Licence de Mathématiques

Module MA5.04

ALGEBRE : Groupes et Applications

Jean-François Havet

Université d'Orléans, Département de Mathématiques
B.P. 6759, 45067 ORLEANS Cedex 2, France

Septembre 2003

Table des matières

Chapitre I : Rappels et Compléments ensemblistes

1 Théorie axiomatique des ensembles

La théorie intuitive des ensembles conduit à des paradoxes. En effet si nous supposons l'existence de $\mathcal{E}$, ensemble de tous les ensembles, nous pouvons considérer l'ensemble $F = \{E \in \mathcal{E} \ ; \ E \notin E\}$ et nous poser la question : a-t-on $F \in F$? On remarque alors que $F \in F \Leftrightarrow F \notin F$.
D'où la nécessité de définitions plus rigoureuses, c'est à dire d'une axiomatique précisant les règles de construction des ensembles et donc les propriétés de l'appartenance, notée $\in$. L'axiomatique qui va être présentée est celle de **Zermelo-Fraenkel** élaborée à partir de 1908.

Axiome d'extensionnalité :

$$\forall x \, \forall y \, [\, \forall z \, (z \in x \Leftrightarrow z \in y) \ \Rightarrow \ (x = y) \,] \ .$$

Deux ensembles sont égaux si et seulement s'ils ont les mêmes éléments.

Axiome de l'ensemble vide :

$$\exists x \, \forall y \ \neg (y \in x) \ .^{1}$$

D'après l'axiome précédent cet ensemble est unique et est noté $\emptyset$.

Définition. Un *énoncé ensembliste* est un énoncé construit à partir des quantificateurs $\forall$, $\exists$, des connecteurs logiques, de $=$ et $\in$ et ne portant que sur des ensembles.

Exemple : l'inclusion $P(x, y)$ défini par $\forall z \, (z \in y \Rightarrow z \in x)$ est un énoncé ensembliste ; on le note $y \subset x$.

Axiome de compréhension : Soit P un énoncé ensembliste.

$$\forall x \, \exists y \, \forall z \ \Big[\, (z \in y) \ \Leftrightarrow \ \Big((z \in x) \wedge P(z) \Big) \, \Big] \ .$$

D'après l'axiome d'extensionnalité l'ensemble y est unique. On le note $\{z \in x \ ; \ P(z)\}$.

Conséquence : Soient x et y des ensembles. On peut alors définir *l'intersection* de x et y par $x \cap y = \{z \in x \ ; \ z \in y\}$. Si on a $y \subset x$ on peut également définir le *complémentaire* de y dans x par $C_x y = \{z \in x \ ; \ z \notin y\}$. On le note aussi $x \setminus y$.

[1] Le symbole $\neg$ est l'écriture mathématique du "non" et $\wedge$ celle du "et"

Axiome des parties :

$$\forall x\, \exists y\, \forall z\ [\, (z \in y) \ \Leftrightarrow\ (z \subset x)\,]\ .$$

L'ensemble y est unique et est noté $\mathcal{P}(x)$.

Conséquence : Pour tout ensemble x il existe un ensemble n'ayant pour élément que x, on le note $\{x\}$, c'est un *singleton*.
En effet $\{x\} = \{z \in \mathcal{P}(x)\ ;\ z = x\}$.

Axiome de la paire :

$$\forall x\, \forall y\, \exists z\, \forall t\ \Big[\, (t \in z) \ \Leftrightarrow\ \Big((t = x) \vee (t = y)\Big)\,\Big]\ .$$

L'ensemble z est unique. Si $x = y$ on retrouve $\{x\}$. Si $x \neq y$, on le note $\{x, y\}$ c'est une *paire*.

Conséquence : Si x et y sont des ensembles, alors $\{\, \{x\}\, ,\, \{x, y\}\, \}$ est un ensemble noté (x, y) et appelé *couple*.

Proposition : *Soient x, x', y et y' des ensembles.*

$$(x, y) = (x', y') \Leftrightarrow ((x = x') \wedge (y = y'))\ .$$

Preuve. La condition suffisante est évidente.
Si $(x, y) = (x', y')$ alors $\{\, \{x\}\, ,\, \{x, y\}\, \} = \{\, \{x'\}\, ,\, \{x', y'\}\, \}$.

- Si $x = y$ alors $\{\, \{x\}\, \} = \{\, \{x'\}\, ,\, \{x', y'\}\, \}$; on doit avoir $\{x\} = \{x'\}$, d'où $x = x'$, et $\{x\} = \{x', y'\}$ d'où $x' = y' = x$.

- Si $x \neq y$ alors nécessairement $x' \neq y'$ d'après le premier cas et on a
  soit $(\{x\} = \{x', y'\}) \wedge (\{x, y\} = \{x'\})$ impossible car $x \neq y$,
  soit $(\{x\} = \{x'\}) \wedge (\{x, y\} = \{x', y'\})$ d'où $x = x'$ et par suite $y = y'$. ∎

Axiome de fondation :

$$\forall x\ \Big[\, (x \neq \emptyset)\ \Rightarrow\ \exists y \Big(\, (y \in x) \wedge (y \cap x = \emptyset)\, \Big)\,\Big]\ .$$

Conséquence : Cet axiome interdit $x \in x$. En effet si nous supposons $x \in x$ alors $\{x\}$ contredit l'axiome : $\{x\} \neq \emptyset$ et pour tout $y \in \{x\}$ (nécessairement $y = x$) $y \cap \{x\} = \{x\} \neq \emptyset$.
De même cet axiome interdit $(x \in y) \wedge (y \in x)$; sinon $\{x, y\}$ contredit l'axiome.

Axiome de la réunion :

$$\forall x\, \exists y\, \forall z\ \Big[(z \in y) \Leftrightarrow \exists t \Big((t \in x) \wedge (z \in t) \Big) \Big]\ .$$

L'ensemble y est unique et est noté $\bigcup_{t \in x} t$ (*union des ensembles de* x).

Exemples : Si $x = \{a, b\}$ on obtient l'ensemble des éléments appartenant à a ou b ; on le note $a \cup b$.
Si $x = \{\, \{a\}, \{b, c\}\, \}$ on trouve $\{a, b, c\}$.

Théorème : *Soient a et b deux ensembles, il existe un ensemble unique noté $a \times b$ appelé produit cartésien dont les éléments sont les couples (x, y) avec $x \in a$ et $y \in b$.*

Preuve. On sait que les couples existent, mais constituent-ils un ensemble ?
On a $(x, y) = \{\, \{x\}\, ,\, \{x, y\}\, \}$ et donc

$$a \times b = \{ z \in \mathcal{P}(\mathcal{P}(a \cup b))\ ;\ \exists x\, \exists y\, (z = (x, y)) \wedge (x \in a) \wedge (y \in b)\, \}\ .$$ ∎

Axiome de l'infini :

$$\exists x\ \ [(\emptyset \in x) \wedge \forall y\, (y \in x \Rightarrow y \cup \{y\} \in x)]\ .$$

Cet axiome nous permettra de construire $\mathbb{N}$. Remarquons que $\emptyset \in x$, donc $\{\emptyset\} \in x$, par suite $\{\, \emptyset, \{\emptyset\}\, \} \in x$, d'où $\{\, \emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\, \}\, \} \in x$, ...

Axiome du choix :
Tout produit cartésien d'une famille non vide d'ensembles non vides est non vide.
Cet axiome ne fait pas partie de la théorie classique de Zermelo-Fraenkel. Historiquement il fit l'objet de nombreuses controverses et nous distinguerons les énoncés obtenus grâce à son utilisation. Il possède différentes formes équivalentes nous en citerons quelques-unes à la section 5.

2 Relations et applications

2.1. Généralités

2.1.1. Définition . Soient E et F deux ensembles. On appelle *relation* de E vers F toute partie R de $E \times F$; on note alors xRy au lieu de $(x, y) \in R$. Lorsque $E{=}F$ on dit que R est une relation sur E.

2.1.2. Définitions. On dit qu'une relation R sur E est :

- *réflexive* si $\forall x \in E \quad xRx$;
- *symétrique* si $\forall (x,y) \in E^2 \quad xRy \Rightarrow yRx$;
- *antisymétrique* si $\forall (x,y) \in E^2 \quad (xRy \quad \text{et} \quad yRx) \Rightarrow x = y$;
- *transitive* si $\forall (x,y,z) \in E^3 \quad (xRy \quad \text{et} \quad yRz) \Rightarrow xRz$.

2.1.3. Définition. On dit qu'une relation G de E vers F est une *application de E vers F (ou de E dans F)* si tout $x \in E$ est en relation avec un unique élément y de F, on note alors $y = G(x)$:

$$\forall x \in E \quad \exists y \in F \quad (\, xGy \quad \text{et} \quad (\forall z \in F \; xGz \Rightarrow y = z)\,) \; .$$

Plus globalement on utilise également les notations $G : E \longrightarrow F$ et $x \longmapsto G(x)$.

2.1.4. Notations. Soient E et F des ensembles. On notera F^E l'ensemble des applications de E vers F.

2.1.5. Exemples. Soient E et F des ensembles.

a) Soit $b \in F$; on définit l'application constante $k_b \in F^E$ par : $\forall x \in E \quad k_b(x) = b$.

b) On définit l'application identique de E par : $\forall x \in E \quad \mathrm{Id}_E(x) = x$.

2.1.6. Définition. Soient E, F, G des ensembles, $f \in F^E$ et $g \in G^F$. On appelle *composée* de g et f l'application de G^E, notée $g \circ f$, définie par : $\forall x \in E \quad (g \circ f)(x) = g(f(x))$.

2.2. Applications injectives et surjectives

2.2.1. Définitions. Soient E et F deux ensembles et f une application de E dans F. On dit que :

- f est *injective* si $\forall (x,x') \in E^2 \quad f(x) = f(x') \Rightarrow x = x'$.
- f est *surjective* si $\forall y \in F \quad \exists x \in E \quad y = f(x)$.
- f est *bijective* si f est injective et surjective, c'est à dire si pour tout $y \in F$ il existe un unique $x \in E$ tel que $y = f(x)$.
  Dans ce cas il existe une unique application notée f^{-1} appartenant à E^F caractérisée par $\forall x \in E \quad \forall y \in F \quad y = f(x) \Leftrightarrow x = f^{-1}(y)$; on dit que f^{-1} est la *bijection réciproque* de f. On a alors $f \circ f^{-1} = \mathrm{Id}_F$ et $f^{-1} \circ f = \mathrm{Id}_E$.

2.2.2. Proposition. *Soient E, F, G des ensembles, $f \in F^E$ et $g \in G^F$.*

(i) *Si f et g sont injectives alors $g \circ f$ est injective.*

(ii) *Si f et g sont surjectives alors $g \circ f$ est surjective.*

(iii) *Si f et g sont bijectives alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

(iv) *Si $g \circ f$ est injective alors f est injective.*

(v) *Si $g \circ f$ est surjective alors g est surjective.*

(vi) *Si $g \circ f$ est bijective alors f est injective et g est surjective, (mais f et g ne sont pas nécessairement bijectives).*

Preuve.

(i) Soient x et x' dans E tels que $g \circ f(x) = g \circ f(x')$. Par injectivité de g on obtient $f(x) = f(x')$, puis par injectivité de f, on a $x = x'$.

(ii) Soit $z \in G$. D'après la surjectivité de g, il existe $y \in F$ tel que $z = g(y)$, puis par surjectivité de f, il existe $x \in E$ tel que $y = f(x)$. D'où $z = g(f(x)) = g \circ f(x)$.

(iii) Les assertions (i) et (ii) assurent que $g \circ f$ est bijective ; on vérifie alors facilement que $f^{-1} \circ g^{-1}$ est la bijection réciproque de $g \circ f$.

(iv) Soient x et x' dans E tels que $f(x) = f(x')$. On a alors $g \circ f(x) = g \circ f(x')$. Par injectivité de $g \circ f$, on obtient $x = x'$.

(v) Soit $z \in G$. Par surjectivité de $g \circ f$, il existe $x \in E$ tel que $z = g \circ f(x)$. Par suite $y = f(x)$ appartient à F et $g(y) = z$.

(vi) Les assertions (iv) et (v) assurent que f est injective et g surjective. Donnons un exemple où elles ne sont pas bijectives : (†)[2] Soient f et g de $\mathbb{N}$ dans $\mathbb{N}$ définies pour tout $n \in \mathbb{N}$ par $f(n) = n+1$ et $g(n) = \begin{cases} 0 & \text{si } n = 0 \\ n-1 & \text{sinon} \end{cases}$. Il est clair que $g \circ f = \mathrm{Id}_{\mathbb{N}}$ bien que f ne soit pas surjective ni g injective. ∎

2.2.3. Définition. Soit E un ensemble. On appelle *permutation* de E toute bijection de E dans lui-même et on note $\mathcal{S}(E)$ l'ensemble des permutations de E.

[2]Le signe (†) signale un énoncé faisant appel à des notions connues du lecteur mais non encore exposées.

2.3. Loi de composition interne

2.3.1. Définitions. Soit E un ensemble. Une application de $E \times E$ vers E est appelée *opération interne* ou *loi de composition* sur E. On utilise généralement une notation de type opération :

$$\begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x * y \end{array} \qquad \text{(au lieu du signe } * \text{ on utilise aussi } +\,,\ \times\,,\ \cdot\,,\ \circ\,,\ \ldots)$$

Soit $*$ une opération interne sur E. On dit que $*$

- est *associative* si $\forall (x,y,z) \in E^3 \quad (x*y)*z = x*(y*z)$,
- est *commutative* si $\forall (x,y) \in E^2 \quad x*y = y*x$,
- *admet un élément neutre à gauche (resp. à droite)* si

$$\exists e \in E \quad \forall x \in E \quad e*x = x \quad (\text{resp.} \quad x*e = x)\,,$$

- *admet un élément neutre* si elle admet un élément neutre à gauche et à droite,
- est *distributive* par rapport à une autre loi $+$ si

$$\forall (x,y,z) \in E^3 \quad \big((x+y)*z = (x*z)+(y*z)\big) \quad \text{et} \quad \big(z*(x+y) = (z*x)+(z*y)\big)\,,$$

On dit qu'un élément a de E est

- *régulier à gauche (resp. à droite)* si

$$\forall (x,y) \in E^2 \quad (a*x = a*y) \Rightarrow (x=y) \quad (\text{resp.} \quad (x*a = y*a) \Rightarrow (x=y)\ ),$$

- *régulier* s'il est régulier à gauche et à droite,
- *inversible à gauche (resp. à droite)* s'il existe $x \in E$ tel que $x*a = e$ (resp. $a*x = e$) où e désigne l'élément neutre de $*$,
- *inversible* s'il est inversible à gauche et à droite, on note alors son (unique) inverse a^{-1}.

2.3.2. Exemple. Soit E un ensemble. La composition des applications $\circ$ est une opération interne sur E^E. Cette loi de composition est associative, Id_E est l'élément neutre et l'ensemble des éléments inversibles est $\mathcal{S}(E)$.

3 Relation d'équivalence

3.1. Ensemble quotient

3.1.1. Définitions. Une relation R sur E est une *relation d'équivalence* si elle est réflexive, symétrique et transitive.
Pour tout $x \in E$ on appelle alors *classe d'équivalence* de x, l'ensemble, noté $\overline{x}$, des éléments qui lui sont équivalents ; on dit que x est un *représentant* de sa classe $\overline{x}$.
L'ensemble des classes d'équivalence, noté E/R, est appelé *ensemble quotient*.

3.1.2. Proposition. *Soit R une relation d'équivalence sur un ensemble E.*

(*i*) *Deux classes d'équivalence sont disjointes ou confondues.*

(*ii*) *La relation R définit une partition de E.*

(*iii*) *L'application p de E vers E/R qui à x associe sa classe $\overline{x}$, est une surjection appelée surjection canonique.*

Preuve.

(*i*) Soient x et y dans E. Si xRy, alors pour tout $z \in \overline{x}$ on a zRx. Par transitivité on déduit zRy et donc z appartient à $\overline{y}$. D'où $\overline{x} \subset \overline{y}$; grâce à la symétrie on obtient l'égalité $\overline{x} = \overline{y}$.
Si maintenant $x \not R\, y$, montrons que $\overline{x} \cap \overline{y} = \emptyset$. Supposons qu'il existe $z \in \overline{x} \cap \overline{y}$. On a alors zRx et zRy, d'où par symétrie et transitivité xRy, ce qui est impossible. Donc $\overline{x} \cap \overline{y} = \emptyset$.

(*ii*) Les classes d'équivalence sont des parties non vides de E, puisque $x \in \overline{x}$. Elles sont 2 à 2 disjointes, d'après (i) et leur union est égale à E, car tout élément x de E appartient à une classe (la sienne).

(*iii*) Les définitions de E/F et de l'application p impliquent que p est surjective. ∎

3.2. Théorème de factorisation

3.2.1. Proposition. *Soient E et F des ensembles, $f \in F^E$ et R une relation d'équivalence sur E telle que :* $\forall (x,y) \in E^2 \quad x\,R\,y \Rightarrow f(x) = f(y)$.
Alors il existe une unique application $\overline{f} : E/R \longrightarrow F$ telle que $f = \overline{f} \circ p$ où p désigne la surjection canonique de E sur E/R.

Preuve. Unicité de $\overline{f}$: Soit g de E/R dans F telle que $f = g \circ p$. Pour tout $\alpha \in E/R$, il existe $x \in E$ tel que $\alpha = p(x)$ et on a donc

$$g(\alpha) = g \circ p(x) = f(x) = \overline{f}(\alpha) \ .$$

D'où l'unicité.
Existence : Pour tout $\alpha \in E/R$, si $x \in E$ et $y \in E$ sont tels que $p(x) = p(y) = \alpha$, on a alors xRy et donc $f(x) = f(y)$. On peut donc définir $\overline{f}(\alpha) = f(x)$ si $\alpha = p(x)$ (indépendant du représentant choisi). On a alors immédiatement $f = \overline{f} \circ p$. ∎

3.2.2. Théorème. *Soit f une application de E dans F. La relation R_f définie sur E par : $xR_fy \Leftrightarrow f(x) = f(y)$ est une relation d'équivalence. Soient p la surjection canonique de E sur E/R_f et i l'injection canonique de $f(E)$ dans F. Alors il existe une unique application $\overline{f}$ de E/R_f dans $f(E)$ telle que le diagramme suivant soit commutatif (c'est à dire $f = i \circ \overline{f} \circ p$) :*

$$\begin{array}{ccc} E & \xrightarrow{\ f\ } & F \\ \Big\downarrow{\scriptstyle p} & & \Big\uparrow{\scriptstyle i} \\ E/R_f & \xrightarrow{\ \overline{f}\ } & f(E) \end{array}$$

De plus $\overline{f}$ est une bijection.

Preuve. Il est immédiat que R_f est une relation d'équivalence. La proposition précédente appliquée à $x \longmapsto f(x)$ de E dans $f(E)$ assure l'existence d'une unique application $\overline{f}$ de E/R_f dans $f(E)$ telle que le diagramme soit commutatif.
Montrons le caractère bijectif de $\overline{f}$. Pour tout $z \in f(E)$, il existe $x \in E$ tel que $f(x) = z$. Posons $\alpha = p(x)$ on a $\overline{f}(\alpha) = f(x) = z$; d'où la surjectivité de $\overline{f}$. Soient $\alpha = \overline{x}$ et $\beta = \overline{y}$ deux classes telles que $\overline{f}(\alpha) = \overline{f}(\beta)$. On a donc $f(x) = i \circ \overline{f} \circ p(x) = \overline{f}(\alpha) = \overline{f}(\beta) = f(y)$ c'est à dire xR_fy soit encore $\alpha = \beta$; d'où l'injectivité de $\overline{f}$. ∎

3.2.3. Exemple. (†) Si $E = \mathbb{N}$, $F = \mathbb{Z}$ et si pour tout $n \in \mathbb{N}$ on a $f(n) = (-1)^n$, alors $m\,R_f\,n$ si et seulement si m et n ont même parité. La relation R_f définit deux classes d'équivalence : $\mathbb{P}$ ensemble des entiers pairs et $\mathbb{I}$ ensemble des entiers impairs ; l'ensemble quotient E/R_f est $\{\mathbb{P}, \mathbb{I}\}$ et on a $\overline{f}(\mathbb{P}) = 1$, $\overline{f}(\mathbb{I}) = -1$.

3.3. Compatibilité avec une opération interne

3.3.1. Définitions. Soit E un ensemble muni d'une opération interne $*$ et d'une relation d'équivalence R. On dit que R est *compatible à gauche* (resp. à droite) avec $*$ si

$$\forall (x, x', y) \in E^3 \quad (xRx') \Rightarrow (y * x\, R\, y * x') \quad (\text{resp.} \quad x * y\, R\, x' * y\,).$$

On dit que R est *compatible* avec $*$ si

$$\forall (x, x', y, y') \in E^4 \quad ((xRx') \quad \text{et} \quad (yRy')) \Rightarrow (x * y\, R\, x' * y')\,.$$

3.3.2. Proposition. *Soit E un ensemble muni d'une opération interne $*$. Une relation d'équivalence R sur E est compatible avec $*$ si et seulement si elle est compatible à droite et à gauche avec $*$.*

Preuve. La preuve est laissée au lecteur. ∎

3.3.3. Théorème. *Soit E un ensemble muni d'une opération interne $\cdot$ et d'une relation d'équivalence R compatible avec $\cdot$. Désignons par p la surjection canonique de E sur E/R. Il existe sur E/R une unique opération interne $*$ telle que*

$$\forall (x,y) \in E^2 \quad p(x) * p(y) = p(x \cdot y) \ .$$

Si $\cdot$ est associative (resp. commutative, resp. admet un élément neutre), alors $*$ possède la même propriété.

Preuve. Soient α et β appartenant à E/R. Il existe $(x,y) \in E^2$ tel que $\alpha = p(x)$ et $\beta = p(y)$. Si une loi satisfaisant aux conditions existe on a : $\alpha * \beta = p(x) * p(y) = p(x \cdot y)$, d'où l'unicité. Pour prouver l'existence, nous allons définir $\alpha * \beta$ en posant $\alpha * \beta = p(x \cdot y)$. Mais nous devons nous assurer que notre définition est indépendante des réprésentants choisis : Si x' et y' dans E sont tels que $\alpha = p(x')$ et $\beta = p(y')$, on a alors xRx' et yRy' ; la compatibilité implique alors $(x \cdot y)\, R\, (x' \cdot y')$, i.e. $p(x \cdot y) = p(x' \cdot y')$. La loi $*$ est donc bien définie.
Supposons que $\cdot$ est associative et soient α, β et γ dans E/R. Il existe $(x,y,z) \in E^3$ tel que $\alpha = p(x)$, $\beta = p(y)$ et $\gamma = p(z)$ et on a :

$$\begin{array}{ccccccccc} (\alpha * \beta) * \gamma & = & (p(x) * p(y)) * p(z) & = & p(x \cdot y)) * p(z) & = & p((x \cdot y) \cdot z) & = & p(x \cdot (y \cdot z)) \\ & = & p(x) * p(y \cdot z) & = & \alpha * (\beta * \gamma) \ . & & & & \end{array}$$

Pour la commutativité, la démonstration est analogue. Si e est élément neutre pour $\cdot$, on vérifie aisément que $p(e)$ est élément neutre pour $*$. ∎

4 Relation d'ordre

4.1. Ensemble ordonné

4.1.1. Définitions. Une relation R sur un ensemble E est une *relation d'ordre* si elle est réflexive, antisymétrique et transitive.
On dit qu'une relation d'ordre R sur E est un *ordre total* ou que E est *totalement ordonné* si deux éléments quelconques de E sont comparables par R : $\forall (x,y) \in E^2 \quad xRy \quad$ ou $\quad yRx$. Dans le cas contraire on dit que R est un *ordre partiel* ou que E est *partiellement ordonné*.

4.1.2. Exemples.

a) Soit X un ensemble. Alors $\subset$ est un ordre sur $\mathcal{P}(X)$; cet ordre est partiel si X est non vide et non réduit à un singleton.

b) (†) $(\mathbb{N}, \leq)$ est un ensemble totalement ordonné.

c) (†) $E = \{d \in \mathbb{N}^* \ ; \ d$ diviseur propre de $24\}$ muni de $|$, relation *divise*, est un ensemble partiellement ordonné.

4.1.3. Définitions. Soient $(E,\ \leq)$ un ensemble ordonné et $m \in E$.
On dit que m est *maximal* si $\forall x \in E \quad m \leq x \ \Rightarrow\ m = x$.
On dit que m est le *plus grand élément* de E si $\forall x \in E \quad x \leq m$.
Un plus grand élément, s'il existe, est unique ; on le note $\max(E)$.
Le lecteur écrira lui-même les définitions d'élément *minimal* et de *plus petit élément* noté $\min(E)$.

4.1.4. Exemples. Reprenons les exemples précédents :

a) X est le plus grand élément de $(\mathcal{P}(X),\ \subset)$.

b) (†) Pas d'élément maximal dans $(\mathbb{N},\ \leq)$.

c) (†) Pas de plus grand élément dans E, mais 8 et 12 sont des éléments maximaux.

4.2. Ensemble inductif

4.2.1. Définitions. Soient $(E,\ \leq)$ un ensemble ordonné et A une partie de E.
Un élément $m \in E$ est un *majorant* de A si $\forall a \in A \quad a \leq m$.
On dit que A est une *chaîne* de E si A est une partie de E non vide et totalement ordonnée.
On dit que E est *inductif* si E est non vide et si toute chaîne de E admet un majorant.

