Résumé de cours :
Semaine 13, du 8 décembre au 12 décembre.

1 La structure d'anneau

1.1 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.

1.2 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 $(b_1, \ldots, b_p) \in A^p$ $\left(\sum_{i=1}^{n} a_i\right) . \left(\sum_{i=1}^{p} b_i\right) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} a_i.b_j$.

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

1.4 Les anneaux produits

Définition. Soient $n \in \mathbb{N}^*$ et $((A_i, +, .))_{i \in \{1,\ldots,n\}}$ 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 $x = (x_1, \ldots, x_n) \in A$ et $y = (y_1, \ldots, y_n) \in A$,
$\boxed{x + y = (x_1 + y_1, \ldots, x_n + y_n) \text{ et } x.y = (x_1.y_1, \ldots, x_n.y_n).}$

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

Propriété. On suppose que $(A, +, \times)$ est un anneau et que B est un ensemble quelconque. A^B est un anneau si l'on convient que, pour tout $f, g \in A^B$, pour tout $b \in B$, $(f + g)(b) = f(b) + g(b)$ et $(f \times g)(b) = f(b) \times g(b)$, ou bien, avec d'autres notations, que pour tout $(a_b)_{b \in B}, (c_b)_{b \in B} \in A^B$, $(a_b)_{b \in B} + (c_b)_{b \in B} = (a_b + c_b)_{b \in B}$ et $(a_b)_{b \in B} \times (c_b)_{b \in B} = (a_b \times c_b)_{b \in B}$.

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

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

1.7 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 $b_1, \dots, b_p$ des éléments de A qui commutent deux à deux. Alors, pour tout $n \in \mathbb{N}$, $(b_1 + \cdots + b_p)^n = \displaystyle\sum_{\alpha_1+\cdots+\alpha_p=n} \frac{n!}{\alpha_1! \cdots \alpha_p!} b_1^{\alpha_1} \cdots b_p^{\alpha_p}$.

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

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

1.8 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.

1.9 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 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 $\boxed{1 \in I \Longleftrightarrow I = A}$.

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.

3 $\mathbb{Z}/n\mathbb{Z}$

3.1 Groupes quotients (suite et fin)

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 $\mathbb{Z}/n\mathbb{Z}$:
$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & (G, .) \\ \overline{k} & \longmapsto & a^k \end{array}$ est un isomorphisme.
Il faut savoir le démontrer.

3.2 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 $h, k \in \mathbb{Z}$, $\overline{hk} = \overline{h}.\overline{k}$.
— $\overline{1} = 1_{\mathbb{Z}/n\mathbb{Z}}$.

3.3 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 $\mathbb{F}_p$.

3.4 Théorème chinois

Théorème des restes chinois : Si a et b sont deux entiers supérieurs à 2 et **premiers entre eux**,
$f : \begin{array}{ccc} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}) \\ \overline{k} & \longmapsto & (\overline{k}, \overline{k}) \end{array}$ 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.

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

4 Caractéristique d'un anneau (début)

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 $m \in \mathbb{Z}$, $m.1_A = 0_A \Longleftrightarrow n|m$.

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.