CLASSE DE MP

Programme de colle N°1

semaine du 16 au 20 septembre 2019

- Groupes : Définition, Produit fini de groupes, Sous-groupe. Caractérisation.
Intersection de sous-groupes, Sous-groupe engendré par une partie, Sous-groupes du groupe $(\mathbb{Z}, +)$.
Morphismes de groupes : Définition, Image et image réciproque d'un sous-groupe par un morphisme. Image et noyau d'un morphisme.
Condition d'injectivité d'un morphisme, Isomorphisme de groupes. Réciproque d'un isomorphisme.
Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, Générateurs de $\mathbb{Z}/n\mathbb{Z}$.
Groupes monogènes, groupes cycliques. Groupe des racines n-ièmes de l'unité.
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 d'un groupe, ordre d'un tel élément (Si x est d'ordre fini, l'ordre de x est le cardinal du sous-groupe de G engendré par x.)
Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour n dans $\mathbb{Z}$, on a $x^n = e \iff d|n$.
L'ordre d'un élément d'un groupe fini divise le cardinal du groupe. La démonstration n'est exigible que pour G commutatif.

- Anneaux : Définition (Les anneaux sont unitaires), Produit fini d'anneaux, Sous-anneaux. Morphisme d'anneaux.
Image et noyau d'un morphisme. Isomorphisme d'anneaux.
Anneau intègre. Corps. Sous-corps (Les corps sont commutatifs.)

- Idéaux d'un anneau commutatif : définition ; Le noyau d'un morphisme d'anneaux est un idéal.
Relation de divisibilité dans un anneau commutatif intègre.
Idéaux de $\mathbb{Z}$

- L'anneau $\mathbb{Z}/n\mathbb{Z}$: Définition ; Inversibles de $\mathbb{Z}/n\mathbb{Z}$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
Théorème chinois, application aux systèmes de congruences.
Indicatrice d'Euler φ. Calcul de $\varphi(n)$ à l'aide de la décomposition de n en facteurs premiers.
Théorème d'Euler. Lien avec le petit théorème de Fermat étudié en première année.

- **Anneaux de polynômes à une indéterminée** *Dans ce paragraphe, K est un sous-corps de* $\mathbb{C}$. : Idéaux de $K[X]$; PGCD de deux polynômes. Par convention, le PGCD est unitaire ; Extension au cas d'une famille finie.
Relation de Bézout. Lemme de Gauss.
Irréductible de $K[X]$. Existence et unicité de la décomposition en facteurs irréductibles ; Irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.
L'étude des polynômes sur un corps fini est hors programme.

- **Algèbres** : Définition (les algèbres sont unitaires) ; Sous-algèbres ; Morphismes d'algèbres.

Séance de révisions sur les manipulations de polynômes.

Le but est de revoir les techniques de base de manipulation de polynômes, sans soulever de question théorique, juste des manipulations dont j'aimerais qu'elles soient effectuées rapidement.
Exemples de questions qu'on peut traiter

- Calcul d'un coefficient donné dans un produit de polynômes, par exemple, donner le coeff de X^3, ou de X^4 dans $(X^4 + 5X3 - X^2 + 8X - 1)(2X^5 + 3X^3 - 12X^2 + X - 4)$ ...

- Factoriser (rapidement) un polynôme connaissant une racine

- Savoir faire la division euclidienne de 2 polynômes, en particulier dans le cas où le polynôme quotient est scindé.

- Si les questions précédentes ne posent pas de pb, résoudre des équations polynomiales simples, du type
$(X - 1)P' = 3P$ ou $P(X + 1) = P(X)$ ou ...

- ou déterminer l'expression ou des propriétés de polynômes définis par une relation de récurrence, l'exemple type étant les polynômes de Tchebychef, mais toute autre formule un peu riche est bienvenue ...