Résumé de cours :
Semaine 12, du 2 au 6 décembre.

Les complexes (fin)

1 Arguments d'un complexe

Propriété. Si $z = a + ib$, où $(a, b) \in \mathbb{R}^2$, $e^z = e^a(\cos(b) + i\sin(b))$.

Définition. Pour tout $z \in \mathbb{C}$, il existe $\rho, \theta \in \mathbb{R}$ tels que $z = \rho e^{i\theta}$. On dit alors que (ρ, θ) est un couple de coordonnées polaires du point $M(z)$ (l'image du complexe z).
On peut imposer $\rho \geq 0$. Dans ce cas, $\rho = |z|$. On dit alors que θ est un argument de z et l'on note $\theta = \arg(z)$.
Lorsque $z \neq 0$, on peut imposer $\rho > 0$ et $\theta \in [0, 2\pi[$. Dans ce cas, le couple (ρ, θ) est unique.

Définition. Un complexe z possède ainsi deux écritures usuelles :
- l'écriture algébrique : $z = a + ib$ avec $a, b \in \mathbb{R}$, ou bien $z = \mathrm{Re}(z) + i\mathrm{Im}(z)$;
- l'écriture trigonométrique (ou exponentielle, ou polaire) : $z = \rho e^{i\theta}$, avec $\rho \in \mathbb{R}_+$ et $\theta \in \mathbb{R}$.

Les relations suivantes font le lien entre ces deux écritures :
lorsque $z = a + ib = \rho e^{i\theta}$ avec $a, b, \rho, \theta \in \mathbb{R}$ et $\rho \geq 0$,
- $\rho = \sqrt{a^2 + b^2}$;
- lorsque $z \neq 0$, $\cos\theta = \dfrac{a}{\sqrt{a^2+b^2}}$ et $\sin\theta = \dfrac{b}{\sqrt{a^2+b^2}}$;
- Lorsque $a \neq 0$, $\tan\theta = \dfrac{b}{a}$;
- Lorsque $z \neq 0$ et $\theta \in [0, \pi]$, $\theta = \arccos\Big(\dfrac{a}{\sqrt{a^2+b^2}}\Big)$;
- Lorsque $z \neq 0$ et $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, $\theta = \arcsin\Big(\dfrac{b}{\sqrt{a^2+b^2}}\Big)$;
- Lorsque $a \neq 0$ et $\theta \in]-\frac{\pi}{2}, \frac{\pi}{2}[$, $\theta = \arctan\Big(\dfrac{b}{a}\Big)$;
- Lorsque $z \neq 0$ et $\theta \in]-\pi, \pi[$, $\theta = 2\arctan\Big(\dfrac{b}{a + \sqrt{a^2+b^2}}\Big)$.

Il faut savoir le démontrer.

Propriétés de l'argument : Si z, z_1, z_2 sont trois complexes non nuls, alors
- $\arg(z_1 z_2) \equiv \arg(z_1) + \arg(z_2)\ [2\pi]$;
- $\arg\Big(\dfrac{1}{z}\Big) \equiv \arg(\overline{z}) \equiv -\arg(z)\ [2\pi]$;
- $\arg\Big(\dfrac{z_1}{z_2}\Big) \equiv \arg(z_1) - \arg(z_2)\ [2\pi]$;
- pour tout $n \in \mathbb{Z}$, $\arg(z^n) \equiv n\arg(z)\ [2\pi]$;
- $\arg(-z) \equiv \arg(z) + \pi\ [2\pi]$;
- $(\arg(z_1) \equiv \arg(z_2)\ [2\pi]) \iff \dfrac{z_1}{z_2} \in \mathbb{R}_+^*$.

Remarque. Pour tout $z \in \mathbb{C}$, $\arg(e^z) \equiv \mathrm{Im}(z)\ [2\pi]$.

Interprétation géométrique du produit dans $\mathbb{C}$: Fixons $z_0 = \rho_0 e^{i\theta_0}$, où $\rho_0 \in \mathbb{R}_+$ et $\theta_0 \in \mathbb{R}$. La multiplication par z_0, c'est-à-dire l'application $z \longmapsto zz_0$ est la composée de $h : z \longmapsto \rho_0 z$ avec $r : z \longmapsto ze^{i\theta_0}$. h s'interprète géométriquement comme une homothétie de centre O et de rapport ρ_0 et r comme la rotation de centre O et d'angle θ_0.

