Programme de colles - Semaine 3 - du 2/10 au 6/10

Structures algébriques usuelles :
Révisions et compléments sur les groupes : Groupe. Sous-groupe. Caractérisation. Sous-groupes du groupe $(\mathbb{Z},+)$. Produit fini de groupes. Intersection de sous-groupes. Sous-groupe engendré par une partie. Partie génératrice d'un groupe.

Morphismes de groupes : Morphisme de groupes. Composée de morphismes de groupes. Réciproque d'un morphisme de groupes bijectif. Image directe 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, automorphismes.

Construction du groupe $\mathbb{Z}/n\mathbb{Z}$: Relation de congruence sur $\mathbb{Z}$. Loi additive sur sur $\mathbb{Z}/n\mathbb{Z}$; $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Groupes monogènes et cycliques : Groupe monogène. Groupe cyclique. Exemples de $\mathbb{Z}$, du groupe des racines n-ièmes de l'unité, du groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$. 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 k dans $\mathbb{Z}$, on a : $x^k = e \Longleftrightarrow d|k$. L'ordre de x est le cardinal du sous-groupe de G engendré par x. L'ordre d'un élément d'un groupe fini divise le cardinal du groupe (la démonstration n'est officiellement exigible que dans le cas abélien mais a été vue dans le cas général ; de même le théorème de Lagrange a été vu mais est hors programme).
Un groupe fini est cyclique si et seulement si il admet un élément d'ordre le cardinal du groupe. Générateurs d'un groupe cyclique. Un produit $G \times H$ de groupes cycliques est cyclique si et seulement si $Card(G) \wedge Card(H) = 1$. Sous-groupes d'un groupe cyclique.

Quelques rappels sur le groupe symétrique.

Compléments sur les anneaux : Anneau. Sous-anneaux. Anneau intègre. Corps. Un corps est toujours un anneau intègre. Morphisme d'anneaux. L'image d'un morphisme d'anneaux est un sous-anneau. Groupe des inversibles d'un anneau. Produit fini d'anneaux. Idéal d'un anneau commutatif. Noyau d'un morphisme d'anneaux commutatifs. Idéal engendré par un élément. Notation xA. Anneau principal. Idéaux de $\mathbb{Z}$, de $\mathbb{K}[X]$.
Anneau $\mathbb{Z}/n\mathbb{Z}$: Loi multiplicative sur $\mathbb{Z}/n\mathbb{Z}$; anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$. L'anneau est intègre si et seulement si n est premier. Groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. Notation $\mathbb{F}_p$ lorsque p est premier. Théorème chinois : si m et n sont deux entiers premiers entre eux, isomorphisme (d'anneaux) naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Application aux systèmes de congruences.

Indicatrice d'Euler : Définition et différentes caractérisations. Calcul de $\varphi(n)$ à l'aide de la décomposition de n en facteurs premiers. Petit théorème de Fermat et Théorème d'Euler : pour tout a premier avec n, $a^{\varphi(n)} \equiv 1[n]$.

Divisibilité dans un anneau commutatif intègre : Interprétation en termes d'idéaux.

Algèbres Algèbre. Les algèbres sont unitaires. Exemples : $\mathbb{K}[X]$, $\mathcal{L}(E)$, $\mathcal{M}_n(\mathbb{K})$, $\mathcal{F}(X,\mathbb{K})$. Sous-algèbre. Morphisme d'algèbres.

Compléments hors-programmes divers : caractéristique d'un corps, idéaux maximaux, un tout petit peu d'action groupe.

Arithmétique dans $\mathbb{Z}$: Exercices de révision de MPSI.

Programme de la semaine prochaine : Révisons d'algèbre générale. Arithmétique dans $\mathbb{K}[X]$; rappels de MPSI sur $\mathbb{K}[X]$, éléments algébriques, extensions de corps.