Semaine 7 - Structures algébriques – Groupes

Nous n'avons pas encore traité d'exercices sur les groupes.
Limiter l'abstraction, surtout en début de semaine.

1 Arithmétique

Reprise du programme précédent

2 Lois de composition interne

- Lois de composition interne (LCI)
- Associativité, élément neutre, symétrique, commutativité, élément simplifiable
- Itérés (ou puissances) d'un élément par une LCI
- Conventions d'écriture additive/multiplicative pour les LCI
- Lois + et × sur $\mathbb{Z}/n\mathbb{Z}$

3 Groupes

La notion d'ordre d'un élément est hors programme.

- Groupe, groupe abélien, exemples (notamment $\mathbb{Z}/n\mathbb{Z}$)
- Produit de groupes
- Sous-groupe
- Caractérisation des sous-groupes de $\mathbb{Z}$
- Caractérisation des sous-groupes de $\mathbb{R}$: de la forme $a\mathbb{Z}$ ou dense (= rencontre tout intervalle $]a, b[$, avec $a < b$)
- Intersection de sous-groupes
- Sous-groupe engendré par une partie A : caractérisation par le haut (intersection des sous-groupes contenant la partie) et par le bas (éléments obtenus par produit des éléments de A et de leur inverse)
- Morphisme de groupes
- Noyau et image d'un morphisme ; ce sont des sous-groupes de l'espace de départ/-d'arrivée
- Le noyau caractérise l'injectivité ; l'image la surjectivité
- Endomorphisme, isomorphisme, automorphisme

– L'ensemble des automorphismes de G est un sous-groupe du groupe des permutations de G.
– Groupes monogènes
– Un groupe monogène infini est isomorphe à $\mathbb{Z}$; un groupe monogène fini de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

4 Exemples de questions de cours

– Petit théorème de Fermat – *démonstration au choix*
– Résolution effective d'un système de congruences par le théorème des restes chinois
– Caractérisation des sous-groupes de $\mathbb{Z}$
– Caractérisation des sous-groupes de $\mathbb{R}$
– Si A est une partie d'un groupe G,

$$\langle A \rangle = \{x_1 \dots x_k, k \in \mathbb{N} \text{ et } \forall i \in [\![1, k]\!], x_i \in A \text{ ou } x_i^{-1} \in A\}.$$

– Caractérisation des groupes monogènes - *On pourra se limiter au cas fini ou infini.*