

# Programme de colle n°14

semaine du 13 au 17 janvier

## Notions vues en cours

### Chapitre 17 : Arithmétique (suite et fin)

- Nombre premier, lemme d'Euclide, tout entier admet un diviseur premier, décomposition en produit de facteurs premiers, il existe une infinité de nombres premiers
- Décomposition (dite généralisée) d'un entier  $n \geq 1$  selon tous les nombres premiers (quitte à avoir des exposants nuls)
- Valuation  $p$ -adique, notation  $v_p(a)$ , lecture des valuations sur la décomposition d'un entier, valuation du produit / pgcd / ppcm, lien entre les valuations et la divisibilité / l'égalité de deux entiers
- Calcul pratique du pgcd et du ppcm en utilisant la décomposition en produit de facteurs premiers,  $n \geq 2$  est premier si et seulement si aucun nombre premier  $p$  inférieur à  $\sqrt{n}$  ne divise  $n$ .
- Congruence : définition, caractérisation, relation d'équivalence, lien avec le reste de la division euclidienne
- Congruence et opérations : addition, soustraction, multiplication (par une constante ou terme à terme d'une autre congruence), puissance, division (crochet inclus) dans une congruence
- Inverse d'un entier  $a$  modulo  $n$  : définition, existence ssi  $a \wedge n = 1$ , "division" dans une congruence (on multiplie par l'inverse), méthode pour trouver un inverse modulo  $n$ , pour résoudre une équation  $ax \equiv b \pmod{n}$
- Petit théorème de Fermat (cas général, cas où l'entier est premier avec  $p$ )

*La méthode de résolution des équations diophantiennes de la forme  $ax + by = c$  ne fait pas partie du programme : une telle résolution doit donc être guidée.*

### Chapitre 18 : Structures algébriques

- Loi de composition interne (l.c.i.), loi commutative, loi associative, définition de "deux éléments commutent"
- Élément neutre : définition et unicité, élément symétrisable : définition, UN symétrique d'un élément
- Groupe, groupe commutatif (ou abélien), dans un groupe il y a unicité de l'élément symétrique
- Formules  $(x')' = x$  et  $(x \top y)' = y' \top x'$  (où  $z'$  désigne le symétrique de l'élément  $z$ )
- Groupes usuels :  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{K}^{\mathbb{N}}, \mathbb{K}^{\mathbb{R}}$  munis de  $+$  ;  $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$  munis de  $\times$ , notations additive et multiplicative
- Partie stable par une l.c.i., loi induite (qu'on note souvent comme la loi initiale), sous-groupe : définition, caractérisations,  $\{e\}$  et  $G$  sont des sous-groupes de  $G$

## Questions de cours

**Question libre.** Une question de cours sans démonstration choisie par l'examineur. Cette question est basée sur un ou plusieurs énoncés encadrés tirés du polycopié (définition, propriété, corollaire, théorème SAUF méthode et SAUF les encadrés "non-officiel"), parmi les chapitres **15 à 17**. *Des exemples de questions figurent en page suivante.*

**Question fixée.** *Sauf mention contraire, les démonstrations sont à connaître.*

1. Énoncé uniquement : décomposition en produit de facteurs premiers, définition de la valuation  $p$ -adique d'un entier, décomposition généralisée et lien avec la valuation, énoncé uniquement : donner les formules de  $v_p(ab)$ ,  $v_p(a \wedge b)$  et  $v_p(a \vee b)$  Chapitre 17, Définitions / Théorèmes 17.35, 17.37, 17.38, 17.39
2. Petit théorème de Fermat. On pourra commencer par énoncer et démontrer un lemme préliminaire Chapitre 17, Lemme 17.47 et Théorème 17.48
3. Définition d'un groupe (avec des quantificateurs) ; pour tous  $a, b$  dans un groupe  $(G, \top)$ , quel est le symétrique du symétrique de  $a$  ? Quel est le symétrique de  $a \top b$  ? Chapitre 18, Définition 18.7 et Théorème 18.8

## Exemples de questions libres :

### Chapitre 15 :

- Donner la définition d'une fonction convexe ; puis à l'oral : qu'est-ce qui change pour une fonction concave ?
- Énoncer l'inégalité de Jensen pour une fonction convexe ; puis à l'oral : qu'est-ce qui change pour une fonction concave ?
- Énoncer l'inégalité des pentes pour une fonction convexe ; puis à l'oral : qu'est-ce qui change pour une fonction concave ?
- Que peut-on dire de la position de la courbe d'une fonction convexe par rapport à une sécante ? On pourra faire un dessin et répondre oralement.

### Chapitre 16 :

- Soit  $E$  un ensemble. Que doit vérifier  $\mathcal{R}$  pour être une relation d'équivalence sur  $E$  ?
- Soit  $x \in E$  et  $\mathcal{R}$  une relation d'équivalence sur  $E$ . Donner la définition de la classe d'équivalence de  $x$ . Puis oralement : que peut-on dire de toutes les classes d'équivalence ?
- Soit  $E$  un ensemble. Que doit vérifier  $\mathcal{R}$  pour être une relation d'ordre sur  $E$  ?
- Soit  $\preceq$  une relation d'ordre sur  $E$ . Que doit vérifier  $\preceq$  pour être un ordre total ? Comment appelle-t-on un ordre qui n'est pas total ?
- Soit  $\preceq$  une relation d'ordre sur  $E$  et  $A \subset E$ . Que doit vérifier  $M$  pour être le maximum de  $A$  pour  $\preceq$  ?

### Chapitre 17 :

- Rappeler le théorème de division euclidienne dans  $\mathbb{Z}$  (avec toutes les hypothèses)
- Énoncer le théorème de Bézout-Bachet (aussi appelé relation de Bézout)
- Énoncer le lemme de Gauss
- Donner la forme générale de la décomposition d'un entier  $n$  sous forme de facteurs premiers.
- Soit  $a, n \in \mathbb{Z}$ . Que doit vérifier  $a$  pour être inversible modulo  $n$  ? Si  $c$  est un tel inverse, donner une relation vérifiée par  $a$  et  $c$ .
- Énoncer le petit théorème de Fermat