

# Master 1 Mathématiques

## *Algèbre 1*

*(Groupes finis et arithmétique dans les anneaux)*

R. Taillefer

Rachel.Taillefer@uca.fr

2024-2025



---

# Préambule

---

Ce texte constitue un support de cours. La version distribuée en cours ne contient pas de démonstrations, qui seront faites en cours.

Le cours est divisé en deux grandes parties :

- Une étude des groupes finis, de certains résultats de classification et des outils pour les établir.
- De l'arithmétique dans les anneaux et les anneaux de polynômes à plusieurs indéterminées.

Ce document contient inévitablement des erreurs et fautes de frappe, merci de me les signaler.

## RÉFÉRENCES

- Jean Delcourt, *Théorie des groupes*, éditions Dunod
- David S. Dummit, Richard M. Foote, *Abstract algebra*, John Wiley and Sons
- Daniel Guin, *Algèbre, tome I : groupes et anneaux*, éditions Belin
- Daniel Perrin, *Cours d'algèbre*, éditions Ellipses

<https://univ-scholarvox-com.ezproxy.uca.fr/> contient également des ouvrages disponibles, accessibles via l'ENT (chercher Scholarvox dans les ressources en ligne des bibliothèques).



# TABLE DES MATIÈRES

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| <b>Première partie : Groupes</b>                                        | <b>9</b>  |
| <b>Chapitre 1 Groupes : rappels et compléments</b>                      | <b>9</b>  |
| I Premières définitions . . . . .                                       | 9         |
| II Classes modulo un sous-groupe . . . . .                              | 12        |
| III Sous-groupes normaux . . . . .                                      | 13        |
| IV Parties génératrices, groupes cycliques . . . . .                    | 16        |
| V Produit direct de groupes . . . . .                                   | 22        |
| VI Suites exactes . . . . .                                             | 27        |
| <b>Chapitre 2 Groupes finis abéliens</b>                                | <b>29</b> |
| I Dual d'un groupe . . . . .                                            | 29        |
| II Application à la classification des groupes finis abéliens . . . . . | 34        |
| <b>Chapitre 3 Produit semi-direct de groupes</b>                        | <b>39</b> |
| I Construction du produit semi-direct . . . . .                         | 39        |
| II Caractérisation du produit semi-direct . . . . .                     | 42        |
| <b>Chapitre 4 Groupes opérant sur un ensemble. Applications.</b>        | <b>45</b> |
| I Définitions et exemples . . . . .                                     | 45        |
| II Orbites, stabilisateurs . . . . .                                    | 47        |
| III Théorèmes de Sylow . . . . .                                        | 51        |
| IV Applications à la classification des groupes finis . . . . .         | 54        |
| <b>Chapitre 5 Groupes symétriques et alternés</b>                       | <b>59</b> |
| I Générateurs du groupe symétrique . . . . .                            | 59        |
| II Le groupe alterné . . . . .                                          | 63        |
| III Quelques résultats sur les sous-groupes de $S_n$ . . . . .          | 66        |
| <b>Chapitre 6 Groupes résolubles</b>                                    | <b>69</b> |
| I Définition et exemples . . . . .                                      | 69        |
| II Groupe dérivé . . . . .                                              | 71        |
| <b>Annexe Annexe A Annexes sur les groupes</b>                          | <b>75</b> |
| I Rappels et compléments sur la dualité (espaces vectoriels) . . . . .  | 75        |
| II Groupes d'ordre $n$ avec $n < 60$ . . . . .                          | 76        |
| III Groupes d'ordre 8 . . . . .                                         | 78        |
| IV Groupes d'ordre 12 . . . . .                                         | 80        |
| V Groupes dicycliques . . . . .                                         | 82        |
| VI Caractères . . . . .                                                 | 84        |

