Semaine 2 : du 22 septembre au 26 septembre

Sauf mention contraire, tout est à savoir.

Rappels de sup sur l'arithmétique dans $\mathbb{Z}$

- Division euclidienne, congruences
- Nombres premiers, décomposition en facteurs premiers, valutation.
- PGCD (de deux ou plusieurs éléments), PPCM, algorithme d'Euclide.
- Théorème de Bézout (de deux ou plusieurs éléments), lemme de Gauss.

Rappels de sup sur $\mathbb{K}[X]$ et $\mathbb{K}(X)$

- Extension des définitions sur un sous-coprs de $\mathbb{C}$.
- Division euclidienne, PGCD (de deux ou plusieurs éléments), PPCM, Algorithme d'Euclide.
- Théorème de Bézout (de deux ou plusieurs éléments), lemme de Gauss.
- Polynômes irréductibles, décomposition en produit d'irreductibles, puis cas réel et complexe
- Sur $\mathbb{R}$ ou $\mathbb{C}$: fractions rationnelles, théorème de décomposition en éléments simples, décompoisition de P'/P, coefficient d'un pôle simple.

Groupes

Rappels de sup sur les groupes

- Définition, exemples, groupe produit.
- Sous-groupe, caractérisation.
- Sous-groupes de $(\mathbb{Z}, +)$ (spé).

Groupe engendré par une partie

- Intersection de sous-groupes.
- Sous-groupe engendré par une partie A, construction et interpréation comme le plus petit sous-groupe contenant A.
- Groupe monogène et cycliques, isomorphisme entre $(\mathbb{Z}, +)$ et un groupe monogène infini. Tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- Générateurs.

Rappels de sup sur les morphismes de groupes

- Définition.
- Image directe et réciproque d'un sous-groupe.
- Image et noyau. Caractérisation de l'injectivité par le noyau.
- Isomorphisme et réciproque d'un isomorphisme.

Rappels de sup sur le groupe $\mathcal{S}_n$.

- Définition, transpositions, cycles.
- Ordre d'un cycle et d'une transposition.
- Décomposition en cycle, les permutations engendrent $\mathcal{S}_n$.
- Le morphisme de groupe signature.

Ordre d'un élément

- Élément d'ordre fini d'un groupe, ordre d'un tel élément.
- Si x est d'ordre d, alors $x^n = e \Leftrightarrow d|n$.
- L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.

Révision de sup sur les anneaux

- Définition, opérations (factorisation $a^n - b^n$, binôme de Newton, sommes doubles,...).
- Le groupe des inversibles, exemples dans $\mathbb{Z}$ et $\mathbb{K}[X]$.
- Sous-anneaux.
- Produits d'anneaux (spé)
- Morphisme d'anneaux, image, noyau. Caractérisation de l'injectivité/surjectivité par l'image et le noyau. Réciproque d'un isomorphisme d'anneaux.
- Intégrité, exemples.

Révisions de sup sur les corps

- Corps et sous-corps. Exemples de $\mathbb{Q}[\sqrt{2}]$.

Idéal

- Définition et exemple (somme de deux idéaux).
- Idéal et noyau.
- Idéal engendré par un élément, lien avec la divisibilité.
- Idéaux de $\mathbb{Z}$ et $\mathbb{K}[X]$. Cela donne une nouvelle définition du PGCD.
- Complément (hors-programme) : nombres algébriques et $\mathbb{K}[\alpha]$ (dimension, corps).

$\mathbb{Z}/n\mathbb{Z}$

Le groupe $\mathbb{Z}/n\mathbb{Z}$

- Définition, description, opérations + et $\times$.
- Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
- Générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

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

- L'anneau $\mathbb{Z}/n\mathbb{Z}$, condition pour que ça soit un corps.
- Description de $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.
- Théorème chinois (deux facteurs et plus), résolution de systèmes de congruences.

Indicatrice d'Euler

- Définition, lien avec $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.
- $k \wedge n = 1 \Rightarrow k^{\varphi(n)} \equiv 1[n]$.
- Calcul de $\varphi(mn)$ si $m \wedge n = 1$, puis de $\varphi(p^k)$, avec p premier et enfin $\varphi(n)$ quand on a la décomposition en facteurs premiers $n = p_1^{k_1}...p_q^{k_q}$.

Banque CCINP

85,86,89, 94