Résumé de cours :
Semaine 13, du 13 décembre au 17.

Groupes et anneaux (fin)

1 $\mathbb{Z}/n\mathbb{Z}$

1.1 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 $xR_Hy \Longleftrightarrow y-x \in H$. Alors R_H est une relation d'équivalence. On note G/H l'ensemble de ses classes d'équivalence.
En posant, pour tout $x,y \in G$, $\overline{x}+\overline{y} \stackrel{\Delta}{=} \overline{x+y}$, 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 $a,b \in \mathbb{Z}$, $\overline{a}=\overline{b} \Longleftrightarrow a \equiv b\ [n]$,
- 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 $h,k \in \mathbb{Z}$, $h\overline{k}=\overline{hk}$.

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 : $\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\overline{1},\overline{2},\dots,\overline{n-1}\}$.
Si $G=Gr(a)$ est un autre groupe cyclique de cardinal n, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$:
$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (G,.) \\ \overline{k} & \longmapsto & a^k \end{array}$ est un isomorphisme.
Il faut savoir le démontrer.

1.2 Anneaux quotients

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

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

Propriété. Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, on dispose des régles supplémentaires de calculs suivantes :
- Pour tout $h,k \in \mathbb{Z}$, $\overline{hk}=\overline{h}.\overline{k}$.
- $\overline{1}=1_{\mathbb{Z}/n\mathbb{Z}}$.

1.3 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 $\overline{k}.\mathbb{Z}/n\mathbb{Z}$, où k est un diviseur de n.

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

1.4 Théorème chinois

Théorème des restes chinois : Si a et b sont deux entiers supérieurs à 2 et **premiers entre eux**,
$\begin{array}{rccc} f: & \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}) \\ & \overline{k} & \longmapsto & (\overline{k}, \overline{k}) \end{array}$ est un isomorphisme d'anneaux.
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 $a_1, \ldots, a_n$ n entiers supérieurs à 2 et **deux à deux premiers entre eux** :
$\begin{array}{ccc} \mathbb{Z}/(a_1 \times \cdots \times a_n)\mathbb{Z} & \longrightarrow & (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z}) \\ \overline{k} & \longmapsto & (\overline{k}, \ldots, \overline{k}) \end{array}$ est un isomorphisme d'anneaux.

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

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

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

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

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 $k \in \mathbb{Z}$, $k^p \equiv k\ [p]$.

2 Caractéristique d'un anneau

Notation. A désigne un anneau commutatif.

Définition. S'il existe $n \in \mathbb{N}^*$ tel que $n.1_A = 0_A$, la caractéristique de A est $\text{car}(A) \stackrel{\Delta}{=} \min\{n \in \mathbb{N}^* \ / \ n.1_A = 0_A\}$. Sinon, on convient que $\text{car}(A) = 0$.

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

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. $\mathbb{Z}.1_A$, 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 $x \longmapsto x^p$ 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 $\mathbb{Z}.1_{\mathbb{K}}$, il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- Si $\text{car}(\mathbb{K}) = 0$, le sous-corps premier de $\mathbb{K}$ est $\{(p.1_{\mathbb{K}})(q.1_{\mathbb{K}})^{-1} \ / \ p \in \mathbb{Z}, q \in \mathbb{N}^*\}$. 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 $x \longmapsto x^p$ 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 $i = j$.

3 La structure algébrique d'espace vectoriel

3.1 Définition et exemples

Définition.
Un $\mathbb{K}$-espace vectoriel est un triplet $(E, +, .)$, où $(E, +)$ est un groupe abélien et "." est une application $\begin{array}{ccc} \mathbb{K} \times E & \longrightarrow & E \\ (\alpha, x) & \longmapsto & \alpha.x \end{array}$ tel que, pour tout $x, y \in E$ et $\alpha, \beta \in \mathbb{K}$,
- $\alpha.(x + y) = (\alpha.x) + (\alpha.y)$,
- $(\alpha + \beta).x = (\alpha.x) + (\beta.x)$,
- $(\alpha \times \beta).x = \alpha.(\beta.x)$,
- $1_{\mathbb{K}}.x = x$.

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.
$\diamond$ 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
$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I}$ et, pour tout $\alpha \in \mathbb{K}$, $\alpha.(x_i)_{i\in I} = (\alpha.x_i)_{i\in I}$.
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 $\alpha \in K$, pour tout $x \in I$,
$(f + g)(x) \stackrel{\Delta}{=} f(x) + g(x)$ et $(\alpha.f)(x) \stackrel{\Delta}{=} a.(f(x))$.
$\diamond$ En particulier, pour tout $n \in \mathbb{N}^*$, $\mathbb{R}^n$ est un $\mathbb{R}$-espace vectoriel.
$\diamond$ Si $\mathbb{L}$ est un sous-corps de $\mathbb{K}$, alors $\mathbb{K}$ est un $\mathbb{L}$-espace vectoriel.
$\diamond$ L'ensemble $\mathbb{K}^{\mathbb{N}}$ des suites de scalaires est un $\mathbb{K}$-espace vectoriel.
$\diamond$ $\mathbb{K}[X]$ est un $\mathbb{K}$-espace vectoriel.