|                                                                                   |            |
|-----------------------------------------------------------------------------------|------------|
| <b>Deuxième partie : Anneaux</b>                                                  | <b>89</b>  |
| <b>Chapitre 7 Rappels et compléments sur les anneaux</b>                          | <b>89</b>  |
| I Rappels de base . . . . .                                                       | 89         |
| II Idéaux premiers et maximaux. . . . .                                           | 93         |
| III Ensembles ordonnés et lemme de Zorn . . . . .                                 | 94         |
| IV Corps des fractions d'un anneau intègre . . . . .                              | 96         |
| <b>Chapitre 8 Arithmétique dans les anneaux</b>                                   | <b>99</b>  |
| I Rappels d'arithmétique. . . . .                                                 | 99         |
| II Anneaux factoriels . . . . .                                                   | 101        |
| <b>Chapitre 9 Anneaux de polynômes</b>                                            | <b>109</b> |
| I Anneaux de polynômes en plusieurs indéterminées . . . . .                       | 109        |
| II Fonctions polynomiales. . . . .                                                | 112        |
| III Arithmétique dans les anneaux de polynômes . . . . .                          | 114        |
| <b>Chapitre 10 Polynômes symétriques</b>                                          | <b>123</b> |
| I L'anneau des polynômes symétriques . . . . .                                    | 123        |
| II Polynômes symétriques élémentaires . . . . .                                   | 124        |
| III Structure des polynômes symétriques . . . . .                                 | 125        |
| IV Coefficients et racines de polynômes . . . . .                                 | 129        |
| V Exemple : le discriminant . . . . .                                             | 132        |
| <b>Annexe Annexe B Annexes sur les anneaux</b>                                    | <b>133</b> |
| I Complément sur le lemme de Zorn . . . . .                                       | 133        |
| II Formule des degrés pour les polynômes en plusieurs indéterminées . . . . .     | 1          |
| III Racines et facteurs irréductibles de polynômes et polynômes dérivés . . . . . | 2          |
| IV Complément : résultant de deux polynômes . . . . .                             | 5          |

**Première partie :**

**Groupes**



## Groupes : rappels et compléments

Les pages qui suivent fournissent des rappels et compléments sur les groupes. Pour plus de détails, on consultera le polycopié de L3.

### I. PREMIÈRES DÉFINITIONS

**Définition 1.1.** Un **groupe**  $G$  est un ensemble non vide muni d'une loi  $*$  :  $G \times G \longrightarrow G$  vérifiant :

(1)  $\forall (x, y, z) \in G^3$  on a  $x * (y * z) = (x * y) * z$  (associativité).

(2)  $\exists e \in G$  tel que  $\forall x \in G$  on a  $x * e = e * x = x$  (élément neutre).

(3)  $\forall x \in G, \exists \tilde{x} \in G$  tel que  $\tilde{x} * x = x * \tilde{x} = e$  (inverse ou symétrique)

Si de plus  $x * y = y * x$  pour tout  $(x, y) \in G^2$ , alors on dit que  $G$  est **abélien** (ou **commutatif**).

**Exercice.** Montrer l'unicité de l'élément neutre d'un groupe, ainsi que l'unicité de l'inverse d'un élément.

**Correction.** ➤ Soient  $e$  et  $e'$  deux éléments neutres de  $G$ . Alors  $e = ee' = e'$  puisque ce sont des éléments neutres.

➤ Soit  $x \in G$  et soient  $x_1$  et  $x_2$  deux inverses de  $x$ . Alors  $xx_1 = e = xx_2$  donc, en multipliant à gauche par  $x_1$  on obtient  $x_1xx_1 = x_1xx_2$  et donc  $x_1 = x_2$  puisque  $x_1x = e$ . ✓

On passera tout de suite aux habituels abus de notation :  $x * y = xy$  pour la loi,  $e = 1$  pour l'élément neutre et  $\tilde{x} = x^{-1}$  pour l'inverse ou, dans le cas d'une loi additive,  $x * y = x + y$ ,  $e = 0$  et  $\tilde{x} = -x$ .

**Exemples.** (1)  $(\mathbb{Z}, +)$  est un groupe abélien.

(2) Soit  $E$  un ensemble. L'ensemble des bijections de  $E$  dans  $E$  est un groupe pour la loi de composition. Il est noté  $S_E$  et il est appelé **groupe symétrique de  $E$** .

Soit  $n \in \mathbb{N}^*$ . Le groupe symétrique de l'ensemble  $E = \{1, \dots, n\} = \llbracket 1; n \rrbracket$  est noté  $S_n$ . Si  $n \geq 3$ , alors  $S_n$  n'est pas abélien.

(3) Le groupe linéaire  $GL_n(\mathbb{C}) = \{M \in M_n(\mathbb{C}) \mid \det(M) \neq 0\}$  est un groupe pour le produit des matrices. Il n'est pas abélien si  $n \geq 2$  (exercice).