4.2.2. Exemple. (†) Soient V un K-espace vectoriel non réduit à $\{0\}$ et F un sous-espace vectoriel de V. Soit $\mathcal{E}$ l'ensemble des sous-espaces vectoriels de V en somme directe avec F i.e. $\mathcal{E} = \{\, G \text{ sous-espace vectoriel de } V\ ;\ F \cap G = \{0\}\,\}$. Alors $(\mathcal{E},\ \subset)$ est inductif.

Preuve. L'ensemble $\mathcal{E}$ est non vide car $\{0\} \in \mathcal{E}$ et il est clair que $\mathcal{E}$ est ordonné par $\subset$. Soit $\mathcal{C}$ une chaîne de $\mathcal{E}$. Posons $H = \bigcup_{G \in \mathcal{C}} G$. Montrons que H est un sous-espace vectoriel. Soient $(x, y) \in H^2$ et $(\lambda, \mu) \in K^2$. Par définition de H, il existe $G \in \mathcal{C}$ tel que $x \in G$ et $G' \in \mathcal{C}$ tel que $y \in G'$. Comme $\mathcal{C}$ est une chaîne, G et G' sont comparables pour l'inclusion ; on a donc $G \subset G'$ ou $G' \subset G$. Sans perte de généralité nous pouvons supposer que $G \subset G'$. Alors comme G' est un sous-espace vectoriel, le vecteur $\lambda x + \mu y$ appartient à G' et donc à H. De plus $F \cap H = F \cap (\bigcup_{G \in \mathcal{C}} G) = \bigcup_{G \in \mathcal{C}} F \cap G = \{0\}$. Donc H appartient à $\mathcal{E}$ et par construction H est un majorant de la chaîne $\mathcal{C}$. ∎

5 Axiome du choix et Axiome de Zorn

5.1. Axiome du choix

5.1.1. Définition. Soit E un ensemble non vide. On appelle *fonction de choix* dans E, toute application φ de $\mathcal{P}(E)\backslash\{\emptyset\}$ dans E telle que $\forall A \subset E \quad A \neq \emptyset \ \Rightarrow \varphi(A) \in A$.

5.1.2. Axiome du choix. *Tout ensemble non vide possède une fonction de choix.*

5.1.3. Proposition. *L'axiome du choix est équivalent à tout produit cartésien d'une famille non vide d'ensembles non vides est non vide.*

Preuve. Supposons que l'on ait l'axiome du choix. Soit $E = \prod_{i\in I} E_i$ avec $I \neq \emptyset$ et pour tout $i \in I$ $E_i \neq \emptyset$. Posons $X = \bigcup_{i\in I} E_i$. Il existe dans X une fonction de choix φ. On a donc $\forall i \in I$ $\varphi(E_i) \in E_i$ d'où $(\varphi(E_i))_{i\in I}$ est élément de E.
Réciproquement soit X un ensemble non vide. Posons $P = \mathcal{P}(X)\backslash\{\emptyset\}$. Cet ensemble est non vide il contient au moins un singleton ; par suite $E = \prod_{A\in P} A$ est non vide. Il existe donc $(x_A)_{A\in P} \in E$. Il suffit de considérer $\varphi : A \longmapsto x_A$ pour obtenir une fonction de choix dans X. ∎

5.1.4. Exemple d'utilisation de l'axiome du choix. (†) *Soient E et F des espaces métriques, $f \in F^E$ et $x \in X$. L'application f est continue en a si pour toute suite $(x_n)_{n\in\mathbb{N}}$ de E convergeant vers a on a $\lim_{n\to\infty} f(x_n) = f(a)$.*
L'assertion se démontre par la contraposée en supposant f non continue en x. On a alors

$$\exists\varepsilon > 0 \quad \forall\eta > 0 \quad \exists x \in E \quad d(x,a) < \eta \quad \text{et} \quad d(f(x), f(a)) \geq \varepsilon \ .$$

Pour tout $n \in \mathbb{N}^*$ on applique ceci avec $\eta_n = \dfrac{1}{n}$, il existe x_n telle que $d(x_n, a) < \dfrac{1}{n}$ et $d(f(x_n), f(a)) \geq \varepsilon$. Pour choisir la suite x_n il nous a fallu faire une infinité de choix ; ce qui n'est possible que si on utilise l'axiome du choix. La suite (x_n) converge vers a, mais $(f(x_n))$ ne converge pas vers $f(a)$. ∎

5.2. Axiome de Zorn

5.2.1. Axiome de Zorn. *Tout ensemble inductif admet un élément maximal.*

5.2.2. Exemple d'utilisation de Zorn : (†) Existence d'un supplémentaire pour un sous-espace vectoriel . *Soit F un sous-espace vectoriel d'un espace vectoriel V sur un corps K. Alors F admet un supplémentaire dans V.*

Preuve. On a montré en 4.2.2 que $\mathcal{E} = \{\, G$ sous-espace vectoriel de V ; $F \cap G = \{0\}\,\}$ muni de $\subset$ est inductif. D'après l'axiome de Zorn, $\mathcal{E}$ admet un élément maximal M. On a $F \cap M = \{0\}$ et il reste à montrer que $F + M = V$. Supposons qu'il existe $x \in V$ tel que $x \notin F + M$. Considérons $N = M \oplus Kx$ (la somme est bien directe car $x \notin M$). Montrons que $F \cap N = \{0\}$. Soit $y \in F \cap N$. Il existe $m \in M$ et $\lambda \in K$ tels que $y = m + \lambda x$. Si $\lambda \neq 0$ on peut écrire $x = \lambda^{-1}(y - m)$, ce qui contredit le fait que $x \notin F + M$. On a donc $\lambda = 0$ et $y = m$ appartient à $F \cap M$; par conséquent $y = 0$. Il en résulte que $N \in \mathcal{E}$. Ceci contredit la maximalité de M dans $(\mathcal{E}, \subset)$. Notre supposition était donc fausse et $V = F \oplus M$. ∎

5.2.3. Théorème. *L'axiome du choix et l'axiome de Zorn sont équivalents.*

Nous admettons ce théorème.

6 L'ensemble des entiers naturels

6.1. Construction de $\mathbb{N}$

Les axiomes évoqués précédemment permettent de construire $\mathbb{N}$. On obtient alors le théorème 6.1.1 que nous admettons. Les propriétés (P_1), (P_2), (P_3), appelées *Axiomes de Péano*, figurant dans ce théorème peuvent servir de définition axiomatique pour l'ensemble $\mathbb{N}$, car d'après la deuxième partie de ce théorème, elles caractérisent $\mathbb{N}$. La propriété (P_3) est la justification du principe de récurrence (cf proposition 6.3.3).

6.1.1. Théorème. *Il existe un triplet* $(\mathbb{N}, 0, S)$ *où* $\mathbb{N}$ *est un ensemble,* $0 \in \mathbb{N}$ *et* S *une application de* $\mathbb{N}$ *dans* $\mathbb{N}$*, tel que*

(P_1) *S est injective.*

(P_2) *L'image de S est $\mathbb{N}\backslash\{0\}$ noté $\mathbb{N}^*$.*

(P_3) *Si $A \subset \mathbb{N}$ vérifie $0 \in A$ et A stable par S, alors $A = \mathbb{N}$.*

Si $(\mathbb{N}', 0', S')$ est un autre triplet vérifiant les trois propriétés (P_1), (P_2), (P_3) alors il existe une unique application φ de $\mathbb{N}$ dans $\mathbb{N}$' telle que $\varphi(0) = 0'$ et $\varphi \circ S = S' \circ \varphi$. De plus φ est bijective.
On a donc le diagramme commutatif :

$$\begin{array}{ccccc} 0 & & \mathbb{N} & \xrightarrow{S} & \mathbb{N} \\ \downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ 0' & & \mathbb{N}' & \xrightarrow{S'} & \mathbb{N}' \end{array}$$

6.1.2. Définitions. Conservons les données du théorème précédent. L'ensemble $\mathbb{N}$ est *l'ensemble des entiers naturels*, l'élément 0 est appelé *zéro* et l'application S est appelée *successeur*. Le successeur de 0 est appelé *un* et est noté 1 $(1 = S(0))$. Le successeur de 1 est appelé *deux* et est noté généralement 2 $(2 = S(1))$. Le successeur de 2 est appelé *trois* et est noté généralement 3 $(3 = S(2))$. ...

6.2. Opérations dans $\mathbb{N}$

6.2.1. Théorème. *Il existe dans* $\mathbb{N}$ *une unique opération interne, notée* $+$ *telle que :*
$\forall n \in \mathbb{N} \quad 0+n=n$,
$\forall (m,n) \in \mathbb{N}^2 \quad S(m)+n=S(m+n)$.

Nous admettons ce théorème dont la démonstration est assez longue.

6.2.2. Proposition. *Dans* $\mathbb{N}$ *l'addition est associative et commutative, 0 est élément neutre, tout élément est régulier. Pour tout* $n \in \mathbb{N}$ *on a* $S(n)=n+1$. *Pour tous* p *et* q *de* $\mathbb{N}$ *on a* $p+q=0 \Leftrightarrow p=q=0$.

Preuve. Démontrons l'associativité. A q et r fixés dans $\mathbb{N}$, considérons l'ensemble $A=\{p \in \mathbb{N}\,;\ (p+q)+r=p+(q+r)\}$. Il est clair que $0 \in A$ et que si $p \in A$ alors

$$(S(p)+q)+r=S(p+q)+r=S((p+q)+r)=S(p+(q+r))=S(p)+(q+r)\ .$$

Donc $S(p) \in A$ et d'après (P_3), $A=\mathbb{N}$.
A l'exception de la dernière assertion que nous allons démontrer, les autres propriétés s'obtiennent de manière analogue.
Supposons que $p+q=0$, si $p \neq 0$ il existe $p' \in \mathbb{N}$ tel que $p=S(p')$ (P_2). On a alors $0=p+q=S(p')+q=S(p'+q)$ ce qui est impossible d'après (P_2). ∎

On peut également définir sur $\mathbb{N}$, une multiplication.

6.2.3. Théorème. *Il existe dans* $\mathbb{N}$ *une unique opération interne, notée* $\cdot$ *telle que :*
$\forall n \in \mathbb{N} \quad 0 \cdot n=0$,
$\forall (m,n) \in \mathbb{N}^2 \quad (m+1) \cdot n=m \cdot n+n$.
Dans $\mathbb{N}$ *la multiplication est associative, commutative, et distributive par rapport à l'addition, 1 est élément neutre, tout élément de* $\mathbb{N}^*$ *est régulier.*

Preuve. La démonstration est analogue aux précédentes. ∎

6.3. Relation d'ordre sur $\mathbb{N}$

6.3.1. Définitions. On dit qu'un entier m est *inférieur ou égal* à un entier n, ce que l'on note $m \leq n$, s'il existe $d \in \mathbb{N}$ tel que $n=m+d$. On écrit $m<n$ si $m \leq n$ et $m \neq n$.
On note $[m,n]_{\mathbb{N}}=\{\,p \in \mathbb{N}\,;\ (m \leq p) \quad \text{et} \quad (p \leq n)\,\}$ et $\mathbb{E}_n$ l'ensemble $[1,n]_{\mathbb{N}}$.

6.3.2. Théorème.

(i) $(\mathbb{N},\leq)$ *est un ensemble totalement ordonné et toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*

(*ii*) *Pour tous* $m, n \in \mathbb{N}$ *on a* $m < n \Leftrightarrow (m+1) \leq n$.

Preuve. La réfléxivité et la transitivité de $\leq$ sont immédiates. Vérifions l'antisymétrie. Si $m \leq n$ et $n \leq m$ il existe d et d' dans $\mathbb{N}$ tels que $n = m + d$ et $m = n + d'$; d'où $m = m + d + d'$. Par régularité il vient $0 = d + d'$ et il suffit d'appliquer la proposition 6.2.2. Donc $\mathbb{N}$ est ordonné.
Démontrons la deuxième assertion. Soient m et n dans $\mathbb{N}$. On a les équivalences :

$$\begin{aligned} n \leq m &\Leftrightarrow \exists d \in \mathbb{N}\ m = n + d \\ n < m &\Leftrightarrow \exists d \in \mathbb{N}\ (m = n + d) \quad \text{et} \quad (d \neq 0) \\ &\Leftrightarrow \exists d' \in \mathbb{N}\ m = n + (d' + 1) \\ &\Leftrightarrow n + 1 \leq m\ . \end{aligned}$$

Il reste à montrer que toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Soit A une partie non vide de $\mathbb{N}$ et soit M l'ensemble des minorants de A. Alors $0 \in M$. Soit $a \in A$; alors $(a+1) \notin M$, donc $M \neq \mathbb{N}$. D'après la contraposée de (P_3) il exite $n_0 \in M$ tel que $(n_0 + 1) \notin M$. Donc n_0 est un minorant de A ; si $n_0 \notin A$ alors pour tout $n \in A$ on a $n_0 < n$, d'où $(n_0 + 1) \leq n$; ce qui est absurde. L'entier n_0 est donc le plus petit élément de A. ∎

6.3.3. Proposition. *Soit* P *une assertion dépendant de* $n \in \mathbb{N}$.

(*i*) *Supposons que* $P(0)$ *est vraie et que pour tout* $n \in \mathbb{N}$, $P(n)$ *vraie implique* $P(n+1)$ *vraie. Alors* $P(n)$ *est vraie pour tout* $n \in \mathbb{N}$.

(*ii*) *Supposons que* $P(0)$ *est vraie et que pour tout* $n \in \mathbb{N}$, $P(k)$ *vraie pour tout* $k \in [0, n]$ *implique* $P(n+1)$ *vraie. Alors* $P(n)$ *est vraie pour tout* $n \in \mathbb{N}$.

Preuve. (i) Posons $A = \{n \in \mathbb{N}\ ;\ P(n) \text{ vraie}\}$. Par hypothèse on a $0 \in A$ et A est stable par S, d'après P_3, $A = \mathbb{N}$.
(ii) Il suffit d'appliquer (i) avec $Q(n) = P(0) \wedge \cdots \wedge P(n)$. ∎

7 Cardinaux

7.1. Ensembles équipotents

7.1.1. Définitions. Soient X et Y deux ensembles. On dit que X et Y sont *équipotents* s'il existe une bijection de X sur Y. On notera $X \simeq Y$. On dira aussi que X et Y ont même *cardinal* s'ils sont équipotents ; on écrira cela $\mathrm{card}\,(X) = \mathrm{card}\,(Y)$.

7.1.2. Lemme. *Soient m et n deux entiers. Les ensembles $[1,m]_{\mathbb{N}}$ et $[1,n]_{\mathbb{N}}$ sont équipotents si et seulement si $m=n$.*

Preuve. Démontrons cette propriété par récurrence sur n. C'est évident si $n=0$ car alors $[1,n]_{\mathbb{N}}=\emptyset$. Supposons la vraie au rang n. Soit φ une bijection de $[1,n+1]_{\mathbb{N}}$ sur $[1,m]_{\mathbb{N}}$; nécessairement on a $m\neq 0$. Considèrons la permutation σ de $[1,m]_{\mathbb{N}}$ qui échange m et $\varphi(n+1)$, et laisse les autres entiers fixes. Alors $\psi=\sigma\circ\varphi$ est une bijection entre $[1,n+1]_{\mathbb{N}}$ et $[1,m]_{\mathbb{N}}$, telle que $\psi(n+1)=m$; par restriction ψ définit une bijection entre $[1,n]_{\mathbb{N}}$ et $[1,m-1]_{\mathbb{N}}$. Par hypothèse de récurrence, on a alors $n=m-1$, soit $n+1=m$. ∎

7.1.3. Définitions. Un ensemble X est dit *fini* s'il existe un entier $n\in\mathbb{N}$ (unique d'après le lemme) tel que X soit équipotent à $[1,n]_{\mathbb{N}}$. On note alors $\mathrm{card}\,(X)=n$.
$\emptyset=[1,0]_{\mathbb{N}}$, donc $\mathrm{card}\,(\emptyset)=0$ et $\{x\}\simeq[1,1]_{\mathbb{N}}$, donc $\mathrm{card}\,(\{x\})=1$.
Un ensemble qui n'est pas fini est dit *infini*.

7.1.4. Proposition. *$\mathbb{N}$ est un ensemble infini.*

Preuve. Supposons qu'il existe φ bijective de $\mathbb{N}$ sur $[1,n]_{\mathbb{N}}$. L'application successeur S étant une bijection de $\mathbb{N}$ sur $\mathbb{N}^*$, l'application $\psi=\varphi\circ S^{-1}$ est une bijection de $\mathbb{N}^*$ sur $[1,n]_{\mathbb{N}}$. En posant $\psi(0)=n+1$ on obtient une bijection entre $\mathbb{N}$ et $[1,n+1]_{\mathbb{N}}$. Ce qui conduit à une contradiction, car d'après le lemme précédent les ensembles $[1,n]_{\mathbb{N}}$ et $[1,n+1]_{\mathbb{N}}$ ne sont pas équipotents. ∎

7.1.5. Remarque. $\mathbb{N}$ apparaît comme l'ensemble des cardinaux finis (alors que l'ensemble de tous les cardinaux n'existe pas).

7.2. Comparaison de deux cardinaux

7.2.1. Lemme. *Soient A, B, A', B' des ensembles tels que $A'\simeq A$ et $B'\simeq B$. S'il existe une injection de A dans B, alors il existe une injection de A' dans B'.*

Preuve. Soit φ (respectivement ψ) une bijection de A dans A' (respectivement de B dans B'). Si f est une injection de A dans B alors $\psi\circ f\circ\varphi^{-1}$ est une injection de A' dans B'. ∎

7.2.2. Définition. Soient a et b deux cardinaux. On notera $a\leq b$ s'il existe deux ensembles A et B avec $a=\mathrm{card}\,(A)$, $b=\mathrm{card}\,(B)$ et une injection de A dans B (d'après le lemme ceci est indépendant des ensembles choisis).

7.2.3. Propriétés immédiates. Soient a, b, c des cardinaux.
$a\leq a$ (on prend l'identité) et si $a\leq b$ et $b\leq c$ alors $a\leq c$ (composition des injections).

7.2.4. Théorème de Cantor-Bernstein. *Soient A et B deux ensembles. S'il existe une injection de A dans B et s'il existe une injection de B dans A, alors A et B sont équipotents.*
Autre version : *Soient a et b deux cardinaux. Si $a \leq b$ et $b \leq a$ alors $a = b$.*

Preuve. Soient f une injection de A dans B et g une injection de B dans A. On va construire une bijection φ de A dans B.
Puisque g est injective il existe une application h bijective de $g(B)$ dans B qui à tout $x \in g(B)$ associe y son unique antécédent par g. On a donc

$$\forall y \in B \quad h \circ g(y) = y \quad \text{et} \quad \forall x \in g(B) \quad g \circ h(x) = x \ .$$

Posons $A_0 = A \backslash g(B)$ (complémentaire dans A de $g(B)$), puis par récurrence pour tout $n \in \mathbb{N}$ $A_{n+1} = g \circ f(A_n)$.
Considérons $X = \bigcup_{n \in \mathbb{N}} A_n$ et $\varphi : \begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & f(x) \text{ si } x \in X \\ x & \longmapsto & h(x) \text{ si } x \notin X. \end{array}$
Injectivité de φ : Soient x et x' dans A tels que $\varphi(x) = \varphi(x')$. Si x et x' sont dans X alors $x = x'$ par injectivité de f. Si x et x' sont dans $A \backslash X$ alors $x = x'$ par injectivité de h. Enfin si $x \in X$ et $x' \notin X$ on a $f(x) = h(x')$ et il existe $n \in \mathbb{N}$ tel que $x \in A_n$; d'où $g(f(x)) \in A_{n+1}$, or $g(f(x)) = g(h(x')) = x'$, ce qui est une contradiction.
Surjectivité de φ : Soit $y \in B$. Si $g(y) \notin X$ alors $y = h(g(y)) = \varphi(g(y))$; donc $y \in \varphi(A)$. Sinon $g(y) \in X$ et comme $g(y) \notin A_0$, il existe $n \in \mathbb{N}^*$ tel que $g(y) \in A_n$. D'où l'existence de $x \in A_{n-1}$ tels que $g(y) = g \circ f(x)$. Par injectivité de g on en déduit $y = f(x) = \varphi(x)$.
L'application φ est bijective et le théorème est démontré. ∎

7.3. Ensembles dénombrables

7.3.1. Définitions. On dit qu'un ensemble est *dénombrable* s'il est en bijection avec $\mathbb{N}$. On appelle *aleph-zéro*, noté $\aleph_0$, le cardinal de $\mathbb{N}$.

7.3.2. Exemple. $\mathbb{N}^*$, $\mathbb{P}$ ensemble des entiers pairs et $\mathbb{I}$ ensemble des entiers impairs sont des ensembles dénombrables ; soit $\text{card}\,(\mathbb{N}^*) = \text{card}\,(\mathbb{P}) = \text{card}\,(\mathbb{I}) = \aleph_0$.

7.3.3. Corollaire. *Toute partie d'un ensemble dénombrable est finie ou dénombrable.*

Preuve. Soit A une partie infinie de $\mathbb{N}$. Puisque A est non vide on peut poser $u_0 = \min(A)$. De même $A_1 = A \backslash \{u_0\}$ est non vide et $u_1 = \min(A_1)$ existe. On construit par récurrence $A_n = A \backslash \{u_0, \ldots, u_{n-1}\}$ qui est non vide car A est infini, et on pose $u_n = \min(A_n)$. Par construction on a $u_n > u_{n-1}$ et u est une injection (strictement croissante) de $\mathbb{N}$ dans A. Par hypothèse il existe une injection (canonique) de A dans $\mathbb{N}$. On conclut grâce au théorème de Cantor-Bernstein que A est dénombrable.
Si B est une partie infinie d'un ensemble dénombrable E en bijection avec $\mathbb{N}$ grâce à φ, alors B est en bijection avec $\varphi(B)$ partie infinie de $\mathbb{N}$, donc dénombrable. ∎

7.3.4. Proposition .

(*i*) $\mathbb{N} \times \mathbb{N}$ *est dénombrable.*

(*ii*) *Si* X *est dénombrable alors* X^n *est dénombrable, pour tout* $n \in \mathbb{N}^*$.

(*iii*) *Toute union finie d'ensembles dénombrables est dénombrable.*

Preuve. (i) Utilisons le principe de l'énumération diagonale de Cantor. Pour tout n dans $\mathbb{N}$, posons $\Delta_n = \{(p,q) \in \mathbb{N}^2 \,;\; p+q = n\}$. On a alors $\mathbb{N} \times \mathbb{N} = \bigcup_{n\in\mathbb{N}} \Delta_n$ et $\operatorname{card}(\Delta_n) = n+1$. Numérotons les éléments de $\mathbb{N} \times \mathbb{N}$ en attribuant 0 à l'unique élément $(0,0)$ de Δ_0, 1 et 2 respectivement aux éléments $(1,0)$ et $(0,1)$ de Δ_1, et ainsi de suite. Comme $\sum_{k=0}^{n-1} \operatorname{card}(\Delta_k) = \sum_{k=0}^{n-1} (k+1) = \dfrac{n(n+1)}{2}$, au premier élément numéroté de Δ_n, à savoir $(n,0)$, nous attribuerons $\dfrac{n(n+1)}{2}$ (nous avons commencé à 0) et $\dfrac{n(n+1)}{2} + q$ correspondra à $(n-q,q)$.
Par construction, l'application φ définie par $\varphi((p,q)) = \dfrac{(p+q)(p+q+1)}{2} + q$ réalise une bijection entre $\mathbb{N} \times \mathbb{N}$ et $\mathbb{N}$.
(ii) Si X est dénombrable, il existe une bijection φ de X sur $\mathbb{N}$ et $\varphi \times \varphi$ réalise une bijection entre $X \times X$ et $\mathbb{N} \times \mathbb{N}$. Donc $X \times X$ est dénombrable. L'assertion (ii) se démontre alors par récurrence.
(iii) Soit $X = \bigcup_{i=1}^{n} X_i$ avec X_i dénombrable. Pour tout $i = 1, \ldots, n$, il existe φ_i bijection de X_i dans $\mathbb{N}$ (on choisit une bijection dans l'ensemble non vide des bijections de X_i dans $\mathbb{N}$, en tout n choix).

$$\text{Soit } \varphi : \begin{array}{ccc} X & \longrightarrow & \mathbb{N} \times \mathbb{N} \\ x & \longmapsto & (i(x), \varphi_{i(x)}(x)) \end{array} \text{ où } i(x) = \min\{\, i \in [1,n]_{\mathbb{N}} \,;\; x \in X_i\}.$$

Montrons que φ est injective. Si $\varphi(x) = \varphi(y)$ alors $i(x) = i(y) = i$ et $\varphi_i(x) = \varphi_i(y)$; par injectivité de φ_i on a $x = y$.
On obtient donc

$$\operatorname{card}(X) \leq \operatorname{card}(\mathbb{N} \times \mathbb{N}) = \aleph_0 \quad \text{et on a} \quad \aleph_0 \leq \operatorname{card}(X) \qquad \text{car} \quad X_1 \subset X \ .$$

Donc $\operatorname{card}(X) = \aleph_0$ et X est dénombrable. ∎

7.3.5. Proposition . *Dans une théorie avec l'axiome du choix, toute union dénombrable d'ensembles dénombrables est dénombrable.*

Preuve. Soit $X = \bigcup_{i\in\mathbb{N}} X_i$ avec X_i dénombrable. Pour tout $i \in \mathbb{N}$, on peut grâce à l'axiome du choix, choisir une bijection φ_i de X_i dans $\mathbb{N}$. La démonstration se termine alors comme la précédente. ∎

7.3.6. Théorème de Cantor. *Pour tout ensemble A on a* $\text{card}(A) < \text{card}(\mathcal{P}(A))$.

Preuve. Comme l'application $x \longmapsto \{x\}$ est une injection de A dans $\mathcal{P}(A)$, on a donc $\text{card}(A) \leq \text{card}(\mathcal{P}(A))$.
Soit g une application de A dans $\mathcal{P}(A)$. Montrons que g n'est pas surjective.
Soit $B = \{x \in A\,;\ x \notin g(x)\}$. Supposons qu'il existe $y \in A$ tel que $B = g(y)$. A-t-on $y \in B$? On remarque que $y \in B \Leftrightarrow y \notin B$ ce qui est absurde. Il n'existe pas de surjection, donc à fortiori pas de bijection entre A et $\mathcal{P}(A)$. Donc $\text{card}(A) < \text{card}(\mathcal{P}(A))$.