Propriété. Soit $(\rho, \theta) \in \mathbb{R}_+^* \times \mathbb{R}$. Pour tout $z \in \mathbb{C}$, $e^z = \rho e^{i\theta} \iff (\exists k \in \mathbb{Z},\ z = \ln(\rho) + i\theta + 2ik\pi)$.
En particulier, l'application exponentielle $\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C}^* \\ z & \longmapsto & e^z \end{array}$ est surjective et $2i\pi$ périodique.
Il faut savoir le démontrer.

Formule de Moivre : Pour tout $n \in \mathbb{N}$ et $t \in \mathbb{R}$, $\boxed{e^{int} = (\cos t + i \sin t)^n}$.

Propriété. Pour tout $z \in \mathbb{C}$, $\dfrac{d}{dt}(e^{zt}) = ze^{zt}$.

Définition. Pour tout $\alpha \in \mathbb{C}$ et $x \in \mathbb{R}_+^*$, on note $x^\alpha \triangleq e^{\alpha \ln x}$.

Propriété. Pour tout $\alpha \in \mathbb{C}$, $\dfrac{d}{dt}(t^\alpha) = \alpha t^{\alpha-1}$.

Technique de l'angle moyen : $e^{i\alpha} + e^{i\beta} = e^{i\frac{\alpha+\beta}{2}}(e^{i\frac{\alpha-\beta}{2}} + e^{i\frac{-\alpha+\beta}{2}}) = 2e^{i\frac{\alpha+\beta}{2}} \cos(\dfrac{\alpha-\beta}{2})$
et $e^{i\alpha} - e^{i\beta} = e^{i\frac{\alpha+\beta}{2}}(e^{i\frac{\alpha-\beta}{2}} - e^{i\frac{-\alpha+\beta}{2}}) = 2ie^{i\frac{\alpha+\beta}{2}} \sin(\dfrac{\alpha-\beta}{2})$.
Technique à connaître.

2 Linéarisation

Définition. Linéariser une expression trigonométrique, c'est transformer un produit de quantités en sin et cos en une somme de sin ou cos. Une méthode de linéarisation consiste à suivre les étapes suivantes :

- On remplace chaque occurrence en cos ou sin par son expression issue des formules d'Euler ;
- On développe les différents produits qui apparaissent alors ;
- On regroupe les différents termes à l'aide des formules d'Euler pour faire apparaître une somme de cos et de sin.

3 Antilinéarisation

Exercice. Il faut savoir le démontrer.
Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique polynôme T_n tel que, pour tout $\theta \in \mathbb{R}$, $T_n(\cos\theta) = \cos n\theta$. T_n est appelé le n-ième polynôme de Tchebychev de première espèce.

4 Équations polynomiales

4.1 Racines n-ièmes d'un complexe

Les racines n-ièmes de $a \in \mathbb{C}^*$ sont les solutions de l'équation $z^n = a$ en l'inconnue $z \in \mathbb{C}^*$.
Posons $a = re^{i\varphi}$. Alors, en notant $z_0 = r^{\frac{1}{n}} e^{i\frac{\varphi}{n}}$ on a $z_0^n = a$. Ainsi,
$z^n = a \iff z^n = z_0^n \iff \left(\dfrac{z}{z_0}\right)^n = 1 \iff \dfrac{z}{z_0} \in \mathbb{U}_n \iff (\exists k \in \{0, \dots, n-1\},\ z = r^{\frac{1}{n}} e^{i\frac{2k\pi+\varphi}{n}})$.

a possède donc exactement n racines n-ièmes, disposées selon un polygone régulier à n côtés, inscrit dans le cercle de centre O et de rayon $|a|^{\frac{1}{n}}$.

4.2 Équations du second degré

4.2.1 Racines carrées

$a = re^{i\varphi}$ (avec $r > 0$) possède exactement deux racines carrées égales à $\pm\sqrt{r}e^{i\frac{\varphi}{2}}$.

Lorsque $a = x+iy$ avec $x, y \in \mathbb{R}$, on peut déterminer les racines carrées de a selon le procédé suivant :

Si $z = \alpha + i\beta$, alors $z^2 = a \iff \begin{cases} x &= \alpha^2 - \beta^2 \\ \sqrt{x^2+y^2} &= \alpha^2 + \beta^2 \\ \text{sgn}(y) &= \text{sgn}(\alpha\beta) \end{cases}$.

Technique à connaître.