(4)  $(\mathbb{C}^*, \cdot) (= (GL_1(\mathbb{C}), \cdot))$  est un groupe abélien.

**Définition 1.2.** Soient  $G$  et  $G'$  des groupes. Un **morphisme de groupes**  $f : G \longrightarrow G'$  est une application  $f$  telle que pour tout  $(x, y) \in G^2$  on a  $f(xy) = f(x)f(y)$ .

L'ensemble des morphismes de groupes de  $G$  dans  $G'$  est noté  $\text{Hom}(G, G')$ .

Un **endomorphisme** de groupes est un morphisme de groupes d'un groupe dans lui-même. L'ensemble des endomorphismes de  $G$  est noté  $\text{End}(G) = \text{Hom}(G, G)$ .

Un **isomorphisme** est un morphisme bijectif. Les groupes  $G$  et  $G'$  sont dits **isomorphes** s'il existe un isomorphisme de  $G$  vers  $G'$ . On note alors  $G \cong G'$ .

Un isomorphisme de  $G$  dans lui-même est appelé **automorphisme**. L'ensemble des automorphismes de  $G$  est noté  $\text{Aut}(G)$ .

**On cherche à classer les groupes à isomorphisme près.**

**Exercices.** (1) Démontrer que la composée de deux morphismes de groupes est encore un morphisme de groupes.

*Correction.* Soient  $f$  et  $g$  deux morphismes de groupes de  $G$  dans  $G'$ . Alors pour tout  $(x, y) \in G^2$  on a  $g \circ f(xy) = g(f(x)g(y)) = g(f(x))g(f(y)) = (g \circ f(x))(g \circ f(y))$  donc  $g \circ f$  est bien un morphisme de groupes. ✓

(2) Démontrer que l'ensemble des automorphismes d'un groupe est un groupe (pour la loi de composition; on doit donc démontrer en particulier que la bijection réciproque d'un isomorphisme est encore un morphisme de groupes).

*Correction.* Démontrons que  $\text{Aut}(G)$  est un sous-groupe du groupe symétrique  $S_G$ .

♦  $\text{Aut}(G)$  n'est pas vide puisque  $\text{id}_G \in \text{Aut}(G)$ .

♦ Soit  $f \in \text{Aut}(G)$ . Il faut démontrer que la bijection réciproque  $f^{-1}$  est dans  $\text{Aut}(G)$ ; c'est déjà une bijection, il suffit de démontrer que c'est un morphisme de groupes.

Soit  $(g, g') \in G^2$  et soit  $(h, h') \in G^2$  tel que  $f(h) = g$  et  $f(h') = g'$ . Alors  $f^{-1}(g)f^{-1}(g') = hh'$ . Or  $f(hh') = f(h)f(h') = gg'$  donc, puisque  $f$  est une bijection,  $hh' = f^{-1}(gg')$ . Ainsi,  $f^{-1}$  est bien un morphisme de groupes.

♦ On a déjà vérifié que si  $f$  et  $g$  sont dans  $\text{Aut}(G)$  alors  $f \circ g \in \text{Aut}(G)$ ; de plus,  $f \circ g$  est une bijection donc  $f \circ g \in \text{Aut}(G)$ . ✓

**Exemple.** Le déterminant,  $\det: \text{GL}_n(\mathbb{C}) \rightarrow \mathbb{C}^*$ , est un morphisme de groupes.

**Définition 1.3.** Un **sous-groupe** d'un groupe  $G$  est une partie non vide  $H$  de  $G$  telle que  $H$  est un groupe pour la loi induite par celle de  $G$ .

Un sous-groupe  $H$  de  $G$  est dit **propre** s'il vérifie  $\{1\} \subsetneq H \subsetneq G$ .

**Proposition 1.4.** Soit  $H$  une partie d'un groupe  $G$ . Alors les assertions suivantes sont équivalentes :

- (1)  $H$  est un sous-groupe de  $G$ .
- (2)  $H$  n'est pas vide et pour tout  $(x, y) \in H^2$  on a  $x^{-1} \in H$  et  $xy \in H$ .
- (3)  $H$  n'est pas vide et pour tout  $(x, y) \in H^2$ , on a  $x^{-1}y \in H$ .
- (4)  $H$  n'est pas vide et pour tout  $(x, y) \in H^2$ , on a  $xy^{-1} \in H$ .

*Démonstration.* Le fait que  $H$  n'est pas vide est contenu dans tous les points (1)–(4).