7.3.7. Définition. On dit qu'un ensemble a *la puissance du continu* s'iil est équipotent à $\mathcal{P}(\mathbb{N})$. La terminologie sera justifiée par l'assertion (iv) de la proposition suivante.

7.3.8. Proposition.

(i) $(\dagger)$ *$\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables.*

(ii) *$\mathcal{P}_f(\mathbb{N})$ ensemble des parties finies de $\mathbb{N}$ est dénombrable.*

(iii) *$\mathcal{P}_\infty(\mathbb{N})$ ensemble des parties infinies de $\mathbb{N}$ a la puissance du continu.*

(iv) $(\dagger)$ *$\mathbb{R}$ a la puissance du continu.*

Preuve. (i) $\mathbb{Z} = (-\mathbb{N}) \cup \mathbb{N}^*$ et on applique la proposition 7.3.4. L'inclusion $\mathbb{N} \subset \mathbb{Q}$ prouve que $\aleph_0 \leq \text{card}(\mathbb{Q})$. L'application de $\mathbb{Q}$ dans $\mathbb{Z} \times \mathbb{N}^*$ qui à $r \in \mathbb{Q}$ associe le couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$ avec p et q premiers entre eux, est injective.
Donc $\text{card}(\mathbb{Q}) \leq \text{card}(\mathbb{Z} \times \mathbb{N}^*) = \aleph_0$. On conclut par Cantor-Bernstein.

(ii) Soit φ de $\mathcal{P}_f(\mathbb{N})$ dans $\mathbb{N}$ qui à X associe $\displaystyle\sum_{i \in X} 2^i$ avec la convention habituelle si $X = \emptyset$ alors $\varphi(X) = 0$. Montrons que φ est injective. Il est clair que seul $\emptyset$ a pour image 0. Soient donc X et Y non vides tels que $\varphi(X) = \varphi(Y)$. Considérons m_X (respectivement m_Y) le plus grand élément de X (respectivement de Y) ; on a alors $2^{m_X} \leq \varphi(X) < 2^{m_X+1}$.
Puisque $\varphi(X) = \varphi(Y)$ on a forcément $m_X = m_Y = m$. On considère alors $X \backslash \{m\}$ et $Y \backslash \{m\}$. Il suffit ensuite d'itérer le raisonnement. Par ailleurs l'application $\psi : x \longmapsto \{x\}$ est injective de $\mathbb{N}$ dans $\mathcal{P}_f(\mathbb{N})$. On conclut encore grâce au théorème de Cantor-Bernstein.

(iii) L'application $\psi : x \longmapsto \mathbb{N} \backslash \{x\}$ est injective de $\mathbb{N}$ dans $\mathcal{P}_\infty(\mathbb{N})$. Soit $C = \mathcal{P}_\infty(\mathbb{N}) \backslash \psi(\mathbb{N})$
On a donc $\mathcal{P}(\mathbb{N}) = \mathcal{P}_f(\mathbb{N}) \cup \mathcal{P}_\infty(\mathbb{N}) = \mathcal{P}_f(\mathbb{N}) \cup \Psi(\mathbb{N}) \cup C$ (ces unions étant disjointes). Or $\mathcal{P}_f(\mathbb{N}) \cup \Psi(\mathbb{N})$ est dénombrable donc équipotent à $\Psi(\mathbb{N})$. Il en résulte que $\mathcal{P}(\mathbb{N})$ est équipotent à $\mathcal{P}_f(\mathbb{N}) \cup \Psi(\mathbb{N}) = \mathcal{P}_\infty(\mathbb{N})$.

(iv) Il est facile de voir que $\mathbb{R}$ est équipotent à $]0, 1[$. Or tout réel $x \in]0, 1[$ admet un développement binaire $x = 0, a_1 a_2 \ldots a_i \ldots$ avec $a_i \in \{0, 1\}$ et $x = \displaystyle\sum_{i=1}^{\infty} \frac{a_i}{2^i}$. Ce développement est unique si on exclut les suites stationnaires de 0 (la convention habituelle est d'exclure les suites stationnaires de 1). Grâce aux fonctions caractéristiques, l'ensemble des suites ainsi obtenues correspond à $\mathcal{P}_\infty(\mathbb{N})$. Donc $\text{card}(\mathbb{R}) = \text{card}(\mathcal{P}(\mathbb{N}))$. ∎

7.3.9. Remarque. Aprés avoir démontré que $\aleph_0 < \text{card}\left(\mathcal{P}(\mathbb{N})\right)$, G. Cantor a émis l'idée qu'il n'existait aucun cardinal intermédiaire (*hypothèse du continu*), autrement dit que toute partie infinie de $\mathbb{R}$ est soit dénombrable, soit a la puissance du continu. Malgré tous ses efforts il n'a pu aboutir à une démonstration, et près d'un demi-siècle plus tard, en 1963, P. Cohen a démontré que l'hypothèse du continu était indécidable.

Chapitre II : Groupes et sous-groupes

1 Généralités

1.1. Structure de groupe

1.1.1. Définitions. On appelle *groupe* un couple $(G, *)$ où G est un ensemble et $*$ une loi de composition interne sur G telle que :

- $*$ est associative,
- $*$ admet un élément neutre,
- tout élément de G est inversible.

Si de plus $*$ est commutative, on dit que le groupe est *commutatif* ou *abélien*.

1.1.2. Exemples.

a) Si $G = \{e\}$ et $*$ définie par $e * e = e$, alors $(G, *)$ est un groupe abélien appelé *groupe trivial*.

b) Soit E un ensemble. Alors $(\mathcal{S}(E), \circ)$ est un groupe (Chap. I Exemple 2.3.2), non abélien si $\text{card}\,(E) \geq 3$.

c) $(\mathbb{N}, +)$ n'est pas un groupe, car $n \neq 0$ n'est pas inversible.

d) $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{R}_+^*, \times)$ sont des groupes abéliens.

e) Si $(A, +, \times)$ est un anneau, l'ensemble A_* des éléments inversibles de A pour $\times$, est un groupe multiplicatif. Si E est un espace vectoriel $(\boldsymbol{GL}(E), \circ)$ est un groupe.

f) Soit Π est un plan affine. L'ensemble constitué des homothéties et des translations de Π est un groupe pour $\circ$.

1.1.3. Remarques. Soit $(G, *)$ un groupe.

a) G n'est pas vide (il contient l'élément neutre).

b) L'élément neutre de G est unique. En général on le note e ou e_G. Si la loi est notée multiplicativement ($\times$ ou $\cdot$) on le note souvent 1 ou 1_G, si la loi est notée additivement ($+$) - ce qui suppose que G est abélien car **$+$ ne peut être utilisé que pour une loi commutative**- on le note 0 ou 0_G.

c) L'inverse d'un élément $x \in G$ est unique. En général on le note x^{-1}. Si la loi est notée additivement on le note $-x$ et on l'appelle alors l'*opposé* de x. On a les relations :

$$\forall x \in G \quad (x^{-1})^{-1} = x \quad (\ -(-x) = x \quad \text{dans le cas additif} \quad),$$

$$\forall x, y \in G \quad (x*y)^{-1} = y^{-1}*x^{-1} \quad (\ -(x+y) = -x + (-y) = -x-y \quad \text{cas additif} \quad).$$

d) Tout élément de G est régulier.

1.1.4. Proposition. *Soit $(G_i, *)_{i\in I}$ une famille de groupes. Alors $G = \Pi_{i\in I} G_i$ est un groupe pour la loi $\cdot$ définie par : $(x_i)_{i\in I} \cdot (y_i)_{i\in I} = (x_i * y_i)_{i\in I}$. De plus $(G, \cdot)$ est abélien si et seulement si pour tout $i \in I$, $(G_i, *)$ est abélien.*

Preuve. Vérification immédiate. ∎

1.1.5. Définition. Le groupe G défini par la proposition précédente est appelé *produit direct* des groupes G_i.

1.1.6. Corollaire. *Soient X un ensemble non vide et $(G, *)$ un groupe. Sur G^X on peut définir une structure de groupe en posant : $\forall f, g \in G^X \ f \cdot g : x \longmapsto f(x) * g(x)$. De plus $(G^X, \cdot)$ est abélien si et seulement si G est abélien.*

Preuve. C'est un cas particulier de la proposition précédente, avec $I = X$ et tous les groupes G_i égaux à G. ∎

1.2. Homomorphismes de groupes

1.2.1. Définition. Soient G et G' deux groupes et $f : G \longrightarrow G'$. On dit que f est un *homomorphisme (de groupes)* si :

- $\forall x, y \in G \quad f(x * y) = f(x) * f(y)$,
- $f(e) = e'$,
- $\forall x \in G \quad f(x^{-1}) = (f(x))^{-1}$.

1.2.2. Caractérisation. *Soient G et G' deux groupes et $f : G \longrightarrow G'$. Alors f est un homomorphisme si et seulement si $\forall x, y \in G \quad f(x * y) = f(x) * f(y)$.*

Preuve. La condition nécessaire est triviale. Montrons le caractère suffisant de cette condition. De $e * e = e$, on déduit $f(e) * f(e) = f(e)$; puis par régularité dans G', $f(e) = e'$.
Pour tout $x \in G$ on a $x*x^{-1} = x^{-1}*x = e$, d'où $f(x)*f(x^{-1}) = f(x^{-1})*f(x) = f(e) = e'$.
Il en résulte que $f(x^{-1})$ est l'inverse de $f(x)$. ∎

1.2.3. Notations. Soient G et G' deux groupes. On désigne par $\mathrm{Hom}\,(G, G')$ l'ensemble des homomorphismes de G dans G'. Les homomorphismes de G dans G sont appelés *endomorphismes* de G et leur ensemble est noté $\mathrm{End}\,(G)$.
Soit $f \in \mathrm{Hom}\,(G, G')$.
On appelle *noyau* de f l'ensemble noté $\mathrm{Ker}\,(f) = \{x \in G\ ;\ f(x) = e'\}$, et *image* de f l'ensemble noté $\mathrm{Im}\,(f) = \{x' \in G'\ ;\ \exists x \in G \quad x' = f(x)\}$.

1.2.4. Proposition. *Soient G et G' deux groupes et $f \in \mathrm{Hom}\,(G, G')$. Alors f est injectif si et seulement si* $\mathrm{Ker}\,(f) = \{e\}$.

Preuve. On a toujours $f(e) = e'$, par conséquent $e \in \mathrm{Ker}\,(f)$. Pour tout $x \in \mathrm{Ker}\,(f)$ on a $f(x) = e' = f(e)$; si f est injectif alors $x = e$. Réciproquement si $\mathrm{Ker}\,(f) = \{e\}$, pour tous x et y de G tels que $f(x) = f(y)$ on a :

$$e' = f(x) * f(y)^{-1} = f(x) * f(y^{-1}) = f(x * y^{-1}) \quad \text{d'où} \quad x * y^{-1} \in \mathrm{Ker}\,(f)\ .$$

Il en résulte $x * y^{-1} = e$, c'est à dire $x = y$. ∎

1.2.5. Exemples.

a) Soient G et G' deux groupes. $\mathrm{Hom}\,(G, G')$ n'est pas vide : il existe toujours *l'homomorphisme trivial* : $g \longmapsto e'$; son noyau est G, son image $\{e'\}$.

b) Soit $G \times G'$ le produit direct de deux groupes. La première projection $\pi_G : G \times G' \to G$ définie par $\pi_G(g, g') = g$, appartient à $\mathrm{Hom}\,(G \times G', G)$; elle est surjective et de noyau $\{e\} \times G'$. De même la deuxième projection $\pi_{G'}$ appartient à $\mathrm{Hom}\,(G \times G', G')$. L'application $\iota_G : G \to G \times G'$ définie par $\iota(g) = (g, e')$ appartient à $\mathrm{Hom}\,(G, G \times G')$; elle est injective et son image est $G \times \{e'\}$.

1.2.6. Proposition. *La composée de deux homomorphismes est un homomorphisme.*

Preuve. Vérification immédiate. ∎

1.3. Isomorphismes de groupes

1.3.1. Définition. Soient G et G' deux groupes. Un homomorphisme $f \in \mathrm{Hom}\,(G, G')$ est un *isomorphisme* s'il existe $g \in \mathrm{Hom}\,(G', G)$ tel que $g \circ f = \mathrm{Id}_G$ et $f \circ g = \mathrm{Id}_{G'}$.

1.3.2. Caractérisation. *Un homomorphisme f est un isomorphisme si et seulement s'il est bijectif.*

Preuve. Soit $f \in \mathrm{Hom}\,(G, G')$. La condition nécessaire est évidente. Supposons maintenant que f est bijectif ; alors $g = f^{-1}$ existe, et $g \circ f = \mathrm{Id}_G$ et $f \circ g = \mathrm{Id}_{G'}$. Il reste à prouver que g appartient à $\mathrm{Hom}\,(G', G)$.
$\forall x', y' \in G' \quad f(g(x' * y')) = x' * y' = f(g(x')) * f(g(y')) = f\,(g(x') * g(y'))$.
Par injectivité de f on en déduit : $g(x' * y') = g(x') * g(y')$. ∎

1.3.3. Notations. Soient G et G' deux groupes. On désigne par $\mathrm{Iso}\,(G, G')$ l'ensemble des isomorphismes de G dans G'. Les isomorphismes de G dans G sont appelés *automorphismes* de G et leur ensemble est noté $\mathrm{Aut}\,(G)$.

1.3.4. Exemples.

a) Id_G appartient à $\mathrm{Aut}\,(G)$.

b) Le logarithme népérien est un isomorphisme de $(\mathbb{R}_+^*, \cdot)$ dans $(\mathbb{R}, +)$, son isomorphisme réciproque est la fonction exponentielle.

1.3.5. Théorème de transport de structure. *Soient $(G, .)$ un groupe, E un ensemble et φ une bijection de E sur G. Alors il existe sur E une unique opération interne $*$ telle que $(E, *)$ soit un groupe et que φ devienne un isomorphisme.*

Preuve. Unicité : Supposons que $(E, *)$ est un groupe tel que $\varphi \in \mathrm{Iso}\,(E, G)$. On a alors :

$$\forall x, y \in E \quad \varphi(x*y) = \varphi(x) \cdot \varphi(y) \quad \text{soit encore} \quad \forall x, y \in E \quad x*y = \varphi^{-1}(\varphi(x) \cdot \varphi(y)) \quad (1)\ .$$

La formule (1) prouve l'unicité.
Existence : Définissons sur E une loi $*$ par (1). On vérifie alors aisément que $(E, *)$ est un groupe et que $\varphi \in \mathrm{Iso}\,(E, G)$. ∎

1.4. Automorphismes de groupes

1.4.1. Proposition. *Soit G un groupe. Alors $(\mathrm{Aut}\,(G), \circ)$ est un groupe.*

Preuve. La composée de deux homomorphismes est un homomorphisme et de deux bijections est une bijection ; par conséquent $\circ$ est une opération interne dans $\mathrm{Aut}\,(G)$. La loi de composition est associative et admet Id_G pour élément neutre. Si $\alpha \in \mathrm{Aut}\,(G)$ alors α^{-1} appartient également à $\mathrm{Aut}\,(G)$. ∎

1.4.2. Proposition. *Soient $(G, \cdot)$ un groupe et u un élément de G. L'application Ad_u de G dans G définie par : $\forall x \in G \quad \mathrm{Ad}_u(x) = u \cdot x \cdot u^{-1}$, est un automorphisme de G.*

Preuve. $\forall x, y \in G \quad \mathrm{Ad}_u(x \cdot y) = u \cdot (x \cdot y) \cdot u^{-1} = u \cdot x \cdot u^{-1} \cdot u \cdot y \cdot u^{-1} = \mathrm{Ad}_u(x) \cdot \mathrm{Ad}_u(y)$.
Donc Ad_u est un endomorphisme de G. Il est clair que $\mathrm{Ad}_{u^{-1}}$ est la réciproque de Ad_u. ∎

1.4.3. Définitions. L'automorphisme Ad_u défini dans la proposition précédente est appelé *automorphisme intérieur défini par u*. L'ensemble des automorphismes intérieurs du groupe G est noté $\mathrm{Int}\,(G)$.

1.4.4. Proposition. *Soit $(G, \cdot)$ un groupe. Alors $\mathrm{Ad} : G \longrightarrow \mathrm{Aut}\,(G)$ est un homomorphisme.*

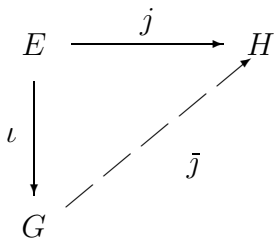
Preuve. Soient u et v dans G, nous devons montrer que : $\mathrm{Ad}_{u \cdot v} = \mathrm{Ad}_u \circ \mathrm{Ad}_v$. Or pour tous $x \in G$ on a
$(\mathrm{Ad}_u \circ \mathrm{Ad}_v)(x) = \mathrm{Ad}_u(v \cdot x \cdot v^{-1}) = u \cdot (v \cdot x \cdot v^{-1}) \cdot u^{-1} = (u \cdot v) \cdot x \cdot (u \cdot v)^{-1} = \mathrm{Ad}_{u \cdot v}(x)$. ∎

1.5. Théorème de symétrisation

1.5.1. Théorème. *Soit $(E,+)$ un ensemble muni d'une loi interne, associative, commutative, admettant un élément neutre et tel que tout élément de E soit régulier pour $+$.*

(i) *Alors il existe un groupe abélien $(G,+)$ et une application injective $\iota : E \longrightarrow G$ tels que :*

- $\forall x, y \in E \quad \iota(x+y) = \iota(x) + \iota(y)$,
- *pour tout groupe $(H,\cdot)$ et tout $j : E \longrightarrow H$ tel que pour tous x et y de E $\quad j(x+y) = j(x)\cdot j(y)$, il existe un unique $\bar{\jmath} \in \mathrm{Hom}\,(G,H)$ tel que $j = \bar{\jmath} \circ \iota$.*



(ii) *Le couple (G,ι) est unique à isomorphisme près. Plus précisément, si K est un groupe abélien et κ une application injective de E dans K tels que les conditions de (i) soient satisfaites, alors il existe un unique $\bar{\iota} \in \mathrm{Iso}\,(K,G)$ tel que $\iota = \bar{\iota} \circ \kappa$.*

Preuve. (i) Sur $E \times E$ on définit une opération $+$ par :
$\forall x, y, s, t \in E \quad (x,y) + (s,t) = (x+s, y+t)$.
On vérifie aisément que cette loi est associative, commutative et admet $(0,0)$ pour élément neutre.
Sur $E \times E$ on définit une relation $\sim$ par : $\forall x, y, s, t \in E \quad (x,y) \sim (s,t) \Leftrightarrow (\, x+t = y+s\,)$.
C'est une relation d'équivalence : la réfléxivité et la symétrie sont évidentes ; pour démontrer la transitivité on utilise la régularité.
Vérifions que $\sim$ est compatible (à droite) avec l'addition :
Soient $x, y, s, t \in E$ tels que $(x,y) \sim (s,t)$ et soit $(u,v) \in E \times E$.
A-t-on $(x,y) + (u,v) \sim (s,t) + (u,v)$? i.e. $(x+u, y+v) \sim (s+u, t+v)$?
Or $(x+u)+(t+v) = (x+t)+u+v = (y+s)+u+v = (y+v)+(s+u)$ par associativité et commutativité de $+$.
Nous pouvons donc définir sur $G = (E \times E)/\sim$ une addition, notée encore $+$, par passage au quotient :

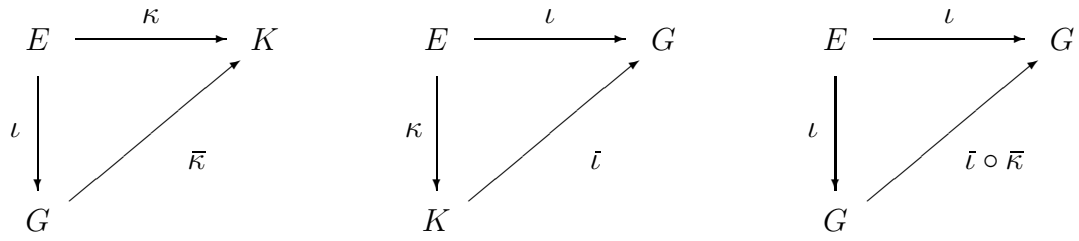
$$\forall x, y, s, t \in E \quad \overline{(x,y)} + \overline{(s,t)} = \overline{(x+s, y+t)}\ .$$

Sur G, la loi $+$ est associative, commutative et admet pour élément neutre $\overline{(0,0)}$ (Chap. I Théorème 3.3.3). Il reste à montrer que tout élément admet un inverse. Or pour $\overline{(x,y)} \in G$ on a $\overline{(x,y)} + \overline{(y,x)} = \overline{(x+y, y+x)} = \overline{(0,0)}$.
Donc G est un groupe abélien.
Soit $\iota : E \longrightarrow G$ défini par $\forall x \in E\ \iota(x) = \overline{(x,0)}$. Il est clair que pour tous x et y de E on a $\iota(x+y) = \iota(x) + \iota(y)$. De plus si $\iota(x) = \iota(y)$ alors $\overline{(x,0)} = \overline{(y,0)}$ i.e. $(x,0) \sim (y,0)$, soit encore $x = x+0 = y+0 = y$. Donc ι est injective.
Soit $j : E \longrightarrow H$ tel que $\forall x, y \in E\ j(x+y) = j(x)\cdot j(y)$. Remarquons tout d'abord que

pour tous x et y dans E, $j(x)$ commute dans H avec $j(y)$ et $j(y)^{-1}$: En effet
$j(x)\cdot j(y) = j(x+y) = j(y+x) = j(y)\cdot j(x)$. En multipliant à gauche et à droite par $j(y)^{-1}$ on obtient
$j(y)^{-1}\cdot j(x)\cdot j(y)\cdot j(y)^{-1} = j(y)^{-1}\cdot j(y)\cdot j(x)\cdot j(y)^{-1}$, d'où $j(y)^{-1}\cdot j(x) = j(x)\cdot j(y)^{-1}$.
Remarquons également que pour tout $\overline{(x,y)} \in G$ on a $\overline{(x,y)} = \overline{(x,0)} + \overline{(0,y)} = \iota(x) - \iota(y)$.
Unicité de $\bar{\jmath}$ tel que $j = \bar{\jmath}\circ\iota$:
$\forall \overline{(x,y)} \in G\ \bar{\jmath}(\overline{(x,y)}) = \bar{\jmath}(\iota(x) - \iota(y)) = \bar{\jmath}(\iota(x))\cdot\bar{\jmath}(\iota(y))^{-1} = j(x)\cdot j(y)^{-1}$.
Existence de $\bar{\jmath}$:
Pour $\overline{(x,y)} \in G$ posons $\bar{\jmath}(\overline{(x,y)}) = j(x)\cdot j(y)^{-1}$. Montrons que $\bar{\jmath}$ est bien défini c'est à dire indépendant du représentant de la classe.
Si $(x,y) \sim (s,t)$ alors $x+t = y+s$, d'où $j(x)\cdot j(t) = j(y)\cdot j(s)$. Multiplions à droite par $j(t)^{-1}\cdot j(y)^{-1}$ on obtient :
$j(x)\cdot j(y)^{-1} = j(y)\cdot j(s)\cdot j(t)^{-1}\cdot j(y)^{-1} = j(s)\cdot j(t)^{-1}\cdot j(y)\cdot j(y)^{-1} = j(s)\cdot j(t)^{-1}$.
Montrons que $\bar{\jmath} \in \mathrm{Hom}\,(G,H)$. Pour tout $\overline{(x,y)}$ et $\overline{(s,t)}$ de G on a :

$$\begin{aligned}\bar{\jmath}(\overline{(x,y)} + \overline{(s,t)}) \;=\; \bar{\jmath}(\overline{x+s, y+s)} \;&=\; j(x+s)\cdot j(y+t)^{-1} \;=\; j(x)\cdot j(s)\cdot(j(y)\cdot j(t))^{-1}\\ &=\; j(x)\cdot j(y)^{-1}\cdot j(s)\cdot j(t)^{-1} \;=\; \bar{\jmath}(\overline{(x,y)})\cdot\bar{\jmath}(\overline{(s,t)})\ .\end{aligned}$$

Il reste à montrer que $j = \bar{\jmath}\circ\iota$.
$\forall x \in E\ \bar{\jmath}\circ\iota(x) = \bar{\jmath}(\overline{(x,0)} = j(x)\cdot j(0)^{-1} = j(x)$ car $j(0)\cdot j(0) = j(0+0) = j(0)$ et par régularité $j(0) = e_H$.
(ii) D'après l'assertion (i) appliquée au couple (G,ι) et à κ, il existe un unique $\bar{\kappa}$ dans $\mathrm{Hom}\,(G,K)$ tel que $\kappa = \bar{\kappa}\circ\iota$. D'après l'assertion (i) appliquée au couple (K,κ) et à ι, il existe un unique $\bar{\iota}$ dans $\mathrm{Hom}\,(K,G)$ tel que $\iota = \bar{\iota}\circ\kappa$. D'où $\iota = \bar{\iota}\circ\bar{\kappa}\circ\iota$.



