit $n \geq 2$. Notons $n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$ sa décomposition en produit de facteurs premiers. Les diviseurs de n sont donc les entiers de la forme $d = p_1^{\beta_1} \times \cdots \times p_r^{\beta_r}$ avec, pour tout i , $\beta_i \leq \alpha_i$. Puisque les entiers ayant un facteur carré ont une image par μ nulle, seuls les diviseurs de la forme $p_1^{\beta_1} \times \cdots \times p_r^{\beta_r}$, avec $\beta_i = 0$ ou 1, apportent une contribution à la somme. Regroupons les diviseurs de n selon le nombre de β_i égaux à 1 :

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{k=0}^r \sum_{\substack{d|n \\ \text{card}(\{i \mid \beta_i=1\})=k}} \mu(d) \\ &= \sum_{k=0}^r \sum_{\substack{d|n \\ \text{card}(\{i \mid \beta_i=1\})=k}} (-1)^k \end{aligned}$$

La deuxième somme est la somme d'un terme constant (on somme sur toutes les façons possibles d'avoir k fois une puissance égale à 1). Or, il y a $\binom{k}{r}$ façons de choisir les k emplacements β_i en lesquels la puissance vaut 1, si bien que

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{k=0}^r \binom{r}{k} (-1)^k \\ &= (1 - 1)^r \\ &= 0 \end{aligned}$$

- Notons S_n la somme de droite. Lorsque d parcourt les diviseurs de n , n/d parcourt lui aussi les diviseurs de n donc, en faisant le changement « d'indice » $\delta = n/d$ puis en remplaçant par d car l'indice est muet, ça donne :

$$\begin{aligned} S_n &= \sum_{\delta|n} \mu(\delta) g\left(\frac{n}{\delta}\right) \\ &= \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \sum_{k|\frac{n}{d}} f(k) \end{aligned}$$

Soit d un diviseur de n . Alors k divise n/d si et seulement si il existe m tel que $km = n/d$ donc tel que $md = n/k$. Il en découle que k divise n/d si et seulement si d divise n/k , d'où l'interversion suivante :

$$S_n = \sum_{k|n} f(k) \sum_{d|\frac{n}{k}} \mu(d)$$

Or, si $k \neq n$, alors $n/k \neq 1$ donc la somme de droite est nulle d'après la question précédente. En d'autres termes, il ne reste que le terme pour $k = n$ qui vaut $f(n)$ ce qui est le résultat voulu.

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 $\llbracket 1; 3 \rrbracket$:

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

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 $n-1$ 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 $\binom{n+k-1}{k}$.

Correction :

1. Une combinaison à k éléments est entièrement déterminée par le nombre de 1, le nombre de 2 etc. jusqu'au nombre de n . On va en fait la coder de la façon suivante : les premiers ronds (il peut n'y en avoir aucun s'il n'y a pas de 1) représentent les 1, ensuite il y a une barre symbolisant la séparation, ensuite les ronds représentent les 2, jusqu'à la prochaine barre verticale, et ensuite les ronds représentent les 3 etc. Par exemple, pour représenter une combinaison à 6 éléments dans un ensemble à 4 éléments, le diagramme $\circ \circ \circ | \circ || \circ \circ$ représente la combinaison (1, 1, 1, 2, 4, 4) car il y a trois 1, un 2, aucun 3 et deux 4. Dans le cas général, il y a $n-1$ barres verticales (une pour séparer les 1 des 2, une pour séparer les 2 des 3 etc. et une barre pour séparer les $n-1$ des n), et il y a k ronds pour les k éléments apparaissant dans la combinaison.
2. Une combinaison est donc entièrement déterminée par la place des barres verticales : il y en a donc $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$ grâce à la propriété de symétrie des coefficients binomiaux.

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 .

Correction :

1. $B_1 = 1$ car la seule partition d'un singleton est le singleton lui-même. $B_2 = 2$ car si $E = \{a; b\}$, il y a deux partitions : soit E tout seul, soit les deux ensembles $\{a\}$ et $\{b\}$. Enfin, $B_3 = 5$ car les seules partitions possibles d'un ensemble à trois éléments $E = \{a; b; c\}$ sont E tout seul, $\{a\}$ et $\{b; c\}$, $\{a; b\}$ et $\{c\}$, $\{b\}$ et $\{a; c\}$, et enfin $\{a\}$, $\{b\}$ et $\{c\}$.
2. Soit donc E un ensemble de cardinal $n+1$, et soit $a \in E$. Soit $k \in \llbracket 0; n \rrbracket$ et supposons que P soit une partition de E dont l'ensemble contenant a , qu'on notera E_a , soit de cardinal $k+1$ (les différents cas de figure sont incompatibles, nous appliquerons ensuite le principe additif). Cette partition est totalement déterminée :
 - par les éléments de $E_a \setminus \{a\}$ qui est de cardinal k , qu'on prend parmi les éléments de $E \setminus \{a\}$ qui est de cardinal n donc il y a $\binom{n}{k}$ choix possibles.
 - par le choix des autres ensembles formant la partition P : ils forment une partition de $P \setminus E_a$ qui est un ensemble à $n-k$ éléments, il y a donc B_{n-k} possibilités. Par principe multiplicatif, il y a $\binom{n}{k} \times B_{n-k}$ telles partitions, et le principe additif permet de conclure.

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 $p \in \llbracket 2; n-1 \rrbracket$, $S(n, p) = p \times (S(n-1, p-1) + S(n-1, p))$. En déduire que :

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

Correction :

1. Lorsque $p > n$, il n'existe (cf. cours) aucune bijection d'un ensemble à n éléments dans un ensemble à p éléments donc $S(n, p) = 0$. Une application d'un ensemble à n éléments dans un ensemble à n éléments est surjective si et seulement si elle est bijective. Dès lors, $S(n, n)$ est le nombre de bijections entre deux ensembles à n éléments donc $S(n, n) = n!$. Il n'y a qu'une application entre un ensemble à n éléments dans un ensemble à 1 élément (l'application qui envoie tous les éléments sur l'unique élément de l'ensemble d'arrivée) et elle est surjective, si bien que $S(n, 1) = 1$. Enfin, il y a 2^n applications d'un ensemble à n éléments dans un ensemble à 2 éléments (rappelons que l'ensemble des fonctions de E dans F est F^E , de cardinal, quand les ensembles sont finis évidemment, $\text{card}(F)^{\text{card}(E)}$) et seules les deux fonctions constantes ne sont pas surjectives, si bien que $S(n, 2) = 2^n - 2$.
2. Une surjection d'un ensemble E à $n+1$ éléments dans un ensemble F à n éléments est entièrement déterminée :
 - par l'unique élément de F atteint deux fois (en effet, une telle application atteint deux fois un élément et une seule fois tous les autres) : n choix possibles.
 - par les deux antécédents de cet élément : $\binom{n+1}{2}$ (car il n'y a pas d'ordre) choix possibles.
 - par les images des autres éléments. Or, si on note y l'unique élément de F admettant deux antécédents, et x_1 et x_2 ses deux antécédents, la restriction de f à $E \setminus \{x_1, x_2\}$ est une bijection de cet ensemble vers $F \setminus \{y\}$, deux ensembles à $n-1$ éléments, donc il y a $(n-1)!$ choix possibles.

Par principe multiplicatif, $S(n+1, n) = n \times \binom{n+1}{2} \times (n-1)! = \frac{n \times (n+1) \times n \times (n-1)!}{2} = \frac{n \times (n+1)!}{2}$.

3. F^E (où on a noté E un ensemble à n éléments et F un ensemble à p éléments) est l'union disjointe des A_k où A_k est l'ensemble des fonctions de E dans F dont l'image a k éléments, pour k allant de 0 à n . Un élément de A_k est entièrement déterminé par les éléments de son image, $\binom{p}{k}$ choix possibles, et par la fonction elle-même, c'est-à-dire « les flèches » i.e. qui est envoyé sur qui. Or, une application est toujours une surjection sur son image : il y a donc $S(n, k)$ façons de définir une application de E dans l'image choisie. Par conséquent, $\text{card}(A_k) = \binom{p}{k} S(n, k)$, si bien que

$$\text{card}(F^E) = p^n = \sum_{k=0}^p \binom{p}{k} S(n, k)$$

L'exercice 24 (avec p à la place de n , $S(n, k)$ à la place de b_k et p^n à la place de a_n ou plutôt de a_p puisqu'on a remplacé n par p , ici n est une constante) donne le bon résultat.

4. Soit $p \in \llbracket 2; n-1 \rrbracket$. Une surjection de E dans F (toujours avec E de cardinal n , qu'on note $\{x_1; \dots; x_n\}$, et F de cardinal p) est entièrement déterminée par :
 - L'image de x_n , qu'on note y : p choix possibles.
 - Les images des autres éléments de E , c'est-à-dire la restriction de f à $E \setminus \{x_n\}$. Deux cas de figure incompatibles : soit f atteint de nouveau y et donc la restriction de f à $E \setminus \{x_n\}$ est une surjection sur F , il y a donc $S(n-1, p)$ choix possibles, soit f n'atteint plus y et donc on a une surjection de $E \setminus \{x_n\}$ dans $F \setminus \{y\}$, ce qui fait $S(n-1, p-1)$ choix possibles, et par principe additif, cela donne $S(n-1, p-1) + S(n-1, p)$ choix possibles.

Le principe multiplicatif donne le résultat voulu. Par conséquent :

$$S(n+2, n) = n \times (S(n+1, n-1) + S(n+1, n))$$

et, en utilisant la question 2 :

$$S(n+2, n) = n \times \left(S(n+1, n-1) + \frac{n \times (n+1)!}{2} \right)$$

Montrons le résultat voulu par récurrence. D'une part, $S(3, 1) = 1$ d'après la question 1, et d'autre part, si $n = 1$,

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

donc le résultat est vrai au rang 1. Soit $n \geq 2$, supposons le résultat vrai au rang $n-1$ et prouvons qu'il est vrai au rang n . D'après ce qui précède puis par hypothèse de récurrence :

$$\begin{aligned}
S(n+2, n) &= n \times \left(S(n+1, n-1) + \frac{n \times (n+1)!}{2} \right) \\
&= n \times \left(\frac{(n-1)(3(n-1)+1)(n-1+2)!}{24} + \frac{n(n+1)!}{2} \right) \\
&= n \times \left(\frac{(n-1)(3n-2)(n+1)! + 12n(n+1)!}{24} \right) \\
&= \frac{n[(n-1)(3n-2) + 12n](n+1)!}{24} \\
&= \frac{n(3n^2 + 7n + 2)(n+1)!}{24}
\end{aligned}$$

Or, $3n^2 + 7n + 2 = (3n+1)(n+2)$ donc

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

ce qui clôt la récurrence.

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 $f : E \rightarrow E$ vérifiant $f \circ f = \text{Id}_E$.

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

Correction :

1. Si $n = 1$, il n'y a qu'une application de E dans E , l'identité, et elle est involutive donc $u_1 = 1$. Si $n = 2$, notons $E = \{a; b\}$. Il n'y a que deux involutions : l'identité, et la fonction f définie par $f(a) = b$ et $f(b) = a$, donc $u_2 = 2$. Enfin, $u_3 = 4$. Notons en effet $E = \{a; b; c\}$. L'identité est évidemment une involution. Cherchons les involutions distinctes de l'identité. Supposons dans un premier temps que $f(a) = a$. Alors $f(b) = c$. En effet, si $f(b) = b$ alors, c étant forcément atteint, on a $f(c) = c$ donc f est l'identité ce qui est exclu. Dès lors, $f(a) = a, f(b) = c$ et $f(c) = b$, qui est bien involutive. Supposons à présent que $f(a) = b$. Puisque f est involutive, alors $f(f(a)) = f(b) = a$ et donc on a forcément $f(c) = c$, et cette fonction est bien une involution. Enfin, si $f(a) = c$, alors de même $f(c) = a$ et $f(b) = b$ ce qui est encore une involution, et cela fait bien 4 involutions.
2. Soit $n \in \mathbb{N}$. Supposons que E ait $n+2$ éléments qu'on note x_1, \dots, x_{n+2} . Il y a deux cas de figure : soit $f(x_{n+2}) = x_{n+2}$, soit non.
 - Si $f(x_{n+2}) = x_{n+2}$, alors f est entièrement déterminée par sa restriction à $E \setminus \{x_1; \dots; x_{n+1}\}$ et est involutive sur cet ensemble : u_{n+1} possibilités.
 - Sinon, f est entièrement déterminée par l'image de x_{n+2} , qu'on note x_i , et par sa restriction à $E \setminus \{x_i; x_{n+2}\}$. En effet, $f(x_i) = x_{n+2}$ puisque f est involutive. Il y a $n+1$ choix pour x_i (x_{n+2} est exclu par hypothèse) et il y a u_n choix pour la restriction puisque celle-ci est une involution sur un ensemble à n éléments (puisque l'on a enlevé x_i et x_{n+2}) : $(n+1)u_n$ possibilités par principe multiplicatif.

Le principe additif permet de conclure.

Exercice 30 - Lemme de Kaplansky : ★★ Pour tout $n \geq 1$, on note u_n le nombre de parties (éventuellement vides) de $\llbracket 1; n \rrbracket$ 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 .

Correction :

1. On a évidemment $u_1 = 2$ puisque les parties de $\{1\}$ sont \emptyset et $\{1\}$ qui ne contiennent pas deux entiers consécutifs. Les parties de $\llbracket 1; 2 \rrbracket$ sont $\emptyset, \{1\}, \{2\}$ et $\llbracket 1; 2 \rrbracket$ donc y en a 3 qui ne contiennent pas deux entiers consécutifs, si bien que $u_2 = 3$. Enfin, les parties de $\llbracket 1; 3 \rrbracket$ sont $\emptyset, \{1\}, \{2\}, \{3\}, \{1; 2\}, \{1; 3\}, \{2; 3\}$ et $\llbracket 1; 3 \rrbracket$ si bien que $u_3 = 5$.

2. Soit E une partie de $\llbracket 1; n+2 \rrbracket$ ne contenant pas deux entiers consécutifs. Si elle contient $n+2$, elle ne contient pas $n+1$ (car elle ne contient pas deux entiers consécutifs) et les éléments restants forment une partie de $\llbracket 1; n \rrbracket$ (éventuellement vide) ne contenant pas deux entiers consécutifs : u_n choix possibles. Si elle ne contient pas $n+2$, alors c'est une partie de $\llbracket 1; n+1 \rrbracket$ ne contenant pas deux entiers consécutifs, il y a u_{n+1} choix possibles. Les deux cas étant incompatibles, par principe additif, on a $u_{n+2} = u_{n+1} + u_n$. On a une suite récurrence linéaire d'ordre 2 (et une relation qu'on connaît : la même que la suite de Fibonacci, mais ce n'est pas la suite de Fibonacci puisque les conditions initiales ne sont pas les mêmes). On peut soit faire la méthode habituelle (c'est long...) soit reconnaître en fait la suite de Fibonacci décalée de 2 ! En effet, on a $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3$ etc. et $u_1 = 2, u_2 = 3$ etc. Les suites $(u_n)_{n \geq 1}$ et $(F_{n+2})_{n \geq 1}$ ont les mêmes deux premiers termes et vérifient la même relation de récurrence donc sont égales. Finalement :

$$\forall n \geq 1, u_n = F_{n+2} = \frac{1}{\sqrt{5}} \times \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+2} \right]$$

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

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

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

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

- (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 :

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

Correction :

- Les 6 compositions de 5 à 3 éléments (n'oublions pas que l'ordre compte) sont : $(1, 1, 3), (1, 3, 1), (3, 1, 1), (1, 2, 2), (2, 1, 2), (2, 2, 1)$.
- Montrons que f est injective. Soient $\alpha = (\alpha_1, \dots, \alpha_k)$ et $\beta = (\beta_1, \dots, \beta_k)$ deux éléments de $C(n, k)$ et supposons que $\alpha \neq \beta$. Soit $i_0 = \min\{i \mid \alpha_i \neq \beta_i\}$ la première coordonnée différente entre α et β (ce minimum existe bien car toute partie non vide de \mathbb{N} admet un minimum, ou car toute partie finie non vide admet un minimum). Prouvons que $i_0 \neq k$: si c'est le cas, alors $\alpha_1 = \beta_1, \dots, \alpha_{k-1} = \beta_{k-1}$, mais la somme des α_i vaut n , tout comme celle des β_i et donc $\alpha_k = 1 - \alpha_1 - \dots - \alpha_{k-1}$ et idem pour β_k , donc $\alpha_k = \beta_k$ ce qui est absurde. Alors

$$\alpha_1 + \dots + \alpha_{i_0-1} = \beta_1 + \dots + \beta_{i_0-1}$$

mais $\alpha_{i_0} \neq \beta_{i_0}$ si bien que

$$\alpha_1 + \dots + \alpha_{i_0-1} + \alpha_{i_0} = \beta_1 + \dots + \beta_{i_0-1} + \beta_{i_0}$$

et donc $f(\alpha) \neq f(\beta)$ car leurs coordonnées en emplacement i_0 sont différentes : f est injective.

Prouvons à présent la surjectivité de f : soit $F = \{x_1; \dots; x_{k-1}\}$ une partie à $k-1$ éléments de $\llbracket 1; n-1 \rrbracket$ avec $x_1 < \dots < x_{k-1}$. Posons :

$$\alpha_1 = x_1 \quad \text{et} \quad \forall i \in \llbracket 2; k-1 \rrbracket, \alpha_i = x_i - x_{i-1}$$

c'est-à-dire que α_1 est le premier élément de F , et les suivants (sauf le k -ième) sont les différences entre deux x_i consécutifs (par exemple, si on prend $F = \{1; 3; 3\}$ alors on pose $\alpha_1 = 1, \alpha_2 = 3 - 1 = 2$ et $\alpha_3 = 5 - 3 = 2$) et on pose enfin $\alpha_k = 1 - \alpha_1 - \dots - \alpha_{k-1}$. Alors on a bien $(\alpha_1, \dots, \alpha_k) \in C(k, n)$ puisque la somme des α_i vaut n , les α_i sont bien strictement positifs car $x_1 < \dots < x_{k-1} < n$ et on a bien $f(\alpha_1, \dots, \alpha_k) = (x_1, \dots, x_k)$. D'où la surjectivité et donc la bijectivité de f .

Par conséquent, il y a autant de compositions de n à k éléments que de parties de $\llbracket 1; n-1 \rrbracket$ à k éléments, c'est-à-dire $\binom{n-1}{k-1}$. Si $k=1$, alors une composition de n à k éléments est une 1-liste dont la somme vaut n , c'est-à-dire

simplement (n) : il y en a donc une seule, et donc encore $\binom{n-1}{k-1}$. Lorsque $n = 1$, on a forcément $k = 1$ donc c'est encore valable. En conclusion, dans tous les cas de figure, le résultat cherché vaut $\binom{n-1}{k-1}$.

3. (a) Notons A_k le nombre recherché. Une telle n -composition est entièrement déterminée par son dernier chiffre (qui vaut 1 ou 2) et les $n-1$ chiffres précédents. Si son dernier chiffre est un 1, alors les chiffres précédents ont une somme égale à $n-1$ (donc il y a A_{n-1} choix possibles) tandis que si le dernier chiffre vaut 2, alors les chiffres précédents ont une somme égale à $n-2$ (A_{n-2} choix possibles). Ces deux possibilités étant incompatibles, $A_n = A_{n-1} + A_{n-2}$: la suite (A_n) vérifie la même relation de récurrence que la suite de Fibonacci. Or, $A_1 = 1 = F_2$ et $A_2 = 2 = F_3$ ((1, 1), (2) sont les seules solutions), donc, par une récurrence double immédiate, $A_n = F_{n+1}$ pour tout n .
- (b) Précisons tout d'abord que cette somme est finie puisque $\binom{n-i}{i}$ est nul dès que $i > n-i$ donc dès que $i > n/2$. Il suffit de choisir le nombre de 2 dans les décompositions de la question précédente (ceux ne comportant que des 1 et des 2).

Plus précisément, soit $i \geq 0$ et soit α une composition de n ne comportant que des 1 et des 2, avec i fois le chiffre 2. Tout d'abord, si on note k la longueur de cette composition, remarquons que k est entièrement déterminé par le nombre de 1 puisqu'alors il y a $(k-i)$ fois le nombre 1, et $i \times 2 + 1 \times (k-i) = n$ ce qui permet de trouver la valeur de k : plus précisément, $k = n-i$. Il y a donc $\binom{n-i}{i}$ façons de choisir les i emplacements où placer des 2, et alors la composition est entièrement déterminée, puisqu'il suffit de mettre des 1 partout ailleurs : une seule façon de faire !

En d'autres termes, une composition de n comportant i fois le nombre 2 est une composition à $n-i$ chiffres et il y a $\binom{n-i}{i}$ façons de faire une telle composition. Les différents cas de figure étant incompatibles, le nombre de telles compositions vaut la somme de l'énoncé, ce qui permet de conclure d'après la question précédente.

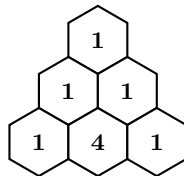
On aurait aussi pu le montrer par récurrence double : cf. DS numéro 1.

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

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

$$\forall k \in \llbracket 1; n-2 \rrbracket, \left\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \right\rangle = (n-k) \left\langle \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\rangle + (k+1) \left\langle \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\rangle$$

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



Correction : Rappelons qu'une permutation est une n -liste d'éléments distincts de $\llbracket 1; n \rrbracket$. En d'autres termes, une permutation de $\llbracket 1; n \rrbracket$ est juste une n -liste contenant les entiers de 1 à n dans un ordre quelconque.

- La seule permutation de $\llbracket 1; 1 \rrbracket$ est (1) qui ne comporte aucune descente, donc $\left\langle \begin{smallmatrix} 1 \\ 0 \end{smallmatrix} \right\rangle = 1$.

Les seules permutations de $\llbracket 1; 2 \rrbracket$ sont (1, 2), (2, 1) : la première n'a aucune descente, la deuxième en a 1, donc $\left\langle \begin{smallmatrix} 2 \\ 0 \end{smallmatrix} \right\rangle = \left\langle \begin{smallmatrix} 2 \\ 1 \end{smallmatrix} \right\rangle = 1$.

Les seules permutations de $\llbracket 1; 3 \rrbracket$ sont (1, 2, 3) qui n'a aucune descente, (1, 3, 2) qui en a une, (2, 1, 3) qui en a une, (2, 3, 1) qui en a une, (3, 1, 2) qui en a une, et (3, 2, 1) qui en a deux. Une permutation n'a aucune descente, quatre en ont une, et une en a deux, donc

$$\left\langle \begin{smallmatrix} 3 \\ 0 \end{smallmatrix} \right\rangle = 1, \left\langle \begin{smallmatrix} 3 \\ 1 \end{smallmatrix} \right\rangle = 4 \quad \text{et} \quad \left\langle \begin{smallmatrix} 3 \\ 2 \end{smallmatrix} \right\rangle = 1$$

2. La seule possibilité pour n'avoir aucune descente est de toujours monter, donc la seule permutation possible est $(1, 2, \dots, n)$, et idem pour n'avoir que des descentes, la seule permutation possible est $(n, n-1, \dots, 1)$. On en déduit les deux premières égalités.

Soit w une permutation avec une seule descente. Soit $k \in \llbracket 1; n-1 \rrbracket$ l'emplacement de sa seule descente. On a donc

$$w_1 < w_2 < \dots < w_k > w_{k+1} < w_{k+2} < \dots < w_n$$

Une telle permutation est entièrement déterminée par l'ensemble $\{w_1, \dots, w_k\}$ (sans notion d'ordre) : en effet, une fois cet ensemble et ses éléments connus, on les ordonne par ordre croissant (une seule possibilité) et idem pour les suivants, les éléments de $\llbracket 1; n \rrbracket$ restants. Cependant, toute partie de $\llbracket 1; n \rrbracket$ à k éléments ne convient pas : il faut pouvoir « glisser » w_{k+1} quelque part, c'est-à-dire qu'il ne faut pas prendre $\llbracket 1; k \rrbracket$. Mais toute autre partie convient : en effet, si on a une partie à k éléments qui n'est pas $\llbracket 1; k \rrbracket$, alors soit son premier élément n'est pas 1, soit elle ne contient pas deux entiers consécutifs, et donc il est possible de prendre cette partie pour former une telle partition. Par conséquent, il y a $\binom{n}{k} - 1$ possibilités pour avoir une partition avec une seule descente en position k , et ces cas de figure étant deux à deux incompatibles, par principe additif :

$$\left\langle \begin{smallmatrix} 1 \\ n \end{smallmatrix} \right\rangle = \sum_{k=1}^{n-1} \left(\binom{n}{k} - 1 \right)$$

et cette quantité vaut bien $2^n - n - 1$ (attention, la somme va de 1 à $n-1$).

3. Prenons une partition de $\llbracket 1; n \rrbracket$ contenant k descentes. Il y a donc, par définition, $\left\langle \begin{smallmatrix} n \\ k \end{smallmatrix} \right\rangle$ possibilités. Retirons n de cette partition (en préservant l'ordre) : cela nous donne donc une partition de $\llbracket 1; n-1 \rrbracket$. Combien contient-elle de descentes ?

- Si, avant de supprimer le n , on avait une situation du type (i, n, j) avec $i < j$, alors on avait une descente avant suppression, et on n'en a plus ensuite : on supprime une descente, donc on se retrouve avec une permutation ayant $k-1$ descentes. C'est également le cas si n est en première position : on commence automatiquement par une descente, que l'on supprime en enlevant n . Il y a $\left\langle \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\rangle$ choix possibles pour l'organisation des autres nombres, et $n-k$ choix possibles pour l'emplacement de n : $n-1-k$ pour la montée au sein de laquelle insérer n , et 1 choix possibles pour le premier emplacement, donc $n-k$ choix possibles pour l'emplacement de n . Par principe multiplicatif, il y a $(n-k) \times \left\langle \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\rangle$ possibilités.
- Si, avant de supprimer le n , on avait une permutation du type (i, n, j) avec $i > j$, alors on avait une descente avant suppression, et on en a toujours une ensuite, donc on se retrouve encore avec k descentes, et c'est aussi le cas si n est en dernière place, le supprimer ne change pas le nombre des descentes. Il y a $\left\langle \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\rangle$ choix possibles pour l'organisation des autres nombres, et k choix possibles pour la descente au sein de laquelle insérer n , et 1 choix pour le placement en dernière position. Par principe multiplicatif, il y a $(k+1) \times \left\langle \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\rangle$ possibilités.

On conclut par le principe additif.

4. On cherche donc $\left\langle \begin{smallmatrix} 4 \\ 0 \end{smallmatrix} \right\rangle, \left\langle \begin{smallmatrix} 4 \\ 1 \end{smallmatrix} \right\rangle, \left\langle \begin{smallmatrix} 4 \\ 2 \end{smallmatrix} \right\rangle, \left\langle \begin{smallmatrix} 4 \\ 3 \end{smallmatrix} \right\rangle$. D'après la question 2, on a $\left\langle \begin{smallmatrix} 4 \\ 0 \end{smallmatrix} \right\rangle = \left\langle \begin{smallmatrix} 4 \\ 3 \end{smallmatrix} \right\rangle = 1$ et $\left\langle \begin{smallmatrix} 4 \\ 1 \end{smallmatrix} \right\rangle = 11$. Enfin, d'après la question précédente avec $k=2$,

$$\begin{aligned} \left\langle \begin{smallmatrix} 4 \\ 2 \end{smallmatrix} \right\rangle &= (4-2) \times \left\langle \begin{smallmatrix} 3 \\ 1 \end{smallmatrix} \right\rangle + (2+1) \times \left\langle \begin{smallmatrix} 3 \\ 2 \end{smallmatrix} \right\rangle \\ &= 2 \times 4 + 3 \times 1 \\ &= 11 \end{aligned}$$

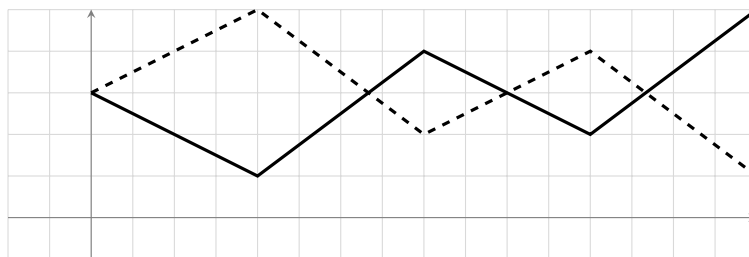
La ligne suivante est donc : 1, 11, 11, 1. On trouve de même (avec $n=5$) que la ligne suivante est 1, 26, 66, 26, 1.

Exercice 33 - Permutations alternées : ♦♦♦♦ On dit qu'une permutation $w = (w_1, \dots, w_n)$ de $\llbracket 1; n \rrbracket$ est alternée si :

$$w_1 < w_2 > w_3 < w_4 > \dots \quad \text{ou} \quad w_1 > w_2 < w_3 > w_4 < \dots$$

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) des permutations alternées bas/haut et 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 :

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

Correction : Rappelons qu'une permutation est une n -liste d'éléments distincts de $\llbracket 1; n \rrbracket$. En d'autres termes, une permutation de $\llbracket 1; n \rrbracket$ est juste une n -liste contenant les entiers de 1 à n dans un ordre quelconque.

1. Il suffit de trouver une bijection entre l'ensemble des permutations alternées haut/bas et l'ensemble des permutations alternées bas/haut. L'idée est de faire une symétrie axiale, par rapport au « milieu » de l'intervalle d'entiers $\llbracket 1; n \rrbracket$: à chaque entier k on associe $n+1-k$ (on parcourt $\llbracket 1; n \rrbracket$ en sens inverse).

Par exemple, si on se place sur $\llbracket 1; 5 \rrbracket$, alors à l'entier 1 on associe 5, à l'entier 2 on associe 4, et 3 est associé à lui-même (au premier entier on associe le dernier, au deuxième on associe l'avant-dernier etc.). Ainsi, à une permutation quelconque, on associe la permutation formée par les images de ses éléments. Par exemple, à la permutation $(3, 1, 4, 2, 5)$ on associe $(3, 5, 2, 4, 1)$. Cette application échange les montées et les descentes, et est bijective : si deux permutations ont la même image, alors, en retournant cette image, on trouve les deux éléments, qui sont donc égaux, et toute permutation peut être atteinte en prenant « son miroir » comme antécédent. D'où la bijectivité, ce qui permet de conclure.

2. Les deux permutations de $\llbracket 1; 2 \rrbracket$ sont $(1, 2)$ et $(2, 1)$: la première est une permutation alternée haut/bas, et la deuxième est une permutation alternée bas/haut : il y en a donc une de chaque, si bien que $E_2 = 1$.

Les 6 permutations de $\llbracket 1; 3 \rrbracket$ sont $(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2)$ et $(3, 2, 1)$: $(1, 3, 2)$ et $(2, 3, 1)$ sont des permutations alternées haut/bas, $(2, 1, 3)$ et $(3, 1, 2)$ sont des permutations alternées bas/haut (et $(1, 2, 3)$ et $(3, 2, 1)$ ne sont pas alternées du tout) : on a 2 permutations de chaque, si bien que $E_3 = 2$.

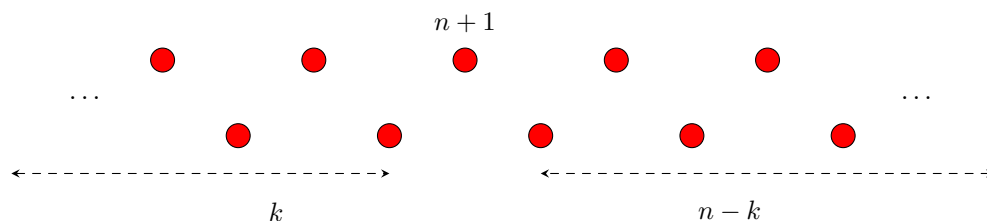
Les 24 permutations de $\llbracket 1; 4 \rrbracket$ sont :

- | | | | | | |
|------------------|------------------|------------------|------------------|------------------|------------------|
| • $(1, 2, 3, 4)$ | • $(1, 4, 2, 3)$ | • $(2, 3, 1, 4)$ | • $(3, 2, 1, 4)$ | • $(3, 4, 2, 1)$ | • $(4, 3, 2, 1)$ |
| • $(1, 2, 4, 3)$ | • $(1, 4, 3, 2)$ | • $(2, 3, 4, 1)$ | • $(3, 2, 4, 1)$ | • $(3, 4, 1, 2)$ | • $(4, 3, 1, 2)$ |
| • $(1, 3, 2, 4)$ | • $(2, 1, 3, 4)$ | • $(2, 4, 1, 3)$ | • $(3, 1, 2, 4)$ | • $(4, 2, 3, 1)$ | • $(4, 1, 2, 3)$ |
| • $(1, 3, 4, 2)$ | • $(2, 1, 4, 3)$ | • $(2, 4, 3, 1)$ | • $(3, 1, 4, 2)$ | • $(4, 2, 1, 3)$ | • $(4, 1, 3, 2)$ |

Les permutations alternées haut/bas sont $(1, 3, 2, 4), (1, 4, 2, 3), (2, 3, 1, 4), (2, 4, 1, 3), (3, 4, 1, 2)$ et les permutations alternées bas/haut sont $(2, 1, 4, 3), (3, 2, 4, 1), (3, 1, 4, 2), (4, 2, 3, 1), (4, 1, 3, 2)$ si bien que $E_4 = 5$.

3. Puisque E_{n+1} est à la fois le nombre de permutations alternées haut/bas et le nombre de permutations bas/haut, et une permutation ne peut pas être des deux types à la fois donc $2E_{n+1}$ est le nombre de permutations alternées (permutations de $\llbracket 1; n+1 \rrbracket$) tout court. Il suffit donc de prouver que le nombre de permutations de $\llbracket 1; n+1 \rrbracket$ qui sont alternées est égal à la somme de droite de l'énoncé.

En fait, tout dépend du nombre de coordonnées se situant avant le $n+1$ dans la permutation : il peut y en avoir de 0 (si le $n+1$ est en première position) à n (si le $n+1$ est en $(n+1)^{\text{e}}$ donc dernière position). Soit donc $k \in \llbracket 0; n \rrbracket$ le nombre de coordonnées se trouvant avant $n+1$:



Il y en a donc $n - k$ se trouvant ensuite (n'oublions pas qu'il y a $n + 1$ entiers).

Il faut déjà commencer par choisir les entiers avant $n + 1$ (sans notion d'ordre) : il y en a $\binom{n}{k}$ puisqu'on doit choisir k entiers appartenant à $\llbracket 1; n \rrbracket$ ($n + 1$ est exclu). Les entiers se trouvant après $n + 1$ sont donc les autres et sont complètement déterminés. Reste à les ordonner.

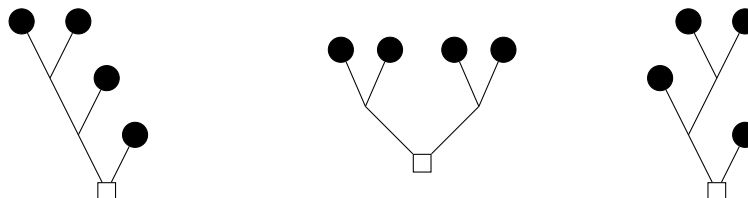
Après $n + 1$, il y a forcément une descente (puisque $n + 1$ est le maximum) donc il y a une montée ensuite (peu importe qu'on soit dans une configuration haut/bas ou bas/haut) : les entiers se trouvant après $n + 1$ forment une partition alternée haut/bas de taille $n - k$, il y a donc E_{n-k} choix possibles pour l'ordre. Les k entiers se trouvant avant $n + 1$ forment une partition alternée de même type que la permutation initiale (haut/bas ou bas/haut, elle finit par une descente puisqu'il y a une montée reliant à $n + 1$, mais cela ne nous avance pas pour savoir par quoi elle commence, tout dépend de la parité de k) mais le type exact n'a aucune importance puisqu'il y en a le même nombre : E_k choix possibles. Par principe multiplicatif, il y a $\binom{n}{k} \times E_k \times E_{n-k}$ choix possibles, et on conclut par le principe additif (les différents cas de figure sont deux à deux incompatibles).

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.

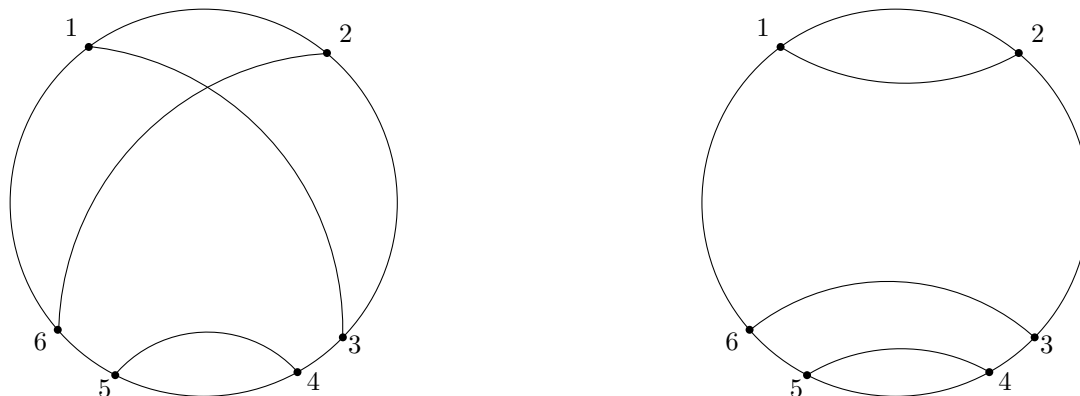
Voici trois exemples d'arbres à 4 feuilles (les disques noirs) :



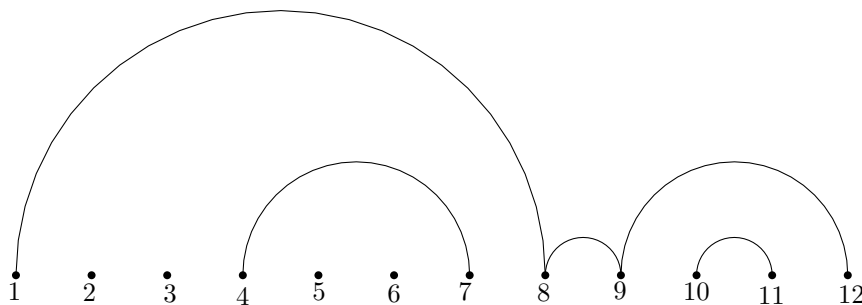
On rappelle que les nombres de Catalan sont définis par $C_0 = 1$ et :

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

2. On dit qu'une partition de l'ensemble $\llbracket 1; k \rrbracket$ 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 $\llbracket 1; n \rrbracket$ (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 $\llbracket 1; n \rrbracket$ 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) .

Correction :

- Il suffit donc de prouver, si on note A_n le nombre cherché, que $A_0 = 1$ et que (A_n) vérifie la même relation de récurrence. Il n'y a qu'un seul arbre à 1 feuille par convention donc $A_0 = 1$. Soit $n \geq 1$, et on se donne un arbre à $n + 1$ feuilles. Si $k \in \llbracket 0; n - 1 \rrbracket$, notons $k + 1$ le nombre de feuilles de l'arbre de gauche (il y a un arbre de gauche et un arbre de droite, qui ont entre 1 et n feuilles). Un tel arbre est entièrement déterminé par l'arbre de gauche qui contient $k + 1$ feuilles, A_k choix possibles, et par l'arbre de droite, qui contient $n - k$ feuilles donc il y a A_{n-k-1} choix possibles. Par principe multiplicatif, il y a $A_k \times A_{n-k-1}$ choix possibles pour un tel arbre puis, ces cas étant incompatibles, par principe additif, on a bien la relation de récurrence voulue ce qui permet de conclure.
- Un bon parenthésage peut-être codé par une $2n$ -liste d'éléments de $\{O; F\}$ où un O représente une parenthèse ouvrante et un F une parenthèse fermante, avec la condition qu'en parcourant la liste de gauche à droite, le nombre de F soit toujours inférieur ou égal au nombre de O , et aussi en se souvenant qu'il y a n fois la lettre O et n fois la lettre F .

On s'inspire du dernier dessin de l'énoncé. Étant donné un bon parenthésage $x = (x_1, x_2, \dots, x_{2n})$ on associe une partition de $\llbracket 1; n \rrbracket$ de la façon suivante : on va de 2 en 2 concernant les parenthèses : (x_1, x_2) puis (x_3, x_4) etc.

- Si les deux parenthèses (x_{2k+1}, x_{2k+2}) sont ouvrantes (c'est-à-dire si on a un couple (O, O)), alors on fait partir un chemin vers le haut comme ce qu'on fait aux points 1, 4 et 10.
- Si les deux parenthèses (x_{2k+1}, x_{2k+2}) sont fermantes (c'est-à-dire si on a un couple (F, F)), alors on fait atterrir un chemin vers le bas comme ce qu'on fait aux points 7, 11 et 12.
- Si on a un couple (O, F) , alors on ne fait rien, comme pour les points 2, 3, 5, 6.
- Si on a un couple (F, O) , on fait atterrir puis repartir le « chemin encore en l'air qui a le point de départ le plus proche » (c'est-à-dire la dernière parenthèse ouvrante encore non refermée), comme pour les points 8, 9.

On définit alors l'image du parenthésage x comme étant la partition dont les éléments sont les ensembles de points reliés entre eux : par exemple, la partition de l'énoncé est la partition formée des ensembles :

$$\{1; 8; 9; 12\}, \{2\}, \{3\}, \{4; 7\}, \{5\}, \{6\}, \{10; 11\}$$

Montrons que la fonction ainsi définie (à un bon parenthésage on associe la partition construite ci-dessus) est une bijection entre ces ensembles :

- L'injectivité est immédiate : si on a une partition, on la dessine comme ci-dessus, et si on a simplement un départ, alors on a deux parenthèses ouvrantes, si on a un point isolé, on a une parenthèse ouvrante suivie d'une parenthèse fermante etc. De façon peut-être plus rigoureuse : si deux parenthésages diffèrent, il y a un endroit où deux couples seront différents et auront donc une image différentes, d'où l'injectivité.
- Il est tout aussi évident qu'une partition aura un antécédent : à un singleton correspond un couple (O, F) etc. Par exemple, pour la partition non croisée de l'exercice (celle en cercle), que je vous laisse dessiner tout seuls « comme un arc-en-ciel », on retrouve le parenthésage $(O, O, F, F, O, O, O, O, F, F, F, F)$.
- Il reste à prouver que l'image d'un bon parenthésage est une partition non croisée, et l'antécédent d'une partition non croisée est un bon parenthésage.

Tout d'abord, par construction, une partition croisée ne peut pas être donnée par la fonction ci-dessus puisque « quand il y a un atterrissage », on ferme le chemin qui est le plus proche, donc un chemin ne peut pas se fermer sur un plus proche, la partition ne peut pas se croiser, et puisqu'on part d'un bon parenthésage, quand on ferme une parenthèse, il y en a au moins une ouverte à ce moment là.

Enfin, il ne peut y avoir d'atterrissage que s'il y a eu décollage auparavant, et donc les parenthèses fermantes ne peuvent arriver que s'il y a eu auparavant des parenthèses ouvrantes en nombre supérieur, et donc on a bien un bon parenthésage au départ. Ce qui permet de conclure.

Il y a donc autant de partitions non croisées que de bons parenthésages : il y en a donc C_n puisque C_n est par définition le nombre de bons parenthésages.

3. Soit $n \geq 1$ et soit $k \in \llbracket 1; n \rrbracket$. Notons k le premier k suivant 1 dans la partition (non croisée) : 8 dans l'exemple arc-en-ciel de l'énoncé. Puisque la partition est croisée, aucun élément compris entre 1 et k n'est relié à un élément strictement supérieur à k . En d'autres termes, les éléments de $\llbracket 2; k-1 \rrbracket$ forment une partition non croisée de $\llbracket 2; k-1 \rrbracket$, et il y a donc γ_{k-2} façons de faire. De même, les entiers de k à n forment une partition de $\llbracket k; n \rrbracket$ et donc il y a γ_{n-k} possibilités (k est exclu dans le premier cas, car $k-1$ ne peut pas être relié à k puisque k est le plus proche voisin de 1, mais il faut prendre k en compte à droite puisque k peut être relié à $k+1$). Par principe additif (tous les cas sont incompatibles : 1 n'a qu'un seul « plus proche voisin »), on a :

$$\gamma_n = \sum_{k=1}^n \gamma_{k-2} \gamma_{n-k}$$

Il suffit de poser $j = k-1, k = j+1$ pour conclure (la relation de récurrence est la même, et $\gamma_0 = C_0 = 1$ par convention : même relation de récurrence, même premier terme, donc même suite par récurrence forte).

17.3 Problèmes ensemblistes

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

Correction : Notons S cette somme. L'ensemble $\mathcal{P}(E)$ étant l'union disjointe des $\mathcal{P}_k(E)$, pour k allant de 0 à n ($\mathcal{P}_k(E)$ désignant l'ensemble des parties de E à k éléments) :

$$S = \sum_{k=0}^n \sum_{X, \text{card}(X)=k} k$$

k ne dépend pas de l'objet sommé sur la deuxième somme qui est X donc est multiplié par le nombre de termes, à savoir le nombre de parties X de cardinal k . Or, il y a $\binom{n}{k}$ telles parties, si bien que

$$S = \sum_{k=0}^n k \binom{n}{k}$$

On raisonne ensuite comme dans l'exercice 41 du chapitre 3.

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 ?

Correction : Soient i et $j \in \llbracket 1; n \rrbracket$, cherchons le nombre de tels couples avec $\text{card}(A) = i$ et $\text{card}(B) = j$. Un tel couple est entièrement déterminé par :

- le choix de A : $\binom{n}{i}$ choix possibles (il y a $\binom{n}{i}$ parties de E à i éléments).
- le choix de l'unique élément de A qui sera le seul élément de $A \cap B$: i choix possibles.
- Les autres éléments de B , au nombre de $j-1$, à choisir parmi les éléments de $E \setminus A$ (les autres éléments de B n'appartiennent pas à A) : il y a donc $\binom{n-i}{j-1}$ choix possibles.

Par principe multiplicatif, il y en a $i \binom{n}{i} \binom{n-i}{j-1}$. Par principe additif (les différents cas de figure sont incompatibles), le nombre cherché est

$$S = \sum_{i=1}^n \sum_{j=1}^n i \binom{n}{i} \binom{n-i}{j-1}$$

Or, le second coefficient binomial est nul si $j-1 > n-i$ donc la deuxième somme va en fait de 1 à $n-i+1$:

$$\begin{aligned}
S &= \sum_{i=1}^n \sum_{j=1}^{n-i+1} i \binom{n}{i} \binom{n-i}{j-1} \\
&= \sum_{i=1}^n i \binom{n}{i} \sum_{k=0}^{n-i} \binom{n-i}{k} \\
&= \sum_{i=1}^n i \binom{n}{i} 2^{n-i} \\
&= \sum_{i=1}^n i \times \frac{n!}{i!(n-i)!} \times 2^{n-i} \\
&= \sum_{i=1}^n \frac{n!}{(i-1)!(n-1-(i-1))!} \times 2^{n-i} \\
&= n \sum_{i=1}^n \frac{(n-1)!}{(i-1)!(n-1-(i-1))!} \times 2^{n-i} \\
&= n \sum_{i=1}^n \binom{n-1}{i-1} \times 2^{n-i} \\
&= n \sum_{k=0}^{n-1} \binom{n-1}{k} \times 2^{n-k-1} \\
&= n \times 2^{n-1} \times \sum_{k=0}^{n-1} \binom{n-1}{k} \times \frac{1}{2^k} \\
&= n \times 2^{n-1} \times \left(1 + \frac{1}{2}\right)^{n-1} \\
&= n \times 2^{n-1} \times \frac{3^{n-1}}{2^{n-1}} \\
&= n \times 3^{n-1}
\end{aligned}$$

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 ?

Correction : Quand on dit « tenir compte de l'ordre », cela signifie qu'une partition E_1, \dots, E_n n'est pas la même que la partition $E_2, E_1, E_3, \dots, E_n$. Cependant, les E_i sont des ensembles : dans les E_i , l'ordre ne compte pas. Une telle partition est entièrement déterminée par l'ordre des éléments de E : les p premiers iront dans E_1 , les p suivants dans E_2 etc. Cela devrait nous donner $(np)!$ permutations, mais à l'intérieur d'un même E_i , l'ordre ne compte pas : pour « annuler » le fait que l'ordre compte (comme pour une anagramme), on divise pour chaque E_i par $p!$. Par conséquent, le nombre cherché est $(np)!/(p!)^n$. On aurait aussi pu raisonner de la façon suivante : $\binom{np}{p}$ choix pour les éléments de E_1 , $\binom{np-p}{p}$ choix pour les éléments de E_2 etc. jusqu'à $\binom{2p}{p}$ pour les éléments de E_{n-1} et $\binom{p}{p}$ pour les éléments de E_n . On fait le produit, on simplifie les factorielles et on obtient le même résultat.

Si l'ordre ne compte pas, il suffit de diviser par $n!$ pour annuler le fait que l'ordre compte dans l'ordre précédent. On trouve finalement

$$\frac{(np)!}{(p!)^n \times n!}$$

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

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

Correction :

1. Donnons le nombre de tels couples avec $\text{card}(Y) = k$, pour $k \in \llbracket 0; n \rrbracket$. Un tel couple est entièrement déterminé par le choix de Y , $\binom{n}{k}$ choix possibles, puis par le choix de X une partie de Y , 2^k choix possibles (car $\text{card}(Y) = k$). Par principe multiplicatif, il y a $2^k \times \binom{n}{k}$ choix possibles puis, par principe additif, le nombre cherché est

$$\sum_{k=0}^n \binom{n}{k} 2^k = (2+1)^n = 3^n$$

2. On trouve 3^n par un raisonnement analogue.
3. Soit $k \in \llbracket 0; n \rrbracket$. Donnons le nombre de tels triplets avec $\text{card}(Z) = k$. Un tel triplet est entièrement déterminé par le choix de Z , $\binom{n}{k}$ possibilités, et par le choix du couple (X, Y) avec $X \subset Y$ parties de Z , ensemble à k éléments, et il y a 3^k possibilités d'après la question 1. Par principe multiplicatif, il y a $\binom{n}{k} 3^k$ tels triplets donc, par principe additif, on trouve de même qu'il y a 4^n tels triplets.

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).

Correction :

1. Soit $k \in \llbracket 1; n-1 \rrbracket$ (les ensembles A et B doivent être non vides). Cherchons les couples solutions avec $\text{card}(A) = k$. Un tel couple est entièrement déterminé par A puisqu'on a $B = \overline{A}$: il y a donc $\binom{n}{k}$ choix possibles. Par principe additif, le nombre cherché est

$$\sum_{k=1}^n \binom{n}{k} = 2^n - 2$$

On aurait aussi pu raisonner de la façon suivante : pour chaque élément, il y a 2 choix possibles : soit il appartient à A , soit à B . Il existe donc 2^n (par principe multiplicatifs) couples (A, B) d'intersection vide tels que $A \cup B = E$, auxquels il faut enlever les deux couples (\emptyset, E) et (E, \emptyset) , ce qui donne encore $2^n - 2$.

2. Soit $k \in \llbracket 1; n-2 \rrbracket$ (B et C doivent être non vides : A ne peut pas avoir plus de $n-2$ éléments). Cherchons le nombre de tels triplets tels que $\text{card}(A) = k$. Un tel triplet est entièrement déterminé par A , $\binom{n}{k}$ choix possibles, et par le couple (B, C) tels que B et C forment une partition de \overline{A} (une partition est non vide par définition). D'après la question précédente, il y a $2^{n-k} - 2$ tels couples, si bien que le nombre cherché est

$$\begin{aligned} \sum_{k=1}^{n-2} \binom{n}{k} \times (2^{n-k} - 2) &= \sum_{k=1}^{n-2} \binom{n}{k} 2^{n-k} - 2 \sum_{k=1}^{n-2} \binom{n}{k} \\ &= (1+2)^n - 2^n - 1 - n \times 2 - 2(2^n - 1 - 1 - n) \\ &= 3^n - 2^n - 1 - 2n - 2 \times 2^n + 2 + 2 + 2n \\ &= 3^n - 3 \times 2^n + 3 \end{aligned}$$

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 ?

Correction : Notons A l'alphabet et $E = A^2$ l'ensemble des initiales (si on a un nom composé, on ne prend que la première lettre) si bien que $\text{card}(E) = 26^2$. D'après le principe des tiroirs, si E contient au moins $26^2 + 1$ éléments, au moins deux sont égaux. En conclusion, si un village contient au moins $26^2 + 1 = 677$ habitants, au moins deux ont les mêmes initiales.

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

Correction : Notons ces entiers $a_1 < a_2 < \dots < a_{51}$ dans l'ordre croissant. Notons, pour tout $i \in \llbracket 1; 50 \rrbracket$, $b_i = a_{i+1} - a_i$. Alors $b_i \geq 1$ car $a_{i+1} > a_i$. Supposons que, pour tout i , $b_i \geq 2$. Alors, par somme :

$$\sum_{i=1}^{50} (a_{i+1} - a_i) \geq \sum_{i=1}^{50} 2$$

c'est-à-dire que $a_{51} - a_1 \geq 100$ ce qui est absurde. Il existe donc i tel que $a_{i+1} - a_i = 1$ ce qui est le résultat voulu.

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...).

Correction : Notons n le nombre d'élèves de la classe, a_1, \dots, a_n le nombre de mains serrées par les élèves, qu'on numérote de 1 à n (a_k est donc le nombre de mains serrées par l'élève numéro k). Les entiers a_k appartiennent à l'ensemble $\llbracket 0; n-1 \rrbracket$ (un élève peut ne serrer aucune main ou serrer la main de tout le monde sauf lui, et tous les cas intermédiaires sont possibles). Le problème est que cet ensemble a n éléments, c'est-à-dire autant qu'il y a d'élèves, ce qui ne nous permet pas d'appliquer le principe des tiroirs. Supposons que tous les a_k soient distincts. Alors tous les tiroirs sont occupés, c'est-à-dire que pour tout $i \in \llbracket 0; n-1 \rrbracket$, il existe k tel que $a_k = i$. En particulier, il existe un élève qui ne serre la main de personne ($a_k = 0$) et un élève qui serre la main de tout le monde ($a_p = n-1$) mais ces deux cas ne peuvent pas se produire en même temps ! Les a_k ne sont pas tous distincts donc deux élèves serrent le même nombre de mains.

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.

Correction :

1. Les congruences modulo n étant en nombre fini, et les puissances de 10 en nombre infini, d'après le principe des tiroirs, il y a une infinité de puissances de 10 ayant la même congruence modulo n donc en particulier il en existe n .
2. Si on somme ces n puissances de 10 (distinctes), on a un nombre qui ne s'écrit qu'avec des 1 et des 0 et qui est divisible par n car on somme n fois la même congruence modulo n .

Exercice 44 : ☼☼ Montrer que si on prend $n+1$ entiers distincts dans $\llbracket 1; 2n \rrbracket$, 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.

Correction : Suivons l'indication de l'énoncé et intéressons-nous à la valuation p -adique de ces nombres (notés a_1, \dots, a_{n+1}). Plus précisément, pour tout k , il existe b_k impair tel que $a_k = 2^{v_2(a_k)} \times b_k$ (tout entier est égal à 2 à la puissance sa valuation 2-adique multiplié par un nombre impair, le produit de ses facteurs premiers impairs restants). Les b_k sont donc des nombres impairs compris entre 1 et $2n$: il y en a n (les entiers 1, 3, 5, \dots , $2n-1$). Puisqu'il y a $n+1$ nombres a_k , il y a $n+1$ nombres b_k à choisir parmi n nombres impairs donc au moins deux sont égaux d'après le principe des tiroirs. Dès lors, il existe k_1 et k_2 tels que $b_{k_1} = b_{k_2}$ si bien que $a_{k_1} = 2^{v_2(a_{k_1})} \times b_{k_1}$ et $a_{k_2} = 2^{v_2(a_{k_2})} \times b_{k_1}$ (les parties impaires sont égales). Celui des deux qui a la plus petite valuation 2-adique divise l'autre.

Enfin, de même que dans l'exercice 41, il y a deux nombres consécutifs parmi les a_k donc ils sont premiers entre eux.

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

Correction : Notons, pour tout $k \in \llbracket 1; n \rrbracket$, b_k la congruence de $a_1 + \dots + a_k$ modulo n . Il y a n congruences modulo n et n entiers b_k . Si deux b_k ont la même congruence, disons b_k et b_l avec $k < l$, alors $b_l - b_k = a_{k+1} + \dots + a_l$ est divisible par n . Sinon, c'est que toutes les congruences modulo n sont atteintes, et en particulier la congruence à 0 modulo n si bien qu'il existe k tel que $a_1 + \dots + a_k$ soit congru à 0 modulo n i.e. soit divisible par 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.

Correction : Notons ces points A_1, \dots, A_{1000} . Les directions des vecteurs $\overrightarrow{A_i A_j}$ directeurs des droites joignant deux points sont en nombre fini, donc il existe un vecteur \vec{i} qui n'est colinéaire à aucun de ces vecteurs. Soit \vec{j} un vecteur orthogonal à \vec{i} et soit O un point quelconque du plan si bien que $(O; \vec{i}, \vec{j})$ soit un repère orthogonal (pas forcément orthonormé). Puisque aucun $\overrightarrow{A_i A_j}$ n'est colinéaire à \vec{i} , aucune droite n'est horizontale : les A_i , dans ce repère, ont tous des ordonnées différentes : on peut ranger ces points dans l'ordre strictement croissant des ordonnées, i.e. $A_i = (x_i, y_i)$ avec $y_1 < y_2 < \dots < y_{1000}$. Il suffit de prendre une droite d'équation $y = \alpha$ avec $y_{500} < \alpha < y_{501}$ i.e. une droite horizontale (dans le repère choisi) avec 500 points au-dessus et 500 points en dessous (ce qui est possible encore une fois car les points ont tous des ordonnées distinctes).

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 .

Correction : De même que dans l'exercice 5, $\text{card}(E) = 2^n$. Il y a 2^n congruences modulo 2^n donc, pour répondre, il suffit de prouver que tous les éléments de E ont une congruence différente modulo 2^n . Soient x et y deux éléments de E ayant la même congruence modulo 2^n , et montrons qu'ils sont égaux, ce qui permettra de conclure. En particulier, $y - x$ est divisible par 2^n . Sans perte de généralité, supposons $y \geq x$. Supposons dans l'absurde que $y \neq x$, donc $y > x$. Notons $y = a_{n-1} \dots a_0$ (avec les a_i égaux à 1 ou 2) et $x = b_{n-1} \dots b_0$. Soit $i \leq n-1$ le plus petit indice tel que $a_i \neq b_i$ i.e. l'indice du premier chiffre différent chez a et chez b . Si $a_i = 2$ et $b_i = 1$ alors $y - x$ est de la forme $c_{n-1} \dots c_{i+1} \underbrace{1}_{1} 0 \dots 0$ (attention, les

c_k ne sont pas forcément égaux à 1 ou 2) donc n'est pas divisible par 2^n car est égal à $c_{n-1} \dots c_{i+1} 1 \times 10^i$ donc $2^i \times 5^i \times N$ avec N impair donc 2^i multiplié par un nombre impair donc n'est pas divisible par 2^n , ce qui est absurde. Si $a_i = 1$ et $b_i = 2$, si bien que $y - x$ est de la forme $c_{n-1} \dots c_{i+1} 90 \dots 0$ et on conclut de la même façon : on a donc forcément $x = y$ ce qui permet de conclure.

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} ?

Correction : Notons ces trois entiers, respectivement, n_1, n_2, n_3 . On a :

$$n_1 = 2^{60} \times 5^{60}, \quad n_2 = 2^{100} \times 5^{50} \quad \text{et} \quad n_3 = 2^{40} \times 3^{40} \times 5^{40}$$

Notons E_1 l'ensemble des diviseurs de n_1 , et idem pour E_2 et E_3 . D'après la formule du crible :

$$\text{card}(E_1 \cup E_2 \cup E_3) = \text{card}(E_1) + \text{card}(E_2) + \text{card}(E_3) - \text{card}(E_1 \cap E_2) - \text{card}(E_1 \cap E_3) - \text{card}(E_2 \cap E_3) + \text{card}(E_1 \cap E_2 \cap E_3)$$

Rappelons que les diviseurs d'un nombre de la forme $p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$ (où les p_i sont premiers distincts) sont exactement les entiers de la forme $p_1^{\beta_1} \times \dots \times p_k^{\beta_k}$, où $\beta_i \in \llbracket 0; \alpha_i \rrbracket$, c'est-à-dire que β_i peut prendre $\alpha_i + 1$ valeurs, et par principe multiplicatif, cet entier a $(\alpha_1 + 1) \dots (\alpha_k + 1)$ diviseurs.

Il en découle que n_1 admet 61^2 diviseurs, n_2 admet 101×51 diviseurs, et n_3 en admet 41^3 . De plus, un entier divise deux entiers a et b si et seulement s'il divise leur PGCD (cf. chapitre 6). Par conséquent, un entier appartient à $E_1 \cap E_2$ si et seulement s'il divise $n_1 \wedge n_2 = 2^{60} \times 5^{50}$ donc il y a 61×51 diviseurs communs à n_1 et n_2 . De même, $n_2 \wedge n_3 = 2^{40} \times 5^{40}$ donc il y a 41^2 diviseurs communs à n_2 et n_3 , et $n_1 \wedge n_3 = 2^{40} \times 5^{40}$ donc il y a aussi 41^2 diviseurs communs à n_1 et n_3 , et enfin $n_1 \wedge n_2 \wedge n_3 = 2^{40} \times 5^{40}$ donc il y a aussi 41^2 diviseurs communs à n_1, n_2, n_3 . Finalement :

$$\begin{aligned} \text{card}(E_1 \cup E_2 \cup E_3) &= 61^2 + 101 \times 51 + 41^3 - 61 \times 51 - 41^2 - 41^2 + 41^2 \\ &= 76363 \end{aligned}$$

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

Correction : D'après la formule du crible pour trois ensembles, si on note E_2 l'ensemble des entiers compris entre 1 et 2024 et divisibles par 2, et idem pour E_3, E_5, E_6 etc. :

$$\text{card}(E_2 \cup E_3 \cup E_5) = \text{card}(E_2) + \text{card}(E_3) + \text{card}(E_5) - \text{card}(E_2 \cap E_3) - \text{card}(E_2 \cap E_5) - \text{card}(E_3 \cap E_5) + \text{card}(E_2 \cap E_3 \cap E_5)$$

Or, 2, 3 et 5 sont premiers entre eux deux à deux donc $E_2 \cap E_3 = E_6$, $E_2 \cap E_5 = E_{10}$, $E_3 \cap E_5 = E_{15}$ et $E_2 \cap E_3 \cap E_5 = E_{30}$. Rappelons (cf. chapitre 2 par exemple) qu'il y a $\lfloor n/k \rfloor$ entiers compris entre 1 et n divisibles par k . Dès lors :

$$\begin{aligned} \text{card}(E_2 \cup E_3 \cup E_5) &= \left\lfloor \frac{2024}{2} \right\rfloor + \left\lfloor \frac{2024}{3} \right\rfloor + \left\lfloor \frac{2024}{5} \right\rfloor - \left\lfloor \frac{2024}{6} \right\rfloor - \left\lfloor \frac{2024}{10} \right\rfloor - \left\lfloor \frac{2024}{15} \right\rfloor + \left\lfloor \frac{2024}{30} \right\rfloor \\ &= 1012 + 674 + 404 - 337 - 202 - 134 + 67 \\ &= 1484 \end{aligned}$$

Exercice 50 - Formule du crible : ★★★ Montrer que si E_1, \dots, E_n sont des ensembles finis, alors :

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

Correction : Montrons la formule du crible par récurrence forte sur n . Si $n = 1$ alors

$$\sum_{k=1}^n (-1)^{k+1} \sum_{J \subset \llbracket 1; n \rrbracket, \text{card}(J)=k} \text{card} \left(\bigcap_{j \in J} A_j \right) = (-1)^2 \sum_{J \subset \{1\}, \text{card}(J)=1} \text{card} \left(\bigcap_{j \in J} A_j \right) = \text{card}(A_1).$$

Soit $n \in \mathbb{N}^*$. Supposons que la propriété soit vraie jusqu'au rang n . Montrons-là au rang $n+1$: donnons-nous A_1, \dots, A_{n+1} des ensembles. La formule de Poincaré (pour deux ensembles) entraîne que

$$\begin{aligned} \text{card} \left(\bigcup_{i=1}^{n+1} A_i \right) &= \text{card} \left(\bigcup_{i=1}^n A_i \right) + \text{card}(A_{n+1}) - \text{card} \left(\left(\bigcup_{i=1}^n A_i \right) \cap A_{n+1} \right) \\ &= \text{card} \left(\bigcup_{i=1}^n A_i \right) + \text{card}(A_{n+1}) - \text{card} \left(\bigcup_{i=1}^n (A_i \cap A_{n+1}) \right). \end{aligned}$$

L'hypothèse de récurrence entraîne que

$$\begin{aligned} -\text{card} \left(\bigcup_{i=1}^n (A_i \cap A_{n+1}) \right) &= -\sum_{k=1}^n (-1)^{k+1} \sum_{J \subset \llbracket 1; n \rrbracket, \text{card}(J)=k} \text{card} \left(\bigcap_{j \in J} (A_j \cap A_{n+1}) \right) \\ &= \sum_{k=1}^n (-1)^{k+2} \sum_{J \subset \llbracket 1; n+1 \rrbracket, n+1 \in J, \text{card}(J)=k+1} \text{card} \left(\bigcap_{j \in J} A_j \right) \\ &= \sum_{p=2}^{n+1} (-1)^{p+1} \sum_{J \subset \llbracket 1; n+1 \rrbracket, n+1 \in J, \text{card}(J)=p} \text{card} \left(\bigcap_{j \in J} A_j \right), \end{aligned}$$

en ayant fait le changement de variable $p = k + 1$. On a aussi

$$\begin{aligned} \text{card}(A_1 \cup A_2 \cup \dots \cup A_n) &= \sum_{k=1}^n (-1)^{k+1} \sum_{J \subset \llbracket 1; n \rrbracket, \text{card}(J)=k} \text{card} \left(\bigcap_{j \in J} A_j \right) \\ &= \sum_{k=1}^n (-1)^{k+1} \sum_{J \subset \llbracket 1; n+1 \rrbracket, n+1 \notin J, \text{card}(J)=k} \text{card} \left(\bigcap_{j \in J} A_j \right) \end{aligned}$$

Ainsi

$$\begin{aligned} \text{card} \left(\bigcup_{i=1}^{n+1} A_i \right) &= \sum_{k=1}^{n+2} \text{card}(A_k) + (-1)^{n+2} \text{card} \left(\bigcap_{1 \leq j \leq n+1} A_j \right) \\ &\quad + \sum_{k=2}^n (-1)^{k+1} \left(\sum_{J \subset \llbracket 1; n+1 \rrbracket, n+1 \in J, \text{card}(J)=k} \text{card} \left(\bigcap_{j \in J} A_j \right) + \sum_{J \subset \llbracket 1; n+1 \rrbracket, n+1 \notin J, \text{card}(J)=k} \text{card} \left(\bigcap_{j \in J} A_j \right) \right) \\ &= \sum_{k=1}^{n+2} \text{card}(A_k) + \sum_{k=2}^n (-1)^{k+1} \sum_{J \subset \llbracket 1; n+1 \rrbracket, \text{card}(J)=k} \text{card} \left(\bigcap_{j \in J} A_j \right) + (-1)^{n+2} \text{card} \left(\bigcap_{1 \leq j \leq n+1} A_j \right) \\ &= \sum_{k=1}^{n+1} (-1)^{k+1} \sum_{J \subset \llbracket 1; n+1 \rrbracket, \text{card}(J)=k} \text{card} \left(\bigcap_{j \in J} A_j \right) \end{aligned}$$

D'où le résultat par récurrence.

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 \mathcal{C}^∞ 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.

Correction : Soit $z = (xy)^{-1}$. Alors $(xy) * z = z * (xy) = e$ (le neutre). La loi étant associative, $x * (yz) = e$ donc x est symétrisable à gauche donc est symétrisable puisque la loi est commutative. Par symétrie des rôles (x et y jouent le même rôle puisque la loi est commutative), y est symétrisable.

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.

Correction :

1. Supposons donc que tout élément de E soit régulier que $*$ soit distributive par rapport à elle-même. Soit $x \in E$. $*$ étant distributive par rapport à elle-même, $x * (x * x) = (x * x) * (x * x)$ et $(x * x)$ est régulier donc $x = x * x$, x est idempotent.
2. Supposons que tout élément de E soit régulier et que $*$ soit associative. Soient x et y idempotents. On a donc : $x * y = (x * x) * y$ et la loi est associative donc $x * y = x * (x * y)$. x est régulier donc $y = x * y$. De même, $x * y = x * (y * y) = (x * y) * y$ et y est régulier donc $x = x * y$ donc $x = y$: il y a au plus un élément idempotents.

Exercice 3 : ★ On munit l'ensemble \mathbb{Q}^2 d'une loi définie par $(x_1, y_1) \otimes (x_2, y_2) = (x_1 x_2, y_1 x_2 + y_2)$ 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.

Correction :

1. Non, elle n'est pas commutative puisque $(1, 1) \otimes (0, 0) = (0, 0)$ et $(0, 0) \otimes (1, 1) = (0, 1)$.
2. Soient $(x_1, y_1), (x_2, y_2)$ et (x_3, y_3) trois éléments de \mathbb{Q}^2 . Tout d'abord :

$$\begin{aligned}
 (x_1, y_1) \otimes ((x_2, y_2) \otimes (x_3, y_3)) &= (x_1, y_1) \otimes (x_2 x_3, y_2 x_3 + y_3) \\
 &= (x_1 x_2 x_3, y_1 (x_2 x_3) + y_2 x_3 + y_3) \\
 &= (x_1 x_2 x_3, y_1 x_2 x_3 + y_2 x_3 + y_3)
 \end{aligned}$$

D'autre part :

$$\begin{aligned}
 ((x_1, y_1) \otimes (x_2, y_2)) \otimes (x_3, y_3) &= (x_1 x_2, y_1 x_2 + y_2) \otimes (x_3, y_3) \\
 &= (x_1 x_2 x_3, (y_1 x_2 + y_2) x_3 + y_3) \\
 &= (x_1 x_2 x_3, y_1 x_2 x_3 + y_2 x_3 + y_3)
 \end{aligned}$$

La loi est donc bien associative. Soit $(a, b) \in \mathbb{Q}^2$.

$$\begin{aligned}
 (a, b) \text{ est un élément neutre} &\iff \forall (x, y) \in \mathbb{Q}^2, (x, y) \otimes (a, b) = (a, b) \otimes (x, y) = (x, y) \\
 &\iff \forall (x, y) \in \mathbb{Q}^2, (xa, ay + b) = (ax, bx + y) = (x, y) \\
 &\iff a = 1 \quad \text{et} \quad \forall (x, y) \in \mathbb{Q}^2, ay + b = bx + y = y \\
 &\iff a = 1 \quad \text{et} \quad b = 0
 \end{aligned}$$

$(1, 0)$ est donc l'unique élément neutre (on peut aussi raisonner par analyse synthèse si on n'est pas à l'aise avec les équivalences).

3. Soit $(x, y) \in \mathbb{Q}^2$. Soit $(a, b) \in \mathbb{Q}^2$.

$$\begin{aligned}
 (a, b) \text{ est le symétrique de } (x, y) &\iff (x, y) \otimes (a, b) = (a, b) \otimes (x, y) = (1, 0) \\
 &\iff (xa, ay + b) = (ax, bx + y) = (1, 0) \\
 &\iff x \neq 0 \quad \text{et} \quad a = \frac{1}{x} \quad \text{et} \quad \frac{y}{x} + b = bx + y = 0 \\
 &\iff x \neq 0 \quad \text{et} \quad a = \frac{1}{x} \quad \text{et} \quad b = -\frac{y}{x}
 \end{aligned}$$

Finalement, (x, y) admet un symétrique si et seulement si $x \neq 0$ et alors son symétrique est $\left(\frac{1}{x}, -\frac{y}{x}\right)$.

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 $a \circ b = a^2b^2$.