➤ (1)⇒(2). Par hypothèse, la restriction de la loi de groupe  $G \times G \rightarrow G$  induit une loi de groupe  $H \times H \rightarrow H$ . On en déduit que si  $(x, y) \in H^2$  alors  $xy \in H$ , que  $H$  possède un élément neutre  $1_H$  et que tout  $x \in H$  admet un inverse dans  $H$ , noté  $\bar{x}$ .

Soit  $x \in H$ . Alors  $1 = xx^{-1} = x1_Hx^{-1} = x\bar{x}xx^{-1} = 1_H1 = 1_H$  donc  $1 \in H$  et c'est l'élément neutre de  $H$ .

Enfin,  $\bar{x}$  est un inverse de  $x$  dans  $G$  puisque  $x\bar{x} = \bar{x}x = 1_H = 1$  donc, par unicité de l'inverse d'un élément (dans  $G$ ), on a  $x^{-1} = \bar{x} \in H$ .

➤ (2)⇒(3). Soit  $(x, y) \in H^2$ . On sait que  $x^{-1} \in H$  puis, comme  $H$  est stable par produit et  $(x^{-1}, y) \in H^2$ , on a  $x^{-1}y \in H$ .

- (3)⇒(4). Soit  $(x, y) \in H^2$ . Alors  $1 = x^{-1}x \in H$  donc  $(x, 1) \in H^2$  donc  $x^{-1} = x^{-1}1 \in H$  par hypothèse, et de même  $y^{-1} \in H$ . On applique à nouveau l'hypothèse à  $(x^{-1}, y^{-1}) \in H^2$  et on obtient  $xy^{-1} = (x^{-1})^{-1}y^{-1} \in H$ .
- (4)⇒(1). Puisque  $H$  n'est pas vide, on peut prendre  $x \in H$ . Alors  $(x, x) \in H^2$  donc  $1 = xx^{-1} \in H$ . De plus, pour tout  $x \in H$  on a  $x \in G$  donc  $1x = x = x1$ . On en déduit que  $H$  possède un élément neutre.
- Soit  $x \in H$ . Alors  $(1, x) \in H^2$  et on en déduit que  $x^{-1} = 1x^{-1} \in H$ , c'est-à-dire que l'inverse de  $x$  dans  $G$  est en fait dans  $H$ . Puisque  $xx^{-1} = 1 = x^{-1}x$  (dans  $G$ ), on en déduit que  $x$  possède un inverse dans  $H$ .
- Soit maintenant  $(x, y) \in H^2$ . D'après ce qui précède,  $(x, y^{-1}) \in H^2$  donc  $xy = x(y^{-1})^{-1} \in H$ .
- La restriction de la loi de  $G$  à  $H \times H$  induit donc une loi sur  $H$ . Cette loi est associative comme celle de  $G$ .
- Donc  $H$  est un groupe pour la loi induite par  $G$ . ✓

**Exemples.** (1) On a la suite de sous-groupes :  $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$ .

(2) Soit  $n \in \mathbb{Z}$ . Alors  $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$  est un sous-groupe de  $\mathbb{Z}$ .

On connaît en fait tous les sous-groupes de  $\mathbb{Z}$ .

**Proposition 1.5.** Soit  $H$  un sous-groupe de  $\mathbb{Z}$ . Alors il existe un unique  $n \in \mathbb{N}$  tel que  $H = n\mathbb{Z}$ .

*Démonstration.* Si  $H = \{0\}$ , le résultat est clair (on prend  $n = 0$ ).

Supposons donc que  $H \neq \{0\}$ . Alors  $H$  contient un élément non nul, et quitte à le remplacer par son opposé, on peut le supposer strictement positif ( $H$  est un sous-groupe de  $\mathbb{Z}$ , donc si  $a \in H$ , alors  $-a \in H$ ). Soit alors  $n = \min\{a \in H \mid a > 0\} \in \mathbb{N}^*$ . Montrons que  $H = n\mathbb{Z}$ .

Puisque  $n \in H$ , on a évidemment  $n\mathbb{Z} \subset H$  (récurrence et stabilité de  $H$  par passage à l'opposé).

