Arithmétique & Structure de groupe (début du chapitre)

Questions de cours

Théorème 1 *Théorème de Bézout - A énoncer et à démontrer, en utilisant l'égalité de Bezout*

Soit $(a,b) \in \mathbb{Z}^2$. on a :

$$a \text{ et } b \text{ sont premiers entre eux} \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 \quad a\,u + b\,v = 1.$$

Théorème 2 *Lemme de Gauss - A énoncer et à démontrer*

Soit $(a,b,c) \in \mathbb{Z}^3$. Si $a|b\,c$ et $a \wedge b = 1$ alors $a|c$.

Théorème 3 *A énoncer et démontrer les deux premiers points*

(i) Soit $(a,b) \in \mathbb{Z}^2$ et $m \in \mathbb{Z}$. On a :

$$a|m \quad \text{et} \quad b|m \quad \Leftrightarrow \quad (a \vee b)\,|m$$

(ii) Soit $(a,b,c) \in \mathbb{Z}^3$. Si $a|c$ et $b|c$ et $a \wedge b = 1$ alors $a\,b|c$.

(iii) Soit $(a_1,\dots,a_n) \in \mathbb{Z}^n$ et $b \in \mathbb{Z}$. Si pour $i \in [\![1;n]\!]$ $a_i|b$ et les entiers $a_1,\dots,a_n$ sont deux à deux premiers entre eux, alors $a_1 \cdots a_n|b$.

Théorème 4 *Résolution des équations de Bézout - A énoncer seulement*

Soit a, b et c des entiers relatifs avec a et b non nuls. L'équation $a\,x + b\,y = c$ admet :

(i) Aucune solution si c n'est pas un multiple de $a \wedge b$.

(ii) Une infinité de solutions si c est un multiple de $a \wedge b$.

De plus, si (x_0,y_0) est une solution particulière et que l'on note $a = a'\,d$ et $b = b'\,d$ avec $d = a \wedge b$ et $a' \wedge b' = 1$, alors les autres solutions sont les couples d'entiers de la forme $(x_0 + b'\,k, y_0 - a'\,k)$ avec $k \in \mathbb{Z}$.

Théorème 5 *Petit théorème de Fermat - A énoncer et à démontrer*

Si p est un nombre premier et $a \in \mathbb{Z}$ alors

$$a^p \equiv a \pmod{p}$$

Théorème 6 *Théorème fondamental de l'arithmétique - A énoncer et démontrer l'existence ou l'unicité*

Soit $n \in \mathbb{N}$ avec $n \geq 2$. il existe $N \in \mathbb{N}^*$, des nombres premiers $p_1 < \cdots < p_N$ et $(\alpha_1, \ldots, \alpha_N) \in (\mathbb{N}^*)^N$ tels que $n = p_1^{\alpha_1} \cdots p_N^{\alpha_N}$. Cette décomposition est unique et $p_1, \ldots, p_N$ sont les facteurs premiers de n.

Définition/Théorème 7 *Valuation p-adique - A énoncer seulement*

- Soit $p \in \mathbb{P}$ et $n \in \mathbb{Z}^*$, on note $\nu_p(n)$ la plus grande puissance de p qui divise n :

$$\nu_p(n) = \max\left\{k \in \mathbb{N} \mid p^k \text{ divise } n\right\}$$

  Par convention, on pose $\nu_p(0) = +\infty$. On appelle **valuation p-adique** l'application ainsi définie :

$$\begin{array}{rl} \nu_p : \mathbb{Z} & \to \mathbb{N} \cup \{+\infty\} \\ n & \mapsto \nu_p(n) \end{array}$$

- Soit $(a, b) \in \mathbb{Z}^2$. on a l'équivalence suivante :

$$a|b \quad \Leftrightarrow \quad \forall p \in \mathbb{P} \quad \nu_p(a) \leq \nu_p(b)$$

  où l'on a étendu la relation d'ordre de $\mathbb{N}$ à $\mathbb{N} \cup \{+\infty\}$.
- Soient a et b deux entiers naturels non nuls et $p_1, \ldots, p_N$ leurs facteurs premiers. on a

$$\text{pgcd}(a, b) = \prod_{i=1}^{n} p_i^{\min(\nu_{p_i}(a), \nu_{p_i}(b))} \qquad \text{et} \qquad \text{ppcm}(a, b) = \prod_{i=1}^{n} p_i^{\max(\nu_{p_i}(a), \nu_{p_i}(b))}$$

Définition/Théorème 8 *Unicité de l'élément neutre et du symétrique - A énoncer et démontrer*

- Soit $\star$ une loi de composition interne sur E et e un élément de E.
  On dit que e est **élément neutre** pour $\star$ si pour tout $x \in E$, $x \star e = e \star x = x$.
  S'il existe, l'élément neutre est unique.
- Soit $\star$ une loi de composition interne sur E, admettant un élément neutre $e \in E$.
  Un élément x de E est dit **symétrisable** pour $\star$ si on a $y \in E$ tel que $x \star y = y \star x = e$.
  Pour tout $x \in E$ symétrisable, l'élément y de E tel que $x \star y = y \star x = e$ est unique et appelé symétrique de x pour $\star$ dans E.