4.2.2 Racines d'un trinôme

Formule : Soit $a, b, c \in \mathbb{C}$ avec $a \neq 0$. Les solutions de l'équation $az^2 + bz + c = 0$ sont $\dfrac{-b \pm \delta}{2a}$, où δ est une racine carrée du discriminant $\Delta = b^2 - 4ac$.

Ces deux racines sont égales si et seulement si $\Delta = 0$. Dans ce cas, l'unique racine vaut $\dfrac{-b}{2a}$. On dit que c'est une racine double.

Il faut savoir le démontrer.

Propriété. Soit $a, b, c \in \mathbb{C}$ avec $a \neq 0$. Notons z_1 et z_2 les deux racines (éventuellement égales à une racine double) du trinôme $aX^2 + bX + c$. Alors $\boxed{z_1 + z_2 = \dfrac{-b}{a} \text{ et } z_1 z_2 = \dfrac{c}{a}}$.

Propriété. Soit $s, p \in \mathbb{C}$.

$\begin{cases} z_1 + z_2 = s \\ z_1 z_2 = p \end{cases}$ si et seulement si $\{z_1, z_2\}$ est l'ensemble des racines du trinôme $X^2 - sX + p$.

Propriété. Pour tout $n \in \mathbb{N}$ avec $n \geq 2$,

$X^n - 1 = \prod_{k=0}^{n-1}(X - e^{\frac{2ik\pi}{n}})$ et $X^{n-1} + \cdots + X + 1 = \prod_{k=1}^{n-1}(X - e^{\frac{2ik\pi}{n}})$.

5 Géométrie du plan complexe

5.1 Distances et angles

Propriété. Soit A, B, C trois points du plan usuel, d'affixes respectifs $a, b, c \in \mathbb{C}$.

- Le vecteur $\overrightarrow{AB}$ est d'affixe $b - a$;
- La distance AB entre A et B est égale à $|b - a|$;
- L'angle orienté $(\widehat{\overrightarrow{CA}, \overrightarrow{CB}})$ vérifie $(\widehat{\overrightarrow{CA}, \overrightarrow{CB}}) \equiv \arg\left(\dfrac{b-c}{a-c}\right)\ [2\pi]$.

Il faut savoir démontrer la dernière propriété.

5.2 Orthogonalité et colinéarité

Propriété. Soit $\vec{u}$ et $\vec{v}$ deux vecteurs non nuls d'affixes $u = a + ib$ et $v = c + id$.

- $\vec{u} \ // \ \vec{v} \iff \dfrac{u}{v} \in \mathbb{R} \iff \text{Im}(\overline{u}v) = 0 \iff ad - bc \overset{\Delta}{=} \begin{vmatrix} a & c \\ b & d \end{vmatrix} \overset{\Delta}{=} \det(\vec{u}, \vec{v}) = 0$.
  $\det(\vec{u}, \vec{v})$ est le déterminant (aussi appelé le produit mixte) des deux vecteurs $\vec{u}$ et $\vec{v}$.
- $\vec{u} \perp \vec{v} \iff \dfrac{u}{v} \in i\mathbb{R} \iff \text{Re}(\overline{u}v) = 0 \iff ac + bd \overset{\Delta}{=} < \vec{u}, \vec{v} > = 0$.
  $< \vec{u}, \vec{v} >$ est le produit scalaire des deux vecteurs $\vec{u}$ et $\vec{v}$.

Il faut savoir le démontrer.

Corollaire. Soit A, B, C trois points du plan usuel, d'affixes respectifs $a, b, c \in \mathbb{C}$.

— (A, B et C sont alignés) $\iff \dfrac{a-b}{c-b} \in \mathbb{R} \iff \mathrm{Im}(\overline{(a-b)}(c-b)) = 0$, c'est-à-dire $C \in (AB) \iff \arg(c-a) \equiv \arg(b-a)\ [\pi] \iff (\exists t \in \mathbb{R},\ \ c = (1-t)a + tb)$.

— (Le triangle ABC est rectangle en B) $\iff \dfrac{a-b}{c-b} \in i\mathbb{R} \iff \mathrm{Re}(\overline{(a-b)}(c-b)) = 0$.