Démontrons que  $H \subset n\mathbb{Z}$ . Soit  $a \in H$ . On effectue la division euclidienne de  $a$  par  $n$  : il existe  $(q, r) \in \mathbb{Z} \times \mathbb{N}$  tels que  $a = nq + r$  avec  $0 \leq r < n$ . Comme  $n \in H$ , on a  $nq \in H$  donc  $r = a - nq \in H$ . Par minimalité de  $n$ , on en déduit que  $r = 0$ . Donc  $a \in n\mathbb{Z}$  et finalement  $H = n\mathbb{Z}$ .

Enfin, vérifions l'unicité du nombre entier  $n \in \mathbb{N}$  tel que  $H = n\mathbb{Z}$ . C'est clair si  $H = \{0\}$ . Si  $(n, m) \in (\mathbb{N}^*)^2$  sont tels que  $n\mathbb{Z} = H = m\mathbb{Z}$ , alors  $n \mid m$  et  $m \mid n$  (dans  $\mathbb{N}^*$ ), ce qui donne  $m = n$  et l'unicité de  $n$ . ✓

La preuve du résultat suivant est laissée en exercice.

**Proposition 1.6.** Soit  $f: G \longrightarrow G'$  un morphisme de groupes.

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

*Démonstration.* Exercice.

(1) Le sous-groupe  $H$  n'est pas vide donc  $f(H)$  n'est pas vide.

Soit  $(k, k') \in f(H)^2$ . Il existe  $(h, h') \in H^2$  tel que  $k = f(h)$  et  $k' = f(h')$ . Alors  $k(k')^{-1} = f(h)f(h')^{-1} = f(h(h')^{-1}) \in f(H)$  car  $h(h')^{-1} \in H$ .

Donc  $f(H)$  est un sous-groupe de  $G'$ .

Enfin,  $\text{Im } f = f(G)$  est donc un sous-groupe de  $G'$  puisque  $G$  est un sous-groupe de  $G$ .

(2) On a  $f(1_G) = 1_{G'} \in H'$  donc  $1_G \in f^{-1}(H')$ .

Soit  $(u, v) \in (f^{-1}(H'))^2$ . Alors  $f(u) \in H'$  et  $f(v) \in H'$  donc  $f(u)f(v)^{-1} \in H'$  et donc  $f(uv^{-1}) \in H'$  car  $f$  est un morphisme de groupes. On en déduit que  $uv^{-1} \in f^{-1}(H')$ .

Donc  $f^{-1}(H')$  est un sous-groupe de  $G$ . C'est le cas en particulier de  $\text{Ker } f = f^{-1}(\{1_{G'}\})$  puisque  $\{1_{G'}\}$  est un sous-groupe de  $G'$ . ✓

## II. CLASSES MODULO UN SOUS-GROUPE

Soit  $G$  un groupe et soit  $H$  un sous-groupe de  $G$ . On définit une relation sur  $G$  :

$$x\mathcal{R}y \iff x^{-1}y \in H.$$

C'est une relation d'équivalence (exercice).

En effet :

- soit  $x \in G$ . Alors  $x^{-1}x = 1 \in H$  (car  $H$  est un sous-groupe de  $G$ ) donc  $x\mathcal{R}x$ . Donc  $\mathcal{R}$  est réflexive.
- soit  $(x, y) \in G^2$  tel que  $x\mathcal{R}y$ , c'est-à-dire  $x^{-1}y \in H$ . Alors, puisque  $H$  est un sous-groupe de  $G$ ,  $y^{-1}x = (x^{-1}y)^{-1} \in H$  et donc  $y\mathcal{R}x$ . Donc  $\mathcal{R}$  est symétrique.
- soit  $(x, y, z) \in G^3$  tel que  $x\mathcal{R}y$  et  $y\mathcal{R}z$ , c'est-à-dire  $x^{-1}y \in H$  et  $y^{-1}z \in H$ . Puisque  $H$  est un sous-groupe de  $G$ , il est stable par produit donc  $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$  et donc  $x\mathcal{R}z$ . Ainsi,  $\mathcal{R}$  est transitive.

La classe d'équivalence d'un élément  $x$  pour la relation d'équivalence  $\mathcal{R}$  est l'ensemble  $xH = \{xh \mid h \in H\}$  (exercice), qui est appelée **classe à gauche modulo  $H$  de  $x$** .

