Résumé de cours :
Semaine 12, du 4 décembre au 8 décembre.

1 Les complexes (fin)

1.1 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.

1.2 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.

2 Les groupes (suite)

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

2.2 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 $Gr(A) = G$.

2.3 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 $n, m \in \mathbb{Z}$, $a^n a^m = a^{n+m}$ 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, $Gr(\{x_1, \dots, x_p\}) = \left\{ \sum_{i=1}^{p} n_i x_i / (n_i)_{1 \le i \le p} \in \mathbb{Z}^p \right\}$.

2.4 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.

2.5 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.

2.6 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 $\mathbb{N}_n$.

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 $\tau_1, \dots, \tau_k$ 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 : $(a_1\ a_2\ \dots\ a_k) = (a_1\ a_2) \circ (a_2\ a_3) \circ \cdots \circ (a_{k-1}\ a_k)$.

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.

2.7 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, $\forall a \in G,\ \ a^{|G|} = 1_G$.

3 La structure d'anneau

3.1 Définition

Définition. On appelle ***anneau*** tout triplet $(A, +, .)$, où A est un ensemble et où "+" et "." sont deux lois internes sur A telles que
- $(A, +)$ est un groupe abélien (l'élément neutre étant noté 0 ou 0_A),
- "." est une loi associative, admettant un élément neutre noté 1 ou 1_A,
- la loi "." est ***distributive*** par rapport à la loi "+", c'est-à-dire que
$\forall (x, y, z) \in A^3\ \ x.(y + z) = (x.y) + (x.z)$ et $(x + y).z = (x.z) + (y.z)$.

Définition. Un anneau $(A, +, .)$ est commutatif ou abélien si et seulement si la loi "." est commutative.

3.2 Calculs dans un anneau

Propriété. Si A est un anneau, pour tout $x, y \in A$ et $n \in \mathbb{Z}$,
$0.x = x.0 = 0$, $(nx).y = x.(ny) = n(x.y)$. En particulier, $-x = (-1_A).x = x.(-1_A)$.
Il faut savoir le démontrer.

Exemple. $\{0\}$ est un anneau en posant $0 + 0 = 0$ et $0.0 = 0$. On l'appelle l'anneau nul.

Propriété. Si A n'est pas l'anneau nul, alors $1_A \neq 0_A$.

Exemples. Si A est un anneau, pour tout ensemble E, $\mathcal{F}(E, A)$ et $A^{\mathbb{N}}$ sont des anneaux.

Propriété. *Généralisation de la distributivité.* Soient A un anneau, et $n, p \in \mathbb{N}$.
Pour tout $(a_1, \ldots, a_n) \in A^n$ et $(b_1, \ldots, b_p) \in A^p$ $\left(\sum_{i=1}^{n} a_i\right).\left(\sum_{i=1}^{p} b_i\right) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} a_i.b_j$.

3.3 Puissances d'un élément

Notation. Dans ce paragraphe on fixe un anneau A.

Définition. $a \in A$ est inversible si et seulement s'il admet un symétrique (un inverse) pour la loi ".".

Définition. Si $a \in A$. On définit la famille (a^n) par les relations suivantes :
- Initialisation : $a^0 = 1_A$;
- Itération : pour tout $n \in \mathbb{N}$, $a^{n+1} = a.a^n$ (donc pour $n \in \mathbb{N}^*$, $a^n = \underbrace{a \times \cdots \times a}_{n fois}$) ;
- Lorsque a est inversible, pour tout $n \in \mathbb{Z}$ avec $n < 0$, on note $a^n = (a^{-n})^{-1}$.

Définition. $a \in A \setminus \{0\}$ est nilpotent si et seulement si il existe $n \in \mathbb{N}$ avec $n \geq 2$ tel que $a^n = 0$.

Propriété. Pour tout $n, m \in \mathbb{N}$ $a^n a^m = a^{n+m}$ et $(a^n)^m = a^{nm}$.
Lorsque a est inversible, c'est valable pour tout $n, m \in \mathbb{Z}$.