5.3 Équation d'un cercle

Notons C le cercle de centre $\alpha = a + ib \in \mathbb{C}$ et de rayon $r > 0$. Alors
$z = x + iy \in C \iff |z - \alpha| = r \iff (z-\alpha)(\overline{z} - \overline{\alpha}) = r^2 \iff x^2 + y^2 - 2ax - 2by = r^2 - a^2 - b^2$.
Réciproquement, un ensemble admettant une équation cartésienne de la forme
$x^2 + y^2 - 2ax - 2by = c$ est un cercle éventuellement réduit à un point ou à l'ensemble vide.

5.4 Les similitudes directes

Définition. Une application $f : \mathbb{C} \longrightarrow \mathbb{C}$ est une isométrie si et seulement si elle conserve les distances, c'est-à-dire si et seulement si , pour tout $z, z' \in \mathbb{C}$, $|f(z) - f(z')| = |z - z'|$.

Définition. La translation de vecteur $b \in \mathbb{C}$ est la transformation $t_b : z \longmapsto z + b$. Elle est bijective, d'application réciproque t_{-b}, elle ne possède aucun point fixe lorsque $b \neq 0$, c'est une isométrie.

Définition. La rotation de centre $z_0 \in \mathbb{C}$ et d'angle $\theta \in \mathbb{R}$ est la transformation $r_{z_0,\theta} : z \longmapsto e^{i\theta}(z - z_0) + z_0$. Elle est bijective, d'application réciproque $r_{z_0,-\theta}$, elle admet z_0 comme unique point fixe lorsque $\theta \notin 2\pi\mathbb{Z}$, c'est une isométrie.

Définition. L'homothétie de centre $z_0 \in \mathbb{C}$ et de rapport $\lambda \in \mathbb{R}^*$ est la transformation $h_{z_0,\lambda} : z \longmapsto \lambda(z - z_0) + z_0$. Elle est bijective, d'application réciproque $h_{z_0,\frac{1}{\lambda}}$, elle admet z_0 comme unique point fixe lorsque $\lambda \neq 1$.

Définition. La similitude directe de centre $z_0 \in \mathbb{C}$, d'angle $\theta \in \mathbb{R}$ et de rapport $\lambda \in \mathbb{R}^*$ est $s_{z_0,\theta,\lambda} = h_{z_0,\lambda} \circ r_{z_0,\theta} = r_{z_0,\theta} \circ h_{z_0,\lambda} = z \longmapsto \lambda e^{i\theta}(z - z_0) + z_0$. Elle est bijective, d'application réciproque $s_{z_0,-\theta,\frac{1}{\lambda}}$, elle admet z_0 comme unique point fixe lorsque $\lambda e^{i\theta} \neq 1$, elle conserve les proportions (pour tout $z, z' \in \mathbb{C}$, en posant $s = s_{z_0,\theta,\lambda}$, $|s(z) - s(z')| = |\lambda||z - z'|$), elle conserve les angles (pour tout a, b, c deux à deux distincts, $\widehat{(\overrightarrow{s(a)s(b)}, \overrightarrow{s(a)s(c)})} = \widehat{(\overrightarrow{ab}, \overrightarrow{ac})}$: Il faut savoir le démontrer.).

Définition. On dit que f est une similitude affine directe si et seulement si c'est une application de $\mathbb{C}$ dans $\mathbb{C}$ de la forme $z \longmapsto az + b$, où $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$.

Propriété. Soit $f : z \longmapsto az + b$ une similitude directe.
Lorsque $a = 1$, c'est une translation.
Lorsque $a \neq 1$, f possède un unique point fixe $z_0 \in \mathbb{C}$ et f est la similitude directe de centre z_0, d'angle $\arg(a)$ et de rapport $|a|$.
Il faut savoir le démontrer.

Propriété. L'ensemble S^+ des similitudes affines directes est un sous-groupe de $\mathcal{S}(\mathbb{C})$.
Il faut savoir le démontrer.

Propriété. L'application qui à la similitude $z \longmapsto az + b$ associe a (resp : $|a|$) est un morphisme de groupes, dont le noyau est le sous-groupe des translations (resp : des rotations et des translations).

Corollaire. Une composée, quel que soit l'ordre, de translations, de rotations dont la somme des angles est égale à θ et d'homothéties dont le produit des rapports est égal à λ est une similitude directe de la forme $z \longmapsto \lambda e^{i\theta} z + b$.

5.5 Les similitudes indirectes

Notation. Notons $c : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$ l'opérateur de conjugaison, qui correspond à la réflexion par rapport à l'axe des x.