Vérifions que  $xH$  est bien la classe d'équivalence de  $x$ . Si  $h \in H$ , alors  $xh\mathcal{R}x$  car  $x^{-1} \cdot xh = h \in H$ , donc  $xH$  est contenu dans la classe d'équivalence de  $x$ . Réciproquement, soit  $y \in G$  tel que  $y\mathcal{R}x$ . Posons  $h = x^{-1}y \in H$ . Alors  $y = xh \in xH$ .

**L'ensemble des classes à gauche modulo  $H$  est noté  $G/H$ .**

**Remarque.** Deux classes à gauche modulo  $H$  ont le même cardinal, qui est le nombre d'éléments  $|H|$  de  $H$  lorsque  $H$  est fini. En effet, pour tout  $x \in G$  l'application  $H \rightarrow xH$  définie par  $h \mapsto xh$  est une bijection, de bijection réciproque  $xH \rightarrow H$  définie par  $y \mapsto x^{-1}y$ .

**Définition 1.7.** (1) Soit  $G$  un groupe fini. L'**ordre** de  $G$ , noté  $|G|$ , est le cardinal de  $G$ .

(Remarque : on notera aussi  $|X|$  le cardinal d'un ensemble fini  $X$  dans ce cours.)

(2) Soit  $H$  un sous-groupe de  $G$ . Si  $G/H$  est fini, l'**indice** de  $H$  dans  $G$ , noté  $[G : H]$ , est le cardinal de l'ensemble  $G/H$ .

Le résultat suivant est fondamental.

**Théorème 1.8** (Théorème de Lagrange). Soit  $G$  un groupe fini et soit  $H$  un sous-groupe de  $G$ . On a

$$|G| = [G : H] |H|.$$

En particulier, l'ordre d'un sous-groupe divise l'ordre du groupe.

**Démonstration.** Soit  $(x_i)_{i \in I}$  une famille de représentants distincts des classes à gauche modulo  $H$ . On a  $G = \cup_{i \in I} x_i H$  et  $x_i H \cap x_j H = \emptyset$  si  $i \neq j$ . Alors  $\text{card}(I) = [G : H]$  et comme  $|x_i H| = |H|$  pour tout  $i \in I$ , on trouve bien que  $|G| = \text{card}(I)|H| = [G : H]|H|$ . ✓

Soit  $G$  un groupe et soit  $H$  un sous-groupe de  $G$ . Peut-on munir l'ensemble  $G/H$  d'une structure de groupe induite par celle de  $G$ ? La notion de sous-groupe normal permet de répondre précisément à cette question.

Pour  $x \in G$ , on note  $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$  et  $Hx = \{hx \mid h \in H\}$ .

**Définition 1.9.** Un sous-groupe  $H \subset G$  est dit **normal** dans  $G$  (ou **distingué** dans  $G$ ) si pour tout  $x \in G$ , on a  $xHx^{-1} = H$ . On note  $H \triangleleft G$  lorsque  $H$  est normal dans  $G$ .

**Remarques.** (1) Pour montrer qu'un sous-groupe  $H$  est normal dans  $G$ , il suffit de montrer que  $xHx^{-1} \subset H$  pour tout  $x \in G$ .

En effet, supposons que pour tout  $x \in G$  on a  $xHx^{-1} \subset H$ . On doit démontrer que pour tout  $y \in G$ , on a  $H \subset yHy^{-1}$ . Soit donc  $y \in G$ . Pour tout  $h \in H$ , on a  $k = y^{-1}hy \in y^{-1}Hy \subset H$ . On en déduit que  $h = yky^{-1} \in yHy^{-1}$  et donc que  $H \subset yHy^{-1}$ .

(2)  $H \triangleleft G \iff \forall x \in G, Hx = xH$ .

( $\Rightarrow$ ) Supposons que  $H$  est normal dans  $G$ . Fixons  $x \in G$ . Soit  $y \in xH$ , alors il existe  $h \in H$  tel que  $y = xh$ . Par hypothèse on a  $xhx^{-1} \in xHx^{-1} = H$  donc  $y = xh = xhx^{-1} \cdot x \in Hx$  et on a  $xH \subset Hx$ . L'autre inclusion se démontre de même.

( $\Leftarrow$ ) Supposons que pour tout  $x \in G$  on a  $xH = Hx$ . Soit  $x \in G$ . Soit  $y \in xHx^{-1}$ . Il existe  $h \in H$  tel que  $y = xhx^{-1}$ . Or  $xh \in xH = Hx$  donc il existe  $k \in H$  tel que  $xh = kx$  et on en déduit que  $y = xhx^{-1} = kxx^{-1} = k \in H$  et donc que  $xHx^{-1} \subset H$ . On conclut en utilisant la remarque (1).