Correction :

1. La loi \circ est commutative, mais $*$ ne l'est pas car $1 * 0 = 1 \neq 2 = 0 * 1$. Soit $(a, b, c) \in \mathbb{N}^3$.

$$\begin{aligned} a \circ (b \circ c) &= a \circ (2bc) \\ &= 2a(2bc) \\ &= 4abc \end{aligned}$$

tandis que

$$\begin{aligned} (a \circ b) \circ c &= (2ab) \circ c \\ &= 2(2ab)c \\ &= 4abc \end{aligned}$$

La loi \circ est donc associative. De plus :

$$\begin{aligned} a * (b * c) &= a * (b + 2c) \\ &= a + 2(b + 2c) \\ &= a + 2b + 4c \end{aligned}$$

et

$$\begin{aligned} (a * b) * c &= (a + 2b) * c \\ &= a + 2b + 2c \end{aligned}$$

Attention, dire qu'on n'obtient pas la même chose est faux et insuffisant : par exemple, pour $a = b = c = 0$, on obtient la même chose, il faut un contre-exemple explicite. En remarque que, si $a = b = c = 1$, les deux quantités sont différentes : la loi $*$ n'est pas associative. Enfin, on a d'une part

$$\begin{aligned} a * (b \circ c) &= a * (2bc) \\ &= a + 2(2bc) \\ &= a + 4bc \end{aligned}$$

et

$$\begin{aligned} (a * b) \circ (a * c) &= (a + 2b) \circ (a + 2c) \\ &= 2(a + 2b)(a + 2c) \\ &= 2a^2 + 4ab + 4ac + 8bc \end{aligned}$$

Idem, il faut un contre-exemple explicite : avec $a = b = c = 1$, on trouve des résultats distincts : la loi $*$ n'est pas distributive par rapport à \circ . De plus :

$$\begin{aligned} a \circ (b * c) &= a \circ (b + 2c) \\ &= 2a(b + 2c) \\ &= 2ab + 4ac \end{aligned}$$

et

$$\begin{aligned}
(a \circ b) * (a \circ c) &= (2ab) * (2ac) \\
&= 2ab + 2(2ac) \\
&= 2ab + 4ac
\end{aligned}$$

La loi \circ est distributive par rapport à la loi $*$.

2. La loi $*$ n'est rien d'autre que la somme, qui est donc commutative et associative. La loi \circ n'est pas commutative car $1 \circ 2 = 4 \neq 2 \circ 1 = 2$. Soit $(a, b, c) \in \mathbb{N}^3$.

$$\begin{aligned}
a \circ (b \circ c) &= a \circ (bc^2) \\
&= a(bc^2)^2 \\
&= ab^2c^4
\end{aligned}$$

tandis que

$$\begin{aligned}
(a \circ b) \circ c &= (ab^2) \circ c \\
&= (ab^2)c^2 \\
&= ab^2c^2
\end{aligned}$$

Là aussi, il faut un contre-exemple explicite, par exemple $a = b = 1$ et $c = 2$: la loi \circ n'est pas associative. Enfin, on a d'une part

$$\begin{aligned}
a * (b \circ c) &= a * (bc^2) \\
&= a + bc^2
\end{aligned}$$

et

$$\begin{aligned}
(a * b) \circ (a * c) &= (a + b) \circ (a + c) \\
&= (a + b)(a + c)^2
\end{aligned}$$

Là aussi, un contre-exemple : $a = 1, b = 0, c = 2$, la loi $*$ n'est pas distributive par rapport à la loi \circ . De plus :

$$\begin{aligned}
a \circ (b * c) &= a \circ (b + c) \\
&= 2a(b + c) \\
&= 2ab + 2ac
\end{aligned}$$

et

$$\begin{aligned}
(a \circ b) * (a \circ c) &= (ab^2) * (ac^2) \\
&= ab^2 + ac^2
\end{aligned}$$

En prenant $a = 1, b = c = 3$, on trouve que la loi \circ n'est pas distributive par rapport à la loi $*$.

3. Les lois $*$ et \circ sont commutatives. Soit $(a, b, c) \in \mathbb{N}^3$.

$$\begin{aligned}
a \circ (b \circ c) &= a \circ (b^2c^2) \\
&= a^2(b^2c^2)^2 \\
&= a^2b^4c^4
\end{aligned}$$

tandis que

$$\begin{aligned}
(a \circ b) \circ c &= (a^2b^2) \circ c \\
&= (a^2b^2)^2c^2 \\
&= a^4b^4c^2
\end{aligned}$$

En prenant $a = b = 1$ et $c = 2$, on a un résultat distinct, la loi \circ n'est pas associative. De plus,

$$\begin{aligned}
a * (b * c) &= a * (b^2 + c^2) \\
&= a^2 + (b^2 + c^2)^2 \\
&= a^2 + b^4 + 2b^2c^2 + c^4
\end{aligned}$$

tandis que

$$\begin{aligned}
(a * b) * c &= (a^2 + b^2) * c \\
&= (a^2 + b^2)^2 + c^2 \\
&= a^4 + 2a^2b^2 + b^4 + c^2
\end{aligned}$$

En prenant $a = b = 0$ et $c = 2$, on trouve que la loi $*$ n'est pas associative. Enfin, on a d'une part

$$\begin{aligned}
a * (b \circ c) &= a * (b^2c^2) \\
&= a^2 + (b^2c^2)^2 \\
&= a^2 + b^4c^4
\end{aligned}$$

et

$$\begin{aligned}
(a * b) \circ (a * c) &= (a^2 + b^2) \circ (a^2 + c^2) \\
&= (a^2 + b^2)^2(a^2 + c^2)^2
\end{aligned}$$

En prenant $a = 2$ et $b = c = 0$, on trouve des résultats distincts : la loi $*$ n'est pas distributive par rapport à la loi \circ .
Finalement :

$$\begin{aligned}
a \circ (b * c) &= a \circ (b^2 + c^2) \\
&= a^2(b^2 + c^2)^2 \\
&= a^2(b^4 + 2b^2c^2 + c^4) \\
&= a^2b^4 + 2a^2b^2c^2 + a^2c^4
\end{aligned}$$

et

$$\begin{aligned}
(a \circ b) * (a \circ c) &= (a^2b^2) * (a^2c^2) \\
&= (a^2b^2)^2 + (a^2c^2)^2 \\
&= a^4b^4 + a^4c^4
\end{aligned}$$

En prenant $b = 0$ et $a = c = 2$, on trouve que \circ n'est pas non plus distributive par rapport à $*$.

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 $x \star x = 3$.

Correction :

1. Elle n'est pas commutative car $1 \star 2 = 7$ et $2 \star 1 = 5$. Soit $(a, b, c) \in \mathbb{R}^3$.

$$\begin{aligned}
a \star (b \star c) &= a \star (b + c + bc^2) \\
&= a + b + c + bc^2 + a(b + c + bc^2)^2
\end{aligned}$$

tandis que

$$\begin{aligned}
(a \star b) \star c &= (a + b + ab^2) \star c \\
&= a + b + ab^2 + c + (a + b + ab^2)c^2
\end{aligned}$$

En prenant $a = 1, b = 1$ et $c = 2$, on trouve que la loi n'est pas associative.

2. Soit $e \in \mathbb{R}$.

$$\begin{aligned}
e \text{ est un élément neutre} &\iff \forall x \in \mathbb{R}, x \star e = e \star x = x \\
&\iff \forall x \in \mathbb{R}, x + e + xe^2 = e + x + ex^2 = x \\
&\iff \forall x \in \mathbb{R}, e + xe^2 = e + ex^2 = 0
\end{aligned}$$

0 est solution évidente donc 0 est élément neutre (et c'est même le seul d'après le cours).

3. Soit $x \in \mathbb{R}^*$. Supposons que x admette un inverse noté y . Alors $x \star y = y \star x = 0$ (le neutre) si bien que

$$x + y + xy^2 = y + x + yx^2 = 0$$

Dès lors, $x + y = -xy^2 = -yx^2$ donc, en particulier, $xy^2 = yx^2$. Puisque x est non nul, $y^2 = yx$. Si y est nul, alors y est le neutre donc $x \star y = x \neq 0$, ce qui est exclu, donc on peut simplifier par y si bien que $y = x : x$ est son propre inverse, ce qui est absurde car $x \star x = 2x + x^3 = x(x^2 + 2)$ qui est non nul car $x \neq 0$ et $x^2 + 2 > 0$. En conclusion, un réel non nul n'est pas inversible.

4. Soit $x \in \mathbb{R}$.

$$\begin{aligned}
x \star x = 3 &\iff 2x + x^3 = 3 \\
&\iff x^3 + 2x - 3 = 0
\end{aligned}$$

$x = 1$ est solution évidente : on peut donc factoriser le membre de gauche par $x - 1$: il existe (a, b, c) tel que

$$x^3 + 2x - 3 = (x - 1)(ax^2 + bx + c) = ax^3 + x^2(b - a) + x(c - b) - c$$

On trouve que $a = 1, c = 3$ et $b = 1$. Dès lors,

$$\begin{aligned}
x \star x = 3 &\iff (x - 1)(x^2 + x + 3) = 0 \\
&\iff x = 1 \quad \text{ou} \quad x^2 + x + 3 = 0
\end{aligned}$$

Or, l'équation $x^2 + x + 3 = 0$ n'a pas de solution car son discriminant est strictement négatif. En conclusion, la seule solution de l'équation $x \star x = 3$ est $x = 1$.

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.

Correction :

1. En composant à gauche par l'élément b tel que $b * a = e$ (un tel élément existe par hypothèse), il vient : $b * (a * a) = b * a$. Or, la loi est associative donc $(b * a) * a = b * a$. Or, $b * a = e$ donc $e * a = b * a$, et $e * a = a$ et $b * a = e$ donc on obtient bien $a = e$.
2. Multiplions à gauche par c , l'élément vérifiant $c * b = e$, et la loi est associative (on peut enlever les parenthèses), ce qui donne : $c * b * a = c$ mais $c * b = e$ donc $e * a = c$. Enfin, $e * a = a$ donc $a = c$ c'est-à-dire que $a * b = e$.
3. Soit $a \in E$. Multiplions $a * e$ à gauche par b , l'élément de E tel que $b * a = e$, ce qui donne $b * a * e = e * e$ (la loi est associative). Or, e est neutre à gauche donc $e * e = e$ si bien que $b * (a * e) = b * a$. En multipliant à gauche par a (et en utilisant l'associativité de la loi), il vient : $(a * b) * (a * e) = (a * b) * a$. Or, $a * b = b * a = e$ si bien que $e * (a * e) = a * e$ et $(a * b) * a = e * a = a$ car e est neutre à gauche. On trouve enfin $a * e = a$ ce qui est le résultat voulu.

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. $\star\star\star$ Calculer, pour a inversible et $n \in \mathbb{Z}$, a^n (il s'agit des puissances au sens de la loi $*$).

Correction :

1. La loi $*$ est évidemment commutative. Soit $(a, b, c) \in \mathbb{Q}^3$. D'une part,

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

et d'autre part,

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= a + b + ab + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \\ &= a * (b * c) \end{aligned}$$

La loi $*$ est donc associative. De plus, il est immédiat que 0 est un élément neutre car, pour tout $a \in \mathbb{Q}$, $a * 0 = 0 * a = a$.

2. Soit $(a, b, c) \in \mathbb{Q}^3$. D'une part :

$$\begin{aligned} a * (b + c) &= a + b + c + a(b + c) \\ &= a + b + c + ab + ac \end{aligned}$$

et, d'autre part :

$$(a * b) + (a * c) = a + b + ab + a + c + ac$$

En prenant $a = 1$ et $b = c = 0$, on voit que la loi $*$ n'est pas distributive par rapport à la somme. De plus :

$$a * (b \times c) = a + bc + abc$$

tandis que

$$(a * b) \times (a * c) = (a + b + ab) \times (a + c + ac)$$

En prenant $a = b = c = 1$, on voit que $*$ n'est pas distributive par rapport au produit.

3. Rappelons que 0 est le neutre de $*$ et que $*$ est commutative : dès lors, un élément est inversible si et seulement s'il est inversible à gauche ou à droite. Soit $x \in \mathbb{Q}$.

$$\begin{aligned} x \text{ est inversible} &\iff \exists y \in \mathbb{Q}, x * y = 0 \\ &\iff \exists y \in \mathbb{Q}, x + y + xy = 0 \\ &\iff \exists y \in \mathbb{Q}, y(1 + x) = -x \end{aligned}$$

Il y a deux cas de figure : si $x \neq -1$, alors x est inversible et $y = \frac{-x}{1+x}$ est l'inverse de x , tandis que si $x = -1$, alors $x * y = -1 + y - y = -1 \neq 0$ pour tout y , c'est-à-dire que -1 n'est pas inversible.

Cherchons à présent les éléments réguliers (idem, un élément est régulier si et seulement s'il est régulier à gauche ou à droite). On pourrait raisonner par équivalences, mais entre les équivalences et les implications, cela donnerait une rédaction délicate. Soit $x \in \mathbb{Q}$ et soit $(y, z) \in \mathbb{Q}^2$ tel que $y * x = z * x$. Alors $y + x + yx = z + x + zx$ donc $y(1 + x) = z(1 + x)$. Si $x \neq -1$, on peut simplifier par $1 + x$ si bien que $y = z$: tout élément différent de -1 est régulier. De plus, d'après la question précédente, pour tous y et z , $y * (-1) = z * (-1) = -1$ donc -1 n'est pas régulier. Enfin, $x * x = 2x + x^2$. Par conséquent, x est idempotent si et seulement si $2x + x^2 = x$ si et seulement si $x + x^2 = x(x + 1) = 0$. On en déduit que 0 et -1 sont les seuls éléments idempotents.

4. Soit $x \in \mathbb{Q}$.

$$7 * x = 3 \iff 7 + x + 7x = 3$$

$$\iff 8x = -4$$

$$\iff x = -1/2$$

puis :

$$x * (-5) = -1 \iff x - 5 - 5x = -1$$

$$\iff -4x = 4$$

$$\iff x = -1$$

puis :

$$x * x = 2 \iff x + x + x^2 = 2$$

$$\iff x^2 + 2x - 2 = 0$$

$$\iff x = \frac{-2 \pm \sqrt{12}}{2} = -1 \pm \sqrt{3}$$

Or, on est sur \mathbb{Q} et $\sqrt{3}$ est irrationnel : l'équation n'a pas de solution. Enfin,

$$x * x = 3 \iff x + x + x^2 = 3$$

$$\iff x^2 + 2x - 3 = 0$$

$$\iff x = 1 \quad \text{ou} \quad x = -3$$

5. On demande donc, si $n \geq 1$ (nous verrons les autres cas plus tard), de donner $\underbrace{a * \dots * a}_{n \text{ fois}}$ (cette notation a du sens car

la loi est associative). On a tout d'abord $a^1 = a$ puis $a^2 = a * a = 2a + a \times a$ (dans cette question, nous gardons la notation puissance pour la loi $*$, quand nous aurons un vrai produit, nous l'écrirons avec la loi \times pour qu'il n'y ait aucune confusion). Ensuite,

$$\begin{aligned} a^3 &= a^2 * a \\ &= a^2 + a + a^2 \times a \\ &= (a + a + a \times a) + a + (a + a + a \times a) \times a \\ &= 3a + 3a \times a + a \times a \times a \end{aligned}$$

On reconnaît un binôme de Newton tronqué, à savoir $(a + 1) \times \dots \times (a + 1)$ (n fois), mais il manque le 1. Prouvons donc que

$$a^n = \underbrace{(a + 1) \times \dots \times (a + 1)}_{n \text{ fois}} - 1$$

Prouvons ce résultat par récurrence sur $n \geq 1$. Le résultat est vérifié aux rangs 1, 2, 3. Soit $n \geq 3$. Supposons qu'il soit vrai au rang n et prouvons qu'il est toujours vrai au rang $n + 1$. $a^{n+1} = a^n * a = a^n + a + a^n \times a$. Par hypothèse de récurrence :

$$\begin{aligned}
a^{n+1} &= \left(\underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} - 1 \right) + a + \left(\underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} - 1 \right) \times a \\
&= \underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} - 1 + a + \underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} \times a - a \\
&= \underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} \times (1+a) - 1 \\
&= \underbrace{(a+1) \times \cdots \times (a+1)}_{n+1 \text{ fois}} - 1
\end{aligned}$$

ce qui clôt la récurrence. Pour $n = 0$, a^0 est, par convention, égal au neutre, c'est-à-dire à 0 ici. Enfin, si $n < 0$, par définition, $a^n = (a^{-1})^{-n}$ (toujours au sens de la loi $*$). En utilisant l'expression de l'inverse d'un élément (en particulier, $a^{-1} + 1 = 1/(1+a)$) et l'expression d'une puissance positive (car $-n > 0$), on trouve finalement :

$$a^n = \underbrace{\left(\frac{1}{1+a} \right) \times \cdots \times \left(\frac{1}{1+a} \right)}_{-n \text{ fois}}$$

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 $\frac{R_1 R_2}{R_1 + R_2}$. 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

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

Cette borne inférieure est-elle atteinte ? Si oui, en quel(s) (y, z) ?

5. ♣♣♣ Soient $n \geq 1$, (a_1, \dots, a_n) et (b_1, \dots, 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.

Correction :

1. Immédiat : si a et b sont strictement positifs, $a//b$ l'est aussi.
2. La commutativité est évidente. Soit $(a, b, c) \in (\mathbb{R}_+^*)^3$. D'une part,

$$\begin{aligned}
a/(b/c) &= a/\left(\frac{bc}{b+c}\right) \\
&= \frac{a \times \frac{bc}{b+c}}{a + \frac{bc}{b+c}} \\
&= \frac{abc}{b+c} \times \frac{b+c}{ab+ac+bc} \\
&= \frac{abc}{ab+ac+bc}
\end{aligned}$$

et d'autre part

$$\begin{aligned}
(a/b)/c &= \left(\frac{ab}{a+b}\right)/c \\
&= \frac{\frac{ab}{a+b} \times c}{\frac{ab}{a+b} + c} \\
&= \frac{abc}{a+b} \times \frac{a+b}{ab+ac+bc} \\
&= \frac{abc}{ab+ac+bc}
\end{aligned}$$

La loi est bien associative.

3. Supposons par l'absurde que $/$ admette un élément neutre x . Alors, pour tout $a > 0$, $a/x = a$ donc

$$\frac{ax}{a+x} = a$$

Ainsi, $ax = a(a+x)$ donc $a^2 = 0$ ce qui est absurde car $a > 0$. Finalement, il n'y a pas d'élément neutre.

4. Soit $(y, z) \in \mathbb{R}^2$ tel que $y + z = x$. L'astuce est de voir qu'il n'y a en fait qu'une variable parmi y et z , l'autre est donnée automatiquement. Plus précisément, $z = x - y$. Par conséquent, on demande de prouver que :

$$\inf_{y \in \mathbb{R}} (ay^2 + b(x-y)^2) = (a/b)x^2$$

et cela ne pose plus de difficulté : posons $\varphi(y) = ay^2 + b(x-y)^2$. Alors

$$\varphi(y) = (a+b)y^2 - 2bxy + bx^2$$

On pourrait donner le tableau de variations de φ mais on reconnaît un trinôme du second degré de coefficient dominant strictement positif : on sait qu'il y a un minimum atteint en « $-b/2a$ » (avec les notations $ax^2 + bx + c$, pas les a et b de l'énoncé) donc, ici, en

$$\frac{2bx}{2(a+b)} = \frac{bx}{a+b}$$

et celui-ci vaut :

$$\begin{aligned}
\varphi\left(\frac{bx}{a+b}\right) &= (a+b)\left(\frac{bx}{a+b}\right)^2 - 2bx \times \frac{bx}{a+b} + bx^2 \\
&= \frac{b^2x^2}{a+b} - \frac{2b^2x^2}{a+b} + bx^2 \\
&= \frac{-b^2x^2}{a+b} + \frac{bx^2(a+b)}{a+b} \\
&= \frac{abx^2}{a+b} \\
&= (a/b)x^2
\end{aligned}$$

Il est de plus atteint uniquement pour $y = bx/(a+b)$ et $z = x - y = ax/(a+b)$.

5. Prouvons le résultat par récurrence sur n . Il n'y a rien à prouver pour $n = 1$ puisque les deux termes de l'inégalité sont égaux à a_1/b_1 . Prouvons le résultat pour $n = 2$. Soient a_1, a_2, b_1, b_2 des réels strictement positifs. Notons

$$D = (a_1 + a_2)/(b_1 + b_2) - (a_1/b_1 + a_2/b_2)$$

Alors :

$$\begin{aligned} D &= \frac{(a_1 + a_2)(b_1 + b_2)}{a_1 + a_2 + b_1 + b_2} - \frac{a_1 b_1}{a_1 + b_1} - \frac{a_2 b_2}{a_2 + b_2} \\ &= \frac{(a_1 + a_2)(b_1 + b_2)(a_1 + b_1)(a_2 + b_2) - a_1 b_1(a_1 + a_2 + b_1 + b_2)(a_2 + b_2) - a_2 b_2(a_1 + a_2 + b_1 + b_2)(a_1 + b_1)}{(a_1 + a_2 + b_1 + b_2)(a_1 + b_1)(a_2 + b_2)} \end{aligned}$$

En faisant le calcul (c'est long...) on trouve que

$$\begin{aligned} D &= \frac{a_1^2 b_2^2 + a_2^2 b_1^2 - 2a_1 a_2 b_1 b_2}{(a_1 + a_2 + b_1 + b_2)(a_1 + b_1)(a_2 + b_2)} \\ &= \frac{(a_1 b_2 + a_2 b_1)^2}{(a_1 + a_2 + b_1 + b_2)(a_1 + b_1)(a_2 + b_2)} \\ &\geq 0 \end{aligned}$$

si bien que

$$(a_1 + a_2)/(b_1 + b_2) \geq a_1/b_1 + a_2/b_2$$

Le résultat est donc vrai pour $n = 2$. Soit $n \geq 1$, supposons le résultat vrai au rang n et prouvons qu'il est encore vrai au rang $n + 1$. Soient donc (a_1, \dots, a_{n+1}) et (b_1, \dots, b_{n+1}) des familles de réels strictement positifs. Tout d'abord, notons

$$S_n = \sum_{i=1}^n a_i \quad \text{et} \quad T_n = \sum_{i=1}^n b_i$$

On en déduit que

$$\left(\sum_{i=1}^{n+1} a_i \right) / \left(\sum_{i=1}^{n+1} b_i \right) = (S_n + a_{n+1}) / (T_n + b_{n+1})$$

D'après le cas $n = 2$, on en déduit que :

$$\left(\sum_{i=1}^{n+1} a_i \right) / \left(\sum_{i=1}^{n+1} b_i \right) \geq S_n / T_n + a_{n+1} / b_{n+1} = \left(\sum_{i=1}^n a_i \right) / \left(\sum_{i=1}^n b_i \right) + a_{n+1} / b_{n+1}$$

Il suffit d'appliquer l'hypothèse de récurrence pour conclure.

6. Pour la question 1 : la résistance équivalente est strictement positive. Pour la question 2 : la commutativité prouve que l'ordre des deux résistances ne change rien, et l'associativité prouve que si on met A et B en parallèle de C ou A en parallèle de B et C , cela ne change rien. La question 3 prouve qu'il n'est pas possible de mettre en parallèle d'une résistance R une autre résistance R' de manière à ce que la résistance totale soit encore R (i.e. soit inchangée) : quand on met une deuxième résistance en parallèle, cela change la résistance totale. Pour la question 4, on se souvient que $P = UI$ et $U = RI$ donc $P = RI^2$: si on a deux résistances R_1 et R_2 en parallèle et une intensité de I , d'après la loi des noeuds, il y a une intensité I_1 qui va chez R_1 et une intensité I_2 qui va chez R_2 , avec $I_1 + I_2 = I$, et la répartition qui minimise la puissance est obtenue avec $I_1 = R_2 I / (R_1 + R_2)$, et cette puissance minimale est la même que celle obtenue avec la résistance équivalente $R_1 // R_2$ (et l'intensité I). Enfin, pour la question 5, cela prouve que si on a des résistances R_1, \dots, R_n et ρ_1, \dots, ρ_n , on a une résistance plus faible en mettant chaque R_i avec chaque ρ_i en parallèle, puis à mettre ces couples en séries, qu'en mettant toutes les R_i en série, les ρ_i en série également, et enfin en mettant ces deux familles de n résistances en série en parallèle.

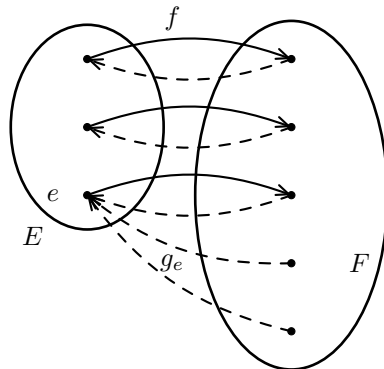
Exercice 9 : ★★ Soient E et F deux ensembles non vides. Soit $f : E \rightarrow F$.

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 ?

Correction :

1. Faisons un dessin :



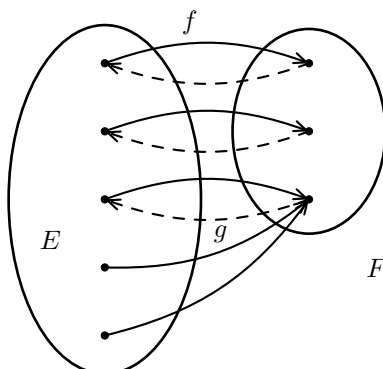
Si $e \in E$, notons g_e l'application définie comme suit :

$$g_e : \begin{cases} F & \rightarrow & E \\ y & \mapsto & \begin{cases} f^{-1}(y) & \text{si } y \in f(E) \\ e & \text{sinon} \end{cases} \end{cases}$$

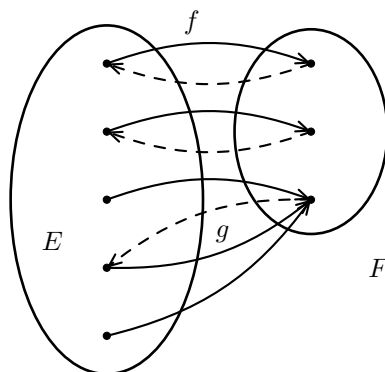
On prouve comme dans l'exercice 42 du chapitre 3 que $g_e \circ f = \text{Id}_E$: g_e est un inverse de f à gauche. Puisque E n'est pas un singleton, il admet plusieurs éléments e donc f admet plusieurs inverses à gauche. Cependant, f n'admet aucun inverse à droite car il n'existe aucune fonction $g : F \rightarrow E$ telle que $f \circ g = \text{Id}_F$: en effet, si on prend $y \in F$ non atteint par f , il n'existe aucun $x \in E$ tel que $f(x) = y$ donc il n'existe aucune fonction g telle que $f(g(y)) = y$: il n'existe aucune fonction g telle que $f \circ g = \text{Id}_F$, f n'est pas inversible à droite.

2. Soit

$$g : \begin{cases} F & \rightarrow & E \\ y & \mapsto & \text{un antécédent de } y \text{ par } f \end{cases}$$



On prouve de même que dans l'exercice 42 du chapitre 3 que $f \circ g = \text{Id}_F$ donc g est un inverse à droite de f . Il y a plusieurs inverses à droite car il suffit de changer la valeur de g en un y qui admet plusieurs antécédents, et donc en envoyant y sur un autre de ses antécédents, on obtient un autre inverse à droite.



Cependant, f n'admet aucun inverse à gauche : en effet, supposons qu'il existe $g : F \rightarrow E$ telle que $g \circ f = \text{Id}_E$. Soient $x_1 \neq x_2$ tels que $f(x_1) = f(x_2)$ (possible car f non injective) donc $g \circ f(x_1) = g \circ f(x_2)$ ce qui est absurde car $g(f(x_1)) = x_1$ et $g(f(x_2)) = x_2$.

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.

Correction :

1. Une loi de composition interne est une application de E^2 dans E donc un élément de $(E^2)^E$, ensemble à $(n^2)^n = n^{2n}$ éléments (cf. chapitre précédent, le cardinal de F^E est $\text{card}(F)^{\text{card}(E)}$).
2. Notons $E = \{x_1; \dots; x_n\}$. Une loi de composition interne commutative est entièrement déterminée par l'image des (x_i, x_j) pour $i \leq j$, les autres sont déduits par commutativité (par exemple, si on connaît l'image de (x_1, x_2) , on connaît automatiquement celle de (x_2, x_1)). Soit $(i, j) \in \llbracket 1; n \rrbracket^2$ avec $i \leq j$. Il y a n choix possibles pour l'image de (x_i, x_j) donc le cardinal recherché est (par principe multiplicatif)

$$\begin{aligned}
 S &= \prod_{i=1}^n \prod_{j=i}^n n \\
 &= \prod_{i=1}^n n^{n-i+1} \\
 &= \prod_{k=1}^n n^k \\
 &= n^{\sum_{k=1}^n k} \\
 &= n^{n(n+1)/2}
 \end{aligned}$$

On peut aussi voir le résultat de la façon suivante : on représente la loi par un tableau, avec, en position (i, j) , l'image de (x_i, x_j) . Alors il suffit de connaître les éléments au-dessus (au sens large) de la diagonale car la loi est commutative, on déduit les autres par symétrie : il faut connaître $n(n+1)/2$ images, n images possibles pour chaque, et on retrouve le même résultat.

3. Une telle loi est totalement déterminée, pour commencer, par le choix de l'élément neutre : n choix possibles. Notons x_e l'élément neutre. Alors les $x_i * x_e$ sont déjà connus puisqu'ils valent x_i . Par conséquent, comme dans la question précédente, une telle loi est totalement déterminée ensuite par les images des (x_i, x_j) avec $i \leq j$ et i et j distincts de e . Le raisonnement est le même qu'à la question précédente, si ce n'est qu'il faut déterminer n images de moins : $(x_1, x_e), (x_2, x_e), \dots, (x_e, x_e), (x_e, x_{e+1}), \dots, (x_e, x_n)$. Il y a donc $n^{n(n+1)/2-n} = n^{n(n-1)/2}$, qu'il ne faut pas oublier de multiplier par n (les n choix possibles pour l'élément neutre). Il y a donc $n^{n(n-1)/2+1}$ telles lois internes.

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 $x^2 = x$.

Correction : Soit $a \in E$. Les puissances de a sont en nombre infini alors que E est fini : d'après le principe des tiroirs, il existe une infinité de puissances égales. Soient par exemple n_1 et n_2 avec $n_2 \geq 2n_1$ (c'est possible car il existe une infinité de puissances égales, on prend donc une puissance n_1 quelconque parmi l'infinité de puissances égales, puis une autre supérieure à son double, ce qui est possible puisqu'il y en a une infinité, nous verrons pourquoi il est intéressant d'avoir $n_2 \geq 2n_1$ dans la suite) $a^{n_1} = a^{n_2}$. On cherche un entier k tel qu'en multipliant par a^k , une des deux puissances serait le double de l'autre, i.e. on cherche k tel que $n_2 + k = 2(n_1 + k)$. Alors $k = n_2 - 2n_1$ convient (d'où la nécessité d'avoir $n_2 \geq 2n_1$). Puisque $a^{n_2} = a^{n_1}$ alors $a^{n_2+k} = a^{n_1+k}$ (en multipliant par a^k) mais, par choix de k , on a $n_2 + k = 2(n_1 + k)$ si bien qu'en posant $x = a^{n_1+k}$, on a bien $x^2 = x$.

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 $(\mathbb{R}, +)$.

Correction :

1. Précisons que, n étant impair, si $x \in \mathbb{R}$, $\sqrt[n]{x^n} = x$ (ce n'est pas vrai si n est pair et x négatif). Le fait que la loi soit interne et commutative est immédiat. Prouvons qu'elle est associative. Soit $(x, y, z) \in \mathbb{R}^3$. D'une part :

$$\begin{aligned} x * (y * z) &= x * \sqrt[n]{y^n + z^n} \\ &= \sqrt[n]{x^n + (\sqrt[n]{y^n + z^n})^n} \\ &= \sqrt[n]{x^n + y^n + z^n} \end{aligned}$$

et d'autre part

$$\begin{aligned} (x * y) * z &= \sqrt[n]{x^n + y^n} * z \\ &= \sqrt[n]{(\sqrt[n]{x^n + y^n})^n + z^n} \\ &= \sqrt[n]{x^n + y^n + z^n} \end{aligned}$$

La loi est bien associative. Il est immédiat que 0 est élément neutre et que, pour tout x , $-x$ est le symétrique de x : $(\mathbb{R}, *)$ est bien un groupe abélien.

2. Soient x et y deux réels.

$$\begin{aligned} \varphi(x * y) &= (x * y)^n \\ &= (\sqrt[n]{x^n + y^n})^n \\ &= x^n + y^n \\ &= \varphi(x) + \varphi(y) \end{aligned}$$

c'est-à-dire que φ est un morphisme de groupes entre $(\mathbb{R}, *)$ et $(\mathbb{R}, +)$. La bijectivité découle directement du théorème de la bijection.

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} ?

Correction : Rappelons (cf. cours) que, pour tout n , \mathbb{U}_n est un sous-groupe de \mathbb{U} (pour la loi \times). Attention, une union de sous-groupes n'est pas forcément un sous-groupe ! Notons cet ensemble G . Rappelons qu'un élément est dans G si et seulement s'il existe un $n \in \mathbb{N}^*$ tel que cet élément soit dans \mathbb{U}_n . Rappelons également que \mathbb{U}_n est inclus dans \mathbb{U}_m si et seulement si $n|m$.

1. G est une union d'ensembles inclus dans \mathbb{U} donc est inclus dans \mathbb{U} .
2. $1 \in \mathbb{U}_1$ donc $1 \in G$: G est non vide.

3. Soient z_1 et z_2 deux éléments de G . Alors il existe n_1 et n_2 dans \mathbb{N}^* tels que $z_1 \in \mathbb{U}_{n_1}$ et $z_2 \in \mathbb{U}_{n_2}$. L'idée est de trouver un même \mathbb{U}_m tel que z_1 et z_2 appartiennent à \mathbb{U}_m . Soit $m = n_1 \vee n_2$. Alors n_1 et n_2 divisent m donc \mathbb{U}_{n_1} et \mathbb{U}_{n_2} sont inclus dans \mathbb{U}_m si bien que z_1 et z_2 appartiennent à \mathbb{U}_m . Or, \mathbb{U}_m est un groupe (pour la loi \times) donc $z_1 \times z_2 \in \mathbb{U}_m$ si bien que $z_1 \times z_2 \in G$: G est stable par produit.
4. Soit $z \in G$. Alors il existe $n \in \mathbb{N}^*$ tel que $z \in \mathbb{U}_n$ qui est un groupe donc $1/z \in \mathbb{U}_n$ et donc $1/z \in G$: G est stable par inverse.

En conclusion, G est un sous-groupe de \mathbb{U} (et donc est un groupe pour la loi \times). Cependant, il existe des éléments de \mathbb{U} qui ne sont pas des racines de l'unité, par exemple $e^{i\pi\sqrt{2}}$, cf. exercice 68 du chapitre 7, donc $G \neq \mathbb{U}$.

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 $x \oplus y = \frac{x+y}{1+xy}$.
3. \mathbb{R}^2 muni de la loi \star définie par $(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 e^{x_2} + y_2 e^{x_1})$.

Correction :

1. On sait que $S_{\mathbb{R}}$ (l'ensemble des bijections de \mathbb{R} dans \mathbb{R}) est un groupe pour la composition. Il suffit donc de prouver que cet ensemble (qu'on notera H) est un sous-groupe de $S_{\mathbb{R}}$.
 - Une fonction affine non constante étant une bijection de \mathbb{R} dans \mathbb{R} , G est inclus dans $S_{\mathbb{R}}$.
 - Soient $f_1 : x \mapsto a_1x + b$ et $f_2 : x \mapsto a_2x + b_2$ avec a_1 et a_2 non nuls appartenant à G . Alors (attention, il faut examiner la stabilité par la loi du groupe, la composition, pas par le produit !), pour tout $x \in \mathbb{R}$:

$$\begin{aligned} f_1 \circ f_2(x) &= f_1(a_2x + b_2) \\ &= a_1(a_2x + b_2) + b \\ &= a_1a_2x + a_1b_2 + b \end{aligned}$$

et puisque $a_1a_2 \neq 0$, $f_1 \circ f_2 \in G$: G est stable par composition.

- Soit $f : x \mapsto ax + b \in G$, avec donc $a \neq 0$. Soit $y \in \mathbb{R}$ et soit $x \in \mathbb{R}$ (méthode pour expliciter f^{-1} : résoudre l'équation, d'inconnue x , $f(x) = y$). Alors : $y = f(x) \iff x = \frac{y-b}{a}$. En d'autres termes, f^{-1} est la fonction $x \mapsto \frac{x}{a} - \frac{b}{a}$ (la variable est muette, l'appeler x ou y ne change rien) et puisque $1/a \neq 0$, on a bien $f^{-1} \in G$: G est stable par inverse (inverse au sens de la composition).

En conclusion, G est un sous-groupe de $S_{\mathbb{R}}$ donc est un groupe (pour la composition). Si on ne pense pas à $S_{\mathbb{R}}$, il faut prouver à la main que c'est un groupe donc préciser que la composition est associative, que $\text{Id} : x \mapsto x \in G$ est un élément neutre (à droite et à gauche car la composition n'est pas commutative) et que, comme ci-dessus, tout élément f de G admet un inverse.

2. Dans cet exemple et le suivant, la loi n'est pas une loi connue : il faut tout montrer, on ne peut pas montrer que les ensembles sont des sous-groupes de groupes connus.
 - Prouvons que la loi \oplus est interne, ce qui n'est pas immédiat à première vue. Soit $(x, y) \in] -1 ; 1 [^2$. Alors $|xy| < 1$ donc $1 + xy > 0$, d'où les équivalences suivantes :

$$\begin{aligned} -1 < x \oplus y < 1 &\iff -1 - xy < x + y < 1 + xy \\ &\iff -1 - xy < x + y \quad \text{et} \quad x + y < 1 + xy \\ &\iff -1 - y < x + xy \quad \text{et} \quad x - xy < 1 - y \\ &\iff -1(1 + y) < x(1 + y) \quad \text{et} \quad x(1 - y) < 1 - y \end{aligned}$$

Or, $1 + y$ et $1 - y$ sont strictement positifs car $y \in] -1 ; 1 [$ donc on peut simplifier par $1 \pm y$ si bien qu'on arrive à $-1 < x$ et $x < 1$ ce qui est vrai : puisqu'on a travaillé par équivalences, l'assertion de départ est vraie aussi, c'est-à-dire que $x \oplus y \in] -1 ; 1 [$: \oplus est bien une loi interne.

- Prouvons que la loi est associative. Soit $(x, y, z) \in] -1 ; 1 [$. D'une part,

$$\begin{aligned}
x \oplus (y \oplus z) &= x \oplus \frac{y+z}{1+yz} \\
&= \frac{x + \frac{y+z}{1+yz}}{1 + x \times \frac{y+z}{1+yz}} \\
&= \frac{x(1+yz) + y+z}{1+yz} \times \frac{1+yz}{(1+yz) + x(y+z)} \\
&= \frac{x+y+z+xyz}{1+yz+xy+xz}
\end{aligned}$$

et d'autre part

$$\begin{aligned}
(x \oplus y) \oplus z &= \frac{x+y}{1+xy} \oplus z \\
&= \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} \times z} \\
&= \frac{x+y+z(1+xy)}{1+xy} \times \frac{1+xy}{(1+xy) + z(x+y)} \\
&= \frac{x+y+z+xyz}{1+yz+xy+xz}
\end{aligned}$$

si bien que la loi est associative.

- Il est évident que 0 est un élément neutre et que, pour tout x , $-x$ est le symétrique de x .

En conclusion, $(]-1; 1[, \oplus)$ est un groupe.

3. Il est immédiat que la loi est interne.

- Prouvons qu'elle est associative. Soient $(x_1, y_1), (x_2, y_2)$ et (x_3, y_3) trois éléments de \mathbb{R}^2 . D'une part :

$$\begin{aligned}
(x_1, y_1) \star ((x_2, y_2) \star (x_3, y_3)) &= (x_1, y_1) \star (x_2 + x_3, y_2 e^{x_3} + y_3 e^{x_2}) \\
&= (x_1 + x_2 + x_3, y_1 e^{x_2+x_3} + (y_2 e^{x_3} + y_3 e^{x_2}) e^{x_1}) \\
&= (x_1 + x_2 + x_3, y_1 e^{x_2+x_3} + y_2 e^{x_1+x_3} + y_3 e^{x_1+x_2})
\end{aligned}$$

et d'autre part

$$\begin{aligned}
((x_1, y_1) \star (x_2, y_2)) \star (x_3, y_3) &= (x_1 + x_2, y_1 e^{x_2} + y_2 e^{x_1}) \star (x_3, y_3) \\
&= (x_1 + x_2 + x_3, (y_1 e^{x_2} + y_2 e^{x_1}) e^{x_3} + y_3 e^{x_1+x_2}) \\
&= (x_1 + x_2 + x_3, y_1 e^{x_2+x_3} + y_2 e^{x_1+x_3} + y_3 e^{x_1+x_2})
\end{aligned}$$

et donc la loi est bien associative.

- Il est immédiat que, pour tout $(x, y) \in \mathbb{R}^2$, $(x, y) \star (0, 0) = (x, y)$ (la loi étant commutative, il suffit de prouver qu'un élément est neutre à droite ou à gauche pour prouver que c'est un neutre) est un élément neutre. Cherchons le symétrique de (x, y) . Soit $(a, b) \in \mathbb{R}^2$.

$$\begin{aligned}
(x, y) \star (a, b) = (0, 0) &\iff (x + a, y e^a + b e^x) = (0, 0) \\
&\iff x + a = 0 \quad \text{et} \quad y e^a + b e^x = 0 \\
&= a = -x \quad \text{et} \quad y e^{-x} + b e^x = 0 \\
&= a = -x \quad \text{et} \quad b = -y e^{-2x}
\end{aligned}$$

Il en découle que $(-x, -y e^{-2x})$ est un inverse à droite de (x, y) donc, par commutativité de \star , un inverse de (x, y) . Finalement, (\mathbb{R}^2, \star) est bien un groupe.

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

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

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

Correction : Il est sous-entendu que la loi est le produit puisque (\mathbb{R}_+^*, \times) est un groupe.

- Prouvons tout d'abord, ce qui n'est pas si évident que ça car y peut être négatif, que G est inclus dans \mathbb{R}_+^* . Soit donc $x + y\sqrt{3}$ (avec x et y vérifiant les bonnes conditions) un élément de G . Alors $x^2 = 1 + 3y^2 > 3y^2$ et la racine carrée est strictement croissante donc

$$\sqrt{x^2} = x > \sqrt{3y^2} = |y|\sqrt{3} \geq -y\sqrt{3}$$

$\sqrt{x^2} = x$ puisque x est positif, et $|y| \geq \pm y$. Finalement, $x + y\sqrt{3} \in \mathbb{R}_+^*$, d'où l'inclusion voulue.

- $1 = 1 + 0\sqrt{3}$ avec $1 \in \mathbb{N}, 0 \in \mathbb{Z}$ et $1^2 - 3 \times 0^2 = 1$ donc $1 \in G$: G est non vide.
- Prouvons que G est stable par produit. Soient $x_1 + y_1\sqrt{3}$ et $x_2 + y_2\sqrt{3}$ deux éléments de G . Alors

$$(x_1 + y_1\sqrt{3})(x_2 + y_2\sqrt{3}) = X + Y\sqrt{3}$$

avec $X = x_1x_2 + 3y_1y_2$ et $Y = x_1y_2 + x_2y_1$. Il est immédiat que $Y \in \mathbb{Z}$. De plus, $X \in \mathbb{Z}$: prouvons que $X \geq 0$. De même que ci-dessus, $x_1 > |y_1|\sqrt{3}$ et $x_2 > |y_2|\sqrt{3}$ donc, par produit (les inégalités sont positives, d'où la nécessité de la valeur absolue), $x_1x_2 > 3|y_1y_2| \geq -3y_1y_2$ (toujours car $|y_1y_2| \geq \pm y_1y_2$) si bien que $X = x_1x_2 + 3y_1y_2 \geq 0$: on a bien $X \in \mathbb{N}$. Enfin :

$$\begin{aligned} X^2 - 3Y^2 &= (x_1x_2 + 3y_1y_2)^2 - 3(x_1y_2 + x_2y_1)^2 \\ &= x_1^2x_2^2 + 6x_1x_2y_2y_1 + 9y_1^2y_2^2 - 3(x_1^2y_2^2 + 2x_1y_2x_2y_1 + x_2^2y_1^2) \\ &= x_1^2x_2^2 + 9y_1^2y_2^2 - 3x_1^2y_2^2 - 3x_2^2y_1^2 \\ &= x_1^2(x_2^2 - 3y_2^2) - 3y_1^2(x_2^2 - 3y_2^2) \\ &= x_1^2 \times 1 - 3y_1^2 \times 1 \\ &= 1 \end{aligned}$$

Finalement, on a bien $(x_1 + y_1\sqrt{3})(x_2 + y_2\sqrt{3}) = X + Y\sqrt{3} \in G$: G est stable par produit.

- Prouvons que G est stable par inverse. Soit $x + y\sqrt{3} \in G$. Tout d'abord, $x + y\sqrt{3} > 0$ comme on l'a déjà vu donc étudier son inverse a du sens. Avec la méthode de l'expression conjuguée :

$$\begin{aligned} \frac{1}{x + y\sqrt{3}} &= \frac{x - y\sqrt{3}}{(x + y\sqrt{3})(x - y\sqrt{3})} \\ &= \frac{x - y\sqrt{3}}{x^2 - 3y^2} \\ &= x - y\sqrt{3} \end{aligned}$$

Or, $x \in \mathbb{N}$, $(-y) \in \mathbb{Z}$ et $x^2 - 3(-y)^2 = x^2 - 3y^2 = 1$ si bien que

$$\frac{1}{x + y\sqrt{3}} = x - y\sqrt{3} \in G$$

En d'autres termes, G est stable par inverse.

En conclusion, G est un sous-groupe de \mathbb{R}_+^* (et, en particulier, G est un groupe pour la loi \times).

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 $(ba)^n = e$.

Correction : Évidemment, le groupe n'est pas supposé abélien sinon $ab = ba$ et alors le résultat est évident. Par définition,

$$\underbrace{(ab) \times \cdots \times (ab)}_{n \text{ fois}} = e$$

En particulier, la loi étant associative :

$$a \times \underbrace{(ba) \times \cdots \times (ba)}_{n-1 \text{ fois}} \times b = e$$

En multipliant par b à gauche :

$$ba \times \underbrace{(ba) \times \cdots \times (ba)}_{n-1 \text{ fois}} \times b = b$$

Dans un groupe, tout élément est régulier donc on peut « simplifier » par b (ou, de façon explicite, on multiplie par b^{-1} à droite) ce qui donne :

$$\underbrace{(ba) \times \cdots \times (ba)}_{n \text{ fois}} = e$$

ce qui est le résultat voulu.

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 $ab^3 = b^3a^2$.

Correction :

1. On utilisera sans arrêt l'associativité de la loi : nous pourrons donc sans arrêt mettre des parenthèses où ça nous arrange, et les supprimer si cela nous arrange aussi. D'une part :

$$\begin{aligned} ab^3 &= (ab)b^2 \\ &= b^2ab^2 \\ &= b^2(ab)b \\ &= b^2(b^2a)b \\ &= b^2b^2(ab) \\ &= b^2b^2b^2a \\ &= b^5ba \\ &= eba \\ &= ba \end{aligned}$$

D'autre part, en utilisant à présent le fait que $ab^3 = ba$:

$$\begin{aligned} a^2b^2 &= a(ab)b \\ &= a(b^2a)b \\ &= ab^2(ab) \\ &= ab^2(b^2a) \\ &= (ab^3)ba \\ &= (ba)ba \\ &= b(ab)a \\ &= b(b^2a)a \\ &= b^3a^2 \end{aligned}$$

2. De même :

$$\begin{aligned}
 a^2b &= a(ab) \\
 &= a(ba^3) \\
 &= (ab)a^3 \\
 &= (ba^3)a^3 \\
 &= ba^6 \\
 &= baa^5 \\
 &= bae \\
 &= ba
 \end{aligned}$$

et, en utilisant le fait que $a^2b = ba$:

$$\begin{aligned}
 ab^3 &= (ab)b^2 \\
 &= (ba^3)b^2 \\
 &= ba^2(ab)b \\
 &= ba^2(ba^3)b \\
 &= b(a^2b)a(a^2b) \\
 &= b(ba)a(ba) \\
 &= b^2(a^2b)a \\
 &= b^2(ba)a \\
 &= b^3a^2
 \end{aligned}$$

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

Correction : Soit $(x, y) \in G^2$. Par hypothèse, $(xy) \times (xy) = x^2y^2$ c'est-à-dire (la loi étant associative donc on peut se passer de parenthèses) $xyxy = xx yy$. Dans un groupe, tout élément est régulier (ou alors, explicitement, en multipliant par x^{-1} à gauche et y^{-1} à droite) donc $yx = xy$: le groupe est abélien.

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

Correction : Soit $(x, y) \in G^2$. Par hypothèse, $(xy)^2 = xyxy = e$. Tout élément est par hypothèse son propre inverse donc, en multipliant par x à gauche et y à droite, il vient : $x^2yxy^2 = xy$ donc $yx = xy$: G est abélien.

18.2.3 Transport de structure

Exercice 20 : $\star\star$ 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.

Correction : Notons $\varphi : G_1 \rightarrow G_2$ un isomorphisme et $\psi : H_1 \rightarrow H_2$ un isomorphisme. Toutes les lois seront notées $*$ par souci de simplicité (nous n'allons pas noter $*_{G_1}$ la loi de G_1 etc.), mais il faut bien garder à l'esprit que les lois n'ont aucune raison d'être les mêmes (il y a quatre lois distinctes : celle de G_1 , celle de G_2 , celle de H_1 , celle de H_2 , c'est un bon exercice de se demander à chaque fois à quel ensemble appartient quel objet). Soit $f : G_1 \times H_1 \rightarrow G_2 \times H_2$ définie par :

$$\forall (a_1, b_1) \in G_1 \times H_1, f(a_1, b_1) = (\varphi(a_1), \psi(b_1))$$

Tout d'abord, φ étant à valeurs dans G_2 et ψ dans H_2 , f va bien de $G_1 \times H_1$ dans $G_2 \times H_2$.

- Montrons que f est un morphisme de groupes (pour la loi produit, cf. cours). Soient (a_1, b_1) et (c_1, d_1) deux éléments de $G_1 \times H_1$. Par définition de la loi produit, $(a_1, b_1) \times (c_1, d_1) = (a_1 * c_1, b_1 * d_1)$ (une dernière fois, précisons que, dans la première coordonnée, $*$ désigne la loi de G_1 et, dans la deuxième coordonnée, $*$ désigne la loi de H_1 , lois qui ne sont pas forcément les mêmes, et ce sera pareil pour les lois de G_2 et H_2 dans la suite). Dès lors :

$$\begin{aligned}
f((a_1, b_1) \times (c_1, d_1)) &= f(a_1 * c_1, b_1 * d_1) \\
&= (\varphi(a_1 * c_1), \psi(b_1 * d_1)) \\
&= (\varphi(a_1) * \varphi(c_1), \psi(b_1) * \psi(d_1)) \quad \text{car } \varphi \text{ et } \psi \text{ sont des morphismes de groupes} \\
&= (\varphi(a_1), \psi(b_1)) \times (\varphi(c_1), \psi(d_1)) \\
&= f(a_1, b_1) \times f(c_1, d_1)
\end{aligned}$$

si bien que f est un morphisme de groupes.

- Soit $(a_1, b_1) \in \ker(f)$. Alors $f(a_1, b_1) = (e_2, \varepsilon_2)$ (où e_2 est le neutre de G_2 et ε_2 le neutre de H_2) mais, par définition, $f(a_1, b_1) = (\varphi(a_1), \psi(b_1))$ donc $\varphi(a_1) = e_2$ et idem pour l'autre, si bien que $a_1 \in \ker(\varphi) = \{e_1\}$ par injectivité de φ donc $a_1 = e_1$. De même, $b_1 = \varepsilon_1$ (le neutre de H) donc $\ker(f) = \{(e_1, \varepsilon_1)\}$, f est injective.
- Enfin, soit $(a_2, b_2) \in G_2 \times H_2$. φ étant surjective, il existe $a_1 \in G_1$ tel que $a_2 = \varphi(a_1)$ et idem il existe $b_1 \in H_1$ tel que $\psi(b_1) = b_2$ et donc $f(a_1, b_1) = (a_2, b_2)$: f est surjective donc bijective donc c'est un isomorphisme.

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

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

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

Correction : On utilisera souvent le fait que, pour tout $y \in E$, $f(f^{-1}(y)) = y$ et que pour tout $g \in G$, $f^{-1}(f(g)) = g$.

- Montrons que la loi $*$ est associative. Soient y_1, y_2, y_3 trois éléments de E .

$$\begin{aligned}
y_1 * (y_2 * y_3) &= y_1 * f(f^{-1}(y_2) \times f^{-1}(y_3)) \\
&= f(f^{-1}(y_1) \times f^{-1}(f(f^{-1}(y_2) \times f^{-1}(y_3)))) \\
&= f(f^{-1}(y_1) \times (f^{-1}(y_2) \times f^{-1}(y_3)))
\end{aligned}$$

et

$$\begin{aligned}
(y_1 * y_2) * y_3 &= f(f^{-1}(y_1) \times f^{-1}(y_2)) * y_3 \\
&= f(f^{-1}(f(f^{-1}(y_1) \times f^{-1}(y_2))) \times f^{-1}(y_3)) \\
&= f((f^{-1}(y_1) \times f^{-1}(y_2)) \times f^{-1}(y_3))
\end{aligned}$$

et ces deux quantités sont bien égales par associativité de la loi \times puisque (G, \times) est un groupe.

- Notons $\varepsilon = f(e)$ où e désigne évidemment le neutre de G . Montrons que e est un élément neutre dans E (attention, il faut regarder les deux sens car la loi n'est pas forcément commutative). Soit $y \in E$. D'une part, e étant le neutre de G ,

$$\begin{aligned}
y * \varepsilon &= f(f^{-1}(y) \times f^{-1}(\varepsilon)) \\
&= f(f^{-1}(y) \times e) \\
&= f(f^{-1}(y)) \\
&= y
\end{aligned}$$

et, d'autre part, on montre de même que $\varepsilon * y = y$: ε est bien le neutre de G .

- Soit $y \in E$. Alors il existe $g \in G$ tel que $y = f(g)$. G étant un groupe, g admet un inverse qu'on note h (il y a assez de -1 comme ça dans cet exercice) et notons $x = f(h)$: montrons que x est l'inverse de y pour la loi $*$.

$$\begin{aligned}
x * y &= f(f^{-1}(x) \times f^{-1}(y)) \\
&= f(h \times g) \\
&= f(e) \\
&= \varepsilon
\end{aligned}$$

et idem pour $y * x$: x est l'inverse de y . Finalement, E est bien un groupe.

- Enfin, f est une bijection de G dans E . Pour montrer que c'est un isomorphisme, il suffit de prouver que c'est un morphisme de groupes entre G et E . Soient g et h deux éléments de G et notons $y = f(g)$ et $x = f(h)$, bien que :

$$\begin{aligned}
f(g \times h) &= f(f^{-1}(y) \times f^{-1}(x)) \\
&= y * x
\end{aligned}$$

par définition de la loi $*$: f est un morphisme, f est bijective donc f est un isomorphisme : G et E sont deux groupes isomorphes.

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 $f : E \rightarrow F$ 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) .

Correction : Il suffit de prouver que (F, \perp) est un groupe : il sera automatiquement isomorphe à (E, \top) puisque f est une bijection de E dans F et que, par définition, elle est compatible entre la loi \top et la loi \perp . Idem que dans l'exercice précédent, f étant bijective, elle admet une bijection réciproque f^{-1} , et $f \circ f^{-1} = \text{Id}_F$ et $f^{-1} \circ f = \text{Id}_E$.

- Montrons que \perp est associative. Soient a, b, c trois éléments de F . Notons $x = f^{-1}(a)$, $y = f^{-1}(b)$ et $z = f^{-1}(c)$ leurs antécédents par f (donc des éléments de E). En utilisant la propriété de la fonction f et le fait que \top est associative puisque (E, \top) est un groupe :

$$\begin{aligned}
a \perp (b \perp c) &= f(x) \perp (f(y) \perp f(z)) \\
&= f(x) \perp f(y \top z) \\
&= f(x \top (y \top z)) \\
&= f((x \top y) \top z) \\
&= f(x \top y) \perp f(z) \\
&= (f(x) \perp f(y)) \perp f(z) \\
&= (a \perp b) \perp c
\end{aligned}$$

c'est-à-dire que la loi \perp est associative.

- Notons $\varepsilon = f(e)$ où e est l'élément neutre de (E, \top) . Soit $y \in F$ et notons $x \in E = f^{-1}(y)$. D'une part,

$$\begin{aligned}
y \perp \varepsilon &= f(x) \perp f(e) \\
&= f(x \top e) \\
&= f(x) \\
&= y
\end{aligned}$$

et on prouve de même que $\varepsilon \perp y = y$: ε est bien le neutre de F .

- Soit $a \in F$. Notons $x = f^{-1}(a)$ son unique antécédent par f . Soit $y \in E$ l'inverse de x , et soit enfin $b = f(y)$. Alors :

$$\begin{aligned}
a \perp b &= f(a) \perp f(b) \\
&= f(a \top b) \\
&= f(e) \\
&= \varepsilon
\end{aligned}$$

et on prouve de même que $b \perp a = \varepsilon$: a admet un inverse, F est bien un groupe et on a déjà dit pourquoi, dans ce cas, il est isomorphe à E .

Exercice 23 : ★★ Soient (G, \cdot) 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, \cdot) .

Correction : Intuitivement, on « fait une rotation de a » : les résultats de cet exercice sont intuitifs une fois que l'on a cette image en tête. Quand on parlera de la loi du groupe, on parlera de la loi \cdot que l'on note multiplicativement : parfois (tout le temps), on écrira ab au lieu de $a \cdot b$.

- Montrons que $*$ est associative. Soit $(x, y, z) \in G^3$. On va utiliser que la loi du groupe (notée multiplicativement) est associative.

$$\begin{aligned}
x * (y * z) &= x * (yaz) \\
&= xa(yaz) \\
&= (xay)az \\
&= (x * y)az \\
&= (x * y) * z
\end{aligned}$$

La loi est bien associative.

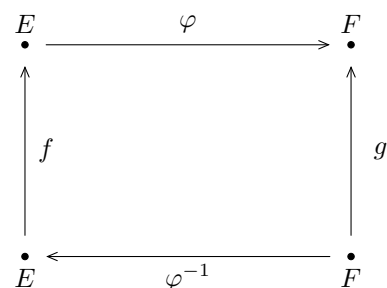
- Notons a^{-1} l'inverse de a pour la loi du groupe et e le neutre de G (qui existent car G est un groupe). On montre aisément que, pour tout $x \in G$, $x * a^{-1} = a^{-1} * x = x$ donc a^{-1} est bien le neutre pour $*$.
- Pour tout $x \in G$, on cherche donc y tel que $xay = a^{-1}$. En multipliant par x^{-1} (l'inverse de x au sens de la loi du groupe, qui existe puisqu'on est sur un groupe justement) à gauche puis a^{-1} , on trouve que $y = a^{-1}x^{-1}a^{-1}$, et il est immédiat (en utilisant l'associativité de la loi du groupe) qu'on a bien $x * y = y * x = a^{-1}$, le neutre, donc $a^{-1}x^{-1}a^{-1}$ est le symétrique de x pour la loi $*$.
- En conclusion, $(G, *)$ est bien un groupe. Exhibons un isomorphisme de (G, \cdot) dans $(G, *)$. Montrons que $\varphi : x \mapsto a^{-1}x$ est un tel isomorphisme (la « rotation » dans le sens inverse). Soit $(x, y) \in G^2$. Alors (on utilise l'associativité de la loi du groupe) :

$$\begin{aligned}
\varphi(xy) &= a^{-1}xy \\
&= a^{-1}xaa^{-1}y \\
&= \varphi(x)a\varphi(y) \\
&= \varphi(x) * \varphi(y)
\end{aligned}$$

c'est-à-dire que φ est un morphisme de groupes. Il est évidemment bijectif : si $\varphi(x_1) = \varphi(x_2)$ alors $a^{-1}x_1 = a^{-1}x_2$ donc, en multipliant par a à gauche (ou car tout élément de G est régulier), $x_1 = x_2$ donc φ est injective, et pour tout $y \in G$, ay est un antécédent de y donc φ est surjective, c'est un isomorphisme.

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 $Z(S_E) = \{\text{Id}_E\}$, c'est-à-dire que Id_E est le seul élément qui commute avec tout le monde.



Correction : Rappelons que S_E est l'ensemble des bijections de E (on dit aussi l'ensemble des permutations, même si on garde plutôt le terme de permutation pour les ensembles finis) et que c'est un groupe pour la composition (cf. cours).

1. Notons donc φ une bijection de E dans F . Montrons que

$$c : \begin{cases} S_E & \rightarrow S_F \\ f & \rightarrow \varphi \circ f \circ \varphi^{-1} \end{cases}$$

est un isomorphisme entre S_E et S_F munis de la composition (φ^{-1} est bien définie puisque φ est bijective).

- Montrons tout d'abord que c est bien définie i.e. va bien de S_E dans S_F . Soit $f \in S_E$. Alors $\varphi^{-1} : F \rightarrow E$, $f : E \rightarrow E$ et $\varphi : E \rightarrow F$ donc $c(f)$ va bien de F dans F et est bijective car composée de bijections donc $c(f)$ est bien un élément de S_F .
- Montrons tout d'abord que c est un morphisme de groupes. Soient f_1 et f_2 deux éléments de S_E (i.e. deux bijections de E dans E). Alors (en utilisant l'associativité de la composition) :

$$\begin{aligned} c(f_1) \circ c(f_2) &= (\varphi \circ f_1 \circ \varphi^{-1}) \circ (\varphi \circ f_2 \circ \varphi^{-1}) \\ &= \varphi \circ f_1 \circ (\varphi^{-1} \circ \varphi) \circ f_2 \circ \varphi^{-1} \\ &= \varphi \circ f_1 \circ (\text{Id}_E) \circ f_2 \circ \varphi^{-1} \\ &= \varphi \circ (f_1 \circ f_2) \circ \varphi^{-1} \\ &= c(f_1 \circ f_2) \end{aligned}$$

si bien que c est bien un morphisme de groupes.

- Montrer que c est une bijection. Attention de ne pas confondre c qui va de S_E dans S_F avec $c(f) = \varphi \circ f \circ \varphi^{-1}$ et de ne pas dire que c est bijective car est une composée de bijections, cela n'aurait aucun sens ! Soient $f \in S_E$ et $g \in S_F$. Alors, en composant à gauche par φ^{-1} et à droite par φ , on obtient : $c(f) = g \iff f = \varphi^{-1} \circ g \circ \varphi$. En d'autres termes, g admet un unique antécédent par c , c est bijective, c'est un isomorphisme de groupes, et en particulier les deux groupes sont isomorphes.
2. Soit $f \in S_E \setminus \{\text{Id}_E\}$ et montrons que f n'appartient pas au centre de S_E donc que f ne commute pas avec tout le monde. Il suffit donc d'exhiber une bijection de E qui ne commute pas avec f . f n'étant pas l'identité, il existe $a \in E$ tel que $f(a) \neq a$. Notons $b = f(a)$: on a donc $a \neq b$ et $f(a) = b$. Il y a deux cas de figure : soit $f(b) = a$ (i.e. f « échange a et b ») soit $f(b) \neq a$. Supposons que $f(b) = a$. Puisque E a au moins trois éléments, soit $c \neq a, b$ et soit $g : E \rightarrow E$ la fonction qui échange a et c i.e. définie par :

$$\forall x \in E, g(x) = \begin{cases} x & \text{si } x \neq a, c \\ c & \text{si } x = a \\ a & \text{si } x = c \end{cases}$$

Il est immédiat que g est bijective. Or, $f(g(b)) = f(b) = a$ et $g(f(b)) = g(a) = c$ donc f et g ne commutent pas. Supposons à présent que $f(b) \neq a$. Puisque $f(a) = b$ et f injective, on a également $f(b) \neq b$: notons $c = f(b)$ et donc $c \neq a, b$. Avec la même fonction g , il vient : $f(g(b)) = f(b) = c$ et $g(f(b)) = g(c) = a$ et on conclut de la même façon.

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.

Correction : Soit $(z_1, z_2) \in (\mathbb{C}^*)^2$. Notons f cette fonction. Alors

$$\begin{aligned} f(z_1 \times z_2) &= (z_1 \times z_2)^n \\ &= z_1^n \times z_2^n \\ &= f(z_1) \times f(z_2) \end{aligned}$$

c'est-à-dire que f est un morphisme de groupe de (\mathbb{C}^*, \times) dans lui-même donc un endomorphisme de groupes. Puisque le neutre est 1, son noyau est $\ker(f) = \{z \in \mathbb{C}^* \mid f(z) = 1\}$ donc l'ensemble des n tels que $z^n = 1$, c'est-à-dire que $\ker(f) = \mathbb{U}_n$, l'ensemble des racines n -ièmes de l'unité. Son image est \mathbb{C}^* tout entier : en effet, si $z \in \mathbb{C}^*$, alors (cf. chapitre 7), z a des racines n -ièmes (et même n distinctes pour être précis) donc au moins une : f est surjective.

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.

Correction :

1. Analyse : soit f un morphisme de groupes de \mathbb{Z} dans lui-même. Alors, pour tout $n \in \mathbb{N}^*$ (le 1 apparaît n fois)

$$\begin{aligned} f(n) &= f(1 + \cdots 1) \\ &= f(1) + \cdots + f(1) \\ &= nf(1) \end{aligned}$$

Si on note $a = f(1)$, alors $f(n) = an$ pour tout $n \in \mathbb{N}$. On sait de plus que $f(0) = 0$ (un morphisme envoie le neutre sur le neutre) et, si $n < 0$, alors $-n \in \mathbb{N}^*$ donc $f(-n) = -na$ et $f(n - n) = f(0) = 0$ mais f est un morphisme donc

$$\begin{aligned} f(n - n) &= f(n) + f(-n) \\ &= -f(-n) \\ &= na \end{aligned}$$

En conclusion, $f(n) = na$ avec $a = f(1)$. Réciproquement, soit $a \in \mathbb{Z}$ et prouvons que $f : n \mapsto na$ est un morphisme de groupe de \mathbb{Z} dans lui-même. Soient n_1 et n_2 dans \mathbb{Z} , alors

$$\begin{aligned} f(n_1 + n_2) &= a(n_1 + n_2) \\ &= an_1 + an_2 \\ &= f(n_1) + f(n_2) \end{aligned}$$

c'est-à-dire que f est un morphisme de groupes. En conclusion, les morphismes de groupes de \mathbb{Z} dans lui-même sont les $n \mapsto an$, pour tout $a \in \mathbb{Z}$. Un tel morphisme est bijectif si et seulement si $a = \pm 1$ donc les seuls automorphismes de \mathbb{Z} sont $n \mapsto \pm n$ donc $\pm \text{Id}_{\mathbb{Z}}$: le groupe des automorphismes de \mathbb{Z} est $\{\pm \text{Id}_{\mathbb{Z}}\}$ (groupe à deux éléments donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$).

2. Notons $a = f(1)$. De même, $f(n) = an$ pour tout $n \in \mathbb{Z}$. Soit $n \in \mathbb{N}^*$. Puisque $1 = \frac{1}{n} + \cdots + \frac{1}{n}$ (n fois) donc

$$f(1) = f\left(\frac{1}{n}\right) + \cdots + f\left(\frac{1}{n}\right)$$

si bien que $f\left(\frac{1}{n}\right) = \frac{a}{n} = \frac{f(1)}{n}$. Soit à présent $r = p/q$ un rationnel avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. On montre de même que $f(p/q) = pf(1/q)$ et d'après ce qui précède, $f(1/q) = f(1)/q$ donc $f(p/q) = pf(1)/q$ donc $f(r) = rf(1)$. On montre réciproquement que toute fonction du type $r \mapsto ar$ convient. En conclusion, les morphismes de \mathbb{Q} dans \mathbb{Q} sont exactement les fonctions de la forme $r \mapsto ar$ avec $a \in \mathbb{Q}$.

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

Correction : De même que dans l'exercice précédent, on montre que $\varphi(r) = r\varphi(1)$ pour tout $r \in \mathbb{Q}$ (ou alors, tout simplement, on utilise l'exercice précédent en disant qu'un morphisme de \mathbb{Q} dans \mathbb{Z} est un morphisme de \mathbb{Q} dans lui-même donc est de cette forme). En particulier, pour tout $n \in \mathbb{N}^*$, $\varphi(1/n) = \varphi(1)/n \xrightarrow{n \rightarrow +\infty} 0$ donc appartient à $] -1; 1[$ pour n assez grand. Or, c'est un entier : on en déduit que $\varphi(1) = 0$, si bien que φ est la fonction nulle, et la synthèse est immédiate : la fonction nulle est donc l'unique morphisme de groupes 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) .

Correction :

1. L'exponentielle est un isomorphisme entre ces deux groupes (cf. cours). Les groupes suivants ne sont pas isomorphes : l'idée est toujours la même (cf. cours), trouver une équation dans un groupe, son analogue dans l'autre groupe, et montrer qu'elles n'ont pas le même nombre de solutions ce qui est absurde si les groupes sont isomorphes.
2. Intéressons-nous à l'équation $y^2 = 2$, qui n'a pas de solution dans \mathbb{Q}_+^* , alors que son analogue dans \mathbb{Q} , $x + x = \dots$ en a. Supposons qu'il existe un isomorphisme φ entre les deux groupes. Soit $x \in \mathbb{Q}$. On a :

$$\begin{aligned}
 \varphi(x)^2 = 2 &\iff \varphi(x) \times \varphi(x) = 2 \\
 &\iff \varphi(x + x) = 2 && \varphi \text{ est un morphisme} \\
 &\iff \varphi(2x) = 2 \\
 &\iff 2x = \varphi^{-1}(2) \\
 &\iff x = \varphi^{-1}(2)/2
 \end{aligned}$$

Dès lors, si on pose $x = \varphi^{-1}(2)/2$, alors $\varphi(x) \in \mathbb{Q}_+^*$ et $\varphi(x)^2 = 2$ donc $\varphi(x) = \sqrt{2}$ (car $\varphi(x) > 0$) ce qui est absurde car $\sqrt{2} \notin \mathbb{Q}$: les deux groupes ne sont pas isomorphes.

3. On a déjà prouvé dans l'exercice précédent qu'ils ne sont pas isomorphes, car le seul morphisme entre de \mathbb{Q} dans \mathbb{Z} est le morphisme nul qui n'est pas bijectif, mais remontrons qu'ils ne sont pas isomorphes. S'ils sont isomorphes, soit $\varphi : \mathbb{Q} \rightarrow \mathbb{Z}$ un isomorphisme. On pense cette fois-ci à l'équation $2x = 1$ qui n'a pas de solutions dans \mathbb{Z} mais son analogue $2x = \dots$ en a dans \mathbb{Q} . Soit $x \in \mathbb{Q}$.

$$\begin{aligned}
 2\varphi(x) = 1 &\iff \varphi(x) + \varphi(x) = 1 \\
 &\iff \varphi(x + x) = 1 && \varphi \text{ est un morphisme} \\
 &\iff \varphi(2x) = 1 \\
 &\iff 2x = \varphi^{-1}(1) \\
 &\iff x = \varphi^{-1}(1)/2
 \end{aligned}$$

Dès lors, si on pose $x = \varphi^{-1}(1)/2$, alors $\varphi(x) \in \mathbb{Z}$ et $2\varphi(x) = 1$ donc $\varphi(x) = 1/2$ ce qui est absurde : les deux groupes ne sont pas isomorphes.

4. Il n'existe de toute façon aucune bijection (morphisme ou non) entre les deux ensembles car l'un est dénombrable et pas l'autre, mais c'est plutôt au programme de deuxième année. La même preuve que pour la question 2 prouve qu'ils ne sont pas isomorphes.
5. Intéressons-nous cette fois à l'équation $x^2 = -1$ qui a des solutions sur \mathbb{C} mais pas sur \mathbb{R} . Supposons qu'il existe un isomorphisme $\varphi : \mathbb{C}^* \rightarrow \mathbb{R}^*$. Soit $x \in \mathbb{C}^*$.

$$\begin{aligned}
 \varphi(x)^2 = -1 &\iff \varphi(x) \times \varphi(x) = -1 \\
 &\iff \varphi(x \times x) = -1 && \varphi \text{ est un morphisme} \\
 &\iff \varphi(x^2) = -1 \\
 &\iff x^2 = \varphi^{-1}(-1)
 \end{aligned}$$

Or, tout complexe admet des racines carrées (et tout complexe non nul en admet exactement deux et $\varphi^{-1}(-1)$ est non nul car appartient à \mathbb{C}^* mais c'est inutile) donc il existe x tel que $x^2 = \varphi^{-1}(-1)$ et donc $\varphi(x)^2 = -1$ ce qui est absurde car φ est à valeurs réelles : les deux groupes ne sont pas isomorphes.