Définition. On note $S^- = \{s \circ c \ / \ s \in S^+\} = \{c \circ s \ / \ s \in S^+\}$.
Les éléments de S^- sont appelés les similitudes indirectes.

5.6 Triangles semblables

Définition. On dit que deux triangles du plan complexe sont directement semblables si et seulement si l'un est l'image de l'autre par une similitude directe.

Propriété. Soit a, b, c trois complexes deux à deux distincts et a', b', c' trois autres complexes deux à deux distincts. Les deux triangles (a, b, c) et (a', b', c') sont directement semblables si et seulement si $\dfrac{c-a}{b-a} = \dfrac{c'-a'}{b'-a'}$, c'est-à-dire si et seulement si (en notant AB la distance entre deux points A et B), $\dfrac{ac}{ab} = \dfrac{a'c'}{a'b'}$ et $\widehat{bac} = \widehat{b'a'c'}$.

Propriété. Deux triangles non plats (a, b, c) et (a', b', c') du plan complexe sont directement semblables si et seulement si ils ont les mêmes angles.

La structure de groupe

6 Définitions

Définition. $(G, .)$ est un groupe si et seulement si G est muni d'une loi interne "." qui vérifie
- l'associativité : pour tout $x, y, z \in G$, $x(yz) = (xy)z$;
- l'existence d'un élément neutre 1_G : pour tout $x \in G$, $1_G.x = x.1_G = x$:
- l'existence, pour tout $x \in G$, d'un symétrique x^{-1} tel que : $xx^{-1} = x^{-1}x = 1_G$.

Définition. Pour un groupe, "commutatif" et "abélien" sont synonymes.

Notation. On utilise principalement deux notations pour désigner la loi interne d'un groupe :
◇ *Notation multiplicative :* dans un groupe $(G, .)$, l'élément neutre est noté 1 ou 1_G, le symétrique de $x \in G$ est noté x^{-1} et si $x_1, \ldots, x_n \in G$, on note $x_1 \times \cdots \times x_n = \prod_{i=1}^{n} x_i$, en convenant que ce produit vaut 1_G lorsque $n = 0$ (produit vide).
◇ *Notation additive :* dans un groupe *abélien* $(G, +)$, l'élément neutre est noté 0 ou 0_G, le symétrique de $x \in G$ est noté $-x$ et si $x_1, \ldots, x_n \in G$, on note $x_1 + \cdots + x_n = \sum_{i=1}^{n} x_i$, en convenant que cette somme vaut 0_G lorsque $n = 0$ (somme vide).

Définition. Si $(G, .)$ est un groupe fini, le cardinal de G est appelé l'***ordre*** de G.

7 Calculs dans un groupe

Propriété. Soit $(G, .)$ un groupe et $a \in G$. Alors a est régulier (ou simplifiable) à gauche et à droite, c'est-à-dire que $\forall x, y \in G$, $[ax = ay \Longrightarrow x = y]$ et $[xa = ya \Longrightarrow x = y]$.

Propriété. Dans un groupe $(G,.)$, $(x_1 \times \cdots \times x_n)^{-1} = x_n^{-1} \times \cdots \times x_1^{-1}$.

Propriété. Dans un groupe abélien $(G,+)$, on pose $x - y \stackrel{\Delta}{=} x + (-y)$.
On dispose des formules : $x-(y+z) = x-y-z$ et $x-(y-z) = x-y+z$.

8 Construction de groupes

8.1 Groupe produit

Définition. Le groupe produit des n groupes $((G_i, ._i))_{i\in\{1,\dots,n\}}$ est $(G,.)$, où $G = G_1 \times \cdots \times G_n$ et où la loi "." est définie par : $(x_1,\dots,x_n).(y_1,\dots,y_n) = (x_1 ._1 y_1, \dots, x_n ._n y_n)$.

8.2 Le groupe symétrique

Propriété. Si E est un ensemble, alors l'ensemble des bijections de E dans E est un groupe pour la loi de composition. On l'appelle le groupe symétrique de E et on le note $\mathcal{S}(E)$. Son élément neutre est l'application identité Id_E et, pour tout $f \in \mathcal{S}(E)$, le symétrique de f est la bijection réciproque de f, dont la notation f^{-1} est en cohérence avec cette propriété.