**Exemples.** (1) On a toujours  $\{1_G\} \triangleleft G$  et  $G \triangleleft G$ .

(2) Dans un groupe abélien, tous les sous-groupes sont normaux.

(3) Soit  $G$  un groupe et soit  $Z(G) = \{x \in G \mid \forall y \in G, yx = xy\}$ . Alors  $Z(G)$  est un sous-groupe normal (et abélien) de  $G$ , appelé le **centre** de  $G$ .

Les résultats suivants sont souvent utiles. Les preuves sont laissées en exercice.

**Proposition 1.10.** Soit  $G$  un groupe et soient  $H$  un sous-groupe de  $G$  et  $K$  un sous-groupe de  $H$ .

(a) Si  $K \triangleleft G$  alors  $K \triangleleft H$  (mais  $H$  peut ne pas être normal dans  $G$ ).

(b) On peut avoir  $K \triangleleft H$  et  $H \triangleleft G$  sans que  $K$  ne soit normal dans  $G$ .

*Démonstration.* Exercice.

(a) Soit  $k \in K$  et soit  $h \in H$ . Alors  $h \in G$  donc par hypothèse  $hkh^{-1} \in K$ . On en déduit que  $K \triangleleft H$ .

On a bien sûr des exemples triviaux où  $K \triangleleft G$  mais  $H$  n'est pas normal dans  $G$ , par exemple  $G = S_4$ ,  $K = \{\text{id}\} \triangleleft S_4$ ,  $H = \{\text{id}; (1\ 2)\}$ .

Autre exemple :  $G = S_4$ ,  $K = V_4 = \{\text{id}; (1\ 2)(3\ 4); (1\ 3)(2\ 4); (1\ 4)(2\ 3)\}$  et  $H = V_4 \cup \{(1\ 2); (3\ 4); (1\ 4\ 2\ 3); (1\ 3\ 2\ 4)\}$ . Alors  $V_4 \triangleleft S_4$ , car si  $\sigma = (i\ j)(k\ \ell) \in V_4$  et  $\tau \in S_4$  alors  $\tau\sigma\tau^{-1} = \tau(i\ j)\tau^{-1}\tau(k\ \ell)\tau^{-1} = (\tau(i)\ \tau(j))(\tau(k)\ \tau(\ell)) \in V_4$  (voir le lemme 5.2).

(Remarque : si on le vérifie sans le lemme 5.2, on peut se contenter de prendre les transpositions pour  $\tau$  car elles engendrent  $S_4$ .) Il faut vérifier que  $H$  est un sous-groupe de  $G$  (on peut le vérifier directement ou par exemple anticiper et remarquer que  $H = V_4L$  avec  $L = \{\text{id}; (1\ 2)\}$  et  $V_4 \triangleleft S_4$  et utiliser la proposition 1.33). Enfin,  $H$  n'est pas normal dans  $S_4$  car  $(1\ 2) \in H$  mais  $(1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3) \notin H$ .

- (b) On considère, dans  $S_4$ , les sous-groupes  $G = A_4$  (groupe alterné),  $H = V_4$  et le sous-groupe  $K = \{\text{id}; (1\ 2)(3\ 4)\}$ . On a vu ci-dessus que  $V_4$  est normal dans  $S_4$  donc dans  $A_4$ . De plus,  $V_4$  est abélien donc  $K$  est normal dans  $V_4$ . Cependant,  $K$  n'est pas normal dans  $A_4$  car  $(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} = (1\ 4)(2\ 3) \notin K$ . ✓

**Proposition 1.11.** Soient  $G$  un groupe et  $H \subset G$  un sous-groupe tel que  $[G : H] = 2$ . Alors  $H \triangleleft G$ .

*Démonstration.* Voir travaux dirigés

Soit  $H$  un sous-groupe d'indice 2 dans  $G$ . Il y a donc deux classes à gauche modulo  $H$  dans  $G$  qui forment une partition de  $G$ ; l'une d'elles est  $H$ , notons l'autre  $gH$  pour un  $g \in G \setminus H$ . On doit démontrer que pour tout  $x \in G$  on a  $xHx^{-1} \subset H$ . Démontrons-le d'abord pour  $x = g$ .

