Mathématiques générales

4 décembre 2006

Table des matières

I	Relations	4
1	Définitions	4
2	Relations de pré ordre	4
3	Relations d'équivalence	4
3.1	Définition	4
3.2	Classes d'équivalences	5
3.3	Ensemble quotient	5
3.4	Factorisation canonique d'une application f	5
4	Relation d'ordre	5
4.1	Définition	5
4.2	Plus petit élément et plus grand élément	6
4.3	Élément minimal, éléments maximal	6
4.4	Majorant, minorant d'une partie de E	7
4.5	Borne inférieure, borne supérieure	7
II	Groupes	8
1	Définitions	8
1.1	Conséquences	8
1.2	Notations	9
1.3	Lois externes sur (G, T)	9
1.3.1	Notation multiplicative	9
1.3.2	Notation additive	9

2	Sous-groupes	9
2.1	Caractérisation	9
2.2	Étude de l'ensemble $\mathcal{G}$ des sous-groupes d'un groupe G	10
III	Groupes quotients. Morphismes	12
1	Classes modulo un sous-groupe. Sous-groupe distingué	12
1.1	Classes à gauche modulo un sous-groupe	12
1.2	Classes à droite modulo un sous-groupe	12
1.3	Théorème de Lagrange	12
1.4	Relation d'équivalence compatible avec la loi de groupe	13
2	Morphismes de groupes	14
2.1	Définition	14
2.2	Isomorphismes	14
2.3	Images directes et réciproques de sous-groupes	15
2.4	Factorisation canonique d'un morphisme de groupe	15
IV	Théorie de la division dans $\mathbb{Z}$	16
1	Les sous-groupes d'un groupe abélien	16
2	Sous-groupes de $\mathbb{Z}$, groupes quotients	16
2.1	Division euclidienne	16
2.2	Sous-groupes de $\mathbb{Z}$	16
2.3	Congruences modulo n . Groupes quotients.	16
3	Théorie du pgcd	17
3.1	Existence du pgcd	17
3.2	Algorithme d'Euclide	18
3.3	pgcd de plusieurs entiers	18
4	Théorie du ppcm	18
V	Les nombres premiers	20

1	Définition	20
2	Théorème d'Euclide	20
3	Le crible d'Eratosthène	20
4	Tests de primalité	21
5	Décomposition en nombres premiers	21
6	Le théorème de Chebyshev	22

Première partie

Relations

1 Définitions

Définition (relation) : Soit E un ensemble. Une relation $\mathcal{R}$ sur E est une partie de $E \times E$. $(x, y) \in \mathcal{R}$ est noté $x\mathcal{R}y$.

Définition (ensemble des relations) : L'ensemble des relations sur E est l'ensemble $\mathcal{P}(E \times E)$ des parties de $E \times E$.

Définition (fonction compatible) : Si E est un ensemble muni d'une relation $\mathcal{R}$, F un ensemble muni d'une relation $\mathcal{S}$ et f une fonction de E dans F . On dit que f est compatible avec les relation $\mathcal{R}$ et $\mathcal{S}$ si :

$$\forall x, y \in E, \quad x\mathcal{R}y \Rightarrow f(x)\mathcal{S}f(y)$$

2 Relations de pré ordre

Définition (pré ordre) : Un pré ordre $\mathcal{R}$ sur E est une relation sur E qui est réflexive ($\forall x \in E, x\mathcal{R}x$) et transitive ($\forall x, y, z \in E, x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$).

Définition (ensemble pré ordonné) : Un ensemble pré ordonné est un couple $(E, \mathcal{R})$ où E est un ensemble et $\mathcal{R}$ un pré ordre sur E .

3 Relations d'équivalence

3.1 Définition

Définition (relation d'équivalence) : Une relation $\mathcal{R}$ sur E est une relation d'équivalence si :

1. $\forall x \in E, x\mathcal{R}x$
2. $\forall x, y \in E, x\mathcal{R}y \Rightarrow y\mathcal{R}x$
3. $\forall x, y, z \in E, x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$

Remarque : Pour les relations d'équivalence, on utilise $x \approx y$ ou $x \equiv y \pmod{\mathcal{R}}$

3.2 Classes d'équivalences

Définition (classe d'équivalence) : Pour $x \in E$, sa classe d'équivalence est $\mathcal{C}(x) = \{y \in E \mid x\mathcal{R}y\}$. On la note parfois $\dot{x}$.