Exercice 29 - Autour de l'inverse : ★★

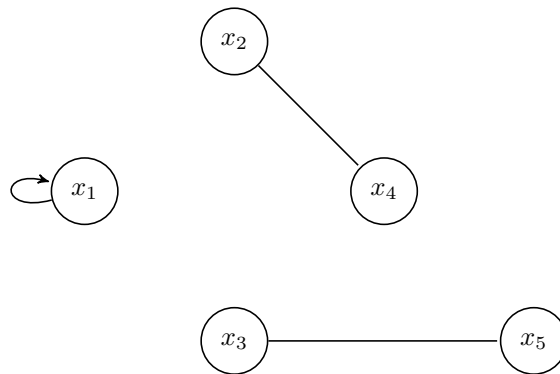
1. Montrer par récurrence que, pour tout n , une involution sur un ensemble à $2n + 1$ éléments admet au moins un point fixe.
2. Soit G un groupe. Montrer que $x \mapsto x^{-1}$ est un automorphisme de G (i.e. un morphisme bijectif de G dans lui-même) si et seulement si G est abélien.
3. On suppose dans 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.

Correction :

- Montrons le résultat par récurrence. Soit H_n : « Toute involution sur un ensemble fini de cardinal $2n + 1$ admet au moins un point fixe. » Si $n = 0$, on a un ensemble à un élément donc la seule involution est l'identité qui admet un point fixe donc H_0 est vraie. Soit $n \geq 0$, supposons que H_n soit vraie. Montrons que H_{n+1} est vraie. Soit E un ensemble de cardinal $2(n+1) + 1 = 2n + 3$ et soit f une involution de E . Soit a un élément de E . Si a est un point fixe c'est terminé. Sinon il existe b distinct de a tel que $b = f(a)$. Or, f est une involution donc $f(b) = a$. f est donc une involution de $E \setminus \{a, b\}$ qui est un ensemble à $2n + 1$ éléments donc admet un point fixe par hypothèse de récurrence. Donc H_{n+1} est vraie donc H_n est vraie pour tout n par le principe de récurrence. Nous le montrerons d'une autre façon dans l'exercice 6 du chapitre 32.
- Notons cette fonction φ . Prouvons que c'est une bijection. Soient g_1 et g_2 tels que $g_1^{-1} = g_2^{-1}$. En passant à l'inverse, $g_1 = g_2$: φ est injective. Soit $y \in G$. Alors $\varphi(y^{-1}) = y$: y^{-1} est un antécédent de y donc φ est surjective donc bijective (on pouvait aussi dire que φ est involutive donc bijective). Prouvons donc que φ est un morphisme de groupes si et seulement si G est abélien. Supposons que φ soit un morphisme et soient a, b deux éléments de G . Alors $\varphi(ab) = \varphi(a)\varphi(b)$ c'est-à-dire que $(ab)^{-1} = a^{-1}b^{-1}$. Or, $a^{-1}b^{-1} = (ba)^{-1}$ (on change l'ordre quand on inverse) si bien que $(ab)^{-1} = (ba)^{-1}$. En passant à l'inverse, il vient : $ab = ba$, G est abélien. Réciproquement, si G est abélien, alors pour tous a et b dans G , $ab = ba$ donc, en passant à l'inverse, $(ab)^{-1} = a^{-1}b^{-1}$ c'est-à-dire que $\varphi(ab) = \varphi(a)\varphi(b)$: φ est un morphisme, d'où l'équivalence.
- (a) Notons cette fonction φ . Soient a et b dans G tels que $f(a)a^{-1} = f(b)b^{-1}$. Alors, en multipliant par a à droite, $f(a) = f(b)b^{-1}a$, et en multipliant par $f(b)^{-1}$ à gauche, $f(b)^{-1}f(a) = b^{-1}a$. Or, f est un morphisme donc $f(b^{-1}a) = b^{-1}a$: $b^{-1}a$ est un point fixe de f , donc $b^{-1}a = e$ par hypothèse sur f , si bien que $a = b$: g est injective. Puisqu'elle est injective entre deux ensembles finis de même cardinal (d'un ensemble fini dans lui-même), c'est une bijection.
- (b) Soit $x \in G$. φ étant surjective, il existe $a \in G$ tel que $\varphi(a) = x$ donc $f(a) = ax$. En appliquant f (morphisme involutif), il vient : $a = f(a)f(x)$ si bien que $f(a) = af(x)^{-1}$ donc, finalement, $ax = af(x)^{-1}$ et tout élément est régulier (ou en multipliant à gauche par a^{-1}) donc $x = f(x)^{-1}$ si bien que $f(x) = x^{-1}$.
- (c) D'après la question 2, G est abélien. Prouvons que le cardinal de G est impair, ce qui se voit très bien sur un dessin en associant chaque élément et son image (rappelons que f est une involution avec un unique point fixe donc, à part le point fixe, les éléments sont regroupés par paires, ce qui donne un nombre impair) :



Supposons que G soit de cardinal pair qu'on note $2p$. Alors $G \setminus \{e\}$ est de cardinal $2p - 1$, et la restriction de G à $E \setminus \{a\}$ est donc une involution sans point fixe ce qui est absurde d'après la question 1.

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 $AB = \{ab \mid a \in A, b \in B\}$.

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

Correction :

- Soit $g \in G$. Soit φ qui va de B dans $\{gb^{-1} \mid b \in B\}$ qui à b associe gb^{-1} . Montrons que φ est bijective. Elle est surjective par définition de l'ensemble $\{gb^{-1} \mid b \in B\}$. Montrons qu'elle est injective. Soient b_1 et b_2 dans B tels que $\varphi(b_1) = \varphi(b_2)$. Alors $gb_1^{-1} = gb_2^{-1}$. En multipliant par g^{-1} à gauche (ou, car dans un groupe, tout élément est régulier), il vient : $b_1^{-1} = b_2^{-1}$. En multipliant par b_1 à gauche, on trouve $e = b_1b_2^{-1}$ et en multipliant par b_2 à droite, on trouve $b_2 = b_1$: φ est injective donc bijective. On en déduit que $\{gb^{-1} \mid b \in B\}$ et B ont le même cardinal. Si A et $\{gb^{-1} \mid b \in B\}$ sont disjoints, le cardinal de l'union est la somme des cardinaux donc est égal à $\text{card}(A) + \text{card}(B) > \text{card}(G)$ ce qui est absurde puisque l'union est incluse dans G : les deux ensembles ne sont pas disjoints.

2. Soit $g \in G$. Soit a dans l'intersection (non vide d'après ce qui précède). Alors $a \in A$ et il existe $b \in B$ tel que $a = gb^{-1}$ donc, en multipliant par b à droite, on obtient : $g = ab$ donc $g \in AB$. En d'autres termes, $G \subset AB$ et l'inclusion réciproque étant évidente, on a l'égalité voulue.

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

- Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$, KH étant défini de façon analogue.
- (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 si 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 $\text{card}(HK) \times \text{card}(H \cap K) = \text{card}(H) \times \text{card}(K)$.

Correction :

- HK est évidemment non vide car H et K sont non vides (ce sont des sous-groupes de G). Plus précisément, $e \in H$ et $e \in K$ donc $e * e = e \in HK$. Ainsi, HK est un sous-groupe de G si et seulement si HK est stable par produit (i.e. la loi de G) et par inverse.

Supposons que HK soit un sous-groupe de G , et soit $g \in HK$. HK étant un sous-groupe de G , il est stable par inverse donc $g^{-1} \in HK$. Il existe alors $h \in H$ et $k \in K$ tels que $g^{-1} = hk$ si bien que $g = k^{-1}h^{-1} \in KH$: on a l'inclusion $HK \subset KH$, et par symétrie des rôles, on a l'inclusion réciproque donc l'égalité.

Réciproquement, supposons que $HK = KH$ (ce qui ne veut pas dire que $hk = kh$ pour tous $h \in H$ et $k \in K$!) et prouvons que HK est un sous-groupe de G . Soient x_1 et x_2 deux éléments de HK : il existe h_1 et h_2 dans H et k_1 et k_2 dans K tels que $x_1 = h_1k_1$ et $x_2 = h_2k_2$ et donc $x_1x_2 = h_1(k_1h_2)k_2$ (la loi est associative). Or, $KH = HK$ donc $k_1h_2 \in HK$: il existe $h_3 \in H$ et $k_3 \in K$ tels que $k_1h_2 = h_3k_3$ si bien que $x_1x_2 = (h_1h_3)(k_3k_1)$. Or, H et K sont stables par produit (la loi de G) donc $h_1h_3 \in H$ et idem pour k_3k_1 , si bien que $x_1x_2 \in HK$: HK est stable par produit. De plus, $x_1^{-1} = k_1^{-1}h_1^{-1}$. De même, il existe $h_4 \in H$ et $k_4 \in K$ tels que $k_1^{-1}h_1^{-1} = h_4k_4$ donc $x_1^{-1} = h_4k_4 \in HK$: HK est stable par inverse, donc c'est un sous-groupe de G .

- (a) Supposons qu'il existe un tel x . Alors $h_2 = h_1x$ donc, en multipliant à gauche par h_1^{-1} , il vient : $x = h_1^{-1}h_2$. De plus, $k_2 = x^{-1}k_1$ donc, de même : $x^{-1} = k_2k_1^{-1}$ donc $x = k_1k_2^{-1}$ (ne pas oublier de changer l'ordre). Dès lors, $h_1^{-1}h_2 = k_1k_2^{-1}$. En multipliant à gauche par h_1 et à droite par k_2 , on trouve bien que $h_2k_2 = h_1k_2$. Réciproquement, supposons que $h_1k_1 = h_2k_2$ et notons $x = h_1^{-1}h_2$ (d'après ce qui précède, si un tel x existe, c'est lui). Puisque $h_1k_1 = h_2k_2$, alors en multipliant par h_1^{-1} à gauche et k_2^{-1} à droite, on trouve que $h_1^{-1}h_2 = k_1k_2^{-1}$ c'est-à-dire que

$$x = h_1^{-1}h_2 = k_1k_2^{-1}$$

On en déduit que $x \in H$ (car H est stable par produit et par inverse puisque c'est un sous-groupe) et que $x \in K$ (pour les mêmes raisons) donc que $x \in H \cap K$, et on a bien $h_2 = h_1x$ (en multipliant à gauche par h_1) et $k_2 = x^{-1}k_1$ (en multipliant à droite par k_2 et à gauche par x^{-1}).

- (b) Soit

$$\varphi : \begin{cases} H \times K & \rightarrow & HK \\ (h, k) & \mapsto & hk \end{cases}$$

Alors φ est surjective par définition mais n'est pas forcément injective. Plus précisément, on vient de voir que, si $g \in HK$ et si (h_1, k_1) est un antécédent de g par φ , alors (h_2, k_2) est un autre antécédent de g si et seulement si il existe $x \in H \cap K$ tel que $h_2 = h_1x$ et $k_2 = x^{-1}k_1$. En d'autres termes, si on note $A = \varphi^{-1}(\{g\})$ l'ensemble des antécédents de g par φ , alors la fonction

$$\psi : \begin{cases} H \cap K & \rightarrow & A \\ x & \mapsto & (h_1x, x^{-1}k_1) \end{cases}$$

est surjective, c'est-à-dire que tous les antécédents de g sont de cette forme. Il est assez simple de voir que ψ est injective (si $\psi(x_1) = \psi(x_2)$ alors $h_1x_1 = h_1x_2$ donc $x_1 = x_2$) donc bijective, si bien que $\text{card}(A) = \text{card}(H \cap K)$. En d'autres termes, tout élément g de G a exactement $\text{card}(H \cap K)$ antécédents, et le lemme des bergers appliqué à φ permet de conclure.

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

Correction : Tout d'abord, $\ker(f)$ est inclus dans G donc est fini (une partie d'un ensemble fini est finie) et $\text{Im}(f)$ est finie car $f : G \rightarrow \text{Im}(f)$ est surjective (si E est fini et $f : E \rightarrow F$ est surjective alors F est fini, cf. chapitre précédent). On va raisonner comme dans l'exercice précédent. Soit $y \in \text{Im}(f)$ et soit $x_1 \in G$ un antécédent de y . Soit enfin $x_2 \in G$. Alors (on note e le neutre de H et on utilise plusieurs fois le fait que f est un morphisme) :

$$\begin{aligned} x_2 \text{ est un antécédent de } y &\iff f(x_2) = y \\ &\iff f(x_2) = f(x_1) \\ &\iff f(x_2)f(x_1)^{-1} = e \\ &\iff f(x_2 * x_1^{-1}) = e \\ &\iff x_2 * x_1^{-1} \in \ker(f) \\ &\iff \exists x \in \ker(f), x_2 * x_1^{-1} = x \\ &\iff \exists x \in \ker(f), x_2 = x * x_1 \end{aligned}$$

Dès lors, si on note A l'ensemble des antécédents de y par f , l'application

$$\varphi : \begin{cases} \ker(f) & \rightarrow & A \\ x & \mapsto & x * x_1 \end{cases}$$

est surjective, et on montre comme ci-dessus qu'elle est injective donc bijective : $\text{card}(A) = \text{card}(\ker(f))$. On en déduit que tout élément de $\text{Im}(f)$ admet exactement $\text{card}(\ker(f))$ antécédents, et on conclut à l'aide du lemme des bergers.

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 $Z(G) = \{x \in G \mid \forall y \in G, xy = yx\}$ c'est-à-dire l'ensemble des éléments qui commutent avec tout le monde.

1. Montrer que si $f : G \rightarrow G$ 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.

Correction :

1. Montrons le résultat par double inclusion. Soit $y \in f(Z(G))$ et prouvons que $y \in Z(G)$, c'est-à-dire qu'il faut prouver que y commute avec tout le monde. Soit donc $x \in G$, et prouvons que $xy = yx$. $y \in f(Z(G))$ donc il existe $a \in Z(G)$ tel que $y = f(a)$. f étant un automorphisme, elle est surjective donc il existe $b \in G$ tel que $x = f(b)$. f étant un morphisme, $yx = f(a)f(b) = f(ab)$. Or, $a \in Z(G)$ donc a commute avec b si bien que

$$\begin{aligned} yx &= f(ba) \\ &= f(b)f(a) \\ &= xy \end{aligned}$$

c'est-à-dire que $y \in Z(G)$: d'où l'inclusion $f(Z(G)) \subset Z(G)$. Prouvons l'inclusion réciproque : soit $y \in Z(G)$. f étant surjective, il existe $x \in G$ tel que $y = f(x)$. Prouvons donc que $x \in Z(G)$ c'est-à-dire que x commute avec tout le monde. Soit $z \in G$. f étant un morphisme, $f(xz) = f(x)f(z) = yf(z)$. Or, $y \in Z(G)$ donc $yf(z) = f(z)y$ si bien que

$$\begin{aligned} f(xz) &= f(z)y \\ &= f(z)f(x) \\ &= f(zx) \end{aligned}$$

et f est injective donc $xz = zx$: $x \in Z(G)$ et donc $y = f(x) \in f(Z(G))$, d'où l'inclusion réciproque, d'où l'égalité.

2. L'inclusion $Z(G) \cap H \subset Z(H)$ est immédiate : un élément de $Z(G) \cap H$ est un élément de H qui commute avec tous les éléments de G , donc il commute en particulier avec tous les éléments de H . Prouvons que l'inclusion réciproque est fautive en général. Il faut taper dans le non abélien pour que ça ait des chances de marcher, car dans un groupe abélien, le centre est le groupe tout entier. Plaçons-nous dans S_E avec E de cardinal au moins 3 si bien que, d'après l'exercice 24, $S_E = \{\text{Id}_E\}$. Soient a et b deux éléments distincts de E et soit g la fonction qui échange a et b , c'est-à-dire que $g(x) = x$ pour tout $x \neq a, b$, $g(a) = b$ et $g(b) = a$. Alors $H = \{\text{Id}_E; g\}$ est un sous-groupe de S_E (c'est le groupe engendré par g). En effet, il est non vide, stable par composition et stable par symétrique (car g est son propre symétrique, toujours pour la composition). H est abélien car le neutre (l'identité ici) commute avec tout le monde donc $Z(H) = H$ mais $Z(S_E) \cap H = \{\text{Id}_E\}$: l'inclusion peut être stricte.

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

1. Montrer que les trois conditions suivantes sont équivalentes :

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

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 $f : G_1 \rightarrow G_2$ 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 .

Correction :

1. Si on les note 1, 2, 3, prouvons que $1 \Rightarrow 2, 2 \Rightarrow 3$ et $3 \Rightarrow 1$.

Supposons 1 et prouvons 2. Soit $x \in G$. Prouvons que $xHx^{-1} = H$ par double inclusion. Soit $h \in H$. Alors $hx \in Hx$ et $xH = Hx$ par hypothèse (ce qui ne veut pas dire que $xh = hx$!) donc il existe $h' \in H$ tel que $hx = xh'$ si bien que (en multipliant par x^{-1} à droite) $h = xh'x^{-1} \in xHx^{-1}$. Réciproquement, soit $y \in xHx^{-1}$: il existe donc $h \in H$ tel que $y = xhx^{-1}$. De même, il existe h' tel que $xh = h'x$ si bien que $y = h'xx^{-1} = h' \in H$. D'où l'inclusion réciproque, d'où l'égalité.

L'implication $2 \Rightarrow 3$ étant évidente (c'est l'inclusion $xHx^{-1} \subset H$ qui est vraie par hypothèse), prouvons que $3 \Rightarrow 1$. Supposons donc 3 et prouvons 1 : soit $x \in G$, prouvons que $xH = Hx$. Soit $g \in xH$: il existe donc $h \in H$ tel que $g = xh$. En multipliant par x^{-1} à droite : $gx^{-1} = xhx^{-1}$ qui est un élément de H par hypothèse (on a supposé 3 vraie). Il existe donc $h' \in H$ tel que $gx^{-1} = h'$ donc $g = h'x \in Hx$: d'où l'inclusion $xH \subset Hx$. L'inclusion réciproque est analogue et laissée en exercice.

2. Supposons G commutatif. Soit H un sous-groupe de G et prouvons la propriété 3 ci-dessus (c'est la seule qui ne demande pas de prouver deux inclusions, c'est la plus simple à manipuler). Soit $x \in G$ et soit $h \in H$. Le groupe étant abélien, $xhx^{-1} = hxx^{-1} = h \in H$, H est distingué.
 3. Soit $x \in \ker(f)$ et soit $h \in \ker(f)$. f étant un morphisme, $f(xhx^{-1}) = f(x)f(h)f(x)^{-1}$. Or, $h \in \ker(f)$ donc $f(h) = e_2$ (le neutre de G_2) si bien que

$$\begin{aligned} f(xhx^{-1}) &= f(x)e_2f(x)^{-1} \\ &= f(x)f(x)^{-1} \\ &= e_2 \end{aligned}$$

c'est-à-dire que $xhx^{-1} \in \ker(f)$: le groupe est distingué.

4. Soit $x \in G$ et soit $h \in Z(G)$. Montrons que $xhx^{-1} \in Z(G)$, c'est-à-dire que xhx^{-1} commute avec tout le monde. Soit donc $y \in G$. Rappelons que $h \in Z(G)$ donc h commute avec tout le monde.

$$\begin{aligned} xhx^{-1}y &= xx^{-1}hy \\ &= eh y \\ &= hy \end{aligned}$$

et

$$\begin{aligned}
yhx^{-1} &= yhx^{-1} \\
&= yh \\
&= hy
\end{aligned}$$

puisque h et y commutent. Finalement, $xhx^{-1}y = yhx^{-1}$ donc $xhx^{-1} \in Z(G)$, $Z(G)$ est distingué.

5. Pour commencer, soit $x \notin H$. Supposons qu'il existe $y \in H \cap xH$. Alors il existe $h \in H$ tel que $y = xh$ donc tel que $x = yh^{-1}$. Or, $y \in H$ et H est un sous-groupe de G donc stable par produit et par inverse : $x \in H$, ce qui est absurde. L'intersection est donc vide, l'union est disjointe. En particulier, $\text{card}(H \cup xH) = \text{card}(H) + \text{card}(xH)$. Or, l'application $h \mapsto xh$ est une bijection de H dans xH (surjective par définition, et injective car tout élément est régulier, donc si $xh_1 = xh_2$ alors $h_1 = h_2$) donc $\text{card}(xH) = \text{card}(H)$. On en déduit que $\text{card}(H \cup xH) = 2\text{card}(H) = \text{card}(G)$ donc $H \cup xH = G$.

Prouvons à présent que H est distingué. Soit $h \in H$ et soit $x \in G$, et prouvons que $xhx^{-1} \in H$. Si $x \in H$, c'est terminé puisque H est un sous-groupe de G . Sinon, d'après ce qui précède, $xhx^{-1} \in G = H \cup xH$. Supposons par l'absurde que $xhx^{-1} \in xH$: il existe $h' \in H$ tel que $xhx^{-1} = xh'$ donc (tout élément d'un groupe est régulier, ou en multipliant par x^{-1} à gauche) $hx^{-1} = h'$ si bien que $h'^{-1}h = x \in H$ ce qui est exclu. En conclusion, $xhx^{-1} \in H$, H est distingué.

Exercice 35 - Théorème de Cayley : $\clubsuit\spadesuit$ 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.

Correction : Prouvons que $f : g \mapsto \varphi_g$ est une injection de G dans S_G . Tout d'abord, f est bien à valeurs dans S_G puisque, pour tout g , φ_g est bijective comme on le montre de même que précédemment. Soient $g_1 \neq g_2$ deux éléments de G . Alors $\varphi_{g_1}(e) = g_1 \neq g_2 = \varphi_{g_2}(e)$: les deux fonctions φ_{g_1} et φ_{g_2} sont différentes en e donc ne sont pas la même fonction, c'est-à-dire que $f(g_1) \neq f(g_2)$: f est injective. Prouvons à présent que f est un morphisme de groupes. Soient g_1 et g_2 deux éléments (pas forcément distincts) de G . Soit $x \in G$. Par associativité de la loi sur G :

$$\begin{aligned}
\varphi_{g_1g_2}(x) &= g_1g_2x \\
&= g_1(g_2x) \\
&= \varphi_{g_1}(g_2x) \\
&= \varphi_{g_1} \circ \varphi_{g_2}(x)
\end{aligned}$$

et cette égalité est valable pour tout $x \in G$ donc $\varphi_{g_1g_2} = \varphi_{g_1g_2} \circ \varphi_{g_1g_2}$, c'est-à-dire que $f(g_1g_2) = f(g_1) \circ f(g_2)$: f est bien un morphisme de groupes, et puisque f est injective, c'est une bijection sur son image, c'est-à-dire que G et $\text{Im}(f)$ sont isomorphes, ce qui est le résultat voulu puisque $\text{Im}(f)$ est un sous-groupe de S_G (l'image d'un morphisme est un sous-groupe). Soit à présent G un groupe à n éléments. Alors G et $\llbracket 1; n \rrbracket$ sont en bijection (car ont le même cardinal) donc, d'après l'exercice 24, S_G et S_n sont isomorphes, c'est-à-dire qu'il existe $\psi : S_G \rightarrow S_n$ isomorphisme, et $\psi \circ f$ est alors un morphisme injectif de G dans S_n et on conclut de la même façon.

Remarque : Ainsi, un groupe à 10 éléments est isomorphe à un sous-groupe de S_{10} . On pourrait se dire que, pour trouver tous les groupes à 10 éléments (à isomorphisme près), il suffit de trouver tous les sous-groupes de S_{10} à 10 éléments... Sauf que S_{10} est tellement énorme ($10! = 3628800$ éléments!) que ce n'est pas du tout réalisable en pratique !

18.2.7 Sous-groupes de \mathbb{R}

Exercice 36 : $\clubsuit\spadesuit$

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

Correction :

- Prouvons que G est un sous-groupe de \mathbb{R} (pour la loi + évidemment).
 - $0 = 0 + 2\pi \times 0 \in \mathbb{Z}$: G est non vide.
 - Soient x_1 et x_2 deux éléments de G : il existe $(n_1, n_2, p_1, p_2) \in \mathbb{Z}^4$ tel que $x_1 = n_1 + 2\pi p_1$ et $x_2 = n_2 + 2\pi p_2$. Alors $x_1 + x_2 = (n_1 + n_2) + 2\pi(p_1 + p_2) \in G$ car $n_1 + n_2$ et $p_1 + p_2$ appartiennent à \mathbb{Z} : G est stable par somme.

- De plus, $-x_1 = (-n_1) + 2\pi \times (-p_1) \in G$ car $-n_1$ et $-p_1$ appartiennent à \mathbb{Z} : G est stable par inverse.

Finalement, G est un sous-groupe de \mathbb{R} . Pour prouver qu'il est dense, il suffit de prouver qu'il n'est pas de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}$. Raisonnons par l'absurde et supposons qu'il existe $\alpha \in \mathbb{R}$ tel que $G = \alpha\mathbb{Z}$. $1 = 1 + 2\pi \times 0 \in G$ donc il existe $k \in \mathbb{Z}$ tel que $1 = \alpha k$, et $2\pi = 0 + 2\pi \times 1 \in G$ donc il existe $n \in \mathbb{Z}$ tel que $2\pi = \alpha n$. Or, $\alpha k = 1$ donc k est non nul et $\alpha = 1/k$ si bien que $\pi = n/2k \in \mathbb{Q}$. Absurde : G n'est pas de la forme $\alpha\mathbb{Z}$ donc est dense dans \mathbb{R} .

2. Soient $x < y$ deux éléments de $[-1; 1]$ et soit $z \in]x; y[$ (on peut prendre par exemple $(x + y)/2$). Soit enfin $a = \arccos(z)$. L'ensemble G étant dense dans \mathbb{R} , par caractérisation de la borne supérieure, il existe une suite $(x_k)_{k \in \mathbb{N}}$ d'éléments de G qui converge vers α . Or, la fonction \cos est continue donc $\cos(x_k) \xrightarrow[k \rightarrow +\infty]{} \cos(\alpha) = z$ donc $\cos(x_k) \in]x; y[$ pour k assez grand. Or, pour tout k , il existe n_k et p_k dans \mathbb{Z} tels que $x_k = n_k + 2\pi p_k$ et donc

$$\cos(x_k) = \cos(n_k) \in \{\cos(n) \mid n \in \mathbb{N}\}$$

c'est-à-dire qu'il existe un élément de cet ensemble dans $]x; y[$, d'où la densité cherchée.

Exercice 37 : ♦♦♦

1. Soit $(a, b) \in \mathbb{R}^2$. Montrer que $a\mathbb{Z} + b\mathbb{Z} = \{an + bk \mid (n, k) \in \mathbb{Z}^2\}$ 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 qu'il existe $z \in \alpha\mathbb{Z} + \mathbb{Z}$ tel que $0 < z < b - a$.
 - (c) Conclure (on pourra s'inspirer de la preuve de la densité de \mathbb{Q} dans \mathbb{R}).

Correction :

1. Notons $G = a\mathbb{Z} + b\mathbb{Z}$. Le fait que G est un sous-groupe de \mathbb{R} a été prouvé en cours. Rappelons qu'un sous-groupe de \mathbb{R} est soit de la forme $\alpha\mathbb{Z}$ (avec α un réel), soit dense. Raisonnons par double implication.
 - Si a est nul, alors $G = a\mathbb{Z}$ donc n'est pas dense. Idem si b est nul. Supposons enfin que a et b soient non nuls, et que a/b est rationnel : attention, a et b ne sont pas forcément entier (par exemple on peut prendre $a = b = \pi$), l'écriture de a/b comme rationnel n'est donc pas a/b . Il existe p et q (que l'on peut prendre premiers entre eux, mais ce n'est pas nécessaire sauf pour l'inclusion réciproque, comme on va le voir ci-dessous) tels que $a/b = p/q$. Dès lors, pour tout $(n, k) \in \mathbb{Z}^2$ (p est déjà pris) :

$$\begin{aligned} an + bk &= b \left(\frac{a}{b} \times n + k \right) \\ &= b \times \left(\frac{p}{q} \times n + k \right) \\ &= b \times \frac{np + kq}{q} \\ &= \frac{b}{q} \times (np + kq) \\ &\in \frac{b}{q} \mathbb{Z} \end{aligned}$$

si bien que $G \subset (b/q)\mathbb{Z}$ donc G n'est pas dense (il n'y a par exemple aucun élément de G entre 0 et b/q). Bien que cela ne soit pas nécessaire, puisqu'on a déjà prouvé que G n'est pas dense, prouvons l'inclusion réciproque (et supposons cette fois que p et q sont premiers entre eux, hypothèse non nécessaire pour l'inclusion prouvée ci-dessus). Soit donc $x \in (b/q)\mathbb{Z}$: il existe $k \in \mathbb{Z}$ tel que $x = bk/q$. D'après le théorème de Bézout (p et q sont premiers entre eux donc k est un multiple de $p \wedge q = 1$), il existe u et v dans \mathbb{Z} tels que $k = up + vq$ si bien que :

$$\begin{aligned}
x &= \frac{b}{q} \times (up + vq) \\
&= ub \times \frac{p}{q} + bv \\
&= ub \times \frac{a}{b} + bv \\
&= au + bv \\
&\in G
\end{aligned}$$

- Supposons à présent a et b non nuls et a/b irrationnel. Supposons que G soit de la forme $\alpha\mathbb{Z}$. Alors, en particulier, $a = a \times 1 + b \times 0$ et $b = 0 \times a + b \times 1$ appartiennent à G donc il existe n et k (non nuls car a et b sont non nuls) tels que $a = \alpha n$ et $b = \alpha k$ si bien que

$$\alpha = \frac{a}{n} = \frac{b}{k}$$

et donc $a/b = n/k \in \mathbb{Q}$: absurde (ou on aurait pu raisonner par contraposée). D'où l'équivalence.

- (a) On prouve aisément que H contient 0 et est stable par somme (exo). Ainsi, c'est un sous-groupe de \mathbb{R} si et seulement si il est stable par opposé.

Supposons α irrationnel. $1 = \alpha \times 0 + 1$, $0 \in \mathbb{N}$ et $1 \in \mathbb{Z}$ donc $1 \in H$. Prouvons que $-1 \notin H$, ce qui prouvera que H n'est pas un sous-groupe car n'est pas stable par différence. Supposons par l'absurde que $-\alpha \in H$: il existe $n \in \mathbb{N}$ et $k \in \mathbb{Z}$ tels que $-\alpha = \alpha n + k$. n étant positif, il est impossible que n soit égal à -1 donc $n + 1 \neq 0$ si bien que

$$\alpha = \frac{-k}{n+1} \in \mathbb{Q}$$

ce qui est absurde.

Supposons à présent α rationnel. On a déjà dit qu'il suffisait de prouver que H est stable par opposé. Soit donc $x = \alpha n + k \in H$ (avec évidemment $n \in \mathbb{N}$ et $k \in \mathbb{Z}$). α est rationnel non nul donc il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $\alpha = p/q$ si bien que

$$-x = \frac{p}{q} \times (-n) - k$$

On veut ajouter un entier à $-n$ pour le rendre positif : on l'ajoute et on n'oublie pas de compenser. Plus précisément, il suffit de voir que, pour tout entier $a \in \mathbb{Z}$,

$$-x = (-k - pa) + \frac{p}{q}(-n + qa)$$

Or, q étant non nul, il existe a tel que $-n + qa > 0$ ce qui permet de conclure. Un raisonnement analogue à celui de la question précédente (Bézout puis ajouter des entiers au bon endroit pour avoir des entiers positifs, exo) permet de prouver plus précisément que, si $\alpha \neq 0$, alors $H = \alpha\mathbb{Z}$ (tandis que $H = \mathbb{Z}$ si $\alpha = 0$, évidemment).

- $\alpha\mathbb{Z} + \mathbb{Z}$ est, lui, un groupe d'après la question 1, et dense, toujours d'après la question 1, car $\alpha/1$ est irrationnel : il existe donc z dans $\alpha\mathbb{Z} + \mathbb{Z}$, qu'on note $\alpha n + k$ avec n et k dans \mathbb{Z} , qui vérifie $0 < z < b - a$. Si $n \geq 0$ alors $z \in H$ donc z convient, et si $n < 0$, alors $-z \in H$ (car $-z = -\alpha n - k$ avec $-n \in \mathbb{N}$) et on a $|-z| = z$ donc $0 < |-z| < b - a$ donc $-z$ convient : dans tous les cas, on a le résultat.
- Supposons dans un premier temps $z > 0$. Suivons l'indication de l'énoncé et raisonnons comme dans la démonstration de la densité de \mathbb{Q} : on va partir d'un élément $n_0 \leq a$ et on va faire des « sauts » d'amplitude z jusqu'à tomber entre a et b (cf. chapitre 12 pour un dessin). Soit $n_0 \in \mathbb{Z}$ tel que $n_0 \leq a$ ($n_0 = \lfloor a \rfloor$ convient, mais on peut le dire directement). introduisons donc l'ensemble

$$A = \{k \in \mathbb{Z} \mid n_0 + kz < b\}$$

$n_0 \leq a < b$ donc $n_0 \in A$: A est non vide. De plus, $k \in A \iff k < \frac{b - n_0}{z}$ (car $z > 0$) donc A est majoré. A est une partie non vide majorée de \mathbb{Z} donc admet un plus grand élément k_0 , et on prouve comme dans la preuve de la densité de \mathbb{Q} (exo, utiliser le fait que $z < b - a$) que $n_0 + k_0 z \in]a; b[$. Enfin, $n_0 \leq a < n_0 + k_0 z$ donc $k_0 z > 0$ et $z > 0$ donc $k_0 \in \mathbb{N}$. Or, $z = \alpha n + k$ avec $n \in \mathbb{N}$ (on a pris z dans H) donc $n_0 + k_0 z = n_0 + k_0 k + n k_0 \alpha \in H$ car n et k_0 sont dans \mathbb{N} .

Supposons à présent $z < 0$: on fait la même chose, mais en partant de b puisque, si on fait des sauts d'amplitude z , z étant négatif, on fait « des sauts en arrière » (le dessin est analogue et laissé à votre charge). On note n_1 un entier supérieur ou égal à b , et on prouve de même que

$$B = \{k \in \mathbb{Z}, |n_1 = kz > a\}$$

admet un plus petit élément k_1 , que $n_1 + k_1 z \in]a; b[$, que $k_1 \in \mathbb{N}$ et on conclut de même.

Dans tous les cas, il existe un élément de H dans $]a; b[$, donc H est dense dans \mathbb{R} puisque a et b sont quelconques.

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).

Correction : Essayons de traduire l'énoncé d'un point de vue mathématique. Notons d la date de naissance. Un nombre commence par d s'il s'écrit sous la forme $da_1a_2 \dots a_n$ où les a_i sont des entiers (par exemple, un nombre qui commence par 1022002 s'écrit sous la forme $1022002a_1a_2 \dots a_n$) donc s'il est compris entre un terme de la forme $d0 \dots 0 = d \times 10^n$ et $d9 \dots 9 = (d+1) \times 10^n - 1$ (un nombre commence par 1022002 s'il est compris entre 1022002 s'il est compris entre 102200200...0 et 102200300...0), donc s'il est supérieur ou égal à $d \times 10^n$ et strictement inférieur à $(d+1) \times 10^n$. D'où les équivalences suivantes (attention à la rédaction!) :

$$\begin{aligned} \text{Il existe une puissance de 2 qui commence par } d &\iff \exists(k, n) \in \mathbb{Z}^2, d \times 10^n \leq 2^k < (d+1) \times 10^n \\ &\iff \exists(k, n) \in \mathbb{Z}^2, n \ln(10) + \ln(d) \leq k \ln(2) < n \ln(10) + \ln(d+1) \\ &\iff \exists(k, n) \in \mathbb{Z}^2, \ln(d) \leq k \ln(2) - n \ln(10) < \ln(d+1) \\ &\iff \exists(k, n) \in \mathbb{Z}^2, \frac{\ln(d)}{\ln(10)} \leq k \frac{\ln(2)}{\ln(10)} - n < \frac{\ln(d+1)}{\ln(10)} \end{aligned}$$

Il suffit de prouver que $G = \left\{ k \frac{\ln(2)}{\ln(10)} - n \mid (k, n) \in \mathbb{Z}^2 \right\}$ est dense dans \mathbb{R} , ce qu'on fait de même que dans l'exercice 36, en utilisant le fait que $\ln(2)/\ln(10)$ est irrationnel. En effet, s'il est rationnel, alors il existe a et b dans \mathbb{N}^* (ce nombre est strictement positif) tels que $\ln(2)/\ln(10) = a/b$ donc $b \ln(2) = a \ln(10)$ si bien que $2^b = 10^a$. En particulier, puisque $a \geq 1$, 2^b est divisible par 5 ce qui est absurde, d'où la conclusion voulue. On voit que l'argument clef est que 2^b n'est pas une puissance de 10, donc cela marche avec n'importe quelle puissance à part les puissances de 10, pour lesquelles il est immédiat que cela ne fonctionne pas puisqu'une puissance de 10 s'écrit forcément 10000...0.

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

Exercice 39 - Produit semi-direct : ★★

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

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

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 .

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

Correction :

- On sait que S_G , l'ensemble des bijections de G dans lui-même, est un groupe pour la loi \circ (cf. cours). Il suffit donc de prouver que $\text{Aut}(G)$ est un sous-groupe de S_G . Il est non vide car convient l'identité, est stable par composition car une composée de morphismes est un morphisme, et une composée de bijections est une bijection, donc une composée d'automorphismes est un automorphisme, et enfin il est stable par inverse puisque la réciproque d'un morphisme bijectif est un morphisme (toujours bijectif). On en déduit le résultat voulu.
- Ici, par contre, il faut tout démontrer. Précisons que la notation $\varphi(k_1)(h_2)$ n'est pas fautive puisque $\varphi(k_1)$ est, par définition, un automorphisme de H donc est en particulier une fonction de H dans H , qu'on peut évaluer en un élément de H .

- Prouvons que la loi est associative. Soient $(h_1, k_1), (h_2, k_2)$ et (h_3, k_3) trois éléments de $H \times K$. Tout d'abord :

$$\begin{aligned} (h_1, k_1) * ((h_2, k_2) * (h_3, k_3)) &= (h_1, k_1) * (h_2 \varphi(k_2)(h_3), k_2 k_3) \\ &= (h_1 \varphi(k_1) [h_2 \varphi(k_2)(h_3)], k_1 (k_2 k_3)) \\ &= (h_1 \varphi(k_1) [h_2 \varphi(k_2)(h_3)], k_1 k_2 k_3) \end{aligned}$$

puisque la loi du groupe est associative (on peut donc enlever les parenthèses dans la deuxième coordonnée). De plus :

$$\begin{aligned} ((h_1, k_1) * (h_2, k_2)) * (h_3, k_3) &= (h_1 \varphi(k_1)(h_2), k_1 k_2) * (h_3, k_3) \\ &= (h_1 \varphi(k_1)(h_2) \varphi(k_1 k_2)(h_3), (k_1 k_2) k_3) \\ &= (h_1 \varphi(k_1)(h_2) \varphi(k_1 k_2)(h_3), k_1 k_2 k_3) \end{aligned}$$

Les deuxièmes coordonnées étant les mêmes, il suffit de prouver que les premières coordonnées sont aussi égales, c'est-à-dire que :

$$h_1 \varphi(k_1) [h_2 \varphi(k_2)(h_3)] = h_1 \varphi(k_1)(h_2) \varphi(k_1 k_2)(h_3)$$

Il suffit donc de prouver que

$$\varphi(k_1) [h_2 \varphi(k_2)(h_3)] = \varphi(k_1)(h_2) \varphi(k_1 k_2)(h_3)$$

Précisons que le membre de gauche est la fonction (plus précisément, l'automorphisme de H) $\varphi(k_1)$ qu'on évalue en $h_2 \varphi(k_2) h_3$ qui est bien un élément de H . Puisque $\varphi(k_1)$ est un morphisme, on peut « casser » ce qu'il y a à l'intérieur, c'est-à-dire que

$$\varphi(k_1) [h_2 \varphi(k_2)(h_3)] = \varphi(k_1)(h_2) \times \varphi(k_1) [\varphi(k_2)(h_3)]$$

où l'on a noté \times la loi du groupe G . En d'autres termes (rappelons que $\varphi(k_2)$ est un automorphisme de H donc en particulier une fonction) :

$$\varphi(k_1) [h_2 \varphi(k_2)(h_3)] = \varphi(k_1)(h_2) \times \varphi(k_1) \circ \varphi(k_2)(h_3)$$

Or, φ est un morphisme de K dans $\text{Aut}(H)$ donc $\varphi(k_1) \circ \varphi(k_2) = \varphi(k_1 k_2)$ si bien que

$$\varphi(k_1) [h_2 \varphi(k_2)(h_3)] = \varphi(k_1)(h_2) \times \varphi(k_1 k_2)(h_3)$$

ce qui est le résultat voulu : la loi $*$ du produit semi-direct est associative.

- Prouvons qu'il y a un élément neutre. On cherche donc un élément (h_1, k_1) tel que, pour tout $(h, k) \in H \times K$, $(h, k) * (h_1, k_1) = (h_1, k_1) * (h, k) = (h, k)$. Or, si $(h, k) \in H \times K$,

$$(h_1, k_1) * (h, k) = (h_1 \varphi(k_1)(h), k_1 k)$$

donc on cherche h_1, k_1 tels que $h_1 \varphi(k_1)(h) = h$ et $k_1 k = k$: prenons $k_1 = e_K$ (le neutre de K) et $h_1 = e_H$ (le neutre de H). Dès lors, $k_1 k = e_K k = k$. De plus, φ étant un morphisme de K dans $\text{Aut}(H)$, $\varphi(e_K)$ est le neutre de $\text{Aut}(H)$ donc Id_H si bien que $\varphi(k_1)(h) = h$ et donc $h_1 \varphi(k_1)(h) = h$. Finalement, on a bien $(e_H, e_K) * (h, k) = (h, k)$. Enfin,

$$(h, k) * (e_H, e_K) = (h \varphi(k)(e_H), k e_K)$$

Il est immédiat que $k e_K = k$. De plus, $\varphi(k)$ est un automorphisme de H donc $\varphi(k)(e_H) = e_H$ si bien qu'on a aussi $(h, k) * (e_H, e_K) = (h, k) : (e_H, e_K)$ est un élément neutre.

- Prouvons enfin que tout élément admet un symétrique pour la loi $*$. Soit $(h, k) \in H \times K$. On cherche (h_1, k_1) tel que $(h, k) * (h_1, k_1) = (h_1, k_1) * (h, k) = (e_H, e_K)$. Or, on a :

$$(h, k) * (h_1, k_1) = (h \varphi(k)(h_1), k k_1) \quad \text{et} \quad (h_1, k_1) * (h, k) = (h_1 \varphi(k_1)(h), k_1 k)$$

Posons tout d'abord $k_1 = k^{-1}$ (K étant un sous-groupe de G , k admet un inverse dans K). Cherchons à présent h_1 . On a $\varphi(k_1) = \varphi(k^{-1})$ si bien qu'on veut avoir

$$h_1 \varphi(k^{-1})(h) = e_H$$

Posons donc $h_1 = (\varphi(k^{-1})(h))^{-1} = \varphi(k^{-1})(h^{-1})$ puisqu'on a un morphisme (attention de ne pas simplifier les -1 , l'un porte sur h et l'autre sur k). Prouvons donc que $(\varphi(k^{-1})(h^{-1}), k^{-1})$ convient. D'une part :

$$(h, k) * (\varphi(k^{-1})(h^{-1}), k^{-1}) = (h\varphi(k) [\varphi(k^{-1})(h^{-1})], kk^{-1})$$

Rappelons que $\varphi(k)$ et $\varphi(k^{-1})$ sont des fonctions donc cette égalité se réécrit :

$$(h, k) * (\varphi(k^{-1})(h^{-1}), k^{-1}) = (h\varphi(k) \circ \varphi(k^{-1})(h^{-1}), kk^{-1})$$

Or, φ est un morphisme donc $\varphi(k) \circ \varphi(k^{-1}) = \varphi(kk^{-1}) = \varphi(e_K) = \text{Id}_H$ comme on l'a déjà vu, si bien que

$$\begin{aligned} (h, k) * (\varphi(k^{-1})(h^{-1}), k^{-1}) &= (hh^{-1}, kk^{-1}) \\ &= (e_H, e_K) \end{aligned}$$

Enfin :

$$(\varphi(k^{-1})(h^{-1}), k^{-1}) * (h, k) = (\varphi(k^{-1})(h^{-1})\varphi(k^{-1})(h), k^{-1}k)$$

$\varphi(k^{-1})$ est un morphisme (c'est un automorphisme de H),

$$\begin{aligned} (\varphi(k^{-1})(h^{-1}), k^{-1}) * (h, k) &= (\varphi(k^{-1})(h^{-1}h), k^{-1}k) \\ &= (\varphi(k^{-1})(e_H), e_K) \\ &= (e_H, e_K) \end{aligned}$$

ce qui permet de conclure.

En conclusion, on a bien un groupe.

3. Le produit direct n'est rien d'autre que le produit semi direct obtenu avec $\varphi : k \mapsto \text{Id}_H$ donc est un cas particulier de produit semi-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 $k_1 \in K$, $f_{k_1} : h \mapsto k_1 h k_1^{-1}$ 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 :

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

On vérifiera bien que φ est un morphisme de groupes.

Correction :

1. Soit $k_1 \in K$. Soient h_1 et h_2 deux éléments de H .

$$\begin{aligned} f_{k_1}(h_1 h_2) &= k_1 h_1 h_2 k_1^{-1} \\ &= k_1 h_1 k_1^{-1} k_1 h_2 k_1^{-1} \\ &= f_{k_1}(h_1) f_{k_1}(h_2) \end{aligned}$$

donc f_{k_1} est bien un morphisme de groupes. Il va bien de H dans H car H est distingué (cf. exercice 34). Prouvons enfin qu'il est bijectif. Soient h_1 et h_2 tels que $f_{k_1}(h_1) = f_{k_1}(h_2)$. Alors $k_1 h_1 k_1^{-1} = k_1 h_2 k_1^{-1}$. Tout élément dans un groupe étant régulier, $h_1 = h_2$: f_{k_1} est injective. Enfin, si $h \in H$, alors on cherche h_1 tel que $k_1 h_1 k_1^{-1} = h$. Alors $h_1 = k_1^{-1} h k_1$ convient et appartient bien à H car H est distingué. En d'autres termes, c'est un antécédent de h donc f_{k_1} est surjective donc bijective : c'est bien un automorphisme de H .

2. Montrons tout d'abord que φ est un morphisme de groupes. Soient k_1 et k_2 deux éléments de K . Alors $\varphi(k_1 k_2) = f_{k_1 k_2}$ c'est-à-dire que c'est la fonction $h \mapsto k_1 k_2 h (k_1 k_2)^{-1} = k_1 k_2 h k_2^{-1} k_1^{-1}$. Or, pour tout $h \in H$,

$$\begin{aligned}\varphi(k_1) \circ \varphi(k_2)(h) &= \varphi(k_1)(k_2 h k_2^{-1}) \\ &= k_1 k_2 h k_2^{-1} k_1^{-1} \\ &= \varphi(k_1 k_2)(h)\end{aligned}$$

et ceci étant valable pour tout h , cela signifie que les deux fonctions $\varphi(k_1 k_2)$ et $\varphi(k_1) \circ \varphi(k_2)$ sont égales : φ est bien un morphisme de groupes. Soit enfin la fonction

$$\psi : \begin{cases} H \times K & \rightarrow G \\ (h, k) & \mapsto hk \end{cases}$$

et prouvons que ψ est un isomorphisme entre $(H \times K, *)$, c'est-à-dire le produit semi-direct $H \rtimes_{\varphi} K$, et G . Puisque $G = HK$, ψ est surjective. Prouvons que c'est un morphisme de groupes (cela nous permettra de prouver ensuite l'injectivité plus simplement, avec le critère du noyau). Soient (h_1, k_1) et (h_2, k_2) deux éléments de $H \times K$.

$$\begin{aligned}\psi((h_1, k_1) * (h_2, k_2)) &= \psi(h_1 \varphi(k_1)(h_2), k_1 k_2) \\ &= h_1 \varphi(k_1)(h_2) k_1 k_2\end{aligned}$$

Or, $\varphi(k_1)(h_2) = k_1 h_2 k_1^{-1}$ si bien que :

$$\begin{aligned}\psi((h_1, k_1) * (h_2, k_2)) &= h_1 k_1 h_2 k_1^{-1} k_1 k_2 \\ &= h_1 k_1 h_2 k_2 \\ &= \psi(h_1, k_1) \psi(h_2, k_2)\end{aligned}$$

c'est-à-dire que ψ est bien un morphisme de groupes. Prouvons enfin qu'elle est injective. Soit $(h, k) \in \ker(\psi)$. Alors $hk = e$ si bien que $h = k^{-1}$. Or, $h \in H$ et $k^{-1} \in K$ donc h est égal à un élément de K donc il appartient aussi à K . Finalement, $h \in H \cap K = \{e\}$ si bien que $h = e$ et donc $k^{-1} = e$ donc $k = e$. On en déduit que $\ker(\psi) = \{(e, e)\}$ donc ψ est injective donc bijective : c'est un isomorphisme. Les deux groupes sont donc bien isomorphes.

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

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 $\varphi : \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/4\mathbb{Z})$ 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). Soit G un groupe d'ordre 8. L'ordre d'un élément de G divise 8 donc vaut 1, 2, 4 ou 8. Plusieurs cas se présentent :

- Si G contient un élément d'ordre 8, alors G est cyclique et isomorphe à $\mathbb{Z}/8\mathbb{Z}$. On suppose dans la suite que G ne contient aucun élément d'ordre 8.
- Si G contient un élément a d'ordre 4 tel que $G \setminus \text{gr}(a)$ contienne un élément d'ordre 2, alors G est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou un groupe non abélien qu'on note D_8 (et qu'on appelle le groupe diédral) d'après ce qui précède.
- Si G contient un élément a d'ordre 4 tel que $G \setminus \text{gr}(a)$ ne contienne aucun élément d'ordre 2, alors G est isomorphe à \mathbb{H}_8 d'après la botanique.
- Enfin, si G n'a que des éléments d'ordre 2 (hormis le neutre), G est abélien d'après l'exercice 18 et on peut montrer (mais ce n'est pas si simple que ça) que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

En conclusion, il n'existe que 5 groupes à 8 éléments à isomorphisme près : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_8 , \mathbb{H}_8 et $(\mathbb{Z}/2\mathbb{Z})^3$.

Correction :

1. H est d'ordre 4 donc est d'indice 2 dans G (c'est-à-dire que son cardinal est la moitié de celui de G). D'après l'exercice 34, il est distingué dans G . Puisque b est d'ordre 2, alors $K = \{e; b\}$ et $b \notin H$ par hypothèse donc $H \cap K = \{e\}$. Enfin, d'après l'exercice 31, puisque $H \cap K$ est de cardinal 1, alors $\text{card}(HK) = \text{card}(H) \times \text{card}(K) = 8 = \text{card}(G)$ si bien que $G = HK$: les groupes H et K vérifient bien les conditions de l'exercice précédent.

2. C'est du cours (enfin, au programme de deuxième année, pas de pression) : si x est d'ordre n , alors $\text{gr}(x)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
3. D'après l'exercice 69, il y a deux endomorphismes de $\mathbb{Z}/4\mathbb{Z}$: l'identité, et la fonction f définie par : $f(\bar{0}) = \bar{0}$, $f(\bar{1}) = \bar{3}$, $f(\bar{2}) = \bar{2}$ et $f(\bar{3}) = \bar{1}$. Le morphisme $\varphi : \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/4\mathbb{Z})$ étant, justement, un morphisme, il envoie le neutre sur le neutre donc $\varphi(\bar{0}) = \text{Id}_{\mathbb{Z}/4\mathbb{Z}}$ et, ensuite, il y a deux possibilités : soit $\varphi(\bar{1}) = \text{Id}_E$, c'est-à-dire que φ est constante égale à Id_E , soit $\varphi(\bar{1}) = f$, l'autre automorphisme de $\mathbb{Z}/4\mathbb{Z}$. Il y a donc au plus deux groupes G (à isomorphisme près) vérifiant les conditions de l'exercice. Supposons que φ soit constante égale à $\text{Id}_{\mathbb{Z}/4\mathbb{Z}}$. Alors le produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$ est en fait le produit direct (on peut appliquer la question 3 de l'exercice 39 ou le refaire à la main) c'est-à-dire que $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ muni de la loi produit c'est-à-dire que $(h_1, k_1) + (h_2, k_2) = (h_1 + h_2, k_1 + k_2)$ puisque $\varphi(k_1)(h_2) = \text{Id}(h_2) = h_2$ (ici, la loi est notée additivement car on se place sur $\mathbb{Z}/4\mathbb{Z}$). On en déduit la table ci-dessous (rappelons que la première coordonnée est dans $\mathbb{Z}/4\mathbb{Z}$ et la deuxième dans $\mathbb{Z}/2\mathbb{Z}$ donc la première est prise modulo 4 et la deuxième modulo 2) :

+	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{0})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$
$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$
$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$
$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{0})$

Supposons à présent que φ soit l'autre morphisme de $\mathbb{Z}/2\mathbb{Z}$ dans $\text{Aut}(\mathbb{Z}/4\mathbb{Z})$ c'est-à-dire que $\varphi(\bar{0}) = \text{Id}_{\mathbb{Z}/4\mathbb{Z}}$ et $\varphi(\bar{1}) = f$ avec f la fonction vue précédemment. Donnons la table du groupe

$$G = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

muni de la loi (encore une fois, la loi est notée additivement) :

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

Par exemple (rappelons que la première coordonnée est dans $\mathbb{Z}/4\mathbb{Z}$ et la deuxième dans $\mathbb{Z}/2\mathbb{Z}$ donc la première est prise modulo 4 et la deuxième modulo 2) :

$$\begin{aligned}
(\bar{1}, \bar{1}) * (\bar{1}, \bar{1}) &= (\bar{1} + \varphi(\bar{1})(\bar{1}), \bar{1} + \bar{1}) \\
&= (\bar{1} + f(\bar{1}), \bar{0}) \\
&= (\bar{1} + \bar{3}, \bar{0}) \\
&= (\bar{0}, \bar{0})
\end{aligned}$$

et idem pour les autres. D'où la table du groupe ci-dessous. Il y a donc au plus deux groupes : réciproquement, ce sont bien des groupes car on sait que les produits (directs ou semi-directs) sont des groupes, et ils sont non isomorphes car ils n'ont pas la même table (l'un est abélien et pas l'autre). Ouf!

+	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{0})$
$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{0})$
$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{0})$	$(\bar{3}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{2}, \bar{1})$
$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{0})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$

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 ?

Correction : Il suffit de prouver que c'est un sous-anneau de $\mathbb{R}^{[0;1]}$ (rappelons que si X est un ensemble quelconque et A un anneau, alors A^X est muni d'une structure d'anneau). L'ensemble $\mathcal{C}([0; 1], \mathbb{R})$ est non vide (il contient la fonction nulle), stable par somme et par opposé (si f et g sont continues sur $[0; 1]$, alors $f + g$ et $-f$ sont continues sur $[0; 1]$) donc $\mathcal{C}([0; 1], \mathbb{R})$ est un sous-groupe (pour l'addition) de $\mathbb{R}^{[0;1]}$. La fonction constante égale à 1 appartient évidemment à $\mathcal{C}([0; 1], \mathbb{R})$ et cet ensemble est stable par produit : c'est donc un sous-anneau de $\mathbb{R}^{[0;1]}$ et en particulier c'est un anneau. Il n'est pas intègre car, si on note f la fonction nulle sur $[0; 1/2]$ et égale à $x - 1/2$ sur $[1/2; 1]$, et g la fonction constante égale à 0 sur $[1/2; 1]$ et égale à $1/2 - x$ sur $[0; 1/2]$, on a $f \times g = 0$ alors que ni f ni g n'est la fonction nulle : l'anneau n'est pas 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 ?

Correction : Il est non vide (contient la fonction nulle), stable par somme et par opposé donc c'est un sous-groupe de A (muni de la loi $+$). La multiplication est toujours associative et distributive par rapport à la somme. Enfin, la fonction φ constante égale à 1 sur $[0; 1]$ et nulle sur $]1; 2]$ (les fonctions ne sont pas forcément continues dans cet exercice) est un élément neutre sur A_1 : en effet, si $f \in A_1$, alors f est nulle sur $]1; 2]$ donc, pour tout $x \in [0; 2]$, soit $x \in [0; 1]$, et alors $\varphi(x) = 1$ si bien que $f(x) \times \varphi(x) = f(x)$, et si $x \in]1; 2]$, alors $f(x) = 0$ donc $f(x) = f(x) \times \varphi(x)$: φ est neutre à droite donc neutre car le produit est commutatif. A_1 est bien un anneau inclus dans A mais ce n'est pas un sous-anneau puisque le neutre n'est pas le même.

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.

Correction : Montrons que c'est un sous-groupe de \mathbb{Q} (pour la loi $+$). Il est non vide car contient $0 = 0/1$. Soient $r_1 = a_1/b_1$ et $r_2 = a_2/b_2$ (on écrit les rationnels sous forme irréductible) deux éléments de \mathbb{Q}_i : les entiers b_1 et b_2 sont donc impairs. Par conséquent, $-r_1 = -a_1/b_1 \in \mathbb{Q}_i$, et

$$r_1 + r_2 = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

Le dénominateur de cette fraction, lorsqu'on la met sous forme irréductible, est un diviseur de $b_1 b_2$ qui est impair (car produit de deux entiers impairs) donc est lui-même impair (les nombres impairs n'ont que des diviseurs impairs). On en déduit que $r_1 + r_2 \in \mathbb{Q}_i$: \mathbb{Q}_i est stable par somme, c'est donc un sous-groupe de \mathbb{Q} . De plus, $1 = 1/1$ donc $1 \in \mathbb{Q}_i$. Enfin, $r_1 r_2 = a_1 a_2 / b_1 b_2$ qui appartient à \mathbb{Q}_i pour la même raison que ci-dessus (que la fraction soit ou non irréductible) : \mathbb{Q}_i est stable par produit, c'est donc un sous-anneau de \mathbb{Q} , en particulier c'est un anneau. r_1 est inversible si et seulement si r_1 est non nul et $1/r_1 = b_1/a_1 \in \mathbb{Q}_i$ si et seulement si a_1 est impair. En conclusion, les inversibles de \mathbb{Q}_i sont exactement les rationnels qui s'écrivent (sous forme irréductible) comme quotient de deux entiers impairs (par exemple, $1/3$ mais pas $2/3$).

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

$$\forall (a, b) \in \mathbb{R}^2, \begin{cases} a\$b = a + b - k \\ a \top b = ab - k(a + b) + k(k + 1) \end{cases}$$

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

Correction : Voyons si $(\mathbb{R}, \$)$ est un groupe abélien : si oui, on verra si $(\mathbb{R}, \$, \top)$ est un anneau, sinon on s'arrêtera là. Ici, rien n'est évident, on n'a pas des lois usuelles : il faut tout montrer à la main.

- La loi $\$$ est bien une loi interne, et il est immédiat qu'elle est commutative. Vérifions qu'elle est associative. Soit $(a, b, c) \in \mathbb{R}^3$. D'une part :

$$\begin{aligned} a\$(b\$c) &= a\$(b + c - k) \\ &= a + (b + c - k) - k \\ &= a + b + c - 2k \end{aligned}$$

et d'autre part :

$$\begin{aligned} (a\$b)\$c &= (a + b - k)\$c \\ &= (a + b - k) + c - k \\ &= a + b + c - 2k \end{aligned}$$

donc la loi $\$$ est bien associative.

- Il est immédiat que k est neutre pour la loi $\$$ et que, pour tout a , $2k - a$ est le symétrique de a pour la loi $\$$: il y a un neutre et tout élément admet un symétrique, $(\mathbb{R}, \$)$ est bien un groupe abélien.
- Regardons si $(A, \$, \top)$ est un anneau : sinon, on s'arrête là, si oui, on verra ensuite si c'est un corps. Regardons si la loi \top est associative. D'une part :

$$\begin{aligned} a \top (b \top c) &= a \top (bc - k(b + c) + k(k + 1)) \\ &= a(bc - k(b + c) + k(k + 1)) - k(a + bc - k(b + c) + k(k + 1)) + k(k + 1) \\ &= abc - ak(b + c) + ak(k + 1) - ak - kbc + k^2(b + c) - k^2(k + 1) + k(k + 1) \\ &= abc - k(ab + ac + bc) + k^2(a + b + c) - k^3 + k \end{aligned}$$

et d'autre part :

$$\begin{aligned} (a \top b) \top c &= (ab - k(a + b) + k(k + 1)) \top c \\ &= (ab - k(a + b) + k(k + 1))c - k(ab - k(a + b) + k(k + 1) + c) + k(k + 1) \\ &= abc - kc(a + b) + ck(k + 1) - kab + k^2(a + b) - k^2(k + 1) - kc + k(k + 1) \\ &= abc - k(ab + ac + bc) + k^2(a + b + c) - k^3 + k \end{aligned}$$

et donc la loi \top est associative. Regardons si elle est distributive par rapport à la loi $\$$. La loi \top étant évidemment commutative, il suffit d'étudier la distributivité à gauche. D'une part :

$$\begin{aligned} a \top (b\$c) &= a \top (b + c - k) \\ &= a(b + c - k) - k(a + b + c - k) + k(k + 1) \\ &= ab + ac - k(2a + b + c) + 2k^2 + k \end{aligned}$$

et, d'autre part :

$$\begin{aligned} (a \top b)\$(a \top c) &= (ab - k(a + b) + k(k + 1))\$(ac - k(a + c) + k(k + 1)) \\ &= (ab - k(a + b) + k(k + 1)) + (ac - k(a + c) + k(k + 1)) - k \\ &= ab + ac - k(2a + b + c) + 2k^2 + k \end{aligned}$$

et donc \top est distributive par rapport à $\$$. Cherchons si \top admet un élément neutre. Soit $b \in \mathbb{R}$ (la loi est commutative, il suffit de chercher un neutre à gauche) :

$$b \text{ est neutre pour } \top \iff \forall a \in \mathbb{R}, a \top b = ab - k(a+b) + k(k+1) = a$$

$$\iff \forall a \in \mathbb{R}, a(b-k) - kb + k^2 + k = a$$

Posons $b = k+1$. Alors on a bien, pour tout $a \in \mathbb{R}$, $a \top b = a : k+1$ est neutre pour la loi \top . Finalement, $(A, \$, \top)$ est un anneau commutatif.

- Cherchons si c'est un corps. Soit donc $a \neq k$ (le neutre de la première loi). On cherche b tel que $a \top b = k+1$ (idem, la loi est commutative, il suffit de chercher un inverse à droite). Soit $b \in \mathbb{R}$.

$$a \top b = k+1 \iff ab - k(a+b) + k(k+1) = k+1$$

$$\iff ab - ka - kb + k^2 = 1$$

$$\iff b(a-k) = 1 + ka - k^2$$

et puisque $a \neq k$, on en déduit que $\frac{1+ak-k^2}{a-k}$ est l'inverse de a pour la loi \top : $(\mathbb{R}, \$, \top)$ est un corps.

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.

Correction : Rappelons qu'un rationnel r est un décimal si et seulement s'il existe $k \in \mathbb{Z}$ et $n \in \mathbb{N}$ tel que $r = k/10^n$. Pour montrer que \mathbb{D} est un anneau, il suffit de prouver que c'est un sous-anneau de \mathbb{Q} .

- $0 = 0/10^1 \in \mathbb{D}$ donc \mathbb{D} est non vide.
- Soient r_1 et r_2 deux décimaux. Il existe alors $(k_1, k_2) \in \mathbb{Z}^2$ et $(n_1, n_2) \in \mathbb{N}^2$ tel que $r_1 = k_1/10^{n_1}$ et $r_2 = k_2/10^{n_2}$. Sans perte de généralité, supposons $n_1 \geq n_2$. Alors :

$$r_1 + r_2 = \frac{k_1 + k_2 10^{n_1-n_2}}{10^{n_2}} \in \mathbb{D}$$

\mathbb{D} est donc stable par somme. De plus, $-n_1 = -k_1/10^{n_1} \in \mathbb{D}$: \mathbb{D} est stable par opposé, c'est un sous-groupe de \mathbb{Q} (muni de la loi $+$ évidemment).

- $1 = 1/10^0 \in \mathbb{D}$.
- Enfin, $r_1 r_2 = k_1 k_2 / 10^{n_1+n_2} \in \mathbb{D}$: \mathbb{D} est stable par produit, c'est un sous-anneau de \mathbb{Q} , et en particulier c'est un anneau. Ce n'est cependant pas un corps car $3 \in \mathbb{D}$ mais $1/3 \notin \mathbb{D}$. Supposons en effet que $1/3 \in \mathbb{D}$: il existe alors $k \in \mathbb{Z}$ et $n \in \mathbb{N}$ tel que $1/3 = k/10^n$ donc $3k = 10^n$ donc 3 divise 10^n . Or, 3 est premier avec 10 donc avec 10^n , donc c'est absurde : \mathbb{D} n'est donc pas un corps. Idem pour l'ensemble des nombres dyadiques en remplaçant 10 par 2 dans ce qui précède.

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

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

Correction :

1. On sait que la différence symétrique est associative. Elle est de plus commutative (cf. chapitre 3). D'après l'exercice 13 du chapitre 4 (mais essayez de le redémontrer), l'ensemble vide est un élément neutre, et A est son propre symétrique (i.e. $A \Delta A = \emptyset$) : on a bien un groupe abélien.
2. L'intersection est commutative, associative et admet un élément neutre (E tout entier). Pour prouver qu'on a un anneau commutatif, il reste à prouver que l'intersection est distributive par rapport à la différence symétrique (et puisque l'intersection est commutative, il suffit de prouver qu'elle est distributive à gauche). Soient A, B, C trois parties de E . D'une part, en utilisant la distributivité de l'intersection sur l'union :

$$\begin{aligned} A \cap (B \Delta C) &= A \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C)) \\ &= (A \cap (B \cap \overline{C})) \cup (A \cap (\overline{B} \cap C)) \end{aligned}$$

et d'autre part :

$$(A \cap B) \Delta (A \cap C) = (A \cap B \cap (\overline{A \cap C})) \cup ((\overline{A \cap B} \cap A \cap C))$$

Or,

$$\begin{aligned} (A \cap B) \cap (\overline{A \cap C}) &= (A \cap B) \cap (\overline{A} \cup \overline{C}) \\ &= (A \cap B \cap \overline{A}) \cup (A \cap B \cap \overline{C}) \\ &= \emptyset \cup (A \cap B \cap \overline{C}) \\ &= (A \cap B \cap \overline{C}) \end{aligned}$$

et on trouve de même que $(\overline{A \cap B} \cap A \cap C) = A \cap \overline{B} \cap C$: l'intersection est distributive par rapport à la différence symétrique, on a bien un anneau commutatif.

- Non car le neutre des deux lois sont les mêmes : à chaque fois, l'ensemble vide.
- Non car il n'y a pas le même neutre pour la deuxième loi : E n'est pas un élément de $\mathcal{P}(F)$ (sauf si $E = F$ mais alors là il n'y a plus de question).
- Si E est fini, oui car alors $\mathcal{P}(E) = \mathcal{P}_f(E)$, mais ce n'est plus le cas si E est infini car il n'y a pas de neutre pour l'intersection (puisque E n'appartient pas à l'ensemble).

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

- Quels sont les diviseurs de 0, les éléments inversibles de \mathbb{Z}^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.
- Déterminer les sous-anneaux de \mathbb{Z}^2 .

Correction :

- D'après l'exercice 61 (mais on peut le reprouver à la main), les inversibles de \mathbb{Z}^2 sont exactement les quatre éléments $(\pm 1, \pm 1)$. Les diviseurs de zéro sont exactement les couples avec exactement une coordonnée nulle. En effet, si $a \neq 0$, $(a, 0) \times (0, 1) = (0, 0)$ et idem pour $(0, a)$: les éléments avec une seule coordonnée nulle sont des diviseurs de 0, et si (a, b) n'a aucune coordonnée nulle, si $(a, b) \times (x, y) = (ax, by) = (0, 0)$ donc $x = y = 0$: (a, b) n'est pas un diviseur de zéro.
- Analyse : soit φ un tel morphisme. Alors $f(1, 1) = 1$. Suivons l'indication de l'énoncé et étudions $f(e_1)$ et $f(e_2)$. Puisque $f(e_1 + e_2) = 1$, alors $f(e_1) + f(e_2) = 1$ donc $f(e_2) = 1 - f(e_1)$. Notons $n = f(e_1)$ si bien que $f(e_2) = 1 - n$. De même que d'habitude, pour tout $k \in \mathbb{Z}$, $f(ke_1) = kf(e_1) = kn$ et $f(ke_2) = kf(e_2) = k - kn$. Finalement, pour tout $(x, y) \in \mathbb{Z}^2$:

$$\begin{aligned} f(x, y) &= f(xe_1 + ye_2) \\ &= xn + y(1 - n) \\ &= n(x - y) + y \end{aligned}$$

Enfin, $f(e_1 \times e_2) = f(0, 0)$ (on fait le produit coordonnée par coordonnée) donc $f(e_1) \times f(e_2) = n(1 - n) = 0$: on en déduit que $n = 0$ ou $n = 1$, c'est-à-dire que $f(x, y) = y$ (cas où $n = 0$) ou $f(x, y) = x$ (cas où $n = 1$). Réciproquement, on montre facilement que ces deux fonctions sont bien des morphismes d'anneaux, ce sont donc les seuls : les seuls morphismes de \mathbb{Z}^2 dans \mathbb{Z} sont les morphismes coordonnées.

- Soit A un sous-anneau de \mathbb{Z}^2 . Alors $(1, 1) \in A$ donc, pour tout $n \in \mathbb{Z}$, $(n, n) \in A$. S'il n'y a aucun élément $(x, y) \in A$ tel que $x \neq y$, alors $A = \{(n, n) \mid n \in \mathbb{Z}\}$, et réciproquement, cet ensemble est bien un sous-anneau de \mathbb{Z}^2 . Supposons à présent qu'il existe $(x, y) \in A$ avec $x \neq y$. Alors $(-x, -y) \in A$ puisque A est un sous-groupe de \mathbb{Z}^2 : il existe dans tous les cas un élément (a, b) avec $a > b$, et en faisant la différence avec (b, b) , il vient $(a - b, 0) \in A$. Notons $n = \min\{a > 0 \mid (a, 0) \in A\}$. Montrons que A est l'ensemble des couples $(n + ak, n)$ avec n et k dans \mathbb{Z} . Soit $(x, y) \in A$. Si $x = y$ alors (x, y) est de la bonne forme avec $n = x = y$ et $k = 0$. Sinon, $(x, y) - (y, y) = (x - y, 0) \in A$. Effectuons la division euclidienne de $x - y$ par a : il existe $k \in \mathbb{Z}$ et $r \in \llbracket 0; a - 1 \rrbracket$ tels que $x - y = ak + r$ donc

$$(x - y, 0) - k(a, 0) = (r, 0) \in A$$

donc $r = 0$ par choix de a si bien que a divise $x - y = ka$ donc $(x, y) = (y + ka, y)$. Réciproquement, pour tout $a \in \mathbb{N}^*$, $A = \{(n + ak, n) \mid (n, k) \in \mathbb{Z}^2\}$ est un sous-anneau de \mathbb{Z}^2 (exo).

18.3.2 Anneaux ou corps obtenus par adjonction d'un élément

Exercice 49 : ★★

1. Montrer que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{Z}^2\}$ est un anneau intègre.
2. On définit sur $\mathbb{Z}[\sqrt{2}]$ 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 $\mathbb{Z}[\sqrt{2}]$ 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.

Correction :

1. Montrons que c'est un sous-anneau de \mathbb{R} .
 - $0 = 0 + \sqrt{2} \times 0$ donc $0 \in \mathbb{Z}[\sqrt{2}] : \mathbb{Z}[\sqrt{2}]$ est non vide.
 - Soient x_1 et x_2 deux éléments de $\mathbb{Z}[\sqrt{2}]$. Alors il existe a_1, b_1, a_2, b_2 dans \mathbb{Z} tels que $x_1 = a_1 + b_1\sqrt{2}$ et $x_2 = a_2 + b_2\sqrt{2}$ si bien que $x_1 + x_2 = a_1 + a_2 + \sqrt{2}(b_1 + b_2)$. Or, $a_1 + a_2$ et $b_1 + b_2$ sont des éléments de \mathbb{Z} donc $x_1 + x_2 \in \mathbb{Z}[\sqrt{2}] : \mathbb{Z}[\sqrt{2}]$ est stable par somme.
 - De plus, $-x_1 = -a - b\sqrt{2}$ et puisque $-a$ et $-b$ appartiennent à \mathbb{Z} , $-x_1 \in \mathbb{Z}[\sqrt{2}] : \mathbb{Z}[\sqrt{2}]$ est un sous-groupe de \mathbb{R} .
 - $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
 - Enfin, $x_1x_2 = (a_1a_2 + 2b_1b_2) + \sqrt{2}(a_1b_2 + a_2b_1) \in \mathbb{Z}[\sqrt{2}] : \mathbb{Z}[\sqrt{2}]$ est stable par produit, c'est donc un sous-anneau de \mathbb{R} , et en particulier c'est un anneau. Il est intègre puisqu'il est inclus dans \mathbb{R} qui est intègre.
2. Avec les mêmes notations que ci-dessus :

$$\begin{aligned} N(x_1x_2) &= (a_1a_2 + 2b_1b_2)^2 - 2(a_1b_2 + a_2b_1)^2 \\ &= a_1^2a_2^2 + 4b_1^2b_2^2 + 4a_1a_2b_1b_2 - 2a_1^2b_2^2 - 2a_2^2b_1^2 - 4a_1a_2b_1b_2 \\ &= a_1^2a_2^2 + 4b_1^2b_2^2 - 2a_1^2b_2^2 - 2a_2^2b_1^2 \end{aligned}$$

et :

$$\begin{aligned} N(x_1)N(x_2) &= (a_1^2 - 2b_1^2)(a_2^2 - 2b_2^2) \\ &= a_1^2a_2^2 + 4b_1^2b_2^2 - 2a_1^2b_2^2 - 2a_2^2b_1^2 \end{aligned}$$

N est bien multiplicative.

