Programme de colle – MPI*

1. Structure de groupe

Extrait du programme officiel :

Contenus	Capacités & commentaires
a) Compléments sur les groupes	
Intersection de sous-groupes.	
Sous-groupe engendré par une partie. Partie génératrice d'un groupe.	
Sous-groupes du groupe $(\mathbb{Z},+)$.	
Groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.	
Groupe monogène, groupe cyclique.	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 d'un groupe.	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 tout $n\in\mathbb{Z}$, $x^n=e\iff d\mid n$.	
L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.	La démonstration n'est exigible que pour G commutatif.

Le théorème de Lagrange est hors-programme mais est considéré comme un résultat de cours à savoir redémontrer.

2. Révisions de MP2I sur le groupe symétrique

Voir programme de MP2I page suivante.
On s'intéresse en particulier aux orbites d'une permutation, à son ordre, au groupe alterné.

3. Révisions de MP2I sur l'arithmétique sur $\mathbb{Z}$

Voir programme de MP2I page suivante.

Semaine prochaine : Pas de colle.
Semaine suivante : Anneaux, corps, algèbres. Révisions d'algèbre linéaire.

4. Questions de cours

(i) **Fonction ζ de Riemann**
Définition, Classe $\mathscr{C}^\infty$, convexité, variations, limite en $+\infty$, équivalent et limite en 1, tracé, absence de convergence uniforme au voisinage de 1.

(ii) **Théorème de Lagrange** : le cardinal d'un sous-groupe d'un groupe fini divise celui du groupe.

(iii) Si $x\in G$ est d'ordre fini, son ordre est le cardinal du sous-groupe $\langle x\rangle$ qu'il engendre.
Si G est fini, alors $x\in G$ est d'ordre fini divisant $|G|$, démonstration dans le cas commutatif.

(iv) Sous-groupes de $(\mathbb{Z},+)$.

(v) Sous-groupes de $(\mathbb{R},+)$.

(vi) Générateurs de $(\mathbb{Z}/n\mathbb{Z},+)$.
Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$.
Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

(vii) Toute permutation se décompose de manière unique en produit de cycles à supports disjoints.

(viii) Les transpositions engendrent $\mathfrak{S}_n$: déduit de la décomposition en cycles à supports disjoints et preuve par récurrence.

(ix) La signature d'une permutation de $\mathfrak{S}_n$ vaut $\varepsilon(\sigma)=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(j)-\sigma(i)}{j-i}$.
Il s'agit d'un morphisme de groupes.

(x) Démonstration du **petit théorème de Fermat** par récurrence (cours de MP2I).

Les étudiants doivent savoir faire les exercices de la **banque CCINP 16, 18, 53, 86, 94** mais ne seront pas interrogés dessus.

5. Programme de MP2I

Extrait du programme officiel :

A. Structure de groupe

Contenus	Capacités & commentaires
a) Loi de composition interne	
Loi de composition interne.	On évite l'étude de lois artificielles.
Associativité, commutativité, élément neutre, inversibilité, distributivité.	Inversibilité et inverse du produit de deux éléments inversibles.
Partie stable.	
b) Structure de groupe	
Groupe.	Notation x^n dans un groupe multiplicatif, nx dans un groupe additif. Exemples usuels : groupes additifs $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, groupes multiplicatifs $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{C}^*$, $\mathbb{U}$, $\mathbb{U}_n$.
Groupe des permutations d'un ensemble.	Notation $\mathfrak{S}_X$.
Groupe produit.	
Sous-groupe : définition, caractérisation.	
Morphisme de groupes. Image et image réciproque d'un sous-groupe par un morphisme.	
Image et noyau d'un morphisme. Condition d'injectivité.	Notations $\operatorname{Im} f$, $\operatorname{Ker} f$.
Isomorphisme.	

B. Groupe symétrique

Le groupe symétrique est introduit en vue de l'étude des déterminants, mais aussi pour son intérêt propre et ses interventions possibles dans diverses questions d'algèbre et de probabilités.

Contenus	Capacités & commentaires
a) Généralités	
Groupe des permutations de l'ensemble $\{1,\dots,n\}$.	Notation S_n.
Cycle, transposition.	Notation $(a_1\ a_2\ \dots\ a_p)$.
Décomposition d'une permutation en produit de cycles à supports disjoints : existence, unicité, commutativité.	La démonstration n'est pas exigible, mais les étudiants doivent savoir décomposer une permutation.
b) Signature d'une permutation	
Décomposition d'une permutation en produit de transpositions.	
Signature : il existe un unique morphisme de groupes de S_n dans $\{-1,1\}$ envoyant toute transposition sur -1.	La démonstration n'est pas exigible.

C. Arithmétique sur $\mathbb{Z}$

L'objectif de cette section est d'étudier les propriétés de la divisibilité des entiers et des congruences. L'approche préconisée reste élémentaire en ce qu'elle ne fait pas appel au langage des structures algébriques.

Contenus	Capacités & commentaires
a) Divisibilité et division euclidienne	
Divisibilité dans $\mathbb{Z}$, diviseurs, multiples.	Caractérisation des couples d'entiers associés.
Théorème de la division euclidienne.	
b) PGCD et algorithme d'Euclide	
PGCD de deux entiers naturels dont l'un au moins est non nul.	Notation $a\wedge b$. Le PGCD de a et b est défini comme étant le plus grand élément (pour l'ordre naturel dans $\mathbb{N}$) de l'ensemble des diviseurs communs à a et b.
Algorithme d'Euclide.	L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de $a\wedge b$. $a\wedge b$ est le plus grand élément (au sens de la divisibilité) de l'ensemble des diviseurs communs à a et b. Pour $k\in\mathbb{N}^*$, PGCD de ka et kb.
Extension au cas de deux entiers relatifs.	
Relation de Bézout.	Détermination d'un couple de Bézout par l'algorithme d'Euclide étendu.
PPCM.	Notation $a\vee b$.
c) Entiers premiers entre eux	
Couple d'entiers premiers entre eux.	
Théorème de Bézout.	Forme irréductible d'un rationnel.
Lemme de Gauss.	
Si a et b sont premiers entre eux et divisent n, alors ab divise n.	
Si a et b sont premiers à n, alors ab est premier à n.	
PGCD d'un nombre fini d'entiers, relation de Bézout. Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux.	
d) Nombres premiers	
Nombre premier.	Crible d'Ératosthène.
L'ensemble des nombres premiers est infini.	
Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.	
Pour p premier, valuation p-adique.	Notation $v_p(n)$.
Valuation p-adique d'un produit.	Caractérisation de la divisibilité en termes de valuations p-adiques. Expressions du PGCD et du PPCM à l'aide des valuations p-adiques.
e) Congruences	
Relation de congruence modulo un entier sur $\mathbb{Z}$.	Notation $a\equiv b\ [n]$.
Opérations sur les congruences : somme, produit.	Les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont hors programme.
Utilisation d'un inverse modulo n pour résoudre une congruence modulo n.	
Petit théorème de Fermat.	