9 Sous-groupes

9.1 Définition

Propriété et définition : Soit $(G,.)$ un groupe et H une partie de G.
H est un groupe pour la restriction de la loi "." à $H \times H$, avec le même élément neutre 1_G si et seulement si
- $H \neq \emptyset$;
- $\forall (x,y) \in H^2$, $xy \in H$ (stabilité du produit) ;
- $\forall x \in H$, $x^{-1} \in H$ (stabilité du symétrique).

Cet ensemble de conditions est équivalent à
- $H \neq \emptyset$;
- $\forall (x,y) \in H^2$, $xy^{-1} \in H$.

Dans ce cas, on dit que H est un ***sous-groupe*** de G.

Propriété de transitivité : Un sous-groupe d'un sous-groupe d'un groupe G est un sous-groupe de G.

9.2 Produit fonctionnel

Définition. Soit $(G,.)$ un groupe et A un ensemble quelconque. Pour tout $f, g \in G^A$, on convient que $f.g$ est l'application de A dans G définie par : $\forall a \in A$, $(f.g)(a) = f(a).g(a)$.
Alors G^A est un groupe, dont l'élément neutre est l'application constante $a \longmapsto 1_G$ et pour lequel le symétrique de $f \in G^A$ est $f^{-1} : \begin{array}{ccc} A & \longrightarrow & G \\ a & \longmapsto & [f(a)]^{-1} \end{array}$.

9.3 Groupe engendré par une partie

Propriété. Soit I un ensemble non vide, éventuellement infini. Soient G un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors l'intersection $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Il faut savoir le démontrer.

Définition. Soit G un groupe et A une partie de G.
Notons $\mathcal{S}$ l'ensemble des sous-groupes de G contenant A. $\mathcal{S}$ est non vide car $G \in \mathcal{S}$.
Alors $\bigcap_{H \in \mathcal{S}} H$ est un sous-groupe de G contenant A et, par construction, c'est le plus petit sous-groupe contenant A. On le note $Gr(A)$.

Propriété. Si $A \subset B$, alors $Gr(A) \subset Gr(B)$.

Propriété. Soit $(G, .)$ un groupe et A une partie de G. Notons $A^{-1} = \{a^{-1} / a \in A\}$.
Alors $Gr(A) = \left\{ \prod_{i=1}^{n} a_i / n \in \mathbb{N},\ \forall i \in \{1, \dots, n\},\ a_i \in A \cup A^{-1} \right\}$.
Il faut savoir le démontrer.

Définition. Si H et K sont deux sous-groupes d'un groupe abélien $(G, +)$, on note $H + K = \{h + k / (h, k) \in H \times K\}$. C'est le groupe engendré par $H \cup K$.

Définition. Soit G un groupe et A une partie de G.
A est une ***partie génératrice*** de G si et seulement si $Gr(A) = G$.

9.4 Puissances d'un élément d'un groupe

Définition. Soit $(G, .)$ un groupe et $a \in G$. On définit la famille $(a^n)_{n \in \mathbb{Z}}$ par les relations suivantes :
- Initialisation : $a^0 = 1_G$ (encore le produit vide) ;
- Itération : pour tout $n \in \mathbb{N}$, $a^{n+1} = a.a^n$ (donc pour $n \in \mathbb{N}^*$, $a^n = \underbrace{a \times \cdots \times a}_{n fois}$) ;
- Symétrique : pour tout $n \in \mathbb{Z}$ avec $n < 0$, $a^n = (a^{-n})^{-1}$.

Formules : pour tout $n, m \in \mathbb{Z}$, $a^n a^m = a^{n+m}$ et $(a^n)^m = a^{nm}$.
Si $ab = ba$ (on dit que a et b commutent), pour tout $n \in \mathbb{Z}$, $(ab)^n = a^n b^n$.

Remarque. Si a et b commutent, alors pour tout $n, k \in \mathbb{Z}$, a^n et b^k commutent également entre eux.
Il faut savoir le démontrer.

En notation additive, dans le cadre des groupes commutatifs, ce qui précède devient :

Définition. soit $(G, +)$ un groupe commutatif et a un élément de G. On **définit** la famille $(na)_{n \in \mathbb{Z}}$ par les relations suivantes :
- Initialisation : $0.a = 0_G$;
- Itération : pour tout $n \in \mathbb{N}$, $(n+1).a = a + (n.a)$
  (donc pour $n \in \mathbb{N}^*$, $n.a = \underbrace{a + \cdots + a}_{n fois}$) ;
- Symétrique : pour tout $n \in \mathbb{Z}$ avec $n < 0$, $n.a = -((-n).a)$.