Mais on a également $\iota = \mathrm{Id}_G\circ\iota$. Par unicité de l'homomorphisme rendant le diagramme commutatif on obtient : $\bar{\iota}\circ\bar{\kappa} = \mathrm{Id}_G$. De même on montre que $\bar{\kappa}\circ\bar{\iota} = \mathrm{Id}_K$ et $\bar{\iota}$ est un isomorphisme. ∎

1.5.2. Définition. On appelle *symétrisé* de E le couple (G,ι) défini dans le théorème précédent.

1.5.3. Cas particulier $E = \mathbb{N}$.

- Par symétrisation de $\mathbb{N}$ on obtient le groupe $(\mathbb{Z},+)$ des *entiers relatifs*.
- On peut construire une multiplication sur $\mathbb{Z}$, par passage au quotient de l'opération sur $\mathbb{N}\times\mathbb{N}$ définie par : $(m,n)\cdot(p,q) = (mp+nq, mq+np)$. *Alors* $(\mathbb{Z},\ +\ ,\ \cdot)$ *est un anneau commutatif avec unité.*

- $\mathbb{Z}$ *est muni d'un ordre total* défini par $m \leq n$ si $\exists p \in \mathbb{N} \;\; n = m + p$.

- Dans $\mathbb{Z}$ il existe une *division euclidienne* : *Soient* $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. *Il existe un unique couple* $(q, r) \in \mathbb{Z} \times \mathbb{N}$ *tel que* $a = bq + r$ *avec* $0 \leq r < b$.
  En effet, si $a = 0$ le couple $(0, 0)$ convient.
  Supposons maintenant $a > 0$, on a $b \geq 1$ et par une récurrence immédiate on montre que pour tout $n \in \mathbb{N}^*$ on a $nb \geq n$ et en particulier $(a + 1)b \geq (a + 1) > a$.
  L'ensemble $A = \{\, n \in \mathbb{N} \,;\; nb > a \,\}$ est donc non vide et ne contient pas 0. Posons $q = \min(A) - 1$ et $r = a - bq$; on a $qb \leq a < (q + 1)b$, d'où $0 \leq r < b$.
  Si $a < 0$, alors il existe (q', r') tels que $-a = bq' + r'$ et $0 \leq r' < b$. Si $r' = 0$ le couple $(-q', 0)$ convient pour a, sinon on vérifie aisément que $(-q' - 1, b - r')$ convient.
  Ceci achève la démonstration de l'existence ; pour l'unicité, soient (q, r) et (q', r') deux couples satisfaisant aux conditions, et supposons $q > q'$. On a alors :
  $a = bq + r = bq' + r'$, d'où $b \leq b(q - q') = r' - r < b$, ce qui est impossible. Par conséquent $q = q'$ et par suite $r = r'$.

2 Sous-groupes

2.1. La notion de sous-groupe

2.1.1. Définition. On dit qu'une partie H d'un groupe $(G \,;\, *)$ est un *sous-groupe* de G si la restriction de $*$ à H le munit d'une structure de groupe i.e. :

- H est stable par $*$ $(\forall x, y \in H \;\; x * y \in H)$,

- $e \in H$,

- $\forall x \in H \quad x^{-1} \in H$.

2.1.2. Caractérisation. *Une partie* H *d'un groupe* $(G, *)$ *est un sous-groupe si et seulement si*

- H *est non vide et*

- $\forall x, y \in H \;\; x * y^{-1} \in H$.

Preuve. La condition nécessaire est immédiate. Montrons la condition suffisante.
Comme H est non vide, il existe $h \in H$ et $h * h^{-1} \in H$; donc $e \in H$.
Pour tout $x \in H$, puisque $e \in H$, on a $e * x^{-1} \in H$; donc $x^{-1} \in H$.
Pour tous x et y dans H, puisque $y^{-1} \in H$, on a $x * (y^{-1})^{-1} \in H$; donc $x * y \in H$. ∎

2.1.3. Exemples .

a) $\{e\}$ et G sont des sous-groupes de G ; les autres sous-groupes de G (s'il en existe) sont appelés *sous-groupes propres* de G.

b) Soient A une partie non vide d'un ensemble E et soit $G = (\mathcal{S}(E), \circ)$. Alors $H = \{ f \in G \,;\ f(A) = A \}$ est un sous-groupe de G.
En effet Id_E appartient à H et pour $f, g \in H$ on a $g(A) = A$ d'où $A = g^{-1}(A)$ et $(f \circ g^{-1})(A) = A$ i.e. $f \circ g^{-1} \in H$.

c) Les translations de direction donnée, les homothéties de même centre constituent des sous-groupes du groupe des homothéties-translations du plan affine Π.

2.1.4. Proposition . *L'application $n \longmapsto n\mathbb{Z}$ est une bijection de $\mathbb{N}$ dans l'ensemble des sous-groupes de $\mathbb{Z}$.*

Preuve. On vérifie aisément que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Réciproquement soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$, sinon il existe $h \neq 0$ dans H. Comme H est stable par passage à l'opposé, $-h$ appartient à H et donc $E = \{ x \in H \,;\ x > 0 \}$ est une partie non vide de $\mathbb{N}$. Soit n le plus petit élément de E (Chap I Théorème 6.3.2). Par récurrence on montre que nk appartient à H, pour tout $k \in \mathbb{N}$, puis par passage à l'opposé que nk appartient à H, pour tout $k \in \mathbb{Z}$. Donc $n\mathbb{Z}$ est inclus dans H. Montrons l'inclusion inverse. Soit $x \in H$. Effectuons la division euclidienne de x par n : $x = nq + r$ avec $0 \leq r < n$. Alors $r = x - nq$ est élément de H. On ne peut avoir $r > 0$ car alors on aurait $r \in E$ et $r < n$ ce qui contredirait le fait que $n = \min(E)$. On a donc $r = 0$ c'est à dire $x \in n\mathbb{Z}$. Il est clair par ailleurs que si m et n sont des entiers naturels distincts alors $n\mathbb{Z} \neq m\mathbb{Z}$. ∎

2.2. Sous-groupes et homomorphismes

2.2.1. Proposition . *L'image directe ou réciproque d'un sous-groupe par un homomorphisme est un sous-groupe.*

Preuve. Soient $f \in \mathrm{Hom}\,(G, G')$, H un sous-groupe de G et H' un sous-groupe de G'. Comme H est non vide, il en est de même pour $f(H)$. Pour tous x' et y' dans $f(H)$ il existe x et y dans H tels que $x' = f(x)$ et $y' = f(y)$; alors $xy^{-1} \in H$ et $x'y'^{-1} = f(x)f(y)^{-1} = f(xy^{-1})$ appartient à $f(H)$. Donc $f(H)$ est un sous-groupe de G'. Comme $f(e) = e' \in H'$, e appartient à $f^{-1}(H')$. Soient x et y dans $f^{-1}(H')$; on alors $f(xy^{-1}) = f(x)f(y)^{-1} \in H'$. Donc $f^{-1}(H')$ est un sous-groupe de G. ∎

2.2.2. Corollaire . *Si $f \in \mathrm{Hom}\,(G, G')$ alors $\mathrm{Ker}\,(f)$ est un sous-groupe de G et $\mathrm{Im}\,(f)$ est un sous-groupe de G'.*

2.2.3. Définition. Soit $(G, \cdot)$ un groupe. On appelle *centre* de G, le sous-ensemble de G, noté $\mathcal{Z}(G)$, constitué des éléments qui commutent à tout $g \in G$:
$\mathcal{Z}(G) = \{\, z \in G \,;\ \forall g \in G\ z \cdot g = g \cdot z \,\}$.

2.2.4. Corollaire. *Soit $(G, \cdot)$ un groupe.*

(i) $\mathrm{Int}\,(G)$ *est un sous-groupe de* $\mathrm{Aut}\,(G)$.

(ii) $\mathcal{Z}(G)$ *est un sous-groupe de* G.

Preuve. (i) $\mathrm{Int}\,(G)$ est l'image de G par l'homomorphisme Ad.
(ii) $\begin{aligned}\mathrm{Ker}\,(\mathrm{Ad}) &= \{\, z \in G \,;\ \mathrm{Ad}_z = \mathrm{Id}_G \,\} = \{\, z \in G \,;\ \forall g \in G\ zgz^{-1} = g \,\} \\ &= \{\, z \in G \,;\ \forall g \in G\ zg = gz \,\} = \mathcal{Z}(G).\end{aligned}$ ∎

2.3. Sous-groupe engendré par une partie

2.3.1. Remarque. L'union de deux sous-groupes n'est pas en général un sous-groupe. En effet $K = 2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$, car 2 et 3 appartiennent à K, mais (2+3) n'appartient pas à K.

2.3.2. Proposition. *Soit $(G, \cdot)$ un groupe.*

(i) *Si $(H_i)_{i \in I}$ est une chaîne, pour l'inclusion, de sous-groupes de G, alors $\bigcup_{i \in I} H_i$ est un sous-groupe de G.*

(ii) *L'intersection d'une famille de sous-groupes est un sous-groupe.*

Preuve. (i) $H = \bigcup_{i \in I} H_i$ est non vide et pour tous x et y de H, il existe i et j dans I tels que $x \in H_i$ et $y \in H_j$. Par hypothèse H_i et H_j sont comparables pour l'inclusion, par exemple $H_i \subset H_j$, d'où $xy^{-1} \in H_j \subset H$.
(ii) vérification facile. ∎

2.3.3. Définition. Soit A une partie d'un groupe G. On appelle *sous-groupe engendré par A* le plus petit sous-groupe de G contenant A, c'est à dire l'intersection de tous les sous-groupes de G contenant A. Nous le noterons $\langle\, A \,\rangle$. Si A est réduit au sigleton $\{a\}$ nous noterons (abusivement) $\langle\, a \,\rangle$.

2.3.4. Proposition. *Soit A une partie non vide d'un groupe $(G, \cdot)$. Le sous-groupe engendré par la partie A est* $\{x \in G\,;\ \exists n \in \mathbb{N}^*\ \exists a_1, \ldots, a_n \in A \cup A^{-1} \quad x = \prod_{i=1}^{n} a_i\}$ *où* $A^{-1} = \{a^{-1}\,;\ a \in A\}$.
Dans le cas additif $\langle A \rangle = \{x \in G\,;\ \exists n \in \mathbb{N}^*\ \exists a_1, \ldots, a_n \in A \cup (-A) \quad x = \sum_{i=1}^{n} a_i\}$.

Preuve. Soit H l'ensemble défini dans l'énoncé. Il est clair que $A \subset H$, donc H est non vide. Soient x et y dans H. On a alors

$$x = \prod_{i=1}^{n} a_i, \quad y = \prod_{j=1}^{m} b_j \quad \text{et} \quad x \cdot y^{-1} = a_1 \cdot \ldots \cdot a_n \cdot b_m^{-1} \cdot \ldots \cdot b_1^{-1}\ .$$

Puisque $a_1\,,\ \ldots\,,\ a_n\,,\ b_1^{-1}\,,\ \ldots\,,\ b_m^{-1}$ appartiennent à $A \cup A^{-1}$, $x \cdot y^{-1}$ appartient à H. Donc H est un sous-groupe contenant A, d'où $\langle A \rangle \subset H$. Montrons maintenant l'inclusion inverse. Soit $x = \prod_{i=1}^{n} a_i$ dans H. Le sous-groupe $\langle A \rangle$ contient A et les inverses des éléments de A, donc contient tous les a_i et par stabilité leur produit ; donc $x \in \langle A \rangle$. ∎

2.3.5. Corollaire. *Soient G et G' des groupes et $f \in \mathrm{Hom}\,(G, G')$. Si G est engendré par une partie A alors* $\mathrm{Im}\,(f)$ *est engendrée par* $f(A)$.

Preuve. Remarquons tout d'abord que $\mathrm{Im}\,(f)$ est un sous-groupe de G' contenant $f(A)$. Donc $\langle f(A) \rangle$ est inclus dans $\mathrm{Im}\,(f)$. Soit maintenant $y \in \mathrm{Im}\,(f)$. Il existe $x \in G$ tel que $y = f(x)$. D'après la proposition précédente, il existe $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n$ dans $A \cup A^{-1}$ tels que $x = \prod_{i=1}^{n} a_i$. Posons $b_i = f(a_i)$ pour $i \in [1, n]_{\mathbb{N}}$. Si a_i appartient à A alors b_i appartient à $f(A)$, si a_i^{-1} appartient à A alors $b_i^{-1} = f(a_i)^{-1} = f(a_i^{-1})$, appartient à $f(A)$. Donc $y = f(x) = f(\prod_{i=1}^{n} a_i) = \prod_{i=1}^{n} b_i$ appartient à $\langle f(A) \rangle$. ∎

2.4. Ordre d'un élément

2.4.1. Lemme. *Soient $(G, \cdot)$ un groupe et $x \in G$. Il existe un unique $\varphi_x \in \mathrm{Hom}\,(\mathbb{Z}, G)$ tel que $\varphi_x(1) = x$. Pour tout $n \in \mathbb{Z}$ on note x^n l'image de n par φ_x ; pour tout $n \in \mathbb{N}^*$ on a $x^n = \underbrace{x \cdot \ldots \cdot x}_{n \text{ fois}}$ et $x^{-n} = \underbrace{x^{-1} \cdot \ldots \cdot x^{-1}}_{n \text{ fois}}$. De plus* $\mathrm{Im}\,(\varphi_x) = \{x^n\,;\ n \in \mathbb{Z}\} = \langle x \rangle$.

Preuve. Posons $\varphi_x(0) = e$ et, par récurrence, pour tout $n \in \mathbb{N}^*$:
$\varphi_x(n) = \varphi_x(n-1) \cdot x = x^n = \underbrace{x \cdot \ldots \cdot x}_{n \text{ fois}}$. On vérifie aisément par récurrence que pour tous m et n dans $\mathbb{N}$ on a $x^{m+n} = x^m \cdot x^n$. D'après le théorème de symétrisation (1.5.1) φ_x se prolonge en un unique homomorphisme, noté encore φ_x, de $\mathbb{Z}$ dans G.
L'unicité de φ_x est immédiate car sa restriction à $\mathbb{N}$ doit vérifier la relation récurrente

$\varphi_x(n+1) = \varphi_x(n) \cdot \varphi_x(1) = \varphi_x(n) \cdot x$ et le prolongement à $\mathbb{Z}$ est unique.
On a $\varphi_x(-1) = (\varphi_x(1))^{-1} = x^{-1}$ et pour tout $n \in \mathbb{N}^*$
$x^{-n} = \varphi_x(-n) = \varphi_x(-(n-1)) \cdot \varphi_x(-1) = \varphi_x(-(n-1)) \cdot x^{-1}$.
Par conséquent les suites $(x^{-n})_{n\in\mathbb{N}}$ et$(\varphi_{x^{-1}}(n))_{n\in\mathbb{N}}$ définies par la même relation de récurrence coïncident.
Il est clair que $\mathrm{Im}\,(\varphi_x)$ est un sous-groupe contenant x, et tout sous-groupe contenant x doit contenir par stabilité tous les x^n pour $n \in \mathbb{N}^*$ ainsi que leurs inverses. Il en résulte que $\mathrm{Im}\,(\varphi_x) = \langle\, x \,\rangle$. ∎

2.4.2. Définitions. Soient $(G, \cdot)$ un groupe, $x \in G$ et φ_x l'homomorphisme défini dans le lemme précédent.
Si φ_x est injectif on dit que x est *d'ordre infini*. Autrement dit x est *d'ordre infini* si $\forall n \in \mathbb{N}^*\ x^n \neq e$.
Si φ_x est non injectif, il existe un unique $d \in \mathbb{N}^*$ tel que $\mathrm{Ker}\,(\varphi_x) = d\mathbb{Z}$ et on dit que x est *d'ordre d*. Autrement dit x est *d'ordre d* si d est le plus petit entier strictement positif tel que $x^d = e$. On note alors $o(x) = d$.
Tout élément m de $\mathrm{Ker}\,(\varphi_x)$ i.e. tel que $x^m = e$ est appelé *période* pour x.

2.4.3. Remarques.

a) Dans le cas d'un groupe abélien dont la loi est notée additivement, $(G, +)$, on note $\varphi_x(n) = n \cdot x$ pour tout $n \in \mathbb{Z}$ et pour tout n positif on a $n \cdot x = \underbrace{x + \cdots + x}_{n \text{ fois}}$.

b) Si $A = \{\, a_1, \ldots, a_k \,\}$ est une partie finie d'un groupe abélien dont la loi est notée additivement, alors le sous-groupe engendré par A est l'ensemble des combinaisons linéaires à coefficients dans $\mathbb{Z}$ des a_i :

$$x \in \langle\, A \,\rangle \Leftrightarrow \exists (n_1, \ldots, n_k) \in \mathbb{Z}^k \quad x = \sum_{i=1}^{k} n_i \cdot a_i \ .$$

c) Soit x un élément d'ordre fini. On a $x^m = e \Leftrightarrow m$ est multiple de $o(x)$.

d) Si x est d'ordre infini, alors $\langle\, x \,\rangle$ est un ensemble infini ; si x est d'ordre d, alors $\langle\, x \,\rangle = \{e, x, \ldots x^{d-1}\}$ est fini de cardinal d.

2.4.4. Exemples.

a) Dans tout groupe, l'élément neutre est d'ordre 1.

b) Dans $\mathbb{Z}$, tout entier non nul est d'ordre infini.

c) Dans $(\mathbb{C}^*, \times)$, 2 est d'ordre infini et i est d'ordre 4.

2.4.5. Proposition. *Soient a un élement d'ordre fini d'un groupe $(G, \cdot)$ et $k \in \mathbb{N}$. L'ordre de a^k est* $\dfrac{o(a)}{\text{PGCD } (o(a), k)}$.

Preuve. Posons $n = o(a)$ et $d = \text{PGCD } (n, k)$. Soient n' et k' tels que $n = dn'$, $k = dk'$. On a $(a^k)^{n'} = a^{kn'} = a^{dk'n'} = (a^n)^{k'} = e$. Donc n' est période pour a^k.
Soit m tel que $(a^k)^m = e$; alors $a^{km} = e$ et n divise km. Il existe $q \in \mathbb{N}$ tel que $km = nq$, d'où $dk'm = dn'q$, soit $k'm = n'q$. Or n' divise $k'm$ et est premier avec m' donc n' divise m. L'ordre de a^k est donc n'. ∎

Chapitre III : Groupes de permutations

1 Actions de groupe

1.1. Groupe opérant sur un ensemble

1.1.1. Définitions. Soient $(G,*)$ un groupe et E un ensemble non vide. On dit que G *agit* ou *opère* sur E, si on se donne un homomorphisme ρ de $(G,*)$ dans $(\mathcal{S}(E),\circ)$.
On dit que l'action de G est *fidèle* si ρ est injectif.

1.1.2. Caractérisation. *Soient $(G,*)$ un groupe et E un ensemble non vide.*

(i) *Si $\rho : g \longmapsto \rho_g$ est une action de G sur E, pour tous $g \in G$ et $x \in E$ posons $g \cdot x = \rho_g(x)$ alors :*

- (1) $\forall x \in E \quad e \cdot x = x$,
- (2) $\forall g_1, g_2 \in G \ \forall x \in E \quad (g_1 * g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

(ii) *Réciproquement la donnée d'une application de $G \times E$ dans E notée $(g,x) \longmapsto g \cdot x$ pour laquelle (1) et (2) sont vérifiées, permet de définir une action ρ de G sur E par $\rho_g(x) = g \cdot x$ pour tous $g \in G$ et $x \in E$.*

Preuve. (i) La relation (1) se déduit de $\rho_e = \mathrm{Id}_E$. Pour tous $g_1, g_2 \in G$ et $x \in E$ on a

$$(g_1 * g_2) \cdot x = \rho_{g_1 * g_2}(x) = (\rho_{g_1} \circ \rho_{g_2})(x) = \rho_{g_1}(g_2 \cdot x) = g_1 \cdot (g_2 \cdot x).$$

(ii) Pour tous $g_1, g_2 \in G$ et $x \in E$ on a compte tenu de (2)

$$\rho_{g_1 * g_2}(x) = (g_1 * g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \rho_{g_1}(g_2 \cdot x) = (\rho_{g_1} \circ \rho_{g_2})(x).$$

D'où $\rho_{g_1 * g_2} = (\rho_{g_1} \circ \rho_{g_2})$. En appliquant cette relation avec g et g^{-1} on obtient grâce à (1) que ρ_g appartient à $\mathcal{S}(E)$. La formule démontrée prouve alors que ρ est un homomorphisme de g dans $\mathcal{S}(E)$. ∎

La notion d'action de groupes intervient dans de nombreuses branches des mathématiques et notamment en géométrie. Donnons ici quelques exemples simples.

1.1.3. Exemples.

a) Soit V un espace vectoriel sur un corps commutatif K. Le groupe $(K^*, \cdot)$ agit sur V par homothéties :
$h : K^* \longrightarrow \mathcal{S}(V)$ $\lambda \longmapsto \lambda \mathrm{Id}_V$ i.e. $\forall \lambda \in K^* \ \forall x \in V \quad h_\lambda(x) = \lambda.x = \lambda x$.
Cette action est fidèle si et seulement si $V \neq \{0\}$.

b) Un groupe $(G, *)$ agit sur lui-même par translations à gauche :
$\lambda : G \longrightarrow \mathcal{S}(G) \quad \forall g \in G \ \forall x \in G \ \lambda_g(x) = g \cdot x = g * x.$
Cette action est fidèle.

c) Un groupe $(G, *)$ agit sur lui-même par translations à droite :
$\rho : G \longrightarrow \mathcal{S}(G) \quad \forall g \in G \ \forall x \in G \ \rho_g(x) = g \cdot x = x * g^{-1}.$
Cette action est fidèle.

d) Un groupe G agit sur lui-même par automorphismes intérieurs ou *conjugaison* :
$\mathrm{Ad}: G \longrightarrow \mathcal{S}(G) \quad \forall g \in G \ \forall x \in G \ \mathrm{Ad}_g(x) = g \cdot x = gxg^{-1}.$
Cette action est fidèle si et seulement si $\mathcal{Z}(G) = \{e\}$.

e) Un groupe G agit sur $\mathcal{G}(G)$, ensemble de ses sous-groupes, par conjugaison :
$\forall g \in G \ \forall H \in \mathcal{G}(G) \quad g \cdot H = \mathrm{Ad}_g(H).$

1.1.4. Lemme. *Soit G un groupe agissant sur un ensemble E.*

(i) *La relation, notée $\underset{G}{\sim}$ (ou $\underset{\rho}{\sim}$ si on désire préciser l'action), définie sur E par $x \underset{G}{\sim} y$ si et seulement s'il existe $g \in G$ tel que $y = g \cdot x$, est une relation d'équivalence.*

(ii) *Pour tout $x \in E$ l'ensemble noté $G_x = \{g \in G \ ; \ g \cdot x = x\}$ est un sous-groupe de G.*

Preuve. (i) Réfléxivité : on a $e \cdot x = x$, donc $x \underset{G}{\sim} x$.
Symétrie : supposons que $x \underset{G}{\sim} y$, il existe $g \in G$ tel que $y = g \cdot x$; on a alors
$g^{-1}.y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$, d'où $y \underset{G}{\sim} x$.
Transitivité : Si on a $x \underset{G}{\sim} y$ et $y \underset{G}{\sim} z$, alors il existe g et h dans G tel que $y = g \cdot x$ et $z = h \cdot y$;
d'où $z = h \cdot (g \cdot x) = (gh) \cdot x$ i.e. $x \underset{G}{\sim} z$.
(ii) La démonstration est immédiate. ∎

1.1.5. Définitions. Soit G un groupe agissant sur un ensemble E.
On dit que deux éléments x et y de E sont *conjugués sous l'action* de G si $x \underset{G}{\sim} y$.
Pour $x \in E$, sa classe d'équivalence, $\{y \in E \ ; \ \exists g \in G \ y = g \cdot x\}$, est notée $\mathcal{O}_x$ et est appelée *orbite* de x (sous l'action de G).
On dit que l'action de G sur E est *transitive* s'il existe une seule orbite.
Pour $x \in E$, on appelle *stabilisateur* de x le sous-groupe G_x.
Dans le cas de l'action de G par automorphismes intérieurs sur lui-même (Exemple d), on l'appelle alors *centralisateur* de x, noté $C_x = \{g \in G \ ; \ gxg^{-1} = x\} = \{g \in G \ ; \ gx = xg\}$; les orbites sont appelées *classes de conjugaison*.
Dans le cas de l'action de G par automorphismes intérieurs sur $\mathcal{G}(G)$ (Exemple e), le stabilisateur de H est appelé *normalisateur* de H, on le note $\mathcal{N}(H)$.

1.2. Classes d'équivalence définies par un sous-groupe

Soit H un sous-groupe d'un groupe G. Toute action de G définit par restriction une action de H. Etudions les actions de H sur G par translations.

