

Structures algébriques usuelles

B. Seddoug. Médiane Sup, Oujda

I Structure de groupe

I.1 Définition-Exemples

Définition 1 (groupe) On appelle groupe tout monoïde dans lequel tout élément est symétrisable. i.e: (G, \cdot) est un groupe si:

- La loi est associative: $\forall (x, y, z) \in G^3, x(yz) = (xy)z$.
- La loi admet un élément neutre $e : \forall x \in G, xe = ex = x$.
- Tout élément est symétrisable: $\forall x \in G, \exists x' \in G \mid xx' = x'x = e$.

On dit alors que (G, \cdot) est un groupe. Si en plus la loi est commutative on dit que G est un groupe abélien.

Remarque 1 Dans le cas de groupe abélien, on utilise par fois une notation additive et note le neutre par 0, le symétrique de x est noté $-x$. Dans le cas général, on utilise une loi sans symbole et le symétrique de x est noté x^{-1} .

Exemple 1

1. $(\mathbb{N}, +)$ n'est pas un groupe.
2. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ et (\mathbb{R}_+^*, \times) sont des groupes abéliens.
3. L'ensemble des permutations (bijections) d'un ensemble E est un groupe pour la composition des application on le note S_E et on l'appelle le groupe symétrique de E .

P I.1 Dans un groupe tout élément est régulier.

i.e: $\forall x \in G : \forall (y, z) \in G^2, xy = xz \implies y = z$.
 $\forall (y, z) \in G^2, yx = zx \implies y = z$.

Exemple 2 (Groupe à deux éléments) Soit $G = \{e; a\}$ une loi de groupe sur G est représentée par la table suivante, on remarque qu'il est abélien:

.	e	a
e	e	a
a	a	e

table de groupe à deux éléments.

Exemple 3 (Groupe à trois éléments) Soit $G = \{e; a; b\}$ une loi de groupe sur G est représentée par la table suivante, on remarque qu'il est abélien:

.	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

table de groupe à trois éléments.

Exercice 1 Donner les tables possibles d'un groupe à 4 éléments.

I.2 Sous groupe

Définition 2 (Sous groupe) On appelle sous groupe d'un groupe (G, \cdot) toute partie H de G stable pour la loi et telle que (H, \cdot) soit un groupe.

Propriétés

P I.2 Si H est un sous groupe de G alors $e_H = e_G$, (même élément neutre). Et pour élément $x \in H$, son symétrique dans H est celui dans G .

P I.3 Propriété caractéristique

Soit $H \subset G$, H est un sous groupe de G si et seulement si

- (i) $H \neq \emptyset$.
- (ii) $\forall (x, y) \in H : xy \in H$.
- (iii) $\forall x \in H : x^{-1} \in H$.

Les conditions (ii) et (iii) peuvent être remplacées par l'unique condition

- (iv) $\forall (x, y) \in H : xy^{-1} \in H$.

P I.4 Intersection de sous groupes

Toute intersection de sous groupes de G est un sous groupe de G .

Remarque 2 L'union de sous groupe n'est pas toujours un sous groupe.

Exemple 4

1. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont deux sous groupes de $(\mathbb{R}, +)$.
2. G et $\{e_G\}$ sont deux sous groupe de G .
3. Centre d'un groupe
Soit G un groupe, on note $C = \{g \in G \mid \forall x \in G : gx = xg\}$. C est un sous groupe de G appelé le centre de G .
4. **Sous groupes additifs de \mathbb{R}**
Soit $G \neq \{0\}$ un sous groupe de $(\mathbb{R}, +)$. On note $a = \inf G \cap \mathbb{R}_+^*$.
 - Si $a > 0$ on montre que $G = a\mathbb{Z}$, on dit que G est discret.
 - Si $a = 0$ on montre que G est dense dans \mathbb{R} .

En effet: 1^{er} cas: D'abord $G \cap \mathbb{R}_+^* \neq \emptyset$ et a existe.

Si $a > 0$ alors $a \in G$, si non $\exists x, y \in G$ tel que $a < x < y < 2a$ et par suite $y - x \in G$ ce qui absurde car $0 < y - x < a$.

Donc $a \in G$ et par suite $a\mathbb{Z} \subset G$.

Réciproquement soit $x \in G, \exists (n, r) \in \mathbb{Z} \times [0, a[$ | $x = na + r$ donc $r = x - na \in G$ et par suite $r = 0$ et donc $x \in a\mathbb{Z}$.

2^{ème} cas: si $a = 0$ alors $\forall x < y \in \mathbb{R}, \exists z \in G$ | $0 < z < y - x$. La division de y par z donne n et $r \in [0, z[$ tels que $y = nz + r$.

Donc $0 \leq r = y - nz < z < y - x$ c.à.d $x - y < nz - y \leq 0$ ou $x < nz \leq y$. cqfd .

I.3 Morphisme de groupe

Définition 3 (homomorphisme) Soient G et G' deux groupes. Une application $f : G \rightarrow G'$ est appelé *homomorphisme* de groupes si

$$\forall (x, y) \in G^2 : f(xy) = f(x)f(y).$$

Si en plus f est bijective, on dit que f est un *isomorphisme*.

Si $G = G'$ on dit que f est *endomorphisme* et *automorphisme* dans le cas f bijective.

Exemple 5

1. Id_G est un automorphisme de G .

2. $(\mathbb{R}, +) \xrightarrow{\exp} (\mathbb{R}_+^*, \times), x \mapsto \exp x$ est un isomorphisme. Sa bijection réciproque: $(\mathbb{R}_+^*, \times) \xrightarrow{\ln} (\mathbb{R}, +), x \mapsto \ln x$ est aussi un isomorphisme.

Propriétés

P I.5 La composée de deux morphismes est un morphisme.

P I.6 Si f est un isomorphisme, f^{-1} est aussi un isomorphisme.

P I.7 Si $f : G \rightarrow G'$ est un morphisme alors

- $f(e_G) = e_{G'}$.
- $\forall x \in G : f(x^{-1}) = [f(x)]^{-1}$.

Théorème I.1 Soit $f : G \rightarrow G'$ un morphisme de groupes.

- Pour tout sous groupe H de G , $f(H)$ est un sous groupe de G' .
- Pour tout sous groupe H' de G' , $f^{-1}(H')$ est un sous groupe de G .

En particulier $\text{Im } f$ est un sous groupe de G' et $f^{-1}\{e_{G'}\}$ est un sous groupe de G .

Définition 4 (Noyau) Le sous groupe $f^{-1}\{e_{G'}\}$ de G est appelé le *noyau* de f . On le note $\ker f$.

Théorème I.2 Soit $f : G \rightarrow G'$ un morphisme de groupes.

- f est injective si et seulement si $\ker f = \{e_G\}$.
- f est surjective si et seulement si $\text{Im } f = G'$.

I.4 Le groupe $(\mathbb{Z}, +)$ des entiers relatifs

$(\mathbb{Z}, +)$ est un groupe abélien d'élément neutre 0.

Si G est un groupe noté multiplicativement, pour tout $x \in G$ et pour tout $m \in \mathbb{N}^*$, le produit $\prod_{i=1}^m x$ est noté x^m .

On pose $x^0 = e_G$ et si $m \in \mathbb{Z}_-^*$, on pose $x^m = (x^{-1})^{-m}$.

Si G est un groupe noté additivement, pour tout $x \in G$ et pour tout $m \in \mathbb{N}^*$, la somme $\sum_{k=1}^m x$ est noté mx .

On pose $0x = 0_G$ et si $m \in \mathbb{Z}_-^*$, on pose $mx = (-m)(-x)$.

Théorème I.3 Soit G un groupe noté multiplicativement, pour tout $a \in G$, l'application

$$\begin{aligned} \varphi_a : \mathbb{Z} &\rightarrow G \\ m &\mapsto a^m \end{aligned}$$

est un morphisme de groupes. Et pour tout morphisme $\varphi : \mathbb{Z} \rightarrow G$, il existe $a \in G$ tel que $\varphi = \varphi_a$.

Preuve: On montre que φ_a est morphisme en distinguant les cas.

Réciproquement si $\varphi : \mathbb{Z} \rightarrow G$ est un morphisme, $a = \varphi(1)$ répond à la question.

En effet $\forall m \in \mathbb{Z}_+^* : \varphi(m) = \varphi(\underbrace{1 + \dots + 1}_{m \text{ fois}}) = \underbrace{\varphi(1) \dots \varphi(1)}_{m \text{ fois}} = \varphi(1)^m = \varphi_a(m)$.

L'égalité s'étend sans difficulté à \mathbb{Z} tout entier .

II Anneaux et Corps

II.1 Définitions-Exemples

Définition 5 (Anneau) Soit A un ensemble muni de deux lois de composition interne notées $+$ et \times (ou sans symbole) on dit $(A, +, \times)$ est un *anneau* si:

(A1) $(A, +)$ est un groupe abélien (on note 0_A son élément neutre).

(A2) \times est associative, admet un neutre (noté 1_A) et distributive par rapport à $+$.
Si en plus la loi \times est commutative l'anneau est dit commutatif.

Définition 6 Si $(A, +, \times)$ est un anneau commutatif, on dit que A est un corps si en plus

- $0_A \neq 1_A$.
- Tout élément non nul (i.e: $\neq 0_A$) est inversible pour la loi \times . On note alors l'inverse de x par x^{-1} ou $\frac{1}{x}$.