Lemme : Si $x, y \in E$, on a soit $\mathcal{C}(x) = \mathcal{C}(y)$, soit $\mathcal{C}(x) \cap \mathcal{C}(y) = \emptyset$.

3.3 Ensemble quotient

Définition (ensemble quotient) : Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence. L'ensemble quotient $E/\mathcal{R}$ est l'ensemble des classes d'équivalence de $\mathcal{R}$. C'est à dire :

$$E/\mathcal{R} = \{\mathcal{C}(x) ; x \in E\} = \{\dot{x} ; x \in E\}$$

Définition (surjection canonique) : L'application

$$\begin{aligned} s : E &\rightarrow E/\mathcal{R} \\ x &\mapsto \dot{x} = \mathcal{C}(x) \end{aligned}$$

est la surjection canonique associée.

Remarque : $\forall x, y \in E, x\mathcal{R}y \Leftrightarrow s(x) = s(y)$

3.4 Factorisation canonique d'une application f

Soit f une application d'un ensemble E dans un ensemble F . La relation $\mathcal{R}$ définie par : $x\mathcal{R}y \Leftrightarrow f(x) = f(y)$ est une relation d'équivalence sur E . Considérons les applications suivantes :

$$\begin{aligned} s : E &\rightarrow E/\mathcal{R} && \text{surjection canonique,} \\ x &\mapsto \dot{x} \end{aligned}$$

$$\begin{aligned} b : E/\mathcal{R} &\rightarrow f(E) && \text{bijection, et} \\ \dot{x} &\mapsto f(x) \end{aligned}$$

$$\begin{aligned} i : f(E) &\rightarrow F && \text{injection canonique.} \\ y &\mapsto y \end{aligned}$$

Alors $f = i \circ b \circ s$.

4 Relation d'ordre

4.1 Définition

Définition (relation d'ordre) : Une relation d'ordre est un pré ordre antisymétrique.

1. $\forall x \in E, x\mathcal{R}x$
2. $\forall x, y \in E, x\mathcal{R}y \text{ et } y\mathcal{R}x \Rightarrow x = y$
3. $\forall x, y, z \in E, x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x\mathcal{R}z$

Notation : $x\mathcal{R}y$ est noté $x \leq y$

Remarque

- Si $\mathcal{R}$ est un ordre, l'ordre $\mathcal{R}'$ opposé à $\mathcal{R}$ est défini par : $x\mathcal{R}'y \Leftrightarrow y\mathcal{R}x$
- On note $x < y \Rightarrow x \leq y$ et $x \neq y$

4.2 Plus petit élément et plus grand élément

Définition (plus petit élément) Soit A une partie de E . A a un plus petit élément s'il existe $a \in A$ tel que : $\forall x \in A, a \leq x$.

Lorsqu'il existe, un plus petit élément est unique. On note alors

$$a = \text{ppe}A = \min A = \min_{x \in A} x$$

Définition (plus grand élément) Soit A une partie de E . A a un plus grand élément s'il existe $b \in A$ tel que : $\forall x \in A, b \geq x$.

Lorsqu'il existe, un plus grand élément est unique. On note alors

$$b = \text{pge}A = \max A = \max_{x \in A} x$$

4.3 Élément minimal, éléments maximal

Définition (élément minimal, éléments maximal) : Soit A une partie de E .

a est un élément minimal de A si $a \in A$ et $\forall x \in A, x \leq a \Rightarrow x = a$.

b est un élément maximal de A si $b \in A$ et $\forall y \in A, y \geq b \Rightarrow y = b$.

Ces éléments n'existent pas toujours et ne sont pas forcément uniques.

Remarque : Dire que a n'est pas minimal dans A revient à dire que $\exists x \in A$ tel que $x < a$.