Si H agit sur G par translations à gauche :
L'orbite de $x \in G$ pour cette action est $\{\lambda_h(x)\,;\ h \in H\} = \{hx\,;\ h \in H\} = Hx$ appelée *classe à droite modulo* H. La relation d'équivalence associée est : $x \underset{\lambda}{\sim} y \Leftrightarrow y \in Hx$.
L'ensemble quotient, ensemble des classes à droite modulo H, est noté $H\backslash G$.

Si H agit sur G par translation à droite :
L'orbite de $x \in G$ pour cette action est $\{\rho_h(x)\,;\ h \in H\} = \{xh^{-1}\,;\ h \in H\} = xH$ appelée *classe à gauche modulo* H. La relation d'équivalence associée est : $x \underset{\rho}{\sim} y \Leftrightarrow y \in xH$.
L'ensemble quotient, ensemble des classes à gauche modulo H, est noté G/H.

1.2.1. Proposition. *Si H est un sous-groupe de G, alors les ensembles quotients G/H et $H\backslash G$ sont équipotents.*

Preuve. Considérons l'application $f : x \longmapsto x^{-1}H$, de G dans G/H. Comme cette application est surjective, il existe, d'après le théorème de factorisation (Chap I Théorème 3.2.2), une bijection entre G/R_f et G/H. Or, pour tous x et y dans G, on a :

$$\begin{aligned} xR_f y &\Leftrightarrow f(x) = f(y) \\ &\Leftrightarrow x^{-1}H = y^{-1}H \\ &\Leftrightarrow H^{-1}x = H^{-1}y \\ &\Leftrightarrow Hx = Hy \\ &\Leftrightarrow x \underset{\lambda}{\sim} y\ . \end{aligned}$$

Par conséquent $G/R_f = H\backslash G$. Il en résulte que $H\backslash G$ et G/H sont équipotents. ∎

1.2.2. Définitions. Soit H un sous-groupe d'un groupe G. On appelle *indice de H dans G*, noté $[G : H]$ le cardinal commun de $H\backslash G$ et de G/H.
Dans le cas du sous-groupe trivial $\{e\}$ on obtient $[G : \{e\}] = \mathrm{card}\,(G)$. On note plutôt $[G : 1] = \mathrm{card}\,(G)$ et on l'appelle *ordre de G*.

1.2.3. Théorème de Lagrange. *Soient G un groupe, H et K deux sous-groupes de G tels que $K \subset H$. Alors $[G : K] = [G : H][H : K]$.*

Preuve. (Avec l'axiome du choix si G est infini.) Le groupe G s'écrit comme une réunion disjointe de classes à gauche modulo H. Dans chaque classe à gauche choisissons un représentant g_i ; on peut alors écrire : $G = \bigcup_{i \in I} g_i H$ avec $\mathrm{card}\,(I) = [G : H]$. De même on peut écrire : $H = \bigcup_{j \in J} h_j K$ avec $\mathrm{card}\,(J) = [H : K]$. On en déduit $G = \bigcup_{(i,j) \in I \times J} g_i h_j K$.
Si $g_i h_j K = g_{i'} h_{j'} K$ il existe $k \in K$ tel que $g_{i'} h_{j'} = g_i h_j k$, donc $g_{i'} H = g_i H$ et par unicité

de notre choix $i' = i$. Il en résulte $h_j K = h_{j'} K$ et toujours par unicité $j' = j$.
Dans G toutes les classes à gauche $(g_i h_j K)_{(i,j)}$ sont deux à deux distinctes et on déduit $[G : K] = \text{card}\,(G/K) = \text{card}\,(I \times J) = [G : H][H : K]$. ∎

1.2.4. Corollaire. *Soit G un groupe fini.*
(i) L'ordre d'un sous-groupe divise l'ordre du groupe : $\forall H \in \mathcal{G}(G) \quad [H : 1]$ *divise* $[G : 1]$.
(ii) L'ordre de G est période pour chacun de ses éléments : $\forall x \in G \quad x^{[G:1]} = e$.

Preuve. *(i)* Appliquons le théorème de Lagrange avec $K = \{e\}$:
$[G : \{e\}] = [G : H][H : \{e\}]$ i.e. $[G : 1] = [G : H][H : 1]$.
(ii) Soit $x \in G$. Comme G est fini, x est nécessairement d'ordre fini ; soit $d = o(x)$. On sait que $d = [\langle\, x \,\rangle : 1]$ et d'après (i), d divise $[G\ ;\ 1]$; donc $[G : 1]$ est période pour x. ∎

1.3. "Equations aux classes"

1.3.1. Lemme. *Soient G un groupe agissant sur un ensemble E et $x \in E$. L'ensemble quotient G/G_x est équipotent à l'orbite de x sous l'action de G.*

Preuve. Considérons l'application $f : G \longrightarrow E$ telle que $f(g) = g \cdot x$. Son image est l'orbite de x. Déterminons la relation d'équivalence R_f associée à f. On a

$$\begin{aligned} g\, R_f\, g' &\Leftrightarrow f(g) = f(g') \\ &\Leftrightarrow g \cdot x = g' \cdot x \\ &\Leftrightarrow x = (g^{-1} g') \cdot x \\ &\Leftrightarrow g^{-1} g' \in G_x \\ &\Leftrightarrow g' \in g G_x \\ &\Leftrightarrow g \ \text{ et } \ g' \ \text{ sont dans la même classe à gauche modolo } \ G_x\ . \end{aligned}$$

Il en résulte que $G/R_f = G/G_x$, et il suffit d'appliquer le théorème de factorisation à f. ∎

1.3.2. Corollaire. *Soit G un groupe agissant sur un ensemble fini E. Si Φ est une partie de E rencontrant chaque orbite en exactement un point, alors*

$$\text{card}\,(E) = \sum_{x \in \Phi} [G : G_x]\ .$$

Preuve. *(i)* D'après le lemme, pour tout $x \in E$ on a $\text{card}\,(\mathcal{O}_x) = \text{card}\,(G/G_x) = [G\ ;\ G_x]$.
Or $E = \bigcup_{x \in \Phi} \mathcal{O}_x$, d'où $\text{card}\,(E) = \sum_{x \in \Phi} \text{card}\,(\mathcal{O}_x) = \sum_{x \in \Phi} [G : G_x]$. ∎

Ce corollaire et le suivant qui en est un cas particulier, portent le nom "d'équations aux classes".

1.3.3. Corollaire. *Soit G un groupe fini. Il existe une famille finie $(H_i)_{i=1\cdots m}$ de sous-groupes propres de G telle que*

$$[G:1] = [\mathcal{Z}(G):1] + \sum_{i=1}^{m} [G:H_i] \ .$$

Preuve. Dans l'action de G sur lui-même par automorphismes intérieurs, l'orbite de $x \in G$ est $\mathcal{O}_x = \{gxg^{-1} \ ; \ g \in G\}$. On remarque donc que $\mathcal{O}_x = \{x\}$ si et seulement si $x \in \mathcal{Z}(G)$. Si Φ est une partie de G rencontrant chaque orbite en exactement un point, elle doit contenir $\mathcal{Z}(G)$. Appliquons le résultat précédent à cette action, on obtient $\text{card}\,(G) = \sum_{x\in\Phi} [G:C_x]$ en désignant par C_x le centralisateur de x dans G.
L'ensemble $\Phi\backslash\mathcal{Z}(G)$ est fini ; soit m son cardinal. Désignons par H_i pour $i = 1\ldots m$, les centralisateurs des éléments de $\Phi\backslash\mathcal{Z}(G)$, on obtient

$$\begin{aligned} \text{card}\,(G) &= \sum_{x\in\mathcal{Z}(G)} [G:C_x] + \sum_{x\in\Phi\backslash\mathcal{Z}(G)} [G:C_x] \\ [G:1] &= [\mathcal{Z}(G):1] + \sum_{i=1}^{m} [G:H_i] \ . \end{aligned}$$

Pour tout i, le sous-groupe H_i est distinct de G car c'est le centralisateur d'un élément non central, et distinct de $\{e\}$ car sinon $[G:1] \geq [\mathcal{Z}(G):1] + [G:H_i] > [G:1]$. ∎

1.4. p-groupes

1.4.1. Définition. Soit p un nombre premier. On dit qu'un groupe fini G est un *p-groupe* si son ordre est une puissance de p.

1.4.2. Proposition. *Soit p un nombre premier. Le centre d'un p-groupe non trivial est un p-groupe non trivial.*

Preuve. Soit G un p-groupe non trivial. Il existe $\alpha \in \mathbb{N}^*$ tel que $[G:1] = p^\alpha$. Ecrivons l'équation aux classes : $p^\alpha = [\mathcal{Z}(G):1] + \sum_{i=1}^{m} [G:H_i]$, avec $H_i \neq G$. D'après le théorème de Lagrange, $[\mathcal{Z}(G):1]$ et $[G:H_i]$ divisent $[G:1]$ et sont donc des puissances de p. Il en résulte que $\mathcal{Z}(G)$ est un p-groupe et comme $[G:H_i]$ est différent de 1, $[G:H_i]$ est divisible par p pour tout i. On en déduit que p divise $[\mathcal{Z}(G):1]$ et par conséquent $\mathcal{Z}(G)$ n'est pas trivial. ∎

1.4.3. Corollaire. *Soit p un nombre premier. Tout groupe d'ordre p^2 est abélien.*

Preuve. Supposons G non abélien. D'après le corollaire précédent $\mathcal{Z}(G)$ est un p-groupe non trivial ; nécessairement $[\mathcal{Z}(G):1] = p$. Soit $x \in G\backslash\mathcal{Z}(G)$. Le centralisateur C_x de x est un sous-groupe de G contenant strictement $\mathcal{Z}(G)$ puisqu'il contient x. Donc $p < [C_x:1]$ et comme $[C_x:1]$ divise p^2 on a $[C_x:1] = p^2$; d'où $C_x = G$ i.e. $x \in \mathcal{Z}(G)$. Ce qui est contradictoire. ∎

2 Groupes Quotients

Si H est un sous-groupe d'un groupe G, on souhaiterait munir l'ensemble G/H d'une structure de groupe par "passage au quotient". Cela n'est pas toujours possible, il faut que H possède des propriétés particulières.

2.1. Sous-groupes distingués

2.1.1. Proposition. *Soit H est un sous-groupe d'un groupe G. Les conditions suivantes sont équivalentes :*

(*i*) *G/H peut être muni d'une structure de groupe telle que la surjection canonique $p : G \longrightarrow G/H$ soit un homomorphisme,*

(*ii*) *H est stable par* $\mathrm{Int}\,(G)$,

(*iii*) $\forall x \in G \quad xHx^{-1} = H$,

(*iv*) *Pour tout $x \in G$ les classes à droite et à gauche modulo H coïncident.*

Preuve. $(i) \Rightarrow (ii)$ Soient $h \in H$ et $x \in G$. Nous voulons montrer que $\mathrm{Ad}_x(h)$ appartient à H. Remarquons que pour tout $g \in G$ on a $g \in H \Leftrightarrow p(g) = p(e) = H$. En utilisant le fait que p est un homomorphisme on obtient :

$$p(xhx^{-1}) = p(x)p(h)p(x^{-1}) = p(x)p(e)p(x^{-1}) = p(xex^{-1}) = p(e) \ .$$

Donc xhx^{-1} appartient à H.
$(ii) \Rightarrow (iii)$ On a : $\forall x \in G \quad xHx^{-1} \subset H$; appliquons cette relation à x^{-1}, il vient : $x^{-1}Hx \subset H$ d'où $x(x^{-1}Hx)x^{-1} \subset xHx^{-1}$ i.e. $H \subset xHx^{-1}$.
$(iii) \Rightarrow (iv)$ Immédiat.
$(iv) \Rightarrow (i)$ Montrons que la relation $\underset{H}{\sim}$ ($x \underset{H}{\sim} y \Leftrightarrow y \in xH$) est compatible avec l'opération de G. Supposons $x \underset{H}{\sim} y$ et $s \underset{H}{\sim} t$, on veut montrer que $xs \underset{H}{\sim} yt$. Il existe h et k dans H tels que $y = xh$ et $t = sk$; d'où $yt = xhsk$. Or $Hs = sH$ et il existe donc $h' \in H$ tel que $hs = sh'$; par suite $yt = xsh'k$ appartient à xsH i.e. $xs \underset{H}{\sim} yt$. On peut donc définir sur G/H une opération par $(xH)\cdot(yH) = (xyH)$ soit encore $p(x)\cdot p(y) = p(xy)$. L'ensemble G/H est alors muni d'une structure de groupe car les propriétés de l'opération de G passent au quotient (Chap. I Théorème 3.3.3), et p est un homomorphisme par construction.
Rappelons que l'élément neutre de G/H est $p(e) = H$ et que l'inverse est donné par $(xH)^{-1} = p(x)^{-1} = p(x^{-1}) = x^{-1}H$. ∎

2.1.2. Définitions. Si H est un sous-groupe de G tels que les conditions équivalentes de la proposition précédente soient satisfaites, on dit que H est *distingué* ou *normal* dans G ; on note $H \lhd G$.
L'ensemble G/H muni de la loi définie ci-dessus est appelé *groupe quotient* de G par H.

2.1.3. Exemples .

a) G et $\{e\}$ sont distingués dans G.

b) Dans un groupe abélien tous les sous-groupes sont distingués.

c) Pour tout $n \in \mathbb{N}$ on a donc $n\mathbb{Z} \lhd \mathbb{Z}$; la relation d'équivalence définie par $n\mathbb{Z}$ est la *congruence modulo* n donnée par :

$$x \equiv y \pmod{n} \Leftrightarrow y - x \in n\mathbb{Z} .$$

La compatibilité de cette relation avec l'addition se traduit alors :

$$\Big(x \equiv y \pmod{n}\Big) \wedge \Big(x' \equiv y' \pmod{n}\Big) \Rightarrow \Big(x + x' \equiv y + y' \pmod{n}\Big) .$$

En notant $\bar{x}$ la classe de $x \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, la structure de groupe quotient est définie par : $\bar{x} + \bar{y} = \overline{x+y}$.
Remarquons que pour tous m dans $\mathbb{Z}$ on a $\overline{m} = m.\overline{1}$
La congruence est également compatible avec la multiplication de $\mathbb{Z}$:

$$\Big(x \equiv y \pmod{n}\Big) \wedge \Big(x' \equiv y' \pmod{n}\Big) \Rightarrow \Big(xx' \equiv yy' \pmod{n}\Big) .$$

On peut donc définir une multiplication sur $\mathbb{Z}/n\mathbb{Z}$ par : $\bar{x} \times \bar{y} = \overline{xy}$.
Alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.
Remarquons que pour tous m et x dans $\mathbb{Z}$ on a $\overline{mx} = (mx) \cdot \overline{1} = m \cdot (x \cdot \overline{1}) = m \cdot \bar{x}$.

d) Soit ABC un triangle équilatéral de centre O dans un plan affine euclidien orienté. Considérons le groupe G des isométries affines laissant ce triangle invariant :
$G = \{\mathrm{Id}, R, R^{-1}, S_A, S_B, S_C\}$ où R est la rotation de centre O et d'angle $2\pi/3$ et S_M la symétrie orthogonale par rapport à la droite OM. Alors $H = \{\mathrm{Id}, S_A\}$ n'est pas distingué dans G car $S_B \circ S_A \circ S_B^{-1} = S_B \circ S_A \circ S_B = S_C \notin H$.

2.1.4. Remarques .

a) Si $H \lhd G$ alors $[G : H] = \mathrm{card}\,(G/H) = [G/H : 1]$. Le théorème de Lagrange peut alors s'écrire : $[G : 1] = [G/H : 1][H : 1]$.

b) La relation $\lhd$ n'est pas transitive : il existe dans le groupe D_4 des isométries du carré, deux sous-groupes H et K tels que $K \lhd H$, $H \lhd D_4$ et $K \not\lhd D_4$ (cf Exercices).

2.1.5. Proposition . *Soit G un groupe. Tout sous-groupe d'indice 2 de G est distingué dans G.*

Preuve. Soit H un sous-groupe d'indice 2 de G. Les classes à gauche modulo H définissent une partition de G en deux classes : $H = eH$ et une autre classe qui ne peut être que le complémentaire de H dans G. Il en est de même pour les classes à droite. D'après la condition (iv) de la proposition 2.1.1 le sous-groupe H est distingué dans G. ∎

2.1.6. Proposition. *Soient $f \in \mathrm{Hom}\,(G, G')$ et K' un sous-groupe distingué de G'. Alors $f^{-1}(K')$ est un sous-groupe distingué de G.*

Preuve. Soit $k \in f^{-1}(K')$. Pour tout $x \in G$ on a $f(xkx^{-1}) = f(x)f(k)f(x)^{-1}$, or $f(k)$ appartient à K' qui est distingué dans G', donc $f(xkx^{-1})$ appartient à K' et $f^{-1}(K')$ est distingué dans G. ∎

2.1.7. Corollaire. *Soient G et G' deux groupes.*

(*i*) *Si $f \in \mathrm{Hom}\,(G, G')$ alors $\mathrm{Ker}\,(f)$ est distingué dans G.*

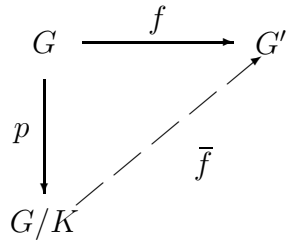
(*ii*) *$\mathcal{Z}(G)$ est distingué dans G.*

Preuve. L'assertion (i) résulte de la proposition précédente car $\{e'\}$ est distingué dans G' et $\mathrm{Ker}\,(f) = f^{-1}(\{e'\})$. Dans le cas particulier de l'homomorphisme Ad on obtient $\mathcal{Z}(G) \lhd G$. ∎

2.2. Théorème de factorisation pour les homomorphismes de groupes

2.2.1. Proposition. *Soient G et G' deux groupes, $f \in \mathrm{Hom}\,(G, G')$ et K un sous-groupe distingué de G tel que $K \subset \mathrm{Ker}\,(f)$.*

Alors il existe un unique $\overline{f} \in \mathrm{Hom}\,(G/K, G')$ tel que $f = \overline{f} \circ p$, où p désigne l'homomorphisme canonique de G sur G/K.



Preuve. Si x et y dans G sont équivalents modulo K, il existe $k \in K$ tel que $y = xk$; comme K est inclus dans le noyau de f, on a donc $f(y) = f(x)f(k) = f(x)e' = f(x)$. D'après la proposition 3.2.1 du chapitre I, il existe une unique application $\overline{f}$ de G/K dans G' telle que $f = \overline{f} \circ p$. Il reste à vérifier que $\overline{f}$ est un homomorphisme.
Soient α et β dans G/K. Puisque p est surjective, il existe x et y dans G tels que $\alpha = p(x)$ et $y = p(y)$. On a alors

$$\overline{f}(\alpha\beta) = \overline{f}(p(x)p(y)) = \overline{f}(p(xy)) = f(xy) = f(x)f(y) = \overline{f}(\alpha)\overline{f}(\beta)\ .$$

∎

2.2.2. Théorème. *Soit f un homomorphisme entre deux groupes G et G'. Désignons par p l'homomorphisme canonique de G sur $G/\mathrm{Ker}\,(f)$ et par i l'injection canonique de $\mathrm{Im}\,(f)$ dans G'.*

Alors il existe un unique isomorphisme $\overline{f}$ de $G/\mathrm{Ker}\,(f)$ dans $\mathrm{Im}\,(f)$ tel que le diagramme suivant soit commutatif.

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ \downarrow{\scriptstyle p} & & \uparrow{\scriptstyle i} \\ G/\mathrm{Ker}\,(f) & \xrightarrow{\ \overline{f}\ } & \mathrm{Im}\,(f) \end{array}$$

Si G est fini alors $[G:1] = [\mathrm{Ker}\,(f):1]\,[\mathrm{Im}\,(f):1]$.

Preuve. Ce théorème résulte immédiatement du théorème de factorisation ensembliste (Chap. I Théorème 3.2.2), de la proposition précédente et du théorème de Lagrange. ∎

2.2.3. Corollaire. *(i) Soient $f \in \mathrm{Hom}\,(G, G')$ et $a \in G$ d'ordre fini. Alors l'ordre de $f(a)$ divise l'ordre de a.*

(ii) Soit $n \in \mathbb{N}^*$. Si dans un groupe G il existe un élément x d'ordre d, diviseur de n, alors il existe un unique $f \in \mathrm{Hom}\,(\mathbb{Z}/n\mathbb{Z}, G)$ tel que $f(\overline{1}) = x$. Pour tout $m \in \mathbb{Z}$ on a alors, $f(\overline{m}) = x^m$.

Preuve. *(i)* Si $n = o(a)$ alors $f(a)^n = f(a^n) = f(e) = e'$. Donc n est période pour $f(a)$ et est un multiple de l'ordre de $f(a)$.
(ii) L'homomorphisme φ_x de $\mathbb{Z}$ dans G (Lemme 2.4.1) admet pour noyau $d\mathbb{Z}$. Puisque d divise n on a $n\mathbb{Z} \subset d\mathbb{Z} = \mathrm{Ker}\,(\varphi_x)$. D'après la proposition précédente, il existe un unique $f \in \mathrm{Hom}\,(\mathbb{Z}/n\mathbb{Z}, G)$ tel que $\varphi_x = f \circ p$. On a en particulier $x = \varphi_x(1) = f(\overline{1})$.
Montrons que f est unique à vérifier cette relation (on sait seulement qu'il est unique à vérifier $\varphi_x = f \circ p$). Si $f(\overline{1}) = x$, alors pour tout $m \in \mathbb{Z}$ on a $f(\overline{m}) = f(m.\overline{1}) = f(\overline{1})^m = x^m$ i.e. $f \circ p = \varphi_x$. ∎

2.3. Théorème d'isomorphisme d'Emmy Nœther

2.3.1. Théorème. *Soient H et K deux sous-groupes d'un groupe $(G, .)$ tels que H soit inclus dans le normalisateur de K. Posons $KH = \{g \in G\,;\ \exists k \in K\ \exists h \in H\ g = kh\}$ et $HK = \{g \in G\,;\ \exists h \in H\ \exists k \in K\ g = hk\}$. Alors*

(i) $H \cap K$ *est distingué dans* H,

(ii) $KH = HK$ *et* HK *est un sous-groupe de* G,

(iii) K *est distingué dans* HK,

(iv) *L'homomorphisme canonique* $f : h \longmapsto hK$ *de* H *dans* HK/K *définit un isomorphisme entre* $H/H \cap K$ *et* HK/K.

Avant de démontrer ce théorème, donnons comme corollaire immédiat, la version commutative.

2.3.2. Corollaire. *Soient H et K deux sous-groupes d'un groupe abélien $(G,+)$. Posons $H+K=\{g\in G\,;\ \exists h\in H\ \exists k\in K\ g=h+k\}$. Alors, $H+K$ est un sous-groupe de G et $H/H\cap K$ est isomorphe à $(H+K)/K$.*

Preuve 1. (i) Soit $x\in H\cap K$. Pour tout $h\in H$, hxh^{-1} appartient à H comme produit d'éléments de H, et à K d'après l'hypothèse $H\subset\mathcal{N}(K)$. Donc hxh^{-1} appartient à $H\cap K$.
(ii) Soit $g\in HK$. Il existe $h\in H$ et $k\in K$ tels que $g=hk$. Or hkh^{-1} est dans K et $g=hk=(hkh^{-1})h$ appartient à KH, d'où $HK\subset KH$. On démontre de même que $KH\subset HK$ et on alors $HK=KH$. Montrons que c'est un sous-groupe. Il est clair que e appartient à HK. Si x et y sont dans HK, il existe $(h,k)\in H\times K$ et $(h',k')\in H\times K$ tels que $x=hk$ et $y=h'k'$; on a alors $xy^{-1}=hkk'^{-1}h'^{-1}=(hkk'^{-1}h^{-1})hh'^{-1}\in KH=HK$.
(iii) Soit $x\in K$. Pour tous $h\in H$ et $k\in K$ l'élément $(hk)x(hk)^{-1}=h(kxk^{-1})h^{-1}$, appartient encore à K car H est inclus dans $\mathcal{N}(K)$.
(iv) On vérifie facilement que l'application $f:h\longmapsto hK$, de H dans HK/K est un homomorphisme, surjectif par définition de HK, et que l'on a :
$\mathrm{Ker}\,(f)=\{h\in H\,;\ hK=eK\}=\{h\in H\,;\ h\in eK\}=H\cap K$.
Il suffit d'appliquer le théorème de factorisation pour conclure. ∎

2.3.3. Remarques.

a) Sous les hypothèses du théorème, HK est le sous-groupe engendré par $H\cup K$.
Dans le cas où $(G,+)$ est abélien on retrouve que $\langle\,\{a_1,\,\ldots,a_k\}\,\rangle=\mathbb{Z}\,a_1+\cdots+\mathbb{Z}\,a_k$.

b) La condition : $H\subset\mathcal{N}(K)$ est en particulier vérifiée lorsque K est distingué dans G puisqu'alors $\mathcal{N}(K)=G$.

c) Dans le cas général HK n'est pas un sous-groupe. Reprenons l'exemple des isométries du triangle équilatéral : soient $H=\{\mathrm{Id},S_A\}$ et $K=\{\mathrm{Id},S_B\}$; alors HK est de cardinal 4 qui ne divise pas 6, ordre de G. Donc HK ne peut être un sous-groupe de G.