3. Supposons que $x = a + b\sqrt{2}$ soit inversible et notons son inverse $x' + y'\sqrt{2}$. Alors $N(xy) = N(1) = 1$ donc $N(x)N(y) = 1$. Or, $N(x) \in \mathbb{Z}$ donc $N(x) = a^2 - 2b^2 = \pm 1$. Réciproquement, supposons que $N(x) = \pm 1$. Notons $y = a - b\sqrt{2}$. Alors $xy = a^2 - 2b^2 = \pm 1$. Si $xy = 1$ alors y est un inverse de x , sinon $-y$ est un inverse de x . Dans tous les cas, x est inversible. D'où l'équivalence.

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 $\mathbb{Q}[\sqrt{2}]$.

Correction :

1. Découle de l'exercice 26 : les morphismes de groupes de \mathbb{Q} dans lui-même sont exactement les fonctions de la forme $r \mapsto ar$ avec $a \in \mathbb{Q}$. Puisqu'un morphisme de corps vérifie $f(1) = 1$, la seule possibilité est d'avoir $a = 1$ donc que le morphisme soit l'identité.
2. Analyse : soit f un automorphisme de corps de $\mathbb{Q}[\sqrt{2}]$. Alors, de même que dans l'exercice 26, puisque $f(1) = 1$, alors $f(r) = r$ pour tout rationnel. Puisque f est un morphisme d'anneaux, $f(\sqrt{2}^2) = f(\sqrt{2})^2$, et puisque $f(2) = 2$, il vient : $f(\sqrt{2}) = \pm\sqrt{2}$. Puisque f est un morphisme d'anneau et que pour tout rationnel, $f(r) = r$, on trouve :

$$\forall (a, b) \in \mathbb{Q}^2, f(a + b\sqrt{2}) = a \pm \sqrt{2}$$

On en déduit que, si $f(\sqrt{2}) = \sqrt{2}$, f est l'identité de $\mathbb{Q}[\sqrt{2}]$, et si $f(\sqrt{2}) = -\sqrt{2}$, alors f est « la conjugaison sur $\mathbb{Q}[\sqrt{2}]$ », c'est-à-dire que, pour tous a et b dans \mathbb{Q} , $f(a + b\sqrt{2}) = a - b\sqrt{2}$. Synthèse : il est immédiat que ce sont des automorphismes de corps.

Exercice 51 : ★

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

Correction :

1. On montre que c'est un corps de la même façon que dans le cours, où l'on a montré que $\mathbb{Q}[\sqrt{2}]$ est un corps. Cependant, B n'est pas un corps car ce n'est pas un anneau puisqu'il n'est pas stable par produit : en effet, $\sqrt{2} \times \sqrt{3} = \sqrt{6} \notin B$.
2. Supposons qu'il existe un isomorphisme d'anneaux (et donc de corps) noté f entre A et $\mathbb{Q}[\sqrt{2}]$. De même que précédemment, $f(r) = r$ pour tout rationnel r . De même que dans l'exercice précédent, $f(\sqrt{3}) = \pm\sqrt{3}$ ce qui est absurde puisque $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

Exercice 52 : ★★

1. Montrer que $\mathbb{Q}[i] = \{a + ib \mid (a, b) \in \mathbb{Q}^2\}$ 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 $\mathbb{Q}[i]$.

Correction :

1. Analogie aux exemples $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[\sqrt{3}]$.
2. Montrons que $\mathbb{Q}[j]$ est un sous-corps de \mathbb{C} . Le fait que ce soit un sous-groupe est immédiat. De plus, $1 = 1 + 0 \times j \in \mathbb{Q}[j]$. Soient $x_1 = a_1 + b_1j$ et $x_2 = a_2 + b_2j$ deux éléments de $\mathbb{Q}[j]$ (avec a_1, a_2, b_1, b_2 rationnels, donc). On a :

$$x_1x_2 = a_1a_2 + b_1b_2j^2 + j(a_1b_2 + a_2b_1)$$

Puisque $1 + j + j^2 = 0$, $j^2 = -1 - j$ et donc :

$$x_1x_2 = a_1a_2 - b_1b_2 + j(a_1b_2 + a_2b_1 - b_1b_2) \in \mathbb{Q}[j]$$

$\mathbb{Q}[j]$ est stable par produit : c'est un sous-anneau de \mathbb{C} . Enfin, si $a + bj \neq 0$:

$$\begin{aligned} \frac{1}{a + bj} &= \frac{1}{a - b/2 + bi\sqrt{3}/2} \\ &= \frac{a - b/2 - i\sqrt{3}/2}{(a - b/2) + b^2 \times 3/4} \\ &= \frac{a}{(a - b/2) + b^2 \times 3/4} + \frac{b}{(a - b/2) + b^2 \times 3/4} \times (-1/2 - i\sqrt{3}/2) \\ &= \frac{a}{(a - b/2) + b^2 \times 3/4} + \frac{b}{(a - b/2) + b^2 \times 3/4} \times j^2 \end{aligned}$$

Or, $1 + j + j^2 = 0$ donc $j^2 = -1 - j$ ce qui permet de conclure comme ci-dessus en regroupant les termes : $1/(a + bj) \in \mathbb{Q}[j]$, $\mathbb{Q}[j]$ est un corps. On trouve de même que précédemment que si $\varphi : \mathbb{Q}[i] \rightarrow \mathbb{Q}[j]$ est un isomorphisme, alors $\varphi(r) = r$ pour tout rationnel, et donc $\varphi(i^2) = -1 = \varphi(i)^2$ donc $\varphi(i) = \pm i$ ce qui est absurde puisque $\pm i \notin \mathbb{Q}[j]$: en effet, si $i \in \mathbb{Q}[j]$, il existe a et b rationnels tels que $i = a + bj$ donc

$$i = a - \frac{b}{2} + bi\frac{\sqrt{3}}{2}$$

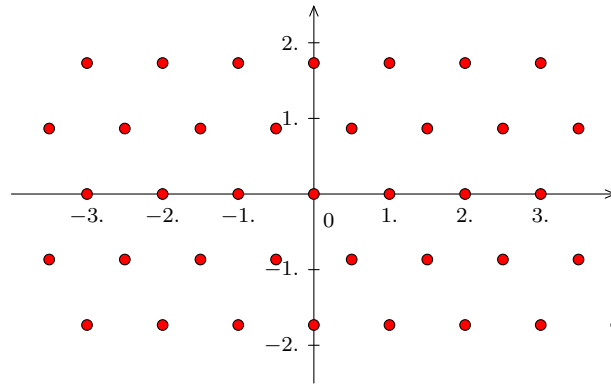
Si $b \neq 0$, par unicité des parties imaginaires, $\sqrt{3} = 2/b \in \mathbb{Q}$ ce qui est absurde.

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 $\mathbb{Z}[j]$.

Correction :

1. Analogie à ce qui précède. On a représenté $\mathbb{Z}[j]$ ci-dessus, de même qu'on a représenté $\mathbb{Z}[i]$ en cours : $\mathbb{Z}[j]$ est formé des points obtenus en mettant côte à côte des triangles équilatéraux de côté 1.



2. Tout d'abord, si $u \in \mathbb{Z}[j]$, il existe a et b entiers tels que $u = a + jb = a - b/2 + ib\sqrt{3}/2$. Par conséquent :

$$\begin{aligned} |u|^2 &= (a - b/2)^2 + 3b^2/4 \\ &= a^2 - ab + b^2/4 + 3b^2/4 \\ &= a^2 - ab + b^2 \end{aligned}$$

Si u est inversible, notons v son inverse. Alors $uv = 1$ donc $u^2v^2 = 1$ si bien que $|u|^2 \times |v|^2 = 1$. Or, on déduit de ce qui précède que $|u|^2$ et $|v|^2$ sont des entiers (et ils sont positifs par propriété d'un carré réel) donc $|u|^2 = 1$ si bien que $|u| = 1$. Réciproquement, supposons que $|u| = 1$. Alors, en mettant au carré, on trouve : $|u|^2 = a^2 - ab + b^2 = 1$. Posons

$$\begin{aligned} v &= \bar{u} \\ &= a - b/2 - ib\sqrt{3} \\ &= a + bj^2 \\ &= a + b(-1 - j) \\ &= (a - b) - bj \in \mathbb{Z}[j] \end{aligned}$$

et $uv = |u|^2 = 1$: u est bien inversible, d'où l'équivalence.

3. On cherche donc les couples d'entiers (a, b) tels que $a^2 - ab + b^2 = 1$. Soit $(a, b) \in \mathbb{Z}^2$.

$$a^2 - ab + b^2 = 1 \iff (a - b)^2 = 1 - ab \quad \text{et} \quad a^2 + b^2 = 1 + ab$$

Par conséquent, si (analyse synthèse) le couple (a, b) convient, alors $1 \pm ab \geq 0$ donc $1 \geq \pm ab$ i.e. $1 \geq |ab|$: il en découle que $ab = \pm 1$ ou 0 . De plus, puisque $ab \leq 1$, alors $a^2 + b^2 \leq 2$ donc $|a|$ et $|b|$ sont inférieurs ou égaux à 1 (sinon a^2 ou $b^2 \geq 4$). On a donc les couples suivants : $(-1, 1), (1, -1), (1, 1), (-1, -1), (\pm 1, 0)$ et $(0, \pm 1)$. En conclusion, les inversibles éventuels (rappelons qu'on est dans la phase analyse) sont :

$$\pm 1, \pm j, -1 + j, 1 - j, 1 + j, -1 - j$$

Synthèse : $j - 1$ et $1 - j$ ne sont pas de norme 1 donc ne sont pas des inversibles. Finalement, les inversibles de $\mathbb{Z}[j]$ sont $\pm 1, \pm j, 1 + j = -j^2$ et $-1 - j = j^2$.

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 ?

Correction : Si I est un singleton, alors K^I et K sont isomorphes (exo) donc K^I est un corps. Supposons K^I n'est pas muni d'une structure de corps car si f est une fonction qui s'annule mais qui n'est pas la fonction nulle, il n'y a aucune fonction g telle que $f \times g$ soit la fonction constante égale à 1. Il n'est pas non plus muni d'une structure d'anneau intègre puisque si f s'annule mais n'est pas la fonction nulle, en prenant g qui s'annule là où f ne s'annule pas, et réciproquement,

on a $f \times g = 0$ mais f et g non nulles : on n'a pas un anneau intègre.

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

Correction : Supposons que E ne soit pas un singleton sinon l'exercice n'a pas beaucoup d'intérêt. Montrons que les diviseurs de 0 sont les fonctions qui s'annulent (sauf la fonction nulle), et les inversibles les fonctions qui ne prennent que les valeurs ± 1 . Soit f une fonction qui s'annule mais différente de la fonction nulle. On note g la fonction qui est nulle là où f ne s'annule pas et qui vaut 1 là où f s'annule, si bien que $f \times g = 0$: f est un diviseur de 0. Réciproquement, si f ne s'annule pas, la seule façon d'avoir $f \times g = 0$ est que g soit la fonction nulle.

Soit f une fonction ne prenant que les valeurs ± 1 . Alors $f \times f$ est la fonction constante égale à 1 donc f est inversible et est sa propre inverse. Si f s'annule, alors f est un diviseur de 0 (ou la fonction nulle) donc n'est pas inversible. Sinon, supposons qu'il existe n tel que $|f(n)| \geq 2$: alors il n'existe pas de fonction g telle que $f(n)g(n) = 1$: f n'est pas inversible.

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

Correction : En d'autres termes, montrons qu'une fonction est inversible (pour le produit) si et seulement si elle ne prend que des valeurs inversibles (de A). Soit $f \in U(A^I)$. Alors il existe $g \in A^I$ telle que $f \times g = 1$ i.e. la fonction constante égale à 1 (le neutre du produit de A i.e. 1_A). En d'autres termes, pour tout $x \in A$, $f(x)g(x) = 1$ donc $f(x) \in U_A : f \in U(A)^I$. Réciproquement, soit $f \in U(A)^I$ i.e. pour tout x , $f(x) \in U(A)$. Soit g définie sur I par : $\forall x, g(x) = f(x)^{-1}$. Alors, pour tout x , $f(x) \times g(x) = 1$ donc $f \in U(A^I)$.

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

- Vérifier que S_t est un sous-anneau de $\mathbb{Z}^{\mathbb{N}}$.
- On souhaite déterminer tous les morphismes d'anneaux de S_t dans \mathbb{Z} .
 - 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} .
 - 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

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

Correction :

- La suite nulle est stationnaire donc S_t est non vide. Soient (u_n) et (v_n) deux suites stationnaires, respectivement à partir d'un rang n_0 et à partir d'un rang n_1 . Alors $(u_n) + (v_n)$ est stationnaire à partir du rang $\max(n_0, n_1)$, donc $(u_n) + (v_n) \in S_t$, S_t est stable par somme, et $-(u_n)$ est aussi stationnaire à partir du rang n_0 donc $-(u_n) \in S_t$, S_t est stable par opposé donc S_t est un sous-groupe de $\mathbb{Z}^{\mathbb{N}}$. La suite constante égale à 1 est stationnaire donc appartient à S_t . Enfin, $(u_n) \times (v_n)$ est stationnaire à partir du rang $\max(n_0, n_1)$, S_t est stable par produit : c'est un sous-anneau de $\mathbb{Z}^{\mathbb{N}}$.
- Immédiat : pour toutes suites u et v , $v_i(u + v) = (u + v)_i = u_i + v_i = v_i(u) + v_i(v)$, idem pour le produit, et si u est la suite constante égale à 1, alors $v_i(u) = 1$.
 - v_∞ est bien définie puisqu'une suite stationnaire converge. Puisque la limite d'une somme est la somme des limites (toutes les suites considérées convergent), que la limite d'un produit est le produit des limites, et que la limite de la suite constante égale à 1 vaut 1, alors v_∞ est un morphisme d'anneaux.
 - Supposons qu'il existe $i \neq j$ tels que $\varphi(e_i)$ et $\varphi(e_j)$ soient non nuls. Alors $\varphi(e_i \times e_j) = \varphi(e_i) \times \varphi(e_j) \neq 0$ mais $e_i \times e_j$ est la suite nulle donc $\varphi(e_i \times e_j) = 0$ ce qui est absurde.
 - si $i \neq i_0$, alors $v_{i_0}(e_i) = 0$ et, d'après ce qui précède, $\varphi(e_i) = 0$ puisque $\varphi(e_{i_0}) \neq 0$ et que φ est non nulle en au plus une suite e_i . De plus, $\varphi(\tilde{1}) = v_{i_0}(\tilde{1}) = 1$, d'où la deuxième égalité voulue. Soit u une suite stationnaire égale à L à partir du rang n_0 . Alors

$$u = L \times \tilde{1} + (u_0 - L)e_0 + (u_1 - L)e_1 + \cdots + (u_{n_0-1} - L)e_{n_0-1}$$

φ et les v_i étant des morphismes d'anneaux, on a :

$$(\varphi - e_i)(u) = L \times (\varphi - e_i)(\tilde{1}) + (u_0 - L)(\varphi - e_i)(e_0) + (u_1 - L)(\varphi - e_i)(e_1) + \cdots + (u_{n_0-1} - L)(\varphi - e_i)(e_{n_0-1})$$

En effet, si $k \in \mathbb{Z}$ et v est une suite, $(\varphi - e_i)(kv) = k(\varphi - e_i)(v)$: on fait comme d'habitude, les entiers positifs puis les entiers négatifs. Finalement, $(\varphi - e_i)(u) = 0$ donc $\varphi = e_i$ puisque c'est vrai pour toute suite stationnaire u .

(e) De même, $(\varphi - v_i \infty)(e_i) = 0$ pour tout i et $(\varphi - v_\infty)(\tilde{1}) = 0$ et on conclut de la même façon.

18.3.4 Anneaux et corps génériques

Exercice 58 : \star Soient A_1 et A_2 deux anneaux et $f : A_1 \rightarrow A_2$ 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 .

Correction : Un morphisme d'anneaux envoie 1_{A_1} sur $1_{A_2} \neq 0_{A_2}$ puisque A_2 a au moins deux éléments. Dès lors, 1_{A_1} n'appartient pas à $\ker(f)$ donc $\ker(f)$ n'est pas un sous-anneau de A_1 .

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

Correction : Nous n'avons pas défini le centre d'un anneau, mais cela n'est pas très difficile de deviner la définition : c'est l'ensemble des éléments de A qui commutent avec tout le monde (au sens de la multiplication : A est un groupe abélien muni de la loi \times) i.e. $Z(A) = \{a \in A \mid \forall b \in A, ab = ba\}$.

- Pour tout $b \in A, 0 \times b = b \times 0 = 0$ donc $0 \in Z(A)$: $Z(A)$ est non vide.
- Soient a_1 et a_2 deux éléments de $Z(A)$. Soit $b \in A$. Par distributivité du produit sur la somme, $(a_1 + a_2)b = a_1b + a_2b$. Or, a_1 et a_2 sont dans $Z(A)$ donc $a_1b = ba_1$ et idem pour l'autre, si bien que $(a_1 + a_2)b = ba_1 + ba_2$, et encore par distributivité, on obtient $(a_1 + a_2)b = b(a_1 + a_2)$: $a_1 + a_2 \in Z(A)$, $Z(A)$ est stable par somme.
- $a_1b - a_1b = 0$ donc $ba_1 - a_1b = 0$ si bien que $-a_1b = -ba_1$: $-a_1 \in Z(A)$, $Z(A)$ est stable par passage à l'opposé : c'est un sous-groupe de A .
- $1 \in Z(A)$ car le neutre commute avec tout le monde.
- Enfin, soit $b \in A$. Puisque a_1 et a_2 appartiennent à $Z(A)$, on a successivement (par associativité du produit) : $a_1a_2b = a_1ba_2 = ba_1a_2$ donc $a_1a_2 \in Z(A)$, $Z(A)$ est stable par produit donc c'est un sous-anneau de A .

Exercice 60 : \star 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.

Correction : Il existe $n \geq 1$ tel que $(ab)^n = 0$. Attention, a et b ne commutent pas forcément donc on n'a pas forcément $(ab)^n = a^n b^n$. On a :

$$(ab)^n = (ab)(ab)(ab)(ab) \cdots (ab) = 0$$

avec ab multiplié par lui-même n fois. En multipliant par b à gauche et par a à droite, on a encore 0 puisque 0 est absorbant, si bien que (toujours par associativité du produit) :

$$b(ab)(ab)(ab)(ab) \cdots (ab)a = (ba) \times \cdots \times (ba) = 0$$

avec ba multiplié par lui-même $n + 1$ fois : en d'autres termes, $(ba)^{n+1} = 0$, ba est encore nilpotent.

Exercice 61 - Anneau produit : \star 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 .

Correction : On sait déjà (cf. cours) que $A_1 \times A_2$ est muni d'une structure de groupe abélien avec la loi produit : $(a_1, a_2) + (b_1, b_2) = (a_1 +_1 b_1, a_2 +_2 b_2)$. On définit de même une loi \times produit : $(a_1, a_2) \times (b_1, b_2) = (a_1 \times_1 b_1, a_2 \times_2 b_2)$. Alors $(A, +, \times)$ est bien un anneau commutatif de neutre pour la loi \times : $(1_{A_1}, 1_{A_2})$ (exo). Prouvons que les inversibles de A sont exactement les couples de la forme (u_1, u_2) avec u_1 inversible de A_1 et u_2 inversible de A_2 . Un élément de cette forme est bien inversible, d'inverse (u_1^{-1}, u_2^{-1}) , et si un élément (x, y) de A a une coordonnée non inversible, disons x , on ne peut pas le multiplier par un autre couple (z, t) tel que $(x, y) \times (z, t) = (1, 1)$ puisqu'il n'existe aucun z tel que $xz = 1$.

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

1. On pose $Z(A) = \{x \in A \mid \forall y \in A, xy = yx\}$ (Z est donc le centre de A) et $Y(A) = \{x \in A \mid \forall y \in A, xy = -yx\}$. 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.

Correction :

1. Pour $Z(A)$: cf. exercice 59. Pour $Y(A)$: idem.
2. Supposons que $A \neq Z(A) \cup Y(A)$: il existe $a \in A$ tel que $a \notin Z(A) \cup Y(A)$: $a \notin Z(A)$ donc il existe y tel que $ay \neq ya$, et $a \notin Y(A)$ donc il existe $z \in A$ tel que $az \neq -za$. Dès lors, par hypothèse sur A , on a forcément $ay = -ya$ et $az = za$ donc $ay + az = za - ya$ donc $a(y+z) = (z-y)a$. Or, toujours par hypothèse sur A , $a(y+z) = (y+z)a$ ou $a(y+z) = -(y+z)a$. Dans le premier cas, $(z-y)a = (y+z)a$ donc $za - ya = ya + za$ si bien que $ya = -ya = ay$ ce qui est exclu. Dans le second cas, $(z-y)a = -(y+z)a$ donc $za - ya = -ya - za$ donc $za = -za = -az$ ce qui est aussi exclu. On en déduit que $A = Z(A) \cup Y(A)$.
3. On a une union de sous-groupes de A qui est un sous-groupe de A (A lui-même) : d'après le cours, l'un est inclus dans l'autre donc soit $A = Z(A)$, et alors A est commutatif, soit $A = Y(A)$. Mais alors, tout élément de A est dans $Y(A)$ c'est-à-dire que pour tous x et y , $xy = -yx$ donc, en particulier, pour tout $a \in A$, $a \times 1 = -1 \times a$ donc $a = -a$ donc tout élément est égal à son opposé. En particulier, pour tous x et y , puisque $xy = -yx$, alors $xy = yx$ (tout élément est égal à son opposé) : l'anneau est tout de même 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 \preceq sur A par : $x \preceq y \iff xy = x$. Montrer que \preceq est une relation d'ordre.

Correction :

1. $\mathbb{Z}/2\mathbb{Z}$ est un anneau de Boole non réduit à un élément.
2. On se place dans un anneau de Boole noté A . Soit $x \in A$. Alors $(x+1)^2 = x^2 + 2x + 1 = x + 2x + 1$ (x et 1 commutent) mais $(x+1)^2 = x+1$ donc $2x = 0$ si bien que $x+x=0$ donc $x = -x$.
3. Soient x et y deux éléments de A , un anneau de Boole. Alors $(x+y)^2 = x+y$ mais on a aussi $(x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$ donc $xy + yx = 0$: on trouve que $xy = -yx$ donc, d'après la question précédente, $xy = yx$, l'anneau est commutatif.
4. On se place dans A un anneau intègre. Soit $x \neq 0$. Alors $x^2 = x$ donc $x(x-1) = 0$ et comme l'anneau est intègre, $x-1 = 0$: A n'a donc que deux éléments, et donc A est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
5.
 - Soit $x \in A$. $x^2 = x$ donc $x \preceq x$: \preceq est réflexive.
 - Soient x et y deux éléments de A tels que $x \preceq y$ et $y \preceq x$ donc $yx = x$ et $xy = y$. Dès lors, l'anneau étant commutatif d'après la question 3, $xy = yx$ donc $x = y$: \preceq est antisymétrique.
 - Soient x, y, z trois éléments de A tels que $x \preceq y$ et $y \preceq z$: on en déduit que $yx = x$ et $zy = y$ si bien que $zx = z(yx) = (zy)x = yx = x$: $x \preceq z$, \preceq est transitive, c'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. :

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

1. Donner les idéaux de \mathbb{Z} .
2. Soit $f : A_1 \rightarrow A_2$ 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 $xA = \{xa \mid a \in A\}$.
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 :

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

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

Correction :

1. Un idéal de \mathbb{Z} étant en particulier un sous-groupe de \mathbb{Z} , les seuls idéaux éventuels de \mathbb{Z} sont les $n\mathbb{Z}$, et il est immédiat que ces ensembles sont absorbants : si $n \in \mathbb{Z}$:

$$\forall a \in \mathbb{Z}, \forall i \in n\mathbb{Z}, a \times i \in n\mathbb{Z} \quad \text{et} \quad i \times a \in n\mathbb{Z}$$

2. On sait que $\ker(f)$ est un sous-groupe de A . Montrons qu'il est absorbant. Soit $(a, i) \in A \times \ker(f)$. f étant un morphisme d'anneaux, $f(a \times i) = f(a) \times f(i)$ et puisque $i \in \ker(f)$, $f(i) = 0$ et on sait que 0 est absorbant donc $f(a \times i) = f(a) \times 0 = 0$ donc $a \times i \in \ker(f)$, et idem pour $i \times a$: $\ker(f)$ est un idéal de A .
3. Si $I = A$ alors I contient un élément inversible (le neutre pour le produit, 1). Réciproquement, supposons que I contienne un élément inversible i . Soit $a \in A$. Alors

$$a = (a \times i^{-1}) \times i \in I$$

car I est absorbant : on en déduit que $A \subset I$, et puisque $I \subset A$ par définition, on a l'égalité $A = I$ voulue.

4. Rappelons que, dans un corps, tout élément non nul est inversible. Ainsi, d'après la question précédente, si un idéal contient un élément non nul, il contient un élément inversible donc est égal à K tout entier. Les seuls idéaux sont donc $\{0\}$ et K . Or, si f est un morphisme de corps, $\ker(f)$ est un idéal distinct de K (puisque $f(1) = 1$, $1 \notin \ker(f)$) donc $\ker(f) = \{0\}$: f est injectif.
5. Soit $x \in A$ non nul. Montrons que x est inversible. Montrons que xA est un idéal de A . $0 = x0$ donc $0 \in xA$: xA est non vide. Soient u et v deux éléments de xA : il existe a et b dans A tels que $u = xa$ et $v = xb$ donc $u + v = x(a + b) \in xA$ et $-u = x(-a) \in xA$: xA est un sous-groupe de A . De plus, pour tout $i \in xA$, il existe $a \in A$ tel que $i = xa$ et pour tout $b \in A$, $bi = x(ab) \in xA$ (l'anneau est commutatif) et $ib = x(ab) \in xA$: xA est absorbant, c'est un idéal. Or, il contient x puisque $x = x \times 1$ donc il contient un élément non nul donc $xA = A$: en particulier, il existe $a \in A$ tel que $xa = 1$: x est inversible, tout élément non nul est inversible, A est un corps.
6. $I = \{0\}$ est un idéal de A donc vérifie la condition de l'énoncé, à savoir : $xy = 0 \Rightarrow x = 0$ ou $y = 0$, l'anneau est intègre. Soit $x \in A$. De même que ci-dessus, x^2A est un idéal de A . Alors $x^3 = x^2 \times x \in x^2A$. Par hypothèse, $x^2 \in x^2A$ ou $x \in x^2A$. Si $x \in x^2A$, c'est bon, sinon $x^2 = x \times x \in x^2A$ donc $x \in x^2A$ ou $x \in x^2A$: dans tous les cas, on a le résultat voulu : il existe $a \in A$ tel que $x = x^2a$ si bien que $x - x^2a = 0$ donc $x(1 - xa) = 0$: si x est non nul, $xa = 1$: x est inversible, A est un corps.
7. I est un idéal donc un sous-groupe de A donc contient 0. En particulier, $0^1 \in I$ donc $0 \in \sqrt{I}$, \sqrt{I} est non vide. Soient x et y deux éléments de \sqrt{I} : il existe n et k tels que x^n et $y^k \in I$. Alors (on peut appliquer le binôme de Newton puisque l'anneau est commutatif) :

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

Si $i \geq k$, $y^{n+k-i} x^i = y^{n+k-i} x^{i-k} x^k \in I$ puisque $x^k \in I$ et I est absorbant. De même, si $i \leq k$, $y^{n+k-i} x^i = x^i y^{k-i} y^n \in I$ pour les mêmes raisons : tous les termes de la somme appartiennent à I donc la somme aussi puisque I est un sous-groupe. On en déduit que $(x + y)^{n+k} \in I$ donc $x + y \in \sqrt{I}$: \sqrt{I} est stable par somme. Enfin $(-x)^k = (-1)^k x^k$ (car l'anneau est commutatif) donc $(-x)^k \in I$ car I absorbant donc $-x \in \sqrt{I}$: \sqrt{I} est un sous-groupe de A . Enfin, il est absorbant : en effet, si $a \in A$, alors (l'anneau est commutatif)

$$(ax)^k = a^k x^k \in I$$

puisque I est absorbant : $ax \in \sqrt{I}$, et l'anneau est commutatif donc $xa \in \sqrt{I}$: \sqrt{I} est absorbant, c'est un idéal. Pour $\sqrt{12\mathbb{Z}}$, on cherche les entiers n dont il existe une puissance divisible par 12. Montrons que $\sqrt{12\mathbb{Z}} = 6\mathbb{Z}$: si $x \in 6\mathbb{Z}$ alors x^2 est divisible par 36 donc par 12 donc $x^2 \in 12\mathbb{Z}$ si bien que $x \in \sqrt{12\mathbb{Z}}$. Réciproquement, si $x \in \sqrt{12\mathbb{Z}}$, alors il existe n tel que x^n soit divisible par 12 donc en particulier x^n est pair et divisible par 3 donc x également : $v_2(x^n) = nv_2(x) > 0$ donc $v_2(x) > 0$ et idem pour $v_3(x)$ donc (2 et 3 sont premiers entre eux) x est divisible par 6, $x \in 6\mathbb{Z}$, ce qui permet de conclure.

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 $A \setminus \{1\}$ qui en fait un groupe.
2. En déduire que A est un corps.

Correction :

1. Montrons tout d'abord que cette loi est bien interne. Soient x et y deux éléments de $A \setminus \{1\}$ et supposons que $x * y = 1$. Alors $x + y - xy = 1$ d'où : $x(1 - y) = 1 - y$ ou encore $(x - 1)(1 - y) = 0$. L'anneau étant intègre, $x = 1$ ou $y = 1$ ce qui est exclu : la loi est bien intègre. Prouvons qu'elle est associative. Soient a, b, c trois éléments de A . D'une part (on ne confondra pas la nouvelle loi $*$ avec le produit qui fait de A un anneau) :

$$\begin{aligned} a * (b * c) &= a * (b + c - cb) \\ &= a + b + c - cb - a(b + c - cb) \\ &= a + b + c - cb - ab - ac + abc \end{aligned}$$

et on trouve la même chose pour $(a * b) * c$: la loi est associative. Il est immédiat que 0 (qui appartient bien à $A \setminus \{1\}$) est un élément neutre (puisqu'il est absorbant, i.e. qu'on a $a0 = 0a = 0$) et, par hypothèse, tout élément $a \in A \setminus \{1\}$ admet un symétrique pour la loi $*$: prouvons que ce symétrique est bien dans $A \setminus \{1\}$. S'il est égal à 1, alors $a + 1 - a = 0$ donc $0 = 1$ ce qui est absurde : le symétrique est bien dans $A \setminus \{1\}$, c'est bien un groupe.

2. On se dit qu'il faut utiliser la question précédente : on a prouvé que $A \setminus \{1\}$ est un groupe (muni d'une certaine loi) et on veut prouver que A^* est un groupe (muni du produit). Il suffit de prouver que ces ensembles sont isomorphes (en faisant un léger abus de langage puisque A^* n'est pas encore un groupe mais ce n'est pas grave). On cherche une bijection de $A \setminus \{1\}$ dans A^* qui envoie le neutre 0 sur le « futur neutre » 1 mais on veut aussi que la valeur interdite 1 corresponde à la valeur interdite d'arrivée, 0 : on aimerait envoyer 0 sur 1 et « éviter d'envoyer 1 sur 0 » : tout ça pour dire qu'on s'intéresse à

$$f : \begin{cases} A \setminus \{1\} & \rightarrow A^* \\ a & \mapsto 1 - a \end{cases}$$

Alors f est évidemment bijective. Prouvons qu'elle est compatible avec les lois $*$ et \times : soient a et b dans $A \setminus \{1\}$. Alors

$$\begin{aligned} f(a * b) &= 1 - a * b \\ &= 1 - a - b + ba \\ &= (1 - a)(1 - b) \\ &= f(a)f(b) \end{aligned}$$

D'après l'exercice 22, A^* , muni de la loi \times , est un groupe : 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.

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

Correction :

- Si \mathbb{K} est fini, alors \mathbb{K} et \mathbb{K}^* n'ont pas le même cardinal (fini) donc il n'existe aucune bijection entre ces deux ensembles, et en particulier aucun isomorphisme.
- (a) Le noyau de φ est un sous-groupe de \mathbb{Z} donc est de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$.
 (b) Tout d'abord, $p \neq 1$ car on ne peut pas avoir $\ker(\varphi) = \mathbb{Z}$ puisque $\varphi(1) = 1$: on en déduit que $p = 0$ ou $p \geq 2$. Supposons que p ne soit pas nulle et ne soit pas un nombre premier : alors il existe $1 < a, b < p$ tels que $p = ab$. Alors $f(ab) = f(p) = 0$ puisque $\ker(\varphi) = p\mathbb{Z}$, donc $f(a)f(b) = 0$. Or, a et b n'appartiennent pas à $\ker(\varphi) = p\mathbb{Z}$ donc $f(a)$ et $f(b)$ sont non nuls mais $f(a)f(b) = 0$ ce qui est absurde puisque \mathbb{K} est un corps donc un anneau intègre.

3. Raisonnons par l'absurde et supposons que ces deux groupes soient isomorphes, avec $\varphi : \mathbb{K}^* \rightarrow \mathbb{K}$ un isomorphisme. Soit $x \in \mathbb{K}$. Puisque φ est un isomorphisme (i.e un morphisme bijectif),

$$\begin{aligned} x^2 = 1 &\iff \varphi(x^2) = \varphi(1) \\ &\iff \varphi(x \times x) = 0 \\ &\iff \varphi(x) + \varphi(x) = 0 \\ &\iff 2\varphi(x) = 0 \end{aligned}$$

Or, $2 = 1_{\mathbb{K}} + 1_{\mathbb{K}} = \varphi(2)$ avec φ la fonction de la question précédente. Supposons que $p \neq 2$ dans la question précédente. Alors $\varphi(2) \neq 0$ donc : $x^2 = 1 \iff \varphi(x) = 0 \iff x = 1$ puisque 1 est l'unique antécédent de 0 par φ , ce qui est absurde puisque $-1 \neq 1$ (puisque $1 + 1 \neq 0$ car $p \neq 2$) est aussi solution de l'équation $x^2 = 1$. Supposons à présent $p = 2$ si bien que $1 + 1 = 0$ et plus généralement $x + x = 0$ pour tout x . Alors tout élément de \mathbb{K} vérifie $x + x = 0$ et, en particulier, vérifie $2\varphi(x) = 0$ c'est-à-dire (par équivalences) que tout élément de \mathbb{K} est solution de $x^2 = 1$: cette équation admet une infinité de solutions, ce qui est absurde car cette équation est équivalente à $(x - 1)(x + 1) = 0$ et \mathbb{K} étant un anneau interne, elle n'admet que ± 1 comme solutions (en fait, une solution puisque $1 = -1$). On en déduit que ces deux groupes ne sont pas isomorphes.

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

Correction : Montrons que les diviseurs de zéro sont exactement les \bar{d} avec d non multiple de n non premier avec n . En particulier, si n est premier, il n'y a aucun diviseur de zéro non nul (i.e. distinct de $\bar{0}$) ce qui est cohérent avec le fait que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Soit d premier avec n . Alors (cf. cours) \bar{d} est inversible donc n'est pas un diviseur de zéro. Si d est un multiple de n alors $\bar{d} = \bar{0}$ donc n'est pas un diviseur de zéro (un diviseur de zéro est non nul par définition). Soit enfin un entier d non multiple de n et non premier avec n . Puisque n ne divise pas d , alors $\bar{n} \neq \bar{0}$. Soit $m = d \wedge n$ et soit $k = n/m$. Alors $m > 1$ donc $n/d < n$ si bien que $\bar{n}/\bar{d} \neq \bar{0}$ et $\bar{d} \times \bar{k} = \bar{d}/m \times \bar{n} = \bar{0}$ puisque d/m est entier donc $(d/m) \times n$ est un multiple de n , c'est-à-dire que \bar{d} est un diviseur de zéro.

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

Correction : Un élément \bar{d} est nilpotent s'il existe $k \geq 1$ tel que $\bar{d}^k = \bar{0}$ donc s'il existe k tel que n divise d^k . Supposons que d soit nilpotent. Alors il existe k tel que n divise d^k donc, pour tout p premier, $v_p(n) \leq v_p(d^k) = kv_p(d)$. En particulier, pour tout p facteur premier de n , $1 \leq kv_p(d)$ donc $v_p(d) \neq 0$: tous les facteurs premiers de n sont aussi facteurs premiers de d . Dès lors, les diviseurs de zéro éventuels sont parmi les nombres ayant les mêmes facteurs premiers que n mais qui ne sont pas divisibles par n (on cherche les éléments nilpotents non nuls). Supposons que les facteurs premiers de n soient tous de multiplicité 1 (i.e. n est de la forme $p_1 \times \dots \times p_k$ avec les p_i premiers distincts). Alors tout nombre d ayant les mêmes facteurs premiers que n est divisible par n donc $\bar{d} = \bar{0}$: il n'y a aucun élément nilpotent non nul. Réciproquement, supposons que les facteurs premiers de n ne soient pas tous de multiplicité 1, i.e. n est de la forme $p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$ avec les p_i premiers distincts et au moins un $\alpha_i > 1$. Posons $d = p_1 \times \dots \times p_k$. Alors d n'est pas divisible par n donc \bar{d} est non nul dans $\mathbb{Z}/n\mathbb{Z}$ et \bar{d} est nilpotent. En conclusion, $\mathbb{Z}/n\mathbb{Z}$ admet des éléments nilpotents non nuls si et seulement si les valuations p -adiques de n ne sont pas toutes égales à 1 i.e. n admet au moins un facteur premier dont la puissance est au moins égale à 2.

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

Correction : Commençons par $\mathbb{Z}/2\mathbb{Z}$. Un morphisme de groupes envoie forcément le neutre sur le neutre donc un automorphisme de groupes vérifie forcément $\varphi(\bar{0}) = \bar{0}$, et puisqu'on cherche un morphisme bijectif, il doit forcément vérifier $\varphi(\bar{1}) = \bar{1}$. On en déduit que le seul automorphisme de $\mathbb{Z}/2\mathbb{Z}$ est l'identité.

Passons à présent à $\mathbb{Z}/3\mathbb{Z}$. Raisonnons par analyse-synthèse (c'est un peu ce que nous avons fait ci-dessus) et supposons que φ soit un automorphisme de $\mathbb{Z}/3\mathbb{Z}$. Pour la même raison que ci-dessus, $\varphi(\bar{0}) = \bar{0}$. Par bijectivité de φ , on a soit $\varphi(\bar{1}) = \bar{1}$ et $\varphi(\bar{2}) = \bar{2}$, et alors φ est l'identité (de $\mathbb{Z}/3\mathbb{Z}$), soit $\varphi(\bar{1}) = \bar{2}$ et $\varphi(\bar{2}) = \bar{1}$. Puisque l'identité est évidemment un automorphisme, vérifions que, dans le deuxième cas, on a bien un automorphisme de groupes. Soient x et y deux éléments de $\mathbb{Z}/3\mathbb{Z}$. Si l'un des deux est égal à $\bar{0}$, disons x , alors $x + y = y$ et $\varphi(x) + \varphi(y) = \varphi(y)$ (puisque $\varphi(\bar{0}) = \bar{0}$) donc on a bien $\varphi(x + y) = \varphi(x) + \varphi(y)$. Si $x = y = 1$, alors

$$\begin{aligned} \varphi(x + y) &= \varphi(\bar{2}) \\ &= \bar{1} \end{aligned}$$

et

$$\begin{aligned}
\varphi(x) + \varphi(y) &= \varphi(\bar{1}) + \varphi(\bar{1}) \\
&= \bar{2} + \bar{2} \\
&= \bar{1}
\end{aligned}$$

puisqu'on travaille modulo 3, si bien qu'on a encore $\varphi(x + y) = \varphi(x) + \varphi(y)$, et idem dans tous les autres cas. Finalement, $\mathbb{Z}/3\mathbb{Z}$ admet exactement deux automorphismes : l'identité, et la fonction φ définie par : $\varphi(\bar{0}) = \bar{0}$, $\varphi(\bar{1}) = \bar{2}$ et $\varphi(\bar{2}) = \bar{1}$.

Plaçons-nous enfin sur $\mathbb{Z}/4\mathbb{Z}$ et raisonnons par analyse synthèse. Soit φ un automorphisme de groupes. On a alors $\varphi(\bar{0}) = \bar{0}$. De plus, toujours car c'est un morphisme :

$$\begin{aligned}
\varphi(\bar{2}) + \varphi(\bar{2}) &= \varphi(\bar{2} + \bar{2}) \\
&= \varphi(\bar{0}) \\
&= \bar{0}
\end{aligned}$$

c'est-à-dire que $2\varphi(\bar{2}) = \bar{0}$. Or, les seules solutions de cette équation sur $\mathbb{Z}/4\mathbb{Z}$ sont $\bar{0}$ et $\bar{2}$. De plus, $\varphi(\bar{0}) = \bar{0}$ et φ est injective donc $\varphi(\bar{2}) = \bar{2}$. Par bijectivité de φ , on a soit $\varphi(\bar{1}) = \bar{1}$ et $\varphi(\bar{3}) = \bar{3}$, et alors φ est l'identité (de $\mathbb{Z}/4\mathbb{Z}$), soit $\varphi(\bar{1}) = \bar{3}$ et $\varphi(\bar{3}) = \bar{1}$. On prouve alors réciproquement que la fonction φ définie par : $\varphi(\bar{0}) = \bar{0}$, $\varphi(\bar{1}) = \bar{3}$, $\varphi(\bar{2}) = \bar{2}$ et $\varphi(\bar{3}) = \bar{1}$ est un automorphisme, ce qui fait deux automorphismes avec l'identité.

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 $n = p^\alpha$.

Correction : Rappelons (cf. exercices 67 et 68) que les diviseurs de zéro sont les \bar{d} avec d non multiple de n et non premiers avec n ou, si on raisonne modulo n , les \bar{d} avec $1 < d < n - 1$ non premier avec n , et que les éléments nilpotents sont exactement les nombres ayant les mêmes facteurs premiers que n . Si n a au moins deux facteurs premiers, alors il existe des diviseurs de 0 qui ne sont pas nilpotents (prendre un seul facteur premier) tandis que si n a un seul facteur premier i.e. n est de la forme p^α , alors un élément est un diviseur de 0 si et seulement s'il n'est pas premier avec n si et seulement s'il est divisible par p si et seulement s'il est nilpotent.

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 ?

Correction : Soit $x \neq e$. Alors $\text{gr}(x) = G$ tout entier car c'est un sous-groupe de G distinct de $\{e\}$. Si G est infini, ce groupe est monogène infini donc isomorphe à \mathbb{Z} ce qui est absurde car \mathbb{Z} admet des sous-groupes distincts de $\{0\}$ et de lui-même : on en déduit que G est fini et cyclique puisque $G = \text{gr}(x)$ monogène fini. Notons p l'ordre de x . Si p n'est pas premier, soit d un diviseur de p distinct de 1 et p . Alors $\text{gr}(x^d)$ est un sous-groupe distinct de $\{e\}$ et de G ce qui est absurde : l'ordre de x est premier, et donc G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

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

Correction : Soit G un groupe cyclique. Plus précisément, on suppose que G est cyclique engendré par x d'ordre n i.e. $G = \{e; x; x^2; \dots; x^{n-1}\}$. Soit H un sous-groupe de G . Si $H = \{e\}$ alors H est cyclique. Sinon, posons $k = \min\{i \in \llbracket 1; n-1 \rrbracket \mid x^i \in H\}$. Montrons que $H = \text{gr}(x^k)$ ce qui permettra de conclure. Soit $y \in H$. Il existe m tel que $y = x^m$. Faisons la division euclidienne de m par k : il existe $q \in \mathbb{Z}$ et $0 \leq r < k$ tel que $m = qk + r$ donc $y = x^{qk+r}$ si bien que

$$x^r = x^y \times (x^{qk})^{-1} \in H$$

Par définition de k , cela implique que $r = 0$ donc que k divise m . On en déduit que $H \subset \text{gr}(x^k)$ et l'inclusion réciproque est immédiate par définition d'un groupe engendré.

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 .

Correction :

1. Soit d un diviseur (positif évidemment de n). Alors \mathbb{U}_d est inclus dans \mathbb{U}_n et est un groupe donc est un sous groupe de \mathbb{U}_n (tout ça pour la multiplication). Réciproquement, montrons que tout sous-groupe de \mathbb{U}_n est de cette forme. Raisonnons comme pour les sous-groupes de \mathbb{Z} : soit H un sous-groupe de \mathbb{U}_n . Si $H = \{1\}$ alors $H = \mathbb{U}_1$. Sinon, il existe $z = e^{2ik\pi/n} \in H$ avec $k \in \llbracket 1; n-1 \rrbracket$. Notons $A = \{k \in \llbracket 0; n-1 \rrbracket \mid e^{2ik\pi/n} \in H\}$. A est une partie non vide

de \mathbb{N} donc admet un plus petit élément b . Notons $\omega = e^{2ib\pi/n}$. Soit $z \in H$ qu'on écrit sous la forme $z = e^{2ik\pi/n}$ avec $k \in \llbracket 0; n-1 \rrbracket$ et faisons la division euclidienne de k par b : il existe q et r avec $0 \leq r < b$ tel que $k = bq + r$. Or,

$$e^{2ir\pi/n} = e^{2ik\pi/n} \times \frac{1}{(e^{2ib\pi/n})^q}$$

Or, $e^{2ib\pi/n} \in H$ et H est stable par produit et par inverse, si bien que $e^{2ir\pi/n} \in H$: par définition de b , cela implique que $r = 0$ donc b divise q : si on note $\omega = e^{2ib\pi/n}$, on vient de prouver que H est inclus dans $\text{gr}(\omega) = \{\omega^k \mid k \in \mathbb{N}\}$. L'inclusion réciproque étant immédiate, $H = \text{gr}(\omega)$. Or, $\omega^n = 1$ donc ω est d'ordre un diviseur de n , qu'on note d , si bien que ω est une racine d -ième de l'unité, et donc $\text{gr}(\omega) \subset \mathbb{U}_d$. Or, ω est d'ordre d donc $\text{gr}(\omega)$ est de cardinal d donc on a égalité. Finalement, $H = \mathbb{U}_d$: les sous-groupes de \mathbb{U}_n sont exactement les \mathbb{U}_d avec $d \mid n$.

2. Les \mathbb{U}_n sont évidemment des sous-groupes finis de \mathbb{C}^* (muni de la multiplication). Réciproquement, soit H un sous-groupe fini de \mathbb{C}^* . H étant fini, tout élément de H est d'ordre fini. Soit n le PPCM des ordres du groupe. Soit $x \in H$. Alors l'ordre de x divise n donc $x^n = 1$ si bien que $x \in \mathbb{U}_n$: $H \subset \mathbb{U}_n$, H est donc un sous-groupe de \mathbb{U}_n donc est de la forme \mathbb{U}_d avec $d \mid n$, ce qui est le résultat voulu.

Exercice 74 : ♦♦♦♦ Soit G un groupe fini non abélien. On pose $A = \{(a, b) \in G^2 \mid ab = ba\}$. 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 $5/8$.

Correction : Rappelons (cela découle du théorème de Lagrange, cf. cours) que si H est un sous-groupe strict d'un groupe fini G , alors $\text{card}(H) \leq \text{card}(G)/2$ puisque $\text{card}(H)$ divise $\text{card}(G)$ et que $H \neq G$. L'idée est de s'intéresser au centre : on a $\text{card}(Z(G)) \leq \text{card}(G)/2$ mais en fait on peut faire mieux en définissant un groupe intermédiaire. Soit $x \notin Z(G)$ (possible car le groupe n'est pas abélien) et posons Z_x l'ensemble des éléments qui commutent avec x . Alors (cf. cours) Z_x est un sous-groupe de G et $Z(G)$ est un sous-groupe de G . De plus, $Z(G) \neq Z_x$ car $x \in Z_x$ (x commute avec lui-même) mais $x \notin Z(G)$ (par hypothèse, x n'est pas dans le centre) et $Z_x \neq G$ car x ne commute pas avec tout le monde par hypothèse donc l'ensemble des éléments qui commutent avec x n'est pas le groupe tout entier. On en déduit que $\text{card}(Z(G)) \leq \text{card}(Z_x)/2$ et que $\text{card}(Z_x) \leq \text{card}(G)/2$ donc $\text{card}(Z(G)) \leq \text{card}(G)/4$. Intéressons-nous à présent au cardinal de A . Tout dépend si la première coordonnée x est dans le centre ou non. Si oui, la seconde coordonnée est quelconque, sinon la seconde coordonnée est dans Z_x . Plus précisément :

$$A = \{(x, y) \mid x \in Z(G), y \in G\} \cup \{(x, y) \mid x \in G \setminus Z(G), y \in Z_x\}$$

On peut même écrire chacun des deux ensembles ci-dessus comme une union disjointe :

$$A = \bigcup_{x \in Z(G)} \{(x, y) \mid y \in G\} \cup \bigcup_{x \notin Z(G)} \{(x, y) \mid y \in Z_x\}$$

Les unions étant disjointes :

$$\text{card}(A) = \sum_{x \in Z(G)} \text{card}(\{(x, y) \mid y \in G\}) + \sum_{x \in G \setminus Z(G)} \text{card}(\{(x, y) \mid y \in Z_x\})$$

Or, chaque élément de la première somme est égal à $\text{card}(G)$ et chaque élément de la deuxième somme à $\text{card}(Z_x)$. Dans la première somme, le terme sommé ne dépend pas de l'indice de sommation si bien que :

$$\text{card}(A) = \text{card}(Z(G)) \times \text{card}(G) + \sum_{x \in G \setminus Z(G)} \text{card}(Z_x)$$

Notons $n = \text{card}(G)$ si bien que $\text{card}(Z_x) \leq n/2$:

$$\begin{aligned} \text{card}(A) &\leq \text{card}(Z(G)) \times n + \sum_{x \in G \setminus Z(G)} \frac{n}{2} \\ &\leq \text{card}(Z(G)) \times n + (n - \text{card}(Z(G))) \frac{n}{2} \\ &\leq \text{card}(Z(G)) \times \frac{n}{2} + \frac{n^2}{2} \end{aligned}$$

Il suffit d'utiliser le fait que $\text{card}(Z(G)) \leq n/4$ pour conclure. Il y a égalité lorsque le centre a un cardinal égal à $n/4$ et si pour tout élément x hors du centre, $\text{card}(Z_x) = n/2$: c'est le cas par exemple pour le groupe des quaternions \mathbb{H}_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 $k \in \llbracket 0 ; n \rrbracket$, $P(k) = k^n$.

Correction : Par analyse-synthèse.

Existence : $P = X^n$ convient.

Unicité : Soit $Q \in \mathbb{R}_n[X]$ un autre polynôme qui convient. Alors P et Q coïncident en $0, \dots, n$ donc en $n + 1$ points. Puisqu'ils sont de degré inférieur ou égal à n , ils sont égaux. Ce résultat n'étant pas explicitement au programme, on peut dire que $P - Q$ a $n + 1$ racines distinctes et qu'il est de degré inférieur ou égal à n donc est égal au polynôme nul, ce qui permet de conclure.

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.

Correction : Montrons que P et Q admettent une infinité de racines. Attention, une somme de termes peut être nulle sans qu'aucun terme soit nul (on pourra se demander combien font $1 - 1$). L'idée est d'abord d'annuler le sinus : on aura alors

$Q(x) \cos(x) = 0$, et puisque le cosinus et le sinus ne s'annulent pas en même temps, on aura forcément $Q(x) = 0$. Montrons cela de façon plus précise.

Pour tout $n \in \mathbb{Z}$, $0 = P(2n\pi) \sin(2n\pi) + Q(2n\pi) \cos(2n\pi) = Q(2n\pi)$: Q admet une infinité de racines donc Q est le polynôme nul. Ainsi, pour tout $x \in \mathbb{R}$, $P(x) \sin(x) = 0$. On pourrait recommencer (avec les réels de la forme $\frac{\pi}{2} + 2n\pi$) mais changeons de méthode : pour tout $x \in]0; \pi[$, $\sin(x) \neq 0$ donc $P(x) = 0$. Comme P est nul sur $]0; \pi[$, P admet une infinité de racines donc P est le polynôme nul.

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

Correction : Pour $n = 0$, cela donne $P(0) = Q(0)$. Pour $n = 1$, cela donne $P(1) = Q(1)$, mais pour $n = 2$, cela donne $P(4) = Q(4)$, pas $P(2) = Q(2)$! A priori, P et Q ne sont pas égaux en 2. Les polynômes P et Q coïncident sur l'ensemble des carrés parfait qui est un ensemble infini donc sont égaux (si on ne veut pas exploiter ce résultat, on peut dire que $P - Q$ s'annule en tous les carrés parfait, il a une infinité de racines donc est égal au polynôme nul, donc $P = Q$).

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 $aX^{n+1} + bX^n + 1$.

Correction : Rappelons que la multiplicité de x_0 en tant que racine de P est le plus petit n tel que $P^{(n)}(x_0) \neq 0$. Par exemple, x_0 est racine triple si et seulement si $P(x_0) = P'(x_0) = P''(x_0) = 0 \neq P^{(3)}(x_0)$.

1. $P(a) = 0$ donc a est racine de P . De plus, $P' = a(X - a)^{n-1} - nX^{n-1}$ si bien que $P'(a) = -na^{n-1} \neq 0$ puisque a est non nul donc a est racine simple de P .
2. $P(1) = 0$ (soit en faisant le calcul, soit en se souvenant que 1 est racine si et seulement si la somme des coefficients est nulle). De plus, $P' = 10X^9 - 150X^5 + 240X^4 - 100X^3$ donc on a aussi $P'(1) = 0$: 1 est racine AU MOINS double (ou est racine multiple). On a aussi $P'' = 90X^8 - 750X^4 + 960X^3 - 300X^2$ donc $P''(1) = 0$. Continuons : $P^{(3)} = 720X^7 - 3000X^3 + 2880X^2 - 600X$ et donc on a encore $P^{(3)}(1) = 0$. Encore : $P^{(4)}(X) = 5040X^6 - 9000X^2 + 5760X - 600$ et là ça ne marche plus, $P^{(4)}(1) \neq 0$ donc 1 est racine de multiplicité 4.
3. On cherche a et b pour que 1 soit racine AU MOINS double : c'est le cas si et seulement si $P(1) = P'(1) = 0$ si et seulement si $a + b + 1 = 0$ et $(n + 1)a + nb = 0$. On trouve $a = n$ et $b = -(n + 1)$.

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

Correction : D'après la formule de Taylor pour les polynômes (P est de degré n) :

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

En particulier, pour tout $x \geq a$,

$$P(x) = P(a) + \sum_{k=1}^n \frac{P^{(k)}(a)(x - a)^k}{k!}$$

$P(a) > 0$ et les termes de la sommes sont positifs donc $P(x) > 0$.

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 $X^2 + 1$?

Correction :

1. Puisque $X^2 + X + 1 = (X - j)(X - j^2)$, pour prouver que $X^2 + X + 1$ divise $X^{3m+2} + X^{3n+1} + X^{3p}$, il suffit de prouver que j et j^2 sont racines de ce polynôme (c'est un résultat de cours : si on a des racines distinctes a_1, \dots, a_n , alors $(X - a_1) \dots (X - a_n)$ divise le polynôme, cela vient du fait que les $X - a_i$ sont premiers entre eux deux à deux). Rappelons que $j^k = 1$ si $k \equiv 0[3]$, $j^k = j$ si $k \equiv 1[3]$ et $j^k = j^2$ si $k \equiv 2[3]$, et que $1 + j + j^2 = 0$. Dès lors :

$$\begin{aligned}
j^{3m+2} + j^{3n+1} + j^{3p} &= j^2 + j + 1 \\
&= 0
\end{aligned}$$

donc j est racine de $X^{3m+2} + X^{3n+1} + X^{3p}$. On montrerait aisément que j^2 est aussi racine de ce polynôme, mais c'est inutile : il est à coefficients réels et j est racine donc $\bar{j} = j^2$ est aussi racine, ce qui permet de conclure.

2. Puisque $X^2 + 1 = (X - i)(X + i)$, $X^2 + 1$ divise $X^n + 1$ si et seulement si i et $-i$ sont racines de P_n . Mais puisque P_n est à coefficients réels, i est racine de P_n si et seulement si $\bar{i} = -i$ l'est aussi. En conclusion, $X^2 + 1$ divise P_n si et seulement si i est racine de P_n donc si et seulement si $i^n + 1 = 0$. Dès lors :

$$\begin{aligned}
i^n + 1 = 0 &\iff i^n = -1 \\
&\iff e^{in\pi/2} = e^{i\pi} \\
&\iff n\pi/2 \equiv \pi[2\pi] \\
&\iff n \equiv 2[4]
\end{aligned}$$

Les entiers n qui conviennent sont donc les entiers congrus à 2 modulo 4 ce qui se voit très bien sur le cercle trigo : les puissances de i successives sont $1, i, i^2 = -1$ et $i^3 = -i$ et on recommence : on se trouve en -1 pour les entiers congrus à 2 modulo 6.

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

Correction : Si P est constant alors P est monotone. Si $\deg(P) = 1$ alors P est strictement monotone. Supposons à présent que P soit de degré $n \geq 2$. Alors $\deg(P') = n - 1$ donc P' a un nombre fini de racines (au plus $n - 1$). Alors il existe $A \in \mathbb{R}$ tel que P' ne s'annule pas sur $]A; +\infty[$ (soit P' n'admet pas de racines et alors P' ne s'annule pas sur \mathbb{R} , soit P' admet un nombre fini de racines, et alors, si on pose A la plus grande des racines de P' , ce qui est possible car il y en a un nombre fini, alors P' ne s'annule pas sur $]A; +\infty[$). Puisque P' est un polynôme, c'est une fonction continue donc P' est de signe constant (raisonnement classique à savoir faire). Finalement, soit P' est strictement positive sur $]A; +\infty[$, et alors P est strictement croissante sur cet intervalle, soit P' est strictement négative sur $]A; +\infty[$, et alors P est strictement décroissante.

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.

Correction : Supposons qu'un tel polynôme P existe. Notons-le $P = a_n X^n + \dots + a_1 X + a_0$ avec $n \geq 1$ et $a_n \neq 0$ (il est supposé non constant donc de degré supérieur ou égal à 1). Alors $P(0) = a_0$ est premier. Par conséquent, $P(a_0)$ est aussi premier mais on a :

$$P(a_0) = a_n \times (a_0)^n + \dots + a_1 \times a_0 + a_0$$

c'est-à-dire que $a_0 | P(a_0)$. Or, $P(a_0)$ est premier et est divisible par a_0 premier donc $P(a_0) = a_0$. De même, pour tout $k \geq 1$, $P(a_0^k)$ est divisible par a_0 donc est égal à a_0 . a_0 est premier donc $a_0 \geq 2$: les a_0^k sont tous distincts, P et le polynôme constant égal à a_0 coïncident en une infinité de points donc sont égaux, et en particulier P est constant, ce qui est absurde.

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 $Q = R$.

Correction : P n'étant pas constant, son image est infinie. En effet, P est une fonction continue (on identifie polynôme et fonction polynomiale), $P(\mathbb{R})$ est un intervalle d'après le TVI (l'image d'un intervalle par une fonction continue est un intervalle) donc est infini car n'est pas un singleton (puisque P n'est pas constant). Puisque $Q \circ P = R \circ P$, Q et R coïncident sur $P(\mathbb{R})$ qui est un ensemble infini donc sont égaux.

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

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

Correction :

1. Supposons P constant solution égal à λ . Alors $\lambda = \lambda^2$ donc $\lambda = 0$ ou 1 , qui sont évidemment solutions (ne pas oublier la synthèse).
2. Découle du théorème de d'Alembert Gauß.
3. $P(a^2) = P(a)P(a+1) = 0$ puisque a est racine de P .
4. En appliquant ce qui précède à a^2 , $(a^2)^2 = a^4$ est racine de P , puis $(a^4)^2 = a^8$ racine de P etc. Par récurrence, on prouve que a^{2^n} (et pas $(a^2)^n = a^{2n}$) est racine de P pour tout n . P n'étant pas constant, il n'admet qu'un nombre fini de racines : d'après le principe des tiroirs, il existe deux termes (et même une infinité) de la forme a^{2^n} qui sont égaux : il existe $n_1 < n_2$ tels que $a^{2^{n_1}} = a^{2^{n_2}}$. Soit $a = 0$, et alors c'est bon, soit on peut simplifier par $a^{2^{n_1}}$ ce qui donne : $a^{2^{n_1}-2^{n_2}} = 1$, 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} .

Correction :

1. P admet 1 comme racine (au moins) simple et 2 comme racine (au moins) double donc est divisible par $(X-1)(X-2)^2$: P étant de degré 4, il existe a et b tels que $P = (aX+b)(X-1)(X-2)^2$. Or, $P(0) = 4$ donc $-4b = 4$ si bien que $b = -1$. Enfin, $P(3) = 1$ donc :

$$(3a-1)(3-1)(3-2)^2 = 1$$

et on trouve donc que $(3a-1) \times 2 = 1$ ce qui donne $a = 1/2$. Finalement, P est le polynôme $(X/2-1)(X-1)(X-2)^2$.

2. Par hypothèse, Q est divisible par $(X+3)^{796}(X-3)^{1227}(X-1)$ qui est de degré 2024. Q étant lui-même de degré 2024, si on note a son coefficient dominant (ne pas l'oublier!), $Q = a(X+3)^{796}(X-3)^{1227}(X-1)$. De plus, le coefficient constant, égal à $Q(0)$, vaut 6^{2024} donc :

$$a \times 3^{796} \times (-3)^{1227} \times (-1) = 6^{2024}$$

si bien que $a \times (-1)^{1228} \times 9^{2023} = a \times 9^{2023} = 6^{2023}$. On en déduit que $a = (6/9)^{2023} = (2/3)^{2023}$ donc

$$Q = \left(\frac{2}{3}\right)^{2023} (X+3)^{796}(X-3)^{1227}(X-1)$$

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

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

Correction : $P - Q$ étant non nul, il n'admet qu'un nombre fini de racines donc ne s'annule pas à partir d'une certaine valeur A donc est de signe constant car est une fonction continue (on identifie polynôme et fonction polynomiale) : si $P - Q < 0$ à partir de A , alors on est dans le premier cas, sinon on est dans le second cas.

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 .

Correction : Supposons que $X-1$ divise $P(X^n)$: il en découle que 1 est racine de $P(X^n)$ donc que $P(1^n) = P(1) = 0$. Par conséquent, pour tout $k \in \llbracket 0; n-1 \rrbracket$, si on pose $\omega = e^{2ik\pi/n}$ une racine n -ième de l'unité, $0 = P(1) = P(\omega^n)$ donc ω est racine de $P(X^n)$. Les $e^{2ik\pi/n}$ étant deux à deux distincts, $P(X^n)$ est divisible par

$$\prod_{k=0}^{n-1} (X - e^{2ik\pi/n}) = X^n - 1$$

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 $(X-1)(X^{pq}-1)$.

Correction : On a tout d'abord :

$$(X^p-1)(X^q-1) = \prod_{k=0}^{p-1} (X - e^{2ik\pi/p}) \times \prod_{k=0}^{q-1} (X - e^{2ik\pi/q})$$

Cherchons les racines communes de ces deux polynômes. Soit z une racine des deux polynômes X^p-1 et X^q-1 : z est donc à la fois une racine p -ième et une racine q -ième de l'unité et donc il existe $k_1 \in \llbracket 0; p-1 \rrbracket$ et $k_2 \in \llbracket 0; q-1 \rrbracket$ tels que

$$z = e^{2ik_1\pi/p} = e^{2ik_2\pi/q}$$

Par conséquent : $2k_1\pi/p \equiv 2k_2\pi/q[2\pi]$ si bien que $qk_1 \equiv pk_2[pq]$: il existe n tel que $qk_1 = pk_2 + npq$: q divise donc pk_2 et puisque $p \wedge q = 1$, alors q divise k_2 mais $k_2 \in \llbracket 0; q-1 \rrbracket$ donc $k_2 = 0$ donc $z = 1 : 1$ est la seule racine commune de ces deux polynômes. En d'autres termes, dans la factorisation ci-dessus, on trouve $(X-1)$ deux fois et tous les autres termes une seule fois. Or, 1 est racine de $X^{pq} - 1$ donc 1 est racine double de $(X-1)(X^{pq} - 1)$ si bien que ce polynôme est divisible par $(X-1)^2$. De plus, les autres racines p -ièmes et q -ièmes de l'unité sont racines de $X^{pq} - 1$: en effet, si ω est racine p -ième de l'unité (idem pour les racines q -ièmes), alors $\omega^p = 1$ donc $\omega^{pq} = 1^q = 1$ donc ω est racine de $X^{pq} - 1$. Toutes ces racines étant distinctes, $X^{pq} - 1$ est divisible par

$$\prod_{k=1}^{p-1} (X - e^{2ik\pi/p}) \times \prod_{k=1}^{q-1} (X - e^{2ik\pi/q})$$

donc $(X-1)(X^{pq} - 1)$ est divisible par

$$(X-1)^2 \prod_{k=1}^{p-1} (X - e^{2ik\pi/p}) \times \prod_{k=1}^{q-1} (X - e^{2ik\pi/q}) = (X^p - 1)(X^q - 1)$$

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

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

Correction : Raisonnons à chaque fois par l'absurde et supposons qu'un tel polynôme existe.

- Si un tel polynôme P existe, alors pour tout $k \geq 1$, $kP(k) = 1$: en d'autres termes, le polynôme $Q = XP - 1$ s'annule en tout $k \geq 1$ donc admet une infinité de racines donc est le polynôme nul si bien que $XP = 1$ ce qui est absurde car le degré de XP ne peut pas être égal à 0 : si $P = 0$ alors $XP = 0$ et sinon alors $\deg(XP) \geq 1$. Dans tous les cas on a l'absurdité voulue.
- Si un tel polynôme existe, de même, le polynôme $Q = P^2 - X^2 - 1$ est le polynôme nul car admet une infinité de racines donc $P^2 = X^2 + 1$. Or, il n'existe aucun polynôme dont le carré soit $X^2 + 1$. Supposons en effet qu'un tel polynôme P existe : puisque $\deg(P^2) = 2\deg(P) = 2$ alors P est de degré 1 : il existe a et b tels que $P = aX + b$ donc $P^2 = a^2X^2 + 2abX + b^2$ donc $a^2 = 1$ donc $a = \pm 1$, idem pour b , mais $2ab = 0$ donc $a = 0$ ou $b = 0$ ce qui est absurde.
- Le raisonnement précédent ne marche plus, il faut plutôt raisonner avec des croissances comparées. Supposons donc qu'un tel polynôme existe, alors la suite de terme général $P(n)/2^n$ est constante égale à 1. Cependant, par croissances comparées, les suites géométriques l'emportent sur les suites polynomiales donc cette suite tend en fait vers 0 ce qui est absurde.

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

Correction : Première méthode : d'après le théorème de factorisation sur \mathbb{R} , P s'écrit comme un produit de polynômes de degré 1 ou de degré 2 de discriminant strictement négatif. Si, dans cette factorisation, on ne trouve que des polynômes de degré 2, alors $\deg(P)$ est pair, ce qui est absurde. Ainsi, P est divisible par un polynôme de degré 1. Or, un polynôme de degré 1 admet une racine donc P admet une racine.

Deuxième méthode : notons n le degré de n (impair) et a_n le coefficient dominant (non nul par définition). Alors $P(x) = a_n x^n + \dots$ donc $P(x) \xrightarrow{x \rightarrow +\infty} +\infty$ si $a_n > 0$ et $-\infty$ si $a_n < 0$, et c'est le contraire en $-\infty$ (car n est impair) et P est une fonction continue (on associe polynôme et fonction polynomiale) donc, d'après le TVI, P s'annule au moins une fois.

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

Correction : Supposons qu'il existe un polynôme P qui convient. Alors, pour tout $z \in \mathbb{R}$, $P(z) = z$ donc P et X coïncident sur \mathbb{R} qui est un ensemble infini donc sont égaux si bien que $P = X$. En d'autres termes, pour tout $z \in \mathbb{C}$, $P(z) = z$ c'est-à-dire que $\bar{z} = z$ pour tout $z \in \mathbb{C}$ ce qui est absurde (prendre par exemple $z = i$).

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.

Correction :

1. Soit $P \in \mathbb{C}[X]$ non constant. Soit $a \in \mathbb{C}$. Alors $P - a$ est toujours non constant donc admet une racine d'après le théorème de d'Alembert-Gauß : il existe $z \in \mathbb{C}$ tel que $P(z) - a = 0$ i.e. tel que $P(z) = a$: a admet un antécédent par P , P est surjectif.
2. (a) Un polynôme constant ne peut pas être injectif puisqu'il prend une infinité de fois la même valeur.
 (b) D'après le théorème de d'Alembert-Gauß, P a au moins une racine complexe. Si P admet au moins deux racines distinctes, alors 0 admet au moins deux antécédents par P ce qui est absurde car P est injectif. Si on note z_0 cette unique racine, $n \geq 1$ le degré de P et $a_n \neq 0$ le coefficient dominant, alors $P = a_n(X - z_0)^n$.
 (c) Supposons donc $n \geq 2$. Soit $z \in \mathbb{C}$. Rappelons que $a_n \neq 0$ par définition d'un coefficient dominant.

$$\begin{aligned} P(z) = a_n &\iff (z - z_0)^n = 1 \\ &\iff z - z_0 \text{ est une racine } n\text{-ième de l'unité} \\ &\iff \exists k \in \llbracket 0; n-1 \rrbracket, z - z_0 = e^{2ik\pi/n} \\ &= \exists k \in \llbracket 0; n-1 \rrbracket, z = z_0 + e^{2ik\pi/n} \end{aligned}$$

Par conséquent, a_n admet exactement $n \geq 2$ antécédents distincts ce qui est absurde par injectivité de P . On en déduit que $n = 1$.

- (d) Lors des questions précédentes, on était dans la phase « analyse » d'un raisonnement par analyse-synthèse, et on avait prouvé que les seuls polynômes injectifs possibles étaient les polynômes de degré 1. Synthèse : soit $P = aX + b$ de degré 1 avec $a \neq 0$. Soient z_1, z_2 tels que $P(z_1) = P(z_2)$. Alors $az_1 + b = az_2 + b$ donc $az_1 = az_2$ et $a \neq 0$ donc $z_1 = z_2$: P est injectif. En conclusion, les polynômes injectifs sont exactement les polynômes de degré 1.

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.

Correction :

1. Soit $n = \deg(P)$. Alors P admet exactement n racines réelles distinctes, puisqu'il est scindé à racines simples. Notons $x_1 < \dots < x_n$ ses racines. En fait comme dans le chapitre 15, i.e. en appliquant $n - 1$ fois le théorème de Rolle, on trouve que P' admet au moins $n - 1$ racines réelles distinctes. Or, $\deg(P') = n - 1$ donc P' admet autant de racines réelles que son degré, et celles-ci sont distinctes : P' est scindé à racines simples.
2. Notons $n = \deg(P)$ et $k \leq n$ le nombre de racines réelles distinctes de P . Plus précisément, notons $x_1 < \dots < x_k$ les racines réelles distinctes de P , de multiplicité respective n_1, \dots, n_k si bien que

$$P = a_n(X - x_1)^{n_1} \times \dots \times (X - x_k)^{n_k}$$

On a en particulier $n = \deg(P) = n_1 + \dots + n_k$. En appliquant encore une fois $k - 1$ fois le théorème de Rolle, on obtient $k - 1$ racines de P' qu'on peut noter y_1, \dots, y_{k-1} avec $y_1 \in]x_1; x_2[$, \dots , $y_{k-1} \in]x_{k-1}; x_k[$. Or, x_1 est racine de multiplicité n_1 de P donc est racine de P' de multiplicité $n_1 - 1$ (cf. cours), x_2 est racine de P de multiplicité n_2 donc est racine de P' de multiplicité $n_2 - 1$ etc. Les x_i forment donc des racines de P' , et quand on les compte avec multiplicité, cela fait

$$(n_1 - 1) + \dots + (n_k - 1) = (n_1 + \dots + n_k) - k = n - k$$

nouvelles racines (distinctes des y_i puisque les y_i appartiennent aux intervalles ouverts). Cela donne $(n - k) + (k - 1) = n - 1$ racines réelles comptées avec multiplicité : on trouve encore que P' est scindé (mais pas forcément à racines simples).