Propriété. Soit $(G, +)$ un groupe abélien et $a, b \in G$. Pour tout $n, m \in \mathbb{Z}$,
$(n.a) + (m.a) = (n + m).a$, $m.(n.a) = (nm).a$ et $n.(a + b) = (na) + (nb)$.

Propriété. Soit $(G, +)$ un groupe abélien et A une partie de G.
Alors $Gr(A) = \left\{ \sum_{a \in A} n_a.a / (n_a)_{a \in A} \in \mathbb{Z}^{(A)} \right\}$.

Remarque. En particulier, $Gr(\{x_1, \dots, x_p\}) = \left\{ \sum_{i=1}^{p} n_i x_i / (n_i)_{1 \le i \le p} \in \mathbb{Z}^p \right\}$.

9.5 Groupe monogène

Propriété. Soit $(G,.)$ un groupe et $a \in G$. Alors le groupe engendré par la partie $\{a\}$ est $Gr(\{a\}) = \{a^n / n \in \mathbb{Z}\}$. On le note plus simplement $Gr(a)$.

Propriété. Soit $(G,+)$ un groupe abélien et $a \in G$. Alors le groupe engendré par la partie $\{a\}$ est $Gr(\{a\}) = \{na / n \in \mathbb{Z}\}$. On le note $Gr(a)$. On peut donc écrire $Gr(a) = \mathbb{Z}.a$.

Propriété. Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$.
Il faut savoir le démontrer.

Définition. Soit a un élément d'un groupe G. Lorsque $Gr(a)$ est de cardinal fini, ce cardinal est appelé l'ordre de a.

Définition. On dit qu'un groupe $(G,.)$ est ***monogène*** si et seulement si il existe $a \in G$ tel que $G = Gr(a)$. On dit alors que a est un ***générateur*** de G.

Remarque. Tout groupe monogène est abélien.

Définition. Un groupe G est dit ***cyclique*** si et seulement si G est monogène et fini.

Exemple. $\mathbb{U}_n = \{e^{2i\pi\frac{k}{n}} / k \in \{0,\dots,n-1\}\}$ est un groupe cyclique.

Propriété. Soit $(G,.)$ un groupe, $a \in G$ et $n \in \mathbb{N}^*$.
Les propriétés suivantes sont équivalentes :
- i) $Gr(a)$ est cyclique de cardinal n.
- ii) $\{k \in \mathbb{N}^* / a^k = 1\}$ est non vide et son minimum est égal à n.
- iii) Pour tout $k \in \mathbb{Z}$, $[a^k = 1 \iff k \in n\mathbb{Z}]$.
- iv) Les éléments de $Gr(a)$ sont exactement $1, a, \dots, a^{n-1}$ et ils sont deux à deux distincts.

Dans ce cas, n est l'ordre de a et de $Gr(a)$.
Il faut savoir le démontrer.

9.6 Morphisme de groupes

Définition. Soient (G,Δ) et (H,∇) deux groupes.
Une application f de G dans H est un ***morphisme*** (on dit aussi un ***homomorphisme***) de groupes si et seulement si

$$\forall (x,y) \in G^2 \quad f(x\Delta y) = f(x)\nabla f(y).$$

Un ***isomorphisme*** est un morphisme bijectif.
Un ***endomorphisme*** est un morphisme de G dans lui-même.
Un ***automorphisme*** est un endomorphisme bijectif.

Propriété. Si a est un élément de $(G,.)$, alors $\begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (G,.) \\ n & \longmapsto & a^n\end{array}$ est un morphisme de groupes.

Propriété. Si f est un morphisme de $(G,.)$ dans $(H,.)$, alors
$f(1_G) = 1_H$ et pour tout $x \in G$, $f(x)^{-1} = f(x^{-1})$.

Propriété. En notation additive, si f est un morphisme entre deux groupes abéliens $(G,+)$ et $(H,+)$, alors $f(0_G) = 0_H$ et, pour tout $x \in G$, $-f(x) = f(-x)$.

Propriété. Soit φ un morphisme du groupe $(G,.)$ vers le groupe $(G',.)$.

Alors, pour tout $n \in \mathbb{N}$ et $x_1,\dots,x_n \in G$, $\varphi\Big(\prod_{i=1}^{n} x_i\Big) = \prod_{i=1}^{n} \varphi(x_i)$.