3 Groupe symétrique $\mathcal{S}_n$

3.1. Cycles

3.1.1. Proposition. *Si E et F sont deux ensembles équipotents alors leurs groupes de permutations $(\mathcal{S}(E),\circ)$ et $(\mathcal{S}(F),\circ)$ sont isomorphes. En particulier pour tout ensemble fini E de cardinal n, le groupe $\mathcal{S}(E)$ est isomorphe à $(\mathcal{S}(\mathbb{E}_n),\circ)$.*
(On rappelle que $\mathbb{E}_n=[1,n]_{\mathbb{N}}$).

Preuve. Soit φ une bijection de E sur F. Considérons l'application Φ de $\mathcal{S}(E)$ dans $\mathcal{S}(F)$ définie par : $\forall f\in\mathcal{S}(E)\ \Phi(f)=\varphi\circ f\circ\varphi^{-1}$. On a alors pour tous f et g dans $\mathcal{S}(E)$:

$$\Phi(f\circ g)=\varphi\circ(f\circ g)\circ\varphi^{-1}=\varphi\circ f\circ(\varphi^{-1}\circ\varphi)\circ g\circ\varphi^{-1}=\Phi(f)\circ\Phi(g)\ .$$

Φ est donc un homomorphisme. De plus Φ admet pour réciproque $\Psi : g \longmapsto \varphi^{-1} \circ g \circ \varphi$. Donc Φ est un isomorphisme. ∎

3.1.2. Définition. Pour $n \in \mathbb{N}^*$, on appelle *groupe symétrique de degré n* le groupe $(\mathcal{S}(\mathbb{E}_n), \circ)$, on le note $\mathcal{S}_n$.

3.1.3. Définitions et Notations. Soient $n \in \mathbb{N}$ un entier supérieur ou égal à 2 et $\sigma \in \mathcal{S}_n$. La permutation σ peut être représentée par son tableau de valeurs :
$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.
On appelle *support de la permutation* σ, noté $\mathrm{supp}(\sigma)$, l'ensemble des éléments $i \in \mathbb{E}_n$ tels que $\sigma(i) \neq i$.
L'application $\varphi_\sigma : m \longmapsto \sigma^m$, définie au lemme 2.4.1 du chapitre II, est un homomorphisme de $\mathbb{Z}$ dans $\mathcal{S}_n$, et définit donc une action de $\mathbb{Z}$ sur $\mathbb{E}_n$.
On dit que σ est un *cycle* si son support est constitué d'une seule orbite pour cette action.
On appelle *longueur du cycle* σ l'entier k égal au cardinal du support de σ.
Donc $c \in \mathcal{S}_N$ est un cycle de longueur k si et seulement s'il existe k entiers distincts $i_1, \ldots, i_k$ dans $\mathbb{E}_n$ tels que $c(i_j) = i_{j+1}$ pour $j \in \mathbb{E}_{k-1}$, $c(e_k) = i_1$ et $c(i) = i$ pour $i \notin \{i_1, \cdots, i_k\}$.
On note alors $c = (i_1, \cdots, i_k)$.
On appelle *transposition* tout cycle de longueur 2 et on désigne par $\mathcal{T}_n$ l'ensemble des transpositions de $\mathcal{S}_n$.
On convient d'omettre la loi de composition de $\mathcal{S}_n$ et on note $\sigma\tau$ au lieu de $\sigma \circ \tau$.

3.1.4. Remarques.

a) Deux permutations dont les supports sont disjoints commutent.

b) Un cycle de longueur k est d'ordre k dans le groupe $\mathcal{S}_n$.

3.1.5. Proposition. *Soit un entier $n \geq 2$.*

(*i*) *Soient $\tau = (i, j)$ une transposition et σ une permutation de $\mathcal{S}_n$. Alors $\mathrm{Ad}_\sigma(\tau)$ est la transposition $\tau' = (\sigma(i), \sigma(j))$.*

(*ii*) *Deux transpositions de $\mathcal{T}_n$ sont conjuguées pour l'action de $\mathcal{S}_n$ par automorphismes intérieurs.*

(*iii*) *$\mathcal{T}_n$ est une classe de conjugaison du groupe $\mathcal{S}_n$.*

Preuve. (*i*) Soit $k \in \mathbb{E}_n$. Calculons $\sigma\,\tau\,\sigma^{-1}(k)$.
Si $k = \sigma(i)$ alors $\sigma\,\tau\,\sigma^{-1}(k) = \sigma\,\tau\,(i) = \sigma(j) = \tau'(k)$; de même si $k = \sigma(j)$ alors $\sigma\,\tau\,\sigma^{-1}(k) = \tau'(k)$.
Sinon $\sigma^{-1}(k) \notin \{i, j\}$ et $\tau(\sigma^{-1}(k)) = \sigma^{-1}(k)$, d'où $\sigma\,\tau\,\sigma^{-1}(k) = k = \tau'(k)$.
(*ii*) Soient $\tau = (i, j)$ et $\tau' = (i', j')$ deux transpositions. Les complémentaires dans $\mathbb{E}_n$ de

leurs supports sont de même cardinal $n-2$ et il existe donc une bijection σ' de $\mathbb{E}_n \setminus \{i,j\}$ sur $\mathbb{E}_n \setminus \{i',j'\}$. L'application σ définie par $\sigma(i)=i'$, $\sigma(j)=j'$ et $\sigma(k)=\sigma'(k)$ si $k \notin \{i,j\}$ est une permutation de $\mathbb{E}_n$. D'après (i) on a : $\sigma\,\tau\,\sigma^{-1} = (\,\sigma(i),\sigma(j)\,) = \tau'$.
L'assertion (iii) résulte immédiatement de (i) et (ii). ∎

3.1.6. Proposition. *Soit $c=(i_1,\,\ldots,i_k)$ un cycle de longueur k. Alors $c=\prod_{j=1}^{k-1}(i_j,i_{j+1})$.*

Preuve. Montrons par récurrence sur k ($k\geq 2$) que si $i_1,\,\ldots,\,i_k$ sont k entiers deux à deux distincts on a $(i_1,\,\ldots,i_k)=\prod_{j=1}^{k-1}(i_j,i_{j+1})$. Si $k=2$ l'égalité est évidente. Supposons le résultat vrai jusqu'au rang k. On a alors

$$\prod_{j=1}^{k}(i_j,i_{j+1}) = \left(\prod_{j=1}^{k-1}(i_j,i_{j+1})\right)(i_k,i_{k+1}) = (i_1,\,\ldots,i_k)(i_k,i_{k+1}) = (i_1,\,\ldots,i_{k+1})\,. \qquad ∎$$

3.2. Générateurs du groupe $\mathcal{S}_n$

3.2.1. Proposition. *Toute permutation de $\mathcal{S}_n$ se décompose de manière unique (à l'ordre près) comme un produit de cycles à supports disjoints : $\sigma=\prod_{j=1}^{p} c_j$.*

L'ordre de σ est alors le ppcm des ordres des c_j.

Preuve. Existence de la décomposition : Si $\sigma=\mathrm{Id}_{\mathbb{E}_n}$ on convient que σ est le produit de 0 cycle. Supposons maintenant que $\sigma\neq\mathrm{Id}_{\mathbb{E}_n}$ et soient $\mathcal{O}_1,\,\ldots,\mathcal{O}_p$ les orbites non réduites à un point, pour l'action de $\mathbb{Z}$ sur $\mathbb{E}_n$ définie précédemment ; ces orbites forment une partition du support de σ. Soient $j\in\mathbb{E}_p$ et $i_j\in\mathcal{O}_j$. Par restriction $\mathbb{Z}$ agit sur $\mathcal{O}_j$ et cette action est transitive. Le stabilisateur de i_j est un sous-groupe de $\mathbb{Z}$, donc de la forme $k_j\mathbb{Z}$, et $\mathcal{O}_j$ est en bijection avec $\mathbb{Z}/k_j\mathbb{Z}$ (Lemme 1.3.1). Par suite $k_j=\mathrm{card}\,(\mathcal{O}_j)$, $\mathcal{O}_j=\{\,i_j,\sigma(i_j),\cdots,\sigma^{k_j-1}(i_j)\,\}$ et $\sigma^{k_j}(i_j)=i_j$. Considérons le cycle $c_j=(i_j,\sigma(i_j),\cdots,\sigma^{k_j-1}(i_j))$. Son support est $\mathcal{O}_j$.
Montrons que $\sigma=\prod_{j=1}^{p} c_j$. Soit $i\in\mathbb{E}_n$. Si $i\notin\mathrm{supp}(\sigma)$ alors pour tout $j\in\mathbb{E}_p$ on a $i\notin\mathcal{O}_j$ et $c_j(i)=i$. Donc $c_1c_2\cdots c_p(i)=i=\sigma(i)$. Si $i\in\mathrm{supp}(\sigma)$ alors il existe un unique $\ell\in\mathbb{E}_p$ tel que $i\in\mathcal{O}_\ell$. On a alors puisque les cycles c_j sont à supports disjoints et donc commutent, $c_1c_2\cdots c_p(i)=c_\ell c_1\cdots c_{\ell-1}c_{\ell+1}\cdots c_p(i)=c_\ell(i)=\sigma(i)$ d'après la définition de c_ℓ.

Unicité de la décomposition : Remarquons tout d'abord que si $\sigma=c_1c_2\cdots c_p$, où les c_j sont des cycles à supports disjoints alors $\mathrm{supp}(\sigma)=\bigcup\mathrm{supp}(c_j)$. De plus pour tout $i\in\mathrm{supp}(c_1)$, en utilisant la commutation des c_j on obtient, pour tout $m\in\mathbb{Z}$:
$\sigma^m(i)=(c_1c_2\cdots c_p)^m(i)=(c_1^mc_2^m\cdots c_p^m)(i)=c_1^m(i)$.
Montrons, par récurrence sur p, que si une permutation σ se décompose en produit de cycles à supports disjoints alors cette décomposition est unique.

Si $p = 0$ alors $\sigma = \mathrm{Id}_{\mathbb{E}_n}$ et l'unicité est évidente.
Supposons la propriété vraie au rang $p-1$. Soient $c_1 \cdots c_p = c'_1 \cdots c'_q$ deux décompositions de σ en produit de cycles à supports disjoints. Considérons $i \in \mathrm{supp}(c_1)$. Il existe un unique $\ell \in \mathbb{E}_q$ tel que $i \in \mathrm{supp}(c'_\ell)$. Puisque les c'_j commutent, nous pouvons supposer que $i \in \mathrm{supp}(c'_1)$. On a alors, pour tout $m \in \mathbb{Z}$, $c_1^m(i) = \sigma^m(i) = {c'_1}^m(i)$. Il en résulte que $\mathrm{supp}(c'_1) = \mathrm{supp}(c_1)$, puis que $c'_1 = c_1$. Nous pouvons simplifier par c_1 l'égalité initiale et on obtient $c_2 \cdots c_p = c'_2 \cdots c'_q$. L'hypothèse de récurrence nous permet d'obtenir l'unicité.

Pour tout $m \in \mathbb{Z}$ on a $\sigma^m = c_1^m c_2^m \cdots c_p^m$. Les supports des cycles c_j étant disjoints on a donc $\sigma^m = \mathrm{Id}_{\mathbb{E}_n}$ si et seulement si pour tout $j \in \mathbb{E}_p \quad c_j^m = \mathrm{Id}_{\mathbb{E}_n}$. Donc m est période pour σ si et seulement si m est un mutiple commun des ordres des c_j. Il en résulte que l'ordre de σ est le ppcm des ordres des c_j. ∎

3.2.2. Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 1 & 4 \end{pmatrix}$.

On a $\sigma(1) = 3$, $\sigma^2(1) = 5$, $\sigma^3(1) = 1$. Donc $c_1 = (1, 3, 5)$.
$\sigma(2) = 2$. Donc 2 n'appartient pas au support de σ.
$\sigma(4) = 6$, $\sigma^2(4) = 4$. Donc $c_2 = (4, 6)$.
Par conséquent $\sigma = (1, 3, 5)\,(4, 6)$.

3.2.3. Corollaire. *Toute permutation de $\mathcal{S}_n$ se décompose en un produit de transpositions. Autrement dit : $S_n = \langle\, \mathcal{T}_n \,\rangle$.*

Preuve. Le corollaire résulte immédiatement de la proposition précédente et de la proposition 3.1.6. ∎

3.3. Signature d'une permutation

3.3.1. Définitions. Soit $\sigma \in \mathcal{S}_n$.
Soient i et j dans $\mathbb{E}_n$. On dit que σ *présente une inversion en* (i, j) si on a $i < j$ et $\sigma(i) > \sigma(j)$. Notons I_σ le nombre d'inversions présentées par σ. On appelle *signature* de σ, notée $\varepsilon(\sigma)$, l'entier $(-1)^{I_\sigma}$.
On dit que σ est une permutation *paire* (resp. *impaire*) si sa signature est 1 (resp. -1).

3.3.2. Lemme. *Pour tout $\sigma \in \mathcal{S}_n$ on a* $\varepsilon(\sigma) = \displaystyle\prod_{\{i,j\} \in \mathcal{P}_2} \frac{\sigma(i) - \sigma(j)}{i - j}$, *où $\mathcal{P}_2$ désigne l'ensemble des parties à 2 éléments de $\mathbb{E}_n$.*

Preuve. Puisque σ est une permutation de $\mathbb{E}_n$, l'application $\{i, j\} \longmapsto \{\sigma(i), \sigma(j)\}$ est une permutation de $\mathcal{P}_2$. Il en résulte que

$$\left| \prod_{\{i,j\} \in \mathcal{P}_2} \frac{\sigma(i) - \sigma(j)}{i - j} \right| = \frac{\displaystyle\prod_{\{i,j\} \in \mathcal{P}_2} |\sigma(i) - \sigma(j)|}{\displaystyle\prod_{\{i,j\} \in \mathcal{P}_2} |i - j|} = 1 \,.$$

Or le nombre d'inversions I_σ est égal au nombre de facteurs tels que $\dfrac{\sigma(i)-\sigma(j)}{i-j} < 0$. Par conséquent $\varepsilon(\sigma)$ et $\displaystyle\prod_{\{i,j\}\in\mathcal{P}_2} \frac{\sigma(i)-\sigma(j)}{i-j}$ sont de même signe. D'où le résultat. ∎

3.3.3. Théorème. *Soit un entier $n \geq 2$. L'application ε est l'unique homomorphisme surjectif de $\mathcal{S}_n$ dans le groupe $\{-1,1\}$. La signature de toute transposition est égale à -1 et si une permutation σ s'écrit comme produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$.*

Preuve. Soient ρ et σ dans $\mathcal{S}_n$. On a :

$$\begin{aligned}
\varepsilon(\rho\circ\sigma) &= \prod_{\{i,j\}\in\mathcal{P}_2} \frac{\rho\circ\sigma(i)-\rho\circ\sigma(j)}{i-j} \\
&= \prod_{\{i,j\}\in\mathcal{P}_2} \frac{\rho\circ\sigma(i)-\rho\circ\sigma(j)}{\sigma(i)-\sigma(j)} \cdot \prod_{\{i,j\}\in\mathcal{P}_2} \frac{\sigma(i)-\sigma(j)}{i-j} \\
&= \prod_{\{i',j'\}\in\mathcal{P}_2} \frac{\rho(i')-\rho(j')}{i'-j'} \cdot \prod_{\{i,j\}\in\mathcal{P}_2} \frac{\sigma(i)-\sigma(j)}{i-j} \\
&= \varepsilon(\rho)\cdot\varepsilon(\sigma)\ .
\end{aligned}$$

Donc ε est un homomorphisme. Il est clair que pour la transposition $\tau_0 = (1,2)$, le nombre d'inversions est égal à 1 et la signature -1. Donc ε est surjectif.
Soit ε' un homomorphisme surjectif de $\mathcal{S}_n$ dans $\{-1,1\}$. Toute transposition τ est conjuguée avec τ_0 (Proposition 3.1.5) et il existe $\rho \in \mathcal{S}_n$ telle que $\tau = \mathrm{Ad}_\rho(\tau_0)$. On a alors $\varepsilon'(\tau) = \varepsilon'(\rho)\varepsilon'(\tau_0)\varepsilon'(\rho)^{-1} = \varepsilon'(\tau_0)$, car le groupe $\{-1,1\}$ est abélien. Si $\varepsilon'(\tau_0) = 1$ alors $\varepsilon'(\tau) = 1$ pour tout $\tau \in \mathcal{T}_n$; toute permutation σ se décomposant comme un produit de transpositions, on obtient alors $\varepsilon'(\sigma) = 1$, ce qui contredit le fait que ε' est surjectif. Donc pour tout $\tau \in \mathcal{T}_n$, on a $\varepsilon'(\tau) = -1$.
Ce résultat peut s'appliquer à ε, donc pour tout $\tau \in \mathcal{T}_n$, on a $\varepsilon(\tau) = -1$.
Soient $\sigma \in \mathcal{S}_n$ et $\sigma = \tau_1 \ldots \tau_p$ une décomposition de σ en produit de transpositions. On a alors $\varepsilon(\sigma) = \varepsilon(\tau_1)\ldots\varepsilon(\tau_p) = (-1)^p = \varepsilon'(\tau_1)\ldots\varepsilon'(\tau_p) = \varepsilon'(\sigma)$. Ce qui prouve l'unicité. ∎

3.3.4. Corollaire. *La signature d'un cycle de longueur k est $(-1)^{k-1}$.*

Preuve. On a vu dans la proposition 3.1.6 qu'un cycle de longueur k peut se décomposer en produit de $k-1$ transpositions. Il suffit alors d'appliquer le théorème précédent. ∎

3.3.5. Définition. On appelle *groupe alterné de degré n*, noté $\mathcal{A}_n$, le noyau de l'homomorphisme signature. $\mathcal{A}_n = \{\,\sigma \in \mathcal{S}_n\ ;\ \varepsilon(\sigma) = 1\,\}$.

3.3.6. Proposition. *Le sous-groupe $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ et est d'indice 2.*

Preuve. Puisque $\mathcal{A}_n = \mathrm{Ker}\,(\varepsilon)$, le sous-groupe $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$.
Appliquons le théorème de factorisation (Théorème 2.2.2) à l'homomorphisme surjectif ε, nous obtenons $\mathcal{S}_n/\mathcal{A}_n \simeq \{-1,1\}$ et donc $[\mathcal{S}_n : \mathcal{A}_n] = 2$. ∎

Chapitre IV : Théorèmes de structures

1 Groupes cycliques

1.1. Structure des groupes cycliques

1.1.1. Définitions. Un groupe G est dit *monogène* s'il peut être engendré par un seul élément. On dit que G est *cyclique* s'il est monogène et fini.

1.1.2. Proposition.

(i) *Tout groupe monogène infini est isomorphe à* $(\mathbb{Z}, +)$.

(ii) *Tout groupe cyclique d'ordre* n *est isomorphe à* $(\mathbb{Z}/n\mathbb{Z}, +)$.

Preuve. Soient G un groupe monogène et a un générateur de G. Soit $\varphi_a \in \mathrm{Hom}\,(\mathbb{Z}, G)$ tel que pour tout $m \in \mathbb{Z}$ on ait $\varphi_a(m) = a^m$. Grâce au théorème de factorisation, $\mathbb{Z}/\mathrm{Ker}\,(\varphi_a)$ est isomorphe à l'image de φ_a qui est G. Si a est d'ordre infini alors G est isomorphe à $\mathbb{Z}$, si a est d'ordre n alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. ∎

1.1.3. Exemple. Soit $n \in \mathbb{N}^*$. Le groupe $\mathbb{U}_n$ des racines $n^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$ est un groupe cyclique engendré par exemple par $e^{2i\pi/n}$.

1.1.4. Notations. L'unique (à isomorphisme près) groupe cyclique d'ordre n est noté C_n.

1.1.5. Proposition. *Tout groupe d'ordre premier* p *est cyclique et donc isomorphe à* C_p.

Preuve. Soit G un groupe d'ordre premier p. Comme 1 n'est pas premier, il existe $a \neq e$ dans G. Soit $H = \langle\, a \,\rangle$. Alors $[H : 1]$ divise p (Th. de Lagrange) et est différent de 1. Donc $[H : 1] = p$ et G est cyclique, engendré par a. ∎

1.1.6. Théorème. *Tout sous-groupe d'un groupe cyclique est cyclique. Plus précisément, soit* a *un générateur d'un groupe cyclique* G *d'ordre* n. *Pour tout diviseur* d *de* n *il existe un unique sous-groupe* H *d'ordre* d.
On a $H = \{\, x \in G\,;\ \ x^d = e \,\} = \{\, x \in G\,;\ \exists y \in G \quad x = y^q \,\} = \langle\, a^q \,\rangle$, *où* $q = n/d$.

Preuve. Posons $H = \langle\, a^q \,\rangle$, $H_1 = \{x \in G\,;\ \ x^d = e\}$ et $H_2 = \{\, x \in G\,;\ \exists y \in G \quad x = y^q \,\}$. On vérifie aisément que H_1 est un sous-groupe de G et que a^q appartient à H_1. Donc $H \subset H_1$.
Pour tout $x \in H_1$, il existe $m \in \mathbb{Z}$ tel que $x = a^m$ et $(a^m)^d = e$. Donc md est période pour

a et par suite n divise md, i.e. il existe $k \in \mathbb{N}$ tel que $md = kn = kdq$. D'où $m = kq$ et $x = a^{kq} = (a^k)^q$. Donc $H_1 \subset H_2$.
Pour tout $x \in H_2$, il existe $y \in G$ tel que $x = y^q$. Comme a est générateur de G il existe $m \in \mathbb{Z}$ tel que $y = a^m$ et $x = (a^m)^q = a^{mq} = (a^q)^m$. Donc $H_2 \subset H$.
De plus $[H : 1] = o(a^q) = d$. Si K est un sous-groupe d'ordre d de G, alors pour tout $x \in K$ on a $x^d = e$; donc K est inclus dans H. Comme H et K ont même ordre, on a $H = K$. ∎

1.1.7. Exemple : les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$. Pour obtenir les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, il faut traduire en notation additive les résultats du théorème précédent : *si $n = dq$ il existe dans $\mathbb{Z}/n\mathbb{Z}$ un unique sous-groupe d'ordre d, il est engendré par $\overline{q}$.*
Les diviseurs de 12 sont : 1, 2, 3, 4, 6 et 12. On obtient donc comme sous-groupes : $H_1 = \{\overline{12}\} = \{\overline{0}\}$, $H_2 = \{\overline{0}, \overline{6}\}$, $H_3 = \{\overline{0}, \overline{4}, \overline{8}\}$, $H_4 = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$, $H_6 = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$ et $\mathbb{Z}/12\mathbb{Z}$.

1.2. Théorème chinois

1.2.1. Théorème. *Le produit direct de deux groupes cycliques est cyclique si et seulement si leurs ordres sont premiers entre eux. Dans ce cas (a, b) est générateur de $C_m \times C_n$ si et seulement si a engendre C_m et b engendre C_n.*

Preuve. Soit $G = C_n \times C_m$. Alors $[G : 1] = mn$.
Supposons que m et n sont premiers entre eux. Soient a un générateur de C_m et b un générateur de C_n. On a pour tout $k \in \mathbb{Z}$:

$$\begin{aligned}(a,b)^k = (e,e) &\Leftrightarrow (a^k, b^k) = (e,e)\\ &\Leftrightarrow (a^k = e) \wedge (b^k = e)\\ &\Leftrightarrow (m/k) \wedge (n/k)\\ &\Leftrightarrow mn/k \quad (\text{car PGCD } (m,n) = 1).\end{aligned}$$

Donc (a, b) est d'ordre mn et est générateur de G.
Réciproquement supposons G cyclique. Soient (x, y) un générateur de G. Il est clair que x engendre C_m et que y engendre C_n. Si d est un diviseur commun de m et n, posons $m = dm'$ et $n = dn'$. Alors $(x, y)^{m'n'd} = (x^{nm'}, y^{mn'}) = (e, e)$. Donc $m'n'd$ est multiple de mn ; nécessairement $d = 1$ et m et n sont premiers entre eux. ∎

1.2.2. Corollaire. *Le groupe $C_{n_1} \times \cdots \times C_{n_k}$ est cyclique si et seulement si les entiers n_i sont deux à deux premiers entre eux.*

Preuve. La démonstration se fait par récurrence sur k. Pour $k = 2$, c'est le théorème précédent. Supposons la propriété vraie jusqu'au rang $k-1$; posons $G = C_{n_1} \times \cdots \times C_{n_k}$, $H = C_{n_1} \times \cdots \times C_{n_{k-1}}$ et $n = n_1 \times \cdots \times n_{k-1}$.

Supposons G cyclique. Le sous-groupe $H \times \{e\}$ de G est cyclique et donc H est cyclique. D'après l'hypothèse de récurrence les entiers n_i pour $i = 1 \dots k-1$ sont 2 à 2 premiers entre eux. Par ailleurs d'après le théorème précédent n et n_k sont premiers entre eux, ce qui implique que n_k est premier avec tous les n_i pour $i = 1 \dots k-1$.
Réciproquement, si les entiers n_i sont deux à deux premiers entre eux, alors, d'après l'hypothèse de récurrence H est cyclique d'ordre n. Comme n est premier avec n_k, le théorème précédent assure que G est cyclique. ∎

1.2.3. Corollaire : Théorème chinois. *Soient $(n_i)_{i=1\dots k}$ des entiers deux à deux premiers entre eux et $n = n_1 \times \cdots \times n_k$. Pour toute famille $(a_i)_{i=1\dots k}$ d'entiers, il existe un entier x unique modulo n tel que pour tout $i = 1 \dots k$,* $\quad x \equiv a_i \pmod{n_i}$.