4.4 Majorant, minorant d'une partie de E

Définition (majorant, minorant) : Soit A une partie de $(E, \leq)$.
 α est un minorant de A dans E si $\alpha \in E$ et $\forall x \in A, \alpha \leq x$.
 β est un majorant de A dans E si $\beta \in E$ et $\forall x \in A, \beta \geq x$.

Définition (partie majorée, minorée, bornée) : A est majorée (resp. minorée) si A admet un majorant (resp. un minorant).
 A est bornée si elle est majorée et minorée.

Remarque : A a un ppe $\Leftrightarrow$ il existe un minorant de A qui est dans A .

4.5 Borne inférieure, borne supérieure

Soit $A \subset E$, posons :
 $m(A) = \{\text{minorants de } A\}$ et $M(A) = \{\text{majorants de } A\}$

Définition (borne inférieure) : Si l'ensemble $m(A)$ possède un pge, ce pge est appelé borne inférieure de A et on le note $\inf A = \inf_{x \in A} x$.

Définition (borne supérieure) : Si l'ensemble $M(A)$ possède un ppe, ce ppe est appelé borne supérieure de A et on le note $\sup A = \sup_{x \in A} x$.

Théorème : Si $A = \bigcup_{i \in I} A_i$ et si pour tout $i \in I$, A_i admet une borne supérieure b_i , alors l'ensemble A a une borne supérieure si et seulement si les $(b_i)_{i \in I}$ ont une borne supérieure et alors on a :

$$\sup A = \sup_{i \in I} b_i = \sup_{i \in I} \sup A_i$$

Deuxième partie

Groupes

1 Définitions

Définition (groupe) : Un groupe G est un ensemble muni d'une loi interne T vérifiant :

1. $\forall x, y, z \in G \quad (xTy)Tz = xT(yTz)$
2. $\exists e \in G, \forall x \in G \quad xTe = eTx = x$
3. $\forall x \in G, \exists x' \in G \quad xTx' = x'Tx = e$

Définition (ensemble sousjacent) : L'ensemble G est appelé ensemble sousjacent du groupe G .

Définition (groupe commutatif) : Si, de plus, on a :

$$\forall x, y \in G \quad xTy = yTx$$

le groupe G est dit commutatif ou abélien.

1.1 Conséquences

- Un groupe n'est jamais vide (il y a au moins l'élément neutre).
- Si $a \in G$, les translations :

$$\gamma_a : x \in G \mapsto aTx$$

$$\delta_a : x \in G \mapsto xTa$$

sont des permutations de G .

- Si G est fini, la table du groupe :

$$\begin{array}{cccccc}
 \nearrow T & a_1 & \cdots & a_j & \cdots & a_n \\
 a_1 & a_1Ta_1 & \cdots & a_1Ta_j & \cdots & a_1Ta_n \\
 \vdots & \vdots & & \vdots & & \vdots \\
 a_i & a_iTa_1 & \cdots & a_iTa_j & \cdots & a_iTa_n \\
 \vdots & \vdots & & \vdots & & \vdots \\
 a_n & a_nTa_1 & \cdots & a_nTa_j & \cdots & a_nTa_n
 \end{array}$$

est un carré latin.

- l'inverse x' de x est unique.

Remarque : Un carré latin n'est pas forcément une loi de groupe.

1.2 Notations

– multiplicative :

$$\mathsf{T} = \cdot, \quad x' = x^{-1}, \quad e = 1$$

– additive :

$$\mathsf{T} = +, \quad x' = -x, \quad e = 0$$

Remarque : La notation additive est réservée aux groupes commutatifs

1.3 Lois externes sur (G, T)

1.3.1 Notation multiplicative

Soit $a \in G$.

$$(n, a) \in \mathbb{N} \times G \mapsto a^n$$

$$a^0 = 1 \text{ et } a^1 = a$$

$$a^{n+1} = a^n \cdot a$$

$$a^{n+m} = a^n \cdot a^m$$

$$(a^n)^m = a^{nm}$$

$$\text{Si } G \text{ est commutatif : } (a\mathsf{T}b)^n = (a^n) \cdot (b^n).$$

1.3.2 Notation additive

Soit $a \in G$.

$$(n, a) \in \mathbb{N} \times G \mapsto na$$

$$0a = 0 \text{ et } 1a = a$$

$$(n+1)a = na + a$$

$$(n+m)a = na + ma$$

$$m(na) = (mn)a$$

$$n(a+b) = (na) + (nb).$$

2 Sous-groupes

2.1 Caractérisation

Définition (sous-groupe) : Une partie H d'un groupe G est un sous-groupe de G si H est stable par T et si la loi induite par la loi de G est une loi de groupe pour H .

