Semaine du 12/11 au 16/11.

1 Structures algébriques

1.1 Structure d'anneau

- Définition d'un anneau.
- Règles de calcul dans un anneau.
- Exemples. Cas de l'anneau nul.
- Anneau intègre.
- Notations $n.x$ et x^n pour $x \in A$ et $n \in \mathbb{N}$. Extension à $n \in \mathbb{Z}$ lorsque c'est possible.
- Binôme de Newton pour deux éléments qui commutent.
- Formule de Bernoulli pour deux éléments x et y qui commutent et $n \in \mathbb{N}^*$:

$$x^n - y^n = (x-y) \times \left(\sum_{k=0}^{n-1} x^k \times y^{n-1-k} \right) = \left(\sum_{k=0}^{n-1} x^k \times y^{n-1-k} \right) \times (x-y).$$

- Produit cartésien d'anneaux.
- Soient A un anneau et X un ensemble non vide. L'ensemble $\mathcal{F}(X, A)$ possède une structure canonique d'anneau.
- Sous-anneau. Un sous-anneau est un anneau pour les lois induites.
- Morphisme d'anneaux.
- Généralisation des propriétés vues pour les groupes et les morphismes de groupes...
- Groupe des unités d'un anneau $(A, +, \times)$. On le note U ou U_A. Exemple de l'anneau $(\mathbb{Z}, +, \times)$.
- Définition d'un corps gauche, d'un corps.
- Un corps gauche est un anneau intègre. Sous-corps. Sur-corps. Exemples.

2 Arithmétique dans $\mathbb{Z}$

2.1 Divisibilité dans $\mathbb{Z}$

- Division dans $\mathbb{Z}$. L'ensemble des multiples de $a \in Z$ est noté $a\mathbb{Z}$ et l'ensemble des diviseurs est noté $D(a)$.
- Propriétés élémentaires des ensembles $a\mathbb{Z}$ et $D(a)$.
- Propriétés élémentaire de la relation $|$. En particulier, pour $(a, b, d) \in \mathbb{Z}^3$, on a :
  - $a|b$ et $b|a$ ssi $|a| = |b|$.
  - Si $d|a$ et $d|b$ alors $d|(au + bv)$ pour tout couple $(u, v) \in \mathbb{Z}^2$.
  - Si $x \in \mathbb{Z}^*$, $a|b \Leftrightarrow ax|bx$.
- Division euclidienne dans $\mathbb{Z}$.
- Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les parties de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$. Sous cette forme, le n est unique.

2.2 PGCD - PPCM

- Définition du pgcd de a et b dans $\mathbb{Z}$ comme l'unique élément de $n \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$. Notation $a \wedge b$.
- Propriétés élémentaires du pgcd.
- Relation de Bézout.
- On a $D(a) \cap D(b) = D(a \wedge b)$.
- Dans le cas où $(a, b) \neq (0, 0)$, $a \wedge b$ est le plus grand diviseur commun strictement positif de a et$b$.
- Pour $(a, b, k) \in \mathbb{Z}^3$, $(ka) \wedge (kb) = |k|(a \wedge b)$.
- Algorithme d'Euclide. Terminaison et correction. Version itérative et récursive.
- Algorithme d'Euclide étendu. Version récursive et version itérative.
- Définition du ppcm de a et b dans $\mathbb{Z}$ comme l'unique élément de $n \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$. Notation $a \vee b$.

- Propriétés élémentaires du ppcm.
- Dans le cas où $a \neq 0$ et $b \neq 0$, $a \vee b$ est le plus plus petit commun multiple strictement positif de a et$b$.
- Pour $(a, b, k) \in \mathbb{Z}^3$, $(ka) \vee (kb) = |k|(a \vee b)$.

2.3 Entiers premiers entre eux

- Définition.
- Pour $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, on note $\delta = a \wedge b$ et $a = \delta a'$, $b = \delta b'$. Dans ce cas, $a' \wedge b' = 1$.
- Théorème de Bézout.
- Lemme de Gauss.
- $(a \wedge b)(a \vee b) = |ab|$ pour tout $(a, b) \in \mathbb{Z}^2$.
- Représentant irréductible d'un rationnel. Unicité.
- Pour $(a_1, \cdots, a_n) \in \mathbb{Z}^n$ et $(b_1, \cdots, b_m) \in \mathbb{Z}^m$ avec $(m, n) \in {\mathbb{N}^*}^2$, on a

$$\forall (i, j) \in [\![1\,,\, n]\!] \times [\![1\,,\, m]\!]\ a_i \wedge b_j = 1 \quad \text{ssi} \quad \left(\prod_{i=1}^{n} a_i\right) \wedge \left(\prod_{j=1}^{m} b_j\right) = 1$$

- Pour $(a, b, c) \in \mathbb{Z}^2$ avec $a \wedge b = 1$, si $a|c$ et $b|c$ alors $ab|c$. Généralisation au cas de n entiers deux à deux premiers entre eux.
- Résolution générale de l'équation $ax + by = c$ avec $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$ fixé.

3 Prévisions

• Fin du chapitre.