Exemple 6

1. $(\mathbb{Z}, +, \times), (\mathbb{R}^N, +, \times)$ sont des anneaux commutatifs.
2. $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ sont des corps.

Remarque 3 Si A est un singleton $\{a\}$, on peut définir une structure d'anneau en posant: $a + a = a \times a = a$ et donc $0_A = 1_A = a$. Cet anneau est appelé *l'anneau nul*. Un corps peut être réduit à la paire $\{0; 1\}$.

Définition 7 (Sous anneau) Soit A un anneau et B une partie de A . On dit que B est un sous anneau de A si

- $(B, +)$ est un sous groupe de $(A, +)$.
- B est stable par la loi \times : $\forall x, y \in B, x \times y \in B$.
- $1_A \in B$.

Dans ce cas les lois de A induisent une structure d'anneau sur B .

Proposition 1 (Propriété caractéristique d'un sous anneau) Soit A un anneau et B une partie de A . B est un sous anneau de A si et seulement si

- $1_A \in B$.
- $\forall (x, y) \in B : x \times y \in B$ et $x - y \in B$.

P II.1 (Intersection de sous anneaux) Toute intersection de sous anneaux de A est un sous anneau de A .

Définition 8 (Sous corps) Soit K un corps et L une partie de K . On dit que L est un sous corps de K si

- $(L, +, \times)$ est un sous anneau de $(K, +, \times)$.
- $\forall x \in L \setminus \{0_K\} : x^{-1} \in L$.

Proposition 2 (Propriété caractéristique d'un sous corps) Soit K un corps et L une partie de K . L est un sous corps de K si et seulement si

- $1_K \in L$.
- $\forall (x, y) \in L : x \times y \in L$ et $x - y \in L$.
- $\forall x \in L \setminus \{0_K\} : x^{-1} \in L$.

P II.2 (Intersection de sous corps) Toute intersection de sous corps de K est un sous corps de K .

Définition 9 (Morphisme d'anneaux) Soient deux anneaux A et A' . On dit qu'une application $f : A \rightarrow A'$ est morphisme d'anneaux si

- $\forall x, y \in A : f(x + y) = f(x) + f(y)$ et $f(x \times y) = f(x) \times f(y)$.
- $f(1_A) = 1_{A'}$.

Si A et A' sont des corps, le morphisme est dit morphisme de corps.

Exercice 2 Déterminer tous les morphismes de l'anneau \mathbb{Z} vers un anneau A .

II.2 Règles de calcul dans un anneau

On considère un anneau $(A, +, \times)$. On a les règles de calcul suivantes:

$$\text{P II.3 } \forall x \in A : 0_A \times x = x \times 0_A = 0_A.$$

$$\text{P II.4 } \forall x \in A : -x = (-1_A) \times x = x \times (-1_A).$$

$$\text{P II.5 } \forall x, y \in A : (-x) \times y = x \times (-y) = -x \times y \text{ et } (-x) \times (-y) = x \times y.$$

Notations

Pour tout $n \in \mathbb{N}$, et pour tout $x \in A$, on note

$$\bullet nx = \begin{cases} \underbrace{x + x + \dots + x}_{n \text{ fois}} & \text{si } n \neq 0 \\ 0 & \text{si } n = 0. \end{cases};$$

$$\bullet (-n)x = n(-x).$$

$$\bullet x^n = \begin{cases} \underbrace{x \times x \times \dots \times x}_{n \text{ fois}} & \text{si } n \neq 0 \\ 1_A & \text{si } n = 0. \end{cases};$$

$$\bullet x^{-n} \text{ n'a de sens que si } x \text{ est inversible.}$$

P II.6 (Binôme de Newton) Si $(x, y) \in A^2$ tel que $x \times y = y \times x$, alors pour tout $n \in \mathbb{N}$, on a

$$(x + y)^n = \sum_{k=0}^n C_n^k x^k y^{n-k}$$

Et pour tout $n \in \mathbb{N}^*$, on a:

$$x^n - y^n = (x - y) \left(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1} \right) = (x - y) \sum_{k=0}^{n-1} x^{n-1-k} y^k.$$

Preuve: Par récurrence sur n et à l'aide des formules de Pascal.

Pour la formule de factorisation, on raisonne par récurrence en remarquant que

$$\begin{aligned} x^{n+1} - y^{n+1} &= xx^n - xy^n + xy^n - yy^n \\ &= x(x^n - y^n) + (x - y)y^n \end{aligned}$$

$$\text{Donc } x^{n+1} - y^{n+1} = (x - y) \left(\sum_{k=0}^{n-1} x^{n-k} y^k + y^n \right) = (x - y) \left(\sum_{k=0}^n x^{n-k} y^k \right). \text{ cqfd.}$$

Conséquence La somme des n premiers termes d'une suite géométrique

Pour tout $x \in A$, si $1_A - x$ est inversible alors pour tout $n \in \mathbb{N}$, on a

$$1 + x + x^2 + \dots + x^n = \frac{1 - x^{n+1}}{1 - x}.$$

Définition 10 (éléments nilpotents dans un anneau) Un élément $a \neq 0_A$ d'un anneau A est dit nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0_A$. Le plus petit entier n vérifiant $a^n = 0$ s'appelle l'indice de nilpotence de l'élément a .

Proposition 3 Si a est nilpotent d'indice n alors $1_A - x$ est inversible et on a

$$(1 - x)^{-1} = 1 + x + x^2 + \dots + x^{n-1}.$$

II.3 Groupe $\mathcal{U}(\mathbf{A})$ des éléments inversibles

Théorème II.1 Soit un anneau $(\mathbf{A}, +, \times)$. On note $\mathcal{U}(\mathbf{A})$ l'ensemble des éléments inversibles pour la loi \times :

$$\mathcal{U}(\mathbf{A}) = \{a \in \mathbf{A} \mid \exists a' \in \mathbf{A} : aa' = a'a = 1_{\mathbf{A}}\}$$

Alors muni de la seconde loi de l'anneau, l'ensemble $(\mathcal{U}(\mathbf{A}), \times)$ a une structure de groupe: c'est le groupe des unités de l'anneau \mathbf{A} .

Exemple 7 $\mathcal{U}(\mathbb{Z}) = \{-1; 1\}$, dans un anneau \mathbf{A} quelconque on a $\{-1_{\mathbf{A}}; 1_{\mathbf{A}}\} \subset \mathcal{U}(\mathbf{A})$. Si \mathbf{A} est un corps alors $\mathcal{U}(\mathbf{A}) = \mathbf{A} \setminus \{0_{\mathbf{A}}\}$.

II.4 Anneau intègre

Définition 11 (Diviseur de zéro) Soit un anneau $(\mathbf{A}, +, \times)$ non nul. Un élément $a \neq 0$ de \mathbf{A} est appelé diviseur de zéro s'il existe $b \neq 0$ tel que $a \times b = 0_{\mathbf{A}}$ ou $b \times a = 0_{\mathbf{A}}$.

Exemple 8 Dans $\mathbf{A} = \mathbb{R}^{\mathbb{R}}$ on considère $f, g : \mathbb{R} \rightarrow \mathbb{R}$ telles que:

$$\begin{cases} f(x) = 1 \text{ si } x > 0, \\ f(x) = 0 \text{ si non} \end{cases} \quad \text{et} \quad \begin{cases} g(x) = 0 \text{ si } x > 0, \\ g(x) = 1 \text{ si non.} \end{cases}$$

On a $fg = gf = 0$ mais $f \neq 0_{\mathbf{A}}$ et $g \neq 0_{\mathbf{A}}$...

Définition 12 (Anneau intègre) On dit qu'un anneau $(\mathbf{A}, +, \times)$ non nul est intègre s'il commutatif et sans diviseurs de zéro:

1. La loi \times est commutative;
2. $\forall x, y \in \mathbf{A} : x \times y = 0_{\mathbf{A}} \implies x = 0_{\mathbf{A}}$ ou $y = 0_{\mathbf{A}}$.

Remarque 4 Dans un anneau intègre, on peut (simplifier) à gauche et à droite:

$$\forall a, x, y \in \mathbf{A} : ax = ay \implies x = y \text{ et } xa = ya \implies x = y.$$

Cette propriété est fautive dans un anneau non intègre. On dit alors que tout élément est régulier.

Exemple 9

1. Tout corps est intègre et tout sous anneau d'un corps est intègre.
2. Les anneaux $\mathbb{R}^{\mathbb{N}}$ et $\mathbb{R}^{\mathbb{R}}$ ne sont pas intègres...

Corps des fractions d'un anneau intègre

Théorème II.2 (admis) Soit un anneau $(\mathbf{A}, +, \times)$ intègre. Il existe un corps \mathbf{K} unique, à isomorphisme près, tel que \mathbf{A} soit un sous anneau de \mathbf{K} et tout élément de \mathbf{K} s'écrit sous la forme $\frac{a}{b}$ avec $a, b \in \mathbf{A}$ et $b \neq 0_{\mathbf{A}}$. à isomorphisme près: si \mathbf{K}' est un corps vérifiant les mêmes propriétés alors il existe un isomorphisme de corps entre \mathbf{K} et \mathbf{K}' . \mathbf{K} est alors appelé le corps des fractions de \mathbf{A} .

Exemple 10 \mathbb{Q} est le corps des fractions de \mathbb{Z} .

II.5 L'anneau \mathbb{Z} des entiers relatifs

II.5.1 Divisibilité dans \mathbb{Z}

Définition 13 Soient a et b deux entiers relatifs. On dit que b divise a s'il existe $q \in \mathbb{Z}$ tel que $a = qb$. On note alors b/a . Si b divise a , on dit que a est un multiple de b .