Remarque :

- Un sous-groupe n'est jamais vide
- l'élément neutre de H est celui de G
- si $x \in H$, alors l'inverse de x dans H est aussi l'inverse de x dans G .

Théorème caractéristique des sous groupes : On a l'équivalence :

1. H est un sous-groupe de G
2. $H \neq \emptyset$, $\forall x, y \in H \ xTy \in H$ et $\forall x \in H \ x' \in H$
3. $H \neq \emptyset$ et $\forall x, y \in H \ xTy' \in H$

Remarque : en pratique, pour "montrer que ... est un groupe", on essaie toujours d'utiliser 2. ou 3..

2.2 Étude de l'ensemble $\mathcal{G}$ des sous-groupes d'un groupe G

L'ensemble $\mathcal{G}$ des sous-groupes de G est une partie de $\mathcal{P}(G)$ muni de l'inclusion.

Proposition :

1. $\mathcal{G}$ a un plus petit élément $\{e\}$ et un plus grand élément G .
2. Toute intersection de sous-groupes est un sous-groupe.
3. Si H est un sous-groupe de G , alors les sous-groupes de H sont les sous-groupes de G inclus dans H .

Définition (sous-groupe engendré) : Soit A une partie de G . Notons :

$$\mathcal{F} = \{H \in \mathcal{G} \mid A \subset H\}$$

On note $\langle A \rangle = \bigcap_{H \in \mathcal{F}} H$ et on l'appelle sous-groupe engendré par la partie A .

Proposition : description de $\langle A \rangle$

1. Si $A = \emptyset$, $\langle A \rangle = \{e\}$
2. Si $A \neq \emptyset$, notons $A^{-1} = \{x^{-1}; x \in A\}$ l'ensemble des inverses des éléments de A .

$$\langle A \rangle = \{x \in G \mid \exists n \in \mathbb{N}^*, \exists x_1, \dots, x_n \in A \cup A^{-1} \quad x = x_1 \cdots x_n\}$$

Définition (groupe monogène) : Un groupe G est dit monogène si $\exists x \in G$ tel que $\langle x \rangle = G$.

Troisième partie

Groupes quotients. Morphismes

1 Classes modulo un sous-groupe. Sous-groupe distingué

Soit G un groupe multiplicatif (non abélien en général), e l'élément neutre.

1.1 Classes à gauche modulo un sous-groupe

Théorème : Toute relation d'équivalence sur G compatible à gauche avec la loi de G est de la forme $x^{-1}y \in H$ où H est un certain sous-groupe de G . La classe de e est H et $\forall x \in G$, la classe de x est $xH = \{xh; h \in H\}$. Il y a bijection entre l'ensemble des relations d'équivalence compatible à gauche avec la loi de G et l'ensemble des sous-groupes de G :

$$\begin{aligned} H &\mapsto {}_H\mathcal{R} \\ e &\leftarrow \mathcal{R}_g \end{aligned}$$

On note $(G/H)_g$ l'ensemble quotient associé à ${}_H\mathcal{R}$.

$$(G/H)_g = \{\dot{x}; x \in G\} = \{xH; x \in G\}$$

1.2 Classes à droite modulo un sous-groupe

Théorème : Toute relation d'équivalence sur G compatible à droite avec la loi de G est de la forme $xy^{-1} \in H$ où H est un certain sous-groupe de G . La classe de e est H et $\forall x \in G$, la classe de x est $Hx = \{hx; h \in H\}$. Il y a bijection entre l'ensemble des relations d'équivalence compatible à droite avec la loi de G et l'ensemble des sous-groupes de G :

$$\begin{aligned} H &\mapsto \mathcal{R}_H \\ e &\leftarrow \mathcal{R}_d \end{aligned}$$

On note $(G/H)_d$ l'ensemble quotient associé à $\mathcal{R}_H$.

$$(G/H)_d = \{\dot{x}; x \in G\} = \{Hx; x \in G\}$$

1.3 Théorème de Lagrange

Définition (ordre d'un groupe) : Si G est fini, son cardinal est aussi appelé son ordre.