Preuve. Désignons par $\overline{a}^i$ la classe de l'entier a dans $\mathbb{Z}/n_i\mathbb{Z}$; alors $(\overline{a_1}^1, \dots, \overline{a_k}^k)$ appartient à $(\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z})$ qui est cyclique engendré par $(\overline{1}^1, \dots, \overline{1}^k)$. Il existe donc un unique $x \in [0, n-1]_{\mathbb{N}}$ tel que $(\overline{a_1}^1, \dots, \overline{a_k}^k) = x \cdot (\overline{1}^1, \dots, \overline{1}^k) = (\overline{x}^1, \dots, \overline{x}^k)$. ∎

1.2.4. Méthode pratique. Reprenons les données du théorème précédent. Pour déterminer x on procède par itération on résout d'abord le système : $x \equiv a_i \pmod{n_i}$ pour $i = 1, 2$.
D'après le théorème de Bézout, il existe (u_1, u_2) tels que $u_1 n_1 + u_2 n_2 = 1$; la détermination pratique d'un tel couple s'obtient à partir de l'algorithme d'Euclide de calcul du pgcd.
Soit $x_1 = a_1 u_2 n_2 + a_2 u_1 n_1$. On a alors $x_1 = a_1(1 - u_1 n_1) + a_2 u_1 n_1$, d'où $x_1 \equiv a_1 \pmod{n_1}$.
De même on obtient $x_1 \equiv a_2 \pmod{n_2}$. On est ramené à résoudre le système obtenu en remplaçant les deux premières équations par : $x \equiv x_1 \pmod{n_1 n_2}$.

Soit à résoudre le système $\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{12} \\ x \equiv 1 \pmod{5} \end{cases}$

On obtient facilement : $3 \times 12 - 5 \times 7 = 1$. D'où $x_1 = 3 \times (3 \times 12) + 4 \times (-5 \times 7) = -32$.
On remplace les deux premières équations par : $x \equiv 52 \pmod{84}$.
On trouve alors $17 \times 5 - 1 \times 84 = 1$ et $x = 52 \times (17 \times 5) + 1 \times (-1 \times 84) = 4336$. En choisissant l'entier dans $[0, 419]_{\mathbb{N}}$ on obtient donc $x = 136$ unique modulo 420.

1.3. Indicateur d'Euler

1.3.1. Proposition. *Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$.*

(*i*) *Soient a un générateur du groupe cyclique C_n. Alors a^k est générateur de C_n si et seulement si n et k sont premiers entre eux.*

(*ii*) *Désignons par A l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, par A^* l'ensemble de ses éléments inversibles et par $\overline{k}$ la classe de k dans $\mathbb{Z}/n\mathbb{Z}$. Alors*

$$A^* = (\mathbb{Z}/n\mathbb{Z}, +, \times)^* = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \,;\, \overline{k} \text{ générateur}\} \simeq \{k \in [1, n]_{\mathbb{N}} \,;\, k \text{ premier avec } n\} \,.$$

Preuve. L'assertion (i) résulte de la proposition 2.4.5.
(ii) On a les équivalences :

$$\begin{aligned} \overline{k} \in A^* &\Leftrightarrow \exists \overline{m} \in A \quad \overline{m} \times \overline{k} = \overline{1} \\ &\Leftrightarrow \exists m \in \mathbb{Z} \quad m \cdot \overline{k} = \overline{1} \\ &\Leftrightarrow \overline{1} \in \langle\, \overline{k} \,\rangle \\ &\Leftrightarrow \overline{k} \quad \text{est générateur de} \quad (\mathbb{Z}/n\mathbb{Z}, +)\ . \end{aligned}$$

D'après l'assertion (i), la classe $\overline{k}$ est génératrice de $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si k est premier avec n. ∎

1.3.2. Définition. Soit $n \in \mathbb{N}^*$. On appelle *indicateur d'Euler*, noté $\varphi(n)$, le cardinal de $\{k \in [1, n]_{\mathbb{N}}\ ;\ k \text{ premier avec } n\}$. C'est le nombre de générateurs dans C_n et l'ordre du groupe multiplicatif $((\mathbb{Z}/n\mathbb{Z})^*, \times)$.

1.3.3. Exemples.

a) Les complexes i et $-i$ sont générateurs dans $\mathbb{U}_4$ et $\varphi(4) = 2$.

b) Les générateurs dans $\mathbb{Z}/12\mathbb{Z}$ sont $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$ et $\varphi(12) = 4$.

1.3.4. Propriétés.

(i) *Si m et n sont deux entiers premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

(ii) *Si p est un entier premier alors $\varphi(p) = p - 1$, plus généralement pour tout $r \in \mathbb{N}^*$ on a $\varphi(p^r) = p^r - p^{r-1}$.*

(iii) *Si $n = \prod_{i=1}^{k} p_i^{r_i}$ est la décomposition de n en facteurs premiers alors*

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{r_i} - p_i^{r_i - 1})\ .$$

Preuve. L'assertion (i) résulte du théorème 1.2.1. La proposition 1.1.5 entraîne que $\varphi(p) = p - 1$ si p est premier. Les entiers de $[1, p^r]$ non premiers avec p^r sont les multiples de p i.e. $p, 2p, \ldots, p^{r-1}p$; ils sont au nombre de p^{r-1} ; d'où l'assertion (ii). Une récurrence immédiate et le résultat des deux premières assertions nous donne (iii). ∎

1.3.5. Théorème d'Euler. *Soit $n \in \mathbb{N}^*$. Pour tout $k \in \mathbb{Z}$ premier avec n on a :*

$$k^{\varphi(n)} \equiv 1 \pmod{n}\ .$$

Preuve. Si k est premier avec n, alors $\overline{k}$ appartient au groupe multiplicatif $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ qui est d'ordre $\varphi(n)$. D'après une conséquence du théorème de Lagrange on a $\overline{k}^{\varphi(n)} = \overline{1}$. ∎

1.3.6. Théorème de Fermat. *Soit p un entier premier. Pour tout $k \in \mathbb{Z}$ non divisible par p on a :*

$$k^{p-1} \equiv 1 \pmod{p} .$$

Preuve. Le théorème de Fermat est conséquence immédiate de celui d'Euler, car p étant premier on a $\varphi(p) = p - 1$. ∎

1.3.7. Proposition. *Soit $n \in \mathbb{N}^*$. L'application $\sigma \longmapsto \sigma(\overline{1})$ est un isomorphisme de groupes de $(\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z}), \circ)$ sur $((\mathbb{Z}/n\mathbb{Z})^*, \times)$. D'où $[\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z}) : 1] = \varphi(n)$.*

Preuve. Puisque $\overline{1}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$, son image par tout automorphisme σ est générateur de $\mathrm{Im}\,(\sigma) = \mathbb{Z}/n\mathbb{Z}$; donc $\sigma(\overline{1})$ appartient à $(\mathbb{Z}/n\mathbb{Z})^*$. Désignons par Ψ l'application $\sigma \longmapsto \sigma(\overline{1})$. Pour tous σ et τ dans $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$ on a, en posant $\Psi(\tau) = \overline{m}$.

$$\Psi(\sigma \circ \tau) = \sigma \circ \tau(\overline{1}) = \sigma(\tau(\overline{1})) = \sigma(\overline{m}) = \sigma(m \cdot \overline{1}) = m \cdot \sigma(\overline{1}) = \overline{m} \times \Psi(\tau) = \psi(\sigma) \times \psi(\tau) .$$

L'application Ψ est donc un homomorphisme. Soit $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$. Alors $\overline{k}$ est d'ordre n dans le groupe additif $(\mathbb{Z}/n\mathbb{Z}), +)$. D'après le corollaire 2.2.3 du chapitre II, il existe un unique endomorphisme α de $(\mathbb{Z}/n\mathbb{Z})$ tel que $\alpha(\overline{1}) = \overline{k}$; $\overline{k}$ étant générateur α est surjectif, donc bijectif puisque $\mathbb{Z}/n\mathbb{Z}$ est fini. Il en résulte que Ψ est bijectif. ∎

2 Produits direct et semi-direct

2.1. Produit direct

Rappelons que si K et H sont deux groupes, nous avons défini le produit direct $G = K \times H$ ainsi que les homomorphismes $\iota_H \in \mathrm{Hom}\,(H, G)$, $\iota_K \in \mathrm{Hom}\,(K, G)$, $\pi_H \in \mathrm{Hom}\,(G, H)$ et $\pi_K \in \mathrm{Hom}\,(G, K)$. Alors $K' = K \times \{e_H\} = \mathrm{Im}\,(\iota_K) = \mathrm{Ker}\,(\pi_H)$ est un sous-groupe distingué de G, de même pour $H' = \{e_K\} \times H = \mathrm{Im}\,(\iota_H) = \mathrm{Ker}\,(\pi_K)$.

2.1.1. Théorème. *Soient G, H et K des groupes. Pour que le groupe G soit isomorphe au produit direct $K \times H$, il faut et il suffit qu'il existe dans G deux sous-groupes distingués K' et H' isomorphes respectivement à K et H tels que $K'H' = G$ et $K' \cap H' = \{e\}$.*

Preuve. La condition nécessaire est immédiate ; en effet $K' = K \times \{e_H\}$ et $H' = \{e_K\} \times H$ possèdent les propriétés voulues.
Montrons le caractère suffisant de cette condition. Prouvons tout d'abord que pour tout k' de K' et tout h' de H' on a $k'h' = h'k'$. En effet puisque H' et K' sont distingués, $k'h'k'^{-1}h'^{-1} = (k'h'k'^{-1})h'^{-1} = k'(h'k'^{-1}h'^{-1})$ appartient à la fois à H' et à K' et on a donc $k'h'k'^{-1}h'^{-1} = e$ i.e. $k'h' = h'k'$.
Soit α (resp. β) un isomorphisme de K sur K' (resp. H sur H'). Désignons par Θ

l'application de $K \times H$ dans G définie par $(k,h) \longmapsto \alpha(k)\beta(h)$. Cette application est surjective puisque $K'H' = G$. Pour tous h_1, h_2 dans H et tous k_1, k_2 dans K on a :

$$\begin{aligned}\Theta\,(\,(k_1,h_1)(k_2,h_2)\,) &= \Theta\,(\,(k_1k_2,h_1h_2)\,) = \alpha(k_1k_2)\beta(h_1h_2) = \alpha(k_1)\alpha(k_2)\beta(h_1)\beta(h_2)\\ &= \alpha(k_1)\beta(h_1)\alpha(k_2)\beta(h_2) = \Theta\,(\,(k_1,h_1)\,)\,\Theta\,(\,(k_2,h_2)\,)\ .\end{aligned}$$

Donc Θ est un homomorphisme. Si (k,h) appartient à $\mathrm{Ker}\,(\Theta)$, alors $\alpha(k)\beta(h) = e$ et $\alpha(k) = \beta(h)^{-1}$ appartient à $K' \cap H'$; il en résulte que $\alpha(k) = \beta(h)^{-1} = e$ et par suite $(k,h) = (e_K, e_H)$. En résumé Θ est un isomorphisme. ∎

2.1.2. Exemple. *Le groupe orthogonal $\boldsymbol{O}_3(\mathbb{R})$ est isomorphe au produit direct de $\boldsymbol{SO}_3(\mathbb{R})$ par $\mathbb{Z}/2\mathbb{Z}$.*
Le groupe $K' = \boldsymbol{SO}_3(\mathbb{R})$, noyau de l'homomorphisme déterminant, est distingué dans $\boldsymbol{O}_3(\mathbb{R})$ ainsi que le sous-groupe $H' = \{\mathrm{Id}\,, -\mathrm{Id}\,\}$ inclus dans le centre. On vérifie ensuite facilement les conditions $K'H' = G$ et $K' \cap H' = \{\mathrm{Id}\,\}$.

2.2. Produit semi-direct

2.2.1. Proposition. *Soient K et H deux groupes. Supposons que le groupe H agisse par automorphismes sur K c'est à dire qu'il existe $\varphi : h \longmapsto \varphi_h$ homomorphisme de H dans* $\mathrm{Aut}\,(K)$. *Pour tous k, k' dans K et tous h, h' dans H posons*

$$(k,h) * (k',h') = (k\varphi_h(k'), hh')\ .$$

Alors $(K \times H, *)$ est un groupe ; son élément neutre est (e_K, e_H) et l'inverse de (k,h) est $(\varphi_{h^{-1}}(k^{-1}), h^{-1})$.

Preuve. Il est clair que la loi $*$ est interne sur $K \times H$; vérifions l'associativité. Avec des notations évidentes on a :

$$\begin{aligned}((k,h) * (k',h')) * (k'',h'') &= (k\varphi_h(k'), hh') * (k'',h'')\\ &= (k\varphi_h(k')\varphi_{hh'}(k''), hh'h'')\\ &= (k\varphi_h(k')(\varphi_h(\varphi_{h'}(k'')), hh'h'')\\ &= (k\varphi_h(k'\varphi_{h'}(k'')), hh'h'')\\ &= (k,h) * (k'\varphi_{h'}, h'h'')\\ &= (k,h) * ((k',h') * (k'',h''))\ .\end{aligned}$$

Les vérifications de l'élément neutre et de l'inverse sont faciles et laissées au lecteur. ∎

2.2.2. Définition. Le groupe défini dans la proposition précédente est appellé *produit semi-direct* de K par H ; on le note $K \underset{\varphi}{\times} H$.

2.2.3. Théorème . *Soient G, H et K des groupes. Pour que le groupe G soit isomorphe à un produit semi-direct de K par H, il faut et il suffit qu'il existe dans G un sous-groupe distingué K' isomorphe à K, et un sous-groupe H' isomorphe à H, tels que $K'H' = G$ et $K' \cap H' = \{e\}$.*

Preuve. La nécessité de la condition est immédiate : les sous-groupes $K' = K \times \{e_H\}$ et $H' = \{e_K\} \times H$ possèdent les propriétés voulues.
Montrons maintenant le caractère suffisant de cette condition. Le sous-groupe K' étant distingué, pour tout $h' \in H'$ l'automorphisme intérieur $\mathrm{Ad}_{h'}$, le laisse invariant et définit donc par restriction un automorphisme de K' que nous noterons $\psi_{h'}$. Puisque Ad est un homomorphisme de G dans $\mathrm{Aut}\,(G)$, il en résulte que $\psi \in \mathrm{Hom}\,(H', \mathrm{Aut}\,(K'))$. Considérons l'application Θ de $K' \underset{\psi}{\times} H'$ dans G définie par $(k', h') \longmapsto k'h'$. Pour tous h'_1, h'_2 dans H' et tous k'_1, k'_2 dans K' on a :

$$\begin{aligned}\Theta\,(\,(k'_1, h'_1) * (k'_2, h'_2)\,) &= \Theta\left((k'_1\psi_{h'_1}(k'_2), h'_1h'_2)\right) = k'_1\psi_{h'_1}(k'_2)h'_1h'_2 = k'_1h'_1k'_2(h'_1)^{-1}h'_1h'_2 \\ &= k'_1h'_1k'_2h'_2 = \Theta\,(\,(k'_1, h'_1)\,)\,\Theta\,(\,(k'_2, h'_2)\,)\ .\end{aligned}$$

Donc Θ est un homomorphisme. Comme dans le théorème de caractérisation du produit direct, on vérifie que Θ est bijectif. On a donc $K' \underset{\psi}{\times} H'$ isomorphe à G.
Soit α (resp. β) un isomorphisme de K sur K' (resp. H sur H'). La bijection $\alpha \times \beta$ de $K \times H$ sur $K' \times H'$ permet par transport de structure de munir $K \times H$ d'une structure de groupe. On vérifie sans peine qu'il s'agit d'une structure de produit semi-direct défini par l'homomorphisme φ de H dans $\mathrm{Aut}\,(K)$ donné par : $\varphi_h = \alpha^{-1} \circ \psi_{\beta(h)} \circ \alpha$. ∎

2.2.4. Exemples .

a) Dans le cas où φ est l'homomorphisme trivial de H dans $\mathrm{Aut}\,(K)$ (i.e. constant égal à Id_K), on retrouve le produit direct.

b) *Soit $n \geq 2$. Le groupe symétrique $\mathcal{S}_n$ est isomorphe à un produit semi-direct du groupe alterné $\mathcal{A}_n$ par $\mathbb{Z}/2\mathbb{Z}$.*
Soient τ une transposition fixée et $H = \{\mathrm{Id}, \tau\}$. Alors $\mathcal{A}_n$ est un sous-groupe distingué de $\mathcal{S}_n$, H est un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$, l'intersection de $\mathcal{A}_n$ et de H est réduite à $\{\mathrm{Id}\}$ et tout $\sigma \in \mathcal{S}_n$ peut se décomposer sous la forme $\sigma = \sigma \circ \mathrm{Id}$ si $\sigma \in \mathcal{A}_n$ et $\sigma = (\sigma \circ \tau) \circ \tau$ sinon.

c) *Le groupe orthogonal $\boldsymbol{O}_2(\mathbb{R})$ est isomorphe à un produit semi-direct, non direct de $\boldsymbol{SO}_2(\mathbb{R})$ par $\mathbb{Z}/2\mathbb{Z}$.*
Le groupe $K = \boldsymbol{SO}_2(\mathbb{R})$, noyau de l'homomorphisme déterminant, est distingué dans $\boldsymbol{O}_2(\mathbb{R})$. Soit S appartenant à $\boldsymbol{O}_2(\mathbb{R}) \backslash \boldsymbol{SO}_2(\mathbb{R})$, ($S$ est la matrice d'une symétrie orthogonale par rapport à une droite). Le sous-groupe $H = \{\mathrm{Id}, S\}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et $H \cap K = \{\mathrm{Id}\}$. Il reste à montrer que $KH = \boldsymbol{O}_2(\mathbb{R})$. Soit $M \in \boldsymbol{O}_2(\mathbb{R})$. Si $M \in \boldsymbol{SO}_2(\mathbb{R})$ alors $M = M\mathrm{Id}$ et appartient à KH, sinon MS est alors élément de $\boldsymbol{SO}_2(\mathbb{R})$ et $M = (MS)S$ appartient à KH.

Les groupes $\boldsymbol{SO}_2(\mathbb{R})$ et $\mathbb{Z}/2\mathbb{Z}$ étant abéliens, le groupe non commutatif $\boldsymbol{O}_2(\mathbb{R})$ ne peut être isomorphe à leur produit direct.

d) *Pour tout entier $n \geq 2$, le groupe $\boldsymbol{GL}_n(\mathbb{R})$ est isomorphe à un produit semi-direct de $\boldsymbol{SL}_n(\mathbb{R})$, sous-groupe des matrices de déterminant 1, par $\mathbb{R}^*$.*
Pour $\lambda \in \mathbb{R}^*$, soit $D_\lambda = \mathrm{Diag}(1, \cdots, 1, \lambda)$. Alors $H = \{ D_\lambda \,;\ \lambda \in \mathbb{R}^* \}$ est un sous-groupe de $\boldsymbol{GL}_n(\mathbb{R})$ isomorphe à $\mathbb{R}^*$, le sous-groupe $\boldsymbol{SL}_n(\mathbb{R})$ est distingué comme noyau du déterminant, l'intersection de $\boldsymbol{SL}_n(\mathbb{R})$ et de H est réduite à $\{\mathrm{Id}\}$, et tout $M \in \boldsymbol{GL}_n(\mathbb{R})$ peut se décomposer sous la forme $M = (D_{\delta^{-1}}\, M)\, D_\delta$ où $\delta = \det(M)$.

e) D'autres exemples seront fournis par la géométrie.

2.2.5. Corollaire. *Soit G un groupe fini d'ordre mn avec m et n premiers entre eux. Si K est un sous-groupe d'ordre m, distingué dans G et si H est un sous-groupe d'ordre n, alors G est isomorphe à un produit semi-direct de K par H. Si de plus H est distingué dans G, alors le produit est direct.*

Preuve. D'après le théorème de Lagrange, comme $K \cap H$ est un sous-groupe de K et de H, son ordre divise m et n. Donc $K \cap H = \{e\}$. Le sous-groupe K étant distingué dans G, nous pouvons appliquer le théorème d'Emmy Nœther (Chap III Théorème 2.3.1) et $HK/K \simeq H/H \cap K$. D'où $\dfrac{[HK : 1]}{[K : 1]} = \dfrac{[H : 1]}{[H \cap K : 1]}$ et $[HK : 1] = mn$. Par conséquent le sous-groupe $KH = HK$ ayant même ordre que G, on a $G = KH$. Les hypothèses du théorème de caractérisation du produit semi-direct sont remplies.
Si de plus H est distingué dans G on peut appliquer le théorème de caractérisation du produit direct (Théorème 2.1.1). ∎

3 Théorèmes de Sylow

Le théorème de Lagrange affirme que l'ordre de tout sous-groupe divise l'ordre du groupe. Réciproquement si d est un diviseur de l'ordre d'un groupe G, existe-t-il un sous-groupe d'ordre d ? Si G est cyclique la réponse est positive (Théorème 1.1.6). Pour les groupes abéliens nous montrerons, tout à la fin du cours, que le résultat est encore vrai. Mais en général la réciproque est fausse : par exemple on peut constater que le groupe $\mathcal{A}_4$ (d'ordre 12) ne possède pas de sous-groupe d'ordre 6. Nous allons cependant démontrer une réciproque partielle lorsque d est puissance d'un nombre premier.

3.1. Sous-groupes de Sylow

3.1.1. Définitions. Soient p un nombre premier et G un groupe d'ordre $p^\alpha m$ avec p ne divisant pas m. On dit qu'un sous-groupe H de G est un *p-sous-groupe de G* si l'ordre de H est une puissance de p i.e. $[H : 1] = p^\beta$ avec $\beta \in [0, \alpha]_{\mathbb{N}}$.

On dit que H est un *p-sous-groupe de Sylow de* G si son ordre est p^α. Un p-sous-groupe de Sylow est donc un p-sous-groupe de G tel que p ne divise pas $[G : H]$.