Remarque 5 Ces définitions s'étendent à un anneau quelconque.

Exemple 11

- $\forall n \in \mathbb{Z} : n/0$.
- $\forall n \in \mathbb{Z} : 0/n \iff n = 0$.

Proposition 4 Soient a, b dans \mathbb{Z} , on a les équivalences suivantes:

$$\begin{aligned} a/b &\iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subset a\mathbb{Z} \\ (a/b \text{ et } b/a) &\iff b\mathbb{Z} = a\mathbb{Z} \iff a = b \text{ ou } a = -b. \end{aligned}$$

Théorème II.3 (Division euclidienne) $\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}, \exists!(q, r) \in \mathbb{Z} \times \mathbb{Z} \mid a = bq + r$ et $0 \leq r < |b|$.
 q est appelé quotient et r le reste dans la division euclidienne de a par b .

Preuve: 1^{er} cas: $a, b \in \mathbb{N}$, déjà démontré.

2^{ème} cas: En général $|a| = |b|q' + r'$, donc $a = b \cdot \text{signe}(ab) \cdot q' + \text{signe}(a) \cdot r'$.

Alors si $a \geq 0$, on pose $r = r'$ et $q = \text{signe}(ab) \cdot q'$, et si $a < 0$, on pose $r = \text{signe}(a) \cdot r' + |b|$ et $q = \text{signe}(ab) \cdot q' - \text{signe}(b)$.

Pour l'unicité c'est le même raisonnement que dans le cas de \mathbb{N} . •

Algorithme de la division euclidienne

On suppose a et b deux entiers naturels $b > 0$.

1. Initialisation: $q \leftarrow 0$;
2. Tant que $a \geq b$
Faire
 $q \leftarrow q + 1; a \leftarrow a - b$;
Fin Faire
3. $r \leftarrow a$;
4. Résultat: $q; r$.

Exemple 12 $a = 17; b = 3$

$$\begin{array}{cccccc} a & 17 & 14 & 11 & 8 & 5 & 2 \\ q & 0 & 1 & 2 & 3 & 4 & 5 \end{array} \quad \text{donc } r = 2 \text{ et } q = 5, \text{ soit } 17 = 5 \times 3 + 2.$$

Théorème II.4 (Sous groupe de $(\mathbb{Z}, +)$) Les sous groupes de \mathbb{Z} sont les ensembles de la forme

$$a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$$

où $a \in \mathbb{Z}$.

Preuve: Soit $\mathbf{G} \neq \{0\}$ un sous groupe de \mathbb{Z} . On considère $a = \min \mathbf{G} \cap \mathbb{N}^*$, et on montre que $\mathbf{G} = a\mathbb{Z}$.

On a $a \in \mathbf{G}$ donc $a\mathbb{Z} \subset \mathbf{G}$. Et réciproquement si $m \in \mathbf{G}$ la Division Euclidienne de m par a donne $m = qa + r$ donc $r = m - qa \in \mathbf{G} \cap \llbracket 1, a \rrbracket$, donc $r = 0$. •

II.5.2 Ordre d'un élément dans un groupe

Soit \mathbf{G} un groupe et $a \in \mathbf{G}$. On considère le morphisme de groupes

$$\begin{aligned} \varphi_a \quad \mathbb{Z} &\longrightarrow \mathbf{G} \\ n &\longmapsto a^n \quad (na \text{ si } \mathbf{G} \text{ est noté additivement.}) \end{aligned}$$

Son noyau $\ker \varphi_a$ est un sous groupe de $(\mathbb{Z}, +)$, donc il existe un unique $n \in \mathbb{N}$ tel que $\ker \varphi_a = n\mathbb{Z}$. Si φ_a n'est pas injective $n \in \mathbb{N}^*$.

Définition 14 (Ordre d'un élément) Si φ_a n'est pas injective, l'unique entier n tel que $\ker \varphi_a = n\mathbb{Z}$ est appelé l'ordre de a .

Si φ_a est injective alors $\forall n \in \mathbb{N}^* : a^n \neq e_{\mathbf{G}}$. On dit que a est d'ordre infini.

Remarque 6 Par définition si $\text{ordre}(a) = n \in \mathbb{N}^*$, alors n est le plus petit entier naturel non nul vérifiant $a^n = e_{\mathbf{G}}$ (ou $na = 0_{\mathbf{G}}$ dans le cas additif):

$$\text{ordre}(a) = \min \{m \in \mathbb{N}^* \mid a^m = e_{\mathbf{G}}\}.$$

Proposition 5 (Caractérisation de l'ordre d'un élément) Soit \mathbf{G} un groupe et $a \in \mathbf{G}$, alors on a l'équivalence suivante

$$\text{ordre}(a) = n \iff \begin{cases} a^n = e_{\mathbf{G}}; \\ \forall k \in \mathbb{N} : [a^k = e_{\mathbf{G}} \implies n/k]. \end{cases}$$

Exemple 13

1. $\text{ordre}(e_{\mathbf{G}}) = 1$.
2. $\mathbf{G} = \{-1; 1\}$ muni de la multiplication $\text{ordre}(-1) = 2$.
3. Dans (\mathbb{C}^*, \times) , $\text{ordre}(i) = 4$; $\text{ordre}(j = e^{i\frac{2\pi}{3}}) = 3$; en général $\text{ordre}(e^{i\frac{2\pi}{n}}) = n$.

Définition 15 (Sous groupe engendré par un élément) Soit \mathbf{G} un groupe et $a \in \mathbf{G}$. Le sous groupe $\text{Im } \varphi_a = \{a^n \mid n \in \mathbb{Z}\}$ de \mathbf{G} est appelé sous groupe engendré par a . On le notera $\langle a \rangle$.

Théorème II.5 (Description de $\langle a \rangle$) Soit \mathbf{G} un groupe et $a \in \mathbf{G}$ d'ordre fini $n \in \mathbb{N}^*$. Le groupe engendré par a est fini de cardinal n et l'application

$$\begin{aligned} \llbracket 0, n-1 \rrbracket &\longrightarrow \langle a \rangle \\ k &\longmapsto a^k \end{aligned}$$

est bijective. i.e: $\langle a \rangle = \{e_{\mathbf{G}} = a^0; a; a^2; \dots; a^{n-1}\}$.

Remarque 7 Dans la cas additif remplacer a^k par ka et $e_{\mathbf{G}}$ par $0_{\mathbf{G}}$.

Preuve: D'abord $\forall k, k' \in \llbracket 0, n-1 \rrbracket$:

$$a^k = a^{k'} \iff \varphi_a(k) = \varphi_a(k') \iff k - k' \in \ker \varphi_a \iff k - k' = 0.$$

D'autre part $\forall k \in \mathbb{Z}$, la D.E de k par n donne $k = aq + r$ et $a^k = a^r$ avec $r \in \llbracket 0, n-1 \rrbracket$.

Remarque 8 Si a est d'ordre infini $\langle a \rangle$ est isomorphe à \mathbb{Z} .

Définition 16 (Groupe monogène, groupe cyclique) Un groupe \mathbf{G} est dit *monogène* s'il existe $a \in \mathbf{G}$ tel que $\mathbf{G} = \langle a \rangle$. Si en plus a est d'ordre fini \mathbf{G} est dit *cyclique*, dans ce cas $\mathbf{G} = \{e_{\mathbf{G}} = a^0; a; a^2; \dots; a^{n-1}\}$, l'ordre de a est aussi appelé l'ordre de \mathbf{G} .

Exemple 14 Tout groupe à deux éléments ou à trois éléments est cyclique.

Exercice 3 Donner un groupe cyclique à 4 éléments; à n éléments $n \geq 1$.

Proposition 6 Tout groupe monogène est abélien.

Remarque 9 Si \mathbf{G} est un groupe et A une partie non vide de \mathbf{G} . On définit le sous groupe de \mathbf{G} engendré par A comme étant l'intersection de tous les sous groupes contenant A .

Arithmétique élémentaire

B. Seddoug. Médiane Sup, Oujda.

I Numération

I.1 Définition - Exemples

Théorème I.1 Soit $q \in \mathbb{N}, q \geq 2$. Pour tout entier $N \in \mathbb{N}$, il existe une unique suite $(s_n)_{n \in \mathbb{N}}$ nulle à partir d'un certain rang telle que

$$N = s_0 + s_1q + \dots + s_nq^n \text{ avec } n = \max \{k \in \mathbb{N} \mid s_k \neq 0\} \quad (I.1)$$

Définition 1 Si N vérifie (I.1), on écrit

$$N = \overline{s_n s_{n-1} \dots s_0}^q \quad (I.2)$$

L'écriture (I.2) est appelé la représentation de N en base q (ou dans le système à base q).

Preuve du théorème I.1: L'existence se fait par récurrence transfinie. L'unicité se fait par absurde. •

Exemple 1 $1 = \overline{1}^q; 2 = \overline{2}^q; \dots; q-1 = \overline{q-1}^q$ et $q = \overline{10}^q; q+1 = \overline{11}^q$.

I.2 Numération décimale

Dans le cas $q = 10$, le système de numération est dit décimale. Les symboles utilisés sont

$$0; 1; 2; 3; 4; 5; 6; 7; 8 \text{ et } 9.$$

Remarque 1 Dans ce cas on écrit sans la barre dessus.

