

Résumé de cours :
Semaine 13, du 11 décembre au 15 décembre.

Groupes et anneaux (fin)

1 Morphismes d'anneaux (fin)

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 $(A, +_A, \cdot_A)$ et $(B, +_B, \cdot_B)$ deux anneaux et $f : A \rightarrow B$ 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 $f : \mathbb{K} \rightarrow \mathbb{L}$ 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 Les anneaux produits

Définition. Soient $n \in \mathbb{N}^*$ et $((A_i, +, \cdot))_{i \in \{1, \dots, n\}}$ une famille de n anneaux.

L'anneau produit de cette famille est $(A, +, \cdot)$, où $A = A_1 \times \dots \times A_n$ et où les lois "+" et "." sont définies par : pour tout $x = (x_1, \dots, x_n) \in A$ et $y = (y_1, \dots, y_n) \in A$,

$$x + y = (x_1 + y_1, \dots, x_n + y_n) \text{ et } x \cdot y = (x_1 \cdot y_1, \dots, x_n \cdot y_n).$$

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.

3 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 $(A, +, \cdot)$ **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 , $Id(B) = \left\{ \sum_{i=1}^n a_i b_i / n \in \mathbb{N}, (a_1, \dots, a_n) \in A^n, (b_1, \dots, b_n) \in B^n \right\}$.

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 $f : A \rightarrow B$ 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.

4 $\mathbb{Z}/n\mathbb{Z}$

4.1 Groupes quotients (suite et fin)

Théorème. Soit $(G, +)$ un groupe **commutatif** et H un sous-groupe de G . Pour tout $x, y \in G$, on convient que $xR_H y \iff y - x \in H$. Alors R_H est une relation d'équivalence. On note G/H l'ensemble de ses classes d'équivalence.

En posant, pour tout $x, y \in G$, $\bar{x} + \bar{y} \triangleq \overline{x + y}$, on définit une loi "+" sur G/H pour laquelle G/H

est un groupe commutatif. De plus, $\begin{matrix} G & \longrightarrow & G/H \\ x & \longmapsto & \bar{x} \end{matrix}$ 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 $a, b \in \mathbb{Z}$, $\bar{a} = \bar{b} \iff a \equiv b [n]$,
- Pour $a, b \in \mathbb{Z}$, $\overline{a + nb} = \bar{a}$,
- $\bar{0} = 0_{\mathbb{Z}/n\mathbb{Z}}$,
- pour tout $k \in \mathbb{Z}$, $-\bar{k} = \overline{-k}$,
- pour tout $h, k \in \mathbb{Z}$, $\overline{h + k} = \bar{h} + \bar{k}$,

— pour tout $h, k \in \mathbb{Z}$, $h\bar{k} = \overline{hk}$.

Propriété. Si $n = 0$, $\mathbb{Z}/n\mathbb{Z}$ est monogène non cyclique. Il est isomorphe à \mathbb{Z} .

Tout groupe monogène non cyclique est isomorphe à \mathbb{Z} .

Propriété. Si $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique de cardinal n : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$.

Si $G = Gr(a)$ est un autre groupe cyclique de cardinal n , il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (G, \cdot) \\ \bar{k} & \longmapsto & a^k \end{array} \text{ est un isomorphisme.}$$

Il faut savoir le démontrer.

4.2 Anneaux quotients

Notation. On fixe un anneau commutatif $(A, +, \cdot)$ et un idéal I de A .

Propriété. $(A/I, +, \cdot)$ est un anneau commutatif en posant, pour tout $x, y \in A$ $\overline{x \cdot y} = \bar{x} \cdot \bar{y}$.

Propriété. Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, on dispose des règles supplémentaires de calculs suivantes :

— Pour tout $h, k \in \mathbb{Z}$, $h\bar{k} = \overline{hk}$.

— $\bar{1} = 1_{\mathbb{Z}/n\mathbb{Z}}$.

4.3 Propriétés spécifiques de $\mathbb{Z}/n\mathbb{Z}$

Notation. On fixe $n \in \mathbb{N}$ avec $n \geq 2$.

