Programme de colle – MPI

1. Structures algébriques

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.
b) Compléments sur les anneaux	
Produit fini d'anneaux.	
Idéal d'un anneau commutatif.	Noyau d'un morphisme d'anneaux commutatifs.
Idéal engendré par un élément.	Notation xA.
Divisibilité dans un anneau commutatif intègre.	Interprétation en termes d'idéaux.
c) Idéaux de $\mathbb{Z}$	
Idéaux de $\mathbb{Z}$.	
Définition du PGCD de $n\geqslant 2$ entiers relatifs en termes d'idéaux, relation de Bézout.	Lien avec le programme de première année.
f) Algèbres	
Algèbre.	Les algèbres sont unitaires. Exemples : $\mathbb{K}[X]$, $\mathscr{L}(E)$, $\mathscr{M}_n(\mathbb{K})$, $\mathscr{F}(X,\mathbb{K})$.
Sous-algèbre.	
Morphisme d'algèbres.	

L'étude de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sera faite plus tard.

Les notions d'idéal et d'anneau principaux ont été introduites.

Semaine prochaine : Suites et séries de fonctions (1re partie). Révisions d'algèbre linéaire.

2. Questions de cours

Les preuves marquées d'un astérisque ✻ *sont réservées aux trinômes 6 et 7.*

(i) Images directe et réciproque d'un sous-groupe par un morphisme de groupe.

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

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

(iv) 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.

(v) Définition d'un idéal.
Les idéaux d'un corps sont triviaux.
Le noyau d'un morphisme d'anneau est un idéal.

(vi) Définition d'un idéal principal, d'un anneau principal.
La somme et l'intersection d'idéaux sont des idéaux.
Tout corps est intègre.

(vii) Sous-groupes de $(\mathbb{Z},+)$, $(\mathbb{Z},+,\times)$ est un anneau principal.

(viii) Montrer que si $f:(A,+,\times)\to(A',\oplus,\otimes)$ est un morphisme d'anneaux :
  - (a) L'image réciproque d'un sous-anneau de $(A',\oplus,\otimes)$ est un sous-anneau de $(A,+,\times)$.
  - (b) L'image directe d'un sous-anneau de $(A,+,\times)$ est un sous-anneau de $(A',\oplus,\otimes)$.
  - (c) L'image réciproque d'un idéal de $(A',\oplus,\otimes)$ par f est un idéal de $(A,+,\times)$.
  - (d) L'image directe d'un idéal de $(A,+,\times)$ par f est un idéal de $\big(f(A)=\operatorname{Im} f,\oplus,\otimes\big)$.

(ix) Exercices CCINP : 86, 94

3. Exercices CCINP

- **CCINP 86 : Preuve directe du petit théorème de Fermat**
  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 $\forall n\in\mathbb{N}$, $n^p\equiv n\ [p]$.
       Indication : procéder par récurrence.
     - (c) En déduire, pour tout entier naturel n, que : p ne divise pas $n \Longrightarrow n^{p-1}\equiv 1\ [p]$.

- **CCINP 94** :
  1. En raisonnant par l'absurde, montrer que le système (S) : $\left\{\begin{array}{lll} x & \equiv & 5\ [6] \\ x & \equiv & 4\ [8]\end{array}\right.$ n'a pas de solution appartenant à $\mathbb{Z}$.
  2. (a) Énoncer le théorème de Bézout dans $\mathbb{Z}$.
     (b) Soit a et b deux entiers naturels premiers entre eux. Soit $c\in\mathbb{N}$.
     Prouver que $(a\mid c$ et $b\mid c)\iff ab\mid c$.
  3. On considère le système (S) : $\left\{\begin{array}{lll} x & \equiv & 6\ [17] \\ x & \equiv & 5\ [16] \\ x & \equiv & 4\ [15]\end{array}\right.$ 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).

4. Programme de MP2I

A. Structures algébriques

Extrait du programme officiel :

Contenus	Capacités & commentaires
a) Loi de composition interne	
Loi de composition interne. Associativité, commutativité, élément neutre, inversibilité, distributivité. Partie stable.	On évite l'étude de lois artificielles. Inversibilité et inverse du produit de deux éléments inversibles.
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 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.	
c) Structures d'anneau et de corps	
Anneau.	Tout anneau est unitaire. Exemples usuels : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
Calcul dans un anneau.	Relation $a^n - b^n$ et formule du binôme si a et b commutent.
Groupe des inversibles d'un anneau.	
Anneau intègre. Corps.	Les corps sont commutatifs.
Sous-anneau. Morphisme d'anneaux. Isomorphisme.	

B. Arithmétique sur $\mathbb{Z}$

Extrait du programme officiel :

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. Théorème de la division euclidienne.	Caractérisation des couples d'entiers associés.
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.	