Application à la divisibilité dans \mathbb{N}

- Divisibilité par 2 et 5: On a $10 = 2 \times 5$, donc

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 2 \iff s_0 \in \{0; 2; 4; 6; 8\}.$$

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 5 \iff s_0 \in \{0; 5\}.$$

- Divisibilité par 3 et 9: On a $10 = 1 + 3 \times 3, 100 = 1 + 3 \times 3 \times 11 \dots$ donc

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 3 \iff \sum_{k=0}^n s_k \text{ est divisible par } 3.$$

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 9 \iff \sum_{k=0}^n s_k \text{ est divisible par } 9.$$

- Divisibilité par 4: On a $100 = 4 \times 25, 1000 = 4 \times 250 \dots$ donc

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 4 \iff s_1 s_0 \text{ est divisible par } 4.$$

I.3 Numération binaire

Dans le cas où $q = 2$, le système de numération est dit binaire. Les symboles utilisés sont

0 et 1.

Exemple 2 Voir S.I : $2 = \overline{10}^2; 3 = \overline{11}^2$.

Exercice 1 Dans quelle base le nombre 880 s'écrit-il 12010?

II Arithmétique dans l'anneau \mathbb{Z}

II.1 La congruence

Définition 2 Deux entiers a et b sont dit congrus modulo n ($n \in \mathbb{N}$) si $a - b \in n\mathbb{Z}$. On note alors $a \equiv b [n]$ ou $a \equiv b \pmod{n}$. On a donc

$$a \equiv b [n] \iff a - b \in n\mathbb{Z} \iff \exists k \in \mathbb{Z} \mid a = nk + b.$$

Propriétés

P II.1 La relation de congruence modulo n est une relation d'équivalence sur \mathbb{Z} .

P II.2 $\forall a, b, a', b' \in \mathbb{Z}$ et $\forall n \in \mathbb{N}$, on a

$$\left. \begin{array}{l} a \equiv b [n] \\ a' \equiv b' [n] \end{array} \right\} \implies a + a' \equiv b + b' [n] \text{ et } a \times a' \equiv b \times b' [n].$$

Cette propriété est appelée la compatibilité de la congruence modulo n avec les opérations $+$ et \times dans \mathbb{Z} . Elle permet de définir sur l'ensemble quotient $\mathbb{Z}/\equiv [n]$ des opérations en posant

$$\bar{a} + \bar{b} = \overline{a + b} \text{ et } \bar{a} \times \bar{b} = \overline{a \times b}. \quad (II.1)$$

P II.3 L'ensemble quotient modulo n est noté $\mathbb{Z}/n\mathbb{Z}$, il est de cardinal n en plus

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \dots; \overline{n-1}\} \text{ en bijection avec } \llbracket 0, n-1 \rrbracket.$$

II.2 Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

Théorème II.1 Les opérations définies sur $\mathbb{Z}/n\mathbb{Z}$ par les relations (II.1) munissent $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau commutatif.

De plus l'application $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}; a \mapsto \bar{a}$ est un morphisme surjectif d'anneaux.

Remarque 2 L'anneau $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n et sa structure sous jacente de groupe est cyclique. $\bar{0}$

Exemple 3 Tables d'anneaux de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$:

$$\begin{array}{c|cc} \mathbb{Z}/2\mathbb{Z} & & \\ \hline + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \hline \bar{1} & \bar{1} & \bar{0} \end{array}$$

$$\begin{array}{c|cc} \mathbb{Z}/2\mathbb{Z} & & \\ \hline \times & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{0} \\ \hline \bar{1} & \bar{0} & \bar{1} \end{array}$$

$$\begin{array}{c|ccc} \mathbb{Z}/3\mathbb{Z} & & & \\ \hline + & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{0} & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{1} & \bar{1} & \bar{2} & \bar{0} \\ \hline \bar{2} & \bar{2} & \bar{0} & \bar{1} \end{array}$$

$$\begin{array}{c|ccc} \mathbb{Z}/3\mathbb{Z} & & & \\ \hline \times & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{0} & \bar{0} & \bar{0} & \bar{0} \\ \hline \bar{1} & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{2} & \bar{0} & \bar{2} & \bar{1} \end{array}$$

Remarque 3 On remarque que $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont des corps, alors que $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre.

Exercice 2 Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ les équations:

$$X^5 - 1 = 0 \quad ; \quad X^5 - 2 = 0 \quad ; \quad X^4 + X^3 + 2 = 0.$$

II.3 PGCD et PPCM

II.3.1 Définitions - Exemples

Définition 3 (PGCD) Soient $a, b \in \mathbb{Z}$, on appelle Plus Grand Diviseur Commun de a et b l'unique entier naturel d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On note $d = \text{pgcd}(a, b)$ ou $d = a \wedge b$. On a donc

$$d = \text{pgcd}(a, b) \iff a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Remarque 4 $a\mathbb{Z} + b\mathbb{Z}$ étant un sous groupe de \mathbb{Z} il est donc de la forme $d\mathbb{Z}$ où $d = \min[(a\mathbb{Z} + b\mathbb{Z}) \cap]$

Proposition 1 (Caractérisation du PGCD) Soient $a, b \in \mathbb{Z}$, et $d \in \mathbb{N}$. Les propriétés suivantes sont équivalentes:

- (i) $d = \text{pgcd}(a, b)$.
- (ii) d est un diviseur commun à a et b , et tout diviseur commun à a et b divise d .
- (iii) d est un diviseur commun à a et b , et tout diviseur commun à a et b est $\leq d$.

Preuve: (i) \implies (ii) et (i) \implies (iii): évident d'après la définition.

(ii) \implies (i): On pose $d' = \text{pgcd}(a, b)$ et on montre que $d' = d$.

Exemple 4 $0 \wedge n = n, \forall n \in \mathbb{Z}; 3 \wedge 2 = 1; 12 \wedge 8 = 4...$

Définition 4 (Entiers premiers entre eux) Si $\text{pgcd}(a, b) = 1$, on dit que a et b sont premiers entre eux. i.e:

$$a \text{ et } b \text{ premier entre eux si et seulement si } a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}.$$

Exemple 5 2 est premier avec tout entier impair.

Définition 5 (PPCM) Soient $a, b \in \mathbb{Z}$, on appelle Plus Petit Multiple Commun de a et b l'unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On note $m = \text{ppcm}(a, b)$ ou $d = a \vee b$. On a donc

$$m = \text{ppcm}(a, b) \iff a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}.$$

Remarque 5 $a\mathbb{Z} \cap b\mathbb{Z}$ étant un sous groupe de \mathbb{Z} il est donc de la forme $m\mathbb{Z}$ où $m = \min[(a\mathbb{Z} \cap b\mathbb{Z}) \cap]$

Proposition 2 (Caractérisation du PPCM) Soient $a, b \in \mathbb{Z}$, et $m \in \mathbb{N}$. Les propriétés suivantes sont équivalentes:

- (i) $m = \text{ppcm}(a, b)$.
- (ii) m est un multiple commun à a et b , et tout multiple commun à a et b est multiple de m .
- (iii) m est un multiple commun à a et b , et tout multiple commun à a et b est $\geq m$.

Preuve: (i) \implies (ii) et (i) \implies (iii): évident d'après la définition.

(ii) \implies (i): On pose $m' = \text{ppcm}(a, b)$ et on montre que $m' = m$.

Exemple 6 $3 \vee 2 = 6; 12 \vee 8 = 24...$

Définition 6 (PPCM et PGCD d'une famille d'entiers) En général si a_1, a_2, \dots, a_n sont des entiers, on définit leur PGCD et PPCM par:

- $\text{pgcd}(a_1, a_2, \dots, a_n) = d$ si et seulement si $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$.
- $\text{ppcm}(a_1, a_2, \dots, a_n) = m$ si et seulement si $a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = m\mathbb{Z}$.

De même on dit que a_1, a_2, \dots, a_n sont premiers entre eux (dans leur ensemble) si

$$\text{pgcd}(a_1, a_2, \dots, a_n) = 1.$$

II.3.2 Propriétés

Soient a, b et c des entiers relatifs.

P II.4 $\text{pgcd}(ab, ac) = |a| \text{pgcd}(b, c)$.

En particulier si $d = \text{pgcd}(b, c)$ alors $\frac{b}{d} \wedge \frac{c}{d} = 1$.

P II.5 $\text{ppcm}(ab, ac) = |a| \text{ppcm}(b, c)$.

P II.6 Si $a = bq + r$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

II.3.3 Algorithme d'Euclide

On suppose $a, b \in \mathbb{N}$. L'algorithme d'Euclide est basé sur la propriété (PII.6) ci-dessus. Donc il consiste à faire des D.E successives jusqu'à avoir un reste nul.

Algorithme

1. Lecture de a et b ;
2. Tant que $b \neq 0$ Faire
3. Division Euclidienne de a par b : $a = bq + r$;
4. $a \leftarrow b; b \leftarrow r$;
5. Fin Faire
6. Résultat $\text{pgcd}(a, b) = a$ (le dernier reste non nul).

Remarque 6 La suites des restes r dans les Divisions Euclidiennes est strictement décroissantes, donc s'arrête à un certain rang, d'où la convergence de l'algorithme.

Exemple 7 Exécuter l'algorithme avec $a = 136$ et $b = 18$.

II.4 Théorème de Bezout et conséquence

Théorème II.2 (de Bezout) Soient $a, b \in \mathbb{Z}$, alors a et b sont premiers entre eux si et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tels que

$$au + bv = 1 \tag{II.2}$$

Définition 7 Un couple (u, v) vérifiant (II.2) est appelé un couple de coefficients de Bezout.