Propriété. (hors programme)

Les sous-groupes (resp : les idéaux) de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k} \cdot \mathbb{Z}/n\mathbb{Z}$, où k est un diviseur de n .

Théorème. Soit $k \in \mathbb{Z}$. \bar{k} engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ (resp : est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$) ssi $k \wedge n = 1$. Dans ce cas, il existe $u, v \in \mathbb{Z}$ tels que $uk + vn = 1$ et $\bar{u} = \bar{k}^{-1}$.

Il faut savoir le démontrer.

Théorème. Soit $n \geq 2$. $\mathbb{Z}/n\mathbb{Z}$ est un corps (resp : est intègre) si et seulement si $n \in \mathbb{P}$.

Il faut savoir le démontrer.

Notation. Lorsque $p \in \mathbb{P}$, le corps $\mathbb{Z}/p\mathbb{Z}$ est souvent noté \mathbb{F}_p .

4.4 Théorème chinois

Théorème des restes chinois : Si a et b sont deux entiers supérieurs à 2 et **premiers entre eux**,

$$f : \mathbb{Z}/ab\mathbb{Z} \longrightarrow (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}) \text{ est un isomorphisme d'anneaux.}$$

$$\bar{k} \longmapsto (\bar{k}, \bar{k})$$

Il faut savoir le démontrer, en incluant la preuve constructive de la surjectivité : pour $h, k \in \mathbb{Z}$, comment déterminer $\ell \in \mathbb{Z}$ tel que $\ell \equiv h [a]$ et $\ell \equiv k [b]$?

Théorème chinois (généralisation) : Soit $n \geq 2$ et a_1, \dots, a_n n entiers supérieurs à 2 et **deux à deux premiers entre eux** :

$$\mathbb{Z}/(a_1 \times \dots \times a_n)\mathbb{Z} \longrightarrow (\mathbb{Z}/a_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/a_n\mathbb{Z}) \text{ est un isomorphisme d'anneaux.}$$

$$\bar{k} \longmapsto (\bar{k}, \dots, \bar{k})$$

Remarque. pour $h_1, \dots, h_n \in \mathbb{Z}$, on peut calculer $\ell \in \mathbb{Z}$ tel que, pour tout $i \in \{1, \dots, n\}$, $\ell \equiv h_i [a_i]$.

À connaître.

4.5 L'indicatrice d'Euler

Définition. Pour tout $n \in \mathbb{N}^*$, on pose $\varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$.

Remarque. $\varphi(1) = 1$, car $\mathbb{Z}/1\mathbb{Z}$ est l'anneau nul, pour lequel 0 est inversible.

Pour $n \geq 2$, $\varphi(n) = \#\{k \in \{1, \dots, n-1\} / k \wedge n = 1\}$.

Propriété. $\varphi(1) = 1$ et si p est un nombre premier, alors $\varphi(p) = p - 1$.

Propriété. Si p est premier et si $k \in \mathbb{N}^*$, alors $\varphi(p^k) = p^k - p^{k-1}$.

Il faut savoir le démontrer.

Propriété. Soit a et b sont deux entiers supérieurs à 2. Si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$.

Il faut savoir le démontrer.

Corollaire. Soit $n \in \mathbb{N}$ avec $n \geq 2$, de décomposition primaire $n = \prod_{i=1}^k p_i^{m_i}$.

Alors $\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$.

Propriété. (hors programme) $\forall n \in \mathbb{N}^*$, $n = \sum_{d|n} \varphi(d)$.

Il faut savoir le démontrer.

Propriété d'Euler-Fermat : Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $k \in \mathbb{Z}$. Si $k \wedge n = 1$, alors $k^{\varphi(n)} \equiv 1 [n]$.

Il faut savoir le démontrer.

Petit théorème de Fermat : Si p est un nombre premier, alors pour tout $k \in \mathbb{Z}$, $k^p \equiv k [p]$.

5 Caractéristique d'un anneau

Notation. A désigne un anneau commutatif.

Définition. S'il existe $n \in \mathbb{N}^*$ tel que $n \cdot 1_A = 0_A$, la caractéristique de A est

$\text{car}(A) \triangleq \min\{n \in \mathbb{N}^* / n \cdot 1_A = 0_A\}$. Sinon, on convient que $\text{car}(A) = 0$.

