Résumé de cours :
Semaine 12, du 1 au 5 décembre.

Les complexes (fin)

1 Les similitudes directes (fin)

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 $z \longmapsto \lambda e^{i\theta} z + b$.

2 Les similitudes indirectes

Notation. Notons $\begin{array}{rccc} c : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \overline{z} \end{array}$ 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.

3 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.

Les groupes

4 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 $x_1,\dots,x_n \in G$, 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 $x_1,\dots,x_n \in G$, 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.

5 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 $x - y \overset{\Delta}{=} x + (-y)$.
On dispose des formules : $x-(y+z) = x-y-z$ et $x-(y-z) = x-y+z$.

6 Construction de groupes

6.1 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 : $(x_1,\dots,x_n).(y_1,\dots,y_n) = (x_1._1y_1,\dots,x_n._ny_n)$.

6.2 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 $\begin{array}{rccc} f^{-1} : & A & \longrightarrow & G \\ & a & \longmapsto & [f(a)]^{-1} \end{array}$.

6.3 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.

7 Sous-groupes

7.1 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.

7.2 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 $Gr(A)=G$.

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

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

7.4 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.

8 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 Le groupe symétrique de degré n

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

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 $\mathbb{N}_n$.

Propriété. Deux cycles dont les supports sont disjoints commutent toujours entre eux.
Il faut savoir le démontrer.

Théorème. Toute permutation de $\mathcal{S}_n$ se décompose de manière unique en un produit (commutatif) de cycles dont les supports sont deux à deux disjoints.

Propriété. Pour tout $n \in \mathbb{N}^*$, pour toute permutation σ de $\mathcal{S}_n$, il existe $k \in \mathbb{N}$ et k transpositions $\tau_1,\ldots,\tau_k$ telles que $\sigma = \tau_1 \circ \cdots \circ \tau_k$. Cependant une telle décomposition n'est pas unique.
La démonstration par récurrence est à connaître.

Formule : $(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_2) \circ (a_2\ a_3) \circ \cdots \circ (a_{k-1}\ a_k)$.

Définition. Soit $n \in \mathbb{N}^*$ et soit $\sigma \in \mathcal{S}_n$. La décomposition de σ en un produit de transpositions $\tau_1 \circ \cdots \circ \tau_k$ n'est pas unique, mais le nombre k de transpositions utilisées a toujours la même parité. Ainsi $(-1)^k$ ne dépend que de σ. On l'appelle la signature de σ et on le note $\varepsilon(\sigma)$.
Les permutations de signature 1 s'appellent les permutations paires,
Les permutations de signature -1 s'appellent les permutations impaires.

Propriété. L'application signature est l'unique morphisme de $\mathcal{S}_n$ dans $(\{-1,1\},\times)$ qui envoie toute transposition sur -1.

Propriété. Soit $n \in \mathbb{N}^*$. On note $\mathcal{A}_n$ l'ensemble des permutations paires de $\mathcal{S}_n$.
C'est un sous-groupe de $\mathcal{S}_n$, appelé le groupe alterné de degré n.

Propriété. Si $n \geq 2$, alors $|\mathcal{A}_n| = \dfrac{n!}{2}$.
Il faut savoir le démontrer.

10 Groupes quotients

Notation. On fixe un groupe $(G,.)$ et un sous-groupe H de G.
On note R_H la relation binaire définie sur G par : $\forall (x,y) \in G^2,\ \ [xR_Hy \iff x^{-1}y \in H]$.

Propriété. R_H est une relation d'équivalence et, pour tout $x \in G$, la classe d'équivalence de x pour R_H est $\overline{x} = \{xh/h \in H\} \overset{\Delta}{=} xH$. On note G/H l'ensemble des classes d'équivalence.
Il faut savoir le démontrer.

Théorème de Lagrange (Hors programme) : Si G est de cardinal fini, alors $|H|$ divise $|G|$.
Il faut savoir le démontrer.

Corollaire. (Hors programme) Si p est un nombre premier, tout groupe de cardinal p est cyclique.

Théorème. (au programme) : Si $(G,.)$ est un groupe fini, $\forall a \in G,\ \ a^{|G|} = 1_G$.

Théorème. Soit $(G,+)$ un groupe **commutatif** et H un sous-groupe de G. Pour tout $x,y \in G$, on convient que $xR_Hy \iff y-x \in H$. Alors R_H est une relation d'équivalence. On note G/H l'ensemble de ses classes d'équivalence.
En posant, pour tout $x,y \in G$, $\overline{x}+\overline{y} \overset{\Delta}{=} \overline{x+y}$, on définit une loi "+" sur G/H pour laquelle G/H est un groupe commutatif. De plus, $\begin{array}{ccc} G & \longrightarrow & G/H \\ x & \longmapsto & \overline{x} \end{array}$ est un morphisme, que l'on appelle la surjection canonique.
Il faut savoir le démontrer.

Propriété. Soit $n \in \mathbb{N}$. Dans $(\mathbb{Z}/n\mathbb{Z},+)$, on dispose des règles de calcul suivantes :
- Pour tout $a,b \in \mathbb{Z}$, $\overline{a} = \overline{b} \iff a \equiv b\ [n]$,
- Pour $a,b \in \mathbb{Z}$, $\overline{a+nb} = \overline{a}$,
- $\overline{0} = 0_{\mathbb{Z}/n\mathbb{Z}}$,
- pour tout $k \in \mathbb{Z}$, $-\overline{k} = \overline{-k}$,
- pour tout $h,k \in \mathbb{Z}$, $\overline{h+k} = \overline{h}+\overline{k}$,
- pour tout $h,k \in \mathbb{Z}$, $h\overline{k} = \overline{hk}$.