ALGÈBRE GÉNÉRALE

Le niveau d'exigence est assez faible. Nos élèves ne sont absolument pas habitués à évoluer dans ce type d'abstraction. Merci d'adapter le niveau de vos exercices en conséquence.

1. Groupes

Groupes, sous-groupes, morphismes de groupes. Groupe engendré par une partie, systèmes de générateurs d'un groupe. Principaux exemples.

Groupes produits.

Théorème de Lagrange : l'ordre d'un sous-groupe divise l'ordre du groupe.

Ordre d'un élément x dans un groupe fini G. C'est le cardinal du groupe engendré (par définition), mais c'est aussi la plus petite puissance strictement positive n telle que $x^n = 1_G$. D'après le théorème de Lagrange, on a donc toujours $x^{\text{card } G} = 1_G$.

Groupe additif $\mathbb{Z}/n\mathbb{Z}$ (seul groupe quotient au programme).

Description des groupes monogènes finis (groupes cycliques).

Rappels des principaux résultats de Sup' concernant le groupe symétrique (décompositions en cycles, en transpositions, signature…) ; ces résultats ont été retrouvés sur des exercices.

2. Anneaux

Anneaux, sous-anneaux, morphismes d'anneaux. Groupe multiplicatif des unités d'un anneau. Multiplication et structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$.

☞ Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

☞ $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Lemme chinois : isomorphisme d'anneaux entre $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ quand a et b sont premiers entre eux. Interprétation en termes de systèmes de congruences. Application à la multiplicativité de la fonction indicatrice d'Euler.

Théorème d'Euler : si a est premier avec n, alors $a^{\varphi(n)} = 1$ dans $\mathbb{Z}/n\mathbb{Z}$.

3. Arithmétique de $\mathbb{Z}$:

☞ Tout sous-groupe additif de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$.

☞ $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ où c est le pgcd de a et b.

Application aux théorèmes de Bézout puis de Gauss, et théorème de décomposition en puissances de nombres premiers.

4. Polynômes

☞ Toute famille de polynômes de degrés deux à deux distincts est libre. Une famille (P_n) de polynômes telle que $\deg P_n = n$ pour tout n est donc une base de $\mathbb{K}[X]$ (critère des degrés étagés).

Arithmétique de $\mathbb{K}[X]$

Théorème de division euclidienne (non redémontré).

Tout idéal de $\mathbb{K}[X]$ est l'ensemble des multiples d'un polynôme particulier (j'ai à peine prononcé le mot « principal » puisque celui-ci ne figure pas au programme).

Théorème de Bézout, théorème de Gauss.

Existence et unicité d'une décomposition en puissances d'irréductibles.

Caractérisation des irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$ (Théorème de d'Alembert-Gauss admis pour l'instant).

Racines d'un polynôme

Un élément a de est racine de P si et seulement si $X-a$ divise P.

Multiplicité d'une racine.

☞ Formule de Taylor dans un corps contenant $\mathbb{Q}$.

Application à la détermination de l'ordre de multiplicité d'une racine.

Relations entre coefficients et racines pour un polynôme scindé.