Propriété. Soit A un anneau de caractéristique n : pour tout $m \in \mathbb{Z}$, $m \cdot 1_A = 0_A \iff n|m$.

Exemples. L'anneau nul est l'unique anneau de caractéristique 1, $\text{car}(\mathbb{Z}/n\mathbb{Z}) = n$, $\text{car}(\mathbb{R}) = 0$.

Propriété. Deux anneaux isomorphes ont la même caractéristique.

Propriété. $\mathbb{Z} \cdot 1_A$, le plus petit sous-anneau de A , est isomorphe à \mathbb{Z} lorsque $\text{car}(A) = 0$ et à $\mathbb{Z}/n\mathbb{Z}$ lorsque $\text{car}(A) = n \in \mathbb{N}^*$.

Il faut savoir le démontrer.

Corollaire. Un anneau de caractéristique nulle est de cardinal infini, la réciproque étant fausse.

Propriété. Si A est intègre et $\text{car}(A) \neq 0$, alors $\text{car}(A) \in \mathbb{P}$.

Il faut savoir le démontrer.

Propriété. Si $\text{car}(A) = p \in \mathbb{P}$, alors $x \mapsto x^p$ est un endomorphisme sur A , dit de Frobenius.

Il faut savoir le démontrer.

Propriété. La caractéristique d'un corps est ou bien nulle, ou bien un nombre premier.

Propriété. On appelle sous-corps premier d'un corps \mathbb{K} le plus petit sous-corps de \mathbb{K} .

— Si $\text{car}(\mathbb{K}) = p \in \mathbb{P}$, le sous-corps premier de \mathbb{K} est $\mathbb{Z} \cdot 1_{\mathbb{K}}$, il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

- Si $\text{car}(\mathbb{K}) = 0$, le sous-corps premier de \mathbb{K} est $\{(p \cdot 1_{\mathbb{K}})(q \cdot 1_{\mathbb{K}})^{-1} \mid p \in \mathbb{Z}, q \in \mathbb{N}^*\}$. Il est isomorphe à \mathbb{Q} . En particulier, \mathbb{K} est de cardinal infini.

Propriété. Si \mathbb{K} est un corps fini de caractéristique p , l'endomorphisme de Frobenius $x \mapsto x^p$ sur \mathbb{K} est un automorphisme de corps. Lorsque $\mathbb{K} = \mathbb{F}_p$, c'est l'identité.

Les espaces vectoriels (début)

Notation. \mathbb{K} désigne un corps quelconque.

Notation. Symbole de Kronecker : $\delta_{i,j} = 0$ lorsque $i \neq j$ et $\delta_{i,i} = 1$ lorsque $i = j$.

6 La structure algébrique d'espace vectoriel

6.1 Définition et exemples

Définition.

Un \mathbb{K} -espace vectoriel est un triplet $(E, +, \cdot)$, où $(E, +)$ est un groupe abélien et “ \cdot ” est une application

$$\mathbb{K} \times E \longrightarrow E$$

tel que, pour tout $x, y \in E$ et $\alpha, \beta \in \mathbb{K}$,

- $\alpha \cdot (x + y) = (\alpha \cdot x) + (\alpha \cdot y)$,
- $(\alpha + \beta) \cdot x = (\alpha \cdot x) + (\beta \cdot x)$,
- $(\alpha \times \beta) \cdot x = \alpha \cdot (\beta \cdot x)$,
- $1_{\mathbb{K}} \cdot x = x$.

Remarque. Lorsque E est un \mathbb{K} -espace vectoriel, ses éléments seront appelés des vecteurs et les éléments de \mathbb{K} seront appelés des scalaires.

Exemples.