Théorème : Si G est un groupe fini d'ordre n , alors l'ordre de tout sous-groupe H de G divise n .

Proposition : Pour tout sous-groupe H d'un groupe G , les ensembles $(G/H)_g$ et $(G/H)_d$ sont équipotents.

Définition (indice d'un sous-groupe) : Leur cardinal commun s'appelle l'indice de H dans G et est noté $[G : H]$.

Remarque : Cette définition s'applique si H et G sont infinis.

Corollaire : Si G est un groupe fini, tout élément de G est d'ordre fini et son ordre divise l'ordre du groupe.

Corollaire : Soit G un groupe fini d'ordre n . Alors $\forall x \in G \ x^n = e$

1.4 Relation d'équivalence compatible avec la loi de groupe

Définition (relation d'équivalence compatible) : $\mathcal{R}$ est dite compatible avec la loi de G si elle est compatible à gauche et à droite.

Définition (sous-groupe distingué) : H est un sous-groupe distingué ou normal si :

1. $\forall x \in G \ xH = Hx$, ou
2. $\forall x \in G \ xHx^{-1} = H$, ou
3. $\forall x \in G \ \forall h \in H \quad xhx^{-1} \in H$

On écrit alors $H \triangleleft G$.

Théorème : $\mathcal{R}$ est une relation d'équivalence compatible avec la loi de G si et seulement si la classe $\hat{e}$ de l'élément neutre est un sous-groupe distingué H de G et si $\mathcal{R} =_H \mathcal{R} = \mathcal{R}_H$.

Définition (groupe quotient) : On définit le groupe quotient (G/H) constitué de l'ensemble quotient $(G/\mathcal{R})$ muni de la loi définie par : $\forall x, y \in G \ \hat{x}\hat{y} = \widehat{xy}$.

Remarque :

- Si G est abélien, tout sous-groupe est distingué
- En notation additive $x\mathcal{R}_Hy \Leftrightarrow x - y \in H$

2 Morphismes de groupes

2.1 Définition

Définition (morphisme) : Soient G, G' deux groupes multiplicatifs. Un morphisme $f : G \rightarrow G'$ est une application telle que :

$$\forall x, y \in G \quad f(yx) = f(x)f(y)$$

Si $G = G'$, f est un endomorphisme de G .

On note $Hom(G, G')$ l'ensemble des morphismes de G vers G' .

Proposition : Soit $f : G \rightarrow G'$ un morphisme. Alors :

1. $f(e_G) = e_{G'}$
2. $\forall x \in G, \quad \forall n \geq 1, \quad f(x^n) = f(x)^n$
3. $\forall x \in G \quad f(x^{-1}) = f(x)^{-1}$

Proposition : Si $f : G \rightarrow G'$ et $g : G' \rightarrow G''$ sont des morphismes, alors $g \circ f : G \rightarrow G''$ est un morphisme.

2.2 Isomorphismes

Définition (isomorphisme) : Un isomorphisme de G sur G' est un morphisme de G sur G' bijectif.

Proposition : Si $f : G \rightarrow G'$ est un isomorphisme, alors f^{-1} , la bijection réciproque, est un morphisme de G' sur G .

Le composé de deux isomorphismes est un isomorphisme.

Définition (automorphisme) : Un isomorphisme de G sur lui-même s'appelle un automorphisme de G .

On note $Aut(G)$ l'ensemble des automorphismes de G .

Proposition : $Aut(G)$ est un groupe pour la composition.

2.3 Images directes et réciproques de sous-groupes

Proposition : Soit f un homomorphisme de G sur G' .

1. Si H est un sous-groupe de G , alors $f(H)$ est un sous-groupe de G' . En particulier $\text{Im} f = f(G)$ est un sous-groupe de G' .
2. Si H' est un sous-groupe de G' , alors $f^{-1}(H')$ est un sous-groupe de G . En particulier $\text{Ker} f = f^{-1}(\{e\})$.