3. (a) Dans la démonstration ci-dessus, les y_i (i.e. les racines obtenues avec le théorème de Rolle) sont forcément simples : en effet, si l'une au moins est racine double, alors cela donne trop de racines par rapport au degré de P' . Il en découle que les seules racines multiples éventuelles de P' se trouvent parmi les x_i , donc parmi celles qui sont déjà racines de P .
- (b) Soit $Q = P^2 + \lambda^2$, si bien que $Q' = 2PP'$. P étant scindé, alors P' est scindé : ses racines sont donc en particulier toutes réelles, et donc les racines de Q' sont aussi toutes réelles. Or, Q n'a aucune racine réelle car est à valeurs strictement positives sur \mathbb{R} (on assimile encore une fois polynôme et fonction polynomiale associée, ce qu'on ne s'est pas privé de faire d'ailleurs pour appliquer le théorème de Rolle) : Q et Q' n'ont donc aucune racine commune, les racines de Q sont toutes simples.
- (c) Si $X^3 + 1$ est scindé à racines simples, son polynôme dérivé également d'après la question 1, ce qui est absurde puisque son polynôme dérivé est $3X^2$ qui admet 0 comme racine double. Plus généralement, soit

$$P = a_n X^n + \cdots + a_{k+2} X^{k+2} + a_{k-1} X^{k-1} + \cdots + a_0$$

un polynôme admettant deux coefficients consécutifs nuls (il n'est dit nulle part que les autres sont non nuls, à part a_n). Si P est scindé à racines simples, alors P' l'est aussi et, par une récurrence finie immédiate, toutes ses dérivées jusqu'à l'ordre n le sont aussi. Or, la dérivée k -ième de P s'écrit

$$P = b_{n-k} X^{n-k} + \cdots + b_2 X^2$$

donc admet 0 comme racine double, ce qui est absurde.

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.

Correction :

1. (a) C'est l'exercice 51 du chapitre 14.
- (b) Raisonnons par l'absurde et supposons qu'elle admet au moins $n + 2$ solutions, notées $x_1 < \cdots < x_{n+2}$. En d'autres termes, la fonction $g : x \mapsto P(x) - e^x$ s'annule en $n + 2$ points. Puisqu'elle est dérivable $n + 1$ fois, d'après la question 1, $g^{(n+1)}$ s'annule. Or, la dérivée $n + 1$ -ème de P est nulle donc la dérivée $n + 1$ -ième de g est la dérivée $n + 1$ -ième de l'exponentielle, c'est-à-dire l'exponentielle elle-même, ce qui est absurde puisqu'elle ne s'annule pas.
2. Le problème est que cela ne fonctionne plus ici puisque la fonction sinus et toutes ses dérivées s'annulent (et même une infinité de fois). L'idée est de borner l'ensemble des solutions éventuelles. Le polynôme P n'étant pas constant, il tend vers $\pm\infty$ en $\pm\infty$ (selon la parité du degré et le signe du coefficient dominant). En particulier, il existe A tel que, pour tout $x \notin [-A; A]$, $|P(x)| > 1$ donc les solutions éventuelles se trouvent sur $[-A; A]$. Supposons par l'absurde que l'équation $P(x) = \sin(x)$ possède un nombre infini de solutions sur cet intervalle. Notons k le nombre de fois que \sin s'annule sur cet intervalle (k est fini car le sinus s'annule un nombre fini de fois sur un intervalle donné). Il en découle que $g : x \mapsto P(x) - \sin(x)$ s'annule au moins $4n + k + 1$ fois (où $n = \deg(P)$) fois, si bien que, de même, $g^{(4n)}$ s'annule au moins $k + 1$ fois. Or, $4n \geq n + 1$ donc la dérivée $4n$ -ième de P est nulle si bien que $g^{(4n)} = \sin^{(4n)}$ ce qui est absurde puisque le sinus s'annule au plus k fois sur $[-A; A]$.

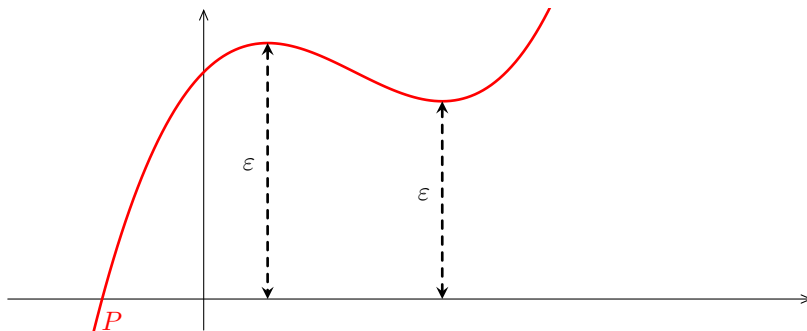
Exercice 21 : ★★ Soit $P \in \mathbb{R}[X]$ de degré n . Montrer que le nombre de réels ε tels que $P + \varepsilon$ admette des racines multiples est inférieur ou égal à $n - 1$. Illustrer par un dessin. En déduire qu'il existe $\alpha > 0$ tel que pour tout $\varepsilon \in]0; \alpha[$, $P + \varepsilon$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

Correction : Soit $\alpha \in \mathbb{R}$ et soit $\varepsilon \in \mathbb{R}$. Notons $Q = P + \varepsilon$. Alors :

$$\alpha \text{ est racine multiple de } Q \iff Q(\alpha) = Q'(\alpha) = 0$$

$$\iff \varepsilon = -P(\alpha) \quad \text{et} \quad P'(\alpha) = 0$$

Par conséquent, Q admet une racine multiple si et seulement s'il existe α racine de P' tel que $\varepsilon = -P(\alpha)$, et donc il y a au plus $n - 1$ telles valeurs de ε puisque P' admet au plus $n - 1$ racines réelles distinctes. Ci-dessous un dessin : on a une racine multiple quand la fonction coupe l'axe des abscisses avec une tangente horizontale, donc la seule façon d'obtenir une racine multiple « par translation verticale », i.e. en ajoutant un réel, est de soustraire l'image de l'un des points où la tangente est horizontale pour qu'elle coupe l'axe des abscisses en ce point :



En particulier, le nombre de tels ε est fini : si on note α le plus petit de ces $\varepsilon > 0$, alors il n'y a aucun ε dans $]0; \alpha[$ ce qui permet de conclure.

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

Correction : Notons $P = a_n X^n + \dots + a_0$. Pour tout $x \in \mathbb{R}$, $P(x) \in \mathbb{R}$ donc $\overline{P(x)} = P(x)$ i.e.

$$\begin{aligned} P(z) &= \overline{a_n x^n + \dots + a_1 x + a_0} \\ &= \overline{a_n x^n} + \dots + \overline{a_1 x} + \overline{a_0} \end{aligned}$$

Or, x est réel donc $\bar{x} = x$ si bien que

$$P(z) = \overline{a_n} x^n + \dots + \overline{a_1} x + \overline{a_0}$$

c'est-à-dire que P et $\overline{a_n} X^n + \dots + \overline{a_1} X + \overline{a_0}$ coïncident sur \mathbb{R} qui est un ensemble infini donc sont égaux i.e. ont les mêmes coefficients. En d'autres termes, pour tout k , $a_k = \overline{a_k}$ i.e. $a_k \in \mathbb{R}$: les coefficients de P sont réels, $P \in \mathbb{R}[X]$.

Exercice 23 : ★★★ Soit $P \in \mathbb{C}[X]$ de degré n tel qu'il existe a_1, \dots, 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.

Correction : Notons $b_1 = P(a_1), \dots, b_n = P(a_n)$. Il existe au plus un polynôme de degré inférieur ou égal à n à coefficients dans \mathbb{Q} (qui est un corps : on obtient le polynôme à l'aide de sommes, produits, quotients d'éléments du corps, cf. cours) et P convient donc ce polynôme est égal à P . En particulier, $P \in \mathbb{Q}[X]$. On aurait pu faire ce raisonnement dans l'exercice précédent.

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 : $\forall n \in \mathbb{Z}, P(n) \in \mathbb{Z}$.

Correction : $P = X(X+1)/2$ convient : que n soit pair ou impair, $P(n) \in \mathbb{Z}$. Le résultat sur les polynômes de Lagrange n'est pas valable car \mathbb{Z} n'est pas un corps : on ne peut pas diviser sur \mathbb{Z} . Par contre, un tel polynôme est forcément à coefficients rationnels.

Exercice 25 : ★★

- Donner tous les polynômes $P \in \mathbb{R}[X]$ vérifiant

$$\forall k \in \mathbb{N}, \quad \int_k^{k+1} P(t) dt = k$$

- Donner tous les polynômes $P \in \mathbb{R}[X]$ vérifiant

$$\forall k \in \mathbb{N}^*, \quad \int_k^{k+1} P(t) dt = \frac{1}{k}$$

Correction :

- Analyse : soit P un polynôme qui convient. Soit Q une primitive de P (une telle primitive existe car P est continue, encore une fois on assimile polynôme et fonction polynomiale : il est légitime d'introduire une primitive de P car on manipule des intégrales). Par conséquent, pour tout k , $Q(k+1) - Q(k) = k$. Par somme (on reconnaît un télescopage) :

$$\sum_{k=0}^{n-1} Q(k+1) - Q(k) = Q(n) - Q(0) = \sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}$$

On en déduit que $Q(n) = \frac{n(n-1)}{2} + Q(0)$. Le polynôme Q et le polynôme $\frac{X(X-1)}{2} + Q(0)$ coïncident sur \mathbb{N} qui est un ensemble infini donc sont égaux. En dérivant (rappelons que $P = Q'$) il vient : $P = X - 1/2$. Synthèse : il est immédiat que pour tout $k \in \mathbb{N}$,

$$\int_k^{k+1} \left(t - \frac{1}{2}\right) dt = k$$

donc ce polynôme convient effectivement. Conclusion : $X - 1/2$ est l'unique solution.

2. Deux façons de prouver qu'il n'y a pas de solution. Supposons par l'absurde qu'il existe une solution. L'une est un copier-coller de ce qui précède mais utilise pour conclure un résultat que nous verrons au second semestre. On trouve donc de la même façon que pour tout n ,

$$Q(n) - Q(1) = \sum_{k=1}^{n-1} \frac{1}{k}$$

Le problème est que le membre de droite n'est pas polynomial en k donc on ne peut pas conclure de la même façon. Nous verrons au second semestre que ce terme est équivalent (nous verrons aussi ce que ça veut dire au second semestre) à $\ln(n)$ donc que

$$Q(n) \sim \ln(n)$$

ce qui est absurde car $Q(n) \sim a_d n^d$ son terme de plus haut degré : absurde, un tel polynôme n'existe pas. Une autre solution consiste à dire qu'un polynôme est soit constant, soit diverge vers $\pm\infty$ en $+\infty$ (selon son coefficient dominant). S'il est constant égal à λ , alors

$$\int_k^{k+1} P(t) dt = \lambda$$

pour tout k . S'il tend vers $+\infty$, pour t assez grand $P(t) \geq 1$ donc, par croissance de l'intégrale,

$$\int_k^{k+1} P(t) dt \leq 1$$

et s'il tend vers $-\infty$, l'intégrale est inférieure à -1 pour k assez grand par un raisonnement analogue. Dans tous les cas, on ne peut pas avoir

$$\int_k^{k+1} P(t) dt \xrightarrow[k \rightarrow +\infty]{} 0^+$$

car la seule façon que cette suite tende vers 0 est que P soit constant égal à 0 mais alors cette suite d'intégrale est constante égale à 0 et ne tend pas vers 0 par valeurs supérieures. Dans les deux cas on conclut à une absurdité : un tel polynôme n'existe pas.

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.

Correction :

1. Montrons que pour tout $n \in \mathbb{Z}$, $P(n)$ est impair : cela impliquera en particulier que $P(n) \neq 0$. Notons $P = \sum_{k=0}^d a_k X^k$ avec les a_k dans \mathbb{Z} . Supposons n pair. Alors :

$$P(n) = \sum_{k=1}^d a_k n^k + a_0$$

La somme ci-dessus est paire car n est pair (il fallait mettre à part le terme pour $k = 0$: ne jamais oublier que $X^0 = 1$!) et $a_0 = P(0)$ est impair : on a la somme d'un nombre pair et d'un nombre impair donc la somme est impaire, si bien que $P(n)$ est impair. Supposons à présent n impair. Le même raisonnement n'est plus valide car,

même si les puissances de n sont impaires, on ne connaît pas la parité des a_k . Pour tout k , n_k est impair : il existe donc β_k tel que $n^k = 2\beta_k + 1$ donc :

$$\begin{aligned} P(n) &= \sum_{k=0}^n a_k (2\beta_k + 1) \\ &= 2 \sum_{k=0}^n a_k \beta_k + \sum_{k=0}^n a_k \end{aligned}$$

Or, $f(1) = \sum_{k=0}^n a_k$ qui est un nombre impair si bien que $P(n)$ est impair car somme d'un nombre pair (car divisible par 2) et d'un nombre impair, ce qui permet de conclure. C'est tout de même fort : il suffit (mais ce n'est pas équivalent sinon ce serait trop facile) que $P(0)$ et $P(1)$ soient impairs pour qu'il n'y ait AUCUNE racine entière !

2. Notons $P = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ avec les a_i dans \mathbb{Z} (rappelons que P est unitaire). Soit $r = p/q$ avec p et q premiers entre eux (pas forcément premiers mais premiers entre eux) une racine rationnelle de P . Alors $P(r) = 0$ c'est-à-dire :

$$\frac{p^n}{q^n} + a_{n-1} \times \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \times \frac{p}{q} + a_0 = 0$$

En multipliant par q^n et en mettant tous les termes sauf le premier à droite :

$$p^n = qa_{n-1}p^{n-1} + \dots + q^{n-1}a_1p + q^na_0$$

Par conséquent, q divise p^n donc $p^n \wedge q = q$ mais p et q sont premiers entre eux donc p^n et q sont premiers entre eux donc $p^n \wedge q = 1$ donc $q = 1$ si bien que $r = p \in \mathbb{Z}$.

3. Si on note a_n le coefficient dominant de P , on arrive à :

$$a_np^n = qa_{n-1}p^{n-1} + \dots + q^{n-1}a_1p + q^na_0$$

q divise a_np^n et q est premier avec p^n donc, d'après le théorème de Gauß, q divise a_n : en conclusion, les racines rationnelles de P ont un dénominateur (quand elles sont écrites sous forme irréductible) qui divise le coefficient dominant de P . Par exemple, si $P = 3X^n + \dots$ alors les racines rationnelles de P (s'il en existe) s'écrivent sous la forme $p/3$ avec $p \in \mathbb{Z}$. Cela ne laisse pas beaucoup de choix, comme on le voit dans la question suivante.

4. Théorème de la bijection (on assimile polynôme et fonction polynomiale) pour l'existence et l'unicité (on dérive ou on dit que P est la somme de trois fonctions croissantes dont deux strictement). D'après la question 2, P étant dans $\mathbb{Z}[X]$ unitaire, si cette racine est rationnelle, elle est entière. Mais d'après la question 1, puisque $P(0) = 1$ et $P(1) = 3$ soit impairs, P n'a pas de racine entière : il en découle que P n'a pas de racine rationnelle, donc que l'unique racine réelle de P est irrationnelle.
5. Notons $\alpha = \sqrt[k]{d}$. Alors α est racine de $P = X^k - d$. d n'est pas la puissance k -ième d'un entier donc P n'a pas de racine entière. Or, P est unitaire à coefficients dans \mathbb{Z} donc, d'après la question 2, les racines rationnelles de P sont entières : puisque P n'a pas de racine entière, P n'a pas de racine rationnelle, donc $\alpha = \sqrt[k]{d}$ est un irrationnel.

Exercice 27 : ♦♦ Trouver tous les polynômes $P \in \mathbb{K}[X]$ tels que :

$$\forall (x, y) \in \mathbb{K}^2, P(xy) = P(x) \times P(y)$$

Correction : Supposons P constant égal à λ . Alors P est solution si et seulement si $\lambda = \lambda^2$ si et seulement si $\lambda = 0$ ou 1. Supposons dans la suite P non constant. Analyse : supposons que P convienne. Soit $z \in \mathbb{C}$ une racine complexe de P (rappelons que $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} donc, dans tous les cas, P peut être considéré comme un polynôme à coefficients complexes) qui existe d'après le théorème de d'Alembert-Gauß, puisque P n'est pas constant. Alors $P(zy) = 0$ pour tout $y \in \mathbb{C}$. Si $z \neq 0$ alors, pour tout $y \in \mathbb{C}$,

$$\begin{aligned} P(y) &= P\left(z \times \frac{y}{z}\right) \\ &= 0 \end{aligned}$$

donc P est le polynôme nul ce qui est exclu (on a supposé P non constant). Par conséquent, 0 est la seule racine de P donc P s'écrit $P = a_nX^n$ avec n le degré de P et $a_n \neq 0$ son coefficient dominant. Finalement, pour tous x et y :

$$a_n(xy)^n = a_nx^n \times a_ny^n$$

En prenant $x = y = 1 : a_n = a_n^2$ donc $a_n = 1$ puisque $a_n = 0$, c'est-à-dire qu'il existe n tel que $P = X^n$. Synthèse : pour tout n , X^n est évidemment solution. Conclusion : les seuls polynômes solutions sont les polynômes constants égaux à 0 et 1 et tous les polynômes de la forme X^n , pour $n \in \mathbb{N}$.

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

Correction : Notons $P = a_n(X - x_1)^{n_1} \times \cdots \times (X - x_k)^{n_k}$ où les x_i sont les racines distinctes de P et les n_i leurs multiplicités respectives (P est forcément scindé puisqu'on est sur \mathbb{C}). Il y a donc k racines distinctes et le but de l'exercice est de prouver que $k = \deg(P) - \deg(P \wedge P')$. On a de plus $\deg(P) = n_1 + \cdots + n_k$. Les x_1, \dots, x_k sont racines de P' de multiplicité respectives $n_1 - 1, \dots, n_k - 1$ et ce sont les seules racines communes de P et P' (les autres racines de P' ne sont pas racines de P puisque P n'a pas d'autres racines que les x_k) si bien que (le PGCD de P et P' est le produit de leurs facteurs irréductibles communs à la puissance la plus petite des deux) :

$$P \wedge P' = (X - x_1)^{n_1-1} \times \cdots \times (X - x_k)^{n_k-1}$$

de degré $n_1 + \cdots + n_k - k$ ce qui permet de conclure.

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

$$|z| \leq \max \left(1, \sum_{i=0}^{n-1} |a_i| \right)$$

Correction : Il suffit de prouver que si $|z| > 1$ alors $|z| \leq \sum_{i=0}^{n-1} |a_i|$. En effet, si $|z| \leq 1$ alors c'est bon, et si $|z| > 1$, prouver que $|z|$ est inférieur ou égal à cette somme permet de conclure. Supposons donc que z soit racine de P . Dès lors :

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = 0$$

si bien que

$$a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = -z^n$$

En prenant le module et en appliquant l'inégalité triangulaire :

$$|z|^n \leq \sum_{k=0}^{n-1} |a_k| \times |z|^k$$

Or, $|z| > 1$ (quand $|z| \leq 1$, les inégalités sont dans l'autre sens) donc, pour tout $k \leq n-1$, $|z|^k \leq |z|^{n-1}$ (l'inégalité est stricte mais, en multipliant par $|a_k|$ qui peut être nul, on obtient de toute façon une inégalité large) donc $|a_k| \times |z|^k \leq |a_k| \times |z|^{n-1}$ et, par somme :

$$|z|^{n-1} \leq \sum_{k=0}^{n-1} |a_k| \times |z|^k = |z|^{n-1} \sum_{k=0}^{n-1} |a_k|$$

En simplifiant par $|z|^{n-1}$ (non nul), on obtient le résultat voulu.

Exercice 30 - Un cas particulier du théorème d'Eneström-Kekeya : ♦♦ 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 $(1 - X) \times P$).

Correction : Raisonnons par l'absurde et supposons que P admette une racine complexe z de module strictement inférieur à 1. Suivons l'indication de l'énoncé et intéressons-nous à $Q = (1 - X) \times P$. Alors $Q(z) = 0$. Or :

$$\begin{aligned}
Q(z) &= (1-z) \times \sum_{k=0}^n a_k z^k \\
&= \sum_{k=0}^n a_k z^k - \sum_{k=0}^n a_k z^{k+1} \\
&= \sum_{k=0}^n a_k z^k - \sum_{k=1}^{n+1} a_{k-1} z^k \\
&= a_0 + \sum_{k=1}^n (a_k - a_{k-1}) z^k - a_n z^{n+1}
\end{aligned}$$

Par conséquent, puisque $Q(z) = 0$, il en découle que

$$a_0 = \sum_{k=1}^n (a_k - a_{k-1}) z^k - a_n z^{n+1}$$

Idem, d'après l'inégalité triangulaire :

$$|a_0| \leq \sum_{k=1}^n |a_k - a_{k-1}| \times |z|^k + |a_{n+1}| \times |z|^{n+1}$$

Or, a_0 et a_n sont positifs et $|a_k - a_{k-1}| = a_{k-1} - a_k$ par hypothèse sur les coefficients de P , si bien que :

$$a_0 \leq \sum_{k=1}^n (a_{k-1} - a_k) \times |z|^k + a_{n+1} \times |z|^{n+1}$$

Or, $|z| < 1$ et $a_{n+1} > 0$ donc $a_{n+1} \times |z|^{n+1} < a_{n+1}$. Cependant, $a_{k-1} - a_k$ peut être nul donc on a seulement $(a_{k-1} - a_k)|z|^k \leq a_{k-1} - a_k$ (l'inégalité n'est pas stricte alors que $|z| < 1$ car $a_{k-1} - a_k$ peut être nul et alors il y a égalité). Cependant, une inégalité est stricte donc la somme l'est, si bien que :

$$a_0 < \sum_{k=1}^n (a_{k-1} - a_k) + a_{n+1}$$

On reconnaît une somme télescopique : on obtient finalement $a_0 < a_0 - a_{n+1} + a_{n+1} = a_0$ ce qui est absurde.

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 $(X + a_1)(X + a_2)(X + a_3)$.

Correction : Notons $Q = (X + a_1)(X + a_2)(X + a_3)$. Puisque le produit des termes de chaque colonne fait 2024, $Q(b_1) = Q(b_2) = Q(b_3) = 2024$, c'est-à-dire que b_1, b_2, b_3 sont racines de $Q - 2024$ qui est unitaire de degré 3. Les réels b_1, b_2, b_3 étant distincts, $Q - 2024 = (X - b_1)(X - b_2)(X - b_3)$ et donc

$$(X + a_1)(X + a_2)(X + a_3) = (X - b_1)(X - b_2)(X - b_3) + 2024$$

En évaluant en $-a_1$:

$$0 = (-a_1 - b_1)(-a_1 - b_2)(-a_1 - b_3) - 2024$$

et puisque $(-1)^3 = -1$, il vient :

$$-(a_1 + b_1)(a_1 + b_2)(a_1 + b_3) - 2024 = 0$$

En d'autres termes : $(a_1 + b_1)(a_1 + b_2)(a_1 + b_3) = -2024$: le produit des termes de la première ligne vaut -2024 , et c'est la même chose pour les deux autres lignes.

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

Correction : Notons $P = \sum_{k=0}^n a_k X^k$ si bien que

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

Or :

$$P^k - X^k = (P - X) \times \sum_{i=0}^{k-1} P^i X^{k-1-i}$$

En particulier, $P^k - X^k$ est divisible par $P - X$ donc, par somme, $P \circ P - P$ l'est aussi. Enfin,

$$P \circ P - X = (P \circ P - P) + (P - X)$$

donc $P \circ P - X$ est somme de deux polynômes divisibles par $P - X$ donc est lui-même divisible par $P - x$.

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 deuxième semestre) :

$$\forall x \in \mathbb{R} \quad \sum_{k=0}^n \frac{x^k}{k!} \xrightarrow{n \rightarrow +\infty} e^x$$

Montrer que $a_n \xrightarrow{n \rightarrow +\infty} -\infty$.

Correction :

1. Remarquons que

$$P_n' = \sum_{k=0}^n \frac{k X^{k-1}}{k!}$$

Le terme pour $k = 0$ étant nul, la somme commence en fait en 1, et alors on peut simplifier par k ce qui donne :

$$\begin{aligned} P_n' &= \sum_{k=1}^n \frac{X^{k-1}}{(k-1)!} \\ &= \sum_{k=0}^{n-1} \frac{X^k}{k!} \\ &= P_n - \frac{X^n}{n!} \end{aligned}$$

Soit $z \in \mathbb{C}$ une racine complexe de P_n . Si z est racine multiple, alors z est aussi racine de P_n' donc est racine de $X^n/n! = P_n' - P_n$. Par conséquent, $z = 0$ car c'est la seule racine de ce polynôme, ce qui est absurde car 0 n'est pas racine de P_n puisque $P_n(0) = 1$. En conclusion, les racines complexes de P_n sont toutes simples.

2. Montrons le résultat par récurrence.

- Pour $n \geq 0$ on note l'hypothèse H_n : « P_{2n} n'a aucune racine réelle, P_{2n+1} a une unique racine réelle a_n , et celle-ci est non nulle. »
- Montrons que H_0 est vraie. D'une part $P_{2 \times 0} = P_0 = 1$ et n'a aucune racine réelle, d'autre part $P_{2 \times 0 + 1} = 1 + X$ a une unique racine réelle, -1 , qui est bien non nulle. Par conséquent, H_0 est vraie.
- Soit $n \geq 0$. Supposons H_n vraie et montrons que H_{n+1} est vraie, c'est-à-dire qu'on veut montrer que P_{2n+2} ne s'annule jamais sur \mathbb{R} , que P_{2n+3} s'annule une unique fois sur \mathbb{R} , et que son unique racine n'est pas nulle. On déduit des calculs de la question 1 que $P_{2n+2}' = P_{2n+1}$. Or, par hypothèse de récurrence, P_{2n+1} s'annule une unique fois en a_{2n+1} . On en déduit que P_{2n+1} est de signe constant sur chacun des intervalles $]-\infty; a_n]$ et $[a_n; +\infty[$. En effet, par exemple sur $] \infty; a_n]$, s'il existe deux réels x_0 et x_1 avec $f(x_0) > 0$ et $f(x_1) < 0$ alors, P_{2n+1} étant polynomiale (on confond encore polynôme et fonction polynomiale associée), elle est continue, et d'après le théorème des valeurs intermédiaires, elle s'annule sur $]x_0; x_1[$ ce qui est exclu. De plus, son coefficient dominant étant égal à $1/(n+1)!$, c'est-à-dire un nombre positif, et son degré étant impair :

$$P_{2n+1}(x) \xrightarrow{x \rightarrow +\infty} +\infty \quad \text{et} \quad P_{2n+1}(x) \xrightarrow{x \rightarrow -\infty} -\infty$$

On en déduit le tableau de signes de P_{2n+1} et le tableau de variations de P_{2n+2} :

	$-\infty$	a_n	$+\infty$
$P_{2n+1}(x)$	$-$	0	$+$
P_{2n+2}	\searrow $P_{2n+2}(a_n)$ \nearrow		

Or, on a également $P_{2n+2} = P_{2n+1} + \frac{X^{2n+2}}{(2n+2)!}$ donc :

$$P_{2n+2}(a_n) = P_{2n+1}(a_n) + \frac{a_n^{2n+2}}{(2n+2)!} = \frac{a_n^{2n+2}}{(2n+2)!} > 0$$

puisque par hypothèse de récurrence, a_n est non nul. D'après le tableau de variations, P_{2n+2} est strictement positif sur \mathbb{R} donc ne s'annule jamais. De plus, on en déduit que P_{2n+3} est strictement croissante sur \mathbb{R} (car sa dérivée P_{2n+2} est strictement positive sur \mathbb{R}) et de même que précédemment

$$P_{2n+3}(x) \xrightarrow{x \rightarrow +\infty} +\infty \quad \text{et} \quad P_{2n+3}(x) \xrightarrow{x \rightarrow -\infty} -\infty$$

P_{2n+3} étant continue sur \mathbb{R} et strictement croissante, d'après le corollaire du théorème des valeurs intermédiaires, P_{2n+3} s'annule une unique fois sur \mathbb{R} . Notons a_{n+1} son unique racine. Pour montrer que a_{n+1} est non nul, il suffit de montrer que $P_{2n+3}(0)$ est non nul, ce qu'on a déjà vu à la question 1. Finalement, H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout n .

3. P_{2n} et P_{2n+2} étant strictement positifs d'après la question précédente (je donne uniquement les tableaux de variations, les tableaux de signes s'en déduisent immédiatement) :

	$-\infty$	a_n	$+\infty$
P_{2n}	$+$		
P_{2n+1}	\nearrow 0 \nearrow $-\infty$		

	$-\infty$	a_{n+1}	$+\infty$
P_{2n+2}	$+$		
P_{2n+3}	\nearrow 0 \nearrow $-\infty$		

4. D'après la question 3, pour tout $n \in \mathbb{N}$: $P_{2n+1}(0) = 1 > 0$, et d'après la question précédente, cela donne le résultat voulu : $\forall n \in \mathbb{N} \quad a_n < 0$.

5. (a) Soit $p \leq n$. En mettant $(2n+3)^{2p}$ en facteur il vient

$$\frac{(2n+3)^{2p}}{(2p)!} - \frac{(2n+3)^{2p+1}}{(2p+1)!} = \frac{(2n+3)^{2p}}{(2p)!} \times \left(1 - \frac{2n+3}{2p+1}\right)$$

et puisque $n \geq p$, $2n+3 > 2p+1$. En d'autres termes

$$\forall p \leq n \quad \frac{(2n+3)^{2p}}{(2p)!} - \frac{(2n+3)^{2p+1}}{(2p+1)!} < 0$$

(b) Par définition de P_{2n+1} :

$$\begin{aligned}
P_{2n+1}(-2n-3) &= \sum_{k=0}^{2n+1} \frac{(-2n-3)^k}{k!} \\
&= (1 - (2n+3)) + \left(\frac{(2n+3)^2}{2!} - \frac{(2n+3)^3}{3!} \right) + \dots + \left(\frac{(2n+3)^{2n}}{(2n)!} - \frac{(2n+3)^{2n+1}}{(2n+1)!} \right)
\end{aligned}$$

Or, d'après la question précédente, tous les termes entre parenthèses sont strictement négatifs. On en déduit que $P_{2n+1}(-2n-3) < 0$ et d'après la question 3, $-2n-3 < a_n$.

(c) Tout d'abord :

$$P_{2n+3} = P_{2n+2} + \frac{X^{2n+3}}{(2n+3)!} = P_{2n+1} + \frac{X^{2n+2}}{(2n+2)!} + \frac{X^{2n+3}}{(2n+3)!}$$

En particulier

$$\begin{aligned}
P_{2n+3}(a_n) &= P_{2n+1}(a_n) + \frac{a_n^{2n+2}}{(2n+2)!} + \frac{a_n^{2n+3}}{(2n+3)!} \\
&= \frac{a_n^{2n+2}}{(2n+2)!} + \frac{a_n^{2n+3}}{(2n+3)!} \\
P_{2n+3}(a_n) &= \frac{a_n^{2n+2}}{(2n+2)!} \left(1 + \frac{a_n}{2n+3} \right)
\end{aligned}$$

D'une part, $\frac{a_n^{2n+2}}{(2n+2)!} > 0$ et d'autre part, d'après la question précédente :

$$1 + \frac{a_n}{2n+3} > 1 + \frac{-2n-3}{2n+3} = 0$$

On en déduit que $P_{2n+3}(a_n) > 0$ et d'après le tableau de signes de la fonction, $P_{2n+3}, a_{n+1} < a_n$: la suite (a_n) est décroissante.

6. La suite (a_n) est décroissante, ce qui implique que soit elle converge, soit elle diverge vers $-\infty$. Supposons qu'elle converge vers L . Soit $x \leq L$. La suite (a_n) étant décroissante :

$$\forall n \in \mathbb{N} \quad a_n \geq L \geq x$$

Toujours d'après le tableau de signes de P_{2n+1} , $P_{2n+1}(x) \leq 0$. Or, $P_{2n+1}(x) \xrightarrow[n \rightarrow +\infty]{} e^x$ et l'inégalité large passe à la limite. D'où $e^x \leq 0$: c'est absurde. On en déduit le résultat voulu.

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 $\hat{P} = \sum_{k=0}^n \overline{a_{n-k}} X^k$.

(a) Dans le cas particulier où $P = (3+i)X^4 + 2X^3 + (1+i)X^2 - 2024$, expliciter \hat{P} .

(b) On revient au cas général. Montrer que pour tout $z \in \mathbb{U}$, $\hat{P}(z) = z^n \overline{P(z)}$.

2. Si $P \in E$, que vaut $P\hat{P}$? En déduire le degré de \hat{P} .

3. Déterminer l'ensemble E .

Correction :

1. (a) La méthode est simple : on change l'ordre des coefficients (le coefficient dominant devient le terme constant, etc.) et on les conjugue. Ici, $n = 4$. Attention, le coefficient de P devant X est nul donc le coefficient de \hat{P} devant X^3 sera nul aussi. Dès lors :

$$\hat{P} = -2024X^4 + 0 \times X^3 + (1-i)X^2 + 2X + (3-i)$$

(b) Soit $z \in \mathbb{U}$. Rappelons que $\bar{z} = 1/z$ puisque z est de module 1.

$$\begin{aligned}\widehat{P}(z) &= \sum_{k=0}^n \overline{a_{n-k}} z^k \\ &= \sum_{j=0}^n \overline{a_j} z^{n-j} \quad j = n - k \\ &= z^n \sum_{j=0}^n \overline{a_j} \times \frac{1}{z^j} \\ &= z^n \sum_{j=0}^n \overline{a_j} \times \bar{z}^j \\ &= z^n \times \overline{\sum_{j=0}^n a_j z^j}\end{aligned}$$

ce qui est le résultat voulu.

(c) Soit $P \in E$. D'après la question précédente, pour tout $z \in \mathbb{U}$:

$$\begin{aligned}P(z) \times \widehat{P}(z) &= z^n \times P(z) \times \overline{P(z)} \\ &= z^n \times |P(z)|^2\end{aligned}$$

Or, $P \in E$ et $z \in \mathbb{U}$ donc $P(z) \in \mathbb{U}$ si bien que $|P(z)|^2 = 1$ donc $P(z) \times \widehat{P}(z) = z^n$. En d'autres termes, les polynômes $P \times \widehat{P}$ et X^n coïncident sur \mathbb{U} qui est un ensemble infini donc sont égaux : $P \times \widehat{P} = X^n$. Par conséquent, $\deg(P) + \deg(\widehat{P}) = n$. Or, $\deg(P) = n$ donc $\deg(\widehat{P}) = 0$.

(d) On en déduit que si $P \in E$ alors \widehat{P} est constant non nul. En d'autres termes, tous les coefficients des X^k , pour $k \geq 1$, de \widehat{P} sont nuls donc $a_{n-k} = 0$ pour tout $k \geq 1$. En d'autres termes, tous les coefficients de P sont nuls à part a_n (tous les a_{n-k} pour $k \geq 1$, cela donne a_{n-1}, \dots, a_0). On en déduit que $P = a_n X^n$: on vient de finir la partie analyse du problème.

Synthèse : soit P de la forme $a_n X^n$ avec $a_n \in \mathbb{C}^*$, cherchons si $P \in E$. Soit $z \in \mathbb{U}$. Alors $P(z) = a_n z^n$ donc $|P(z)| = |a_n|$ puisque $z \in \mathbb{U}$. En particulier, $P(z) \in \mathbb{U}$ si et seulement si $|a_n| = 1$. En conclusion, E est l'ensemble des polynômes de la forme $a_n X^n$ avec $|a_n| = 1$.

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 $R = P - Q$.

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

Correction :

- P et $P - 1$ n'ont aucune racine commune car, si z est une racine de P , alors $P(z) - 1 = -1 \neq 0$. Par conséquent, si z est une racine de $P \wedge P'$, alors z est une racine de P donc n'est pas racine de $P - 1$ donc n'est pas un racine de $(P - 1) \wedge P'$: $P \wedge P'$ et $(P - 1) \wedge P'$ n'ont aucune racine complexe commune donc sont premiers entre eux.
- Les racines communes de P et Q sont racines de R , ainsi que les racines de $P - 1$ et $Q - 1$ puisqu'on a également $R = (P - 1) - (Q - 1)$. Or, P et $P - 1$ n'ont aucune racine commune : on peut donc sommer leur nombre de racines distinctes.

D'après l'exercice 28, le nombre de racines distinctes de P est $\deg(P) - \deg(P \wedge P')$ et le nombre de racines distinctes de $P - 1$ est $\deg(P - 1) - \deg((P - 1) \wedge (P - 1)') = \deg(P) - \deg((P - 1) \wedge P')$. Par conséquent, R admet au moins

$$k = \deg(P) - \deg(P \wedge P') + \deg(P) - \deg((P - 1) \wedge P') = 2 \deg(P) - (\deg(P \wedge P') + \deg((P - 1) \wedge P'))$$

racines distinctes. Or, d'après la question précédente, les deux PGCD sont premiers entre eux et divisent P' donc leur produit divise P' . En particulier, leur produit a un degré inférieur à celui de P' : en d'autres termes, $\deg(P \wedge P') + \deg((P - 1) \wedge P') \leq n - 1$ donc le nombre de racines distinctes de R est supérieur à k qui est lui-même supérieur à $2n - (n - 1) = n + 1$ mais $\deg(R) \leq n$ donc R est le polynôme nul : $P = Q$.

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

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

On pourra utiliser l'exercice 28.

Correction : Notons $E = \{x_1; \dots; x_n\}$ si bien que $\text{card}(E) = n$. $P^{-1}(E)$ est l'union disjointes des antécédents des x_i si bien que

$$\text{card}(P^{-1}(E)) = \sum_{i=1}^n \text{card} P^{-1}(\{x_i\})$$

Soit $i \in \llbracket 1; n \rrbracket$. $P^{-1}(\{x_i\})$ est l'ensemble des racines distinctes du polynôme $P - x_i$. D'après l'exercice 28, cet ensemble a $\deg(P - x_i) - \deg((P - x_i) \wedge (P - x_i)') = \deg(P) - \deg((P - x_i) \wedge P')$ éléments donc :

$$\text{card}(P^{-1}(E)) = \sum_{i=1}^n \deg(P) - \deg((P - x_i) \wedge P') = n \deg(P) - \sum_{i=1}^n \deg((P - x_i) \wedge P')$$

Or, les $P - x_i$ n'ont aucune racine complexe commune donc sont premiers entre eux donc les $(P - x_i) \wedge P'$ aussi et ceux-ci divisent P' donc leur produit divise P' donc

$$\sum_{i=1}^n \deg((P - x_i) \wedge P') \leq \deg(P') = \deg(P) - 1$$

On en déduit que :

$$\text{card}(P^{-1}(E)) \geq n \deg(P) - (\deg(P) - 1)$$

ce qui est le résultat voulu puisque $n = \text{card}(E)$.

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 $\mathbb{R}[X]$.

Correction :

1. On a :

$$\begin{aligned} P(j) &= (j^2 - 1)^2 - 3j(j^2 + 1) \\ &= j^4 - 2j^2 + 1 - 3j^3 - 3j \\ &= j - 2j^2 + 1 - 3 - 3j \\ &= -2(j^2 + j + 1) \\ &= 0 \end{aligned}$$

De plus, P est à coefficients réels donc $\bar{j} = j^2$ est aussi racine de P .

2. P est donc divisible par $(X - j)(X - j^2) = X^2 + X + 1$. Or,

$$P = X^4 - 3X^3 - 2X^2 - 3X + 1$$

En effectuant la division euclidienne de P par $X^2 + X + 1$, on trouve : $P = (X^2 + X + 1)(X^2 - 4X + 1)$. Or,

$X^2 - 4X + 1 = (X - x_1)(X - x_2)$ avec $x_{1,2} = \frac{4 \pm \sqrt{12}}{2} = 2 \pm \sqrt{3}$. Finalement :

$$P = (X^2 + X + 1)(X - 2 + \sqrt{3})(X - 2 - \sqrt{3})$$

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

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

Correction : Aucune méthode ne semble fonctionner : regardons pour de petites valeurs de n pour nous donner une idée. On a $P_1 = 1 - X = -(X-1)$ qui est déjà sous forme factorisée. On a également

$$P_2 = 1 - X + \frac{X(X-1)}{2!} = (1-X) \times \left(1 - \frac{X}{2!}\right) = (1-X) \times \left(\frac{2-X}{2!}\right) = \frac{1}{2!}(1-X)(2-X)$$

Finalement, $P_2 = (X-1)(X-2)/2!$. Montrons par récurrence que, pour tout $n \geq 1$,

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

Le résultat est vrai aux rangs 1 et 2. Soit $n \geq 2$: supposons le résultat vrai au rang n et prouvons qu'il l'est encore au rang $n+1$. Remarquons qu'on passe de P_n à P_{n+1} en ajoutant un terme. Plus précisément,

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

Par hypothèse de récurrence,

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

On peut factoriser par P_n qui est en facteur dans les deux termes :

$$P_{n+1} = \frac{(-1)^n}{n!} \times (X-1) \cdots (X-n) \times \left(1 - \frac{X}{n+1}\right) = \frac{(-1)^n}{n!} \times (X-1) \cdots (X-n) \times \left(\frac{n+1-X}{n+1}\right)$$

ce qui permet de conclure en remarquant que $n+1-X = (-1) \times (X-(n+1))$ et que $n! \times (n+1) = (n+1)!$.

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

Correction : À l'aide du triangle de Pascal :

$$P_7 = 7X^6 + 21X^5 + 35X^4 + 35X^3 + 21X^2 + 7X$$

On rappelle que $j^3 = 1, j^4 = j, j^5 = j^2, j^6 = 1$ et $j^7 = j$. Le résultat en découle : $P_7(j) = 42 + 42j + 42j^2 = 0$: j est racine de P_7 . De plus, P_7 étant à coefficients réels, $j^2 = \bar{j}$ est également racine de P_7 , ce qui implique que $(X-j)(X-j^2) = 1 + X + X^2$ divise P_7 . On cherche à présent des racines évidentes, jusqu'à obtenir un polynôme de degré 2. En évaluant en $x = 0$ et $x = -1$, on trouve que 0 et -1 sont racines évidentes. Ainsi, P est divisible par $X(X+1)(X^2+X+1)$: il existe un polynôme Q tel que $P = X(X+1)(X^2+X+1)Q$. Or, P est de degré 6 donc $\deg(Q) = 2$ et il existe a, b, c réels tels que $Q = aX^2 + bX + c$. En développant il vient

$$P = aX^6 + (2a+b)X^5 + (c+2b+2a)X^4 + (2c+2b+a)X^3 + (2c+b)X^2 + cX$$

Par unicité des coefficients, on obtient :

$$Q = 7X^2 + 7X + 7 = 7(X^2 + X + 1)$$

Finalement, $P_7 = 7X(X+1)(X^2+X+1)^2$.

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

Correction : Notons $P_1 = X^8 + X^4 + 1$ et $P_2 = X^{12} + 1$. Soit $z \in \mathbb{C}$. z est racine de P_2 si et seulement si $z^{12} = -1$. Or, $-1 = e^{i\pi}$: les racines 12-ièmes de -1 (cf. chapitre 7) sont donc les

$$e^{i\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right)}$$

pour $k \in \llbracket 0; 11 \rrbracket$. On a un polynôme de degré 12 avec 12 racines distinctes donc elles sont simples, le polynôme est unitaire, donc on trouve (sur \mathbb{C}) :

$$P_2 = \prod_{k=0}^{11} \left(X - e^{i\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right)}\right)$$

Pour factoriser sur \mathbb{R} , il faut regrouper les racines conjuguées. Explicitons le produit ci-dessus :

$$P_2 = (X - e^{i\pi/12})(X - e^{3i\pi/12})(X - e^{5i\pi/12})(X - e^{7i\pi/12})(X - e^{9i\pi/12})(X - e^{11i\pi/12}) \\ \times (X - e^{13i\pi/12})(X - e^{15i\pi/12})(X - e^{17i\pi/12})(X - e^{19i\pi/12})(X - e^{21i\pi/12})(X - e^{23i\pi/12})$$

Or, $e^{23i\pi/12} = \overline{e^{i\pi/12}}$. En effet :

$$\overline{e^{i\pi/12}} = e^{-i\pi/12} \\ = e^{2i\pi - i\pi/12}$$

ce qui donne le résultat voulu. De même, $e^{21i\pi/12} = \overline{e^{3i\pi/12}}$ et ainsi de suite. En regroupant chaque terme (correspondants aux indices de k allant de 0 à 5) avec son conjugué :

$$P_2 = \prod_{k=0}^5 \left(X - e^{i\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right)} \right) \times \left(X - \overline{e^{i\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right)}} \right) \\ = \prod_{k=0}^5 \left(X^2 - 2X \cos\left(\frac{\pi}{12} + \frac{2k\pi}{12}\right) + 1 \right)$$

Passons à P_1 . Il suffit de voir que $P_1 = (X^4)^2 + X^4 + 1$. Soit $z \in \mathbb{C}$. Alors z est racine de P_1 si et seulement si z_1^4 est racine de $X^2 + X + 1$ si et seulement si z_1 est quatrième des racines de $X^2 + X + 1$ c'est-à-dire j et j^2 . Or :

$$j = e^{2i\pi/3} \quad \text{et} \quad j^2 = e^{4i\pi/3}$$

Toujours d'après le chapitre 7, les racines quatrièmes de j sont les $e^{i\left(\frac{2\pi}{12} + \frac{2k\pi}{4}\right)}$ pour $k \in \llbracket 0; 3 \rrbracket$ et les racines quatrièmes de j^2 sont les $e^{i\left(\frac{4\pi}{12} + \frac{2k\pi}{4}\right)}$. On en déduit la factorisation sur \mathbb{C} :

$$P_1 = \prod_{k=0}^3 \left(X - e^{i\left(\frac{\pi}{6} + \frac{k\pi}{2}\right)} \right) \times \prod_{k=0}^3 \left(X - e^{i\left(\frac{\pi}{3} + \frac{k\pi}{2}\right)} \right)$$

De même :

$$P_1 = (X - e^{i\pi/6})(X - e^{4i\pi/6})(X - e^{7i\pi/6})(X - e^{10i\pi/6})(X - e^{2i\pi/6})(X - e^{5i\pi/6})(X - e^{8i\pi/6})(X - e^{11i\pi/6})$$

Attention, il y a des trous, il manque des termes (par exemple $e^{3i\pi/6}$) donc on ne peut pas mettre un symbole \prod . Tant pis, on le fait à la main. On regroupe les termes conjugués entre eux ($e^{i\pi/6}$ avec $e^{11i\pi/6}$, $e^{2i\pi/6}$ avec $e^{10i\pi/6}$, $e^{4i\pi/6}$ avec $e^{8i\pi/6}$ et enfin $e^{5i\pi/6}$ avec $e^{7i\pi/6}$), on trouve de même :

$$P_1 = (X^2 - 2X \cos(\pi/6) + 1)(X^2 - 2X \cos(2\pi/6) + 1)(X^2 - 2X \cos(4\pi/6) + 1)(X^2 - 2X \cos(5\pi/6) + 1)$$

Avec les valeurs explicites des cosinus :

$$P_1 = (X^2 - X\sqrt{3} + 1)(X^2 - X + 1)(X^2 + X + 1)(X^2 + X\sqrt{3} + 1)$$

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

Correction :

1. 1 n'est pas racine de P . Soit $z \in \mathbb{C} \setminus \{1\}$. Alors :

$$P(z) = 0 \iff \frac{1 - z^{n+1}}{1 - z} = 0 \\ \iff z^{n+1} = 1 \\ \iff \exists k \in \llbracket 1; n \rrbracket, z = e^{2ik\pi/(n+1)}$$

On a pris $k \in \llbracket 1; n \rrbracket$ et non pas $\llbracket 0; n \rrbracket$ car on a supposé $z \neq 1$. P étant de degré n et admettant n racines distinctes, elles sont simples, et P étant unitaire :

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

Deuxième méthode : à l'aide du chapitre 20. Une fois que l'on connaît les fractions rationnelles, il suffit de voir que

$$P = \frac{X^{n+1} - 1}{1 - X}$$

On retrouve le même résultat (encore heureux : il y a unicité!) en se souvenant (cf. cours) que la factorisation de $X^p - 1$ est $\prod_{k=0}^{p-1} \left(X - e^{2ik\pi/p} \right)$ et en simplifiant par $X - 1$ qui est le terme pour $k = 0$.

2. En évaluant en 1, d'une part, $P(1) = n + 1$, et d'autre part :

$$\begin{aligned} P(1) &= \prod_{k=1}^n \left(1 - e^{2ik\pi/(n+1)} \right) \\ &= \prod_{k=1}^n e^{ik\pi/(n+1)} \left(e^{-ik\pi/(n+1)} - e^{ik\pi/(n+1)} \right) && \text{(angle moitié)} \\ &= \prod_{k=1}^{n+1} e^{ik\pi/(n+1)} \times \prod_{k=1}^n (-2i) \times \sin \left(\frac{k\pi}{n+1} \right) \\ &= e^{\sum_{k=1}^{n+1} ik\pi/(n+1)} \times (-2i)^n \prod_{k=1}^n \sin \left(\frac{k\pi}{n+1} \right) \\ &= e^{i(n+1)(n+2)\pi/2(n+1)} \times (-2)^n \times e^{in\pi/2} \prod_{k=1}^n \sin \left(\frac{k\pi}{n+1} \right) \\ &= e^{i(2n+2)\pi/2} \times (-2)^n \times \prod_{k=1}^n \sin \left(\frac{k\pi}{n+1} \right) \\ &= (e^{i\pi})^{n+1} \times (-2)^n \times \prod_{k=1}^n \sin \left(\frac{k\pi}{n+1} \right) \\ &= (-1)^{n+1} \times (-2)^n \times \prod_{k=1}^n \sin \left(\frac{k\pi}{n+1} \right) \end{aligned}$$

Finalement :

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

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

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

Correction : On définit le polynôme

$$Q = \prod_{k=1}^n (X - e^{2ik\pi/n})$$

si bien que $P = Q(1)$. Or, Q est presque égal à

$$R = \prod_{k=0}^{n-1} (X - e^{2ik\pi/n}) = X^n - 1$$

Finalement, $X^n - 1 = (X - 1) \times Q$ (je préfère ne pas faire de quotient de polynômes avant le chapitre suivant). Or, on a aussi : $X^n - 1 = (X - 1)(1 + X + \dots + X^{n-1})$. Un polynôme non nul étant régulier puisque $\mathbb{K}[X]$ est un anneau intègre :

$$Q = 1 + X + \dots + X^{n-1}$$

si bien que $P = Q(1) = n$.

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 $1 + X + \dots + X^{2p-1}$. En déduire que

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

Correction :

1. À savoir faire :

$$X^{2p} - 1 = (X - 1)(X + 1) \prod_{k=1}^{n-1} (X^2 - 2 \cos(k\pi/n)X + 1)$$

2. Raisonnons avec les outils du chapitre suivant : on a

$$\begin{aligned} 1 + X + \dots + X^{2p-1} &= \frac{X^{2p} - 1}{X - 1} \\ &= \frac{(X - 1)(X + 1) \prod_{k=1}^{n-1} (X^2 - 2 \cos(k\pi/n)X + 1)}{X - 1} \\ &= (X + 1) \prod_{k=1}^{n-1} (X^2 - 2 \cos(k\pi/n)X + 1) \end{aligned}$$

Ensuite on fait comme dans l'exercice précédent : on évalue en 1, on utilise la formule de trigo $1 - \cos(2u) = 2 \sin^2(u)$ et on utilise le fait que pour tout $k \in \llbracket 1; p-1 \rrbracket$, $k\pi/2p \in [0; \pi/2]$ donc $\sin(k\pi/2p) \geq 0$ si bien que $\sqrt{\sin^2(k\pi/2p)} = \sin(k\pi/2p)$ et on trouve la valeur voulue.

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 $|P(z)| \geq |\operatorname{Im}(z)|^n$ pour tout $z \in \mathbb{C}$.

Correction : P est scindé sur \mathbb{R} si et seulement si ses racines complexes sont toutes réelles i.e. ont toutes une partie imaginaire nulle.

Supposons que $|P(z)| \geq |\operatorname{Im}(z)|^n$ pour tout $z \in \mathbb{C}$. C'est en particulier vrai si z est une racine de P , ce qui donne : $0 \geq |\operatorname{Im}(z)|^n$ donc $\operatorname{Im}(z) = 0$. En d'autres termes, les racines complexes de P sont toutes réelles, P est scindé sur \mathbb{R} .

Réciproquement, supposons P scindé sur \mathbb{R} , notons x_1, \dots, x_n les racines réelles de P (pas forcément distinctes) et P étant unitaire :

$$P = (X - x_1) \cdots (X - x_n)$$

Soit $z \in \mathbb{C}$. $|P(z)| = |z - x_1| \times \dots \times |z - x_n|$. Or, le module d'un complexe est supérieur à la valeur absolue de sa partie imaginaire (cf. chapitre 7) donc, pour tout i , $|z - x_i| \geq |\operatorname{Im}(z - x_i)| = |\operatorname{Im}(z)|$ puisque x_i est un réel. Par produit d'inégalités positives, on en déduit que $|P(z)| \geq |\operatorname{Im}(z)|^n$.

Exercice 45 : ♦♦

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

Correction :

1. Si $k \in \llbracket 1; n+1 \rrbracket$, le fait que $P(k) = 1/k^2$ implique que $k^2 P(k) - 1 = 0$, c'est-à-dire que $Q(k) = 0 : k$ est racine de Q . Dès lors, Q est divisible par $B = (X-1) \times \cdots \times (X-(n+1))$. Or, $\deg(P) = n$ donc $\deg(Q) = n+2$. Or, $\deg(B) = n+1$: le quotient est donc de degré 1. Il existe ainsi $(a, b) \in \mathbb{R}^2$ tels que $Q = (X-1) \times \cdots \times (X-n-1) \times (aX+b)$. Comme P est unitaire, Q l'est aussi donc $a = 1$. Nous avons exploité toutes les informations : pour obtenir la valeur de b , il nous faut une nouvelle équation. On remarque que $Q(0) = -1$, ce qui donne :

$$(-1) \times \cdots \times (-n-1) \times b = (-1)^{n+1}(n+1)!b = -1$$

si bien que $b = (-1)^n/(n+1)!$. Enfin,

$$\begin{aligned} Q(n+2) &= (n+2-1) \times \cdots \times (n+2-n-1) \times \left(n+2 + \frac{(-1)^n}{(n+1)!} \right) \\ &= (n+1) \times \cdots \times (1) \times \left(\frac{(n+2)(n+1)! + (-1)^n}{(n+1)!} \right) \\ &= (n+1)! \times \left(\frac{(n+2)! + (-1)^n}{(n+1)!} \right) \\ &= (n+2)! + (-1)^n. \end{aligned}$$

En conclusion, $P(n+2) = \frac{Q(n+2) + 1}{(n+2)^2} = \frac{(n+2)! + (-1)^n + 1}{(n+2)^2}$.

2. Posons $Q = (X+1) \times P - X$. Alors Q est de degré $n+1$ et s'annule en tous les $k \in \llbracket 0; n \rrbracket$ donc admet $n+1$ racines distinctes : si on note a_n le coefficient dominant de P , c'est aussi le coefficient dominant de Q donc $Q = a_n X(X-1) \cdots (X-n)$. On en déduit que $Q(n+1) = a_n \times n(n-1) \times \cdots \times 1 = a_n \times n!$. Dès lors :

$$P(n+1) = \frac{Q(n+1)}{(n+2)} + n+1 = \frac{a_n \times n!}{n+2} + n+1$$

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

Correction : Notons h la raison de la progression arithmétique entre les trois (car de degré 3) racines de P . On pourrait noter les racines $a, a+h, a+2h$ mais on va plutôt les noter $a-h, a, a+h$ pour avoir un problème plus symétrique et pour simplifier les calculs. On a trois racines distinctes donc elles sont simples puisque $\deg(P) = 3$, et P est de coefficient dominant égal à 8 donc :

$$P = 8(X-a)(X-a+h)(X-a-h)$$

En développant, il vient :

$$\begin{aligned} P &= 8X^3 - 8 \times 3aX^2 + 8[a(a-h) + a(a+h) + (a-h)(a+h)]X - 8a(a-h)(a+h) \\ &= 8X^3 - 24aX^2 + 8(a^2 - ah + a^2 + ah + a^2 - h^2)X - 8a(a^2 - h^2) \\ &= 8X^3 - 24aX^2 + 8(3a^2 - h^2)X - 8a(a^2 - h^2) \end{aligned}$$

Par unicité des coefficients :

$$-24a = -12, 8(3a^2 - h^2) = -2 \quad \text{et} \quad -8a(a^2 - h^2) = 3$$

On trouve donc $a = 1/2$ et $h^2 = 1$ donc $a = \pm 1$ (il est logique qu'on trouve deux valeurs opposées de h , prendre l'une ou l'autre valeur de h ne fera qu'invertir $a-h$ et $a+h$). Finalement, les racines sont $1/2, 1/2 \pm 1$ c'est-à-dire $1/2, -1/2$ et $3/2$ si bien que :

$$P = 8 \left(X - \frac{1}{2} \right) \left(X + \frac{1}{2} \right) \left(X - \frac{3}{2} \right)$$

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

- Montrer que si A et B sont deux polynômes qui sont sommes de deux carrés (de polynômes), il en est de même pour AB .
- 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 $P = C^2 + XD^2$. Le sens indirect est immédiat : s'il existe C et D tels que $P = C^2 + XD^2$ alors P est positif sur \mathbb{R}_+ .

Correction :

1. Par hypothèse, il existe C, D, E, F dans $\mathbb{R}[X]$ tels que $A = C^2 + D^2$ et $B = E^2 + F^2$ donc

$$\begin{aligned} AB &= (C^2 + D^2)(E^2 + F^2) \\ &= C^2E^2 + C^2F^2 + D^2E^2 + D^2F^2 \\ &= C^2E^2 + 2CEDF + D^2F^2 + C^2F^2 - 2CEDF + D^2E^2 \\ &= (CE + DF)^2 + (CF - DE)^2 \end{aligned}$$

2. Il est évident qu'un polynôme somme de deux carrés est positif (rappelons qu'on se place sur $\mathbb{R}[X]$), prouvons la réciproque : supposons donc que P soit positif. Écrivons P comme produit de facteurs irréductibles sur \mathbb{R} :

$$P = a_n(X - x_1)^{\alpha_1} \cdots (X - x_r)^{\alpha_r} Q_1^{\beta_1} \cdots Q_s^{\beta_s}$$

où les Q_i sont des polynômes unitaires (car on a factorisé par le coefficient dominant de P) de degré 2 de discriminant strictement négatif. D'après la question précédente, il suffit de prouver que chacun des termes du produit est somme de deux carrés.

Tout d'abord, les α_i sont forcément pairs sinon P s'annule en changeant de signe en x_i ce qui est contraire à l'hypothèse $P(x) \geq 0$: il en découle que, pour tout i , $(X - x_i)^{\alpha_i} = ((X - x_i)^{\alpha_i/2})^2 + 0^2$.

De plus, $a_n > 0$ car P est positif (si $a_n < 0$ alors P tend vers $-\infty$ en $+\infty$ ce qui est exclu) donc $a_n = \sqrt{a_n^2} + 0^2$.

Soit $i \in \llbracket 1; s \rrbracket$. Prouvons enfin que Q_i est somme de deux carrés. Par produit, on en déduira que $Q_i^{\beta_i}$ l'est aussi et donc que P l'est ce qui terminera l'exercice. On note $Q = X^2 + bX + c$ avec $\Delta = b^2 - 4c < 0$. Il suffit d'écrire Q_i sous forme canonique :

$$\begin{aligned} Q_i &= X^2 + 2 \times b \times X + c \\ &= \left(X + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c \\ &= \left(X + \frac{b}{2}\right)^2 + \frac{4c - b^2}{4} \\ &= \left(X + \frac{b}{2}\right)^2 + \frac{-\Delta}{4} \\ &= \left(X + \frac{b}{2}\right)^2 + \left(\sqrt{\frac{-\Delta}{4}}\right)^2 \end{aligned}$$

ce qui permet de conclure (rappelons que $-\Delta > 0$).

3. Le raisonnement est le même.

Prouvons que cette propriété passe au produit i.e. si A et B vérifient cette propriété alors AB aussi. Supposons qu'il existe C, D, E, F tels que $A = C^2 + XD^2$ et $B = E^2 + XF^2$. Par conséquent :

$$\begin{aligned} AB &= C^2E^2 + X(C^2F^2 + D^2E^2) + X^2D^2F^2 \\ &= C^2E^2 + 2XCDEF + X^2D^2F^2 + X(C^2F^2 - 2CDEF + D^2E^2) \\ &= (CE + XCF)^2 + X(CF + DE)^2 \end{aligned}$$

Supposons que P soit positif sur \mathbb{R}_+ . Là aussi donnons la décomposition de P en produit de facteurs irréductibles :

$$P = a_n(X - x_1)^{\alpha_1} \cdots (X - x_r)^{\alpha_r} Q_1^{\beta_1} \cdots Q_s^{\beta_s}$$

Là aussi, il suffit de prouver que tous les éléments du produit vérifient la condition voulue.

De même que ci-dessus, $a_n > 0$ donc $a_n = \sqrt{a_n^2} + X \times 0^2$.

Soit $i \in \llbracket 1; r \rrbracket$. Si α_i est pair, alors $(X - x_i)^{\alpha_i} = ((X - x_i)^{\alpha_i/2})^2 + X \times 0^2$.

Supposons α_i impair. Si $x_i > 0$ alors P change de signe en x_i ce qui est exclu car P est positif sur \mathbb{R}_+ . Par conséquent, $x_i \leq 0$ donc $-x_i \geq 0$ si bien que $X - x_i = \sqrt{-x_i^2} + X \times 1^2$.

Passons aux polynômes Q_i qui sont de la forme $X^2 + bX + c$ avec $b^2 - 4c < 0$. Alors $c > 0$ sinon $b^2 - 4c \geq 0$. Par conséquent :

$$\begin{aligned} Q_i &= (X - \sqrt{c})^2 + 2\sqrt{c}X + bX \\ &= (X + \sqrt{c})^2 + X(b + 2\sqrt{c}) \end{aligned}$$

Or, $b^2 < 4c$ donc $|b| < 2\sqrt{c}$ donc $-b \leq |b| < 2\sqrt{c}$ si bien que $2\sqrt{c} + b > 0$ et donc on a finalement

$$Q_i = (X + \sqrt{c})^2 + X \times \sqrt{b + 2\sqrt{c}}^2$$

ce qui permet de conclure en passant au produit.

Exercice 48 : ★★ Soient a_1, \dots, 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).

Correction : Supposons que P s'écrive sous la forme $P = AB$ avec A et B dans $\mathbb{Z}[X]$. Supposons dans un premier temps que A et B soient non constants. En les évaluant en a_k , pour $k \in \llbracket 1; n \rrbracket$, on trouve $A(a_k) \times B(a_k) = P(a_k) = 1$. Puisque A et B sont à coefficients entiers, $A(a_k)$ et $B(a_k)$ appartiennent à \mathbb{Z} donc $A(a_k) = B(a_k) = \pm 1$. Précisons que P n'a aucune racine réelle puisque ne prend que des valeurs strictement positives sur \mathbb{R} (on identifie encore polynôme et fonction polynomiale). Dès lors, A et B (qui sont des fonctions continues, encore une fois en les identifiant à leur fonction polynomiale associée) sont de signe constant (à savoir faire!). Puisqu'elles coïncident en les a_k , elles sont de signe constant et de même signe : supposons sans perte de généralité que A et B sont strictement positives sur \mathbb{R} . On en déduit que :

$$\forall k \in \llbracket 1; n \rrbracket, A(a_k) = B(a_k) = 1$$

c'est-à-dire que les a_k sont racines de $A - 1$ et $B - 1$. Par conséquent, les a_k étant deux à deux distincts, $A - 1$ et $B - 1$ sont divisibles par $\prod_{k=1}^n (X - a_k)$ c'est-à-dire qu'il existe C et D dans $\mathbb{R}[X]$ (en fait dans $\mathbb{Z}[X]$ car on divise par un polynôme unitaire, cf. exercice sur l'âge du fils et l'âge du chien, mais nous n'en avons pas besoin ici) tels que

$$A = C \prod_{k=1}^n (X - a_k) + 1 \quad \text{et} \quad B = D \prod_{k=1}^n (X - a_k) + 1$$

A et B étant non constants, C et D sont non nuls donc $\deg(A) \geq n$ et $\deg(B) \geq n$. Or, $AB = P$ de degré $2n$ donc $2n = \deg(A) + \deg(B) \geq 2n$: il y a donc égalité, ce qui implique que C et D soient constants. En développant le produit AB :

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

Il en découle que $CD = 1$ et $C + D = 0$ ce qui n'est pas possible sur \mathbb{R} : c'est absurde. On en déduit que A ou B est constant. Supposons A constant : alors A fois le coefficient dominant de B donne le coefficient dominant de P c'est-à-dire 1, et puisqu'on a des entiers, A est 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 $R = XP' + P$.

Correction : P n'étant pas constant, P' est de degré $n - 1$ donc Q est de degré $n + 1$. De plus, XP' est aussi de degré n donc R est la somme de deux polynômes de même degré n : on en déduit que $\deg(P) \leq n$ mais pour donner le degré exact de R , il faut s'intéresser au coefficient dominant. Notons a_n le coefficient dominant de P (non nul par définition d'un coefficient dominant). Le coefficient dominant de XP' est donc na_n si bien que le coefficient devant X^n est $na_n + a_n = (n + 1)a_n \neq 0$ donc R est de degré n .

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 $n \geq 3$.

Correction : Analyse : si P convient. Alors $\deg(P) \geq 2$: en effet, rappelons que si P est de degré d alors $P^{(d+1)} = 0$. Rappelons aussi que si P est de degré $d \geq 0$, alors $P^{(d)}$ est constant non nul. On en déduit que P est de degré 2. Notons $P = aX^2 + bX + c$. Alors $P' = 2aX + b$ et $P'' = 2a$. On déduit des données de l'énoncé que $a = 2$ puis que $b = -7$ et enfin $c = 12$.

Synthèse : il est immédiat que $P = 2X^2 - 7X + 12$ convient. C'est donc l'unique solution du problème.

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 .

Correction : Il est immédiat que $Q(0) = 0$. Il suffit de prouver que $Q' = P$.

$$\begin{aligned} Q' &= \sum_{k=0}^n (-1)^k \times \frac{P^{(k+1)}(X) \times X^{k+1}}{(k+1)!} + \sum_{k=0}^n (-1)^k \times \frac{P^{(k)}(X) \times (k+1)X^k}{(k+1)!} \\ &= \sum_{j=1}^{n+1} (-1)^{j-1} \times \frac{P^{(j)}(X) \times X^j}{j!} + \sum_{k=0}^n (-1)^k \times \frac{P^{(k)}(X) \times X^k}{k!} \\ &= \sum_{k=1}^n P^{(k)}(X) \times (-1)^k \times \left(\frac{1}{k!} - \frac{1}{k!} \right) + (-1)^n \frac{P^{(n+1)}(X) \times X^{n+1}}{(n+1)!} + (-1)^0 \frac{P^{(0)}(X) \times X^0}{0!} \end{aligned}$$

Or, $P^{(n+1)}(X) = 0$ puisque $P \in \mathbb{K}_n[X]$. Tous les termes ci-dessus sont donc nuls à part le dernier qui 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.

Correction : Soient

$$P = \sum_{n=0}^{+\infty} (-1)^n a_n X^n \quad \text{et} \quad Q = \sum_{n=0}^{+\infty} (-1)^n b_n X^n$$

deux polynômes alternés i.e. avec (a_n) et (b_n) deux suites presque nulles positives. Par conséquent,

$$PQ = \sum_{n=0}^{+\infty} c_n X^n$$

avec, pour tout $n \in \mathbb{N}$:

$$\begin{aligned}
c_n &= \sum_{k=0}^n (-1)^k a_k (-1)^{n-k} b_{n-k} \\
&= \sum_{k=0}^n (-1)^n a_k b_{n-k} \\
&= (-1)^n \sum_{k=0}^n a_k b_{n-k}
\end{aligned}$$

Or, par somme et produit, la somme ci-dessus est positive si bien que c_n est égal à $(-1)^n$ multiplié par un terme positif : PQ est alterné.

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

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

Correction : Le degré d'un produit étant la somme des degrés :

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

Or, $\deg(P^k) = k \deg(P)$ si bien que :

$$\deg(P) = \sum_{\ell=1}^n \ell^2 \deg(64X^6 + 2024X^4 + \ell)$$

Finalement :

$$\begin{aligned}
\deg(P) &= \sum_{\ell=1}^n 6\ell^2 \\
&= n(n+1)(2n+1)
\end{aligned}$$

De plus le coefficient dominant est égal à

$$\prod_{\ell=1}^n 64^{\ell^2} = 64^{\sum_{\ell=1}^n \ell^2} = 64^{n(n+1)(2n+1)/6}$$

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 trapeuse, 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 ?

Correction :

1. L et P sont deux polynômes de degré inférieur ou égal à 2 qui coïncident en au moins trois points distincts (a_1, a_2 et a_3) donc ils sont égaux.
2. Comme en cours, le polynôme L est donné par (on n'oublie pas que $-(-1) = +1$)

$$L = 5 \times \frac{(X-2)(X+1)}{(1-2)(1+1)} + 3 \times \frac{(X-1)(X+1)}{(2-1)(2+1)} + 36 \times \frac{(X-1)(X-2)}{(-1-1)(-1-2)}$$

Après calculs, on trouve $L = \frac{9X^2}{2} - \frac{31X}{2} + 16$. Finalement, le code du coffre est $L(42) = 7303$.

3. (a) Le polynôme d'interpolation passant par les trois points $(1, 5), (2, 3)$ et $(42, \alpha)$ convient (et c'est même le seul!) :

$$Q = 5 \times \frac{(X-2)(X-42)}{(1-2)(1-42)} + 3 \times \frac{(X-1)(X-42)}{(2-1)(2-42)} + \alpha \times \frac{(X-1)(X-2)}{(42-1)(42-2)}$$

- (b) Pour tout $\alpha \in \mathbb{R}$, il existe un polynôme Q tel que $Q(1) = 10, Q(2) = 9$ et $Q(42) = \alpha$. Aucun réel n'est privilégié, et on ne peut exclure aucun réel : Pierre et Jules ne peuvent absolument pas deviner la combinaison du coffre : Pierre et Jules ne peuvent pas ouvrir le coffre sans Jean.

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

Correction : On a : $P^3 - Q^3 = (P - Q)(P^2 + PQ + Q^2)$ si bien que

$$\deg(P^3 - Q^3) = \deg(P - Q) + \deg(P^2 + PQ + Q^2)$$

Or, $P - Q \neq 0$ donc $\deg(P - Q) \geq 0$: il suffit donc de prouver que $P^2 + PQ + Q^2 \geq 2n$. Notons a_n le coefficient dominant de P et b_n le coefficient dominant de Q (réels et non nuls par définition d'un coefficient dominant). On a des produits de polynômes de degré n donc on a des polynômes de degré $2n$. Plus précisément, le coefficient de X^{2n} dans l'écriture de $P^2 + PQ + Q^2$ est $a_n^2 + a_nb_n + b_n^2$. Or :

$$a_n^2 \pm 2a_nb_n + b_n^2 = (a_n \pm b_n)^2 \geq 0$$

si bien que $a_n^2 + b_n^2 \geq 2|a_nb_n| > |a_nb_n| \geq -a_nb_n$ (l'inégalité stricte vient du fait que a_nb_n n'est pas nul). Par conséquent, $a_n^2 + a_nb_n + b_n^2 > 0$ donc $P^2 + PQ + Q^2$ est de degré $2n$ ce qui est le résultat voulu. Le résultat est faux sur \mathbb{C} car on peut avoir $P = jQ$ et alors $P^3 = Q^3$ donc $P^3 - Q^3 = 0$ qui est de degré $-\infty$.

Exercice 56 : $\star\star$ 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.

Correction : Soit $\alpha \in \mathbb{K}$. D'après la formule de Taylor :

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

Soit $x \in \mathbb{K}$. En évaluant cette égalité en $x+1$:

$$P(x+1) = \sum_{n=1}^{+\infty} \frac{P^{(n)}(\alpha) \times (x+1 - \alpha)^n}{n!}$$

α étant quelconque, cette égalité est vraie pour $\alpha = x$ si bien que :

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

Par conséquent, les deux polynômes $P(X+1)$ et $\sum_{n=1}^{+\infty} \frac{P^{(n)}(X)}{n!}$ sont égaux car coïncident en tout point.

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 $P(X^2) = (X^2+1)P(X)$ (débrouillez-vous!).