Remarque 7 Le théorème sans difficulté à une famille d'entiers:

$$\text{pgcd}(a_1, a_2, \dots, a_n) = 1 \iff \exists (u_1, \dots, u_n) \in \mathbb{Z}^n \mid \sum_{i=1}^n a_i u_i = 1.$$

Démonstration du théorème de Bezout: \implies Si $a \wedge b = 1$ alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ donc u et v existent.

\impliedby Si $\exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$ alors $1 \in a\mathbb{Z} + b\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. .

Proposition 3 Si $a \wedge b = 1$ alors il existe une infinité de couples de coefficients de Bezout.

En effet: Si (u_0, v_0) vérifient $au_0 + bv_0 = 1$ alors $\forall m \in \mathbb{Z} : (u = u_0 + mb, v = v_0 - ma)$ répond à la question. .

Exemple de détermination d'un couple de coefficients de Bezout

La méthode des divisions successives avec $a = 132, b = 35$, on a successivement:

$$\begin{array}{ll} 132 = 35 \times 3 + 27 & 132 \wedge 35 = 35 \wedge 27 \\ 35 = 27 \times 1 + 8 & 35 \wedge 27 = 27 \wedge 8 \\ 27 = 8 \times 3 + 3 & 27 \wedge 8 = 8 \wedge 3 \\ 8 = 3 \times 2 + 2 & 8 \wedge 3 = 3 \wedge 2 \\ 3 = 2 \times 1 + 1 & 3 \wedge 2 = 2 \wedge 1 = 1 \end{array}$$

Remontée:

$$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (8 - 3 \times 2) \times 1 = 3 + 8 + 3 \times 2 \\ &= 3 \times 3 - 8 = 3 \times (27 - 3 \times 8) - 8 = -9 \times 8 - 8 + 3 \times 27 \\ &= -10 \times 8 + 3 \times 27 \\ &= -10 \times (35 - 27) + 3 \times 27 = 10 \times 27 + 3 \times 27 - 10 \times 35 \\ &= 13 \times 27 - 10 \times 35 \\ &= 13 \times (132 - 35 \times 3) - 10 \times 35 = 13 \times 132 - (13 \times 3 + 10) \times 35 \\ &= 13 \times 132 - 49 \times 35. \end{aligned}$$

Donc $u = 13$ et $v = -49$ répondent à la question.

Théorème II.3 (de Gauss) Soient $a, b, c \in \mathbb{Z}$. On a

$$\left. \begin{array}{l} a \text{ divise } bc \\ \text{et} \\ a \wedge b = 1 \end{array} \right\} \implies a \text{ divise } c.$$

Preuve: $a \wedge b = 1$ donc il existe (u, v) tel que $au + bv = 1$ et par suite $acu + bcv = c$.

Et comme a divise bc alors il existe a' tel que $bc = aa'$.

Donc $acu + aa'v = c$ c'est à dire $a(cu + a'v) = c$.

Donc c divise a . .

Théorème II.4 Soient a, b_1, b_2, \dots, b_n des entiers

Si $a \wedge b_i = 1$ pour tout $i \in \llbracket 1, n \rrbracket$ alors $a \wedge \prod_{i=1}^n b_i = 1$.

Preuve: Bezout et une récurrence. .

Théorème II.5 Soient a, b deux entiers tels que $a \wedge b = 1$ alors $a \vee b = ab$.

En général si b_1, b_2, \dots, b_n sont des entiers deux à deux premiers entre eux alors

$$\text{ppcm}(b_1, \dots, b_n) = \prod_{i=1}^n b_i.$$

Remarque 8 On a aussi la réciproque $a \vee b = ab \implies a \wedge b = 1$.

En effet: Si on suppose $a \wedge b = d > 1$ alors

$$\text{ppcm}(a, b) = d \times \text{ppcm}\left(\frac{a}{d}, \frac{b}{d}\right) = d \times \frac{a}{d} \times \frac{b}{d} = \frac{ab}{d} \neq d$$

Ce qui absurde. .

Démonstration du théorème II.5: Posons $m = a \vee b$,

Il existe a', b' tels que $m = aa' = bb'$, donc a divise bb' .

Comme $a \wedge b = 1$ alors a divise b' et par suite il existe b'' tel que $b' = ab''$.

Donc $m = bab''$ c'est à dire ab divise m et comme m divise ab alors $m = ab$. .

Théorème II.6 Soient a, b deux entiers et $d \in \mathbb{N}$, on a l'équivalence

$$a \wedge b = d \iff \frac{a}{d} \wedge \frac{b}{d} = 1.$$

Théorème II.7 (Calcul du PPCM) Pour tout $(a, b) \in \mathbb{Z}^2$, on a

$$\text{ppcm}(a, b) \times \text{pgcd}(a, b) = |a \times b|.$$

Exercice 3 Déterminer tout les couples $(u, v) \in \mathbb{Z}^2$ tels que

$$323u - 391v = 612. \tag{II.3}$$

Réponse: On a $323 \wedge 391 = 323 \wedge 68 = 68 \wedge 51 = 51 \wedge 17 = 17$ car $51 = 3 \times 17$.

Donc

$$\begin{aligned} 323u - 391v &= 612 \iff \frac{323}{17}u - \frac{391}{17}v = \frac{612}{17} \\ &\iff 19u - 23v = 36 \end{aligned}$$

Comme $19 \wedge 23 = 1$ alors si (u_0, v_0) est un couple de coefficients de Bezout alors $(36u_0, 36v_0)$ est une solution particulière de (II.3).

Donc les solutions sont de la forme $(u = 36u_0 + 23k, v = 36v_0 + 19k)$. .

Forme irréductible d'un rationnel

Proposition 4 Pour tout rationnel $r \in \mathbb{Q}^*$, il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que

$$r = \frac{p}{q} \text{ et } p \wedge q = 1.$$

Le couple (p, q) est alors appelé représentant irréductible de r .

Preuve: Si $r = \frac{a}{b}$ tel que $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ et $d = a \wedge b$, alors $p = \frac{a}{d}$ et $q = \frac{b}{d}$ répondent à la question d'existence.

Pour l'unicité, si $\frac{p}{q} = \frac{p'}{q'}$ avec $p \wedge q = p' \wedge q' = 1$ alors $pq' = p'q$.

Donc p divise $p'q$ et comme $p \wedge q = 1$ alors p divise p' , de même p' divise p par un même raisonnement.

Enfin $p = p'$ et $q = q'$, d'où l'unicité. .

Générateurs d'un groupe cyclique

Proposition 5 Soit $G = \{e; a; a^2; \dots; a^{n-1}\}$ un groupe cyclique de cardinal n . Alors a^k est un générateur de G si et seulement si $k \wedge n = 1$.

Preuve: \implies Si a^k est un générateur de G alors $\exists p \in \mathbb{Z}$ tel que $(a^k)^p = a$, c'est à dire $a^{kp-1} = e$ donc $\exists q \in \mathbb{Z}$ tel que $kp-1 = nq$ donc $k \wedge n = 1$.

\impliedby si $k \wedge n = 1$ alors $\exists u, v \in \mathbb{Z}$ tels que $ku + vn = 1$ ou $ku - 1 = -vn$,

donc $a^{ku-1} = (a^n)^{-v} = e$, c'est à dire $(a^k)^u = a$, donc a^k est générateur de G . .

Inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 6 Soit $n \in \mathbb{N}^*$, Pour tout $a \in \mathbb{Z}$, on a

\bar{a} inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.

En particulier: $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Preuve: La même que celle de la proposition 5. .

Ordre de produit d'élément d'un groupe

Proposition 7 Soient G un groupe, a et b deux éléments de G d'ordre respectifs n et m .

Si $ab = ba$ et $gr(a) \cap gr(b) = \{e\}$ alors $ord(ab) = ppcm(m, n)$.

En particulier: si $m \wedge n = 1$ et $ab = ba$ alors $ord(ab) = mn$.

Preuve: Soit $\mu = m \vee n$, on a $(ab)^\mu = a^\mu b^\mu = e$.

Réciproquement, si $(ab)^k = e$, alors $a^k = b^{-k} \in gr(a) \cap gr(b)$, donc $a^k = b^k = e$.

Donc m et n divisent k donc μ divise k .

En particulier si $m \wedge n = 1$ alors $gr(a) \cap gr(b) = \{e\}$, car si non, il existent u, v dans \mathbb{Z} tels que $a^u = b^v \neq e$. .

III Nombres premiers**III.1 Définitions - Exemples**

Définition 8 On appelle nombre premier tout entier naturel $p \geq 2$ dont les seuls diviseurs dans \mathbb{N} sont 1 et p .

Exemple 8 Les entiers 2; 3; 5; 7; 11; 13 sont premiers.

Les nombres de Fermat: $F_n = 2^{2^n} + 1$ sont premiers pour $n = 0, 1, 2, 3, 4$ mais pour $n = 5$.

Théorème III.1 Soit p un nombre premier.

1. p est premier avec tout entier qu'il ne divise pas:

$$\forall k \in \mathbb{Z} : p \wedge k = 1 \iff p \text{ ne divise pas } k.$$

2. En particulier deux entiers premiers distincts sont premiers entre eux.

Exercice 4 Si p premier alors p divise \mathbb{C}_p^k pour tout k tel que $1 \leq k \leq p-1$.

