Programme semaine 3

Algèbre générale

Groupes, sous-groupes

Groupe, produit fini de groupes.

Sous-groupe, intersection de sous-groupes.

Sous-groupe $\langle A \rangle$ de G engendré par une partie $A \subseteq G$.

Les sous-groupes de $(\mathbb{Z}, +)$.

Morphismes de groupes

Définition. Composition de morphismes.

Image directe, image réciproque d'un sous-groupe par un morphisme (de groupes). Image et noyau d'un morphisme.

Un morphisme est injectif ssi son noyau est nul.

Isomorphismes de groupes. Composition d'isomorphismes.

Bijection réciproque d'un isomorphisme.

Groupes monogènes, groupes cycliques

Définitions.

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, ses générateurs.

Classification des groupes monogènes :

— Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.

— Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Ordre d'un élément dans un groupe

Élément d'ordre fini, ordre d'un tel élément.

Si $g \in G$ est d'ordre $m \in \mathbb{N}$:

· $\forall k \in \mathbb{Z}, \quad g^k = 1_G \iff m|k$

· $\forall k_1, k_2 \in \mathbb{Z}, \quad g^{k_1} = g^{k_2} \iff k_1 \equiv k_2[m]$

· $\langle g \rangle$ est cyclique de cardinal m

· si de plus G est fini alors m divise $\#G$ (ADMIS si G non commutatif)

Anneaux

Anneau, produit fini d'anneaux.

Sous-anneau, morphisme d'anneaux.

Image et noyau d'un morphisme. Isomorphisme d'anneaux.

Anneau intègre : non nul, commutatif et sans « diviseurs de 0 ».

Corps. Sous-corps.

Algèbre, sous-algèbre, morphisme d'algèbres.

Si $a \in A$ est un élément d'une K-algèbre, l'application

$$\varphi : \begin{array}{ccc} K[X] & \longrightarrow & A \\ P & \longmapsto & P(a) \end{array}$$

est un morphisme d'algèbres. De plus :

— son noyau $\ker \varphi$ est l'idéal des polynômes qui annulent a.

— son image $K[a]$ est une sous-algèbre commutative de A.

Idéaux

Idéal d'un anneau commutatif.

Le noyau d'un morphisme d'anneaux est un idéal.

Relation de divisibilité dans un anneau intègre.

Interprétation de la divisibilité en termes d'idéaux.

Les idéaux de $\mathbb{Z}$.

L'anneau $\mathbb{Z}/n\mathbb{Z}$

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, ses éléments inversibles.

$\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est un nombre premier.

Théorème des restes chinois.

Indicatrice d'Euler φ.

Calcul de $\varphi(n)$ à l'aide de la décomposition de n en produit de nombres premiers.

Théorème d'Euler (qui généralise le petit théorème de Fermat).

Exercices de la banque CCP **à préparer** : 66, 86, 94