Correction :

1. On veut s'intéresser au degré : rappelons que, si on veut donner le degré de P' en fonction du degré de P , il faut séparer les cas selon que P est constant ou non. Le polynôme nul est évidemment solution. Si P est constant non nul, alors P n'est pas solution car $P(2X)$ est constant non nul et P' est nul. Examinons le cas où P est de degré 1 (car alors P' est constant et on s'intéresse au degré de P''). Si P est constant alors $P'' = 0$ et $P(2X)$ n'est pas nul donc P n'est pas solution. Supposons à présent P de degré $n \geq 2$.

Analyse : si P convient. P étant de degré $n \geq 2$, P' est de degré $n-1$ et P'' de degré $n-2$. Alors $\deg(P(2X)) = \deg(P) \times \deg(2X) = \deg(P) = n$ et $\deg(P' \times P'') = \deg(P') + \deg(P'') = n-1 + n-2 = 2n-3$. Puisque P est solution, alors $P(2X) = P' \times P''$ donc en particulier ils ont le même degré, c'est-à-dire que $n = 2n-3$ donc $n = 3$. Il en découle qu'il existe a, b, c, d tels que $P = aX^3 + bX^2 + cX + d$. D'une part :

$$\begin{aligned} P(2X) &= a(2X)^3 + b(2X)^2 + c(2X) + d \\ &= 8aX^3 + 4bX^2 + 2cX + d \end{aligned}$$

et d'autre part, $P' = 3aX^2 + 2bX + c$ et $P'' = 6aX + 2b$ si bien que

$$P' \times P'' = 18a^2X^3 + 18abX^2 + (6ac + 4b^2)X + 2bc$$

Par unicité des coefficients :

$$8a = 18a^2, 4b = 18ab, 2c = 6ac + 4b^2 \quad \text{et} \quad d = 2bc$$

Or, P est supposé de degré 3 donc $a \neq 0$ (sinon P n'est pas de degré 3) donc $18a = 8$ si bien que $a = 4/9$. Par conséquent, $4b = 8b$ (on réinjecte dans la deuxième égalité) donc $b = 0$. Avec la troisième équation, on trouve $2c = 8c/3$ donc $c = 0$ et $d = 2bc = 0$. Finalement, $P = 4X^3/9$.

Synthèse : Posons $P = 4X^3/9$. Alors $P(2X) = 32X^3/9$ et $P' = 12X^2/9 = 4X^2/3$ et $P'' = 8X/3$ si bien que $P' \times P'' = 32X^3/9 = P(2X)$: P est bien solution. En conclusion, les seules solutions sont le polynôme nul et $4X^3/9$.

2. Suivons l'indication de l'énoncé et cherchons les racines des solutions éventuelles (la démarche précédente ne fonctionne pas ici puisque les deux membres de l'égalité ont le même degré : $\deg(P) + 1$). **Analyse :** Soit P un polynôme qui convient. Alors $(X+4)P(X) = XP(X+1)$. En évaluant en 0 : $4P(0) = 0 \times P(1) = 0$ donc $P(0) = 0$: 0 est racine de P . Par conséquent, P est divisible par X : il existe $Q \in \mathbb{R}[X]$ tel que $P = XQ$. En réinjectant dans l'égalité, cela donne :

$$(X+4)XQ(X) = X(X+1)Q(X+1)$$

puisque $P(X) = XQ(X)$ donc $P(X+1) = (X+1)Q(X+1)$. De même, en évaluant en -1 : $(-3)(-1)Q(-1) = (-1) \times 0 \times Q(0)$ donc $Q(-1) = 0$: -1 est racine de Q , Q est donc divisible par $X+1$ (et pas $X-1$: α est racine de Q si et seulement si Q est divisible par $X-\alpha$) donc il existe R tel que $Q(X) = (X+1)R(X)$. En réinjectant dans l'égalité :

$$(X+4)X(X+1)R(X) = X(X+1)(X+2)R(X+1)$$

De même, -2 est racine de R donc il existe S tel que $R(X) = (X+2)S(X)$ et donc :

$$(X+4)X(X+1)(X+2)S(X) = X(X+1)(X+2)(X+3)S(X+1)$$

De même, -3 est racine de S donc il existe T tel que $S(X) = (X+3)T(X)$ et donc :

$$(X+4)X(X+1)(X+2)(X+3)T(X) = X(X+1)(X+2)(X+3)(X+4)T(X+1)$$

Ici, par contre, cette méthode ne marche plus : si on évalue en -4 , cela donne $0 \times \dots \times T(-4) = 0$ mais puisqu'on multiplie $T(-4)$ par 0 , on ne peut pas affirmer que $T(-4)$ est nul. Dans l'égalité ci-dessus, simplifions par $X(X+1)(X+2)(X+3)(X+4)$ (on peut simplifier par un polynôme non nul, $\mathbb{K}[X]$ est un anneau intègre, tout élément non nul est régulier) ce qui donne $T(X) = T(X+1) : T$ est périodique donc est constant (cf. cours, ce n'est pas explicitement au programme, à savoir redémontrer!) disons constant égal à λ . Par conséquent, $S = \lambda(X+3)$, $R = \lambda(X+2)(X+3)$, $Q = \lambda(X+1)(X+2)(X+3)$ et finalement $P = \lambda X(X+1)(X+2)(X+3)$.

Synthèse : Soit $\lambda \in \mathbb{R}$ et soit $P = \lambda X(X+1)(X+2)(X+3)$. Alors P est solution (exo). En conclusion, les polynômes solutions sont exactement les polynômes de la forme $P = \lambda X(X+1)(X+2)(X+3)$ avec $\lambda \in \mathbb{R}$.

3. Idem, ici le degré ne marche pas car les degrés sont les mêmes, et aucune racine (réelle) ne saute aux yeux. Suivons l'indication de l'énoncé et intéressons-nous au coefficient dominant. Pour cela, le polynôme doit être non nul. Remarquons que le polynôme nul est solution. Soit à présent P non nul. Tout d'abord, si $\deg(P) \leq 1$ alors $P'' = 0$ donc P n'est pas solution. Supposons à présent P de degré $n \geq 2$ et notons $a_n \neq 0$ son coefficient dominant. Le coefficient dominant de $6P$ est $6a_n$ et le coefficient dominant de P'' est $n(n-1)a_n$ (le terme dominant de P est $a_n X^n$ et on dérive deux fois) donc le coefficient dominant de $(X^2+1)P''$ est aussi $n(n-1)a_n$ si bien que $n(n-1)a_n = 6a_n$ et $a_n \neq 0$ donc $n(n-1) = 6$ si bien que $n^2 - n - 6 = 0$. Par conséquent, $n = 3$ ou $n = -2$ mais n est un entier positif donc $n = 3$: P est de degré 3, donc il existe a, b, c, d avec a non nul (le coefficient dominant) tels que $P = aX^3 + bX^2 + cX + d$. D'une part, $6P = 6aX^3 + 6bX^2 + 6cX + 6d$ et d'autre part, $P' = 3aX^2 + 2bX + c$ et $P'' = 6aX + 2b$ donc

$$(X^2 + 1)P'' = 6aX^3 + 2bX^2 + 6aX + 2b$$

Par unicité des coefficients, $6a = 6a$ (les coefficients dominants sont égaux : on le savait déjà!), $6b = 2b$ donc $b = 0$, $6c = 6a$ donc $a = c$, et enfin $6d = 2b$ donc $d = 0$. Finalement, $P = a(X^3 + X)$.

Synthèse : Soit $a \in \mathbb{R}^*$ et soit $P = a(X^3 + X)$. Alors $6P = 6a(X^3 + X)$ et $P'' = 6aX$ si bien que $(X^2 + 1)P'' = 6aX^2 + 6aX = 6P$: P est solution.

En conclusion, les solutions sont exactement les polynômes du type $P = a(X^3 + X)$ avec $a \in \mathbb{R}$ (y compris $a = 0$ puisque le polynôme nul est solution).

4. Intéressons-nous au degré. Le polynôme nul est solution : supposons à présent que P soit de degré n avec $n \geq 0$. **Analyse :** supposons P solution. Alors $\deg(P(X^2)) = \deg(P) \times \deg(X^2) = 2n$ et $\deg((X^2+1)P(X)) = \deg(X^2+1) + \deg(P) = n+2$ donc $2n = n+2$. On en déduit que $n = 2$: il existe a, b, c tels que $P = aX^2 + bX + c$. Par conséquent, $(X^2+1)P(X) = aX^4 + bX^3 + (a+c)X^2 + bX + c$ et d'autre part, $P(X^2) = aX^4 + bX^2 + c$. Par unicité des coefficients, $a = a$, ce qui n'apporte aucune information, $b = 0$, $(a+c) = b$ donc $a = -c$, $b = 0$ et $c = c$. On en déduit que $P = a(X^2 - 1)$.

Synthèse : Soit $a \in \mathbb{R}^*$ et soit $P = a(X^2 - 1)$. Alors P est solution (exo). En conclusion, les solutions sont exactement les polynômes du type $P = a(X^2 - 1)$ avec $a \in \mathbb{R}$ (y compris $a = 0$ puisque le polynôme nul est solution).

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

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

- Déterminer le degré et le coefficient dominant de L_n .
- 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.

Correction :

- P_n étant de degré $2n$, sa dérivée n -ième est de degré n donc L_n également. P_n est unitaire de degré $2n$ donc son terme dominant est X^{2n} : en dérivant n fois, le terme dominant est $2n(2n-1) \dots (n+1)X^n$ donc le coefficient dominant de L_n est

$$\frac{(2n)!}{2^n \times n!^2}$$

- On sait que $P_n = A_n B_n$ avec $A_n = (X-1)^n$ et $B_n = (X+1)^n$. D'après la formule de Leibniz :

$$P_n^{(n)} = \sum_{k=0}^n \binom{n}{k} A_n^{(k)} B_n^{(n-k)}$$

Or, 1 est racine de multiplicité n de A_n : il en découle que $A_n^{(k)}(1) = 0$ pour tout $k \leq n-1$. En d'autres termes, tous les termes de la somme sont nuls en 1 à part le terme pour $k = n$ qui vaut $A_n^{(n)}(1) \times B_n(1)$. Or, $A_n^{(n)}$ est le polynôme constant égal à $n!$ et $B_n(1) = 2^n$ si bien que $P_n^{(n)}(1) = 2^n \times n!$ et donc $L_n(1) = 1$. On trouve de même que $L_n(-1) = (-1)^n$.

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.

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

Correction :

- Une partie non vide de \mathbb{N} admet toujours un minimum : il suffit de prouver que ces parties sont non vides, donc qu'il existe i et j tel que $p \nmid a_i$ et $p \nmid b_j$. Or, P et Q sont primitifs donc leurs coefficients ne peuvent tous être divisibles par p , sinon le PGCD des coefficients serait divisible par p ce qui n'est pas le cas.
- Suivons l'indication de l'énoncé et intéressons-nous au coefficient d'indice $i_0 + j_0$ de PQ , coefficient qu'on note $c_{i_0+j_0}$. Par définition :

$$c_{i_0+j_0} = \sum_{i=0}^{i_0+j_0} a_i b_{i_0+j_0-i}$$

Si $i < i_0$, alors $p \mid a_i$ puisque, par définition de i_0 , p divise tous les coefficients avant a_{i_0} , donc $p \mid a_i b_{i_0+j_0-i}$. Si $i > i_0$, alors $i_0 - i < 0$ donc $i_0 + j_0 - i < j_0$ et, de même, p divise $b_{i_0+j_0-i}$ donc $a_i b_{i_0+j_0-i}$. On en déduit que p divise tous les termes de la somme sauf (peut-être) celui d'indice i_0 . Dès lors :

$$c_{i_0+j_0} \equiv a_{i_0} b_{j_0} [p]$$

Cependant, p ne divise par a_{i_0} ni b_{j_0} donc ne divise pas leur produit (car p est premier!). Il en découle que $c_{i_0+j_0} \not\equiv 0[p]$ donc p ne divise pas ce coefficient. On en déduit que les coefficients de PQ n'ont aucun facteur premier commun puisque, pour tout p premier, il existe un coefficient qui n'est pas divisible par p . Finalement, PQ est primitif : si d est le PGCD des coefficients de PQ , alors d n'est divisible par aucun nombre premier d'après ce qui précède donc $d = 1$ (un PGCD est forcément strictement positif).

- Notons $A = P/c(P)$ et $B = Q/c(Q)$. A et B sont non nuls et à coefficients dans \mathbb{Z} puisque $c(P)$ est le PGCD des coefficients de P donc les divise tous, et idem pour $c(Q)$. De plus, A et B sont primitifs : en effet, si d est le PGCD des coefficients de A donc tous les coefficients de A sont divisibles par d donc tous les coefficients de P sont divisibles par $c(P) \times d$: or, $c(P)$ est le plus grand diviseur commun des coefficients donc $d = 1$. Idem pour B . D'après la question précédente, AB est primitif. Or, $PQ = c(P)c(Q)AB$. En d'autres termes, tous les coefficients de AB sont multipliés par $c(P)c(Q)$: leur PGCD est donc aussi multiplié par $c(P)c(Q)$ (cf. chapitre 6). En d'autres termes, $c(PQ) = c(P)c(Q)c(AB)$ mais $c(AB) = 1$, ce qui permet de conclure.

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

Correction : Les polynômes non constants (à valeurs dans \mathbb{Q}) ne sont évidemment pas solutions. Soit $P = aX + b \in \mathbb{Q}[X]$ de degré 1 (donc avec $a \neq 0$). Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Si $P(\alpha) \in \mathbb{Q}$ alors

$$\alpha = \frac{P(\alpha) - b}{a} \in \mathbb{Q}$$

en tant que quotient de rationnels, ce qui est absurde. En d'autres termes, $P(\alpha) \in \mathbb{R} \setminus \mathbb{Q}$: les polynômes de degré 1 conviennent. Montrons que ce sont les seuls. Soit $P \in \mathbb{Q}[X]$ de degré $n \geq 2$, qu'on note comme d'habitude $P = a_n X^n + \dots + a_1 X + a_0$ avec $a_n \neq 0$. Suivons l'indication de l'énoncé et utilisons l'exercice 26. Cet exercice parlant de polynômes à coefficients entiers, transformons P de manière à ce qu'il soit à coefficients entiers. Plus précisément, soit m le PPCM des dénominateurs des coefficients de P . Alors $mP \in \mathbb{Z}[X]$. Notons $Q = mP = b_n X^n + \dots + b_1 X + b_0 \in \mathbb{Z}[X]$ avec $b_n \neq 0$.

Supposons $b_n > 0$ (raisonnement analogue dans l'autre cas). Alors (on identifie polynôme et fonction polynomiale) $Q(x) \xrightarrow{x \rightarrow +\infty} +\infty$: tout $k \in \mathbb{Z}$ et supérieur à $Q(0)$ est atteint par Q (TVI, Q est continu). Puisque l'exercice 26 parle de racine, transformons ceci en racine : un réel x_k est solution de $Q(x_k) = k$ si et seulement si x_k est racine de $Q_k = Q - k$.

Soit donc $k \in \mathbb{Z}$ tel que $k \geq Q(0)$. Supposons que $x_k \in \mathbb{Q}$. D'après l'exercice 26, x_k est de la forme a/b_n avec b_n le coefficient dominant de Q_k donc de Q (Q et Q_k ont même coefficient dominant, seul change leur terme constant). En d'autres termes, tous les antécédents d'entiers (assez grands) par Q sont de la forme a/b_n . En particulier, deux antécédents d'entiers sont distants d'au moins $1/b_n$, c'est-à-dire que si x_k est l'antécédent de k et x_{k+1} celui de $k+1$, alors $x_{k+1} - x_k \geq 1/b_n$. Montrons que ce n'est pas possible pour k assez grand car « Q devient de plus en plus raide donc, en un laps de temps $1/b_n$, fait des bonds plus grands que 1 ».

Puisque Q est de degré supérieur ou égal à 2, alors Q' est de degré supérieur ou égal à 1 et de coefficient dominant $nb_n > 0$ donc $Q'(x) \xrightarrow{x \rightarrow +\infty} +\infty$. En particulier, il existe A tel que, pour tout $x \geq A$, $Q'(x) > b_n$. Soit $k \in \mathbb{Z}$ tel que $k \geq Q(A)$: d'après le TVI, il existe $x_k \leq x_{k+1}$ supérieurs à A tels que $Q(x_k) = k$ et $Q(x_{k+1}) = k+1$. Si x_k et x_{k+1} sont rationnels, d'après ce qui précède, $x_{k+1} - x_k \geq 1/b_n$. Or, d'après l'IAF, Q' étant strictement supérieur à b_n à partir de A , il vient :

$$Q(x_{k+1}) - Q(x_k) > b_n \times (x_{k+1} - x_k) \geq b_n \times \frac{1}{b_n} = 1$$

ce qui est absurde puisque $Q(x_{k+1}) = k+1$ et $Q(x_k) = k$: il en découle que l'un des deux est irrationnels, et puisqu'il a une image entière (donc rationnelle), Q n'envoie pas les irrationnels sur des irrationnels, Q n'est pas solution du problème. En conclusion, les seuls polynômes qui conviennent sont exactement les polynômes de degré 1.

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

1. Rappelons qu'on s'arrête quand on a un reste qui a un degré strictement inférieur au polynôme par lequel on divise.

$$\begin{array}{r|l}
 6X^6 - 3X^5 & 4X^3 + X + 1 \\
 - (6X^6 & 3X^3/2 - 3X^2/4 - 3X/8 - 3/16 \\
 + 3X^4/2 + 3X^3/2) & \\
 \hline
 - 3X^5 - 3X^4/2 - 3X^3/2 - 5X^2 + 10X - 6 & \\
 - (-3X^5 & - 3X^3/4 - 3X^2/4) \\
 \hline
 - 3X^4/2 - 3X^3/4 - 17X^2/4 + 10X - 6 & \\
 - (-3X^4/2 & - 3X^2/8 - 3X/8) \\
 \hline
 - 3X^3/4 - 31X^2/8 + 83X/8 - 6 & \\
 - (-3X^3/4 & - 3X/16 - 3/16) \\
 \hline
 - 31X^2/8 + 169X/16 - 93/16 &
 \end{array}$$

2. Là, c'est beaucoup plus simple :

$$\begin{array}{r|l}
 7X^7 - 5X^5 + 3X^3 - X & 6X^6 - 4X^4 + 2X^2 \\
 - (7X^7 - 14X^5/3 + 7X^3/3) & 7X/6 \\
 \hline
 - X^5/3 + 2X^3/3 - X &
 \end{array}$$

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 $(X-1)^3$.

Correction : Effectuer la division euclidienne n'est pas imaginable : P est de degré $2n$, le quotient serait de degré $2n-2$, nous n'y arriverions pas. Heureusement, on ne demande que le reste ! Il suffit d'appliquer le théorème de division euclidienne (on peut le faire car on ne divise pas par le polynôme nul) : il existe Q et R uniques tels que $P = Q \times (X-3)(X-2) + R$ avec $\deg(R) < \deg((X-3)(X-2)) = 2$. Ainsi, $\deg(R) \leq 1$: il existe a et b tels que $R = aX + b$ donc tels que

$$(X-3)^{2n} + (X-2)^n - 2 = Q \times (X-3)(X-2) + aX + b.$$

On cherche la valeur de a et la valeur de b . Évaluons l'égalité ci-dessus en 2 : on ne connaît pas $Q(2)$, mais puisque Q est multiplié par $(X-3)(X-2)$ qui est nul en 2, ce n'est pas grave. On a donc :

$$(2-3)^{2n} + (2-2)^n - 2 = Q(2) \times (2-3)(2-2) + 2a + b$$

c'est-à-dire que $(-1)^{2n} - 2 = -1 = 2a + b$. De même, en évaluant en 3, on obtient $-1 = 3a + b$. On a donc $a = 0$ et $b = -1$, si bien que $R = -1$. De même, il existe $Q \in \mathbb{R}[X]$ et $(a, b) \in \mathbb{R}^2$ (distincts des Q, a, b du cas précédent) tels que (nous noterons (E) cette égalité dans la suite) :

$$(X - 3)^{2n} + (X - 2)^n - 2 = Q \times (X - 2)^2 + aX + b.$$

En évaluant en 2, il vient $2a + b = -1$. Cependant, on ne peut pas évaluer en un autre réel ici : si on évalue en un autre réel que 2, $X - 2$ ne sera pas nul et donc on aura une égalité faisant intervenir $Q(2)$, dont on ne connaît pas la valeur. Suivons l'indication de l'énoncé et dérivons l'égalité (E) :

$$2n(X - 3)^{2n-1} + n(X - 2)^{n-1} = Q' \times (X - 2)^2 + Q \times 2(X - 2) + a.$$

En évaluant en 2, il vient $a = 2n \times (-1)^{2n-1} = -2n$, si bien (à l'aide de l'égalité $2a + b = -1$ obtenue précédemment) que $b = 4n - 1$. Finalement, $R = -2nX + 4n - 1$.

De même, il existe Q et a et b uniques tels que $(X^n + 1)^2 = Q \times (X + 1)^2 + aX + b$. En évaluant en -1 , on trouve que $b - a = ((-1)^n + 1)^2$. En dérivant l'égalité précédente, on trouve :

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

et donc, en évaluant en -1 , on trouve que $a = 2n \times (-1)^{n-1} \times ((-1)^n + 1)$ ce qui permet de trouver b et donc de conclure.

Idem, il existe Q et a, b, c uniques tels que $X^n = (X - 1)^3Q + aX^2 + bX + c$. En évaluant en 1, on trouve $a + b + c = 1$. En dérivant, il vient : $nX^{n-1} = 3(X - 1)^2Q + (X - 1)^3Q' + 2aX + b$ et en évaluant en 1 on trouve $n = 2a + b$. En dérivant encore une fois et en évaluant en 1 on trouve $a = n(n - 1)$ et donc on trouve b et ensuite c .

Exercice 63 : ★★ Soit $(n, p) \in (\mathbb{N}^*)^2$. S'inspirer de l'exercice 59 du chapitre 6 pour prouver que $(X^n - 1) \wedge (X^p - 1) = X^{n \wedge p} - 1$.

Correction : Notons r la division euclidienne de la division euclidienne (d'entiers) de n par p . Puisque $r < p$ et $a \geq 2$, alors $\deg(X^r - 1) < \deg(X^p - 1)$. De l'écriture

$$X^n - 1 = X^r \times (X^{qp} - 1) + X^r - 1$$

on déduit que le reste dans la division euclidienne de $X^n - 1$ par $X^p - 1$ vaut $X^r - 1$. On itère ensuite le procédé : si on note $(r_1, \dots, r_k, 0)$ les restes successifs dans l'algorithme d'Euclide donnant $n \wedge p$ (et donc $r_k = n \wedge p$), les restes successifs dans l'algorithme d'Euclide donnant $(X^n - 1) \wedge (X^p - 1)$ sont $(X^{r_0} - 1, \dots, X^{r_k} - 1, X^0 - 1 = 0)$ si bien que $(X^n - 1) \wedge (X^p - 1)$, le dernier reste non nul, est égal à $X^{r_k} - 1 = X^{n \wedge p} - 1$.

Exercice 64 : ★★ Trouver les réels a tels que $X^2 - aX + 1$ divise $X^4 - X + a$ dans $\mathbb{R}[X]$.

Correction : Effectuons la division euclidienne de $X^4 + X + a$ par $X^2 - aX + 1$. Au bout de deux étapes, comme dans l'exercice 61, on se retrouve avec l'égalité suivante :

$$X^4 - X + a = (X^2 - aX + 1) \times (X^2 + aX) + (a^2 - 1)X^2 - (a + 1)X + a$$

On peut se dire qu'on n'a pas terminé puisque le reste n'est pas de degré < 2 , mais attention : $a^2 - 1$ peut être nul, il faut différencier les cas. Si $a = \pm 1$, la quantité de droite est de degré strictement inférieur à 2 donc c'est bien le reste, et il n'est pas nul (le terme constant vaut ± 1) donc $X^2 - aX + 1$ ne divise pas $X^4 - X + a$. Supposons donc $a \neq \pm 1$. Avec une dernière étape de division euclidienne, on obtient finalement que le reste est égal à

$$(-2a - 1 + a^2)X + (a - a^2 + 1)$$

et les deux coefficients ne sont jamais nuls en même temps : il n'y a aucune valeur de a qui convienne.

Exercice 65 : ★ Montrer que $X^5 - 1$ et $X^2 + X + 1$ sont premiers entre eux. Déterminer une relation de Bézout entre ces polynômes.

Correction : Pour prouver qu'ils sont premiers entre eux, il suffit de prouver qu'ils n'ont aucune racine complexe commune donc que j et j^2 (les racines de $X^2 + X + 1$) ne sont pas racines de $X^5 - 1$. Puisque $X^5 - 1$ est à coefficients réels, il suffit même de prouver que j n'est pas racine de $X^5 - 1$ ce qui est immédiat puisque $j^5 = j \neq 1$. Cependant, on demande une relation de Bézout : on n'y coupe pas, il faut appliquer l'algorithme d'Euclide étendu. Je ne détaille pas les calculs de division euclidienne.

$$\begin{array}{r|l} X^5 - 1 & X^2 + X + 1 \\ & X^3 - X^2 + 1 \\ \hline -X - 2 & \end{array}$$

$$\begin{array}{r|l} X^2 + X + 1 & -X - 2 \\ & -X + 1 \\ \hline & 3 \end{array}$$

$$\begin{array}{r|l} -X - 2 & 3 \\ & -X - 2 \\ \hline & 3 \\ \hline 0 & \end{array}$$

Puisque le dernier reste non nul est constant, les deux polynômes sont premiers entre eux. De plus,

$$-3 = (X^2 + X + 1) - (-X + 2)(-X + 1)$$

donc :

$$\begin{aligned} 1 &= -\frac{1}{3}(X^2 + X + 1) + \frac{1}{3}(-X + 2)(-X + 1) \\ &= -\frac{1}{3}(X^2 + X + 1) + \frac{1}{3}(-X + 1) \times [(X^5 - 1) - (X^2 + X + 1)(X^3 - X^2 + 1)] \\ &= \frac{1}{3} \times (-X + 1) \times (X^5 - 1) + (X^2 + X + 1) \times \left[-\frac{1}{3} - \frac{1}{3} \times (X + 1) \times (X^3 - X^2 + 1) \right] \end{aligned}$$

ce qui est bien une relation de Bézout.

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 $AP = BQ$.

Correction : Rappelons que, sur \mathbb{C} , « ne pas être premiers entre eux » est équivalent à « admettre une racine complexe commune ». Supposons que P et Q admettent une racine complexe commune notée z_0 . Alors il existe A de degré $m - 1$ et B de degré $n - 1$ tels que $P = (X - z_0)B$ et $Q = (X - z_0)A$ et $AP = BQ = AB(X - z_0)$. Réciproquement, supposons qu'il existe de tels polynômes A et B . Raisonnons par l'absurde et supposons que P et Q soient premiers entre eux. $AP = BQ$ donc P divise BQ donc, d'après le théorème de Gauss (P et Q sont premiers entre eux) P divise B ce qui est absurde puisque B est non nul de degré strictement inférieur au degré de P : P et Q ne sont pas premiers entre eux, d'où l'équivalence.

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 ?

Correction :

1. Recopier la preuve du cours en remplaçant b_p par 1.
2. D'après le théorème de la division euclidienne sur \mathbb{Z} (car $X - 7$ est unitaire), il existe Q_1 et R_1 uniques dans $\mathbb{Z}[X]$ tels que $P = Q_1 \times (X - 7) + R_1$ et $\deg(R_1) < \deg(X - 7)$. Donc, $\deg(R_1) < 1$ ce qui implique que R_1 est constant. En évaluant en $x = 7$ on obtient $P(7) = 0 + R_1$ c'est-à-dire que $R_1 = 77$. La méthode pour trouver R_2 est tout-à-fait analogue. Ainsi, il existe Q_1 et Q_2 dans $\mathbb{Z}[X]$ tels que $P = Q_1 \times (X - 7) + 77 = Q_2 \times (X - y) + 85$.

En évaluant en y on obtient $Q_1(y) \times (y - 7) + 77 = 85$. Puisque $Q_1(y) \in \mathbb{Z}$ (car Q_1 est à coefficients dans \mathbb{Z} et $y \in \mathbb{Z}$), il vient, en posant $k = Q_1(y)$: il existe $k \in \mathbb{Z}$ tel que $k \times (y - 7) = 8$. Or, $y - 7 > 0$ d'après l'énoncé, et les seuls diviseurs entiers positifs sont 1, 2, 4 et 8, si bien que $y - 7 = 1, 2, 4$ ou 8.

On a également $P = Q_1 \times (X - y) + 77$. α étant racine de P , on a $-Q_1(y) \times (\alpha - 7) = 77 = 7 \times 11$. $\alpha - 7$ est par conséquent positif (d'après l'énoncé) et un diviseur dans \mathbb{Z} de 77 (car $Q_1(y) \in \mathbb{Z}$) et les seuls diviseurs de 77 étant

1, 7, 11, 77, ce qui implique également que $\alpha - 7 = 1, 7, 11$ ou 77.

De même en utilisant l'écriture $P = Q_2 \times (X - y) + 85$ et en voyant que $85 = 5 \times 17 : \alpha - y = 1, 5, 17$ ou 85. D'après ce qui précède, $y = 8, 9, 11$ ou 15 et $\alpha = 8, 14, 18$ ou 84 (dans ce cas le père ne doit plus être tout jeune...). Enfin, on a aussi $\alpha - y = 1, 5, 17$ ou 85.

- Si $y = \alpha = 8, \alpha - y = 0$ ce qui n'est pas possible (déjà car le chien est plus jeune que le fils).
- Si $y = 8$ et $\alpha = 14, \alpha - y = 6$ ce qui n'est pas possible.

Et ainsi de suite : la seule possibilité est d'avoir $\alpha = 14$ et $y = 9$: le fils a 14 ans et le chien a 9 ans.

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 $X + 2, \dots, X + n + 1$ sont égaux.

Correction : Raisonnons par analyse synthèse.

Analyse : Notons R le reste commun des divisions euclidiennes de P par $(X + 2), \dots, (X + n + 1)$. D'après le théorème de division euclidienne, $\deg(R) < \deg(X + 2) = 1$ si bien que R est constant, disons égal à β . Notons respectivement Q_1, \dots, Q_{n+1} les restes dans les divisions euclidiennes de P par, respectivement, $X + 2, \dots, X + n + 1$, si bien que

$$P = (X + 2) \times Q_2 + \beta = \dots = (X + n + 1) \times Q_{n+1} + \beta$$

Il en découle que $P(-2) = P(-3) = \dots = P(-(n + 1)) = \beta$. En d'autres termes, $-2, \dots, -(n + 1)$ sont racines de $P - \beta$. Or, ce polynôme est de degré n (car P est de degré n) et admet n racines distinctes : celles-ci sont donc simples, et si l'on note a_n le coefficient dominant de P , on obtient :

$$P - \beta = a_n(X + 2) \times \dots \times (X + n + 1)$$

Si bien que $P = a_n(X + 2) \times \dots \times (X + n + 1) + \beta$. Enfin, $X + 1$ divise P donc $P(-1) = 0$, d'où :

$$0 = a_n(-1 + 2) \times \dots \times (-1 + n + 1) + \beta$$

et donc $\beta = -a_n \times n!$. Finalement, $P = a_n \times [(X + 2) \times \dots \times (X + n + 1) - n!]$.

Synthèse : Soit $a_n \in \mathbb{R}^*$ et soit $P = a_n \times [(X + 2) \times \dots \times (X + n + 1) - n!]$. Montrons que P convient. Rappelons qu'il y a unicité dans le théorème de division euclidienne. Ainsi, si on a une écriture du type $P = BQ + R$ avec $\deg(R) < \deg(B)$ alors Q est le quotient et R est le reste. En particulier, si on a une écriture du type $P = BQ + R$ avec $\deg(B) = 1$ et R constant, alors R est le reste. Or,

$$P = (X + 2) \times a_n(X + 3) \dots (X + n + 1) - a_n \times n!$$

est une écriture de ce type : le reste de la division de P par $X + 2$ est donc $-a_n \times n!$. On montre de même que c'est aussi le reste quand on divise par $(X + 3), \dots, (X + n + 1)$. Enfin, un calcul simple donne bien $P(-1) = 0$ donc $X + 1$ divise P : P est bien solution.

Conclusion : les polynômes solutions sont exactement les polynômes de la forme

$$P = a_n \times [(X + 2) \times \dots \times (X + n + 1) - n!]$$

avec $a_n \neq 0$.

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.

Correction :

1. A et B sont premiers entre eux car n'ont aucune racine complexe commune. D'après le théorème de Bézout, il existe U et V dans $\mathbb{Q}[X]$ tels que $AU + BV = D$, où D est un PGCD de A et B (pas forcément $A \wedge B$). En effet, U et V sont obtenus à l'aide de divisions d'entiers donc sont à coefficients rationnels (ou, si on veut faire les choses proprement : l'algorithme d'Euclide étendu et le théorème de Bézout qui en découle sont valables sur un corps, A et B sont à coefficients dans \mathbb{Q} qui est un corps donc U, V et D sont à coefficients rationnels, pas forcément entiers car \mathbb{Z} est un anneau et pas un corps). En multipliant par m le PPCM des dénominateurs de U, V, D , on obtient : $(mU)P + (mV)Q = (mD)$. Or, m étant un multiple de tous les dénominateurs, mU, mV et mD sont à coefficients entiers. Enfin, P et Q étant premiers entre eux, tous leurs PGCDs sont constants donc mD est constant (entier). Il suffit de poser $A = mU, B = mV$ et $d = mD$ pour conclure.

2. Notons $P = \sum_{k=0}^d a_k X^k$ avec d le degré de P (et donc a_d est le coefficient dominant de P). Soit $n \in \mathbb{N}$.

$$P(n+d) - P(n) = \sum_{k=0}^d a_k (n+d)^k - \sum_{k=0}^d a_k n^k$$

Or, pour $k=0$, $a_k(n+d)^k = a_0 = a_k n^k$ donc les deux termes se compensent : les deux sommes commencent en 1. Dès lors :

$$P(n+d) - P(n) = \sum_{k=1}^d a_k ((n+d)^k - n^k)$$

Or, pour tout $k \geq 1$:

$$(n+d)^k - n^k = (n+d-n) \sum_{i=0}^{k-1} (n+d)^i n^{k-1-i}$$

Puisque $n+d-n=d$, ce terme est divisible par d donc tous les termes de la somme ci-dessus sont divisibles par d , ce qui permet de conclure.

3. Soit $n \in \mathbb{N}$. D'après la question 1, $A(n)P(n) + B(n)Q(n) = d$ donc, d'après le théorème de Bézout (pour les entiers), u_n (le PGCD de $P(n)$ et $Q(n)$) divise d . Par conséquent, d'après la question précédente, u_n divise $P(n+d) - P(n)$. Or, u_n divise $P(n)$ donc u_n divise $P(n+d)$. Par symétrie des rôles, u_n divise $Q(n+d)$ donc u_n divise u_{n+d} car est un diviseur commun de $P(n+d)$ et $Q(n+d)$. On prouve de même que u_{n+d} divise u_n donc u_n et u_{n+d} sont associés : ils sont soit égaux soit opposés, et puisqu'ils sont positifs, ils sont égaux, ce qui permet de conclure.

19.5 Relations coefficients-racines

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

Correction : Pour un polynôme de degré n dont les coefficients sont notés a_0, \dots, a_n , on sait que la somme des racines vaut $-a_{n-1}/a_n$ et le produit des racines $(-1)^n a_0/a_n$. On en déduit que la somme cherchée vaut $-3/2$ et le produit $-2024/2 = -1012$ (car $(-1)^5 = -1$).

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.

Correction : Notons $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ avec $a_n \neq 0$. D'après le cours, la somme des racines est égale à $-a_{n-1}/a_n$ donc

$$\mu(P) = -\frac{a_{n-1}}{n \times a_n}$$

De plus, $P' = na_n X^{n-1} + (n-1)a_{n-1} X^{n-2} + \dots + 2a_2 X + a_1$. Par conséquent, la somme des racines de P' est $-(n-1)a_{n-1}/na_n$ (moins l'avant dernier coefficient divisé par le dernier i.e. le coefficient dominant). Par conséquent (en n'oubliant pas que P' est de degré $n-1$ donc on divise par $n-1$ et pas par n dans la moyenne arithmétique) :

$$\begin{aligned} \mu(P') &= \frac{1}{n-1} \times \frac{-(n-1)a_{n-1}}{na_n} \\ &= -\frac{a_{n-1}}{na_n} \\ &= \mu(P) \end{aligned}$$

On peut évidemment continuer : tant que $k \leq n-1$ (on ne l'applique qu'à des polynômes de degré supérieur ou égal à 1), on peut itérer (i.e. dériver et la moyenne ne change pas) donc $\mu(P) = \mu(P^{(k)})$. En particulier, $\mu(P) = \mu(P^{(n-1)})$. Or, $P = a_n X^n + a_{n-1} X^{n-1} + \dots$ si bien que

$$P^{(n-1)} = a_n \times n! \times X + a_{n-1} \times (n-1)!$$

En particulier, son unique racine est $-a_{n-1}(n-1)!/(a_n n!) = -a_{n-1}/na_n$ (rappelons que $a_n \neq 0$) si bien que

$$\mu(P) = \mu(P') = \mu(P^{(n-1)}) = \frac{1}{n} \frac{a_{n-1}}{a_n} = \frac{a_{n-1}}{na_n}$$

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.

Correction : P étant unitaire, pour tout $k \leq n-1$ (il est important que P soit unitaire sinon a_n apparaît dans la formule ci-dessous) :

$$a_{n-k} = (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} z_{i_1} \cdots z_{i_k}$$

où on a noté évidemment z_1, \dots, z_n les racines complexes (pas forcément distinctes) de P . D'après l'inégalité triangulaire, et les z_i étant de module 1 :

$$|a_{n-k}| \leq \sum_{1 \leq i_1 < \dots < i_k \leq n} 1$$

On pourrait dire que cette somme est égale à $\binom{n}{k}$ mais sa valeur exacte importe peu : seul compte le fait que les coefficients soient bornés. Puisqu'ils sont entiers, il y a un nombre fini de valeurs possibles pour a_0 , disons M_0 valeurs possibles, et ainsi de suite jusque M_{n-1} valeurs possibles pour a_{n-1} . Par principe multiplicatif, il y a $M_0 \times \dots \times M_{n-1}$ choix possibles pour les coefficients, donc un nombre fini.

Exercice 73 : ★★ Résoudre le système suivant :

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

Correction : Utilisons les relations coefficients racines pour un polynôme de degré 3 (puisque on a trois inconnues x, y et z) :

$$\begin{aligned} (X-x)(X-y)(X-z) &= X^3 - (x+y+z)X^2 + (xy+xz+yz)X - xyz \\ &= X^3 - X^2 + (xy+xz+yz)X - xyz \end{aligned}$$

Or,

$$\begin{aligned} (x+y+z)^2 &= x^2 + y^2 + z^2 + 2xy + 2yz + 2zx \\ &= x^2 + y^2 + z^2 + 2(xy + yz + zx) \end{aligned}$$

Or, $x+y+z=1$ et $x^2+y^2+z^2=9$ donc $2(xy+yz+zx)=-8$ donc $xy+yz+zx=-4$. Enfin, en mettant au même dénominateur :

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{yz+xz+xy}{xyz}$$

c'est-à-dire que $1 = \frac{-4}{xyz}$ donc $xyz = -4$. Finalement :

$$(X-x)(X-y)(X-z) = X^3 - X^2 - 4X + 4$$

1 est racine évidente. En factorisant, il vient : $X^3 - X^2 + 4X - 4 = (X-1)(X^2 - 4) = (X-1)(X-2)(X+2)$, c'est-à-dire que les racines de $(X-x)(X-y)(X-z)$ sont 1 et ± 2 . Or, ce sont aussi x, y, z donc x, y, z valent 1 et ± 2 . Qui est qui ? x, y, z jouent des rôles symétriques donc ils peuvent valoir n'importe quelle valeur. En conclusion, il y a 6 triplets solutions : tous les triplets contenant 1 et ± 2 dans les 6 ordres possibles (6 car il y a $3! = 6$ permutations d'un ensemble à 3 éléments).

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.

Correction :

1. $P' = 3X^2 + p$ donc

$$\begin{aligned} P'(x)P'(y)P'(z) &= (3x^2 + p)(3y^2 + p)(3z^2 + p) \\ &= (9x^2y^2 + p(3x^2 + 3y^2) + p^2)(3z^2 + p) \\ &= 27x^2y^2z^2 + p(9x^2y^2 + 9x^2z^2 + 9y^2z^2) + p^2(3z^2 + 3x^2 + 3y^2) + p^3 \end{aligned}$$

Or, $P = (X - x)(X - y)(X - z)$ donc, d'après les relations coefficients racines :

$$-x - y - z = 0, \quad xy + xz + yz = p \quad \text{et} \quad -xyz = q$$

Dès lors, $P'(x)P'(y)P'(z) = 27q^2 + 9p(x^2y^2 + x^2z^2 + y^2z^2) + 3p^2(z^2 + x^2 + y^2) + p^3$. D'une part, $(x + y + z)^2 = 0$, et d'autre part :

$$\begin{aligned} (x + y + z)^2 &= x^2 + y^2 + z^2 + 2xy + 2xz + 2yz \\ &= x^2 + y^2 + z^2 + 2p \end{aligned}$$

si bien que $x^2 + y^2 + z^2 = -2p$. Enfin, $(xy + xz + yz)^2 = p^2$ et

$$\begin{aligned} (xy + xz + yz)^2 &= x^2y^2 + x^2z^2 + y^2z^2 + 2x^2yz + 2y^2xz + 2z^2xy \\ &= x^2y^2 + x^2z^2 + y^2z^2 + 2xyz(x + y + z) \\ &= x^2y^2 + x^2z^2 + y^2z^2 + 0 \end{aligned}$$

Finalement, $x^2y^2 + x^2z^2 + y^2z^2 = p^2$. On en déduit que :

$$\begin{aligned} P'(x)P'(y)P'(z) &= 27q^2 + 9p \times p^2 + 3p^2 \times -2p + p^3 \\ &= 27q^2 + 4p^3 \end{aligned}$$

2. P admet une racine multiple si et seulement si x, y ou z est racine de P' donc si et seulement si $27q^2 + 4p^3 = 0$. Par analogie avec le degré 2, cette quantité est donc appelée le discriminant de P .

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

Correction : Notons $P = \sum_{k=0}^n a_k X^k$ avec $a_n \neq 0$. Notons, pour tout $k \in \llbracket 0; n-1 \rrbracket$, S_k la somme des racines (comptées avec multiplicité) de $P^{(k)}$. D'après les relations coefficients racines, $S_0 = -a_{n-1}/a_n$ (moins l'avant-dernier coefficient divisé par le dernier). Calculons S_1 . Tout d'abord :

$$P' = \sum_{k=1}^n k a_k X^{k-1}$$

Par conséquent (toujours : moins l'avant-dernier coefficient divisé par le dernier) :

$$\begin{aligned} S_1 &= \frac{-(n-1)a_{n-1}}{na_n} \\ &= \frac{n-1}{n} \times S_0 \\ &= \left(1 - \frac{1}{n}\right) \times S_0 \\ &= S_0 - \frac{S_0}{n} \end{aligned}$$

Ensuite :

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

donc

$$\begin{aligned} S_2 &= \frac{(n-1)(n-2)a_{n-1}}{-n(n-1)a_n} \\ &= \frac{n-2}{n} \times S_0 \\ &= \left(1 - \frac{2}{n}\right) \times S_0 \\ &= S_0 - \frac{2S_0}{n} \end{aligned}$$

On généralise facilement le résultat : pour tout k , $S_k = S_0 - kS_0/n$, donc cette famille est en progression arithmétique (de raison $-S_0/n$).

Exercice 76 : ★★☆☆ Soit $n \geq 1$ et soit $f : \mathbb{C}^n \rightarrow \mathbb{C}^n$ qui à (z_1, \dots, z_n) associe $(\sigma_1, \dots, \sigma_n)$ 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 $f(z_1, \dots, z_n) \neq f(a_1, \dots, a_n)$.

Correction : Rappelons que si z_1, \dots, z_n sont les racines de P de degré n , alors on a :

$$P = a_n (X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \dots + (-1)^n \sigma_n)$$

avec les σ_k les fonctions symétriques élémentaires.

1. Soit $(\sigma_1, \dots, \sigma_n) \in \mathbb{C}^n$ et posons

$$P = -\sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \dots + (-1)^n \sigma_n$$

Notons z_1, \dots, z_n les racines complexes de P . Alors les fonctions symétriques élémentaires des z_i sont exactement les σ_i c'est-à-dire que $f(z_1, \dots, z_n) = (\sigma_1, \dots, \sigma_n) : f$ est surjective.

2. f n'est pas injective car tout n -uplet de racines qu'on peut déduire l'un de l'autre a les mêmes fonctions symétriques élémentaires. Par exemple, les racines $(1, 0, \dots, 0)$ et les racines $(0, \dots, 0, 1)$ donnent les mêmes polynômes donc les mêmes coefficients donc les mêmes fonctions symétriques élémentaires.
3. Supposons que (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, et notons

$$P = (X - z_1) \dots (X - z_n) \quad \text{et} \quad Q = (X - a_1) \dots (X - a_n)$$

Notons $(\sigma_1, \dots, \sigma_n)$ l'image de (z_1, \dots, z_n) par f , et (τ_1, \dots, τ_n) l'image de (a_1, \dots, a_n) . Par conséquent, en utilisant les relations coefficients racines :

$$P = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \dots + (-1)^n \sigma_n \quad \text{et} \quad Q = X^n - \tau_1 X^{n-1} + \tau_2 X^{n-2} - \tau_3 X^{n-3} + \dots + (-1)^n \tau_n$$

P et Q n'ont pas les mêmes racines donc ne sont pas égaux donc n'ont pas les mêmes coefficients c'est-à-dire que $(\sigma_1, \dots, \sigma_n) \neq (\tau_1, \dots, \tau_n) : les deux images sont bien distinctes.$

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.

Correction : De même que dans l'exercice 40 du chapitre 13 : l'équation

$$\sum_{k=1}^{100} \frac{k}{x-k} = 1$$

admet une unique solution x_1 sur $]1; 2[$, une unique solution x_2 sur $]2; 3[$, ..., une unique solution x_{99} sur $]99; 100[$ et une unique solution x_{100} sur $]100; +\infty[$. L'ensemble des solutions est donc

$$]1; x_1] \cup]x_1; x_2] \cup \dots \cup]x_{99}; x_{100}] \cup]x_{100}; +\infty[$$

On cherche donc la valeur de $S = \sum_{k=1}^{100} (x_k - k)$. Les x_k sont les solutions de l'équation

$$\sum_{k=1}^{100} \frac{k}{x - k} - 1 = \sum_{k=1}^{100} \frac{2k - x}{x - k} = 0$$

En mettant au même dénominateur, on trouve que les x_k sont solutions de l'équation

$$\frac{P(x)}{(x-1) \cdots (x-100)} = 0$$

où P est le polynôme

$$P = \sum_{k=1}^{100} (2k - X) \prod_{i \neq 100} (X - i)$$

donc les x_k sont les racines du polynôme P . On cherche la somme des racines : c'est (cf. relations coefficients racines) « moins le terme de degré $n - 1$ sur le terme de degré n ». P est la somme de 100 polynômes de degré 100 de coefficient dominant -1 donc est de degré 100 de coefficient dominant -100 . Cherchons à présent le coefficient de degré 99. Il suffit de sommer tous les coefficients d'ordre 99 des polynômes de la somme. Or, le coefficient d'ordre 99 de

$$P_k = (2k - X) \prod_{i \neq 100} (X - i)$$

vaut (ici, on prend le problème à l'envers : le coefficient d'ordre $n - 1$ vaut moins la somme des racines multipliée par le coefficient dominant) :

$$\begin{aligned} (-1) \times - \left(2k + \sum_{i \neq k} i \right) &= k + \sum_{i=1}^{100} i \\ &= k + \frac{100 \times 101}{2} \\ &= k + 5050 \end{aligned}$$

Finalement, le coefficient d'ordre 99 de P vaut

$$\begin{aligned} \sum_{k=1}^{100} (k + 5050) &= \sum_{k=1}^{100} k + \sum_{k=1}^{100} 5050 \\ &= \frac{100 \times 101}{2} + 5050 \times 100 \\ &= 5050 + 5050 \times 100 \\ &= 5050 \times 101 \end{aligned}$$

Finalement, la somme des racines de P , c'est-à-dire la somme des x_k , vaut $-5050 \times 101 / (-100) = 5050 \times 101 / 100$. En conclusion, la somme des longueurs cherchée vaut :

$$\begin{aligned}
S &= \sum_{k=1}^{100} x_k - \sum_{k=1}^{100} k \\
&= \frac{5050 \times 101}{100} - 5050 \\
&= \frac{5050 \times 101 - 5050 \times 100}{100} \\
&= \frac{5050}{100} \\
&= \frac{505}{10} \\
&= \frac{101}{2}
\end{aligned}$$

19.6 Quantités polynomiales en quelque-chose

Exercice 78 : ♣

- 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 $x \in \left[0; \frac{\pi}{2}\right]$, $\tan^{(n)}(x) \geq 0$.
- 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 $x \in \mathbb{R}$, $f^{(n)}(x) = P_n(e^x)$.

Correction :

- Montrons que les dérivées successives de la tangente sont des polynômes à coefficients entiers positifs évalués en la tangente (cf les polynômes de Tchebychev, c'est un argument du même genre). Montrons cela de façon plus précise.
 - Si $n \geq 0$, soit l'hypothèse de récurrence H_n : « Il existe $P_n \in \mathbb{N}[X]$ tel que $\tan^{(n)} = P_n(\tan)$ ».
 - Si $n = 0$, $\tan^{(0)} = \tan : P_0 = X$ convient donc H_0 est vraie. De plus, $\tan^{(1)} = 1 + \tan^2 : P_1 = 1 + X^2$ convient, H_1 est également vraie.
 - Soit n quelconque supérieur ou égal à 1. Supposons H_n vraie et montrons que H_{n+1} est vraie. Par hypothèse de récurrence, il existe $d \geq 0$ (le degré de P_n) et a_0, \dots, a_d entiers positifs (ses coefficients) tels que

$$\tan^{(n)} = \sum_{k=0}^d a_k \tan^k$$

En dérivant cette égalité, il vient (le terme pour $k = 0$ est nul, la somme commence donc en $k = 1$)

$$\begin{aligned}
\tan^{(n+1)} &= \sum_{k=1}^d k a_k \tan^{k-1} (1 + \tan^2) \\
&= \sum_{k=1}^d k a_k \tan^{k-1} + \sum_{k=1}^d k a_k \tan^{k+1}
\end{aligned}$$

Il suffit de poser

$$P_{n+1} = \sum_{k=1}^d k a_k X^{k-1} + \sum_{k=1}^d k a_k X^{k+1}$$

qui est bien à coefficients entiers positifs (car somme de deux polynômes à coefficients entiers positifs) pour conclure : H_{n+1} est vraie.

- D'après le principe de principe de récurrence, H_n est vraie pour tout $n \geq 0$.

Ainsi, pour tout $n \geq 0$, $\tan^{(n)}(x)$ est un polynôme à coefficients entiers positifs évalué en $\tan(x)$, qui est un nombre positif. Or, un polynôme à coefficients positifs évalué en un nombre positif est lui-même positif : $\tan^{(n)}(x) \geq 0$.

Pour l'unicité : si deux polynômes P_n et Q_n conviennent, alors $P_n(\tan(x)) = Q_n(\tan(x))$ pour tout $x \in \left[0; \frac{\pi}{2}\right]$ donc P_n et Q_n coïncident en tout élément de la forme $\tan(x)$ avec $x \in \left[0; \frac{\pi}{2}\right]$ donc P_n et Q_n coïncident sur \mathbb{R}_+ qui est infini donc sont égaux : ceci prouve l'unicité.

2. Pour l'existence, raisonnons par récurrence sur n .

- Si $n \in \mathbb{N}$, notons H_n : « $\exists P_n \in \mathbb{R}[X], \forall x \in \mathbb{R}, f_n(x) = P_n(e^x) \times e^{e^x}$ ».
- Puisque, pour tout $x \in \mathbb{R}$, $f_0(x) = 1 \times e^{e^x}$, $P_0 = 1$ convient : H_0 est vraie.
- Bien que ce ne soit pas nécessaire, montrons que H_1 et H_2 sont vraies pour nous donner une idée. Soit $x \in \mathbb{R}$. On a $f_1(x) = f_0'(x) = e^x \times e^{e^x}$. Ainsi, $P_1 = X$ convient. Attention, ne pas écrire « Donc $P_1 = X$ » ou, pire avec des équivalences ! Pour l'instant, nous ne montrons que l'existence et nous nous contentons d'exhiber des polynômes qui **conviennent**.

En effet, $P_1(e^x) = e^x$ et donc on a bien $f_1(x) = P_1(e^x) \times e^{e^x}$. De plus, $f_2 = f_1'(x)$, si bien que $f_2(x) = (e^x + e^x \times e^x) \times e^{e^x} = (e^x + e^{2x}) \times e^{e^x}$. Dès lors, $P_2 = X + X^2$ convient. En effet, $P_2(e^x) = e^x + e^{2x}$ et on a bien l'égalité voulue.

- Soit $n \in \mathbb{N}$. Supposons H_n vraie et prouvons que H_{n+1} est vraie. Par hypothèse de récurrence, il existe $P_n \in \mathbb{R}[X]$ tel que, pour tout $x \in \mathbb{R}$, $f_n(x) = P_n(e^x) \times e^{e^x}$. Soit $x \in \mathbb{R}$. En dérivant, il vient $f_{n+1}(x) = (e^x \times P_n'(e^x) + P_n(e^x) \times e^x) \times e^{e^x}$. Ainsi, $P_{n+1} = X P_n' + X P_n \in \mathbb{R}[X]$ convient : H_{n+1} est vraie.
- D'après le principe de récurrence, H_n est vraie pour tout n .

Unicité : Soit $n \in \mathbb{N}$. Soit Q_n un autre polynôme qui convient. Ainsi, pour tout $x \in \mathbb{R}$, $P_n(e^x) = Q_n(e^x)$. Attention, cela ne signifie pas (encore) que $P_n = Q_n$! En effet, on ne peut pas encore dire que P_n et Q_n coïncident en tout réel (par exemple, quoi qu'on fasse, on ne peut pas trouver de réel x tel que $e^x = -1$ et donc on ne peut pas encore affirmer que $P_n(-1) = Q_n(-1)$). On sait juste que, pour tout $x \in \mathbb{R}$, $P_n(e^x) = Q_n(e^x)$, c'est-à-dire que P_n et Q_n coïncident en tout réel de la forme e^x . Ils coïncident donc sur $\{e^x \mid x \in \mathbb{R}\} = \mathbb{R}_+^*$, qui est un ensemble infini, donc sont égaux. D'où l'unicité.

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 $x \neq 0$, $P_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$.

Correction :

1. On trouve :

$$\left(x^n + \frac{1}{x^n}\right) \times \left(x + \frac{1}{x}\right) = x^{n+1} + \frac{x^{n+1}}{+} x^{n-1} + \frac{1}{x^{n-1}}$$

2. **Existence :** Par récurrence sur n . Vu la question précédente, on se dit qu'il va y avoir un lien entre les rangs $n-1$, n et $n+1$: on va donc faire une récurrence double et, pour cela, il faut montrer l'initialisation pour au moins deux valeurs. Ici, donc, montrer que H_1 est vraie est indispensable.

- Si $n \in \mathbb{N}$, notons H_n : « $\exists P_n \in \mathbb{R}[X], \forall x \in \mathbb{R}^*, P_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$ ».
- Soit $x \neq 0$. On a $x^0 + \frac{1}{x^0} = 2$, si bien que $P_0 = 2$ convient : H_0 est vraie.
- Soit $x \neq 0$. Le polynôme $P_1 = X$ convient. En effet, $P_1\left(x + \frac{1}{x}\right) = x + \frac{1}{x}$: H_1 est donc vraie.
- Bien que ce ne soit pas nécessaire, montrons que H_2 est vraie. Soit $x \neq 0$. Tout d'abord, $\left(x + \frac{1}{x}\right)^2 = x^2 + \frac{1}{x^2} + 2$ donc $x^2 + \frac{1}{x^2} = \left(x + \frac{1}{x}\right)^2 - 2$. Par conséquent, $P_2 = X^2 - 2$ convient. En effet, pour tout $x \neq 0$,

$$P_2\left(x + \frac{1}{x}\right) = \left(x + \frac{1}{x}\right)^2 - 2 = x^2 + \frac{1}{x^2}$$

ce qui est le résultat voulu. Ainsi, H_2 est vraie.

- Soit $n \geq 1$. Supposons H_n et H_{n-1} vraies, et prouvons que H_{n+1} est vraie. Soit $x \neq 0$. D'après la question 1,

$$x^{n+1} + \frac{1}{x^{n+1}} = \left(x + \frac{1}{x}\right) \times \left(x^n + \frac{1}{x^n}\right) - \left(x^{n-1} + \frac{1}{x^{n-1}}\right).$$

Or, par hypothèse de récurrence, il existe $(P_n, P_{n-1}) \in \mathbb{R}[X]^2$ tels que, pour tout $x \in \mathbb{R}^*$,

$$x^n + \frac{1}{x^n} = P_n\left(x + \frac{1}{x}\right) \quad \text{et} \quad x^{n-1} + \frac{1}{x^{n-1}} = P_{n-1}\left(x + \frac{1}{x}\right).$$

Ainsi, $x^{n+1} + \frac{1}{x^{n+1}} = \left(x + \frac{1}{x}\right) \times P_n\left(x + \frac{1}{x}\right) - P_{n-1}\left(x + \frac{1}{x}\right)$. Finalement, $P_{n+1} = X P_n - P_{n-1}$ convient : H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \in \mathbb{N}$.

Unicité : Soit $n \in \mathbb{N}$. Soit Q_n un polynôme qui convient. Alors, pour tout $x \neq 0$, $P_n\left(x + \frac{1}{x}\right) = Q_n\left(x + \frac{1}{x}\right)$, c'est-à-dire que P_n et Q_n coïncident en tout point de la forme $x + \frac{1}{x}$. Soit φ la fonction définie sur \mathbb{R}^* par $\varphi : x \mapsto x + \frac{1}{x}$. Alors P_n et Q_n coïncident sur $\{\varphi(x) \mid x \in \mathbb{R}^*\}$. On trouve facilement le tableau de variations de φ :

x	$-\infty$	-1	0	1	$+\infty$
$\varphi'(x)$		$+$	0	$-$	$+$
$\varphi(x)$	$-\infty$	$\nearrow -2$	$\searrow -\infty$	$+\infty \searrow 2$	$\nearrow +\infty$

Comme φ est continue, strictement croissante sur $]1; +\infty[$ et telle que $\varphi(1) = 2$ et $\varphi(x) \xrightarrow{x \rightarrow +\infty} +\infty$, c'est une bijection de $]1; +\infty[$ dans $]2; +\infty[$. φ étant impaire, c'est également une bijection de $] -\infty; -1]$ dans $] -\infty; -2]$. Enfin, d'après le tableau de variations, φ ne prend aucune valeur dans $] -2; 2[$. En conclusion, $\{\varphi(x) \mid x \in \mathbb{R}^*\} =] -\infty; -2] \cup [2; +\infty[$ donc est un ensemble infini : P_n et Q_n coïncident sur un ensemble infini donc $Q_n = P_n$. D'où l'unicité.

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 $\theta \in \mathbb{R}$, $\sin(\theta)Q_n(\cos(\theta)) = \sin((n+1)\theta)$.

Correction : Existence : Montrons l'existence par récurrence sur n .

- Si $n \geq 1$, notons H_n : « il existe $Q_n \in \mathbb{R}[X]$ tel que, pour tout $\theta \in \mathbb{R}$, $\sin(\theta)Q_n(\cos(\theta)) = \sin((n+1)\theta)$ ».
- Pour $n = 1$: pour tout $\theta \in \mathbb{R}$, $\sin(2\theta) = 2\sin(\theta)\cos(\theta) = \sin(\theta) \times 2\cos(\theta)$ donc $2X$ convient : H_1 est vraie.
- Pour $n = 2$: pour tout $\theta \in \mathbb{R}$,

$$\begin{aligned}
 \sin(3\theta) &= 3\sin(\theta) - 4\sin^3(\theta) \\
 &= \sin(\theta) \times (3 - 4\sin^2(\theta)) \\
 &= \sin(\theta) \times (3 - 4(1 - \cos^2(\theta))) \\
 &= \sin(\theta) \times (4\cos^2(\theta) - 1)
 \end{aligned}$$

c'est-à-dire que $4X^2 - 1$ convient : H_2 est vraie.

- Soit $n \geq 2$. Supposons H_n et H_{n-1} vraies (on pense à faire une récurrence double puisque c'est une récurrence double pour les polynômes de Tchebychev classiques, mais si on n'y pense pas, on s'en rend compte plus tard et on revient sur ses pas) et prouvons que H_{n+1} est vraie. Soit $\theta \in \mathbb{R}$.

$$\begin{aligned}
 \sin((n+2)\theta) &= \sin((n+1)\theta + \theta) \\
 &= \sin((n+1)\theta)\cos(\theta) + \sin(\theta)\cos((n+1)\theta)
 \end{aligned}$$

Or, à l'aide de la formule $\sin(a)\cos(b)$:

$$\sin(\theta)\cos((n+1)\theta) = \frac{1}{2}(\sin((n+2)\theta) - \sin(n\theta))$$

donc :

$$\sin((n+2)\theta) = \sin((n+1)\theta)\cos(\theta) + \frac{1}{2}(\sin((n+2)\theta) - \sin(n\theta))$$

Par conséquent :

$$2\sin((n+2)\theta) = 2\sin((n+1)\theta)\cos(\theta) + \sin((n+2)\theta) - \sin(n\theta)$$

Finalement, en mettant tous les $\sin((n+2)\theta)$ du même côté :

$$\sin((n+2)\theta) = 2\sin((n+1)\theta)\cos(\theta) - \sin(n\theta)$$

Par hypothèse de récurrence, il existe Q_n et Q_{n-1} tels que $\sin((n+1)\theta) = Q_n(\cos(\theta)) \times \sin(\theta)$ et $\sin(n\theta) = Q_{n-1}(\cos(\theta)) \times \sin(\theta)$ (c'est-là qu'on se rend compte qu'il faut une récurrence double) si bien que :

$$\begin{aligned}
 \sin((n+2)\theta) &= 2Q_n(\cos(\theta)) \times \sin(\theta)\cos(\theta) - Q_{n-1}(\cos(\theta)) \times \sin(\theta) \\
 &= \sin(\theta) \times (2\cos(\theta)Q_n(\cos(\theta)) - Q_{n-1}(\cos(\theta)))
 \end{aligned}$$

En conclusion, $Q_{n+1} = 2XQ_n - Q_{n-1}$ convient (on remarque que c'est la même relation de récurrence que les polynômes de Tchebychev « classiques ») : H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \geq 1$. D'où l'existence.

Unicité : Soit $n \geq 1$, soient P_n et Q_n deux polynômes qui conviennent. Alors, pour tout $\theta \in \mathbb{R}$, $\sin(\theta)P_n(\cos(\theta)) = \sin(\theta)Q_n(\cos(\theta))$. En particulier, pour tout $\theta \neq 0[\pi]$, le sinus n'est pas nul donc $P_n(\cos(\theta)) = Q_n(\cos(\theta))$: P_n et Q_n coïncident sur $\cos(\mathbb{R} \setminus \pi\mathbb{Z})$ donc sur $] -1; 1[$ (ou on peut dire aussi qu'ils coïncident au moins sur $\cos([0; \pi]) =] -1; 1[$) qui est un ensemble infini donc sont égaux. D'où l'unicité.

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 ?

Correction : Supposons \mathbb{K} fini et notons $\mathbb{K} = \{a_1; \dots; a_n\}$. Soit $P = (X - a_1) \dots (X - a_n) + 1$ (avec 1 le neutre du produit sur \mathbb{K} i.e. $1_{\mathbb{K}}$). Alors P est constant égal à 1 sur \mathbb{K} donc n'admet aucune racine dans \mathbb{K} . Il existe un polynôme à coefficients dans \mathbb{K} qui n'admet aucune racine sur \mathbb{K} donc \mathbb{K} n'est pas algébriquement clos. Par contraposée, on a le résultat voulu. Réciproque évidemment fausse : \mathbb{R} est infini mais n'est pas algébriquement clos car $X^2 + 1$ est à coefficients réels mais n'admet aucune racine réelle.

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

Correction : Notons $\mathbb{K} = \{a_1; \dots; a_n\}$ (avec les a_i deux à deux distincts) et $b_1 = f(a_1), \dots, a_n = f(a_n)$ (les b_i ne sont pas forcément distincts). À l'aide d'un polynôme d'interpolation de Lagrange, il existe $P \in \mathbb{K}_{n-1}[X]$ tel que $P(a_1) = b_1, \dots, P(a_n) = b_n$ i.e. $P \in \mathbb{K}_{n-1}[X]$ 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 $(p-1)! \equiv -1[p]$.

Correction :

1. On sait (cf. chapitre 18) que, dans un groupe d'ordre n , $y^n = e$. Or, $\mathbb{Z}/p\mathbb{Z}$ est un corps car p est premier donc $(\mathbb{Z}/p\mathbb{Z}, \times)$ est un groupe d'ordre $p-1$. Par conséquent, pour tout $k \neq 0$ (on travaille dans $\mathbb{Z}/p\mathbb{Z}$), $k^{p-1} = 1$ (le neutre du produit). Les $p-1$ éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont donc racines de $X^{p-1} - 1$: on a $p-1$ racines distinctes, le polynôme est de degré $p-1$ donc les racines sont simples, le polynôme est unitaire donc on a la factorisation voulue.
2. Si $p = 2$ le résultat est immédiat. Supposons $p \geq 3$. Il suffit d'évaluer en 0 : dans $\mathbb{Z}/p\mathbb{Z}$, cela donne : $-1 = (-1)^{p-1} \times (p-1)!$ et p est impair (c'est un nombre premier différent de 2) donc $-1 = -(p-1)!$. Rappelons que l'égalité dans $\mathbb{Z}/p\mathbb{Z}$ est équivalente à la congruence modulo p ce qui permet de conclure.

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 $x^{\frac{p-1}{2}} = 1$.

Correction : Supposons p impair sinon il n'y a rien à prouver (il n'y a qu'un élément qui est un carré et qui vérifie la deuxième condition). Si x est un carré alors il existe y tel que $x = y^2$ si bien que $x^{\frac{p-1}{2}} = y^{p-1}$ et on sait (cf. chapitre 18) que, dans un groupe d'ordre n , $y^n = e$. Or, $\mathbb{Z}/p\mathbb{Z}$ est un corps car p est premier donc $(\mathbb{Z}/p\mathbb{Z}, \times)$ est un groupe d'ordre $p-1$. Par conséquent, $y^{p-1} = 1$ (le neutre du produit) donc $x^{\frac{p-1}{2}} = 1$.

Réciproquement : montrons que $\mathbb{Z}/p\mathbb{Z}^*$ admet exactement $(p-1)/2$ carrés. L'application $f : x \mapsto x^2$ est évidemment un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ dans lui-même (il est impératif d'enlever 0 car ce n'est pas un morphisme de groupe de $(\mathbb{Z}/p\mathbb{Z}, +)$ dans lui-même). Son noyau (i.e. l'ensemble des antécédents de 1) est $\{\pm 1\}$ qui a deux éléments ($1 \neq -1 = p-1$, rappelons qu'on travaille modulo p , car p est impair donc différent de 2) donc, d'après l'exercice 32 du chapitre 18, l'image de f est de cardinal $(p-1)/2$, c'est-à-dire qu'il y a exactement $(p-1)/2$ carrés qui sont, d'après ce qui précède, racines du polynôme $X^{\frac{p-1}{2}} - 1$. Or, il ne peut pas admettre d'autre racines à cause de son degré, donc les nombres qui ne sont pas des carrés ne sont pas des racines de ce polynôme donc ne vérifient pas l'égalité $x^{\frac{p-1}{2}} = 1$, d'où l'équivalence.

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} .

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 :

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

Correction : En clair, on fait comme au chapitre 9, à ceci près qu'on n'a plus à s'embêter avec des limites.

1. Tout d'abord, la partie entière vaut 1 (ne pas l'oublier !). Puisque $X^4 - 1 = (X - 1)(X + 1)(X - i)(X + i)$ (on est sur \mathbb{C}), alors il existe $a, b, c, d \in \mathbb{C}$ uniques tels que :

$$\frac{X^4 + 1}{X^4 - 1} = \frac{X^4 + 1}{(X - 1)(X + 1)(X - i)(X + i)} = 1 + \frac{a}{X - 1} + \frac{b}{X + 1} + \frac{c}{X + i} + \frac{d}{X - i}$$

Ici, utilisons la formule explicite pour trouver les coefficients. Notons $P = X^4 + 1$ et $Q = X^4 - 1$. On sait (cf. cours) que si α est un pôle simple (ce qui est le cas ici), alors le coefficient de $1/(X - \alpha)$ est $P(\alpha)/Q'(\alpha)$. Puisque $Q' = 4X^3$, alors on trouve immédiatement :

$$\begin{aligned} a &= \frac{P(1)}{Q'(1)} \\ &= \frac{2}{4} \\ &= \frac{1}{2} \\ b &= \frac{P(-1)}{Q'(-1)} \\ &= \frac{2}{-4} \\ &= -\frac{1}{2} \\ c &= \frac{P(i)}{Q'(i)} \\ &= \frac{2}{-4i} \\ &= \frac{i}{2} \end{aligned}$$

puisque $1/i = -i$, et enfin

$$\begin{aligned} d &= \frac{P(-i)}{Q'(-i)} \\ &= \frac{2}{4i} \\ &= -\frac{i}{2} \end{aligned}$$

Finalement :

$$\frac{X^4 + 1}{X^4 - 1} = 1 + \frac{1}{2(X-1)} - \frac{1}{2(X+1)} + \frac{i}{2(X-i)} - \frac{i}{2(X+i)}$$

2. La partie entière ici est nulle. Là, revenons à la méthode du premier semestre (mais il n'est plus nécessaire de passer à la limite, il suffit d'évaluer) : il existe a, b, c réels tels que

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

En multipliant par $X-1$ et en évaluant en 1, on trouve $a = 1$. En multipliant par $X-2$ et en évaluant en 2, on trouve $b = -5$. Enfin, en multipliant par $X-3$ et en évaluant en 3, on trouve $c = 5$.

3. Là aussi, la partie entière est nulle. Les pôles sont doubles : il existe a, b, c, d réels tels que

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

En multipliant par X^2 et en évaluant en 0, on trouve $b = 1$. En multipliant par $(X-1)^2$ et en évaluant en 1, on trouve $d = 2$. En multipliant par X :

$$\frac{X^2 + 1}{X(X-1)^2} = a + \frac{b}{X} + \frac{cX}{X-1} + \frac{dX}{(X-1)^2}$$

En évaluant en x et en faisant tendre x vers $+\infty$, on trouve $a + c = 0$. Enfin, en évaluant en -1 , on trouve :

$$\begin{aligned} \frac{2}{4} &= -a + b - \frac{c}{2} + \frac{d}{4} \\ &= -a + 1 - \frac{c}{2} + \frac{2}{4} \end{aligned}$$

donc $a + \frac{c}{2} = 1$. On trouve par conséquent $c = -2$ et $a = 2$. En conclusion :

$$\frac{X^2 + 1}{X^2(X-1)^2} = \frac{2}{X} + \frac{1}{X^2} - \frac{2}{X-1} + \frac{2}{(X-1)^2}$$

4. Commençons par la division euclidienne de $X^{16} + 1$ par $X^4 + 1$. On trouve comme d'habitude :

$$X^{16} + 1 = (X^{12} - X^8 + X^4 - 1)(X^4 + 1) + 2$$

De plus, $X^4 - 1 = (X - e^{i\pi/4})(X - e^{3i\pi/4})(X - e^{5i\pi/4})(X - e^{7i\pi/4})$ (cf. cours). Il existe donc $a, b, c, d \in \mathbb{C}$ tels que :

$$\frac{X^{16} + 1}{X^4 + 1} = X^{12} - X^8 + X^4 - 1 + \frac{a}{X - e^{i\pi/4}} + \frac{b}{X - e^{3i\pi/4}} + \frac{c}{X - e^{5i\pi/4}} + \frac{d}{X - e^{7i\pi/4}}$$

Là aussi, utilisons l'expression explicite des coefficients : si on pose $A = X^{16} + 1$ et $B = X^4 + 1$, alors le coefficient de $1/(X - \alpha)$ vaut $A(\alpha)/B'(\alpha)$ avec $B' = 4X^3$. On trouve de même que ci-dessus (à l'aide de la 2π -périodicité) :

$$a = \frac{e^{-3i\pi/4}}{2}, b = \frac{e^{-9i\pi/4}}{2} = \frac{e^{-i\pi/4}}{2}, c = \frac{e^{-15i\pi/4}}{2} = \frac{e^{i\pi/4}}{2}, d = \frac{e^{-21i\pi/4}}{2} = \frac{e^{-5i\pi/4}}{2}$$

et on conclut comme précédemment.