◇ Soient E un \mathbb{K} -espace vectoriel et I un ensemble quelconque. Alors l'ensemble E^I des familles $(x_i)_{i \in I}$ d'éléments de E indexées par I est un \mathbb{K} -espace vectoriel si l'on convient que

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I} \text{ et, pour tout } \alpha \in \mathbb{K}, \alpha \cdot (x_i)_{i \in I} = (\alpha \cdot x_i)_{i \in I}.$$

De même, l'ensemble $\mathcal{F}(I, E)$ des applications de I dans E est un \mathbb{K} -espace vectoriel si l'on convient que, pour tout $f, g \in \mathcal{F}(I, E)$ et $\alpha \in \mathbb{K}$, pour tout $x \in I$,

$$(f + g)(x) \triangleq f(x) + g(x) \text{ et } (\alpha \cdot f)(x) \triangleq \alpha \cdot (f(x)).$$

- ◇ En particulier, pour tout $n \in \mathbb{N}^*$, \mathbb{R}^n est un \mathbb{R} -espace vectoriel.
- ◇ Si \mathbb{L} est un sous-corps de \mathbb{K} , alors \mathbb{K} est un \mathbb{L} -espace vectoriel.
- ◇ L'ensemble $\mathbb{K}^{\mathbb{N}}$ des suites de scalaires est un \mathbb{K} -espace vectoriel.
- ◇ $\mathbb{K}[X]$ est un \mathbb{K} -espace vectoriel.

Propriété. Soit E un \mathbb{K} -espace vectoriel. Soit $x, y \in E$ et $\lambda, \mu \in \mathbb{K}$:

- $0_{\mathbb{K}} \cdot x = 0_E$ et $\lambda \cdot 0_E = 0_E$;
- $(-1_{\mathbb{K}}) \cdot x = -x$;
- $(\lambda - \mu)x = \lambda \cdot x - \mu \cdot x$;
- $\lambda x = 0 \iff (\lambda = 0) \vee (x = 0)$;
- $(\lambda x = \lambda y) \wedge (\lambda \neq 0) \implies x = y$;
- $(\lambda x = \mu x) \wedge (x \neq 0) \implies \lambda = \mu$.

Définition. Soient $n \in \mathbb{N}^*$ et $((E_i, +, \cdot))_{i \in \{1, \dots, n\}}$ une famille de n \mathbb{K} -espaces vectoriels.

On structure $E = E_1 \times \dots \times E_n$ en un \mathbb{K} -espace vectoriel en convenant que

- $\forall x = (x_1, \dots, x_n) \in E, \forall y = (y_1, \dots, y_n) \in E, x + y = (x_1 + y_1, \dots, x_n + y_n)$,
- $\forall \alpha \in \mathbb{K}, \forall x = (x_1, \dots, x_n) \in E, \alpha \cdot x = (\alpha \cdot x_1, \dots, \alpha \cdot x_n)$.

6.2 Sous-espaces vectoriels

Propriété et définition : Soit E un \mathbb{K} -espace vectoriel et F une partie de E .

F est un *sous-espace vectoriel* de E si et seulement si

- $F \neq \emptyset$;
- $\forall (x, y) \in F^2$, $x + y \in F$ (stabilité de la somme de deux vecteurs);
- $\forall (\alpha, x) \in \mathbb{K} \times F$, $\alpha \cdot x \in F$ (stabilité du produit externe).

Cet ensemble de conditions est équivalent à

- $F \neq \emptyset$;
- $\forall (\alpha, x, y) \in \mathbb{K} \times F \times F$, $\alpha \cdot x + y \in F$ (stabilité par combinaison linéaire).

Exemples.

- Pour tout $n \in \mathbb{N}^*$, pour tout $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n \setminus \{0\}$, $\left\{ (x_i)_{1 \leq i \leq n} / \sum_{i=1}^n \alpha_i x_i = 0 \right\}$ est un sous-espace vectoriel de \mathbb{K}^n .
- $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$, pour tout $n \in \mathbb{N}$.
- L'ensemble $C^p([0, 1], \mathbb{C})$ des applications de classe C^p de $[0, 1]$ dans \mathbb{C} , où $p \in \mathbb{N}$, est un sous-espace vectoriel de $\mathcal{F}([0, 1], \mathbb{C})$.
- L'ensemble $l^1(\mathbb{C}) = \{(a_n)_{n \in \mathbb{N}} / \sum a_n \text{ ACV}\}$ est un sous-espace vectoriel de $\mathbb{C}^{\mathbb{N}}$.
Il faut savoir le démontrer.