III.2 Décomposition d'un entier en facteurs premiers

Théorème III.2 Tout entier $N \geq 2$ admet au moins un diviseur premier.

Preuve: p = plus petit élément de l'ensemble des diviseurs de N , i.e:

$$p = \min \{q \in \mathbb{N}^* \setminus \{1\} \mid q \text{ divise } N\}$$

est un entier premier, si non il est composée: $p = p_1 p_2$ avec $2 \leq p_i \leq p-1$ ce qui est absurde. .

Corollaire III.3 (Euclide) L'ensemble \mathcal{P} des nombres premiers est infini.

Preuve: Si \mathcal{P} est fini alors il est majoré par un $N \geq 2$. L'entier $N! + 1$ admet un diviseur premier différent de tous les entier de l'intervalle $\llbracket 1, N \rrbracket$, ce qui est absurde. .

Théorème III.4 (Décomposition en facteurs premiers) Soit N un entier $N \geq 2$. On note p_1, p_2, \dots, p_n tous les diviseurs premiers de N .

Il existe un unique n -uplet $(\alpha_1, \alpha_2, \dots, \alpha_n) \in (\mathbb{N}^*)^n$ tel que

$$N = \prod_{i=1}^n p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}.$$

Preuve: Pour chaque $i \in \llbracket 1, n \rrbracket$, on pose $\alpha_i = \max \{\alpha \in \mathbb{N} \mid p_i^\alpha \text{ divise } N\}$. .

Théorème III.5 (Calcul du PGCD et PPCM) Soient $a = \prod_{i=1}^n p_i^{\alpha_i}$ et $b = \prod_{i=1}^n p_i^{\beta_i}$.

$$a \wedge b = \prod_{i=1}^n p_i^{\min\{\alpha_i; \beta_i\}} \text{ et } a \vee b = \prod_{i=1}^n p_i^{\max\{\alpha_i; \beta_i\}}.$$

Nombres entiers naturels, Ensembles finis, dénombrements.

B. Seddoug. Médiane Sup, Oujda

I Nombres entiers naturels

I.1 Propriétés fondamentales

L'ensemble \mathbb{N} des entiers naturels est muni:

1. de deux l.c.i, addition et multiplication.

- L'addition $+$ est commutative, associative et admet 0 pour élément neutre. En plus, on a la propriété:

$$\forall a, b \in \mathbb{N} : (a + b = 0 \iff a = b = 0).$$

- La multiplication \times est commutative, associative, distributive par rapport à l'addition et admet 1 pour élément neutre. En plus, on a les propriétés:

$$\forall a, b \in \mathbb{N} : (ab = 0 \iff a = 0 \text{ ou } b = 0).$$

$$\forall a, b \in \mathbb{N} : (ab = 1 \iff a = b = 1).$$

2. d'une relation d'ordre notée \leq appelé ordre naturel entre les entiers, définie par

$$\forall a, b \in \mathbb{N} : (a \leq b \iff \exists c \in \mathbb{N} \mid b = a + c).$$

qui vérifie les propriétés suivantes:

- (\mathbb{N}, \leq) est totalement ordonné, en plus \leq est compatible avec les lois $+$ et \times .
- 0 est le plus petit élément de \mathbb{N} , et \mathbb{N} n'est pas majoré.
- Tout entier n admet un successeur $n + 1$, avec $n < n + 1$ et

$$\forall p, q \in \mathbb{N} : (p < q \iff p + 1 \leq q)$$

ie: il n'y a aucun entier entre un entier et son successeur.

- Tout entier $n \neq 0$ admet un prédécesseur $n - 1$.

On admet que \mathbb{N} vérifie la propriété suivante, connue sous le nom de *axiome de récurrence*:

3. Pour toute partie A de \mathbb{N} , on a:

$$\left. \begin{array}{l} (i) 0 \in A \\ (ii) \forall n \in \mathbb{N} : n \in A \implies n + 1 \in A \end{array} \right\} \implies A = \mathbb{N}.$$

I.1.1 Principe de récurrence

Théorème I.1 (dit de récurrence) Soit $P(n)$ une assertion dépendant de la variable n dans \mathbb{N} . On suppose que:

- (i) $P(0)$ est vrai,
- (ii) $\forall n \in \mathbb{N} : P(n) \implies P(n + 1)$, on dit que $P(n)$ est héréditaire.

Alors la propriété $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Preuve: Considérer $A = \{n \in \mathbb{N} \mid P(n)\}$.

Remarque 1 Une variante du principe de récurrence s'obtient, en modifiant (i) et (ii) ci-dessus, comme suit:

- (i) $\exists n_0 \in \mathbb{N} \mid P(n_0)$ est vrai,
- (ii) $\forall n \geq n_0 : P(n) \implies P(n + 1)$.

Alors la propriété $P(n)$ est vraie pour tout $n \geq n_0$.

Théorème I.2 Toute partie non vide de \mathbb{N} admet un plus petit élément.

Preuve: Soit $A \subset \mathbb{N}$, $A \neq \emptyset$. On note M l'ensemble des minorants de A .
 $0 \in M$ et $M \neq \mathbb{N}$, donc M ne vérifie pas la propriété (ii) de l'axiome de récurrence.
C'est à dire:

$$\exists n_0 \in M \mid n_0 + 1 \notin M$$

On montre alors que $n_0 \in A$. En effet, si par absurde on suppose que $n_0 \notin A$ alors
 $\forall n \in A : n_0 < n$,
donc $\forall n \in A : n_0 + 1 \leq n$, c'est à dire que $n_0 + 1 \in M$, ce qui absurde .

Corollaire I.3 (récurrence forte) Soit $P(n)$ une assertion dépendant de la variable n dans \mathbb{N} . On suppose que:

- (i) $P(0)$ est vrai,
- (ii) $\forall n \in \mathbb{N} : (P(0) \text{ et } P(1) \text{ et } \dots \text{ et } P(n)) \implies P(n + 1)$.

Alors la propriété $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Preuve: Considérons $A = \{n \in \mathbb{N} \mid P(n)\}$, par absurde supposons que $B = \mathbb{N} \setminus A \neq \emptyset$, Alors B possède un minimum $n_0 > 0$. Donc $\forall p < n_0 : p \in A$ et d'après (ii) du corollaire $P(n_0)$ est vraie, ce qui contredit le fait que $n_0 \in B$.

Exemple 1 (principe de descente infinie de Fermat) Il n'existe aucune suite strictement décroissante dans \mathbb{N} .

En effet si $(u_k)_{k \in \mathbb{N}}$ est strictement décroissante dans \mathbb{N} , alors l'ensemble $U = \{u_k \mid k \in \mathbb{N}\}$ n'admet pas de minimum, ce qui est absurde.

Théorème I.4 Toute partie non vide et majorée de \mathbb{N} admet un plus grand élément.

Preuve: Soit $A \subset \mathbb{N}$, $A \neq \emptyset$. On note M l'ensemble des majorants de A et $m_0 = \min(M)$.
Si $m_0 \notin A$ alors $\forall n \in A : n < m_0$, donc $m_0 \neq 0$ et $\forall n \in A : n \leq m_0 - 1$, ce qui contredit le fait que $m_0 = \min(M)$.

I.1.2 Division euclidienne

Théorème I.5 $\forall (a, b) \in \mathbf{N} \times \mathbf{N}^*, \exists!(q, r) \in \mathbf{N} \times \mathbf{N} \mid a = bq + r \text{ et } 0 \leq r < b$.
 q : quotient, r : reste dans la division euclidienne de a par b .

Preuve: La faire en exercice.. s'inspirer de la démonstration dans \mathbb{R} .
 Considérer $A = \{n \in \mathbf{N} \mid nb \leq a\}$. $A \neq \emptyset$ et majoré, on pose $q = \max(A)$,
 alors $q + 1 \notin A$ c'est à dire $r = a - qb < b$, d'autre part $r \geq 0$, d'où l'existence.
 Pour l'unicité, on raisonne par absurde .

I.2 Notion de suites

Définition 1 Soit E un ensemble non vide, on appelle suite d'éléments de E toute application de \mathbf{N} (ou d'une partie de \mathbf{N}) dans E .

Notation $(u_n)_{n \in \mathbf{N}}$ ou $(u_n)_{n \in I}$ avec $I \subset \mathbf{N}$, où pour tout $n, u_n \in E$.

Théorème I.6 (admis) Soit E un ensemble non vide, $f : E \rightarrow E$ et $a \in E$.
 Il existe une suite $(u_n)_{n \in \mathbf{N}}$ d'éléments de E , unique telle que:

$$\begin{cases} u_0 = a, \\ \forall n \in \mathbf{N} : u_{n+1} = f(u_n). \end{cases}$$

On dit que $(u_n)_{n \in \mathbf{N}}$ est définie par une relation de récurrence.

Exemple 2 Suites arithmétiques, géométriques et arithmético-géométrique.

II Ensembles finis

II.1 Cardinal d'un ensemble fini

Lemme II.1 Soit $(p, q) \in \mathbf{N}^{*2}$; on a:

- (i) $p \leq q \iff (\exists f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket \text{ injective})$.
- (ii) $p \geq q \iff (\exists f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket \text{ surjective})$.

