Semaine du 18 novembre : algèbre générale, arithmétique

Partie I - Anneaux

- Définition d'un anneau $(A, +, \times)$, exemples.
- Absorbance de 0 pour la loi $\times$. "Règle des signes" dans un produit.
- Définition d'un anneau intègre, d'un anneau-produit. Groupe des unités.
- Calculs algébriques dans un anneau.
  - Définition de la loi externe $n \cdot x$ ($n \in \mathbb{Z},\ x \in A$), c'est-à-dire de l'itération de la loi $+$. Propriétés usuelles[1].
  - Définition de x^n pour $n \in \mathbb{N}$. Élément nilpotent, indice de nilpotence.
  - Distributivité généralisée : $\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{(i,j)\in[\![1,m]\!]\times[\![1,n]\!]} a_i b_j$.
  - Développement de $(a_1 + \ldots + a_n)^2$. Cas où les a_i commutent deux à deux.
  - Si x et y commutent : formule du binôme, formule de Bernoulli.
- Sous-anneau, condition suffisante. Morphisme d'anneaux.

Partie II - Corps

- Par définition, tous les corps sont non triviaux et commutatifs.
- La construction du corps des fractions d'un anneau intègre a été vue à titre culturel, mais elle ne saurait <u>en aucun cas</u> être exigible.
- Tout corps est un anneau intègre.
- Sous-corps. Sous-corps engendré par une partie. Morphisme de corps.

Partie III - Arithmétique

- Multiple, diviseur. La divisibilité est une relation d'ordre (partielle) sur $\mathbb{N}$.
- Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Réciproquement, tout sous groupe de $(\mathbb{Z}, +)$ s'écrit d'une unique manière $n\mathbb{Z}$ avec $n \in \mathbb{N}$.
- Pour deux entiers $a, b \in \mathbb{Z}^\star$, le pgcd et le ppcm sont définis au choix :

  i) au sens "naïf" :
  $$\begin{cases} a \wedge b = \max\{\delta \in \mathbb{N}^\star \ : \delta | a \text{ et } \delta | b\} \\ a \vee b = \min\{\mu \in \mathbb{N}^\star \ : a | \mu \text{ et } b | \mu\} \end{cases}$$
  le max et le min étant à comprendre au sens de la relation d'ordre $\leq$.

  ii) ou alors par la caractérisation
  $$\begin{cases} a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z} \\ a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z} \end{cases}$$

  On vérifie que ces deux définitions sont équivalentes. La deuxième s'étend naturellement au cas $(a, b) \in \mathbb{Z}^2$.

[1] À l'attention des colleurs : le terme de "$\mathbb{Z}$-algèbre" n'a pas été évoqué, mais c'est précisément de ces propriétés qu'il s'agit.

- d est un diviseur commun de a et b ssi il divise $a \wedge b$. m est un multiple commun de a et b ssi c'est un multiple de $a \vee b$. On en déduit que

$$\forall (a,b) \in \mathbb{Z}^2,\ \begin{cases} a \wedge b = \max\{d \in \mathbb{N} \,:\, d|a \text{ et } d|b\} \\ a \vee b = \min\{m \in \mathbb{N} \,:\, a|m \text{ et } b|m\} \end{cases}$$

  le max et le min étant cette fois à comprendre au sens de la relation d'ordre | dans $\mathbb{N}$.

- Généralisation à plus de deux entiers.

- Distributivité du pgcd : $\forall (k,a,b) \in \mathbb{N} \times \mathbb{Z}^2,\ (ka) \wedge (kb) = k(a \wedge b)$.

- Entiers premiers entre eux. Généralisation à plus de deux entiers.

- Théorème de Bézout. Généralisation à n entiers premiers entre eux dans leur ensemble. Corollaire : si a est premier avec $b_1, \ldots, b_n$ alors il est premier avec leur produit.

- Invariance du pgcd par transvection. Application : algorithme d'Euclide.

- Théorème de Gauss. Corollaire : si $a_1, \ldots, a_n$ divisent b et s'ils sont 2 à 2 premiers entre eux, alors leur produit divise b.

- Écriture irréductible d'un rationnel.

- Lemme d'Euclide (si p premier divise $a_1 \ldots a_n$, alors il divise l'un des a_i).

- Tout entier $n \geq 2$ admet un diviseur premier.

- Il existe une infinité de nombres premiers.

- Pour p premier, valuation p-adique d'un entier non nul. Relation $v_p(mn) = v_p(m) + v_p(n)$.

- Existence d'une décomposition en facteurs premiers pour $n \geq 1$:

$$n = \prod_{p \in I} p^{\alpha_p},$$

  avec I une partie finie de $\mathcal{P}$ et $(\alpha_p)_{p \in I}$ une famille à valeurs dans $\mathbb{N}^\star$. Lien avec les valuations p-adiques. On en déduit l'unicité de la DFP. Pour les exercices, on préfèrera la forme

$$n = p_1^{\alpha_1} \times \ldots \times p_r^{\alpha_r},$$

  où les p_i sont deux à deux distincts.

- Deux entiers strictement positifs sont premiers entre eux ssi leurs DFP sont disjointes.

- Soit $m, n \in \mathbb{Z}^\star$. Alors $m|n$ ssi pour tout p premier, $v_p(m) \leq v_p(n)$. Soit $m, n \in \mathbb{N}^\star$. Alors $m = n$ ssi pour tout p premier, $v_p(m) = v_p(n)$.

- Vu à titre d'exercice : ensemble des diviseurs strictement positifs de $n = \prod_{p \in I} p^{\alpha_p}$. Nombre de ces diviseurs.

- Valuation d'un pgcd, d'un ppcm. Application :

$$\forall (a,b) \in (\mathbb{N}^\star)^2,\ (a \wedge b)(a \vee b) = ab.$$

- Rien de ce qui concerne les congruences n'a été traité pour l'instant. Toutefois, il est vrai que certains résultats ont déjà été vus en classe de terminale. Mais en aucun cas, les exercices posés sur ce sujet ne devront excéder le programme du baccalauréat.

Partie IV - Shortlist (questions de cours)

i) Anneau : absorbance de 0 pour la loi $\times$. "Règle des signes" dans un produit.

ii) La divisibilité est une relation d'ordre sur $\mathbb{N}$.

iii) Soit H un sous-groupe de $(\mathbb{Z}, +)$. Alors il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

iv) Distributivité du pgcd.

v) Théorème de Bézout et théorème de Gauss.

vi) Il existe une infinité de nombres premiers.

Morceau de la semaine : `https://www.youtube.com/watch?v=NBpHdzZyQAc`