Proposition : Soit f un homomorphisme de G sur G' .

1. f est surjective si et seulement si $\text{Im} f = G'$
2. f est injective si et seulement si $\text{Ker} f = \{e\}$

2.4 Factorisation canonique d'un morphisme de groupe

Remarque : Le noyau d'un morphisme de G sur G' est un sous-groupe distingué.

$$s: G \rightarrow G/\text{Ker} f \quad \text{surjection canonique,} \\ x \mapsto \dot{x}$$

$$b: G/\text{Ker} f \rightarrow \text{Im} f \quad \text{bijection, et} \\ \dot{x} \mapsto f(\dot{x}) = f(x)$$

$$i: \text{Im} f \rightarrow G' \quad \text{injection canonique.} \\ y \mapsto y$$

Alors $f = i \circ b \circ s$.

Quatrième partie

Théorie de la division dans $\mathbb{Z}$

1 Les sous-groupes d'un groupe abélien

Proposition : Soit $(G, +)$ un groupe abélien et H, K deux sous-groupes de G . On a :

$$\inf\{H, K\} = H \cap K \text{ et}$$

$$\sup\{H, K\} = H + K = \{h + k : h \in H, k \in K\}$$

2 Sous-groupes de $\mathbb{Z}$, groupes quotients

2.1 Division euclidienne

Définition (division euclidienne) : $\forall (a, b) \in \mathbb{Z} \times \mathbb{N}^*, \exists!(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < b$.

Lemme : Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$
 $\exists!q \in \mathbb{Z}$ tel que $bq \leq a < b(q + 1)$

2.2 Sous-groupes de $\mathbb{Z}$

Théorème : Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$

2.3 Congruences modulo n . Groupes quotients.

La relation $x \equiv y \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $x - y = nk$ est une relation d'équivalence dans $\mathbb{Z}$ compatible avec l'addition et la multiplication de $\mathbb{Z}$.

Toute relation d'équivalence compatible avec l'addition dans $\mathbb{Z}$ est de la forme $x \sim y \Leftrightarrow x - y \in n\mathbb{Z}$ avec $n \in \mathbb{N}$.

L'ensemble quotient est noté $\mathbb{Z}/n\mathbb{Z}$.

Si $n = 0$, alors $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$.

Sinon $\mathbb{Z}/n\mathbb{Z}$ a n éléments $\{\hat{0}, \hat{1}, \dots, \widehat{n-1}\}$.

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe :

$$\begin{aligned} \hat{x} + \hat{y} &= \widehat{x + y} \\ \hat{x}\hat{y} &= \widehat{xy} \end{aligned}$$

3 Théorie du pgcd

3.1 Existence du pgcd

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

Il existe $d \in \mathbb{Z}^*$ tel que :

1. $d|a$ et $d|b$
2. Si $d' \in \mathbb{Z}^*$ est tel que $d'|a$ et $d'|b$, alors $d'|d$

Si, de plus, d_1 est un autre entier vérifiant ces propriétés, alors $d_1 = \pm d$

Théorème : d est un pgcd de a et b si et seulement si :

1. $d|a$ et $d|b$
2. $\exists(u, v) \in \mathbb{Z}^2$ tels que $d = au + bv$

Corollaire : $\text{pgcd}(ac, bc) = c \text{pgcd}(a, b)$

Corollaire : si $d|a$ et $d|b$, alors :

$$\text{pgcd}(a, b) = d \Leftrightarrow \text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Définition (nombres premiers entre eux) : Soient $(a, b) \in \mathbb{Z}^2$.

Si $\text{pgcd}(a, b) = 1$, alors a et b sont dits premiers entre eux.