Preuve: (i) \implies si $p \leq q$, alors $\llbracket 1, p \rrbracket \subset \llbracket 1, q \rrbracket$ et f : injection canonique.
 \impliedby Par récurrence sur p en considérant la proposition:

$$P(p) : \llcorner \forall q \in \mathbf{N}^*, \text{ s'il existe une injection de } \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket \text{ alors } p \leq q \lrcorner$$

- $p = 1$, on a $\forall q \in \mathbf{N}^* : 1 \leq q$ donc $P(1)$ est vraie.
- Supposons $P(p)$ vraie, et soit $q \in \mathbf{N}^*$ et $f : \llbracket 1, p + 1 \rrbracket \rightarrow \llbracket 1, q \rrbracket$ injective.

D'abord $q \geq 2$; on distingue les deux cas: $f(p + 1) = q$ et $f(p + 1) < q$:
 1^{er} cas : $f(p + 1) = q$, alors $f' : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q - 1 \rrbracket$; $x \mapsto f(x)$ est une application injective et d'après le HR, $p \leq q - 1$ c.à.d $p + 1 \leq q$.
 2^{eme} cas : $f(p + 1) = q' < q$, on considère $\tau : \llbracket 1, q \rrbracket \rightarrow \llbracket 1, q \rrbracket$ telle que

$$\begin{cases} \tau(q) = q'; \tau(q') = q \text{ et} \\ \forall i \in \llbracket 1, q \rrbracket \mid i \neq q \text{ et } i \neq q' : \tau(i) = i \end{cases}$$

et on considère $\tau \circ f : \llbracket 1, p + 1 \rrbracket \rightarrow \llbracket 1, q \rrbracket$ injective et telle que $\tau \circ f(p + 1) = q$, donc d'après le 1^{er} cas, $p + 1 \leq q$.

(i) \implies si $p \geq q$, alors $\llbracket 1, q \rrbracket \subset \llbracket 1, p \rrbracket$ et l'application $f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket$ telle que

$$\begin{cases} \forall i \in \llbracket 1, q \rrbracket : f(i) = i \text{ et} \\ \forall i \in \llbracket q + 1, p \rrbracket : f(i) = q. \end{cases}$$

est surjective.

\impliedby Soit $f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket$ surjective, considérons $g : \llbracket 1, q \rrbracket \rightarrow \llbracket 1, p \rrbracket$ telle que, $g(k) = \min f^{-1}(\{k\})$. On montre que g est injective, en effet si $g(k) = g(h)$ alors $f^{-1}(\{k\}) \cap f^{-1}(\{h\}) \neq \emptyset$, donc il existe i tel que $f(i) = k$ et $f(i) = h$, donc $h = k$.

Remarque 2 On déduit du lemme que

- $p = q \iff (\exists f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket \text{ bijective})$.

Définition 2 Deux ensembles E et F sont dits *équipotents*, s'il existe une bijection de E dans F .

Définition 3 Un ensemble E est dit *fini*, s'il existe un entier n non nul et une bijection $\varphi : \llbracket 1, n \rrbracket \rightarrow E$. Par convention, on dira que l'ensemble vide est fini.
 Si non, on dit que E est *infini*.

Exemple 3 Pour tout $m \in \mathbf{N}^*$, $\llbracket 1, m \rrbracket$ est fini.
 Pour tout $p \leq q \in \mathbf{N}$, $\llbracket p, q \rrbracket$ est fini.

Théorème II.1 Si E est un ensemble fini, alors l'entier n de la définition précédente est unique. On dit que E est de *cardinal* n , on note $\text{card}(E) = n$ ou $|E| = n$.
 Par convention $\text{card}(\emptyset) = 0$.

Preuve: Si $\varphi : \llbracket 1, n \rrbracket \rightarrow E$ et $\varphi' : \llbracket 1, n' \rrbracket \rightarrow E$ sont deux bijections alors $\varphi^{-1} \circ \varphi'$ définit une bijection de $\llbracket 1, n' \rrbracket \rightarrow \llbracket 1, n \rrbracket$, donc d'après le lemme précédent $n = n'$.

Exemple 4 $\text{card}(\llbracket 1, m \rrbracket) = m$, et $\text{card}(\llbracket m, n \rrbracket) = n - m + 1$.

II.2 Applications entre ensembles finis

Théorème II.2 Soient E et F deux ensembles finis, p et q tels que $\text{card}(E) = p$, $\text{card}(F) = q$. Alors on a:

- (i) $p \leq q \iff (\exists f : E \rightarrow F \text{ injective})$.
- (ii) $p \geq q \iff (\exists f : E \rightarrow F \text{ surjective})$.
- (iii) $p = q \iff (\exists f : E \rightarrow F \text{ bijective})$.

Preuve: $E \xrightarrow{\text{bijective}} \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket \xrightarrow{\text{bijective}} F \dots$ et le lemme précédent .

Corollaire II.3 Soient E et F deux ensembles finis tels que $\text{card}(E) = \text{card}(F)$, et $f : E \rightarrow F$. Alors f injective ssi f surjective ssi f bijective.

Preuve: Soit $p = \text{card}(E) = \text{card}(F)$, E et F sont équipotents, on peut donc supposer $E = F = \llbracket 1, p \rrbracket$, et $f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, p \rrbracket$.

- Supposons f injective, si f n'est pas surjective alors $\text{Im } f \subsetneq \llbracket 1, p \rrbracket$, on distingue deux cas:
 - $p \notin \text{Im } f$: alors f induit une injection de $\llbracket 1, p \rrbracket$ dans $\llbracket 1, p-1 \rrbracket$, ce qui est absurde.
 - $p \in \text{Im } f$: on considère $g = \tau_{p,k} \circ f$, où $k \notin \text{Im } f$, alors $g : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, p \rrbracket$ injective et $p \notin \text{Im } g$, ce qui est absurde, d'après le cas précédent.
- Supposons f surjective, si f n'est pas injective alors il existe $i \neq j$ tels que $f(i) = f(j)$ (quite à considérer $f \circ \tau_{i,p}$, on peut supposer que $f(p) = f(i)$ avec $i < p$). Donc f induit une surjection de $\llbracket 1, p-1 \rrbracket$ dans $\llbracket 1, p \rrbracket$, ce qui est absurde.

Ce qui achève la démonstration .

Remarque 3 On peut déduire que l'ensemble \mathbf{N} est infini, $n \mapsto n+1$ injective et non surjective... Et on peut caractériser les ensembles infinis par:

Théorème II.4 Un ensemble E est infini, si et seulement s'il existe une application $f : \mathbf{N} \rightarrow E$ injective.

Preuve: Si E est infini, on construit par récurrence une application f injective de \mathbf{N} dans E par:

$$f(0) = x_0 \in E, \text{ et pour tout } n, f(n+1) = x_{n+1} \in E \setminus \{x_0, \dots, x_n\}.$$

Réciproquement si $f : \mathbf{N} \rightarrow E$ injective, on construit $g : E \rightarrow E$, par:

$$\begin{cases} \forall x \in E \setminus \text{Im } f : g(x) = x, \\ \forall n \in \mathbf{N} : g(f(n)) = f(n+1). \end{cases}$$

et on montre que g est injective mais pas surjective .

Théorème II.5 Soit F un ensemble fini et E tel qu'il existe une application $\exists f : E \rightarrow F$ injective, alors E est fini et $\text{card}(E) \leq \text{card}(F)$.

Preuve: Si on suppose par absurde E infini alors $\mathbf{N} \xrightarrow{\text{injective}} E \xrightarrow{\text{injective}} F$, ce qui contredit le fait que F est fini .

Corollaire II.6 Si F est fini et $E \subset F$, alors E est fini et $\text{card}(E) \leq \text{card}(F)$, avec égalité si et seulement si $E = F$.

Corollaire II.7 Les parties finies de \mathbf{N} sont les parties majorées.

Preuve: En effet si $A \subset \mathbf{N}$ est majorée, avec $m = \max A$, on a $A \subset \llbracket 0, m \rrbracket$ qui est fini. .

II.3 Opérations sur les ensembles finis

Théorème II.8 Soient E et F deux ensembles finis. $E \cup F$ est fini, et on a

$$\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F).$$

Preuve: On traite d'abord le cas $E \cap F = \emptyset$: si $f : E \rightarrow \llbracket 1, m \rrbracket$ bijective et $g : E \rightarrow \llbracket 1, n \rrbracket$ bijective, on considère $h : E \rightarrow \llbracket 1, m+n \rrbracket$, telle que:

$$\begin{cases} \forall x \in E : h(x) = f(x), \\ \forall x \in F : h(x) = g(x) + n. \end{cases}$$

h est bijective. Si $E \cap F \neq \emptyset$, on écrit $E = (E \cap F) \cup (E \setminus F)$, $F = (E \cap F) \cup (F \setminus E)$ et $E \cup F = (E \cap F) \cup (E \setminus F) \cup (F \setminus E)$. Donc

$$\begin{aligned} \text{card}(E \cup F) &= \text{card}(E \cap F) + \text{card}(E \setminus F) + \text{card}(F \setminus E) \\ &= \text{card}(E \cap F) + (\text{card}(E) - \text{card}(E \cap F)) + (\text{card}(F) - \text{card}(E \cap F)) \\ &= \text{card}(E) + \text{card}(F) - \text{card}(E \cap F). \end{aligned}$$

ce qui achève la démonstration .

Exercice 1 $\text{card}(E \cup F \cup G)$?