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

Correction : Soit $n \geq 1$. Tout d'abord, si $k \geq 1$, $1+2+\dots+k = \frac{k(k+1)}{2}$ donc :

$$u_n = 2 \sum_{k=1}^n \frac{1}{k(k+1)}$$

Décomposons $1/X(X+1)$ en éléments simples : il existe a et b tels que

$$\frac{1}{X(X+1)} = \frac{a}{X} + \frac{b}{X+1}$$

En multipliant par X et en évaluant en 0 il vient $a = 1$ et en multipliant par $X+1$ et en évaluant en -1 il vient $b = -1$ si bien que

$$\begin{aligned} u_n &= 2 \sum_{k=1}^n \left(\frac{1}{k} - \frac{1}{k+1} \right) \\ &= 2 \times \left(1 - \frac{1}{n+1} \right) \\ &\xrightarrow{n \rightarrow +\infty} 2 \end{aligned}$$

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

Correction : cf. cours : si une telle fraction rationnelle existe, alors $\deg(F^2) = 2 \deg(F) = 1$ donc $\deg(F) = 1/2$ ce qui est impossible (le degré d'une fraction rationnelle est soit un entier **relatif**, soit $-\infty$).

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

Correction : La partie entière n'est rien d'autre que le quotient de la division euclidienne : en posant la division euclidienne, on trouve qu'il vaut $X^2 + X + 1$.

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 $F = G$.

Correction : Notons F et G sous forme irréductible, c'est-à-dire $F = P/Q$ et $G = A/B$ avec P et Q (respectivement A et B) premiers entre eux. Alors $P/Q = A/B$ en une infinité de points donc $BP = AQ$ en une infinité de points donc $BP = AQ$ (ce sont des polynômes). Puisque P divise AQ et P et Q sont premiers entre eux, alors P divise A . Par symétrie des rôles, A divise P donc A et P sont associés : il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda P$. Dès lors, $BP = \lambda PQ$. Si $P = 0$ alors $A = 0$ donc $F = G = 0$. Sinon, on peut simplifier par P ($\mathbb{K}[X]$ est un anneau intègre) donc $B = \lambda Q$. Finalement,

$$G = \frac{\lambda P}{\lambda Q} = \frac{P}{Q} = F$$

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

Correction : Là aussi, utilisons la formule donnant le coefficient d'un pôle simple à l'aide de la dérivée du dénominateur. Tout d'abord : les deux parties entières sont nulles, et $X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2ik\pi/n})$. Pour la première, il existe donc $a_0, \dots, a_{n-1} \in \mathbb{C}$ tels que :

$$\frac{X}{X^n - 1} = \sum_{k=0}^{n-1} \frac{a_k}{X - e^{2ik\pi/n}}$$

avec, pour tout k ($P(\alpha)/Q'(\alpha)$ avec $P = X$ et $Q = X^n - 1$ donc $Q' = nX^{n-1}$) :

$$\begin{aligned}
a_k &= \frac{e^{\frac{2ik\pi}{n}}}{ne^{\frac{2i(n-1)k\pi}{n}}} \\
&= \frac{e^{\frac{2ik\pi}{n}}}{ne^{2ik\pi - \frac{2ik\pi}{n}}} \\
&= \frac{e^{\frac{2ik\pi}{n}}}{ne^{-\frac{2ik\pi}{n}}} \\
&= \frac{e^{\frac{4ik\pi}{n}}}{n}
\end{aligned}$$

Pour la deuxième, il existe $a_0, \dots, a_{n-1} \in \mathbb{C}$ tels que :

$$\frac{X^{n-1}}{X^n - 1} = \sum_{k=0}^{n-1} \frac{a_k}{X - e^{2ik\pi/n}}$$

De même, pour tout $k \in \llbracket 0; n-1 \rrbracket$:

$$\begin{aligned}
a_k &= \frac{e^{\frac{2i(n-1)k\pi}{n}}}{ne^{\frac{2i(n-1)k\pi}{n}}} \\
&= \frac{1}{n}
\end{aligned}$$

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

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

Correction :

1. Puisque $\mathbb{C}(X)$ est un corps, c'est un anneau : il suffit donc de prouver que A est un sous-anneau de $\mathbb{C}(X)$.
 - $\deg(0) = -\infty \leq 0$ donc $0 \in A$: A est non vide.
 - Soient R_1 et R_2 dans A . Alors $\deg(R_1 + R_2) \leq \max(\deg(R_1), \deg(R_2)) \leq 0$: $R_1 + R_2 \in A$, A est stable par somme.
 - $\deg(-R_1) = \deg(R_1)$: A est stable par somme, c'est un sous-groupe de $\mathbb{C}(X)$.
 - $\deg(1) = 0$: $1 \in A$.
 - $\deg(R_1 R_2) = \deg(R_1) + \deg(R_2) \leq 0$: $R_1 R_2 \in A$, A est stable par produit.

En conclusion, A est bien un sous-anneau de \mathbb{C} , et en particulier c'est un anneau.

2. Non car il n'est pas stable par somme. Par exemple, $1/X$ et $1/(X+1)$ appartiennent à cet ensemble mais par leur somme qui vaut $(2X+1)/(X(X+1))$.

Exercice 8 : ♣♣ Décomposer en éléments simples sur \mathbb{C} la fraction rationnelle

$$F = \frac{1}{(X^3 - 1)^2}$$

On pourra comparer $F(X)$ et $F(jX)$.

Correction : Tout d'abord, $X^3 - 1 = (X-1)(X-j)(X-j^2)$ donc il existe a, b, c, d, e, f uniques tels que

$$F = \frac{a}{X-1} + \frac{b}{X-j} + \frac{c}{X-j^2} + \frac{d}{(X-1)^2} + \frac{e}{(X-j)^2} + \frac{f}{(X-j^2)^2}$$

Rappelons que $F = F(X)$. Calculons $F(jX)$: d'une part,

$$\begin{aligned}
F(jX) &= \frac{1}{((jX)^3 - 1)^2} \\
&= \frac{1}{(X^3 - 1)^2} \\
&= F(X)
\end{aligned}$$

D'autre part (on rappelle que $j^3 = 1$ donc $jX - 1 = j(X - j^2)$) :

$$\begin{aligned} F(jX) &= \frac{a}{jX-1} + \frac{b}{jX-j} + \frac{c}{jX-j^2} + \frac{d}{(jX-1)^2} + \frac{e}{(jX-j)^2} + \frac{f}{(jX-j^2)^2} \\ &= \frac{a}{j} \times \frac{1}{X-j^2} + \frac{b}{j} \times \frac{1}{X-1} + \frac{c}{j} \times \frac{1}{X-j} + \frac{d}{j^2} \times \frac{1}{(X-j^2)^2} + \frac{e}{j^2} \times \frac{1}{(X-1)^2} + \frac{f}{j^2} \times \frac{1}{(X-j)^2} \end{aligned}$$

Or, $F(jX) = F(X)$ donc

$$F(jX) = \frac{a}{X-1} + \frac{b}{X-j} + \frac{c}{X-j^2} + \frac{d}{(X-1)^2} + \frac{e}{(X-j)^2} + \frac{f}{(X-j^2)^2}$$

Par unicité des coefficients (rappelons que $1/j = j^2$ et $1/j^2 = j$) :

$$a = b/j = bj^2, b = c/j = cj^2, c = a/j = aj^2, d = e/j^2 = ej, e = f/j^2 = fj, f = d/j^2 = dj$$

Les équations $c = aj^2$ et $f = dj$ sont redondantes puisqu'elles découlent des autres : en effet, $a = bj^2$ et $b = cj^2$ donc $a = cj^4 = cj$ donc $c = aj^2$, et idem pour l'autre. Ainsi, on obtient quatre équations :

$$a = cj, b = cj^2, d = fj^2, e = fj,$$

Par conséquent :

$$F = \frac{cj}{X-1} + \frac{cj^2}{X-j} + \frac{c}{X-j^2} + \frac{fj^2}{(X-1)^2} + \frac{fj}{(X-j)^2} + \frac{f}{(X-j^2)^2}$$

Maintenant, il n'y a plus que deux inconnues, on peut les trouver à la main. En évaluant en 0, on trouve (en se souvenant que $1/j = j^2$ et $1/j^2 = j$) :

$$1 = -cj - cj - cj + fj^2 + fj^2 + fj^2$$

c'est-à-dire que $3fj^2 - 3cj = 1$. Enfin, en évaluant en -1 (rappelons que $1 + j + j^2 = 0$ donc $-1 - j = j^2$ etc.) :

$$\begin{aligned} \frac{1}{4} &= \frac{-cj}{2} + c + cj^2 + \frac{fj^2}{4} + f + fj \\ &= \frac{-cj}{2} + c(1 + j^2) + \frac{fj^2}{4} + f(1 + j) \\ &= \frac{-cj}{2} - cj + \frac{fj^2}{4} - fj^2 \\ &= \frac{-3cj}{2} - \frac{3fj^2}{4} \end{aligned}$$

si bien que $1 = -6cj - 3fj^2$. En sommant avec l'équation trouvée précédemment, il vient $-9cj = 2$ donc $c = \frac{-2}{9j} = \frac{-2j^2}{9}$ et donc

$$\begin{aligned} 3fj^2 &= 1 + 3cj \\ &= 1 - \frac{6}{9} \\ &= \frac{1}{3} \end{aligned}$$

et on trouve $f = 1/9j^2 = j/9$ ce qui permet de conclure.

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

Correction : Si P est constant (non nul) alors $P' = 0$ donc ne divise que lui-même donc ne divise pas P . Supposons à présent P non constant i.e. de degré $n \geq 1$. Alors P' est de degré $n - 1$ donc P' divise P si et seulement s'il existe Q de degré 1 tel que $P = P' \times Q$ c'est-à-dire

$$\frac{P'}{P} = \frac{1}{Q}$$

En d'autres termes, P' divise P si et seulement si la décomposition en éléments simples de P'/P ne comporte qu'un seul terme. Notons $P = a_n(X - x_1)^{\alpha_1} \times \cdots \times (X - x_k)^{\alpha_k}$ sous forme scindée (avec les x_i deux à deux distincts) si bien que (cf. cours) la décomposition de P'/P en éléments simples est :

$$\frac{P'}{P} = \sum_{i=1}^k \frac{\alpha_i}{X - x_i}$$

Par unicité, P' divise P si et seulement si $k = 1$ si et seulement si P admet une seule racine (multiple) si et seulement si P est de la forme $a_n(X - x_1)^n$.

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.

Correction : On suppose donc sans le dire que P n'est pas constant. Soit $n = \deg(P) \geq 1$. Notons $P = a_n(X - x_1) \cdots (X - x_n)$ où $x_1 < \cdots < x_n$ (en particulier, les x_k sont réels). Supposons enfin $\alpha \neq 0$ sinon le fait que Q_α soit à racines simples est immédiat.

1. Précisons que le domaine de définition de Q_α/P (une dernière fois : de la fonction rationnelle associée) est :

$$\mathbb{R} \setminus \{x_1; \dots; x_n\} =]-\infty; x_1[\cup]x_1; x_2[\cup \cdots \cup]x_{n-1}; x_n[\cup]x_n; +\infty[$$


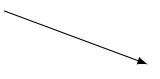
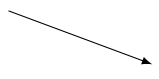

On a :

$$\begin{aligned} \frac{Q_\alpha}{P} &= 1 + \alpha \times \frac{P'}{P} \\ &= 1 + \sum_{k=1}^n \frac{1}{X - x_k} \end{aligned}$$

en utilisant la décomposition en éléments simples de P'/P . Q_α est dérivable et, pour tout $t \neq x_1, \dots, x_n$:

$$\left(\frac{Q_\alpha}{P}\right)'(t) = \sum_{k=1}^n \frac{-\alpha}{(t - x_k)^2}$$

Supposons $\alpha > 0$ (raisonnement analogue dans l'autre cas). On obtient le tableau de variations suivant de la même façon que dans l'exercice 40 du chapitre 13 :

x	$-\infty$	x_1	x_2	\dots	x_{n-1}	x_n	$+\infty$
$(Q_\alpha/P)'(x)$		—	—	\dots	\dots	—	—
Q_α/P							

Les limites en $\pm\infty$ valant 1 (ne pas l'oublier!), les limites à gauche en les x_i valant $-\infty$ et les limites à droite $+\infty$ (idem que dans l'exercice 40 du chapitre 13).

2. En appliquant n fois le théorème de la bijection (sur chaque intervalle $]x_i; x_{i+1}[$ pour $i \in \llbracket 1; n-1 \rrbracket$ et sur $] -\infty; x_1 [$), on trouve que Q_α/P s'annule exactement n fois sur \mathbb{R} . Or, Q_α est la somme d'un polynôme de degré n et d'un polynôme de degré $n-1$ donc est de degré n : Q_α a un nombre de racines distinctes égal à son degré, il est scindé à racines simples.

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

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

Correction :

1. Suivons l'indication de l'énoncé :

$$\begin{aligned} G(X-1) &= \frac{(X-1)^n}{X^n} \\ &= \frac{\sum_{k=0}^n \binom{n}{k} (-1)^k X^{n-k}}{X^n} \\ &= \sum_{k=0}^n \frac{\binom{n}{k} (-1)^k}{X^k} \end{aligned}$$

C'est une décomposition en éléments simples : par unicité, c'est la bonne. Dès lors, la décomposition en éléments simples de G est :

$$G = \sum_{k=0}^n \frac{\binom{n}{k} (-1)^k}{(X+1)^k}$$

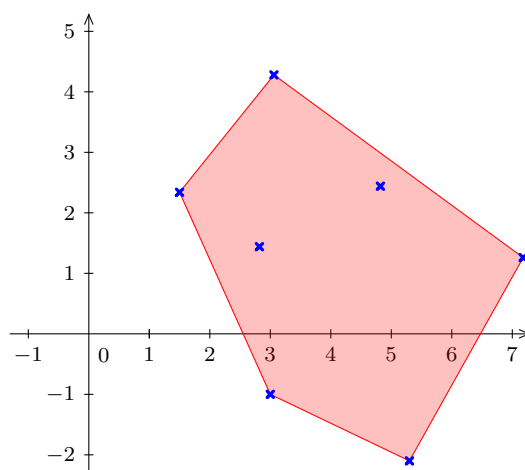
2. Notons H cette fraction rationnelle. Alors $H = G(X^2)$. D'après ce qui précède :

$$G = \sum_{k=0}^n \frac{\binom{n}{k} (-1)^k}{(X^2+1)^k}$$

Puisqu'on est sur \mathbb{R} et pas sur \mathbb{C} , on a une décomposition en éléments simples : c'est la bonne par unicité.

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 $\bar{0} = 0$...

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 colorée :



Correction : Notons $P = a_n(X - z_1) \dots (X - z_n)$ où les z_k sont des complexes distincts. Soit $z \in \mathbb{C}$ une racine de P' ($z \neq z_1, \dots, z_n$ puisque P est à racines simples donc P et P' n'ont aucune racine commune). Dès lors, en utilisant la décomposition en éléments simples de P'/P :

$$\frac{P'(z)}{P(z)} = 0 = \sum_{k=1}^n \frac{1}{z - z_k}$$

Suivons l'indication de l'énoncé et conjuguons cette égalité, ce qui donne :

$$\begin{aligned}\bar{0} &= 0 = \sum_{k=1}^n \frac{1}{z - z_k} \\ &= \sum_{k=1}^n \frac{z - z_k}{|z - z_k|^2}\end{aligned}$$

Isolons z :

$$z \times \sum_{k=1}^n \frac{1}{|z - z_k|^2} = \sum_{k=1}^n \frac{z_k}{|z - z_k|^2}$$

Pour tout $k \in \llbracket 1; n \rrbracket$, notons $\alpha_k = 1/|z - z_k|^2 \in \mathbb{R}_+$ et

$$S = \sum_{k=1}^n \frac{1}{|z - z_k|^2} = \sum_{k=1}^n \alpha_k$$

Alors $z \times S = \sum_{k=1}^n \alpha_k z_k$ si bien que :

$$z = \sum_{k=1}^n \frac{\alpha_k z_k}{S}$$

z est combinaison linéaire des z_k , les racines de P , avec des coefficients positifs, les α_k/S , de somme 1, puisque

$$\begin{aligned}\sum_{k=1}^n \frac{\alpha_k}{S} &= \frac{1}{S} \times \sum_{k=1}^n \alpha_k \\ &= \frac{1}{S} \times S \\ &= 1\end{aligned}$$

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

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

Correction :

1. Cela ressemble au résultat du cours, disant que les coefficients de $1/(X - \alpha)$ lorsque α est racine simple de Q , dans la décomposition en éléments simples de P/Q , est $P(\alpha)/Q'(\alpha)$. En suivant cette idée, $1/P'(z_k)$ est le coefficient de $1/(X - z_k)$ dans la décomposition en éléments simples de $1/P$. En d'autres termes :

$$\frac{1}{P} = \sum_{k=1}^n \frac{1}{P'(z_k) \times (X - z_k)}$$

En évaluant en 0 et en multipliant par -1 , on a le résultat voulu.

2. Si $n = 1$ alors P' est constant égal au coefficient dominant a_1 de P donc cette somme vaut $1/a_1$. Supposons dorénavant que $n = 2$. Reprenons l'égalité de la question précédente :

$$\frac{1}{P} = \sum_{k=1}^n \frac{1}{P'(z_k) \times (X - z_k)}$$

En évaluant en $x \in \mathbb{R}$, différent des z_k , et en multipliant par x :

$$\frac{x}{P(x)} = \sum_{k=1}^n \frac{x}{P'(z_k) \times (x - z_k)}$$

Si on fait tendre x vers $+\infty$, le membre de droite tend vers la somme voulue, et le terme de gauche vers 0 puisque P est de degré $n \geq 2$. Par unicité de la limite, la somme est nulle.

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

Correction : Comme précédemment, les racines de R étant simples, cela évoque la décomposition en éléments simples de P/R , qui est donc :

$$\frac{P}{R} = \sum_{k=0}^n \frac{P(k)}{R'(k)(X-k)}$$

Comme dans l'exercice précédent, en évaluant en x puis en faisant tendre x vers $+\infty$, le membre de droite tend vers la somme voulue, tandis que le membre de gauche tend vers 1 : en effet, P est unitaire de degré n et R unitaire de degré $n+1$ donc, quand on multiplie par x , on a le quotient de deux fonctions polynômes unitaires de degré $n+1$ donc de la forme $x^{n+1} + \dots$ donc le rapport tend bien vers 1. En conclusion, par unicité de la limite :

$$\sum_{k=0}^n \frac{P(k)}{R'(k)} = 1$$

Raisonnons par l'absurde et supposons que $|P(0)|, \dots, |P(n)|$ soient tous inférieurs stricts à $n!/2^n$. D'après ce qui précède et l'inégalité triangulaire,

$$1 \leq \sum_{k=0}^n \left| \frac{P(k)}{R'(k)} \right| < \frac{n!}{2^n} \sum_{k=0}^n \frac{1}{|R'(k)|}$$

c'est-à-dire que

$$\sum_{k=0}^n \frac{1}{|R'(k)|} > \frac{2^n}{n!}$$

Or :

$$R' = \sum_{k=0}^n \prod_{i \neq k} (X-i)$$

si bien que, pour tout $k \in \llbracket 0; n \rrbracket$ (il ne reste que le terme d'indice k car les autres sont nuls en k car contiennent $(X-k)$) :

$$\begin{aligned} R'(k) &= \prod_{i \neq k} (k-i) \\ &= k(k-1) \dots (k-(k-1)) \times (k-(k+1)) \dots (k-n) \\ &= k! \times (-1)(-2) \dots (k-n) \\ &= (-1)^{n-k} k!(n-k)! \\ &= \frac{(-1)^n n!}{\binom{n}{k}} \end{aligned}$$

Finalement :

$$\sum_{k=0}^n \frac{1}{|R'(k)|} = \frac{1}{n!} \sum_{k=0}^n \binom{n}{k} = \frac{2^n}{n!}$$

ce qui est absurde.

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

Correction : On montre comme en DM que

$$T_n = 2^{n-1} \prod_{k=0}^{n-1} \left(X - \cos \left(\frac{(2k+1)\pi}{2n} \right) \right)$$

Pour tout $k \in \llbracket 0; n-1 \rrbracket$, posons $x_k = \cos \left(\frac{(2k+1)\pi}{2n} \right)$ si bien que

$$\frac{1}{T_n} = \sum_{k=0}^{n-1} \frac{1}{P'(x_k)(X - x_k)}$$

Or, pour tout $\theta \in \mathbb{R}$, $T_n(\cos(\theta)) = \cos(n\theta)$. En dérivant, il vient : $-\sin(\theta) \times T_n'(\cos(\theta)) = -n \sin(n\theta)$. Ainsi :

$$\forall k \in \llbracket 0; n-1 \rrbracket, \sin\left(\frac{(2k+1)\pi}{2n}\right) \times T_n'(x_k) = -n \sin\left(\frac{(2k+1)\pi}{2}\right)$$

D'une part, $(2k+1)\pi/2n \not\equiv 0[\pi]$ donc on peut diviser par le sinus de gauche, et d'autre part,

$$\sin\left(\frac{(2k+1)\pi}{2}\right) = \sin(k\pi + \pi/2) = (-1)^k$$

Finalement :

$$\frac{1}{T_n} = \sum_{k=0}^{n-1} \frac{n(-1)^{k+1}}{\sin\left(\frac{(2k+1)\pi}{2n}\right) \left(X - \cos\left(\frac{(2k+1)\pi}{2n}\right)\right)}$$

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

1. Soit $z = x + iy \in \mathbb{C} \setminus \mathbb{R}$. Soit $x \in \mathbb{R}$. Montrer que l'intégrale $\int_{-x}^x \frac{dt}{t-z}$ est bien définie puis que

$$\int_{-A}^A \frac{dt}{t-z} \xrightarrow{A \rightarrow +\infty} \operatorname{sgn}(y) \times i\pi$$

où $\operatorname{sgn}(a)$ 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 $\frac{X^{2n}}{1+X^{2m}}$ est :

$$\frac{X^{2n}}{1+X^{2m}} = \sum_{k=0}^{2m-1} \frac{\alpha_k}{X - \omega^{2k+1}}$$

où, pour tout $k \in \llbracket 0; 2m-1 \rrbracket$, $\alpha_k = \frac{-\omega^{(2k+1)(2n+1)}}{2m}$.

3. Montrer que $\sum_{k=m}^{2m-1} \alpha_k = -\sum_{k=0}^{m-1} \alpha_k$.

4. Donner le signe de $\operatorname{Im}(\omega^{2k+1})$ selon la valeur de $k \in \llbracket 0; 2m-1 \rrbracket$.

5. Montrer que

$$\int_{-x}^x \frac{t^{2n}}{1+t^{2m}} dt \xrightarrow{x \rightarrow +\infty} \frac{\pi}{m \sin\left(\frac{2n+1}{2m}\pi\right)}$$

On pourra poser $\beta = \omega^{2n+1}$ pour simplifier les calculs.

Correction :

1. Rappelons que z est un complexe non réel, donc la valeur interdite de $t \mapsto \frac{1}{t-z}$ n'est pas réelle : cette fonction est donc continue sur \mathbb{R} . Par conséquent, l'intégrale $\int_{-A}^A \frac{dt}{t-z}$ est bien définie en tant qu'intégrale d'une fonction continue sur un segment. Notons cette intégrale I_A . On a alors

$$\begin{aligned} I_A &= \int_{-A}^A \frac{dt}{t-x-iy} \\ &= \int_{-A}^A \frac{t-x+iy}{(t-x)^2+y^2} dt \\ &= \int_{-A}^A \frac{t-x}{(t-x)^2+y^2} dt + iy \int_{-A}^A \frac{dt}{(t-x)^2+y^2} \end{aligned}$$

La première intégrale est (à un facteur 2 près) l'intégrale d'une fonction de la forme u'/u et, dans la seconde, on pense à de l'Arctan : on met donc le y^2 en facteur pour faire apparaître une quantité de la forme $1/(1+u^2)$.

$$I_A = \frac{1}{2} \int_{-A}^A \frac{2(t-x)}{(t-x)^2 + y^2} dt + \frac{iy}{y^2} \int_{-A}^A \frac{dt}{1 + \left(\frac{t-x}{y}\right)^2}$$

Par conséquent :

$$I_A = \frac{1}{2} [\ln((t-x)^2 + y^2)]_{-A}^A + \frac{i}{y} \left[y \times \text{Arctan}\left(\frac{t-x}{y}\right) \right]_{-A}^A$$

Ainsi :

$$I_A = \frac{1}{2} \ln\left(\frac{(A-x)^2 + y^2}{(-A-x)^2 + y^2}\right) + i \text{Arctan}\left(\frac{A-x}{y}\right) - i \text{Arctan}\left(\frac{-A-x}{y}\right)$$

La quantité dans le \ln tend vers 1 quand A tend vers $+\infty$ donc le \ln tend vers 0 (continuité du \ln). Intéressons-nous à présent aux Arctan. Cherchons la limite des quantités à l'intérieur. Il faut pour cela connaître le signe de y . Supposons $y > 0$. Alors,

$$\frac{A-x}{y} \xrightarrow{A \rightarrow +\infty} +\infty \quad \text{et} \quad \frac{-A-x}{y} \xrightarrow{A \rightarrow +\infty} -\infty$$

Dès lors :

$$\text{Arctan}\left(\frac{A-x}{y}\right) \xrightarrow{A \rightarrow +\infty} \frac{\pi}{2} \quad \text{et} \quad \text{Arctan}\left(\frac{-A-x}{y}\right) \xrightarrow{A \rightarrow +\infty} -\frac{\pi}{2}$$

ce qui implique que $I_A \xrightarrow{A \rightarrow +\infty} i\pi$. Supposons à présent $y < 0$. Alors :

$$\frac{A-x}{y} \xrightarrow{A \rightarrow +\infty} -\infty \quad \text{et} \quad \frac{-A-x}{y} \xrightarrow{A \rightarrow +\infty} +\infty$$

Dès lors :

$$\text{Arctan}\left(\frac{A-x}{y}\right) \xrightarrow{A \rightarrow +\infty} -\frac{\pi}{2} \quad \text{et} \quad \text{Arctan}\left(\frac{-A-x}{y}\right) \xrightarrow{A \rightarrow +\infty} \frac{\pi}{2}$$

ce qui implique que $I_A \xrightarrow{A \rightarrow +\infty} -i\pi$. Dans tous les cas :

$$I_A \xrightarrow{A \rightarrow +\infty} \text{sgn}(y) \times i\pi$$

En effet, y est non nul car $z \notin \mathbb{R}$.

2. Cherchons tout d'abord les pôles de cette fraction rationnelle. Soit $z \in \mathbb{C}$. Alors :

$$\begin{aligned} z^{2m} + 1 = 0 &\iff z^{2m} = -1 \\ &\iff z \text{ est une racine } 2m\text{-ième de } -1 = e^{i\pi} \\ &\iff \exists k \in \llbracket 0; 2m-1 \rrbracket, z = e^{i\left(\frac{\pi}{2m} + \frac{2k\pi}{2m}\right)} \\ &\iff \exists k \in \llbracket 0; 2m-1 \rrbracket, z = e^{\frac{(2k+1)\pi}{2m}} \\ &\iff \exists k \in \llbracket 0; 2m-1 \rrbracket, z = \omega^{2k+1} \end{aligned}$$

On a $2m$ racines distinctes et $Q = 1 + X^{2m}$ est de degré $2m$ donc elles sont simples : si on note $P = X^{2n}$, alors

$$\frac{X^{2n}}{1 + X^{2m}} = \sum_{k=0}^{2m-1} \frac{\alpha_k}{X - \omega^{2k+1}}$$

où, pour tout $k \in \llbracket 0; 2m-1 \rrbracket$:

$$\begin{aligned}
\alpha_k &= \frac{P(\omega^{2k+1})}{Q'(\omega^{2k+1})} \\
&= \frac{(\omega^{2k+1})^{2n}}{2m(\omega^{2k+1})^{2m-1}} \\
&= \frac{(\omega^{2k+1})^{2n}}{2m(\omega^{2m-1})^{2k+1}} \\
&= \frac{(\omega^{2k+1})^{2n}}{2m\left(-\frac{1}{\omega}\right)^{2k+1}} \\
&= -\frac{(\omega^{2k+1})^{2n}\omega^{2k+1}}{2m}
\end{aligned}$$

La troisième ligne vient du fait que $(z^a)^b = (z^b)^a$, la quatrième vient du fait que $\omega^{2m} = -1$ donc $\omega^{2m-1} = -1/\omega$ et la dernière vient du fait que $(-1)^{2k+1} = -1$, ce qui permet de conclure.

3. En utilisant encore une fois le fait que $\omega^{2m} = -1$, et en faisant un changement d'indice :

$$\begin{aligned}
\sum_{k=m}^{2m-1} \alpha_k &= -\frac{1}{2m} \sum_{k=m}^{2m-1} \omega^{(2n+1)(2k+1)} \\
&= -\frac{1}{2m} \sum_{j=0}^{m-1} \omega^{(2n+1)(2j+2m+1)} \\
&= -\frac{1}{2m} \sum_{k=0}^{m-1} \omega^{(2n+1)(2k+1)} \times \omega^{2m(2n+1)} \\
&= -\frac{1}{2m} \sum_{k=0}^{m-1} \omega^{(2n+1)(2k+1)} \times (-1)^{2n+1} \\
&= \frac{1}{2m} \sum_{k=0}^{m-1} \omega^{(2n+1)(2k+1)}
\end{aligned}$$

ce qui est le résultat voulu.

4. Tout d'abord, $\text{Im}(\omega^{2k+1}) = \sin\left(\frac{(2k+1)\pi}{2m}\right)$. Cherchons à quel intervalle appartient la quantité à l'intérieur du sinus. Puisque $0 \leq k \leq 2m-1$ alors (notez l'absence subtile d'équivalences) en multipliant par 2, en ajoutant 1, en multipliant par π et en divisant par $2m$, il vient :

$$\frac{\pi}{2m} \leq \frac{(2k+1)\pi}{2m} \leq 2\pi - \frac{\pi}{2m}$$

donc

$$\frac{(2k+1)\pi}{2m} \in]0; 2\pi[$$

Or, sur $[0; 2\pi]$, le sinus est strictement positif sur $]0; \pi[$ et strictement négatif sur $] \pi; 2\pi[$ (la quantité ne peut pas être égale à π car on ne peut pas avoir $2m = 2k+1$ car l'un est pair et l'autre impair). Cherchons pour quelles valeurs de k la quantité dans le sinus est inférieure strictement à π .

$$\frac{(2k-1)\pi}{2m} < \pi \iff (2k-1) < 2m \iff k < \frac{2m-1}{2} = m - \frac{1}{2}$$

Or, k est à valeurs entières, donc cela équivaut à $k \leq m-1$. Le résultat en découle : $\text{Im}(\omega^{2k+1}) > 0$ si $k \in \llbracket 0; m-1 \rrbracket$ et < 0 si $k \in \llbracket m; 2m-1 \rrbracket$.

5. Soit $A \geq 0$. D'après la question 2, et par linéarité de l'intégrale :

$$\begin{aligned}
\int_{-A}^A \frac{x^{2n}}{1+x^{2m}} dx &= \sum_{k=0}^{2m-1} \alpha_k \int_{-A}^A \frac{dx}{x - \omega^{2k+1}} \\
&= \sum_{k=0}^{m-1} \alpha_k \int_{-A}^A \frac{dx}{x - \omega^{2k+1}} + \sum_{k=m}^{2m-1} \alpha_k \int_{-A}^A \frac{dx}{x - \omega^{2k+1}}
\end{aligned}$$

Or, d'après la question 1, quand $A \rightarrow +\infty$, les intégrales de la première somme tendent vers $i\pi$ (car les ω^{2k+1} ont une partie imaginaire strictement positive d'après la question précédente), et celles de la seconde vers $-i\pi$. Par conséquent,

$$\int_{-A}^A \frac{x^{2n}}{1+x^{2m}} dx \xrightarrow{A \rightarrow +\infty} \sum_{k=0}^{m-1} i\pi \alpha_k - \sum_{k=m}^{2m-1} i\pi \alpha_k$$

Donc, d'après la question 3,

$$\int_{-A}^A \frac{x^{2n}}{1+x^{2m}} dx \xrightarrow{A \rightarrow +\infty} \sum_{k=0}^{m-1} i\pi \alpha_k + \sum_{k=0}^{m-1} i\pi \alpha_k = 2i\pi \sum_{k=0}^{m-1} \alpha_k = 2i\pi \sum_{k=0}^{m-1} \alpha_k$$

Il suffit à présent de calculer cette somme pour conclure. Suivons l'indication de l'énoncé et posons $\beta = \omega^{2n+1}$ ce qui donne

$$\begin{aligned}
\sum_{k=0}^{m-1} \alpha_k &= -\frac{1}{2m} \sum_{k=0}^{m-1} \beta^{2k+1} \\
&= -\frac{\beta}{2m} \sum_{k=0}^{m-1} (\beta^2)^k \\
&= -\frac{\beta}{2m} \times \frac{1 - \beta^{2m}}{1 - \beta^2} \\
&= -\frac{e^{\frac{(2n+1)i\pi}{2m}}}{2m} \times \frac{1 - e^{(2n+1)i\pi}}{1 - e^{\frac{(2n+1)i\pi}{m}}} \quad (\text{car } \beta = e^{\frac{(2n+1)i\pi}{2m}}) \\
&= -\frac{e^{\frac{(2n+1)i\pi}{2m}}}{2m} \times \frac{2}{1 - e^{\frac{(2n+1)i\pi}{m}}} \quad (\text{car } e^{i\pi} = -1 \text{ et } 2n+1 \text{ est impair}) \\
&= -\frac{e^{\frac{(2n+1)i\pi}{2m}}}{m} \times \frac{1}{e^{\frac{(2n+1)i\pi}{2m}} \left(e^{-\frac{(2n+1)i\pi}{2m}} - e^{\frac{(2n+1)i\pi}{2m}} \right)} \quad (\text{angle-moitié}) \\
&= -\frac{1}{m} \times \frac{1}{-2i \sin\left(\frac{(2n+1)\pi}{2m}\right)} \quad (\text{formules d'Euler})
\end{aligned}$$

En conclusion, on a bien :

$$\int_{-A}^A \frac{x^{2n}}{1+x^{2m}} dx \xrightarrow{A \rightarrow +\infty} \frac{\pi}{m \sin\left(\frac{(2n+1)\pi}{2m}\right)}$$

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, \dots sont des entiers naturels supérieurs ou égaux à 1 et les matrices considérées appartiennent à $\mathcal{M}_n(\mathbb{K})$.

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 $\mathcal{M}_n(\mathbb{K})$.
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 $\mathcal{M}_n(\mathbb{K})$.
5. L'ensemble des matrices triangulaires supérieures avec des 1 sur la diagonale est un sous-groupe de $\text{GL}_n(\mathbb{K})$.
6. $\mathcal{M}_n(\mathbb{N})$ est stable par produit.
7. Si $M \in \mathcal{M}_n(\mathbb{Z})$ est inversible alors $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$.
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. $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ | 3. $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ | 5. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix}$ | 7. $\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$ |
| 2. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | 4. $\begin{pmatrix} 0 & 4 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix}$ | 6. $\begin{pmatrix} 3 & 6 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} -2 & 2 \\ 1 & -1 \end{pmatrix}$ | |

Exercice 2 : ✪ Soient les matrices suivantes :

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

$$E = (5 \quad 2 \quad -4)$$

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

Correction : Rappelons qu'un produit de matrice existe si et seulement si le nombre de colonnes de la matrice de gauche est égal au nombre de lignes de la matrice de droite. Par conséquent, parmi les 25 produits possibles, les seuls bien définis sont les suivants :

$$\begin{aligned} \bullet A^2 &= \begin{pmatrix} 34 & 13 & 21 & 24 \\ 60 & 33 & 23 & 28 \\ 14 & 18 & 34 & 44 \\ 17 & 1 & 12 & 13 \end{pmatrix} & \bullet BC &= \begin{pmatrix} 12 & 29 & -10 & 32 \\ 1 & 0 & 2 & 7 \\ 1 & 7 & 0 & 11 \\ -3 & 13 & -2 & 7 \end{pmatrix} & \bullet CB &= \begin{pmatrix} 7 & -6 & 0 \\ 17 & 3 & 5 \\ 38 & 27 & 9 \end{pmatrix} \\ \bullet AB &= \begin{pmatrix} 30 & 7 & 7 \\ 58 & 33 & 17 \\ 11 & 44 & 19 \\ 10 & -6 & 1 \end{pmatrix} & \bullet BD &= \begin{pmatrix} -3 \\ 7 \\ 6 \\ 2 \end{pmatrix} & \bullet DE &= \begin{pmatrix} 5 & 2 & -4 \\ -10 & -4 & 8 \\ 15 & 6 & -12 \end{pmatrix} \\ & & \bullet CA &= \begin{pmatrix} 8 & 0 & 12 & 13 \\ 5 & 6 & 41 & 47 \\ 1 & 24 & 27 & 32 \end{pmatrix} & \bullet EC &= (-19 \quad 16 \quad -4 \quad -21) \\ & & & & \bullet ED &= (-11) \end{aligned}$$

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

Correction :

$$A^\top = \begin{pmatrix} 1 & 5 & 9 & -1 \\ 2 & 0 & 1 & 2 \\ 3 & 7 & 0 & 1 \\ 4 & 8 & 0 & 1 \end{pmatrix} \quad B^\top = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & -1 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{pmatrix} \quad C^\top = \begin{pmatrix} -1 & 1 & 4 \\ 2 & 5 & 1 \\ 0 & -2 & 0 \\ 1 & 3 & 8 \end{pmatrix}$$

$$D^\top = (1 \quad -2 \quad 3) \quad E^\top = \begin{pmatrix} 5 \\ 2 \\ -4 \end{pmatrix}$$

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

$$\forall (i, j) \in \llbracket 1; n \rrbracket^2, \quad A_{i,j} = i + j \quad \text{et} \quad B_{i,j} = i - j$$

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

Correction : C et D sont toutes les deux carrées de taille n . On a $C = (A_{i,j} + B_{i,j}) = (2i)_{1 \leq i, j \leq n}$ et, pour tous i et j :

$$\begin{aligned} D_{i,j} &= \sum_{k=1}^n A_{i,k} B_{k,j} \\ &= \sum_{k=1}^n (i+k) \times (k-j) \\ &= \sum_{k=1}^n (k^2 + k(i-j) - ij) \\ &= \frac{n(n+1)(2n+1)}{6} + (i-j) \times \frac{n(n+1)}{2} - nij \end{aligned}$$

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

Correction : On a AB est symétrique $\iff (AB)^\top = AB$ ssi $B^\top A^\top = AB$ (car on inverse l'ordre quand on transpose un produit) ssi $BA = AB$ (car A et B sont symétriques), ce qui est le résultat voulu.

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 $A \in \mathcal{M}_n(\mathbb{K})$ 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 $A \in \text{GL}_n(\mathbb{K})$.

Correction : On trouve $A^2 + 5A = -4I_3$ et donc $A \times \left(-\frac{1}{4}(A + 5I_3)\right) = I_n$: A est inversible et $A^{-1} = -\frac{1}{4}(A + 5I_3)$.

Dans le cas général :

$$A^{2024} + \sum_{k=1}^{2023} \lambda_k A^k = -\lambda_0 I_n$$

et $\lambda_0 \neq 0$ donc on peut diviser par $-\lambda_0$ ce qui donne :

$$A \times \left[\frac{-1}{\lambda_0} \left(A^{2023} + \sum_{k=1}^{2023} \lambda_k A^{k-1} \right) \right] = I_n$$

donc A est inversible et

$$A^{-1} = \frac{-1}{\lambda_0} \left(A^{2023} + \sum_{k=1}^{2023} \lambda_k A^{k-1} \right)$$

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

Correction : Raisonnons par l'absurde et supposons qu'il y a au plus une matrice non inversible. En d'autres termes, il y a au moins deux matrices inversibles. Supposons que A et C soient inversibles. Alors, en multipliant par A^{-1} à gauche et par C^{-1} à droite, il vient $B = 0$ ce qui est absurde car B est non nulle. Supposons à présent A et B inversibles. En multipliant par A^{-1} à gauche, il vient : $BC = 0$. En multipliant à présent par B^{-1} (toujours à gauche), il vient $C = 0$ ce qui est aussi absurde. Le cas où B et C sont inversibles est analogue. Il n'est pas nécessaire de traiter le cas où A, B, C sont inversibles : il est contenu dans les cas précédents. En effet, quand nous avons supposé A et C inversibles, nous n'avons pas supposé B non inversible : nous avons donc examiné le cas où les trois matrices sont inversibles. En conclusion, dans tous les cas, c'est absurde : au moins deux matrices 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. $\begin{pmatrix} 1 & 2 & -1 \\ 2 & -1 & -1 \\ -1 & 2 & 0 \end{pmatrix}$

Correction :

1.

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 3 & 1 & 2 & 0 & 1 & 0 \\ 2 & 3 & 1 & 0 & 0 & 1 \end{array} \right)$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -5 & -7 & -3 & 1 & 0 \\ 0 & -1 & -5 & -2 & 0 & 1 \end{array} \right) \begin{array}{l} L_2 \leftarrow L_2 - 3L_1 \\ L_3 \leftarrow L_3 - 2L_1 \end{array}$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -1 & -5 & -2 & 0 & 1 \\ 0 & -5 & -7 & -3 & 1 & 0 \end{array} \right) L_3 \leftrightarrow L_2$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 5 & 2 & 0 & -1 \\ 0 & -5 & -7 & -3 & 1 & 0 \end{array} \right) L_2 \leftarrow -L_2$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 5 & 2 & 0 & -1 \\ 0 & 0 & 18 & 7 & 1 & -5 \end{array} \right) L_3 \leftarrow L_3 + 5L_2$$

À ce stade, on sait que la matrice est bien inversible (mais c'est inutile de le préciser).

$$\begin{pmatrix} 1 & 2 & 3 & | & 1 & 0 & 0 \\ 0 & 1 & 5 & | & 2 & 0 & -1 \\ 0 & 0 & 1 & | & 7/18 & 1/18 & -5/18 \end{pmatrix} L_3 \leftarrow L_3/18$$

$$\begin{pmatrix} 1 & 2 & 0 & | & -3/18 & -3/18 & 15/18 \\ 0 & 1 & 0 & | & 1/18 & -5/18 & 7/18 \\ 0 & 0 & 1 & | & 7/18 & 1/18 & -5/18 \end{pmatrix} \begin{matrix} L_1 \leftarrow L_1 - 3L_3 \\ L_2 \leftarrow L_2 - 5L_3 \end{matrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & | & -5/18 & 7/18 & 1/18 \\ 0 & 1 & 0 & | & 1/18 & -5/18 & 7/18 \\ 0 & 0 & 1 & | & 7/18 & 1/18 & -5/18 \end{pmatrix} L_1 \leftarrow L_1 - 2L_2$$

On a donc :

$$A^{-1} = \begin{pmatrix} -5/18 & 7/18 & 1/18 \\ 1/18 & -5/18 & 7/18 \\ 7/18 & 1/18 & -5/18 \end{pmatrix}$$

2. Pour la deuxième matrice :

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

$$\begin{pmatrix} 2 & 3 & -2 & | & 0 & 1 & 0 \\ 0 & 1 & 0 & | & 1 & 0 & 0 \\ 4 & -1 & -2 & | & 0 & 0 & 1 \end{pmatrix} L_1 \leftrightarrow L_2$$

$$\begin{pmatrix} 1 & 3/2 & -1 & | & 0 & 1/2 & 0 \\ 0 & 1 & 0 & | & 1 & 0 & 0 \\ 4 & -1 & -2 & | & 0 & 0 & 1 \end{pmatrix} L_1 \leftarrow L_1/2$$

$$\begin{pmatrix} 1 & 3/2 & -1 & | & 0 & 1/2 & 0 \\ 0 & 1 & 0 & | & 1 & 0 & 0 \\ 0 & -7 & 2 & | & 0 & -2 & 1 \end{pmatrix} L_3 \leftarrow L_3 - 4L_1$$

$$\begin{pmatrix} 1 & 3/2 & -1 & | & 0 & 1/2 & 0 \\ 0 & 1 & 0 & | & 1 & 0 & 0 \\ 0 & 0 & 2 & | & 7 & -2 & 1 \end{pmatrix} L_3 \leftarrow L_3 + 7L_2$$

$$\begin{pmatrix} 1 & 3/2 & -1 & | & 0 & 1/2 & 0 \\ 0 & 1 & 0 & | & 1 & 0 & 0 \\ 0 & 0 & 1 & | & 7/2 & -1 & 1/2 \end{pmatrix} L_3 \leftarrow L_3/2$$

$$\begin{pmatrix} 1 & 3/2 & 0 & | & 7/2 & -1/2 & 1/2 \\ 0 & 1 & 0 & | & 1 & 0 & 0 \\ 0 & 0 & 1 & | & 7/2 & -1 & 1/2 \end{pmatrix} L_1 \leftarrow L_1 + L_3$$

$$\begin{pmatrix} 1 & 0 & 0 & | & 2 & -1/2 & 1/2 \\ 0 & 1 & 0 & | & 1 & 0 & 0 \\ 0 & 0 & 1 & | & 7/2 & -1 & 1/2 \end{pmatrix} L_1 \leftarrow L_1 - 3L_2/2$$

On a donc :

$$A^{-1} = \begin{pmatrix} 2 & -1/2 & 1/2 \\ 1 & 0 & 0 \\ 7/2 & -1 & 1/2 \end{pmatrix}$$

3. Pour la dernière :

$$\begin{pmatrix} 1 & 2 & -1 & | & 1 & 0 & 0 \\ 2 & -1 & -1 & | & 0 & 1 & 0 \\ -1 & 2 & 0 & | & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & -1 & | & 1 & 0 & 0 \\ 0 & -5 & 1 & | & -2 & 1 & 0 \\ 0 & 4 & -1 & | & 1 & 0 & 1 \end{pmatrix} \begin{array}{l} L_2 \leftarrow L_2 - 2L_1 \\ L_3 \leftarrow L_3 + L_1 \end{array}$$

$$\begin{pmatrix} 1 & 2 & -1 & | & 1 & 0 & 0 \\ 0 & 1 & -1/5 & | & 2/5 & -1/5 & 0 \\ 0 & 4 & -1 & | & 1 & 0 & 1 \end{pmatrix} L_2 \leftarrow -L_2/5$$

$$\begin{pmatrix} 1 & 2 & -1 & | & 1 & 0 & 0 \\ 0 & 1 & -1/5 & | & 2/5 & -1/5 & 0 \\ 0 & 0 & -1/5 & | & -3/5 & 4/5 & 1 \end{pmatrix} L_3 \leftarrow L_3 - 4L_2$$

$$\begin{pmatrix} 1 & 2 & -1 & | & 1 & 0 & 0 \\ 0 & 1 & -1/5 & | & 2/5 & -1/5 & 0 \\ 0 & 0 & 1 & | & 3 & -4 & -5 \end{pmatrix} L_3 \leftarrow -5L_3$$

$$\begin{pmatrix} 1 & 2 & 0 & | & 4 & -4 & -5 \\ 0 & 1 & 0 & | & 1 & -1 & -1 \\ 0 & 0 & 1 & | & 3 & -4 & -5 \end{pmatrix} \begin{array}{l} L_1 \leftarrow L_1 + L_3 \\ L_2 \leftarrow L_2 + L_3/5 \end{array}$$

$$\begin{pmatrix} 1 & 0 & 0 & | & 2 & -2 & -3 \\ 0 & 1 & 0 & | & 1 & -1 & -1 \\ 0 & 0 & 1 & | & 3 & -4 & -5 \end{pmatrix} L_1 \leftarrow L_1 - 2L_2$$

Finalement :

$$A^{-1} = \begin{pmatrix} 2 & -2 & -3 \\ 1 & -1 & -1 \\ 3 & -4 & -5 \end{pmatrix}$$

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

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

Correction : Montrons par récurrence que, pour tout $n \geq 1$, il existe α_n et β_n tels que $A^n = \alpha_n A + \beta_n A^2$ (l'existence de tels réels pour tout n implique l'existence des deux suites). On donnera ensuite la valeur de α_n et β_n pour tout n . Commençons déjà par donner A^2 :

$$A^2 = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

- Si $n \geq 1$, on note H_n : « il existe $(\alpha_n, \beta_n) \in \mathbb{R}^2$ tels que $A^n = \alpha_n A + \beta_n A^2$ ».
- Si on pose $\alpha_1 = 1$ et $\beta_1 = 0$, alors on a bien $A^1 = \alpha_1 A + \beta_1 A^2$. H_1 est vraie.
- Soit $n \in \mathbb{N}$. Supposons H_n vraie et montrons que H_{n+1} est vraie. Par hypothèse de récurrence, il existe $(\alpha_n, \beta_n) \in \mathbb{R}^2$ tels que $A^n = \alpha_n A + \beta_n A^2$. En multipliant par A (à gauche ou à droite, cela n'a aucune importance car des puissances d'une même matrice commutent), il vient $A^{n+1} = \alpha_n A^2 + \beta_n A^3$. Or,

$$A^3 = \begin{pmatrix} 5 & 3 & 3 \\ 3 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix} = A^2 + 2A$$

Par conséquent, $A^{n+1} = (2\beta_n)A + (\alpha_n + \beta_n)A^2$. Si on pose $\alpha_{n+1} = 2\beta_n$ et $\beta_{n+1} = \alpha_n + \beta_n$, alors on a bien $A^{n+1} = \alpha_{n+1}A + \beta_{n+1}A^2$: H_{n+1} est vraie.

- D'après le principe de récurrence, H_n est vraie pour tout $n \geq 1$.

Donnons à présent les valeurs de α_n et de β_n pour tout n . Pour cela, prouvons que (α_n) est une suite récurrente linéaire d'ordre 2. Soit $n \geq 1$. D'après ce qui précède, $\alpha_{n+2} = 2\beta_{n+1} = 2(\alpha_n + \beta_n)$. Or, $\beta_n = \alpha_{n+1}/2$ si bien que $\alpha_{n+2} = 2\alpha_n + \alpha_{n+1}$:

(α_n) est une suite récurrente linéaire d'ordre 2, d'équation caractéristique $r^2 = r + 2 \iff r^2 - r - 2 = 0$. Cette équation admet deux racines simples, $r_1 = -1$ et $r_2 = 2$ donc il existe $(\lambda_1, \lambda_2) \in \mathbb{R}^2$ tels que, pour tout $n \geq 1$,

$$\alpha_n = \lambda_1 \times (-1)^n + \lambda_2 \times 2^n$$

En prenant $n = 1$ et $n = 2$ (attention, ici, les suites sont définies à partir du rang 1), il vient $1 = -\lambda_1 + 2\lambda_2$ (car $\alpha_1 = 1$) et $0 = \lambda_1 + 4\lambda_2$ (car $\alpha_2 = 0$), donc $\lambda_2 = 1/6$ et $\lambda_1 = -2/3$. Finalement, pour tout $n \geq 1$,

$$\alpha_n = -\frac{2}{3} \times (-1)^n + \frac{1}{6} \times 2^n \quad \text{et} \quad \beta_n = \frac{\alpha_{n+1}}{2} = -\frac{1}{3} \times (-1)^{n+1} + \frac{1}{6} \times 2^n$$

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} .

Correction :

1. Calcul immédiat. C'est le cas particulier pour $n = 2$ du théorème de Cayley-Hamilton, au programme de deuxième année.
2. Montrons que A est inversible si et seulement si $ad - bc \neq 0$ (c'est-à-dire si son déterminant est non nul : cf. second semestre). Supposons $ad - bc \neq 0$. Alors, de même que dans l'exercice 6 :

$$A \times \left[\frac{-1}{ad - bc} (A - (a + d)I_2) \right] = I_2$$

si bien que A est inversible et

$$A^{-1} = \frac{-1}{ad - bc} (A - (a + d)I_2) = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

Supposons à présent que $ad - bc = 0$. Il en découle que $A^2 - (a + d)A = 0$ donc $A^2 = (a + d)A$. Si A est inversible, alors on peut multiplier cette égalité par A^{-1} ce qui donne : $A = (a + d)I_2$ c'est-à-dire

$$A = \begin{pmatrix} a + d & 0 \\ 0 & a + d \end{pmatrix}$$

Dès lors, $b = c = 0$ et $a = d = 0$ donc A est la matrice nulle, ce qui est absurde puisque la matrice nulle n'est pas inversible.

3. Fait dans la question précédente.

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

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

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

Correction : Calculons le produit du terme d'indice i, j du produit. Si on fait le produit « avec les mains », on a des produits 1×1 : combien y en a-t-il ? En fait, cela dépend de si $i = j$ ou non : si $i = j$, alors le 0 de la matrice de gauche rencontre le 0 de la matrice de droite : il n'y a qu'un seul terme nul, donc $n - 1$ termes égaux à 1, et donc le coefficient vaut $n - 1$. Si $i \neq j$, alors les deux 0 ne se rencontrent pas, il y a deux termes nuls, donc $n - 2$ termes égaux à 0 donc le coefficient vaut $n - 2$. Finalement :

$$\begin{aligned} J^2 &= \begin{pmatrix} n-1 & n-2 & n-2 & \dots & n-2 \\ n-2 & n-1 & n-2 & \dots & n-2 \\ \vdots & & \ddots & & \vdots \\ n-2 & n-2 & \dots & n-1 & n-2 \\ n-2 & n-2 & \dots & n-2 & n-1 \end{pmatrix} \\ &= (n-2)J + (n-1)I_n \end{aligned}$$

On obtient l'inversibilité de J ainsi que son inverse de même que dans l'exercice 6 : on trouve

$$J^{-1} = \frac{1}{n-1} (J - (n-2)I_n)$$

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

Correction : On pourrait aussi le faire avec les mains, mais nous allons le calculer à l'aide de la formule du produit matriciel. Soit $(i, j) \in \llbracket 1; 2n+1 \rrbracket$. On sait que $A_{i,j} = 1$ si i ou j vaut n et 0 sinon. Par conséquent, si $i \neq n$, alors $A_{i,k} = 0$ sauf si $k = n$ ce qui donne :

$$\begin{aligned} (A^2)_{i,j} &= \sum_{k=1}^{2n+1} A_{i,k} A_{k,j} \\ &= A_{i,n} A_{n,j} \\ &= 1 \times 1 \\ &= 1 \end{aligned}$$

On trouve de même que $(A^2)_{i,j} = 1$ si $j \neq n$. Supposons à présent $i = j = n$. Alors tous les termes de la somme valent 1 donc $(A^2)_{i,j} = 2n+1$: A^2 est la matrice carrée de taille $2n+1$ dont tous les coefficients valent 1 sauf celui en position (n, n) qui vaut $2n+1$.

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 $B \in \mathcal{M}_3(\mathbb{C})$ 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.

Correction :

1. $AB = B^2B = B^3 = BB^2 = BA$. Écrivons B sous la forme

$$B = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix}$$

Alors on a

$$AB = \begin{pmatrix} d+g & e+h & f+k \\ g & h & k \\ 0 & 0 & 0 \end{pmatrix} \quad \text{et} \quad BA = \begin{pmatrix} 0 & a & a+b \\ 0 & d & d+e \\ 0 & g & g+h \end{pmatrix}$$

Or, $AB = BA$ donc $g = 0$ (coefficient 2-1), donc $d+g = d = 0$ (coefficient 1-1) et enfin $h = d = 0$ (coefficient 2-2). Il en découle que B est bien triangulaire supérieure.

2. D'après la question précédente,

$$B = \begin{pmatrix} a & b & c \\ 0 & e & f \\ 0 & 0 & k \end{pmatrix}$$

donc

$$B^2 = \begin{pmatrix} a^2 & ab+e^2 & ac+bf+kc \\ 0 & e^2 & ef+fk \\ 0 & 0 & k^2 \end{pmatrix}$$

Or, rappelons qu'on a supposé que $B^2 = A$. Par conséquent, les coefficients diagonaux de B^2 et de A sont égaux donc $a = e = k = 0$, si bien que

$$B^2 = \begin{pmatrix} 0 & 0 & bf \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ce qui est absurde car $B^2 = A$. Ainsi, une telle matrice B n'existe pas.

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

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

Correction :

1. $A(B - I_n) = I_n$ donc A est inversible et $A^{-1} = B - I_n$.
2. D'après la question précédente, A^{-1} commute avec B , c'est-à-dire que $A^{-1}B = BA^{-1}$. Le résultat en découle en multipliant par A à gauche et à droite.

Exercice 15 : $\star\star$

1. Soit $A \in \mathcal{M}_{n,p}(\mathbb{R})$ 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 $A \in \mathcal{M}_{n,p}(\mathbb{C})$? Recommencer l'exercice en supposant cette fois que $A \times (\overline{A})^\top = 0$.

Correction :

1. Commençons par dire que le 0 dans la première égalité est 0_n , tandis que le 0 dans la seconde est $0_{n,p}$ (il suffit d'étudier les tailles des matrices). Soit $i \in \llbracket 1; n \rrbracket$. Le terme d'indice (i, i) (l'énoncé nous dit de nous intéresser aux coefficients diagonaux) est

$$\sum_{k=1}^p A_{i,k} (A^\top)_{k,i} = \sum_{k=1}^p A_{i,k} A_{i,k} = \sum_{k=1}^p A_{i,k}^2.$$

Or, ce coefficient est nul puisque $A \times A^\top = 0_n$. Une somme de termes positifs est nulle si et seulement si tous les termes sont nuls, il en découle que $A_{i,k} = 0$ pour tout $k \in \llbracket 1; n \rrbracket$. L'entier i étant quelconque, $A_{i,k} = 0$ pour tous i et k , c'est-à-dire que tous les coefficients de A sont nuls : A est bien la matrice nulle.

2. Non, ce résultat n'est plus valable sur \mathbb{C} . Par exemple, si $A = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$, alors $A \times A^\top = 0$ mais A n'est pas la matrice nulle. Si on conjugue en plus la transposée, le résultat est encore valable et la preuve est analogue, il suffit de remplacer (dans les coefficients diagonaux du produit) $A_{i,k}^2$ par $|A_{i,k}|^2$.

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

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

Correction :

1. Rappelons que $\overline{\omega} = \omega^{-1}$. Soient k et ℓ dans $\llbracket 1; n \rrbracket$.

$$\begin{aligned} (\Omega \times \overline{\Omega})_{k,\ell} &= \sum_{p=1}^n \Omega_{k,p} \overline{\Omega_{p,\ell}} \\ &= \sum_{p=1}^n \omega^{(k-1)(p-1)} \times \omega^{-(p-1)(\ell-1)} \end{aligned}$$

Si $k = \ell$:

$$\begin{aligned}
(\Omega \times \overline{\Omega})_{k,k} &= \sum_{p=1}^n \omega^{(k-1)(p-1)-(p-1)(k-1)} \\
&= \sum_{k=1}^n \omega^0 \\
&= \sum_{k=1}^n 1 \\
&= n
\end{aligned}$$

Supposons à présent $k \neq \ell$. On a alors :

$$\begin{aligned}
(\Omega \times \overline{\Omega})_{k,\ell} &= \sum_{p=1}^n \omega^{(p-1) \times (k-1-\ell+1)} \\
&= \sum_{p=1}^n \omega^{(p-1) \times (k-\ell)} \\
&= \sum_{p=1}^n \left(\omega^{(k-\ell)} \right)^{p-1} \\
&= \sum_{p=0}^{n-1} \left(\underbrace{\omega^{(k-\ell)}}_{\neq 1} \right)^p \\
&= \frac{1 - \omega^{n(k-\ell)}}{1 - \omega^{k-\ell}} \\
&= 0
\end{aligned}$$

puisque $\omega^n = 1$ donc $-\omega^{n(k-\ell)} = 1^{k-\ell} = 1$. Finalement, les coefficients non diagonaux sont nuls et les coefficients diagonaux égaux à n : $\Omega \times \overline{\Omega} = nI_n$.

2. Ω est donc inversible et $\Omega^{-1} = \frac{1}{n} \cdot \overline{\Omega}$.

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

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

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

- Calculer A^2 .
- 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 $n \in \mathbb{N}^*$.

Correction :

1. Soit $n \geq 2$. On va appliquer le binôme de Newton : remarquons que $A = \pi I_3 + B$ où

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

Les matrices πI_3 et B commutent (les homothéties commutent avec tout le monde) donc, d'après la formule du binôme de Newton :

$$\begin{aligned} A^n &= \sum_{k=0}^n \binom{n}{k} B^k (\pi I_3)^{n-k} \\ &= \sum_{k=0}^n \pi^{n-k} \binom{n}{k} B^k \end{aligned}$$

Or :

$$B^2 = \begin{pmatrix} 0 & 0 & ac \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

et $B^3 = 0$, ce qui implique que $B^k = B^{k-3}B^3 = 0$ pour tout $k \geq 3$. Par conséquent, la somme ci-dessus ne va que jusque 2, les termes suivants sont nuls (ce qui ne veut pas dire que $n = 2!$). Par conséquent :

$$\begin{aligned} A^n &= \pi^n \binom{n}{0} B^0 + \pi^{n-1} \binom{n}{1} B + \pi^{n-2} \binom{n}{2} B^2 \\ &= \pi^n I_3 + n\pi^{n-1} B + \pi^{n-2} \times \frac{n(n-1)}{2} B^2 \\ &= \begin{pmatrix} \pi^n & n\pi^{n-1}a & n\pi^{n-1}b + \pi^{n-2} \times \frac{n(n-1)}{2} \times ac \\ 0 & \pi^n & n\pi^{n-1}c \\ 0 & 0 & \pi^n \end{pmatrix} \end{aligned}$$

2. On trouve :

$$A^2 = \begin{pmatrix} 1 & -2 & -6 \\ -3 & 2 & 9 \\ 2 & 0 & -3 \end{pmatrix} \begin{pmatrix} 1 & -2 & -6 \\ -3 & 2 & 9 \\ 2 & 0 & -3 \end{pmatrix} = \begin{pmatrix} -5 & -6 & -6 \\ 9 & 10 & 9 \\ -4 & -4 & -3 \end{pmatrix} \quad \text{et} \quad A^3 = A$$

Par conséquent, $A^4 = A \times A^3 = A^2$, $A^5 = A \times A^4 = A \times A^2 = A^3 = A$ et, par une récurrence immédiate, $A^{2p} = A^2$ et $A^{2p+1} = A$ pour tout $p \in \mathbb{N}^*$, c'est-à-dire que toutes les puissances paires (à partir de A^2 , puisque $A^0 = I_3$) sont égales à A^2 et toutes les puissances impaires sont égales à A . A n'est pas inversible : en effet, si A est inversible, alors $A^2 = I_2$ car $A^3 = A$ (on multiplie, à gauche ou à droite, par A^{-1}), ce qui est absurde.

3. (a) Tout d'abord, on trouve comme d'habitude que

$$P^{-1} = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$$

ce qui donne :

$$\begin{aligned} P^{-1}AP &= \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ -6 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 3 & -1 \\ -4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \end{aligned}$$

Notons D cette matrice (diagonale : penser à Médor). Tout d'abord, $A = PDP^{-1}$ donc :

$$\begin{aligned} A^2 &= PDP^{-1} \times PDP^{-1} \\ &= PDI_2DP^{-1} \\ &= PD^2P^{-1} \end{aligned}$$

De plus :

$$\begin{aligned} A^3 &= A^2 \times A \\ &= PD^2P^{-1} \times PDP^{-1} \\ &= PD^2I_2DP^{-1} \\ &= PD^3P^{-1} \end{aligned}$$

Par une récurrence immédiate (faites-la!), $A^n = PD^nP^{-1}$ pour tout $n \in \mathbb{N}$. L'avantage de cette écriture est que D^n est très facile à calculer puisque D est diagonale. Soit $n \in \mathbb{N}$.

$$D^n = \begin{pmatrix} 1 & 0 \\ 0 & 2^n \end{pmatrix}$$

Par conséquent :

$$\begin{aligned} A^n &= PD^nP^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2^n \end{pmatrix} \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2^n \\ 2 & 3 \times 2^n \end{pmatrix} \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 3 \times 2^n - 2^{n+1} & 2^n - 1 \\ 6 - 6 \times 2^n & 3 \times 2^n - 2 \end{pmatrix} \end{aligned}$$

(b) Notons, pour tout n , $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$. Par conséquent, la relation de récurrence de l'énoncé devient :

$$\forall n \in \mathbb{N}, X_{n+1} = AX_n$$

où A est la matrice de la question précédente. Cela ressemble à une suite géométrique de raison A , mais on garde cette terminologie pour les réels ou les complexes. Néanmoins, le résultat est le même :

$$\forall n \in \mathbb{N}, X_n = A^n X_0$$

Finalement, d'après la question précédente, pour tout $n \in \mathbb{N}$:

$$\begin{aligned} \begin{pmatrix} u_n \\ v_n \end{pmatrix} &= \begin{pmatrix} 3 \times 2^n - 2^{n+1} & 2^n - 1 \\ 6 - 6 \times 2^n & 3 \times 2^n - 2 \end{pmatrix} \times \begin{pmatrix} 1 \\ 3 \end{pmatrix} \\ &= \begin{pmatrix} 3 \times 2^n - 2^{n+1} + 3 \times 2^n - 3 \\ 6 - 6 \times 2^n + 9 \times 2^n - 6 \end{pmatrix} \end{aligned}$$

4. (a) On a :

$$\begin{aligned} A^2 &= \begin{pmatrix} 0 & a & a^2 \\ 1/a & 0 & a \\ 1/a^2 & 1/a & 0 \end{pmatrix} \begin{pmatrix} 0 & a & a^2 \\ 1/a & 0 & a \\ 1/a^2 & 1/a & 0 \end{pmatrix} \\ &= \begin{pmatrix} 2 & a & a^2 \\ 1/a & 2 & a \\ 1/a^2 & 1/a & 2 \end{pmatrix} \\ &= A + 2I_3 \end{aligned}$$

(b) Soit $X = (x, y, z) \in \mathbb{R}^3$. Résolvons ce système.

$$\begin{aligned}
 AX = -X &\iff \begin{cases} ay + a^2z = -x \\ \frac{x}{a} + az = -y \\ \frac{x}{a^2} + \frac{y}{a} = -z \end{cases} \\
 &\iff \begin{cases} x + ay + a^2z = 0 \\ \frac{x}{a} + y + az = 0 \\ \frac{x}{a^2} + \frac{y}{a} + z = 0 \end{cases} \\
 &\iff \begin{cases} x + ay + a^2z = 0 \\ x + ay + a^2z = 0 \\ x + ay + a^2z = 0 \end{cases} \\
 &\iff x = -ay - a^2z
 \end{aligned}$$

Finalement, $X = (-a, 1, 0)$ et $Y = (-a^2, 0, 1)$ conviennent.

(c) Soit $X = (x, y, z) \in \mathbb{R}^3$. Résolvons ce système.

$$\begin{aligned}
 AX = 2X &\iff \begin{cases} ay + a^2z = 2x \\ \frac{x}{a} + az = 2y \\ \frac{x}{a^2} + \frac{y}{a} = 2z \end{cases} \\
 &\iff \begin{cases} -2x + ay + a^2z = 0 \\ \frac{x}{a} - 2y + az = 0 \\ \frac{x}{a^2} + \frac{y}{a} - 2z = 0 \end{cases} \\
 &\iff \begin{cases} -2x + ay + a^2z = 0 \\ x - 2ay + a^2z = 0 \\ x + ay - 2a^2z = 0 \end{cases} \\
 &\iff \begin{cases} x - 2ay + a^2z = 0 \\ -2x + ay + a^2z = 0 \\ x + ay - 2a^2z = 0 \end{cases}
 \end{aligned}$$

Appliquons ensuite la méthode du pivot de Gauß :

$$\begin{aligned}
AX = 2X &\iff \begin{cases} x - 2ay + a^2z = 0 \\ -3ay + 3a^2z = 0 \\ 3ay - 3a^2z = 0 \end{cases} \\
&\iff \begin{cases} x - 2ay + a^2z = 0 \\ ay = a^2z \\ ay = a^2z \end{cases} \\
&\iff \begin{cases} x = 2ay - a^2z \\ y = az \end{cases} \\
&\iff \begin{cases} x = a^2z \\ y = az \end{cases}
\end{aligned}$$

Par conséquent, $Z = (a^2, a, 1)$ convient.

(d) Par conséquent :

$$P = \begin{pmatrix} -a & -a^2 & a^2 \\ 1 & 0 & a \\ 0 & 1 & 1 \end{pmatrix}$$

Encore une fois, appliquons la méthode du pivot de Gauß :

$$\begin{aligned}
&\left(\begin{array}{ccc|ccc} -a & -a^2 & a^2 & 1 & 0 & 0 \\ 1 & 0 & a & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array} \right) \\
&\left(\begin{array}{ccc|ccc} 1 & 0 & a & 0 & 1 & 0 \\ -a & -a^2 & a^2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array} \right) L_1 \leftrightarrow L_2 \\
&\left(\begin{array}{ccc|ccc} 1 & 0 & a & 0 & 1 & 0 \\ 0 & -a^2 & 2a^2 & 1 & a & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array} \right) L_2 \leftarrow L_2 + aL_1 \\
&\left(\begin{array}{ccc|ccc} 1 & 0 & a & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & -a^2 & 2a^2 & 1 & a & 0 \end{array} \right) L_2 \leftrightarrow L_3 \\
&\left(\begin{array}{ccc|ccc} 1 & 0 & a & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 3a^2 & 1 & a & a^2 \end{array} \right) L_3 \leftarrow L_3 + a^2L_2 \\
&\left(\begin{array}{ccc|ccc} 1 & 0 & a & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1/3a^2 & 1/3a & 1/3 \end{array} \right) L_3 \leftarrow L_3/3a^2 \\
&\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1/3a & 2/3 & -a/3 \\ 0 & 1 & 0 & -1/3a^2 & -1/3a & 2/3 \\ 0 & 0 & 1 & 1/3a^2 & 1/3a & 1/3 \end{array} \right) L_1 \leftarrow L_1 - aL_3 \\
&\hspace{1.5cm} L_2 \leftarrow L_2 - L_3
\end{aligned}$$

(e) Par conséquent :

$$\begin{aligned}
D &= \begin{pmatrix} -1/3a & 2/3 & -a/3 \\ -1/3a^2 & -1/3a & 2/3 \\ 1/3a^2 & 1/3a & 1/3 \end{pmatrix} \begin{pmatrix} 0 & a & a^2 \\ 1/a & 0 & a \\ 1/a^2 & 1/a & 0 \end{pmatrix} \begin{pmatrix} -a & -a^2 & a^2 \\ 1 & 0 & a \\ 0 & 1 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1/3a & -2/3 & a/3 \\ 1/3a^2 & 1/3a & -2/3 \\ 2/3a^2 & 2/3a & 2/3 \end{pmatrix} \begin{pmatrix} -a & -a^2 & a^2 \\ 1 & 0 & a \\ 0 & 1 & 1 \end{pmatrix} \\
&= \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}
\end{aligned}$$

D est inversible car diagonale de coefficients tous non nuls, et $A = PDP^{-1}$ est inversible car produit de matrices inversibles. De même que précédemment, pour tout n , $A^n = PD^nP^{-1}$ et D est diagonale donc on trouve finalement :

$$\begin{aligned}
A^n &= \begin{pmatrix} -a & -a^2 & a^2 \\ 1 & 0 & a \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} (-1)^n & 0 & 0 \\ 0 & (-1)^n & 0 \\ 0 & 0 & 2^n \end{pmatrix} \begin{pmatrix} -1/3a & 2/3 & -a/3 \\ -1/3a^2 & -1/3a & 2/3 \\ 1/3a^2 & 1/3a & 1/3 \end{pmatrix} \\
&= \begin{pmatrix} a \times (-1)^{n+1} & a^2 \times (-1)^{n+1} & a^2 \times 2^n \\ (-1)^n & 0 & a \times 2^n \\ 0 & (-1)^n & 2^n \end{pmatrix} \begin{pmatrix} -1/3a & 2/3 & -a/3 \\ -1/3a^2 & -1/3a & 2/3 \\ 1/3a^2 & 1/3a & 1/3 \end{pmatrix} \\
&= \begin{pmatrix} 2(-1)^n/3 + 2^n/3 & a(-1)^{n+1}/3 + a2^n/3 & a^22^n/3 \\ (-1)^{n+1}/3a + a2^{n+1}/3 & (-1)^n2/3 + a2^n/3 & a(-1)^{n+1}/3 + a2^n/3 \\ (-1)^{n+1}/3a^2 + 2^n/3a^2 & (-1)^{n+1}/3a + 2^n/3a & (-1)^n2/3 + 2^n/3 \end{pmatrix}
\end{aligned}$$

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

Correction : Afin d'éviter toute confusion, nous noterons L_i et L_j les lignes i et j originelles, et quand nous parlerons d'opérations élémentaires, nous parlerons de la ligne i et de la ligne j pour les lignes modifiées.