Notation : $\text{pgcd}(a, b) = a \wedge b$

Théorème : Il y a équivalence entre :

1. a et b sont premiers entre eux
2. $\exists(p, q) \in \mathbb{Z}^2$ tels que $ap + bq = 1$
3. $\forall z \in \mathbb{Z}, \exists(x, y) \in \mathbb{Z}^2$ tel que $z = ax + by$
4. $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

Théorème de Gauss : Si $a|bc$ et $a \wedge b = 1$, alors $a|c$

Corollaire : Si a est premier avec b_1 et b_2 , alors il est premier avec b_1b_2

3.2 Algorithme d'Euclide

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$

On construit la suite $(r_i)_{i \in \mathbb{N}}$ par :

$$r_0 = a, r_1 = b$$

$$\forall i \geq 2, \quad r_{i-2} = r_{i-1}q_i + r_i \quad \text{avec } 0 \leq r_i < r_{i-1}$$

La suite des r_i est strictement décroissante et minorée par 0, elle est donc finie.

Le dernier reste non nul est le pgcd de a et b .

3.3 pgcd de plusieurs entiers

Si $a_1, \dots, a_p$ sont p éléments de $\mathbb{Z}$, ils ont un pgcd d qui vérifie :

1. $\forall i \in \{1, \dots, p\}, d|a_i$
2. $\forall \delta \in \mathbb{Z} [\forall i \in \{1, \dots, p\}, \delta|a_i] \Rightarrow \delta|d$

On a également

- $a_1\mathbb{Z} + \dots + a_p\mathbb{Z} + d\mathbb{Z}$
- $\exists u_1, \dots, u_p \in \mathbb{Z}$ tels que : $d = a_1u_1 + \dots + a_pu_p$

Définition (nombres premiers entre eux) : $a_1, \dots, a_p$ sont dits premiers entre eux si le pgcd est 1.

Théorème : $\text{pgcd}(a_1, \dots, a_p) = 1 \Leftrightarrow \exists u_1, \dots, u_p \in \mathbb{Z}$ tels que :
 $a_1u_1 + \dots + a_pu_p = 1$

Remarque : $a_1, \dots, a_p$ sont premiers entre eux $\neq a_1, \dots, a_p$ sont 2 à 2 premiers entre eux

4 Théorie du ppcm

Théorème : Si $a, b \in \mathbb{Z}^*$, il existe $m \in \mathbb{Z}$ tel que :

1. $a|m$ et $b|m$
2. $\forall x \in \mathbb{Z}, a|x$ et $b|x \Rightarrow m|x$

Remarque : $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

Théorème : Il y a équivalence entre :

1. a et b sont premiers entre eux
2. $\forall x \in \mathbb{Z}, a|x \text{ et } b|x \Rightarrow ab|x$
3. $\text{ppcm}(a, b) = ab$

Corollaire : Pour tout $a, b \in \mathbb{Z}$, $\text{pgcd}(a, b)\text{ppcm}(a, b) = ab$

Notation : $\text{ppcm}(a, b) = a \vee b$

Cinquième partie

Les nombres premiers

1 Définition

Définition (nombre premier) : Un nombre $p \in \mathbb{Z}$ est dit premier s'il n'est ni nul, ni inversible et si ses seuls diviseurs sont les inversibles et ses associés.

Lemme : Si p est premier et $a \in \mathbb{Z}$, alors $p \wedge a = 1$ ou $p|a$

2 Théorème d'Euclide

Théorème : Tout nombre de $\mathbb{Z} - \{-1; 0; 1\}$ peut s'écrire comme un produit de nombres premiers.

Théorème d'Euclide : L'ensemble des nombres premiers est infini.

3 Le crible d'Eratosthène

Méthode : On écrit la liste des entiers et on barre le 1.

On entoure le 1^{er} nombre non barré et on barre tous ses multiples.

On répète cette opération jusqu'à ce que tous les nombres soient entourés ou barrés.

Les nombres entourés sont les nombres premiers.

Formule de Legendre pour le crible Soient $m \in \mathbb{N}$ et $x \in \mathbb{N}$.

Notons $N_m(x) = \text{card} \{n \leq x \mid n \wedge m = 1\}$.

Alors :

$$N_m(x) = \sum_{\substack{d \in \mathbb{N} \\ d|m}} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor$$

avec $\mu(d)$ la fonction de Mobus :

$$\mu(d) = \begin{cases} (-1)^{\omega(d)} & \text{si } d \text{ n'a pas de facteur carré} \\ 0 & \text{sinon} \end{cases}$$

et $\omega(d)$ le nombre de facteurs premiers de d .

