Colle de la semaine du 17/12

Le programme porte sur les groupes et les anneaux :

Groupes :

- Définitions groupes, sous-groupes, les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.
- Classe d'équivalence à gauche, à droite selon un sous-groupe, théorème de Lagrange, groupe quotient dans le cas de groupes abéliens (tous ces points sont hors programmes).
- Groupe $\mathbb{Z}/n\mathbb{Z}$.
- Morphismes de groupes, propriétés des morphismes de groupes.
- Sous-groupe engendré par une partie, groupe monogène, groupe cyclique.
- Ordre d'un élément, théorème faible de Lagrange : l'ordre d'un élément divise le cardinal du groupe.
- Groupe produit.
- Groupe symétrique : rappels de MPSI

Anneaux :

- Définitions, rappels de MPSI.
- Idéaux d'un anneau commutatif, idéal principal, anneau principal, $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.
- Le noyau d'un morphisme d'anneaux est un idéal, l'image réciproque d'un idéal est un idéal.
- L'intersection et la somme d'idéaux est un idéal.
- Divisibilité dans un anneau commutatif intègre, lien avec les idéaux.
- Arithmétique dans $\mathbb{Z}$ et $\mathbb{K}[X]$, écriture du PGCD et PPCM en termes d'idéaux, théorème et relation de Bézout, éléments irréductibles.
- Irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$; exemples dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.
- Anneau $\mathbb{Z}/n\mathbb{Z}$, définition, $\overline{k}$ est inversible $\Leftrightarrow\ k \wedge n = 1$ et si $\overline{k}$ n'est pas inversible c'est un diviseur de $\overline{0}$.
- Théorème chinois : pour $m \wedge n = 1$ $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
- Indicatrice d'Euler, définition, $\varphi(mn) = \varphi(n)\varphi(n) = 1$ pour $m \wedge n = 1$, $\varphi(p^k) = p^k - p^{k-1}$ pour p premier et calcul de $\varphi(n)$, $n \in \mathbb{N}^*$.
- Théorème d'Euler : si $a \wedge n = 1$, $a^{\varphi(n)} \equiv 1[n]$, petit théorème de Fermat.

Énoncés, exemples et démonstrations à préparer :

- Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.
- Si f est un morphisme de groupes, $f(e) = e^{'}$ et $f(x^{-1}) = f(x)^{-1}$.
- Pour $a \in G$ d'ordre fini p (où G un groupe), $< a >= \{e, a, a^2, ..., a^{p-1}\}$ et $a^q = e \Leftrightarrow p|q$.
- Théorème faible de Lagrange (dem. dans le cas d'un groupe abélien).
- Si $ab = ba$ avec $\omega(a) \wedge \omega(b) = 1$ alors $\omega(ab) = \omega(a)\omega(b)$.
- Si G est cyclique de cardinal $n \geq 2$, et $G =< a >$. Alors pour $k \in \mathbb{Z}$, a^k est générateur de G si et seulement si $k \wedge p = 1$. (avec Bezout)
- La signature d'une transposition vaut -1.
- Le noyau d'un morphisme d'anneaux est un idéal, l'image réciproque d'un idéal est un idéal.
- L'intersection et la somme d'idéaux est un idéal.
- Si $P \in \mathbb{R}[X]$ est scindé alors $P^{'}$ est scindé.
- Théorème chinois.
- $\overline{k}$ est inversible $\Leftrightarrow\ k \wedge n = 1$ et si $\overline{k}$ n'est pas inversible c'est un diviseur de $\overline{0}$.
- Théorème d'Euler.
- $\varphi(p^k) = p^k - p^{k-1}$ pour p premier.

Approfondissements :