Définition 9 *Groupe, Sous-groupe, Morphisme de groupes - A énoncer seulement*

- On appelle **groupe** tout couple $(G,\star)$ où G est un ensemble tel que
  - $\rightarrow$ $\star$ est une loi de composition interne sur G
  - $\rightarrow$ $\star$ est associative
  - $\rightarrow$ G admet un élément neutre pour $\star$
  - $\rightarrow$ tout élément de G admet un symétrique dans G pour $\star$.

  Si, de plus, $\star$ est commutative, on dit que $(G,\star)$ est un **groupe commutatif** ou **groupe abélien**.
- Soit $(G,\star)$ groupe.
  On dit que H est un **sous-groupe** de $(G,\star)$ si $H \subset G$ et $(H, \star|_{H^2})$ est un groupe.
  On note $H < G$.
- Soient $(G,\star)$ et $(G',\bullet)$ deux groupes.
  $f : (G,\star) \longrightarrow (G',\bullet)$ est un **morphisme de groupes** si et seulement si

$$\forall\,(x,y) \in G^2,\ \ f(x\star y) = f(x)\bullet f(y)$$

Proposition 10 *Caractérisation d'un sous-groupe - A énoncer seulement*

Soit $(G,\star)$ un groupe. Les propositions suivantes sont équivalentes :

(i) H est un sous-groupe de $(G,\star)$

(ii) $\begin{cases} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ H \text{ est stable par } \star \ : \ \forall\, x,y \in H,\ \ x\star y \in H \\ H \text{ est stable par inverse} \ \ : \ \forall\, x \in H,\ \ \text{sym}(x) \in H \end{cases}$

(iii) $\begin{cases} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ \forall\, x,y \in H,\ \ x\star \text{sym}(y) \in H \end{cases}$

Proposition 11 *Réunion de sous-groupes - A énoncer et à démontrer*

Soit $(G,\star)$ un groupe, H,K sont des sous groupes de $(G,\star)$, alors

$$H\cup K \text{ sous-groupe de } (G,\star) \iff H\subset K \text{ ou } K\subset H.$$

Définition/Théorème 12 *Image et noyau d'un morphisme de groupes - A énoncer et à démontrer*

- Soit $f : (G, \star) \longrightarrow (G', \bullet)$ un morphisme de groupes.
  On appelle **noyau** de f :
  $$\mathrm{Ker} f = f^{-1}(\{e_{G'}\}) = \{x \in G \mid f(x) = e_{G'}\}.$$
  Ainsi, $x \in \mathrm{Ker} f \iff f(x) = e_{G'}$.
  On appelle **image** de f :
  $$\mathrm{Im}\, f = f(G) = \{f(x),\ x \in G\}.$$
  Ainsi, $y \in \mathrm{Im}\, f \iff \exists\, x \in G,\ \ y = f(x)$.
- Soit $f : (G, \star) \longrightarrow (G', \bullet)$ un morphisme de groupe.
  $\rightarrow$ f **est injectif si et seulement si** $\mathrm{Ker} f = \{e_G\}$.
  $\rightarrow$ f **est surjectif si et seulement si** $\mathrm{Im}\, f = G'$.

Proposition 13 *Image directe/réciproque par un morphisme de groupes - A énoncer et démontrer un point*

Soit $f : (G, \star) \longrightarrow (G', \bullet)$ un morphisme de groupes.

(i) Si H est un sous-groupe de $(G, \star)$, alors $f(H)$ est un sous-groupe de $(G', \bullet)$

(ii) Si H' est un sous-groupe de $(G', \bullet)$, $f^{-1}(H')$ est un sous-groupe de $(G, \star)$.

Cas particulier : $\mathrm{Ker} f$ est un sous-groupe de G et $\mathrm{Im}\, f$ est un sous-groupe de G'.

Points du programme officiel abordés

Arithmétique

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.

Contenus	Capacités & Commentaires
PPCM.	Notation $a \vee b$.
c) Entiers premiers entre eux	
Couple d'entiers premiers entre eux. Théorème de Bézout. 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.	Forme irréductible d'un rationnel.
d) Nombres premiers	
Nombre premier. L'ensemble des nombres premiers est infini. Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.	Crible d'Ératosthène.
Pour p premier, valuation p-adique. Valuation p-adique d'un produit.	Notation $v_p(n)$. 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 $\mathbb{Z}$. Opérations sur les congruences : somme, produit. Utilisation d'un inverse modulo n pour résoudre une congruence modulo n. Petit théorème de Fermat.	Notation $a \equiv b\ [n]$. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont hors programme.

Structure de groupe

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 $\mathrm{Im}\, f$, $\mathrm{Ker} f$.
Isomorphisme.	