Propriété. Soit E un $\mathbb{K}$-espace vectoriel. Soit $x, y \in E$ et $\lambda, \mu \in \mathbb{K}$:
- $0_{\mathbb{K}}.x = 0_E$ et $\lambda.0_E = 0_E$;
- $(-1_{\mathbb{K}}).x = -x$;
- $(\lambda - \mu)x = \lambda.x - \mu.x$;
- $\lambda x = 0 \iff (\lambda = 0) \vee (x = 0)$;
- $(\lambda x = \lambda y) \wedge (\lambda \neq 0) \Longrightarrow x = y$;
- $(\lambda x = \mu x) \wedge (x \neq 0) \Longrightarrow \lambda = \mu$.

Définition. Soient $n \in \mathbb{N}^*$ et $((E_i, +, .))_{i\in\{1,\dots,n\}}$ une famille de n $\mathbb{K}$-espaces vectoriels.
On structure $E = E_1 \times \cdots \times E_n$ en un $\mathbb{K}$-espace vectoriel en convenant que
- $\forall x = (x_1, \dots, x_n) \in E,\ \forall y = (y_1, \dots, y_n) \in E,\ x + y = (x_1 + y_1, \dots, x_n + y_n)$,
- $\forall \alpha \in \mathbb{K},\ \forall x = (x_1, \dots, x_n) \in E,\ \alpha.x = (\alpha.x_1, \dots, \alpha.x_n)$.

3.2 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) ;
- $\forall (\alpha, x) \in \mathbb{K} \times F\ ,\ \alpha.x \in F$ (stabilité du produit externe).

Cet ensemble de conditions est équivalent à
- $F \neq \emptyset$;
- $\forall (\alpha, x, y) \in \mathbb{K} \times F \times F\ ,\ \alpha.x + y \in F$ (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 $\mathbb{C}^{\mathbb{N}}$.

Définition. Soient E un $\mathbb{K}$-espace vectoriel et I un ensemble quelconque. Soit $(x_i)_{i\in I}$ une famille de E^I. On dit que c'est une famille presque nulle si et seulement si $\{i \in I/x_i \neq 0\}$ est un ensemble fini. On note $E^{(I)}$ l'ensemble des familles presque nulles de E^I. $E^{(I)}$ est un sous-espace vectoriel de E^I.

3.3 Sous-espace vectoriel engendré par une partie

Propriété. Une intersection d'une famille de sous-espaces vectoriels est un sous-espace vectoriel.
Il faut savoir le démontrer.

Définition. Soit E un $\mathbb{K}$-espace vectoriel et A une partie de E. Notons $\mathcal{S}$ l'ensemble des sous-espaces vectoriels de E contenant A. Alors $\bigcap_{F\in\mathcal{S}} F$ est un sous-espace vectoriel de E contenant A et, par construction, c'est le plus petit sous-espace vectoriel contenant A. On le note $\text{Vect}(A)$.

Exemple. $\text{Vect}(\emptyset) = \{0\}$, puisque $\{0\}$ est le plus petit sous-espace vectoriel de E.
Si F est un sous-espace vectoriel d'un $\mathbb{K}$-espace vectoriel E, $\text{Vect}(F) = F$.

Propriété. Si $A \subset B$, alors $\text{Vect}(A) \subset \text{Vect}(B)$.

Propriété. Soient E un $\mathbb{K}$-espace vectoriel et A une partie de E. Alors $Vect(A)$ est l'ensemble des combinaisons linéaires de vecteurs de A : $\text{Vect}(A) = \left\{\sum_{a\in A} \alpha_a a / (\alpha_a)_{a\in A} \in \mathbb{K}^{(A)}\right\}$.
Il faut savoir le démontrer.

Notation. Si $(x_i)_{i\in I} \in E^I$, on note $\text{Vect}(x_i)_{i\in I} = \text{Vect}(\{x_i \ / \ i \in I\})$.
En particulier, $\text{Vect}(x_1, \ldots, x_n) = \{\sum_{i=1}^{n} \alpha_i x_i \ / \ a_1, \ldots, a_n \in \mathbb{K}\}$.
Si $u \in E \setminus \{0\}$, $\text{Vect}(u) = \{\alpha u / \alpha \in \mathbb{K}\}$ est appelé la droite vectorielle engendrée par le vecteur u.