- Théorème de Lagrange
- Théorème d'isomorphisme : Si $f : G \to G^{'}$ est un morphisme de groupe avec G abélien, $\mathrm{Im}(f)$ est isomorphe à $G/\mathrm{Ker}(f)$.
- Pour $k \in \mathbb{Z}$, $\omega(a^k) = \dfrac{\omega(a)}{\omega(a) \wedge k}$.
- Si H est un sous-groupe distingué de S_n contenant une transposition alors $H = S_n$.
- Toute permutation peut se décomposer en produit de transpositions.
- Soit $\sigma \in S_n$ et $(a_1, ..., a_r)$ un cycle de S_n. Montrer que $\sigma \circ (a_1, ..., a_r) \circ \sigma^{-1} = (\sigma(a_1, ..., \sigma(a_r))$.
- Il existe une infinité de nombres premiers de la forme $-1 + 4k$, $k \in \mathbb{N}^*$.
- Pour p premier, x est un carré dans $(\mathbb{Z}/p\mathbb{Z})^* \Leftrightarrow x^{\frac{p-1}{2}} = \overline{1}$.
- Soit $P \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R}$, $P(x) \geq 0$ alors il existe A et B dans $\mathbb{R}[X]$ tels que $P = A^2 + B^2$.
- Pour $P = \sum_{k=0}^{n} a_k X^k$, P est scindé à racines simples $\Rightarrow \forall k \in [\![0, n-1]\!]$, $a_k^2 + a_{k+1}^2 > 0$.
- Pour $P = \sum_{k=0}^{n} a_k X^k$, P est scindé $\Rightarrow \forall k \in [\![0, n-2]\!]$, $a_k a_{k+2} \leq a_{k+1}^2$.
- Pour $n \in \mathbb{N}^*$, $n = \sum_{d|n} \varphi(d)$.

Les approfondissements concernent les élèves suivants : Chaubin, Maniols, Lagrue, Eymard-Leblanc, Koueta, Grandville, Rousselier, Chaumont, Benyeloul, Le Roy.

Exercices de la banque CCINP à préparer :

— (CCINP 86) 1. Soit $(a,b,p) \in \mathbb{Z}^3$. Prouver que : si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.
2. Soit p un nombre premier.
a. Prouver que $\forall k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ puis en déduire que p divise $\binom{p}{k}$.
b. Prouver que : $\forall n \in \mathbb{N},\ n^p \equiv n \mod p$.
c. En déduire, pour tout entier naturel n, que : p ne divise pas $n \Longrightarrow n^{p-1} \equiv 1 \mod p$.

— (CCINP 85) 1. Soient $n \in \mathbb{N}^*$, $P \in \mathbb{R}_n[X]$ et $a \in \mathbb{R}$.
a. Donner sans démonstration, en utilisant la formule de Taylor, la décomposition de $P(X)$ dans la base $\left(1, X-a, (X-a)^2, \cdots, (X-a)^n\right)$.
b. Soit $r \in \mathbb{N}^*$. En déduire que :
a est une racine de P d'ordre de multiplicité r si et seulement si $P^{(r)}(a) \neq 0$ et $\forall k \in [\![0, r-1]\!]$, $P^{(k)}(a) = 0$.
2. Déterminer deux réels a et b pour que 1 soit racine double du polynôme $P = X^5 + aX^2 + bX$ et factoriser alors ce polynôme dans $\mathbb{R}[X]$.

— (CCINP 94) 1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.
2. Soit a et b deux entiers naturels premiers entre eux. Soit $c \in \mathbb{N}$.
Prouver que : $(a|c \text{ et } b|c) \Longleftrightarrow ab|c$.
3. On considère le système (S) : $\left\{ \begin{array}{rcll} x & \equiv & 6 & [17] \\ x & \equiv & 4 & [15] \end{array} \right.$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.
a. Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
b. Déduire des questions précédentes la résolution dans $\mathbb{Z}$ du système (S).

— (CCINP 84) 1. Donner la définition d'un argument d'un nombre complexe non nul (on ne demande ni l'interprétation géométrique, ni la démonstration de l'existence d'un tel nombre).
2. Soit $n \in \mathbb{N}^*$. Donner, en justifiant, les solutions dans $\mathbb{C}$ de l'équation $z^n = 1$ et préciser leur nombre.
3. En déduire, pour $n \in \mathbb{N}^*$, les solutions dans $\mathbb{C}$ de l'équation $(z+\mathrm{i})^n = (z-\mathrm{i})^n$ et démontrer que ce sont des nombres réels.

— (CCINP 87) Soient $a_0, a_1, \cdots, a_n$, $n+1$ réels deux à deux distincts.
1. Montrer que si $b_0, b_1, \cdots, b_n$ sont $n+1$ réels quelconques, alors il existe un unique polynôme P vérifiant

$$\deg P \leqslant n \text{ et } \forall i \in [\![0,n]\!],\ P(a_i) = b_i.$$

2. Soit $k \in [\![0,n]\!]$. Expliciter ce polynôme P, que l'on notera L_k, lorsque :$\forall i \in [\![0,n]\!]$, $b_i = \left\{ \begin{array}{lll} 0 & \text{si} & i \neq k \\ 1 & \text{si} & i = k \end{array} \right.$.
3. Prouver que $\forall p \in [\![0,n]\!]$, $\displaystyle\sum_{k=0}^{n} a_k^p L_k = X^p$.