Remarque 4 Si A_1, A_2, \dots, A_k sont des parties deux à deux disjointes d'un ensemble fini alors

$$\text{card}\left(\bigcup_{i=1}^k A_i\right) = \sum_{i=1}^k \text{card}(A_i).$$

Théorème II.9 Soient E et F deux ensembles finis. $E \times F$ est fini, et on a

$$\text{card}(E \times F) = \text{card}(E) \cdot \text{card}(F).$$

Preuve: On pose $\text{card}(E) = n$ et $\text{card}(F) = p$, et on raisonne par récurrence sur $n \geq 1$.

- Si $n = 1$ alors $E = \{a\} : E \times F \rightarrow F; (a, y) \mapsto y$ est bijective.
- On suppose la relation vraie pour n quelque soit p .
- Soit $E = E' \cup \{a\}$ de cardinal $n+1$, $E \times F = (E' \times F) \cup (\{a\} \times F)$ union disjointe.

Ce qui achève la démonstration .

III Dénombrements

On définit pour tout entier naturel $n \neq 0$, factoriel n comme étant l'entier noté $n!$ tel que

$$n! = \prod_{k=1}^n k = 1 \times 2 \times \dots \times n \text{ et on convient que } 0! = 1.$$

III.1 Le principe des bergers et conséquences

Soit E un ensemble fini de cardinal $n \geq 1$, $\varkappa_E : E \rightarrow \mathbf{N}; x \mapsto 1$, alors on a

$$\text{card}(E) = \sum_{x \in E} \varkappa_E(x) = \sum_{x \in E} 1 \tag{1}$$

Preuve: Par récurrence sur n .

Si $n = 1$, posons $E = \{a\}$ alors $\sum_{x \in E} \varkappa_E(x) = \varkappa_E(a) = 1 = \text{card}(E)$.

Supposons la propriété vraie pour n . Soit E de cardinal $n+1$, posons $E = E' \cup \{a\}$, avec $\text{card}(E') = n$. $\text{card}(E) = 1 + \text{card}(E') = 1 + \sum_{x \in E'} \varkappa_{E'}(x) = \sum_{x \in E} \varkappa_E(x)$, cqfd .

Remarque 5 La relation (1) exprime le fait *pratique* que le cardinal de E est égal au nombre d'éléments de E .

Exemple 5 $n = \sum_{i=1}^n 1$.

Exercice 2 calculer $\sum_{1 \leq i, j \leq n} 1$; $\sum_{1 \leq i < j \leq n} 1$.

Théorème III.1 (Principe des bergers) Soit E un ensemble, (A_1, \dots, A_k) un partage de E (ie: $E = \bigcup_{i=1}^k A_i$ et $A_i \cap A_j = \emptyset$ si $i \neq j$). Alors $\text{card}(E) = \sum_{i=1}^k \text{card}(A_i)$.

Remarque 6 La relation (1) et le principe des bergers, sont les bases de l'analyse combinatoire.

Théorème III.2 Soient E et F finis alors F^E est fini est $\text{card}(F^E) = \text{card}(F)^{\text{card}(E)}$.

Preuve: par récurrence sur $n = \text{card}(E)$.

Si $n = 1$, posons $E = \{a\}$, l'application $\varphi : F^E \rightarrow F; f \mapsto f(a)$ est bijective, donc F^E est fini et $\text{card}(F^E) = \text{card}(F)$.

Supposons la propriété vraie pour n . Soit E de cardinal $n + 1$, posons $E = E' \cup \{a\}$, avec $\text{card}(E') = n$. Pour tout $b \in F$, posons

$$\mathcal{E}_b = \{f \in F^E \mid f(a) = b\}$$

Pour tout $b \in F$, l'application

$$\psi : \mathcal{E}_b \rightarrow F^{E'}; f \mapsto f|_{E'}$$

est bijective, donc \mathcal{E}_b est fini et $\text{card}(\mathcal{E}_b) = p^n$, d'après l'hypothèse de récurrence.

On montre que $(\mathcal{E}_b)_{b \in F}$ est une partition de F^E , et on déduit que

$$\text{card}(F^E) = \sum_{b \in F} \text{card}(\mathcal{E}_b) = p^n \cdot p = p^{n+1}$$

Ce qui achève la démonstration .

Corollaire III.3 Si E est fini de cardinal n , alors $\mathcal{P}(E)$ est fini, et on a: $\text{card}(\mathcal{P}(E)) = 2^{\text{card}(E)}$.

Preuve: $\mathcal{P}(E)$ est équipotent à $\{0; 1\}^E$.

III.2 Arrangements

Théorème III.4 (Nombres d'injections) Soient E et F finis, $p = \text{card}(E)$, $n = \text{card}(F)$ tels que $p \leq n$. Le nombre des applications injectives de E dans F est:

$$A_n^p = \frac{n!}{(n-p)!} = n(n+1)\dots(n-p+1) = \prod_{i=1}^p (n-p+i)$$

appelé le nombre d'arrangements sans répétition de n objets pris p à p .

Remarque 7 le nombre d'arrangements avec répétition de n objets pris p à p est $\text{card}(E^p)$.

Preuve: Par récurrence sur $p = \text{card}(E)$. On note $\mathcal{I}(E, F)$ l'ensemble des applications injectives de E dans F .

Si $p = 1$, avec $\text{card}(F) = n \geq 1$, toute application de E dans F est injective, donc $\text{card}(\mathcal{I}(E, F)) = \text{card}(F^E) = n$.

Supposons la propriété vraie pour p . Soit E de cardinal $p + 1$, posons $E = E' \cup \{a\}$, avec $\text{card}(E') = p$. Pour tout $b \in F$, posons

$$\mathcal{J}_b = \{f \in \mathcal{I}(E, F) \mid f(a) = b\}$$

Pour tout $b \in F$, l'application

$$\psi : \mathcal{J}_b \rightarrow \mathcal{I}(E', F \setminus \{b\}); f \mapsto f_b : x \mapsto f(x)$$

est bijective, donc \mathcal{J}_b est fini et $\text{card}(\mathcal{J}_b) = A_{n-1}^p$, d'après l'hypothèse de récurrence.

D'autre part $(\mathcal{J}_b)_{b \in F}$ est une partition de $\mathcal{I}(E, F)$, donc

$$\text{card}(\mathcal{I}(E, F)) = \sum_{b \in F} A_{n-1}^p = n \cdot A_{n-1}^p = n \frac{(n-1)!}{(n-1-p)!} = \frac{n!}{(n-(p+1))!} = A_n^{p+1}$$

Ce qui achève la démonstration .

Model: Tirage dans une population de taille n d'un échantillon ordonnée de taille p sans remise.

Remarque 8 Avec remise correspond à avec répétition.

Théorème III.5 Si $\text{card}(E) = \text{card}(F) = n$, alors le nombre de bijections de E dans F est $n!$.

En particulier: $\text{card}(\mathcal{S}_n) = n!$, où \mathcal{S}_n est l'ensemble des bijections de $\llbracket 1, n \rrbracket$.

III.3 Combinaisons

Théorème III.6 Soient E fini de cardinal $n \geq 1$, et $0 \leq p \leq n$. Le nombre de parties de E à p éléments est

$$\mathbb{C}_n^p = \frac{n!}{p!(n-p)!} = \frac{1}{p!} A_n^p.$$

Preuve: On note $\mathcal{F}_p(E)$ l'ensemble des parties à p éléments de E ; l'application

$$\varphi : \begin{array}{ccc} \mathcal{I}(\llbracket 1, p \rrbracket, E) & \longrightarrow & \mathcal{F}_p(E) \\ f & \longmapsto & \text{Im } f \end{array}$$

est surjective, et le principe des bergers implique

$$A_n^p = \text{card}(\mathcal{I}(\llbracket 1, p \rrbracket, E)) = \sum_{A \in \mathcal{F}_p(E)} \text{card}(\varphi^{-1}(A)).$$

Et pour tout $A \in \mathcal{F}_p(E) : \varphi^{-1}(A) = \{f \in \mathcal{I}(\llbracket 1, p \rrbracket, E) \mid \text{Im } f = A\}$ et

$$\varphi_A : \begin{array}{ccc} \varphi^{-1}(A) & \longrightarrow & \mathcal{I}(\llbracket 1, p \rrbracket, A) \\ f & \longmapsto & f|_A \end{array}$$

est bien une application et elle est bijective, donc $\text{card}(\varphi^{-1}(A)) = \text{card}(\mathcal{I}(\llbracket 1, p \rrbracket, E)) = p!$.

On déduit donc que $A_n^p = \text{card}(\mathcal{F}_p(E)) \cdot p!$, c.à.d que $\text{card}(\mathcal{F}_p(E)) = \frac{1}{p!} A_n^p$ cqfd .

Modél: Nombre de combinaisons de p objet dans une population de taille n .

Remarque 9 Si $p > n$, on pose $C_n^p = 0$.

Propriétés

P III.1 $C_n^p = C_n^{p-1}$. $C_n^{p+1} = \frac{n-p}{p+1} C_n^p$. $C_n^p = \frac{n}{p} C_{n-1}^{p-1}$.

P III.2 $\sum_{p=0}^n C_n^p = 2^n$.

P III.3 $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$: relation de Pascal

Triangle de Pascal

$n = 1.$	1	1				
$n = 2.$	1	2	1			
$n = 3.$	1	3	3	1		
$n = 4.$	1	4	6	4	1	
$n = 5.$	1	5	10	10	5	1
					

Exercice 3 Combinaison avec répétition

$K_p^p = C_{n+p-1}^{n-1}$ (nombre de solution dans \mathbb{N}^n de l'équation: $x_1 + x_2 + \dots + x_n = p$).

Exercice 4 Dérangements...