Semaine du 16/01 au 20/01

1 Cours

Groupes, anneaux, corps

Notion de loi interne Définition. Associativité, commutativité. Définition d'un élément neutre, unicité sous réserve d'existence. Inversibilité, unicité de l'inverse si la loi est associative.

Groupes Définition. Sous-groupe : définition et caractérisation.

Morphismes de groupes Définition, image de l'élément neutre et d'un inverse, composition de morphismes. Images directe et réciproque d'un sous-groupe par un morphisme de groupes. Noyau et image d'un morphisme de groupes. Caractérisation de l'injectivité par le noyau (et de la surjectivité par l'image). Le noyau et l'image sont des sous-groupes. Isomorphisme : définition, la bijection réciproque d'un isomorphisme est un isomorphisme.

Anneaux Définition. Groupe des éléments inversibles. Règles de calcul dans les anneaux. Intégrité. Formule du binôme de Newton et factorisation de $a^n - b^n$ si **commutativité**. Sous-anneaux : définition et caractérisation.

Corps Définition. Tout corps est intègre. Sous-corps : définition et caractérisation.

Arithmétique

Division dans $\mathbb{Z}$ Relation de divisibilité. Opérations sur la divisibilité. Relation de congruence. Opérations sur la congruence. Division euclidienne.

PGCD Définition, existence et unicité. Opérations sur le pgcd. Algorithme d'Euclide. Théorème de Bézout. Nombres premiers entre eux. Théorème de Bézout (équivalence). Théorème de Gauss. Si $a|n$ et $b|n$ avec $a \wedge b = 1$, alors $ab|n$. Si $a \wedge n = 1$ et $b \wedge n = 1$, alors $ab \wedge n = 1$. Équations diophantiennes $ax + by = c$.

2 Méthodes à maîtriser

- Dans un anneau, on prendra garde à se méfier des habitudes de calcul.
  - La seconde loi n'est pas toujours commutative.
  - Un produit d'éléments d'un anneau non intègre peut-être nul sans qu'aucun des facteurs soit nul.
  - Un élément d'un anneau n'est pas forcément inversible.
- Pour montrer qu'un ensemble est un groupe/anneau/corps, on peut montrer que c'est un sous-groupe/sous-anneau/sous-corps d'un groupe/anneau/corps déjà connu.
- Dans un corps, on calcul comme on en a l'habitude.
- Se ramener à des entiers premiers entre eux en factorisant par le pgcd.
- Résoudre des équations diophantiennes linéaires i.e. du type $ax + by = c$ avec $a, b, c \in \mathbb{Z}$ et x, y des inconnues entières.
- Caractériser le reste d'une division euclidienne par une relation de congruence.
- Montrer que deux couples d'entiers ont même pgcd/ppcm en montrant qu'ils se divisent l'un l'autre.
- Savoir montrer que deux entiers sont premiers entre eux en exhibant une relation de Bézout.

3 Questions de cours

- Soient $(A, +, \times)$ un anneau et $(x, y) \in A^2$. Montrer que si x et y sont nilpotents et commutent, $x + y$ est nilpotent.
- Soit $(A, +, \times)$ un anneau. Montrer que si $x \in A$ est nilpotent, $1_A - x$ est inversible et déterminer son inverse.
- Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$ et déterminer ses éléments inversibles.
- Résoudre une équation diophantienne du type $ax + by = c$ au choix de l'examinateur.
- Montrer que tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{Z}$.