Fonction d'Euler :

$$\varphi(n) = N_n(n) = n \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right)$$

4 Tests de primalité

Problème : étant donné $n \in \mathbb{N}$, on veut savoir si n est premier.

1^{er} test : On divise n par tous les entiers $i \in \{2, \dots, n-1\}$.
On fait $n-2$ divisions : test en $o(n)$

2^e test : On divise n par tous les entiers $i \in \{2, \dots, \lfloor \sqrt{n} \rfloor\}$.
On fait $\lfloor \sqrt{n} \rfloor - 1$ divisions : test en $o(\sqrt{n})$

3^e test : On divise n par 2 puis par tous les entiers impaires de 3 à $\lfloor \sqrt{n} \rfloor$.
On fait $\left\lfloor \frac{\lfloor \sqrt{n} \rfloor + 1}{2} \right\rfloor$ divisions : test en $o\left(\frac{\sqrt{n}}{2}\right)$

Remarque : en 2002 : Algorithme AKS en $o((\ln n)^{11})$

5 Décomposition en nombres premiers

Théorème : Tout entier relatif non nul et non inversible se décompose de façon essentiellement unique en un produit de nombres premiers.

Définition (essentiellement unique) : unique à l'ordre et au signe près.

Lemme : Si p est premier et $p|ab$, alors $p|a$ ou $p|b$.

Remarque : Soit $\mathcal{P}$ une collection d'entiers contenant un représentant de chaque nombre premier.

Tout nombre entier $a \in \mathbb{Z}^*$ s'écrit de manière unique

$$a = \pm \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

avec $v_p(a)$ la puissance de p dans la décomposition en facteurs premiers de a . $v_p(a) \in \mathbb{N}$, les $v_p(a)$ sont nuls sauf un nombre fini.

Remarque : Si $a = \pm \prod_{p \in \mathcal{P}} p^{v_p(a)}$ et $b = \pm \prod_{p \in \mathcal{P}} p^{v_p(b)}$ alors :

$$\text{pgcd}(a, b) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a), v_p(b)\}}$$

$$\text{ppcm}(a, b) = \prod_{p \in \mathcal{P}} p^{\max\{v_p(a), v_p(b)\}}$$

6 Le théorème de Chebyshev

Notons $\pi(x) = \text{card} \{p \leq x \mid p \text{ premier}\}$.

$$\lim_{x \rightarrow +\infty} \pi(x) = +\infty$$

Théorème des nombres premiers :

$$\pi(x) \approx \frac{x}{\ln x}$$

Index

- algorithme d'Euclide, 18
- automorphisme, 14

- borne inférieure, 7
- borne supérieure, 7

- classe d'équivalence, 5
- crible d'Eratosthène, 20

- division euclidienne, 16

- élément maximal, 6
- élément minimal, 6
- endomorphisme, 14
- ensemble des relations, 4
- ensemble pré ordonné, 4
- ensemble quotient, 5
- ensemble sousjacent, 8
- essentiellement unique, 21

- fonction compatible, 4

- groupe, 8
- groupe abélien, 8
- groupe commutatif, 8
- groupe monogène, 11
- groupe quotient, 13

- indice d'un sous-groupe, 13
- isomorphisme, 14

- majorant, 7
- minorant, 7
- morphisme, 14

- nombre premier, 20
- nombres premiers entre eux, 17, 18

- ordre d'un groupe, 12

- partie bornée, 7

- partie majorée, 7
- partie minorée, 7
- pgcd, 17
- plus grand élément, 6
- plus petit élément, 6
- pré ordre, 4

- relation, 4
- relation d'équivalence, 4
- relation d'équivalence compatible, 13
- relation d'ordre, 5

- sous-groupe, 9
- sous-groupe distingué, 13
- sous-groupe engendré, 10
- sous-groupe normal, 13
- surjection canonique, 5

- théorème caractéristique des sous groupes,
10
- théorème d'Euclide, 20
- théorème de Bezout, 17
- théorème de Gauss, 17
- théorème des nombres premiers, 22