De plus, pour tout $n \in \mathbb{Z}$ et $a \in G$, $\varphi(a^n) = \varphi(a)^n$.
Il faut savoir le démontrer.

Propriété. Soit φ un morphisme du groupe abélien $(G,+)$ vers le groupe abélien $(G',+)$. Alors, pour tout $n \in \mathbb{N}$ et $x_1, \dots, x_n \in G$, $\varphi\Big(\sum_{i=1}^{n} x_i\Big) = \sum_{i=1}^{n} \varphi(x_i)$.
De plus, pour tout $n \in \mathbb{Z}$ et $a \in G$, $\varphi(na) = n\varphi(a)$.

Propriété. La composée de deux morphismes de groupes est un morphisme de groupes.

Propriété. Si $f : G \longrightarrow H$ est un isomorphisme de groupes, f^{-1} est encore un isomorphisme de groupes, de H dans G.

Propriété. Soit $(G,.)$ un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. C'est un sous-groupe de $\mathcal{S}(G)$.

Définition. Soit $\varphi : G \longrightarrow G$ un endomorphisme et H un sous-groupe de G. On peut définir $\varphi|_H^H$ si et seulement si H est stable par φ, c'est-à-dire si et seulement si $[\forall x \in H,\ \varphi(x) \in H]$. Dans ce cas, $\varphi|_H^H$ est aussi un **endo**morphisme, appelé l'endomorphisme induit par φ sur H, ou plus simplement la restriction de φ à H (il y a bien sûr ambiguïté).

Propriété. Soit f un morphisme de G dans H, G' un sous-groupe de G et H' un sous-groupe de H. Alors $f(G')$ est un sous-groupe de H et $f^{-1}(H')$ est un sous-groupe de G.
Il faut savoir le démontrer.

Définition. Soient $(G,.)$ et $(H,.)$ deux groupes, et f un morphisme de G dans H.
On appelle ***noyau*** de f le sous-groupe de G suivant :

$$\boxed{Ker(f) = f^{-1}(\{1_H\}) = \{x \in G / f(x) = 1_H\}.}$$

On appelle ***image*** de f le sous-groupe de H suivant :

$$\boxed{Im(f) = f(G) = \{f(x) / x \in G\}.}$$

Remarque. En notation additive, Si f est un morphisme dont le groupe d'arrivée $(H,+)$ est abélien, alors $Ker(f) = f^{-1}(\{0_H\}) = \{x \in G / f(x) = 0_H\}$.

Propriété. Soient $(G,.)$ et $(H,.)$ deux groupes, et f un morphisme de G dans H.

$$\begin{array}{ll} f \text{ est injective si et seulement si} & Ker(f) = \{1_G\}, \\ f \text{ est surjective si et seulement si} & Im(f) = H. \end{array}$$

Propriété. Un groupe est monogène non cyclique si et seulement si il est isomorphe à $(\mathbb{Z},+)$.
Il faut savoir le démontrer.

9.7 Groupe symétrique

Notation. Pour tout $n \in \mathbb{N}$, on pose $\mathbb{N}_n = \{k \in \mathbb{N} / 1 \leq k \leq n\}$. En particulier $\mathbb{N}_0 = \emptyset$.

Définition. Soit $n \in \mathbb{N}$. $\mathcal{S}(\mathbb{N}_n)$ s'appelle le groupe symétrique de degré n. Il est plus simplement noté $\mathcal{S}_n$. Ses éléments sont les bijections sur $\mathbb{N}_n$, que l'on appelle aussi des permutations.

Notation. Si $f \in \mathcal{S}_n$, on note $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$.

Définition. Soient $k \in \mathbb{N}_n$ et $a_1, a_2 \dots a_k$ k éléments distincts de $\mathbb{N}_n$.
On note $(a_1\ a_2\ \dots\ a_k)$ la permutation f telle que : $\forall i \in \{1, \dots, k-1\}\ \ f(a_i) = a_{i+1}$, $f(a_k) = a_1$, les autres éléments de $\mathbb{N}_n$ étant invariants par f.
On dit que $(a_1\ \dots\ a_k)$ est un ***cycle*** de longueur k dont le ***support*** est $\{a_1, \dots, a_k\}$.

Définition. On appelle ***transposition*** tout cycle de longueur 2.
Si $a, b \in \mathbb{N}_n$ avec $a \neq b$, la transposition $(a\ b)$ échange a et b sans modifier les autres éléments de $\mathbb{N}_n$.