Résumé de cours :
Semaine 12, du 06 décembre au 10.

1 La structure de groupe

1.1 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 $x_1, \ldots, x_n \in G$, $\varphi\Big(\prod_{i=1}^{n} x_i\Big) = \prod_{i=1}^{n} \varphi(x_i)$.
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 $x_1, \ldots, x_n \in G$, $\varphi\Big(\sum_{i=1}^{n} x_i\Big) = \sum_{i=1}^{n} \varphi(x_i)$.
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.

1.2 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 $\ldots a_k$ 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.

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

2 La structure d'anneau

2.1 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.

2.2 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 $(a_1,\dots,a_n)\in A^n$ et $(b_1,\dots,b_p)\in A^p$ $\left(\sum_{i=1}^{n}a_i\right).\left(\sum_{i=1}^{p}b_i\right)=\sum_{\substack{1\leq i\leq n\\1\leq j\leq p}}a_i.b_j$.

2.3 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 $n, m \in \mathbb{Z}$.

2.4 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 $\mathbb{Z}.1_A = \{n.1_A / n \in \mathbb{Z}\}$.

2.5 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 : $\forall x \in \mathbb{L} \setminus \{0\}$ $x^{-1} \in \mathbb{L}$.

2.6 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 $m \leq n$, $(1_A - x).\sum_{i=m}^{n} x^i = x^m - x^{n+1}$.

2.7 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 $ba = 0$.

Propriété. Un élément non nul d'un anneau est régulier à gauche si et seulement si ce n'est pas un diviseur à gauche de 0. Idem à droite.

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.

2.8 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 $Ker(f) = f^{-1}(\{0\})$.

Propriété. Soient A et B deux anneaux et f un morphisme d'anneaux de A dans B.
Pour tout $a \in A$, $p \in \mathbb{N}$ et $n \in \mathbb{Z}$, $f(na) = nf(a)$, $f(a^p) = f(a)^p$.
Si a est inversible, alors $f(a)$ est inversible et $f(a^n) = f(a)^n$. En particulier, $f(a^{-1}) = f(a)^{-1}$.

Propriété. La composée de deux morphismes d'anneaux est un morphisme d'anneaux.

Propriété. Si f est un isomorphisme d'anneaux, f^{-1} est encore un isomorphisme d'anneaux.

Propriété. Soient $(A, +_A, .{}_A)$ et $(B, +_B, .{}_B)$ deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux.
L'image directe par f de tout sous-anneau de A est un sous-anneau de B.
L'image réciproque selon f de tout sous-anneau de B est un sous-anneau de A.

Définition. Soit $\mathbb{K}$ et $\mathbb{L}$ deux corps et f une application de $\mathbb{K}$ dans $\mathbb{L}$. On dit que f est un morphisme de corps si et seulement si c'est un morphisme d'anneaux.

Propriété. (hors programme) Un morphisme de corps est toujours injectif.
Il faut savoir le démontrer.

Propriété. Soit $f : \mathbb{K} \longrightarrow \mathbb{L}$ un morphisme de corps.
Si $\mathbb{K}'$ est un sous-corps de $\mathbb{K}$, alors $f(\mathbb{K}')$ est un sous-corps de $\mathbb{L}$.
Si $\mathbb{L}'$ est un sous-corps de $\mathbb{L}$, alors $f^{-1}(\mathbb{L}')$ est un sous-corps de $\mathbb{K}$.

2.9 Les anneaux produits

Définition. Soient $n \in \mathbb{N}^*$ et $((A_i, +, .))_{i\in\{1,\dots,n\}}$ une famille de n anneaux.
L'anneau produit de cette famille est $(A, +, .)$, où $A = A_1 \times \cdots \times A_n$ et où les lois "+" et "." sont définies par : pour tout $x = (x_1, \dots, x_n) \in A$ et $y = (y_1, \dots, y_n) \in A$,
$\boxed{x + y = (x_1 + y_1, \dots, x_n + y_n) \text{ et } x.y = (x_1.y_1, \dots, x_n.y_n).}$

Définition. Pour tout $i \in \mathbb{N}_n$, la $i^{\text{ème}}$ projection, $p_i : \begin{array}{ccc} A & \longrightarrow & A_i \\ (a_1, \dots, a_n) & \longmapsto & a_i \end{array}$ est un morphisme surjectif d'anneaux.

2.10 Les idéaux

Définition. Une partie I d'un anneau A est un ***idéal*** de A à gauche (resp : à droite) si et seulement si $I \neq \emptyset$, $\forall (x, y) \in I^2$, $x + y \in I$ et $\forall (x, y) \in \boxed{A \times I,}$ $x.y \in I$ (resp : $y.x \in I$).
On dit qu'un idéal est absorbant pour le produit.
Lorsque I est un idéal à gauche et à droite, on dit que c'est un idéal bilatère.

Notation. Pour la suite, on fixe un anneau $(A, +, .)$ **que l'on suppose commutatif**.

Propriété. Tout idéal est un groupe pour la loi "+".

Propriété. Soit A un anneau commutatif et I un idéal de A. Alors $\boxed{1 \in I \iff I = A}$.

Propriété. Une intersection d'idéaux de A est un idéal de A.
Il faut savoir le démontrer.

Définition. Soit B une partie de A. L'idéal engendré par B est l'intersection des idéaux de A contenant B. C'est le plus petit idéal (au sens de l'inclusion) contenant B. On le note $Id(B)$.

Propriété. Soient B et C deux parties de A telles que $C \subset B$. Alors $Id(C) \subset Id(B)$.

Propriété. Si B est une partie de A, $Id(B) = \{\sum_{i=1}^{n} a_i b_i / n \in \mathbb{N}, (a_1, \dots, a_n) \in A^n, (b_1, \dots, b_n) \in B^n\}$.
Il faut savoir le démontrer.

Définition. Un idéal I de A est principal si et seulement si il existe $b \in A$ tel que $I = Id(b)$.

Définition. Un anneau est principal si et seulement si c'est un anneau commutatif, intègre et dont tous les idéaux sont principaux.

Théorème. $\mathbb{Z}$ est un anneau principal.

Propriété. Soit I et J deux idéaux de A. Alors $I + J$ est un idéal de A.

Propriété. Soient A et B deux anneaux commutatifs et $f : A \longrightarrow B$ un morphisme d'anneaux.
$Ker(f)$ est un idéal de A et si I est un idéal de B, $f^{-1}(I)$ est un idéal de A contenant $Ker(f)$.
Il faut savoir le démontrer.