Programme de colle semaine 13 - 12 janvier

Le cours doit être parfaitement su.

Groupes, anneaux, corps

Groupes

Anneaux, corps

1. Anneau : définition, anneau commutatif, exemples. Sous-anneau. Calcul dans un anneau : formule du binôme pour deux éléments a et b qui commutent, factorisation de $a^n - b^n$ si a et b commutent.
2. Groupe multiplicatif des éléments inversibles d'un anneau $(\mathrm{A}, +, \times)$, groupe noté $(\mathrm{A}^\times, \times)$ ou $(\mathrm{U}(\mathrm{A}), \times)$. *En exercice : détermination du groupe des inversibles de $\mathbb{Z}[i]$, de $\mathbb{Z}[j]$,*
3. Anneau intègre. Corps, sous-corps, exemples vus en classe : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ et $\mathbb{Q}(\sqrt{2})$ et $\mathcal{C}$ l'ensemble des nombres constructibles à la règle et au compas.
4. Corps, sous-corps. Exemples.
5. Morphisme d'anneaux.

N.B. Nous n'avons pas encore défini l'anneau $\mathbb{Z}/n\mathbb{Z}$. *Vu en exercice seulement : notion d'idéal d'un anneau commutatif.*

Arithmétique dans $\mathbb{Z}$

1. Relation de divisibilité et division euclidienne

1. Relation de divisibilité dans $\mathbb{Z}$. Propriétés élémentaires (réflexivité, transitivité, antisymétrie dans $\mathbb{N}$). Lien avec les sous-groupes additifs de $\mathbb{Z}$.
2. Division euclidienne dans $\mathbb{Z}$. Algorithme de la division euclidienne. Application : sous-groupes de $\mathbb{Z}$.
3. Relation de congruence. Définition. Opération de somme et de produit. Application aux critères de divisibilité usuels (3,9,11).

2. PGCD, PPCM

1. Définition du pgcd de deux entiers. (pour $(a, b) \neq (0, 0)$ le pgcd de a, b se note $a \wedge b$ et est le plus grand diviseur commun des entiers a et b. Algorithme d'Euclide. Il existe u, v entiers tels que $a \wedge b = au + bv$. Si on note $\mathrm{D}(n)$ l'ensemble des diviseurs de n, on a $\mathrm{D}(a) \cap \mathrm{D}(b) = \mathrm{D}(a \wedge b)$. Propriété : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.
   Algorithme d'Euclide étendu.
2. Entiers premiers entre eux. Théorème de Bezout. Théorème de Gauss. Application à la définition du représentant irréductible d'un rationnel.
3. Définition du ppcm. Propriétés élémentaires. a$\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. Conséquence : un multiple commun à a et b est un multiple du ppcm.
4. Produit du pgcd et du ppcm de deux entiers.
5. Extension des notions de pgcd et ppcm de n entiers.

EXOS À MAÎTRISER :

— Savoir utiliser des congruences pour répondre à des questions de divisibilité.

— Résolution d'équations diophantiennes du type $ax + by = n$ avec n multiple du pgcd de (a, b)

3. Nombres premiers

Définition. Pté : un nombre premier est premier avec tous les entiers qu'il ne divise pas. Si p premier, et $p|ab$ alors $p|a$ ou $p|b$.
Exo : Si p est un nombre premier alors pour tout entier $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$. Petit théorème de Fermat.
Sera vu lundi : Théorèmes.

1. Tout entier naturel $n \geq 2$ admet un diviseur premier.
2. L'ensemble des nombres premiers est infini.
3. Théorème de décomposition en facteur premiers.

p-valuation d'un entier. Utilisation pour caractériser la divisibilité, pour exprimer le pgcd ou le ppcm d'une famille d'entiers.

N.B. Nous n'avons pas eu le temps de faire beaucoup d'exercices d'arithmétique.
Les exercices d'arithmétiques seront corrigés en début de semaine (lundi et mercredi).
Cette semaine, vous pourrez, au choix, poser des exercices sur les groupes/anneaux/corps ou sur l'arithmétique. L'arithmétique restera au programme de colle de la semaine du 26 janvier 2026 (avec le début de l'algèbre linéaire probablement).

QUESTIONS de COURS ou EXOS :

1. Exo : montrer que $\mathbb{Z}[\sqrt{2}]$ est un anneau (sous-anneau de $\mathbb{R}$) puis que $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $\mathbb{R}$.
2. Exo : Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. Démontrer que z est inversible dans $\mathbb{Z}[i]$ si et seulement si $|z|^2 = 1$. En déduire le groupe des inversibles $(\mathbb{Z}[i])^\times$.
3. Exo : Si A est un anneau, on dit qu'un élément x de A est nilpotent, s'il existe $n \in \mathbb{N}^*$ tel que $a^n = e$.
   (1) Donner un exemple d'élément nilpotent de l'anneau $\mathrm{M}_2(\mathbb{R})$
   (2) Démontrer que si $a \in \mathrm{A}$ et $b \in \mathrm{A}$ sont deux éléments nilpotents et qui commutent, alors ab et $a+b$ sont nilpotents.
4. Donner la définition d'un morphisme d'anneaux.
   Exo : Si A est un anneau commutatif et $f : \mathrm{A} \to \mathrm{B}$ est un morphisme d'anneaux, justifier que $\ker f$ est un idéal de A (si besoin, on pourra redonner la définition d'un idéal de A).
5. *Exo du début de cours d'arithmétique* : Soit $a \in \mathbb{N}$ un entier dont l'écriture décimale est $a = \sum_{k=0}^{n} a_k 10^k$ où $n \in \mathbb{N}$, $a_0, a_1, \dots, a_n \in [\![0, 9]\!]$.
   (1) Justifier $a \equiv \sum_{k=0}^{n} a_k \quad [3]$. En déduire un critère de divisibilité de a par 3.
   (2) Démontrer le critère usuel de divisibilité par 9. Déterminer le reste dans la DE de 12341234^{2025} par 9.
   (3) Déterminer un critère de divisibilité de a par 11.
6. Faire résoudre une équation du type $ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$ où (a, b, c) est choisi par le colleur.
7. Corollaire du théorème de Gauss : si a et b divisent n et que a et b sont premiers entre eux, alors ab divise n.
8. Écriture des rationnels : si $r \in \mathbb{Q}$, il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{p}{q}$ avec $p \wedge q = 1$. De plus, pour $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, on a $r = \frac{a}{b}$ si et seulement si il existe $k \in \mathbb{Z} \setminus \{0\}$ tel que $p = ka$ et $q = kb$.
9. Si p est un nombre premier alors pour tout entier $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$

Pas de colle la semaine du 19 janvier. Reprise des colles le 28 janvier

PRÉVISIONS : Arithmétique. Puis algèbre linéaire

Meilleurs voeux à tous pour cette nouvelle année !