Propriété. Soit $a, b \in A$ tels que $ab = ba$ (on dit que a et b commutent).
Pour tout $n, m \in \mathbb{N}$, $(ab)^n = a^n b^n$. Lorsque a et b sont inversibles, c'est valable pour tout $n, m \in \mathbb{Z}$.

3.4 Les sous-anneaux

Définition. Soit $(A, +, .)$ un anneau et $B \subset A$. B est un sous-anneau de A si et seulement si, en le munissant des restrictions sur B^2 des lois "+" et ".", B est un anneau possédant les mêmes éléments neutres que ceux de A.

Propriété. B est un sous-anneau de A ssi $1_A \in B$, et $\forall (x, y) \in B^2$, $x - y \in B$ et $xy \in B$.

Propriété. Si A est un anneau, son plus petit sous-anneau est $\mathbb{Z}.1_A = \{n.1_A / n \in \mathbb{Z}\}$.

3.5 Les corps

Propriété. L'ensemble $U(A)$ des éléments inversibles d'un anneau A est un groupe multiplicatif.

Définition. Un anneau A est un ***corps*** si et seulement si
- A n'est pas réduit à $\{0_A\}$,
- A est commutatif,
- et tout élément de A différent de 0_A est inversible.

Définition. Soit $(\mathbb{K}, +, .)$ un corps et $\mathbb{L} \subset \mathbb{K}$. $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ si et seulement si, en le munissant des restrictions sur $\mathbb{L}^2$ des lois "+" et ".", $\mathbb{L}$ est un corps possédant les mêmes éléments neutres que ceux de $\mathbb{K}$.

Propriété. $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ ssi c'est un sous-anneau de $\mathbb{K}$ tel que : $\forall x \in \mathbb{L} \setminus \{0\}$ $x^{-1} \in \mathbb{L}$.

3.6 Formules

Notation. On fixe un anneau $(A, +, .)$.

Formule du *binôme de Newton*. Si $a, b \in A$ avec $ab = ba$, alors $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.

Formule du *multinôme* (hors programme) : Soit $b_1, \ldots, b_p$ des éléments de A qui commutent deux à deux. Alors, pour tout $n \in \mathbb{N}$, $(b_1 + \cdots + b_p)^n = \sum_{\alpha_1 + \cdots + \alpha_p = n} \frac{n!}{\alpha_1! \cdots \alpha_p!} b_1^{\alpha_1} \cdots b_p^{\alpha_p}$.

Formule de Bernoulli : Si $a, b \in A$ avec $ab = ba$, alors $a^{n+1} - b^{n+1} = (a-b) \sum_{k=0}^{n} a^k b^{n-k}$.

Sommes partielles d'une série géométrique.
Si $x \in A$ et $m, n \in \mathbb{N}$ avec $m \leq n$, $(1_A - x). \sum_{i=m}^{n} x^i = x^m - x^{n+1}$.

3.7 Anneaux intègres

Définition. Soit A un anneau.
$a \in A \setminus \{0\}$ est un diviseur à gauche de 0 si et seulement s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$.
C'est un diviseur à droite de 0 si et seulement s'il existe $b \in A \setminus \{0\}$ tel que $ba = 0$.

Définition. Un anneau A est intègre si et seulement si il est commutatif et non nul et s'il n'admet aucun diviseur de 0, ni à gauche ni à droite, c'est-à-dire si et seulement si, pour tout $a, b \in A$, $ab = 0 \Longrightarrow (a = 0) \vee (b = 0)$.

Propriété. Un corps est en particulier un anneau intègre.

3.8 Morphismes d'anneaux

Définition. Soient $(A, +_A, .{}_A)$ et $(B, +_B, .{}_B)$ deux anneaux.
Une application $f : A \longrightarrow B$ est un ***morphisme d'anneaux*** si et seulement si

- $f(1_A) = 1_B$,
- $\forall (x, y) \in A^2 \;\; f(x +_A y) = f(x) +_B f(y)$,
- $\forall (x, y) \in A^2 \;\; f(x._A y) = f(x)._B f(y)$.

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

Remarque. Lorsque f est un morphisme d'anneaux, c'est un morphisme de groupes, d'où $Im(f)$ et $Ker(f) = f^{-1}(\{0\})$.