Toutes les définitions /énoncés du cours sont à connaître précisément.

GROUPES ET ANNEAUX

1 Lois de composition internes

- Loi de composition interne
- Associativité, commutativité
- Loi produit sur $E \times F$
- Elément neutre
- Eléments inversibles (et propriétés dans le cas d'une loi associative)

2 Groupes

2.1 Généralités

Définition

Soit G un ensemble muni d'une loi de composition interne $\star$.
On dit que $(G,\star)$ est un groupe si :
i) $\star$ est associative ;
ii) $(G,\star)$ possède un élément neutre ;
iii) Tout élément de G est inversible.
Si de plus, $\star$ est commutative, on dit que G est commutatif.

- **Remarque.** Si $(G,\star)$ et $(G',\cdot)$ sont des groupes, alors $G \times G'$ est un groupe pour la loi produit.

Définition

Soit E un ensemble non vide. Une *permutation* de E est une bijection de E sur E
- L'ensemble des permutations de E est noté S_E.
- $(S_E, \circ)$ est un groupe, d'élément neutre Id_E.

2.2 Sous-groupes

- **Cadre.** • $(G,\star)$ est un groupe • H est une partie de G.

Définition

On dit que H est un sous-groupe de G si :
i) H est non vide
ii) H est stable par $\star$: $\forall x, y \in H, \quad x \star y \in H$;
iii) H est stable par passage à l'inverse : $\forall x \in H, \quad x^{-1} \in H$.

- **Remarque.** On note e l'élément neutre de G. Si H un sous-groupe de G : $e \in H$.

Théorème

Si H est un sous-groupe de G, alors $(H,\star)$ est un groupe.

En pratique : pour montrer que G est groupe

On peut montrer que G est un sous-groupe d'un groupe de référence.

Exemple 1 — $(\mathbb{U}, \times)$ est un groupe et $\mathbb{U}_n$ en est un sous groupe pour tout $n \in \mathbb{N}^*$.

2.3 Morphismes de groupes

- **Cadre.** • $(G,\cdot)$ est un groupe d'élément neutre e.
  • $(G',\star)$ est un groupe d'élément neutre e'.

Définition

Une application $f : G \to G'$ est un *morphisme de groupes* si :
$$\forall x, y \in G, \qquad f(x \cdot y) = f(x) \star f(y)$$

- **Vocabulaire.** On appelle *isomorphisme* de G sur G' tout morphisme de groupe bijectif de G sur G'.
- **Remarque.** Si $f : G \to G'$ est un morphisme de groupe :
  • $f(e) = e'$ • $\forall x \in G, \quad f(x^{-1}) = f(x)^{-1}$

Définition

Soit $f : G \to G'$ un morphisme de groupe.
- Le *noyau* de f, noté $\mathrm{Ker}\, f$, est le sous-groupe de G :
$$\mathrm{Ker}\, f = \{x \in G \mid f(x) = e'\} = f^{-1}\left(\{e'\}\right)$$
- L'*image* de f, notée $\mathrm{Im}\, f$, est le sous-groupe de G' : $\mathrm{Im}\, f = f(G) = \{f(x)\,;\, x \in G\}$.

Théorème

Soit $f : G \to G'$ un morphisme de groupe.
- f est injectif ssi : $\mathrm{Ker}\, f = \{e\}$ • f est surjectif ssi : $\mathrm{Im}\, f = G'$.

3 Anneaux

3.1 Généralités

Définition

Soit A un ensemble muni de deux lois de compositions internes $+$ et $\times$.
On dit que $(A,+,\times)$ est un *anneau* si :

i) $(A,+)$ est un groupe commutatif, d'élément neutre noté 0_A.
ii) La loi $\times$: • est associative • possède un élément neutre noté 1_A.
iii) $\times$ est distributive sur $+$.

Si de plus, $\times$ est commutative, on dit que l'anneau est *commutatif*.

Définition

Un *corps* est un anneau commutatif, non réduit à $\{0\}$ et dans lequel tout élément autre que 0 est inversible.

Théorème : Règles de calcul

Soit $(A,+,\times)$ un anneau et soient $a,b \in A$. Si $a\times b = b\times a$ alors, pour tout $n \in \mathbb{N}$:

- $\boxed{a^n - b^n = \sum_{k=0}^{n-1} a^k \times b^{n-1-k}.}$
- $\boxed{(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k}}$

Définition

Soit $(A,+,\times)$ un anneau. On note $U(A)$ l'ensemble des éléments de A inversibles pour $\times$. $(U(A),\times)$ est un groupe.

3.2 Sous-anneaux

- **Cadre.** • $(A,+,\times)$ est un anneau. • B est une partie de A.

Définition

On dit que B est un *sous-anneau* de A si :

i) $1_A \in B$
ii) B est un sous-groupe de $(A,+)$.
iii) B stable par $\times$: $\forall x,y \in B,\quad x\times y \in B$

3.3 Morphisme d'anneaux

- **Cadre.** $(A,+,\cdot)$ et $(B,+,\times)$ sont des anneaux [1]

Définition

Une application $f : A \to B$ est un *morphisme d'anneaux* si :

i) $f(1_A) = 1_B$ *ii)* $\forall x,y \in A,\ f(x+y) = f(x)+f(y)$ *iii)* $\forall x,y \in A,\ f(x\cdot y) = f(x)\times f(y)$

- **Remarque.** Si $f : A \to B$ est un morphisme d'anneau, alors f est un morphisme de groupes entre $(A,+)$ et $(B,+)$. En particulier : $\boxed{f \text{ est injectif ssi } \operatorname{Ker} f = \{0_A\}}$.
- **Vocabulaire.** Un *isomorphisme d'anneaux* est un morphisme d'anneau bijectif.

3.4 Anneaux intègres

Définition

Un anneau commutatif, non nul $(A,+,\times)$ est *intègre* si pour tous $x,y \in A$:

$$x\times y = 0 \implies x = 0 \quad \text{ou} \quad y = 0$$

- **Remarque.** Dans un anneau intègre il est licite de *simplifier* une égalité par un élément *non nul* : si $x \neq 0_A$, l'égalité : $x\times y = x\times z$ impose : $y = z$

L'adresse de la page des maths est : `https://mathieucathala.fr`

1. on note abusivement par le même symbole les additions de A et B