3.1.2. Exemple. *Soient p un nombre premier et $\mathbb{F}_p$ le corps $(\mathbb{Z}/p\mathbb{Z},\ +\ ,\times)$. Pour tout $n \in \mathbb{N}^*$ le groupe $\boldsymbol{GL}_n(\mathbb{F}_p)$ possède un p-sous-groupe de Sylow.*

Preuve. Rappelons tout d'abord que p étant premier, $\varphi(p) = p - 1$ c'est à dire que $(\mathbb{Z}/p\mathbb{Z},\ +\ ,\times)$ est un corps. Déterminons l'ordre de $\boldsymbol{GL}_n(\mathbb{F}_p)$. Il suffit de dénombrer les bases de $\mathbb{F}_p^n$ car à toute matrice de $\boldsymbol{GL}_n(\mathbb{F}_p)$ on associe bijectivement la base constituée par ses vecteurs colonnes. Or dans $\mathbb{F}_p^n$, un sous-espace vectoriel de dimension k est de cardinal p^k. Le premier vecteur de base e_1 ne doit pas être nul, donc $p^n - 1$ possibilités ; le deuxième vecteur de base e_2 ne doit pas être dans $\mathrm{Vect}\{e_1\}$, donc $p^n - p$ possibilités, ..., le k-ième vecteur de base e_k ne doit pas être dans $\mathrm{Vect}\{e_1, \cdots, e_{k-1}\}$, donc $p^n - p^{k-1}$ possibilités, ..., le n-ième vecteur de base e_n ne doit pas être dans $\mathrm{Vect}\{e_1, \cdots, e_{n-1}\}$, donc $p^n - p^{n-1}$ possibilités. Il en résulte que

$$\begin{aligned}
[\,\boldsymbol{GL}_n(\mathbb{F}_p) : 1] &= (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}) \\
&= p^{1+\cdots+(n-1)}\, m \quad \text{avec } p \text{ ne divisant pas } m \\
&= p^{\frac{n(n-1)}{2}}\, m \quad \text{avec } p \text{ ne divisant pas } m.
\end{aligned}$$

L'ensemble des matrices triangulaires supérieures dont la diagonale principale est constituée de 1 est un sous-groupe H d'ordre $p^{\frac{n(n-1)}{2}}$ de $\boldsymbol{GL}_n(\mathbb{F}_p)$
$(H = \{\, A = (a_{i\,j}) \in G\ ;\ \forall (i,j)\ 1 \le j < i \le n \quad a_{i\,j} = 0 \quad \text{et} \quad a_{i\,i} = 1\,\})$. ∎

3.2. Premier théorème de Sylow

3.2.1. Lemme. *Si un groupe fini G possède un p-sous-groupe de Sylow S, alors pour tout sous-groupe H de G il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-sous-groupe de Sylow de H.*

Preuve. Le groupe G opère par translation à gauche sur l'ensemble quotient G/S ; par restriction le groupe H opère également sur G/S : pour tout $h \in H$ et tout $g \in G$ on a $\lambda_h(gS) = hgS$. Déterminons, pour cette action, le stabilisateur H_{gS} de la classe gS. Pour tout $h \in H$, on a

$$\begin{aligned}
h \in H_{gS} &\Leftrightarrow hgS = gS \\
&\Leftrightarrow \exists s \in S \quad hg = gs \\
&\Leftrightarrow \exists s \in S \quad h = gsg^{-1} \\
&\Leftrightarrow h \in gSg^{-1}
\end{aligned}$$

Donc $H_{gS} = H \cap gSg^{-1}$. Ecrivons l'équation aux classes :

$$[G : S] = \mathrm{card}\,(G/S) = \sum_{g \in \Phi} [H : H_{gS}]\,.$$

Comme p ne divise pas $[G : S]$, il existe $a \in G$ tel que p ne divise pas $[H : H_{aS}]$. Le sous-groupe $K = aSa^{-1} \cap H$ est un p-sous-groupe (car inclus dans aSa^{-1}, conjugué de S) de H tel que $[H : K]$ n'est pas divisible par p ; c'est donc un p-sous-groupe de Sylow de H. ∎

3.2.2. Théorème. *Soient p un entier premier et G un groupe fini. Alors G possède un p-sous-groupe de Sylow.*

Preuve. Soit G un groupe d'ordre n. L'action de G sur lui-même par translation à gauche est fidèle (Chap. III Exemple 1.1.3.b) ; G est donc isomorphe à un sous-groupe de $\mathcal{S}(G)$ et par suite à un sous-groupe de $\mathcal{S}_n$ (Chap. III Proposition 3.1.1). Or $\mathcal{S}_n$ peut être plongé dans $\boldsymbol{GL}_n(\mathbb{F}_p)$ en envoyant $\sigma \in \mathcal{S}_n$ sur l'endomorphisme u_σ défini sur la base canonique de ${\mathbb{F}_p}^n$ par $u_\sigma(e_i) = e_{\sigma(i)}$ pour $i = 1 \dots n$. Il en résulte que G est isomorphe à un sous-groupe de $\boldsymbol{GL}_n(\mathbb{F}_p)$. Il suffit donc d'appliquer le lemme précédent dans le cas de l'exemple 3.1.2 pour conclure. ∎

3.3. Autres théorèmes de Sylow

3.3.1. Théorème. *Soient p un entier premier et G un groupe fini d'ordre $n = p^\alpha m$ avec p ne divisant pas m. Alors*

(*i*) *Tout p-sous-groupe de G est inclus dans un p-sous-groupe de Sylow.*

(*ii*) *Les p-sous-groupes de Sylow de G sont conjugués dans G.*

(*iii*) *Le nombre de p-sous-groupes de Sylow de G, divise m et est congru à 1 modulo p.*

Preuve. D'après le théorème précédent, il existe dans G un p-sous-groupe de Sylow S. Soit H un p-sous-groupe de G. D'après le lemme 3.2.1, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-sous-groupe de Sylow de H. Puisque H est un p-groupe il possède un unique p-sous-groupe de Sylow, lui-même ; on a donc $aSa^{-1} \cap H = H$ i.e. $H \subset aSa^{-1}$. L'assertion (i) est prouvée. Si de plus H est un p-sous-groupe de Sylow on a alors $H = aSa^{-1}$, ce qui démontre (ii).
Pour établir l'assertion (iii), faisons opérer G par conjugaison sur l'ensemble $\boldsymbol{S}_p$, des p-sous-groupes de Sylow de G. D'après (ii) cette action est transitive ; par conséquent $n_p = \text{card}\,(\boldsymbol{S}_p) = \text{card}\,(\mathcal{O}_S) = [G : G_S]$ est un diviseur de n.
Par restriction S agit sur $\boldsymbol{S}_p$; écrivons l'équation aux classes : $\text{card}\,(\boldsymbol{S}_p) = \sum [S : S_{K_i}]$; or $[S : S_K] = 1 \Leftrightarrow S \subset \mathcal{N}(K)$, où $\mathcal{N}(K)$ désigne le normalisateur de K.
D'après le théorème d'Emmy Nœther, si S est inclus dans $\mathcal{N}(K)$ alors KS est un groupe et $KS/K \simeq S/K \cap S$; il en résulte que KS est un p-sous-groupe contenant S, d'où $KS = S = K$. Dans l'équation aux classes il existe donc un seul terme valant 1 et les autres sont multiples de p. D'où n_p est congru à 1 modulo p. On en déduit que n_p est premier avec p^α ; comme il divise $p^\alpha m$, il doit diviser m. ∎

3.3.2. Remarque. Si p ne divise pas $[G : 1]$ alors $\{e\}$ est l'unique p-sous-groupe de Sylow de G.

3.3.3. Corollaire. *Soient p un nombre premier, G un groupe fini et S un p-sous-groupe de Sylow de G. Alors S est distingué dans G si et seulement si S est l'unique p-sous-groupe de Sylow de G.*

Preuve. Tout sous-groupe conjugué de S a même ordre que S et est un p-sous-groupe de Sylow de G. D'après l'assertion (ii) du théorème précédent, S coïncide avec tous ses conjugués si et seulement s'il n'existe qu'un unique p-sous-groupe de Sylow de G. ∎

3.3.4. Applications.

(i) *Tout groupe d'ordre 15 est cyclique.*

(ii) *Tout groupe d'ordre 45 est abélien.*

(iii) *Tout groupe d'ordre 6 est isomorphe à C_6 ou $\mathcal{S}_3$.*

Preuve. (i) Soit G un groupe d'ordre 15. On a $15 = 3 \times 5$. Il existe dans G un 3-sous-groupe de Sylow K (d'ordre 3) et le nombre n_3, de 3-sous-groupes de Sylow de G, divise 5 et est congru à 1 modulo 3 ; donc $n_3 = 1$ et K est distingué dans G. De même il existe un unique 5-sous-groupe de Sylow H (d'ordre 5) qui est distingué. Comme 3 et 5 sont premiers, K et H sont cycliques. D'après le corollaire 2.2.5, G est isomorphe au produit direct $K \times H$. D'après le théorème chinois (1.2.1), G est cyclique.
(ii) Soit G un groupe d'ordre 45. On a $45 = 3^2 \times 5$. En reprenant le même raisonnement que précédemment, on prouve qu'il existe dans G un unique 3-sous-groupe de Sylow K (d'ordre 9) et un unique 5-sous-groupe de Sylow H (d'ordre 5), tous deux distingués, puis que G est isomorphe au produit direct $K \times H$. Or H, isomorphe à C_5, est abélien, et K, d'ordre 3^2, est également abélien (Chap III Corollaire 1.4.3) ; leur produit direct est abélien.
(iii) Soit G un groupe d'ordre 6. D'après les théorèmes de Sylow, il existe dans G un unique sous-groupe K d'ordre 3 et un sous-groupe H d'ordre 2 ; le nombre n_2 de 2-sous-groupes de Sylow de G est 1 ou 3. Si $n_2 = 1$, on obtient $G \simeq C_3 \times C_2 \simeq C_6$.
Si $n_2 = 3$, en utilisant le théorème de caractérisation du produit semi-direct, on obtient $G \simeq C_3 \underset{\psi}{\times} C_2$ avec $\psi \in \mathrm{Hom}\,(C_2, \mathrm{Aut}\,(C_3))$. Or $\mathrm{Aut}\,(C_3)$ est un groupe d'ordre $\varphi(3) = 2$; i.e. $\mathrm{Aut}\,(C_3) = \{\mathrm{Id}, \alpha\}$. ll existe donc exactement deux homomorphismes de C_2 dans $\mathrm{Aut}\,(C_3)$ l'homorphisme trivial (constant de valeur Id) et ψ envoyant le générateur de C_2 sur α. L'homomorphisme trivial donne un produit direct, exclu ici car H n'est pas distingué. Il y a donc dans ce cas, au plus une seule structure. Comme par ailleurs nous connaissons l'existence de $\mathcal{S}_3$ possédant trois sous-groupes d'ordre 2, nous obtenons bien le résultat voulu. ∎

4 Groupes abéliens finis

4.1. Décomposition cyclique canonique d'un groupe abélien

4.1.1. Lemme. *Soient $(G, \cdot)$ un groupe abélien fini et $a \in G$ d'ordre maximum. Pour tout $\beta \in G/\langle a \rangle$ il existe un représentant $x \in G$ de β dont l'ordre est égal à l'ordre de β.*

Preuve. Posons $s = o(\beta)$ et notons φ l'homomorphisme canonique de G sur $G/\langle a \rangle$. Remarquons que pour tout représentant x de β, l'ordre $s = o(\beta) = o(\varphi(x))$ divise $o(x)$. Considérons un tel représentant x. Comme $\varphi(x^s) = \beta^s = \varphi(e)$, on a $x^s \in \mathrm{Ker}\,(\varphi) = \langle a \rangle$ et il existe $m \in \{0, \ldots, o(a) - 1\}$ tel que $x^s = a^m$. Par division euclidienne de m par s on obtient $m = sq + r$ avec $0 \leq r < s$. Posons $y = xa^{-q}$. C'est un représentant de β et donc s divise $o(y)$. De plus $y^s = x^s a^{-sq} = a^{m-sq} = a^r$. D'après la proposition 2.4.5, on obtient :

$$o(y^s) = \frac{o(y)}{\mathrm{PGCD}\ (o(y), s)} = \frac{o(y)}{s} \quad \text{et} \quad o(a^r) = \frac{o(a)}{\mathrm{PGCD}\ (o(a), r)}\ .$$

Ces ordres sont égaux, et a est d'ordre maximal, d'où $o(a) \geq o(y) = s\,\dfrac{o(a)}{\mathrm{PGCD}\ (o(a), r)}$. Soit $s \leq \mathrm{PGCD}\ (o(a), r)$. Compte tenu de l'inégalité $0 \leq r < s$, on a nécessairement $r = 0$ et $y^s = e$. La remarque initiale permet alors de conclure que y a le même ordre que β. ∎

4.1.2. Théorème. *Soit G un groupe abélien fini. Il existe une suite d'entiers croissante $1 < q_1 \leq q_2 \leq \cdots \leq q_\ell$, unique, telle que q_i divise q_{i+1} pour $i = 1, \ldots, \ell - 1$ et telle que G soit isomorphe à $C_{q_1} \times \cdots \times C_{q_\ell}$.*

Preuve. La démonstration se fait par récurrence sur $n = [G : 1]$. Pour $n = 1$ on $G = \{e\} \simeq C_1$.
Soit $n \geq 2$. Supposons établi le résultat pour tous les groupes abéliens d'ordre strictement inférieur à n. Considérons dans G un élément a d'ordre maximum. Le groupe G n'est pas réduit à $\{e\}$, on a $o(a) > 1$ et, $G/\langle a \rangle$ est d'ordre m avec $m = \dfrac{n}{o(a)} < n$. D'après l'hypothèse de récurrence et la caractérisation du produit direct il existe $k \in \mathbb{N}^*$, une suite d'entiers croissante $1 < q_1 \leq q_2 \leq \cdots \leq q_k$ avec q_i divise q_{i+1} et des sous-groupes cycliques $\Gamma_1, \ldots, \Gamma_k$ de $G/\langle a \rangle$ d'ordres respectifs $q_1, \ldots, q_k$ tels que $G/\langle a \rangle = \Gamma_1\Gamma_2 \cdots \Gamma_k$. Posons $\ell = k + 1$, $q_\ell = o(a)$ et $G_\ell = \langle a \rangle$. Pour $i = 1, \ldots, k$ soit α_i un générateur de Γ_i ; d'après le lemme, il existe dans G des représentants $a_1, \ldots, a_k$ de $\alpha_1, \ldots, \alpha_k$ ayant les mêmes ordres. Posons $G_i = \langle a_i \rangle$. Soit Ψ l'application du produit direct $G_1 \times \cdots \times G_\ell$ dans G définie pour tout (g_i) par : $\Psi(g_1, \ldots, g_\ell) = \prod_{i=1}^{\ell} g_i$. Le groupe G étant abélien, Ψ est un homomorphisme. Montrons qu'il est surjectif. Notons φ l'homomorphisme canonique de

G sur G/G_ℓ. Soit $x \in G$. Comme $\varphi(x)$ appartient à G/G_ℓ, Il existe des entiers $n_1, \ldots, n_k$ tels qu'en posant $g_i = a_i^{n_i}$ on ait

$$\varphi(x) = \prod_{i=1}^{k} \alpha_i^{n_i} = \prod_{i=1}^{k} \varphi(a_i)^{n_i} = \varphi\left(\prod_{i=1}^{k} g_i\right) .$$

Les éléments x et $y = \prod_{i=1}^{k} g_i$ ayant même image dans le quotient par G_ℓ, il existe $g_\ell \in G_\ell$ tel que $x = yg_\ell$. Par suite $x = \Psi(g_1, \ldots, g_\ell)$.

Or $[G : 1] = [G/G_\ell : 1][G_\ell : 1]$ et $[G/G_\ell] = \prod_{i=1}^{k} [\Gamma_i : 1] = \prod_{i=1}^{k} o(\alpha_i) = \prod_{i=1}^{k} o(a_i) = \prod_{i=1}^{k} [G_i : 1]$.

Donc $\prod_{i=1}^{\ell} G_i$ et G ont même ordre et Ψ est bijectif. D'où

$$G \simeq \prod_{i=1}^{\ell} G_i \simeq \prod_{i=1}^{\ell} C_{q_i} .$$

Par ailleurs $o((a_1, \ldots, a_\ell)) = \text{PPCM } (o(a_1), \ldots, o(a_\ell)) = \text{PPCM } (q_k, q_\ell)$ Comme a est d'ordre maximum q_ℓ, on a nécessairement q_k divise q_ℓ ; ce qui achève la démonstration de l'existence.

Supposons que l'on ait deux décompositions $G = G_1 \times \cdots \times G_\ell = H_1 \times \cdots \times H_k$ avec $G_i \simeq C_{q_i}$ et $H_j \simeq C_{q'_j}$. Soit p un facteur premier de q_1 et donc de $q_2, \ldots, q_\ell$. Comme G est abélien, l'application $f_p : x \longmapsto x^p$, est un endomorphisme. Il laisse stable chacun des sous-groupes G_i ou H_j. De plus G_i étant cyclique engendré par a_i d'ordre q_i, son image $f_p(G_i)$ est cyclique engendré par $f_p(a_i) = a_i^p$ d'ordre $\dfrac{q_i}{p}$. De même H_j étant cyclique engendré par b_j d'ordre q'_j, son image $f_p(H_j)$ est cyclique engendré par $f_p(b_j) = b_j^p$ d'ordre $\dfrac{q'_j}{\text{PGCD } (q'_j, p)} = \dfrac{q'_j}{p}$ si $p | q'_j$ et q'_j sinon. Comme $q'_1 | q'_2 | \cdots | q'_k$, il existe un entier m tel que p ne divise pas $q'_1, \ldots, q'_m$ et p divise q'_j pour $j > m$. On a alors

$$C_{\frac{q_1}{p}} \times \cdots \times C_{\frac{q_\ell}{p}} \simeq \prod_{i=1}^{\ell} f_p(G_i) = f_p(G) = \prod_{j=1}^{k} f_p(H_j) \simeq \prod_{j=1}^{m} C_{q'_j} \times \prod_{j>m} C_{\frac{q'_j}{p}} \quad (*) .$$

En calculant l'ordre de ces groupes, il vient $\dfrac{n}{p^\ell} = \dfrac{q_1 \times \cdots \times q_\ell}{p^\ell} = \prod_{j=1}^{m} q'_j \times \prod_{j>m} \dfrac{q'_j}{p} = \dfrac{n}{p^{(k-m)}}$.

On en déduit que $k \geq \ell$. Les deux décompositions jouant le même rôle on a en fait $k = \ell$, d'où $m = 0$. Supprimons, s'il y a lieu, les facteurs réduits à $\{e\}$ dans l'égalité $(*)$, c'est à dire si $q_i = p$ (pour $i < \ell'$) et $q'_j = p$ (pour $j < k'$). Par hypothèse de récurrence appliquée à $f_p(G)$, les suites d'exposants : $\dfrac{q_{\ell'}}{p}, \cdots, \dfrac{q_\ell}{p}$ et $\dfrac{q'_{k'}}{p}, \cdots, \dfrac{q'_\ell}{p}$ coïncicent ; on a donc $k' = \ell'$ et $q_i = q'_i$ pour $i \geq \ell'$. Quant aux groupes G_i pour $i < \ell'$ et H_j pour $j < \ell' = k'$, s'il en existe, ils ont tous pour ordre p. Comme $[G : 1] = \prod_{i=1}^{\ell} [G_i : 1] = \prod_{j=1}^{k} [H_j : 1]$, on voit qu'il en existe le même nombre dans les deux décompositions. ∎

4.1.3. Définition. Soit G un groupe abélien fini. La suite des entiers $q_1, \ldots, q_\ell$ définie dans le théorème précédent est appelée *suite des diviseurs élémentaires* ou *suite des invariants* de G. Cette suite caractérise G à isomorphisme près.

4.1.4. Corollaire. *Soit G un p-groupe abélien fini. Il existe des entiers $1 \leq r_1 \leq \cdots \leq r_k$, uniques, tels que G soit isomorphe à $C_{p^{r_1}} \times \cdots \times C_{p^{r_k}}$.*

Preuve. Ce corollaire résulte immédiatement du théorème 4.1.2. ∎

4.1.5. Corollaire. *Soit K un corps fini (commutatif)[3]. Le groupe multiplicatif K^* est cyclique.*

Preuve. Le groupe K^* est un groupe abélien fini. Soit $(q_1, \ldots, q_\ell)$ la suite de ses invariants : $K^* \simeq C_{q_1} \times \cdots \times C_{q_\ell}$. Comme q_ℓ est multiple de tous les q_j on a donc $x^{q_\ell} = 1$ pour tout $x \in K^*$. Le polynôme, non nul, $X^{q_\ell} - 1$ de $K[X]$ admet donc tout élément de K^* pour racine. Donc son degré q_ℓ est supérieur ou égal à $\operatorname{card}(K^*) = \prod_{j=1}^{\ell} q_j$. Ceci n'est possible que si $\ell = 1$ c'est à dire si K^* est cyclique. ∎

4.1.6. Corollaire. *Soit G un groupe abélien fini d'ordre n. Pour tout diviseur d de n, il existe (au moins) dans G un sous-groupe d'ordre d.*

Preuve. Soit $(q_1, \ldots, q_\ell)$ la suite des invariants de G ; on a $n = \prod_{j=1}^{\ell} q_j$. Comme d divise n, on peut écrire d sous la forme $d = \prod_{j=1}^{\ell} d_j$ avec d_j divisant q_j pour tout j. (Par exemple $d_1 = \text{PGCD}\,(d, q_1)$, …, $d_2 = \text{PGCD}\,(\frac{d}{d_1}, q_2)$, …, $d_\ell = \text{PGCD}\,(\frac{d}{d_1 \cdots d_{\ell-1}}, q_\ell) = \frac{d}{d_1 \cdots d_{\ell-1}}$).
Dans le groupe cyclique C_{q_j}, soit H_j le sous-groupe d'ordre d_j. Alors $H_1 \times \cdots \times H_\ell$ est un sous-groupe d'ordre d de $C_{q_1} \times \cdots \times C_{q_\ell}$. Comme G est isomorphe à $C_{q_1} \times \cdots \times C_{q_\ell}$, il possède un sous-groupe d'ordre d. ∎

4.2. Composantes primaires

Nous allons voir maintenant qu'il existe une autre décomposition des groupes abéliens finis, très liée à la précédente et qui dans la pratique sera la première étape pour obtenir la décomposition cyclique canonique.

4.2.1. Lemme. *Soit G un groupe abélien fini. Pour tout entier p premier,*
$G_p = \{x \in G\ ;\ \exists \alpha \in \mathbb{N}\ o(x) = p^\alpha\}$ est l'unique p-sous-groupe de Sylow de G.

[3] D'après le théorème de Wedderburn tout corps fini est commutatif.

Preuve. Comme G est commutatif, tout sous-groupe de G est distingué et G possède un unique p-sous-groupe de Sylow S d'ordre p^r. L'ordre de tout $y \in S$ divise p^r, donc est une puissance de p, et y appartient à G_p. Réciproquement soit $x \in G_p$. Son ordre est une puissance de p ; le p-sous groupe de G engendré par x est contenu dans un p-sous groupe de Sylow de G, c'est-à-dire dans S et x appartient à S. ∎

4.2.2. Définition. Soient G un groupe abélien fini et p un entier premier divisant l'ordre de G. On appelle *composante p-primaire* de G le sous-groupe G_p défini dans le lemme précédent.

4.2.3. Proposition. *Tout groupe abélien fini $(G, \cdot)$ est isomorphe au produit direct de ses composantes primaires : $G \simeq G_{p_1} \times \cdots \times G_{p_k}$ si $[G : 1] = p_1^{r_1} \cdots p_k^{r_k}$ est la décomposition en facteurs premiers de son ordre. De plus, si $G \simeq \prod H_j$ est une autre décomposition de G en un produit fini de q_j-sous-groupes, où les nombres premiers q_j sont deux à deux distincts, alors les H_j sont les composantes primaires de G.*

Preuve. Soit Ψ l'application du produit direct $G_{p_1} \times \cdots \times G_{p_k}$ dans G définie pour tout (x_i) par : $\Psi(x_1, \cdots, x_k) = \prod_{i=1}^{k} x_i$. Le groupe G étant abélien, Ψ est un homomorphisme. Soit $(x_i) \in \mathrm{Ker}\,(\Psi)$. On a $x = \prod_{i=1}^{k} x_i = e$. Pour $j \in [1, k]_{\mathbb{N}}$, posons $m_j = \prod_{i \neq j} p_i^{r_i}$; pour tout $i \neq j$ on a $x_i^{m_j} = e$ et par suite $e = x^{m_j} = x_j^{m_j}$. Donc m_j est un multiple de $o(xj)$ qui est une puissance de p_j, nécessairement $o(x_j) = 1$ et $x_j = e$. Il en résulte que Ψ est injective et par suite bijective puisque $[G_{p_1} \times \cdots \times G_{p_k} : 1] = [G : 1]$.
Si $G \simeq \prod_{j=1}^{\ell} H_j$ alors $\prod_{i=1}^{k} p_i^{r_i} = [G : 1] = \prod_{j=1}^{\ell} [H_j : 1] = \prod_{j=1}^{\ell} q_j^{\alpha_j}$. Par unicité de la décomposition d'un entier en produit de facteurs premiers on obtient $k = \ell$ et quitte à modifier la numérotation $[H_j : 1] = p_j^{r_j}$. Il en résulte que H_j est l'unique p_j-sous-groupe de Sylow de G, c'est à dire G_{p_j}. ∎

4.2.4. Exemples.

a) $G = \mathbb{Z}/300\mathbb{Z}$, d'ordre $300 = 2^2 \times 3 \times 5^2$, est produit de ses sous-groupes de Sylow, qui dans cet exemple sont cycliques comme sous-groupes d'un groupe cyclique :
$G_2 = \{\overline{k} \in G\ ;\ 4\overline{k} = \overline{0}\}$ engendré par $\overline{75}$, d'ordre 4,
$G_3 = \{\overline{k} \in G\ ;\ 3\overline{k} = \overline{0}\}$ engendré par $\overline{100}$, d'ordre 3,
$G_5 = \{\overline{k} \in G\ ;\ 25\overline{k} = \overline{0}\}$ engendré par $\overline{12}$, d'ordre 25.
Ainsi G est isomorphe à $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/25\mathbb{Z})$. Cela se vérifie directement, car un produit de groupes cycliques d'ordres deux à deux premiers entre eux est cyclique.

b) Considérons $G = C_{60} \times C_{72}$. On a $60 = 2^2 \times 3 \times 5$ et $72 = 2^3 \times 3^2$.
Comme dans l'exemple précédent, la décomposition primaire de C_{60} est $C_4 \times C_3 \times C_5$

et celle de C_{72} est $C_8 \times C_9$.
On en déduit la décomposition primaire de G : $(C_4 \times C_8) \times (C_3 \times C_9) \times C_5$.
Nous pouvons d'abord regrouper les facteurs d'ordre maximum dans chaque composante primaire : $C_8 \times C_9 \times C_5 \simeq C_{360}$, puis itérer le procédé avec les facteurs restants $C_4 \times C_3 \simeq C_{12}$. On obtient donc $G \simeq C_{12} \times C_{360}$. C'est la décomposition cyclique canonique de G. Par conséquent 12 et 360 sont les invariants de $G = C_{60} \times C_{72}$.

c) Cherchons quelles structures peut avoir, à isomorphisme près, un groupe abélien d'ordre $600 = 2^3 \times 5^2 \times 3$.
La composante 2-primaire G_2 est un groupe d'ordre 2^3. Ses structures possibles sont classifiées, par les suites d'entiers $r_1 \leq \cdots \leq r_k$ telles que $r_1 + \cdots + r_k = 3$. Donc G_2 est, à isomorphisme près, l'un des groupes suivants : C_8, $C_2 \times C_4$ ou $C_2 \times C_2 \times C_2$.
De même, G_3 d'ordre 3 est isomorphe à C_3 et G_5, d'ordre 5^2, est isomorphe à C_{25} ou $C_5 \times C_5$.
Il existe donc $3 \times 1 \times 2 = 6$ structures possibles pour G qui sont :

$$\begin{aligned}
C_8 \times C_3 \times C_{25} &\simeq C_{600} \\
C_8 \times C_3 \times (C_5 \times C_5) &\simeq C_5 \times C_{120} \\
(C_2 \times C_4) \times C_3 \times C_{25} &\simeq C_2 \times C_{300} \\
(C_2 \times C_4) \times C_3 \times (C_5 \times C_5) &\simeq C_{10} \times C_{60} \\
(C_2 \times C_2 \times C_2) \times C_3 \times C_{25} &\simeq C_2 \times C_2 \times C_{150} \\
(C_2 \times C_2 \times C_2) \times C_3 \times (C_5 \times C_5) &\simeq C_2 \times C_{10} \times C_{30}.
\end{aligned}$$

Index