- Ajoutons la ligne i à la ligne j : la ligne j contient alors $L_i + L_j$, et la ligne i contient encore L_i .
- Soustrayons la ligne j à la ligne i : la ligne i contient alors $-L_j$, et la ligne j contient encore $L_i + L_j$.
- Multiplions la ligne i par -1 : la ligne i contient alors L_j , et la ligne j contient encore $L_i + L_j$.
- Soustrayons la ligne i à la ligne j : la ligne i contient encore L_j et la ligne j contient L_i .

On a échangé L_i et L_j sans matrices de permutation, juste à l'aide de matrices de transvections et de dilatations. On pourrait donc se contenter de ce type de matrices pour engendrer $\text{GL}_n(\mathbb{K})$.

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

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} ?

Correction :

1. Notons P la matrice inversible correspondant à la permutation des colonnes i et j . Par conséquent, $B = AP$ (effectuer une opération élémentaire sur les colonnes revient à multiplier à droite par la matrice élémentaire correspondante). Or, A est inversible par hypothèse et P est inversible d'après le cours donc B est inversible car produit de matrices inversibles. De plus, $B = P^{-1}A^{-1}$ mais $P^{-1} = P$ d'après le cours donc $B = P \times A^{-1}$. En conclusion, B^{-1} est la matrice obtenue en permutant les **lignes** (car on multiplie à gauche) i et j de A^{-1} .
2. De même que ci-dessus, si on note T la matrice de transvection associée (ajouter 2 fois la colonne i à la colonne j), alors $C = AT$ donc C est inversible et $C^{-1} = T^{-1} \times A^{-1}$. Or :

$$T = I_n + 2E_{i,j} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 2 & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ \\ j \end{matrix}$$

donc, en faisant l'opération élémentaire $L_i \leftarrow L_i - 2L_j$ sur T et sur I_n :

$$T^{-1} = I_n - 2E_{i,j} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & -2 & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ \\ j \end{matrix}$$

et (cf. cours) multiplier par T^{-1} à gauche revient à ajouter $-2L_j$ à L_i (attention, l'effet change selon qu'on est à droite ou à gauche, cf. cours). Finalement, C^{-1} est obtenue à partir de A^{-1} en retirant deux fois L_j à L_i .

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 $\mathcal{M}_n(\mathbb{R})$.
2. Montrer que C est un corps.
3. Montrer que l'application

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

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 $J^2 = -I_2$.

Correction :

1. • La matrice nulle appartient à C avec $a = b = 0$ donc C est non vide.
• C est évidemment stable par somme et par opposé : c'est un sous-groupe de $\mathcal{M}_n(\mathbb{R})$.
• $I_2 \in C$, avec $a = 1$ et $b = 0$.
• Montrons que C est stable par produit. Soient M_1 et M_2 appartenant à C . Il existe $a_1, a_2, b_1, b_2 \in \mathbb{R}$ tels que

$$A_1 = \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \quad \text{et} \quad A_2 = \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix}$$

Dès lors :

$$A_1 A_2 = \begin{pmatrix} a_1 a_2 - b_1 b_2 & -(a_1 b_2 + b_1 a_2) \\ b_1 a_2 + a_1 b_2 & -b_1 b_2 + a_1 a_2 \end{pmatrix} \in C$$

C est stable par produit : c'est un sous-anneau de $\mathcal{M}_n(\mathbb{R})$, et il est commutatif puisque, dans le produit ci-dessus, les indices 1 et 2 jouent le même rôle.

2. Il ne manque que l'inversibilité de tout élément non nul. Soit donc $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in C$ non nul i.e. a et b sont non tous nuls. On pourrait utiliser l'exercice 10, mais on va le redémontrer à la main. Si $a = 0$ alors $b \neq 0$ donc

$$M = \begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix}$$

La méthode du pivot de Gauß prouve que M est inversible et que

$$M^{-1} = \begin{pmatrix} 0 & 1/b \\ -1/b & 0 \end{pmatrix}$$

Si $b = 0$ alors $a \neq 0$ si bien que $M = aI_2$ donc M est inversible d'inverse $(1/a)I_2$. Supposons enfin a et b non nuls. Avec la méthode du pivot de Gauß, on trouve que M est inversible d'inverse

$$M^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Tout élément de C non nul est inversible : c'est un corps.

3. On montre aisément que, pour tous $z_1 = a_1 + ib_1$ et $z_2 = a_2 + ib_2 \in \mathbb{C}$, $\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2)$, $\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$ et enfin que $\varphi(1) = I_2$: φ est bien un morphisme de corps. De plus, si $z = a + ib \in \ker(\varphi)$, alors $a = b = 0$ donc $z = 0$: φ est injectif, et il est surjectif par définition de C , c'est bien un isomorphisme de corps. Enfin, si on pose

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in C$$

alors on a bien $J^2 = -I_2$.

Exercice 21 - Le corps des quaternions : $\clubsuit\spadesuit$ Le corps des quaternions, construit par Hamilton en 1843, est un surcorps de \mathbb{C} non commutatif¹. 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 $\mathcal{M}_2(\mathbb{C})$ constitué des matrices h de la forme $\begin{pmatrix} z_1 & -\bar{z}_2 \\ z_2 & \bar{z}_1 \end{pmatrix}$ avec $z_1, z_2 \in \mathbb{C}$: on dit que \mathbb{H} est l'ensemble des quaternions. On considère les quatre éléments suivants de \mathbb{H} :

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

1. Montrer que \mathbb{H} est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$ 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 $\bar{h} = \begin{pmatrix} \bar{z}_1 & \bar{z}_2 \\ -z_2 & z_1 \end{pmatrix}$. Montrer que l'application qui à h associe \bar{h} est un isomorphisme d'anneaux involutif de \mathbb{H} .
5. Calculer $h\bar{h}$ 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 second semestre. Frobenius a prouvé en 1877 qu'il n'existe pas de surcorps de \mathbb{R} de dimension 3.

Correction :

1. La matrice nulle est évidemment un élément de \mathbb{H} donc cet ensemble n'est pas vide. Soient h_1 et h_2 deux éléments de \mathbb{H} . Par définition, il existe $(z_1, z_2, z_3, z_4) \in \mathbb{C}^4$ tels que

$$h_1 = \begin{pmatrix} z_1 & -\bar{z}_2 \\ z_2 & \bar{z}_1 \end{pmatrix} \quad \text{et} \quad h_2 = \begin{pmatrix} z_3 & -\bar{z}_4 \\ z_4 & \bar{z}_3 \end{pmatrix}$$

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...

Par conséquent :

$$h_1 + h_2 = \begin{pmatrix} z_1 + z_3 & -\overline{(z_2 + z_4)} \\ z_2 + z_4 & \overline{z_1 + z_3} \end{pmatrix} \in \mathbb{H}$$

En d'autres termes, \mathbb{H} est stable par somme. De plus,

$$-h_1 = \begin{pmatrix} -z_1 & \overline{z_2} \\ -z_2 & -\overline{z_1} \end{pmatrix} \in \mathbb{H}$$

donc \mathbb{H} est un sous-groupe de $\mathcal{M}_n(\mathbb{C})$. De plus,

$$I_2 = \begin{pmatrix} 1 & -\overline{0} \\ 0 & \overline{1} \end{pmatrix} \in \mathbb{H}$$

Montrons enfin que \mathbb{H} est stable par produit. Avec les mêmes notations :

$$h_1 h_2 = \begin{pmatrix} z_1 z_3 - \overline{z_2} z_4 & -z_1 \overline{z_4} - \overline{z_3} z_2 \\ z_2 z_3 + \overline{z_1} z_4 & -z_2 \overline{z_4} + \overline{z_1} z_3 \end{pmatrix} \in \mathbb{H}$$

Finalement, \mathbb{H} est bien un sous-anneau de $\mathcal{M}_n(\mathbb{C})$. Soit $\lambda \in \mathbb{R}$, si bien que $\overline{\lambda} = \lambda$. Par conséquent,

$$\lambda h_1 = \begin{pmatrix} \lambda z_1 & -\overline{\lambda z_2} \\ \lambda z_2 & \overline{\lambda z_1} \end{pmatrix} \in \mathbb{H}$$

Montrons que \mathbb{H} n'est pas stable par multiplication par un complexe. En effet,

$$i e_0 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \notin \mathbb{H}$$

2. Soit $h \in \mathbb{H}$. Par définition de \mathbb{H} , il existe quatre réels (a, b, c, d) tels que :

$$h = \begin{pmatrix} a + ib & -c + id \\ c + id & a - ib \end{pmatrix} = a e_0 + b e_1 + c e_3 + d e_2$$

où l'on a bien sûr pris $z_1 = a + ib$ et $z_2 = c + id$.

3. Je vous passe les calculs... mais je vous donne deux astuces pour gagner du temps. On peut remarquer que $e_0 = I_2$ donc on peut déjà dire que $e_0 e_i = e_i e_0 = e_i$ pour tout i . De plus, e_1 est diagonale donc e_1^2 est facile à calculer (et hop, déjà 8 cases de remplies!). Dans le tableau suivant, le résultat au croisement de la ligne e_i et de la colonne e_j est le produit $e_i e_j$, et pas $e_j e_i$.

	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	$-e_0$	e_3	$-e_2$
e_2	e_2	$-e_3$	$-e_0$	e_1
e_3	e_3	e_2	$-e_1$	$-e_0$

On remarque (entre autres) que $e_1 e_2 = -e_2 e_1$ ce qui implique que la multiplication n'est pas commutative sur \mathbb{H} .

4. Notons $\varphi : h \rightarrow \overline{h}$. Pour montrer que φ est à valeurs dans \mathbb{H} , il suffit de voir que pour tout $h \in \mathbb{H}$,

$$\varphi(h) = \begin{pmatrix} z_3 & -\overline{z_4} \\ z_4 & \overline{z_3} \end{pmatrix} \in \mathbb{H}$$

où l'on a posé $z_3 = \overline{z_1}$ et $z_4 = -z_2$. Le fait que $\varphi(\varphi(h)) = h$ est trivial. φ est donc une involution de \mathbb{H} dans lui-même. Le fait que c'est un morphisme d'anneaux est immédiat et laissé à votre charge ($\varphi(h_1 + h_2) = \varphi(h_1) + \varphi(h_2)$, $\varphi(I_2) = I_2$ et $\varphi(h_1 h_2) = \varphi(h_1) \varphi(h_2)$).

5. On rappelle que $z \overline{z} = |z|^2$. Un calcul simple donne : $h \varphi(h) = (|z_1|^2 + |z_2|^2) I_2$.

Il en découle que si h est non nul, alors en particulier z_1 ou z_2 est non nul, donc $(|z_1|^2 + |z_2|^2) \neq 0$, et on peut diviser par ce terme pour obtenir :

$$h \times \left(\frac{1}{(|z_1|^2 + |z_2|^2)} \varphi(h) \right) = I_2$$

C'est-à-dire que tout élément h non nul est inversible d'inverse $\frac{1}{(|z_1|^2 + |z_2|^2)} \varphi(h)$: on en déduit que \mathbb{H} est un corps (non commutatif).

6. L'application

$$z \mapsto \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$$

est clairement un morphisme de corps injectif de \mathbb{C} dans \mathbb{H} donc son image est un corps isomorphe à \mathbb{C} (rappelons qu'une fonction est surjective sur son image, donc une injection est une bijection sur son image).

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 :

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

Correction : Ce système est équivalent au système suivant :

$$\begin{cases} (\cos(1) - 1) \times L_1 + \sin(1) \times L_2 = 0 \\ -\sin(1) \times L_1 + (\cos(1) - 1) \times L_2 = 0 \end{cases}$$

La matrice associée à ce système est $A = \begin{pmatrix} \cos(1) - 1 & \sin(1) \\ -\sin(1) & \cos(1) - 1 \end{pmatrix}$. Or

$$(\cos(1) - 1)^2 + \sin^2(1) = \cos^2(1) - 2\cos(1) + 1 + \sin^2(1) = 1 - 2\cos(1) + 1 = 2(1 - \cos(1))$$

et $1 \in]0; 2\pi[$ donc $\cos(1) \neq 1$. Le déterminant de A est non nul (cf. exercice 10) donc A est inversible : ce système est donc un système de Cramer, il admet donc une unique solution. La solution nulle (c'est-à-dire $L_1 = L_2 = 0$) est solution évidente, c'est donc la seule.

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

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

Correction :

1.
 - $0_n = 0.J_n + 0.I_n \in \mathcal{A}$: \mathcal{A} est non vide.
 - Soient M_1 et $M_2 \in \mathcal{A}$. Alors il existe $(a_1, b_1, a_2, b_2) \in \mathbb{C}^4$ tel que $M_1 = a_1J_n + b_1I_n$ et $M_2 = a_2J_n + b_2I_n$. Dès lors, $M_1 + M_2 = (a_1 + a_2)J_n + (b_1 + b_2)I_n \in \mathcal{A}$ et $-M_1 = (-a_1)J_n + (-b_1)I_n \in \mathcal{A}$: \mathcal{A} est stable par somme et par opposé, c'est un sous-groupe de $\mathcal{M}_n(\mathbb{C})$.
 - $I_n = 0.J_n + 1.I_n \in \mathcal{A}$.
 - Enfin, avec les notations ci-dessus :

$$M_1M_2 = a_1a_2J_n^2 + (a_1b_2 + a_2b_1)J_n + b_1b_2I_n$$

Or, comme en classe, on trouve que $J_n^2 = nJ_n$ si bien que

$$M_1M_2 = (a_1b_2 + a_2b_1 + na_1a_2)J_n + b_1b_2I_n \in \mathcal{A}$$

c'est-à-dire que \mathcal{A} est stable par produit : c'est un sous-anneau de $\mathcal{M}_n(\mathbb{C})$. Enfin, J_n n'est pas inversible car a deux lignes égales. D'une autre manière : si J est inversible, alors, puisque $J_n^2 = nJ_n$, en multipliant par J_n^{-1} , on trouve que $J_n = nI_n$ ce qui est absurde, donc J_n n'est vraiment pas inversible.

2. Soit $M = aJ_n + bI_n \in \mathcal{A}$. Travaillons par équivalences.

$$M^n = I_n \iff (aJ_n + bI_n)^n = I_n$$

Or, aJ_n et bI_n commutent donc on peut appliquer la formule du binôme de Newton :

$$\begin{aligned} M^n = I_n &\iff \sum_{k=0}^n \binom{n}{k} (bI_n)^{n-k} (aJ_n)^k = I_n \\ &\iff \sum_{k=0}^n \binom{n}{k} b^{n-k} a^k J_n^k = I_n \end{aligned}$$

Or, pour tout $k \geq 1$, $J_n^k = n^{k-1} J_n$ donc (attention à bien mettre à part le cas $k = 0$) :

$$\begin{aligned}
M^n = I_n &\iff b^n I_n + \sum_{k=1}^n \binom{n}{k} b^{n-k} a^k n^{k-1} J_n = I_n \\
&\iff b^n I_n + \left(\sum_{k=1}^n \binom{n}{k} b^{n-k} a^k n^{k-1} \right) J_n = I_n \\
&\iff b^n I_n + \left(\frac{1}{n} \sum_{k=1}^n \binom{n}{k} b^{n-k} a^k n^k \right) J_n = I_n \\
&\iff b^n I_n + \frac{1}{n} ((b+an)^n - b^n) J_n = I_n
\end{aligned}$$

La dernière ligne provient du binôme de Newton (complexe). Montrons qu'on peut « identifier » les coefficients (grrrrr). Plus proprement : montrons que, dans l'écriture $aJ_n + bI_n$, il y a unicité des coefficients a et b . Soient $M = a_1 J_n + b_1 I_n = a_2 J_n + b_2 I_n$, si bien que $(a_1 - a_2)J_n = (b_2 - b_1)I_n$. Si $a_1 \neq a_2$, alors

$$J_n = \frac{b_2 - b_1}{a_1 - a_2} I_n$$

ce qui est absurde, J_n n'étant pas proportionnelle à I_n . On en déduit que $a_1 = a_2$ donc $b_1 = b_2$: il y a bien unicité des coefficients. Par conséquent :

$$\begin{aligned}
M^n = I_n &\iff b^n = 1 \quad \text{et} \quad \frac{1}{n} ((b+an)^n - b^n) = 0 \\
&\iff b^n = 1 \quad \text{et} \quad (b+an)^n = 1 \\
&\iff \exists k \in \llbracket 0; n-1 \rrbracket, b = e^{2ik\pi/n} \quad \text{et} \quad (e^{2ik\pi/n} + an)^n = 1 \\
&\iff \exists (k, p) \in \llbracket 0; n-1 \rrbracket^2, b = e^{2ik\pi/n} \quad \text{et} \quad e^{2ik\pi/n} + an = e^{2ip\pi/n} \\
&\iff \exists (k, p) \in \llbracket 0; n-1 \rrbracket^2, b = e^{2ik\pi/n} \quad \text{et} \quad a = \frac{e^{2ip\pi/n} - e^{2ik\pi/n}}{n}
\end{aligned}$$

3. Attention à bien lire l'énoncé : on ne demande pas quand M est inversible, mais quand M admet un inverse **dans** \mathcal{A} ! Là aussi, travaillons par équivalences.

$$\begin{aligned}
M \text{ admet un inverse dans } \mathcal{A} &\iff \exists N \in \mathcal{A}, MN = I_n \\
&\iff \exists (c, d) \in \mathbb{C}^2, (aJ_n + bI_n)(cJ_n + dI_n) = I_n \\
&\iff \exists (c, d) \in \mathbb{C}^2, bdI_n + (bc + ad + nac)J_n = I_n \\
&\iff \exists (c, d) \in \mathbb{C}^2, bd = 1 \quad \text{et} \quad bc + ad + nac = 0
\end{aligned}$$

Dans l'avant-dernière équivalence, on a développé et encore utilisé le fait que $J_n^2 = nJ_n$, et dans la dernière équivalence, on a encore utilisé l'unicité des coefficients dans l'écriture $aJ_n + bI_n$. Travailler par équivalences semble difficile : travaillons par double implication.

Supposons donc que $b(b+na) \neq 0$ et prouvons qu'il existe $(c, d) \in \mathbb{C}^2$, $bd = 1$ et $bc + ad + nac = c(b+na) + ad = 0$, ce qui prouvera (par équivalences) que M admet un inverse dans \mathcal{A} . Puisque $b(b+na) \neq 0$, alors $b \neq 0$ donc, en posant $d = 1/b$, il existe bien d tel que $bd = 1$. De plus, $b+na \neq 0$ donc, en posant

$$c = \frac{-ad}{b+na}$$

on a bien la deuxième condition : il existe c et d tels que ... donc M est bien inversible dans \mathcal{A} et

$$M^{-1} = cJ_n + dI_n = \frac{-a}{b(b+na)} J_n + \frac{1}{b} I_n$$

Réciproquement, supposons qu'il existe d et c tels que $bd = 1$ et $bc + ad + nac = c(b+na) + ad = 0$: alors $b \neq 0$ puisque $bd = 1$. Si $a = 0$ alors $b+na = b \neq 0$, et si $a \neq 0$, alors $c(b+na) = -ad \neq 0$ (car $d \neq 0$ pour la même raison que b) donc, dans tous les cas, $b+na \neq 0$ donc $b(b+na) \neq 0$: d'où l'équivalence (et l'expression de M^{-1} est donnée ci-dessus).

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

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

Montrer que $P^2 = P$.

Correction : Gros classique ! Attention, le groupe n'a aucune raison d'être commutatif. Cependant, le produit est distributif par rapport à la somme donc (faire attention de changer l'indice de sommation d'une des deux sommes en développant) :

$$\begin{aligned} P^2 &= \left(\frac{1}{\text{card}(G)} \sum_{g \in G} g \right) \times \left(\frac{1}{\text{card}(G)} \sum_{g \in G} g \right) \\ &= \frac{1}{\text{card}(G)^2} \sum_{g \in G} \sum_{h \in G} gh \end{aligned}$$

Soit $g \in G$. L'application $h \mapsto gh$ est à valeurs dans G , car G est un sous-groupe donc stable par produit, injective (car si $gh_1 = gh_2$ alors $h_1 = h_2$ en multipliant à gauche par g^{-1} ou car tout élément d'un groupe est régulier) donc bijective puisque G est un ensemble fini. On peut donc poser $u = gh$ et, quand h varie, u décrit G . En d'autres termes, pour tout $g \in G$:

$$\sum_{h \in G} gh = \sum_{u \in G} u$$

Par conséquent :

$$P^2 = \frac{1}{\text{card}(G)^2} \sum_{g \in G} \left(\sum_{u \in G} u \right)$$

Cette deuxième somme ne dépend pas de g (l'indice de sommation de la première somme) : on peut donc la multiplier par le nombre de termes, c'est-à-dire $\text{card}(G)$, ce qui donne finalement :

$$\begin{aligned} P^2 &= \frac{1}{\text{card}(G)^2} \times \text{card}(G) \sum_{u \in G} u \\ &= \frac{1}{\text{card}(G)} \sum_{u \in G} u \end{aligned}$$

L'indice étant muet, $P^2 = P$.

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

1. On dit qu'une matrice $M \in \mathcal{M}_n(\mathbb{K})$ 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 $\mathcal{M}_n(\mathbb{K})$.
2. Même question avec l'ensemble des matrices centrosymétriques : on dit que $M \in \mathcal{M}_n(\mathbb{K})$ est centrosymétrique si $M_{i,j} = M_{n+1-i, n+1-j}$ pour tout $(i, j) \in \llbracket 1; n \rrbracket^2$.

Correction :

1. Tout d'abord, un modèle de matrice en damier, pour bien comprendre le nom :

$$\begin{pmatrix} * & 0 & * & 0 & \dots \\ 0 & * & 0 & * & \dots \\ * & 0 & * & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

En effet, le coefficient en position $(1, 2)$ est nul puisque $1 - 2$ est un nombre impair, et idem pour les autres (mais les coefficients représentés par des étoiles sont quelconques, nuls ou non, nous n'avons aucune information sur eux). D'où le nom de matrice en damier. Notons D l'ensemble des matrices en damier.

- La matrice nulle est en damier.
- Soient M_1 et M_2 en damier. Soient i et j tels que $i - j$ soit impair. Alors

$$\begin{aligned} (M_1 + M_2)_{i,j} &= (M_1)_{i,j} + (M_2)_{i,j} \\ &= 0 \end{aligned}$$

puisque M_1 et M_2 sont en damier : $M_1 + M_2 \in D$, D est stable par somme. De plus, $(-M_1)_{i,j} = 0$ donc $-M \in D$: D est stable par opposé, c'est un sous-groupe de $\mathcal{M}_n(\mathbb{C})$.

- Si $i - j$ est impair, alors $i \neq j$ donc $(I_n)_{i,j} = 0$: $I_n \in D$.
- Montrons enfin que D est stable par produit. Reprenons les notations ci-dessus (M_1, M_2 et i et j tels que $i - j$ soit impair).

$$(M_1 M_2)_{i,j} = \sum_{k=1}^n (M_1)_{i,k} (M_2)_{k,j}$$

Soit $k \in \llbracket 1; n \rrbracket$. Si $i - k$ est impair, alors $(M_1)_{i,k} = 0$. Si $i - k$ est pair, alors $j - k$ est impair : en effet, $j - k$ ne peut pas être pair si $i - k$ est pair puisque $(i - k) - (j - k) = i - j$ est impair. Dès lors, $(M_2)_{j,k} = 0$: dans tous les cas, $(M_1)_{i,k} (M_2)_{k,j} = 0$ dans tous les cas, tous les termes de la somme sont nuls, donc $(M_1 M_2)_{i,j} = 0$: $M_1 M_2 \in D$, D est stable par produit, c'est un sous-anneau de $\mathcal{M}_n(\mathbb{K})$.

- Une matrice est centrosymétrique si elle est symétrique « par rapport au centre de la matrice » : par exemple, $a_{1,1} = a_{n,n}$ c'est-à-dire que le coefficient en haut à gauche est égal au coefficient en bas à droite. Le fait que C (l'ensemble des matrices centrosymétriques) soit un sous-groupe de $\mathcal{M}_n(\mathbb{K})$ est analogue à la question précédente. Soient i et $j \in \llbracket 1; n \rrbracket$. Si $i \neq j$ alors $n + 1 - i \neq n + 1 - j$ donc on a $(I_n)_{i,j} = (I_n)_{n+1-i, n+1-j} = 0$, et si $i = j$, alors $n + 1 - i = n + 1 - j$ donc on a $(I_n)_{i,j} = (I_n)_{n+1-i, n+1-j} = 1$: $I_n \in C$. Montrons enfin que C est stable par produit. Soient M_1 et $M_2 \in C$. Soit $(i, j) \in \llbracket 1; n \rrbracket^2$.

$$\begin{aligned} (M_1 M_2)_{i,j} &= \sum_{k=1}^n (M_1)_{i,k} (M_2)_{k,j} \\ &= \sum_{k=1}^n (M_1)_{n+1-i, n+1-k} (M_2)_{n+1-k, n+1-j} \\ &= \sum_{p=1}^n (M_1)_{n+1-i, p} (M_2)_{p, n+1-j} \\ &= (M_1 M_2)_{n+1-i, n+1-j} \end{aligned}$$

ce qui permet de conclure.

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

Correction : Il suffit de prouver que A est symétrique. Par hypothèse : $A \times (A^\top \times A) = I_n$ donc A est inversible et $A^{-1} = A^\top \times A$. En multipliant l'égalité $A \times A^\top \times A = I_n$ à gauche et à droite par A^{-1} , il vient :

$$\begin{aligned} A^\top &= A^{-1} \times A^{-1} \\ &= A \times A^\top \times A \times A^\top \\ &= A \times (A \times A^\top \times A)^\top \\ &= A \times I_n^\top \\ &= A \times I_n \\ &= A \end{aligned}$$

ce qui permet de conclure.

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

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

Les trois questions sont indépendantes.

1. Montrer que N est une norme, c'est-à-dire :

- $\forall A \in \mathcal{M}_n(\mathbb{C}), N(A) = 0 \iff A = 0$.
- $\forall (A, B) \in \mathcal{M}_n(\mathbb{C})^2, N(A + B) \leq N(A) + N(B)$.

- $\forall (A, \lambda) \in \mathcal{M}_n(\mathbb{C}) \times \mathbb{C}, N(\lambda A) = |\lambda|A.$

2. (a) Montrer que :

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

(b) Montrer que les constantes $1/n$ et n sont les meilleures possibles.

3. Montrer que : $\forall (A, B) \in \mathcal{M}_n(\mathbb{C})^2, N(A \times B) \leq N(A) \times N(B).$

Correction : Pour faire simple : $N(A)$ est le max des sommes des modules des lignes, et $N'(A)$ idem pour les colonnes. En d'autres termes, pour chaque ligne, on somme les modules des coefficients, et la plus grande somme est égale à $N(A)$, et idem pour les colonnes pour $N'(A)$. Par exemple, (dans le cas $n = 3$), si

$$A = \begin{pmatrix} 5 & -6 & -1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

alors $N(A) = 12$ et $N'(A) = 7$.

1. • Soit $A \in \mathcal{M}_n(\mathbb{C})$. L'implication : $A = 0 \Rightarrow N(A) = 0$ est évidente, car si tous les coefficients sont nuls, toutes les sommes de chaque ligne sont nulles dont le maximum est nul. Réciproquement, supposons que $N(A) = 0$. $N(A)$ étant un maximum de nombres positifs, si $N(A) = 0$, c'est que tous les termes sont nuls. En d'autres termes, pour tout $i \in \llbracket 1; n \rrbracket$,

$$\sum_{j=1}^n |A_{i,j}| = 0$$

On a une somme de termes positifs donc tous les termes sont nuls : pour tout j , $|A_{i,j}| = 0$ donc $A_{i,j} = 0$. En d'autres termes : pour tous i et j , $A_{i,j} = 0$, c'est-à-dire que tous les coefficients de A sont nuls donc $A = 0$.

- Soient A et B dans $\mathcal{M}_n(\mathbb{C})$. Soit $i \in \llbracket 1; n \rrbracket$. D'après l'inégalité triangulaire,

$$\sum_{j=1}^n |A_{i,j} + B_{i,j}| \leq \sum_{j=1}^n |A_{i,j}| + \sum_{j=1}^n |B_{i,j}|$$

Or, par définition de $N(A)$ et $N(B)$, le terme de droite est inférieur à $N(A) + N(B)$, c'est-à-dire :

$$\forall i \in \llbracket 1; n \rrbracket, \sum_{j=1}^n |A_{i,j} + B_{i,j}| \leq N(A) + N(B)$$

En particulier, le maximum de ces quantités est inférieur ou égal à $N(A) + N(B)$ c'est-à-dire que $N(A + B) \leq N(A) + N(B)$.

- Pour tout $i \in \llbracket 1; n \rrbracket$,

$$\sum_{i=1}^n |\lambda A_{i,j}| = |\lambda| \times \sum_{i=1}^n |A_{i,j}|$$

En d'autres termes, les sommes pour λA sont les sommes pour A multipliées par $|\lambda|$: en particulier, le maximum est lui-aussi le maximum multiplié par $|\lambda|$, ce qui est le résultat voulu.

N est bien une norme. On prouverait évidemment de la même façon que N' en est une.

2. (a) Soit $A \in \mathcal{M}_n(\mathbb{C})$. Notons i_0 l'indice de la ligne maximale, c'est-à-dire :

$$N(A) = \sum_{j=1}^n |A_{i_0,j}|$$

Or, pour tout $j \in \llbracket 1; n \rrbracket$, $|A_{i_0,j}|$ (qui se trouve donc en colonne j) est inférieur à la somme de tous les modules des termes de la colonne j , c'est-à-dire :

$$|A_{i_0,j}| \leq \sum_{i=1}^n |A_{i,j}|$$

Dès lors :

$$N(A) \leq \sum_{j=1}^n \sum_{i=1}^n |A_{i,j}|$$

Or, la deuxième somme (celle d'indice de sommation i , qui représente la somme de la j -ième colonne) est inférieure au maximum, lorsque i varie, donc est inférieure à $N'(A)$. Finalement :

$$N(A) \leq \sum_{j=1}^n N'(A) = nN'(A)$$

On prouve de même que $N'(A) \neq nN(A)$ ce qui donne l'autre inégalité.

- (b) Cherchons lorsqu'il y a égalité dans les inégalités précédentes. L'inégalité $N(A) \leq nN'(A)$ découle du fait :
- que le terme $|A_{i_0,j}|$ est inférieur à la somme des termes de toute sa colonne : il y a donc égalité lorsque les autres termes sont nuls.
 - que la somme des termes de la j -ième colonne est inférieure au maximum des sommes des colonnes : il y a égalité lorsque ces deux quantités sont égales, c'est-à-dire que toutes les colonnes ont une somme égale au maximum, donc que toutes les colonnes ont même somme.

Finalement, il y a égalité lorsqu'il n'y a qu'un terme non nul par colonne, qui se trouve en ligne i_0 , la ligne ayant la somme maximale, et que toutes les colonnes ont la même somme. En d'autres termes, lorsque A a une ligne non nulle dont tous les termes sont égaux, et tous les autres coefficients de A sont nuls. Par exemple, si

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

alors $N(A) = n$ et $N'(A) = 1$ donc on a $N(A) = nN'(A)$: on ne peut pas améliorer la constante n , et on prouve de même que la constante $1/n$ est optimale.

3. Soit $i \in \llbracket 1; n \rrbracket$.

$$\begin{aligned} \sum_{j=1}^n |(AB)_{i,j}| &= \sum_{j=1}^n \left| \sum_{k=1}^n A_{i,k} B_{k,j} \right| \\ &\leq \sum_{j=1}^n \sum_{k=1}^n |A_{i,k} B_{k,j}| \quad (\text{I.T.}) \\ &\leq \sum_{k=1}^n \sum_{j=1}^n |A_{i,k} B_{k,j}| \\ &\leq \sum_{k=1}^n \left(|A_{i,k}| \times \sum_{j=1}^n |B_{k,j}| \right) \end{aligned}$$

Or, pour tout $k \in \llbracket 1; n \rrbracket$,

$$\sum_{j=1}^n |B_{k,j}| \leq N(B)$$

donc

$$|A_{i,k}| \times \sum_{j=1}^n |B_{k,j}| \leq |A_{i,k}| \times N(B)$$

Dès lors :

$$\begin{aligned} \sum_{j=1}^n |(AB)_{i,j}| &\leq N(B) \sum_{k=1}^n |A_{i,k}| \\ &\leq N(B) \times N(A) \end{aligned}$$

et ceci étant valable pour tout i , c'est valable pour le maximum, ce qui permet de conclure.

Exercice 28 : ★★ Soit $M \in \mathcal{M}_n(\mathbb{Z})$. On suppose qu'il existe $P \in \text{GL}_n(\mathbb{C})$ et $D \in \mathcal{M}_n(\mathbb{C})$ 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.

Correction :

1. D est inversible car diagonale avec des coefficients diagonaux tous non nuls, P et P^{-1} sont inversibles donc M est inversible car produit de matrices inversibles.
2. Par une récurrence immédiate, comme d'habitude, pour tout $q \in \mathbb{N}$, $M^q = PD^qP^{-1}$. Calculons le coefficient d'indice i, j de M^q :

$$\begin{aligned}(M^q)_{i,j} &= \sum_{k=1}^n (PD^q)_{i,k} (P^{-1})_{k,j} \\ &= \sum_{k=1}^n \sum_{m=1}^n P_{i,m} (D^q)_{m,k} (P^{-1})_{k,j}\end{aligned}$$

Or, D est diagonale donc D^q également : $(D^q)_{m,k} = 0$ si $m \neq k$: de la deuxième somme il ne reste donc que le terme pour $m = k$:

$$(M^q)_{i,j} = \sum_{k=1}^n P_{i,k} (D^q)_{k,k} (P^{-1})_{k,j}$$

Dès lors, par inégalité triangulaire :

$$|(M^q)_{i,j}| \leq \sum_{k=1}^n |P_{i,k}| \times |(D^q)_{k,k}| \times |(P^{-1})_{k,j}|$$

Or, les coefficients diagonaux de D sont de module 1, donc c'est aussi le cas de ceux de D^q (les puissances des matrices diagonales s'obtiennent en mettant à la puissance correspondante les coefficients diagonaux), ce qui donne :

$$|(M^q)_{i,j}| \leq \sum_{k=1}^n |P_{i,k}| \times |(P^{-1})_{k,j}|$$

La quantité de droite est peut-être un peu rébarbative, mais elle ne dépend pas de q ! Notons la A , ce qui permet d'affirmer que tous les coefficients de M^q , peu importe q , sont bornés par A . De plus, les puissances de M sont à coefficients entiers, et il y a au plus $2 \lfloor A \rfloor + 1$ entiers entre $-A$ et A (ne pas oublier 0) : il y a $2 \lfloor A \rfloor + 1$ choix pour chaque coefficient. Par principe multiplicatif, il y a $(2 \lfloor A \rfloor + 1)^{n^2}$ choix possibles pour les puissances de M , et ce nombre est peut-être énorme, mais il est fini.

3. D'après le principe des tiroirs, il existe deux (et même une infinité de) puissances de M qui sont égales : il existe $q_1 < q_2$ tels que $M^{q_1} = M^{q_2}$. M étant inversible, $M^{q_2 - q_1} = I_n$: en posant $p = q_2 - q_1$, on a bien $M^p = I_n$. Enfin, $M^p = PD^pP^{-1} = I_n$: en multipliant à gauche par P^{-1} et à droite par P , on trouve que $D^p = I_n$, c'est-à-dire que les coefficients diagonaux de D à la puissance p valent 1, ce qui permet de conclure.

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 $\Omega^\top \times \Omega = I_n$.

Correction : Puisque A est antisymétrique, alors $A^\top = -A$. De plus, on rappelle que la transposition est linéaire, que la transposition change l'ordre d'un produit, et enfin que la transposée de l'inverse est l'inverse de la transposée. Par conséquent :

$$\begin{aligned}\Omega^\top &= ((I_n - A) \times (I_n + A)^{-1})^\top \\ &= ((I_n + A)^{-1})^\top \times (I_n - A)^\top \\ &= ((I_n + A)^\top)^{-1} \times (I_n^\top - A^\top) \\ &= (I_n^\top + A^\top)^{-1} \times (I_n^\top - A^\top) \\ &= (I_n - A)^{-1} \times (I_n + A)\end{aligned}$$

Par conséquent :

$$\Omega^\top \times \Omega = (I_n - A)^{-1} \times (I_n + A) \times (I_n - A) \times (I_n + A)^{-1}$$

Pour conclure, il suffit de vérifier que $I_n + A$ et $I_n - A$ commutent, ce qui est immédiat en calculant les deux produits $(I_n - A)(I_n + A)$ ainsi que $(I_n + A)(I_n - A)$: les deux matrices commutent, on peut donc écrire

$$\Omega^\top \times \Omega (I_n - A)^{-1} (I_n - A) \times (I_n + A) (I_n + A)^{-1} = I_n$$

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 $O_n(\mathbb{Z})$.

Correction : Donnons simplement son cardinal. Un élément de $O_n(\mathbb{Z})$ est totalement caractérisé par

- La place de l'unique coefficient non nul de la première colonne : n choix possibles.
- Sa valeur (± 1) : 2 choix possibles.
- La place de l'unique coefficient non nul de la deuxième colonne : $(n - 1)$ choix possibles (tous sauf celui de la première colonne).
- Sa valeur : encore 2 choix possibles.
- Et ainsi de suite.

Ainsi, il y a $n \times 2 \times (n - 1) \times 2 \times (n - 2) \times 2 \times \dots \times 1 \times 2 = n! \times 2^n$ éléments dans $O_n(\mathbb{Z})$. On peut tout simplement dire qu'il y a $n!$ places possibles pour les coefficients égaux à ± 1 (puisque les lignes où on les trouve forment une permutation de $\llbracket 1; n \rrbracket$) et qu'il y a 2 choix pour chaque coefficient (1 ou -1), donc 2^n choix en tout, et on retrouve le même résultat.

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

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

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

puis préciser cette intersection.

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

Correction :

1. Analogie à l'exercice 59 du chapitre 18.
2. Soit $M \in \mathcal{M}_n(\mathbb{K})$. Soient $(i, j) \in \llbracket 1; n \rrbracket^2$. On a

$$(ME_{k\ell})_{i,j} = \sum_{p=1}^n M_{ip}(E_{k\ell})_{pj}$$

Or, si $j \neq \ell$ alors $(E_{k\ell})_{pj} = 0$ pour tout p donc la somme est nulle, si bien que $(ME_{k\ell})_{i,j} = 0$. Il en découle que toutes les colonnes de $ME_{k\ell}$ sont nulles sauf **éventuellement** la ℓ -ième. Supposons à présent que $j = \ell$. Puisque $(E_{k\ell})_{p\ell} = 0$ si $p \neq k$ et vaut 1 si $p = k$, il vient :

$$(ME_{k\ell})_{i\ell} = \sum_{p=1}^n M_{ip}(E_{k\ell})_{p\ell} = M_{i,k}$$

Finalement, on a :

$$\begin{array}{c} ME_{k\ell} = \\ \left(\begin{array}{cccccc} 0 & \cdots & 0 & \cdots & M_{1k} & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & \vdots & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & M_{k,k} & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & M_{nk} & \cdots & 0 \end{array} \right) \begin{array}{c} k \\ \ell \end{array} \end{array}$$

$$\begin{array}{c} E_{k\ell}M = \\ \left(\begin{array}{cccccc} 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ M_{\ell 1} & \cdots & \cdots & \cdots & M_{\ell \ell} & \cdots & M_{\ell n} \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & \cdots & \cdots & 0 \end{array} \right) \begin{array}{c} k \\ \ell \end{array} \end{array}$$

Si vous êtes habiles de vos doigts, vous aurez peut-être trouvé ce produit « à la main ». On reconnaît la k -ième colonne de M mais attention : elle se trouve en position ℓ de $ME_{k\ell}$! En d'autres termes, la ℓ -ième colonne de $ME_{k\ell}$ est la j -ième colonne de M . De même la k -ième ligne de $E_{k\ell}M$ est la ℓ -ième colonne de M . Par conséquent, $M \in C(E_{k\ell})$ si et seulement si

$$\begin{pmatrix} 0 & \cdots & 0 & \cdots & M_{1k} & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & \vdots & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & \boxed{M_{k,k}} & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & M_{nk} & \cdots & 0 \end{pmatrix}_k = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ M_{\ell 1} & \cdots & \cdots & \cdots & \boxed{M_{\ell\ell}} & \cdots & M_{\ell n} \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & \vdots & \cdots & 0 \end{pmatrix}_\ell$$

Avec les mains : on a une ligne et une colonne qui se croisent, donc les deux matrices sont égales si et seulement si tous les termes sont nuls, sauf les termes « là où la colonne et la ligne se croisent » qui sont égaux. Plus précisément, $M \in C(E_{k\ell})$ si et seulement si $M_{1k} = \cdots = M_{nk} = 0$ (sauf $M_{k,k}$) et $M_{\ell 1} = \cdots = M_{\ell n} = 0$ (sauf $M_{\ell\ell}$) et $M_{k,k} = M_{\ell\ell}$. Finalement, $C(E_{k\ell})$ est l'ensemble des matrices ayant leur k -ième colonne et leur ℓ -ième ligne nulle, sauf en les deux coefficients diagonaux $M_{k,k}$ et $M_{\ell\ell}$ qui sont égaux. Nous n'avons aucune condition sur les autres coefficients de la matrices : ils sont donc quelconques !

3. Montrons cette égalité par double inclusion. L'inclusion $Z \subset \cap \dots$ est triviale : si une matrice commute avec toutes les autres, alors en particulier elle commute avec toutes les matrices élémentaires. Réciproquement, soit $M \in \cap \dots$. Soit $A \in \mathcal{M}_n(\mathbb{R})$. Il suffit de se souvenir (cf. I.2.a) que

$$A = \sum_{i=1}^n \sum_{j=1}^n A_{i,j} E_{i,j}$$

Or, M commute avec toutes les matrices élémentaires donc commute avec A :

$$AM = \sum_{i=1}^n \sum_{j=1}^n A_{i,j} E_{i,j} M = \sum_{i=1}^n \sum_{j=1}^n A_{i,j} M E_{i,j} = M \times \sum_{i=1}^n \sum_{j=1}^n A_{i,j} E_{i,j} = MA$$

En d'autres termes, M commute avec toutes les matrices de $\mathcal{M}_n(\mathbb{R})$ donc $M \in Z$: on en déduit l'inclusion réciproque et l'égalité. Or, d'après la question précédente, si une matrice est dans tous les $E_{k\ell}$, toutes les lignes et toutes les colonnes sont nulles (car k et ℓ prennent toutes les valeurs de 1 à n) sauf les termes diagonaux qui sont égaux. En conclusion, $M \in Z$ si et seulement si tous les coefficients non diagonaux sont nuls et les coefficients diagonaux tous égaux, donc si et seulement s'il existe $\lambda \in \mathbb{R}$ tel que $M = \lambda I_n$. En d'autres termes, $Z = \{\lambda I_n \mid \lambda \in \mathbb{R}\}$: les seules matrices qui commutent avec tous les éléments de $\mathcal{M}_n(\mathbb{R})$ sont les matrices de la forme λI_n .

4. On montre de même qu'une matrice commute avec toutes les matrices diagonales si et seulement si elle commute avec toutes les matrices élémentaires diagonales $E_{i,i}$ donc l'ensemble cherché est

$$\bigcap_{i=1}^n C(E_{i,i})$$

D'après la question 2, une matrice dans cette intersection a des lignes et des colonnes nulles (car i varie de 1 à n) sauf les termes diagonaux, mais ceux-ci ne sont pas forcément égaux. En d'autres termes, les matrices qui commutent avec toutes les matrices diagonales sont exactement les matrices elles-mêmes diagonales.

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

Correction : Devinons une expression que nous prouverons par récurrence. Tout d'abord, A et A^{-1} commutent ($AA^{-1} = A^{-1}A = I_n$) donc on peut utiliser les identités remarquables, à savoir :

$$(A + A^{-1})^2 = A^2 + A^{-2} + 2I_n$$

Or, $A + A^{-1} = I_n$ donc $A^2 + A^{-2} = -I_n$. Multiplions ensuite par $A + A^{-1} = I_n$ pour obtenir :

$$\begin{aligned} -I_n &= (A + A^{-1})(A^2 + A^{-2}) \\ &= A^3 + A^{-1} + A + A^{-3} \\ &= A^3 + I_n + A^{-3} \end{aligned}$$

Dès lors, $A^3 + A^{-3} = -2I_n$. Multiplions ensuite par $A + A^{-1} = I_n$ pour obtenir :

$$\begin{aligned} -2I_n &= (A + A^{-1})(A^3 + A^{-3}) \\ &= A^4 + A^{-2} + A^2 + A^{-4} \\ &= A^4 - I_n + A^{-4} \end{aligned}$$

si bien que $A^4 + A^{-4} = I_n$. Prouvons par récurrence (double) que, pour tout $k \in \mathbb{N}$, il existe α_k tel que $A^k + A^{-k} = \alpha_k I_n$. Le résultat est vrai jusqu'au rang 4 comme on l'a déjà vu. Soit $k \geq 4$, supposons qu'il soit vrai aux rangs k et $k-1$, c'est-à-dire qu'il existe α_{k-1} et α_k tels que

$$A^{k-1} + A^{-(k-1)} = \alpha_{k-1} I_n \quad \text{et} \quad A^k + A^{-k} = \alpha_k I_n$$

En multipliant l'égalité $A^k + A^{k-1} = I_n$ par $A + A^{-1} = I_n$, on obtient comme précédemment :

$$\begin{aligned} \alpha_k I_n &= (A + A^{-1})(A^k + A^{-k}) \\ &= A^{k+1} + A^{k-1} + A^{-(k-1)} + A^{-(k+1)} \\ &= A^{k+1} + \alpha_{k-1} I_n + A^{-(k+1)} \end{aligned}$$

On en déduit que $A^{k+1} + A^{-(k+1)} = (\alpha_k - \alpha_{k-1}) I_n$: il suffit de poser $\alpha_{k+1} = \alpha_k - \alpha_{k-1}$ pour clore la récurrence. Donnons à présent la valeur de α_k pour tout k . On sait que la suite (α_k) vérifie la relation de récurrence : $\forall k \in \mathbb{N}, \alpha_{k+2} = \alpha_{k+1} - \alpha_k$. On reconnaît une suite récurrente linéaire d'ordre 2, dont l'équation caractéristique est $r^2 - r + 1 = 0$ dont les racines (complexes) sont $-j$ et $-j^2$. Par conséquent, il existe x et y (complexes) uniques tels que :

$$\forall k \in \mathbb{N}, \alpha_k = x \times (-j)^k + y \times (-j^2)^k$$

Or, $\alpha_0 = 2$ (puisque $A^0 + A^{-0} = 2I_n$) donc $x + y = 2$, et $\alpha_1 = 1$ donc $-xj - yj^2 = 1$. Par conséquent, $y = 2 - x$ et :

$$\begin{aligned} 1 &= -xj - (2-x)j^2 \\ &= -xj - 2j^2 + xj^2 \\ &= x(j^2 - j) - 2j^2 \\ &= -xi\sqrt{3} - 2j^2 \end{aligned}$$

Finalement, $-xi\sqrt{3} = 1 + 2j^2 = -i\sqrt{3}$ donc $x = 1$ et $y = 1$. En conclusion, pour tout $k \in \mathbb{N}$, $A^k + A^{-k} = \alpha_k I_n$ où $\alpha_k = (-j)^k + (-j^2)^k$. Pour être plus précis, il faut raisonner modulo 6 (modulo 2 à cause du -1 et modulo 3 à cause du j) :

- Si $k \equiv 0[6]$ alors $\alpha_k = 1 + 1 = 2$.
- Si $k \equiv 1[6]$ alors k est impair et congru à 1 modulo 3 donc $\alpha_k = -j - j^2 = 1$.
- Si $k \equiv 2[6]$ alors k est pair et congru à 2 modulo 6 et $2k$ est congru à 4 modulo 6 donc $\alpha_k = j^2 + j = -1$.
- Si $k \equiv 3[6]$ alors k est impair et congru à 3 modulo 6 et $2k$ est congru à 6 modulo 6 donc $\alpha_k = -1 - 1 = -2$.
- Si $k \equiv 4[6]$ alors k est pair et congru à 4 modulo 6 et $2k$ est congru à 8 modulo 6 donc $\alpha_k = j + j^2 = -1$.
- Si $k \equiv 5[6]$ alors k est impair et congru à 5 modulo 6 et $2k$ est congru à 10 modulo 6 donc $\alpha_k = -j^2 - j = 1$.

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

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

On définit $H = \{I_3 + M \mid M \in L\}$. Si A et B appartiennent à $\mathcal{M}_3(\mathbb{R})$, 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 $\text{GL}_3(\mathbb{R})$ et que

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

est un isomorphisme de groupes.

Correction :

1. C'est immédiat :

$$\exp(M_{p,q,r}) = \begin{pmatrix} 1 & p & r + \frac{pq}{2} \\ 0 & 1 & q \\ 0 & 0 & 1 \end{pmatrix}$$

2. Montrons que $(L, *)$ est un groupe.

- Montrons que $*$ est une loi interne sur L . Soit $(p, q, r, a, b, c) \in \mathbb{R}^6$.

$$M_{p,q,r} M_{a,b,c} = \begin{pmatrix} 0 & 0 & pb \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

et

$$M_{a,b,c} M_{p,q,r} = \begin{pmatrix} 0 & 0 & aq \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Par conséquent :

$$M_{p,q,r} * M_{a,b,c} = \begin{pmatrix} 0 & a+p & c+r + \frac{1}{2}(pb-aq) \\ 0 & 0 & q+b \\ 0 & 0 & 0 \end{pmatrix} \quad (1)$$

Il en découle que $*$ est interne sur L .

- Montrons que la loi $*$ est associative dans L . Soient M, N, P trois éléments de L . Par définition de la loi $*$:

$$\begin{aligned} (M * N) * P &= \left(M + N + \frac{1}{2}(MN - NM) \right) * P \\ &= M + N + \frac{1}{2}(MN - NM) + P + \frac{1}{2} \left[\left(M + N + \frac{1}{2}(MN - NM) \right) P \right. \\ &\quad \left. - P \left(M + N + \frac{1}{2}(MN - NM) \right) \right] \\ &= M + N + P + \frac{1}{2}(MN - NM + MP + NP - PM - PN) + \frac{1}{4}(MNP - NMP - PMN + PNM) \end{aligned}$$

De même :

$$M * (N * P) = M + N + P + \frac{1}{2}(NP - PN + MN + MP - NM - PM) + \frac{1}{4}(MNP - MPN - NPM + PNM)$$

Notons $M = M_{p,q,r}$, $N = M_{a,b,c}$ et $P = M_{d,e,f}$. En reprenant le calcul fait à la question précédente :

$$MNP = \begin{pmatrix} 0 & 0 & aq \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & d & f \\ 0 & 0 & e \\ 0 & 0 & 0 \end{pmatrix} = 0_3$$

Par symétrie des rôles, tous les triples produits sont nuls. Ainsi :

$$(M * N) * P = M + N + P + \frac{1}{2}(MN - NM + MP + NP - PM - PN) = M * (N * P)$$

pour tout $(M, N, P) \in L^3$: la loi est associative.

- Soit $M \in L$. Alors :

$$M * 0_3 = M + 0_3 + \frac{1}{2}(M0_3 - 0_3M) = M = 0_3 * M$$

Il en découle que 0_3 est l'élément neutre de la loi $*$ et puisque $0_3 = M_{0,0,0}$, alors $0_3 \in L$: $(L, *)$ admet un élément neutre.

- Soit $M_{p,q,r} \in L$. Notons $N = M_{a,b,c}$ et travaillons par équivalences. On utilise pour cela l'égalité (1) ci-dessus.

$$\left\{ \begin{array}{l} M * N = 0_3 \\ N * M = 0_3 \end{array} \right\} \iff \left\{ \begin{array}{l} a + p = 0 \\ q + b = 0 \\ r + c + \frac{1}{2}(pb - aq) = 0 \\ r + c + \frac{1}{2}(aq - bp) = 0 \end{array} \right\} \iff \left\{ \begin{array}{l} a + p = 0 \\ a = -p \\ b = -q \\ c = -r \end{array} \right.$$

Puisqu'on a travaillé par équivalences, on en déduit que $M_{p,q,r}$ est inversible, d'inverse $M_{-p,-q,-r} = -M_{p,q,r}$. En conclusion, $(L, *)$ est un groupe et l'inverse de $M_{p,q,r}$ est $M_{-p,-q,-r} = -M_{p,q,r}$.

- Notons $Z(L)$ l'ensemble des matrices $M_{p,q,r} \in L$ qui commutent avec tous les éléments de L pour la loi $*$, c'est-à-dire le centre de L :

$$Z(L) = \{M_{p,q,r} \in L \mid \forall M_{a,b,c} \in L, M_{p,q,r} * M_{a,b,c} = M_{a,b,c} * M_{p,q,r}\}$$

Dès lors, $(L, *)$ est commutatif si et seulement si $Z(L) = L$. Travaillons par équivalences.

$$\begin{aligned} M_{p,q,r} \in Z(L) &\iff \forall (a, b, c) \in \mathbb{R}^3, M_{p,q,r} * M_{a,b,c} = M_{a,b,c} * M_{p,q,r} \\ &\iff \forall (a, b, c) \in \mathbb{R}^3, \begin{pmatrix} 0 & a + p & c + r + \frac{1}{2}(pb - aq) \\ 0 & 0 & q + b \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & p + a & r + c + \frac{1}{2}(aq - bp) \\ 0 & 0 & b + q \\ 0 & 0 & 0 \end{pmatrix} \\ &\iff \forall (a, b, c) \in \mathbb{R}^3, c + r + \frac{1}{2}(pb - aq) = r + c + \frac{1}{2}(aq - bp) \\ &\iff \forall (a, b, c) \in \mathbb{R}^3, pb - aq = aq - bp \\ &\iff \forall (a, b, c) \in \mathbb{R}^3, 2pb = 2aq \end{aligned}$$

ce qui est équivalent à $p = q = 0$ en prenant successivement $(a, b) = (1, 0)$ puis $(a, b) = (0, 1)$ (puisque ce résultat est censé être vrai pour tous a, b, c , on peut prendre ceux qui nous arrangent). D'où :

$$Z(L) = \left\{ \begin{pmatrix} 0 & 0 & r \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mid r \in \mathbb{R} \right\} \neq L$$

donc $(L, *)$ n'est pas commutatif.

- Notons $M = M_{p,q,r}$ et $N = M_{a,b,c}$. D'après la question 1 :

$$\exp(M) = \begin{pmatrix} 1 & p & r + \frac{pq}{2} \\ 0 & 1 & q \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad \exp(N) = \begin{pmatrix} 1 & a & c + \frac{ab}{2} \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

Dès lors :

$$\exp(M) \times \exp(N) = \begin{pmatrix} 1 & a + p & \alpha \\ 0 & 1 & b + q \\ 0 & 0 & 1 \end{pmatrix}$$

avec

$$\alpha = r + c + bp + \frac{pq}{2} + \frac{ab}{2}$$

De plus, d'après la question 2, $M * N = M_{a+p, b+q, c+r+\frac{1}{2}(pb-aq)}$ donc

$$\exp(M * N) = \begin{pmatrix} 1 & a+p & \beta \\ 0 & 1 & b+q \\ 0 & 0 & 1 \end{pmatrix}$$

avec

$$\begin{aligned} \beta &= c + r + \frac{1}{2}(pb - aq) + \frac{(a+p)(b+q)}{2} \\ &= c + r + \frac{pb - aq + ab + aq + pb + pq}{2} \\ &= \alpha \end{aligned}$$

ce qui permet de conclure.

5. D'après la question précédente, puisque $-M$ et $-N$ appartiennent aussi à L :

$$\begin{aligned} \exp(M) \exp(N) \exp(-M) \exp(-N) &= \exp(M * N) \exp((-M) * (-N)) \\ &= \exp((M * N) * ((-M) * (-N))) \\ &= \exp\left(M * N + (-M) * (-N) + \frac{1}{2}[M * N, (-M) * (-N)]\right) \end{aligned}$$

Tout d'abord :

$$(-M) * (-N) = -M - N + \frac{1}{2}(MN - NM) = -M - N + \frac{1}{2}[M, N]$$

Il en découle :

$$\exp(M) \exp(N) \exp(-M) \exp(-N) = \exp\left([M, N] + \frac{1}{2}[M * N, (-M) * (-N)]\right)$$

Montrons à présent que $(M * N)$ et $(-M) * (-N)$ commutent, ce qui implique que le commutateur est nul, et donne ainsi le résultat voulu.

$$\begin{aligned} (M * N) * ((-M) * (-N)) &= \left(M + N + \frac{1}{2}[M, N]\right) \left(-M - N + \frac{1}{2}[M, N]\right) \\ &= \left(M + N + \frac{1}{2}(MN - NM)\right) \left(-M - N + \frac{1}{2}(MN - NM)\right) \end{aligned}$$

Or, d'après la question 2, le produit de trois éléments (ou plus) de L est nul donc

$$(M * N) * ((-M) * (-N)) = -M^2 - MN - NM - N^2$$

Le membre de droite étant invariant en changeant (M, N) en $(-M, -N)$:

$$(M * N) * ((-M) * (-N)) = ((-M) * (-N)) * (M * N)$$

ce qui permet de conclure.

6. Montrons que H est un sous-groupe de $\text{GL}_3(\mathbb{R})$.

- Tous les éléments de H sont triangulaires supérieurs avec des 1 dans la diagonale donc sont inversible : H est bien inclus dans $\text{GL}_3(\mathbb{R})$.
- La matrice I_3 peut s'écrire $I_3 + M_{0,0,0}$ et est par conséquent un élément de H : l'élément neutre de la multiplication appartient bien à H , H est non vide.

- Soient $A = I_3 + M_{p,q,r}$ et $B = I_3 + M_{a,b,c}$ deux éléments de H . Il vient :

$$\begin{aligned} AB &= I_3 + M_{p,q,r} + M_{a,b,c} + M_{p,q,r}M_{a,b,c} \\ &= I_3 + M_{p,q,r} + M_{a,b,c} + M_{0,0,pb} \\ &= I_3 + M_{p+a, q+b, r+c+pb} \in H \end{aligned}$$

En d'autres termes, H est stable par produit.

- Soit $M = I_3 + M_{p,q,r} \in H$. Le pivot de Gauß appliqué à M nous dit encore une fois que M est inversible et que

$$M^{-1} = \begin{pmatrix} 1 & -p & pq-r \\ 0 & 1 & -q \\ 0 & 0 & 1 \end{pmatrix} = I_3 + M_{-p, -q, -pq-r} \in H$$

H est stable par inverse, c'est bien un sous-groupe de $\text{GL}_3(\mathbb{R})$.

D'après la question 1, pour tout $(p, q, r) \in \mathbb{R}^3$,

$$\exp(M_{p,q,r}) = I_3 + M_{p,q,r+\frac{pq}{2}} \in H$$

Il en découle que l'image de L par \exp est incluse dans H . D'après la question 3, pour toutes matrices M et N appartenant à L :

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

donc c'est bien un morphisme de groupes. Montrons enfin qu'il est bijectif. Soit $M = I_3 + M_{p,q,r} \in H$. Cherchons les solutions éventuelles de l'équation $\exp(M_{a,b,c}) = M$.

$$\exp(M_{a,b,c}) = M \iff \begin{pmatrix} 1 & a & c+\frac{ab}{2} \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p & r \\ 0 & 1 & q \\ 0 & 0 & 1 \end{pmatrix} \iff \begin{cases} a = p \\ b = q \\ c = r - \frac{pq}{2} \end{cases}$$

En d'autres termes, M admet un unique antécédent par \exp dans L : \exp est bijective.

Exercice 34 : ★★

1. Soit $A \in \text{GL}_n(\mathbb{R})$ 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 $A \in \text{GL}_n(\mathbb{R})$ 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.

Correction :

1. Tout d'abord, aucune ligne ni aucune colonne de A ou A^{-1} ne peut être totalement nulle car une matrice avec une ligne ou une colonne nulle n'est pas inversible. Ainsi, il y a au moins un terme non nul (donc strictement positif) par ligne et par colonne.

Soient $i \neq j$ deux éléments de $\llbracket 1; n \rrbracket$. Alors $(AA^{-1})_{i,j} = 0$ (puisque $AA^{-1} = I_n$) donc

$$\sum_{k=1}^n A_{i,k}(A^{-1})_{k,j} = 0$$

Puisqu'on a une somme de termes positifs, cela implique que tous les termes de la somme sont nuls :

$$\forall i \neq j, \forall k \in \llbracket 1; n \rrbracket, A_{i,k}(A^{-1})_{k,j} = 0$$

En d'autres termes :

$$\forall (i, j, k) \in \llbracket 1; n \rrbracket^3, i \neq j \Rightarrow A_{i,k}(A^{-1})_{k,j} = 0$$

c'est-à-dire qu'on peut choisir i, j, k dans l'ordre qu'on veut, tant que $i \neq j$. Soit $j \in \llbracket 1; n \rrbracket$ et soit k tel que $(A^{-1})_{k,j} \neq 0$ (un tel k existe d'après ce qui précède). Il en découle que pour tout $i \neq j$, $A_{i,k} = 0$: la k -ième colonne de A a au plus un coefficient non nul, et on sait qu'elle a au moins un coefficient non nul, donc cette colonne a exactement

un coefficient non nul : k étant quelconque, toute colonne de A a exactement un terme non nul.

A^\top et $(A^{-1})^\top$ sont aussi à coefficients positifs ou nuls donc le résultat précédent est encore valable pour A^\top : A^\top a exactement un coefficient non nul par colonne, mais les colonnes de A^\top sont exactement les lignes de A , donc A a exactement un coefficient non nul par ligne.

2. Par une succession de permutation des lignes (on met en premier l'unique ligne avec le coefficient en première colonne non nul, etc.), on arrive à une matrice diagonale à coefficients tous non nuls, et ensuite on multiplie chaque ligne par l'inverse de son coefficient diagonal, strictement positif. En d'autres termes, dans l'algorithme du pivot de Gauß, on obtient A^{-1} en partant de I_n à l'aide de permutations et de multiplications par des scalaires positifs donc A^{-1} est à coefficients positifs ou nuls.

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

1. Soit $\sigma \in S_n$. Décrire plus précisément M_σ .
2. Montrer que $G = \{M_\sigma \mid \sigma \in S_n\}$, l'ensemble des matrices de permutation, est un sous-groupe de $\text{GL}_n(\mathbb{K})$ isomorphe à S_n .
3. Soit $A \in \mathcal{M}_n(\mathbb{K})$ 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.

Correction :

1. Pour tout i , l'unique j pour lequel le coefficient ne vaut pas 0 est $j = \sigma(i)$, l'image de i par σ , et alors l'indice vaut 1. En d'autres termes, pour chaque ligne, il y a un unique coefficient non nul, qui vaut 1, et ceci en la colonne $\sigma(i)$. De plus, il y a un unique coefficient non nul par colonne : pour la colonne j , le seul (par bijectivité de σ) indice i tel que le coefficient d'indice i, j soit non nul est celui en ligne $i = \sigma^{-1}(j)$ i.e. l'antécédent de j par σ . Par exemple, si σ est la bijection de $\llbracket 1; 4 \rrbracket$ définie par $\sigma(1) = 2, \sigma(2) = 4, \sigma(3) = 1$ et $\sigma(4) = 3$, alors

$$M_\sigma = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

2. $I_n = M_{\text{Id}}$ où Id est évidemment l'identité de $\llbracket 1; n \rrbracket$: G est non vide. Soit σ_1 et σ_2 deux éléments de S_n . Montrons que $M_{\sigma_1} \times M_{\sigma_2} = M_{\sigma_1 \circ \sigma_2}$. Soit $(i, j) \in \llbracket 1; n \rrbracket^2$.

$$(M_{\sigma_1} \times M_{\sigma_2})_{i,j} = \sum_{k=1}^n (M_{\sigma_1})_{i,k} (M_{\sigma_2})_{k,j}$$

Si $k \neq \sigma_1(i)$ alors $(M_{\sigma_1})_{i,k} = 0$ donc il ne reste que le terme pour $k = \sigma_1(i)$:

$$(M_{\sigma_1} \times M_{\sigma_2})_{i,j} = (M_{\sigma_1})_{i, \sigma_1(i)} (M_{\sigma_2})_{\sigma_1(i), j} = (M_{\sigma_2})_{\sigma_1(i), j}$$

Si $j \neq \sigma_2(\sigma_1(i))$, alors le terme en M_2 est nul donc le coefficient est nul, et si $j = \sigma_2(\sigma_1(i))$ alors le coefficient vaut 1, ce qui permet de conclure. En particulier,

$$\begin{aligned} M_\sigma \times M_{\sigma^{-1}} &= M_{\sigma \circ \sigma^{-1}} \\ &= M_{\text{Id}} \\ &= I_n \end{aligned}$$

et donc, en particulier, M_σ est inversible d'inverse $M_{\sigma^{-1}} \in G$: G est bien un sous-groupe de $\text{GL}_n(\mathbb{K})$. L'application $\varphi : \sigma \mapsto M_\sigma$ est surjective de S_n dans G et, d'après ce qui précède, est un morphisme de groupes. Il suffit donc de prouver que φ est injective. Soit $\sigma \in \ker(\varphi)$ i.e. tel que $\varphi(\sigma) = M_\sigma = I_n$. Alors, pour tout i , le terme d'indice (i, i) vaut 1 donc $\sigma(i) = i$: σ est l'identité, $\ker(\varphi) = \{\text{Id}\}$ donc φ est injective ce qui permet de conclure.

Remarque : Ceci, couplé au théorème de Cayley (exercice 35 du chapitre 18) implique que tout groupe à n éléments est isomorphe à un sous-groupe de $\text{GL}_n(\mathbb{K})$. En d'autres termes, $\text{GL}_n(\mathbb{K})$ contient (à isomorphisme près, c'est-à-dire une copie de) tout sous-groupe d'ordre n .

3. Montrons que $A \times M_\sigma$ est la matrice obtenue en permutant les colonnes (car on multiplie à droite) de A selon la permutation σ , c'est-à-dire que si on note C_1, \dots, C_n les colonnes de A , alors les colonnes de $A \times M_\sigma$ sont $C_{\sigma(1)}, \dots, C_{\sigma(n)}$. Au second semestre, nous pourrions le montrer en utilisant l'écriture de toute permutation comme produit de transposition, mais ici, nous sommes obligés de le prouver à la main. Prenons le problème à l'envers : si on note D_1, \dots, D_n les colonnes de $A \times M_\sigma$, il suffit de prouver que les colonnes de A sont $D_{\sigma^{-1}(1)}, \dots, D_{\sigma^{-1}(n)}$, c'est-à-dire que le terme d'indice i, j de $A \times M_\sigma$ est $a_{i, \sigma^{-1}(j)}$. On a :

$$(A \times M_\sigma)_{i,j} = \sum_{k=1}^n A_{i,k} (M_\sigma)_{k,j}$$

Si $j \neq \sigma(k)$ i.e. si $k \neq \sigma^{-1}(j)$ alors $(M_\sigma)_{k,j} = 0$ et si $k = \sigma^{-1}(j)$ alors $(M_\sigma)_{k,j} = 1$ donc :

$$(A \times M_\sigma)_{i,j} = A_{i, \sigma^{-1}(j)}$$

ce qui est le résultat voulu. On trouve de même que $M_\sigma \times A$ est la matrice obtenue de A en permutant les lignes de A selon la permutation σ .

4. Cela généralise le résultat du cours sur les matrices de permutation car, dans le cours, on a vu le résultat de la question précédente, mais uniquement pour les permutations qui échangent deux valeurs (nous dirons au second semestre que ce sont les transpositions), et là on a montré ce résultat pour des permutations quelconques.

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

- 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 $A = LU$.
- Prouver que cette décomposition est unique.

Correction : Tout d'abord, l'hypothèse « pour tout $k \in \llbracket 1; n \rrbracket$, la sous-matrice $(a_{i,j})_{1 \leq i,j \leq k}$ est inversible » signifie que, pour tout k , la matrice carrée située « en haut à gauche de A » formée des k premières lignes et des k premières colonnes de A , est inversible.

$$\left(\begin{array}{ccc|ccc} a_{1,1} & \dots & a_{1,k} & a_{1,k+1} & \dots & a_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{k,1} & \dots & a_{k,k} & & & \\ \hline a_{k+1,1} & \dots & & a_{k+1,k+1} & & a_{k+1,n} \\ \vdots & & & \vdots & & \vdots \\ a_{n,1} & \dots & & \dots & & a_{n,n} \end{array} \right)$$

- Suivons l'indication de l'énoncé et appliquons la méthode du pivot de Gauß. Plus précisément, appliquons la méthode du pivot de Gauß pour transformer A en matrice triangulaire inférieure avec des 1 sur la diagonale.
 - Tout d'abord, multiplions la première ligne par $1/a_{1,1}$. En effet, la sous-matrice $(a_{1,1})$ de taille 1×1 en haut à gauche est inversible donc $a_{1,1}$ est non nul, ce qui donne une matrice du type :

$$\begin{pmatrix} 1 & b_{1,2} & \dots & b_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & & & \vdots \\ a_{n,1} & \dots & & a_{n,n} \end{pmatrix}$$

On a noté $b_{1,2}$ le coefficient $a_{1,2}/a_{1,1}$ etc.

- Ensuite, mettons des 0 à droite du 1 en faisant, pour tout $j \geq 2$, $C_j \leftarrow C_j - b_{1,j}C_1$:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ c_{2,1} & c_{2,2} & \dots & c_{2,n} \\ \vdots & & & \vdots \\ c_{n,1} & \dots & & c_{n,n} \end{pmatrix}$$

Là aussi, on donne de nouveaux noms aux coefficients (et nous arrêterons de le préciser).

- Multiplions la deuxième ligne par $1/c_{2,2}$. En effet, celui-ci est non nul : la matrice de taille 2

$$\begin{pmatrix} 1 & 0 \\ c_{2,1} & c_{2,2} \end{pmatrix}$$

est obtenue à partir de la sous-matrice de taille 2 originelle

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

par des opérations élémentaires sur les colonnes, et la deuxième est inversible donc la première l'est aussi. Or, celle-ci est triangulaire donc $c_{2,2}$ est bien non nul. On multiplie donc par $1/c_{2,2}$ et ensuite on « nettoie ce qu'il y a à droite » donc on a une matrice de la forme

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ d_{2,1} & 1 & 0 & \dots & 0 \\ d_{3,1} & d_{3,2} & d_{3,3} & \dots & d_{3,n} \\ \vdots & & & & \vdots \\ d_{n,1} & \dots & & & d_{n,n} \end{pmatrix}$$

Là aussi, la matrice de taille 3

$$\begin{pmatrix} 1 & 0 & 0 \\ d_{2,1} & 1 & 0 \\ d_{3,1} & d_{3,2} & d_{3,3} \end{pmatrix}$$

est obtenue à partir de la matrice originelle de taille 3

$$\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

à l'aide d'opérations élémentaires sur les colonnes donc, de même que ci-dessus, $d_{3,3}$ est non nul.

- On multiplie la troisième ligne par $1/d_{3,3}$ et ensuite on nettoie à droite.
- Et ainsi de suite, à chaque fois on divise par le coefficient diagonal restant (non nul par le même argument que ci-dessus) et on nettoie à droite.
- On arrive ainsi à une matrice triangulaire inférieure avec des 1 sur la diagonale qu'on note L .

En d'autres termes, à l'aide d'opérations élémentaires sur les colonnes du type dilatation (diagonale avec des coefficients diagonaux tous non nuls donc triangulaire supérieure inversible) et transvection du type $I_n + \lambda E_{i,j}$ avec $j > i$ (on ajoute λC_i à C_j avec $j > i$) donc triangulaire supérieure (supérieure car à chaque fois on nettoie les colonnes à droite de C_i donc on fait bien $C_j \leftarrow C_j - \dots C_i$ avec $j > i$) inversible : on multiplie A par une succession de matrices triangulaires supérieures inversibles pour obtenir L , c'est-à-dire qu'il existe T_1, \dots, T_k triangulaires supérieures inversibles telles que

$$AT_1 \dots T_k = L$$

Par conséquent, en multipliant successivement par T_k^{-1} à droite, etc., il vient :

$$A = LT_k^{-1} \dots T_1^{-1}$$

Notons $U = T_k^{-1} \dots T_1^{-1}$: les T_k étant triangulaires supérieures inversibles, leurs inverses le sont aussi, et donc leur produit aussi : U est triangulaire supérieure inversible, et $A = LU$, d'où l'existence.

2. Supposons qu'il existe $A = L_1 U_1 = L_2 U_2$ deux décompositions LU . Alors (tout le monde est inversible)

$$L_2^{-1} L_1 = U_2 U_1^{-1}$$

À gauche, on a un produit de matrices triangulaires inférieures avec des 1 sur la diagonale, donc leur produit l'est aussi, et à droite un produit de matrices triangulaires supérieures, et il y a égalité, donc on a des matrices diagonales avec des 1 sur la diagonale, c'est-à-dire l'identité : $L_2^{-1} L_1 = I_n$ donc $L_1 = L_2$ et de même $U_1 = U_2$, d'où l'unicité.