Soit  $y \in gHg^{-1}$ . Posons  $y = ghg^{-1}$  avec  $h \in H$ . On sait que  $y \in H$  ou  $y \in gH$ . Si  $y \in gH$ , alors  $g^{-1}y \in H$  donc  $hg^{-1} = g^{-1}ghg^{-1} = g^{-1}y \in H$ , par conséquent  $g^{-1} \in H$  et enfin  $g \in H$  : on a obtenu une contradiction. Donc  $y \in H$  et par suite  $gHg^{-1} \subset H$ .

Soit maintenant  $x \in G$  quelconque. Si  $x \in H$ , il est clair que  $xHx^{-1} \subset H$ . Supposons donc que  $x \in gH$  et posons  $x = gh$  pour un  $h \in H$ . Soit  $y \in xHx^{-1}$ , il existe  $k \in H$  tel que  $y = xkx^{-1}$ . On en déduit que  $y = ghkh^{-1}g^{-1} \in gHg^{-1} \subset H$ . Finalement on a bien  $xHx^{-1} \subset H$ .

On a donc démontré que  $H$  est normal dans  $G$ . ✓

**Proposition 1.12.** Soit  $f: G \longrightarrow G'$  un morphisme de groupes.

(1) Soit  $H' \triangleleft G'$ . Alors  $f^{-1}(H') \triangleleft G$ . En particulier  $\text{Ker } f \triangleleft G$ .

(2) Soit  $H \triangleleft G$ . Alors  $f(H) \triangleleft f(G) = \text{Im } f$ .

*Démonstration.* Exercice.

(1) Soit  $(h, g) \in f^{-1}(H') \times G$ . Alors  $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H'$  car  $f(h) \in H'$  et  $H' \triangleleft G'$ , donc  $ghg^{-1} \in f^{-1}(H')$ . Donc  $f^{-1}(H')$  est normal dans  $G$ .

(2) Soit  $(g', h') \in f(G) \times f(H)$ . Il existe donc  $(g, h) \in G \times H$  tel que  $g' = f(g)$  et  $h' = f(h)$ . On a alors  $g'h'(g')^{-1} = f(g)f(h)f(g)^{-1} = f(ghg^{-1})$ . Or  $H \triangleleft G$  donc  $ghg^{-1} \in H$  et donc  $g'h'(g')^{-1} \in f(H)$ . Donc  $f(H)$  est normal dans  $f(G)$ . ✓

**Exercice.** Soit  $\text{SL}_n(\mathbb{C}) = \{M \in \text{GL}_n(\mathbb{C}) \mid \det M = 1\}$ . Montrer que  $\text{SL}_n(\mathbb{C}) \triangleleft \text{GL}_n(\mathbb{C})$ .

**Correction.** Le groupe  $\text{SL}_n(\mathbb{C})$  est le noyau du morphisme de groupes  $\det: \text{GL}_n(\mathbb{C}) \rightarrow \mathbb{C}^*$ . Il est donc normal dans  $\text{GL}_n(\mathbb{C})$ . ✓

On répond maintenant à la question initiale.

**Théorème 1.13.** Soient  $G$  un groupe et  $H \triangleleft G$ . Soit  $\pi: G \longrightarrow G/H$  la surjection canonique qui associe à un élément  $x$  de  $G$  sa classe à gauche  $xH$  modulo  $H$ . Il existe sur  $G/H$  une unique structure de groupe telle que  $\pi$  soit un morphisme de groupes.

*Démonstration.* Soit  $x \in G$ , par définition  $\pi(x) = xH$ . Puisque  $\pi$  doit être un morphisme de groupes, la seule structure possible est  $xH.yH = \pi(x)\pi(y) = \pi(xy) = xyH$ . On vérifie que cette loi est bien définie (si  $xH = x'H$  et  $yH = y'H$ , alors  $xyH = x'y'H$ ) et qu'elle fait de  $G/H$  un groupe (exercice).

➤ Soit  $(x, x', y, y') \in G^4$  tel que  $xH = x'H$  et  $yH = y'H$ . Alors  $x^{-1}x' \in H$  et  $y^{-1}y' \in H$ . Posons  $h = x^{-1}x'$  et  $k = y^{-1}y'$ . On a donc  $x' = xh$  et  $y' = yk$  donc  $(xy)^{-1}(x'y') = y^{-1}x^{-1}x'hyk = y^{-1}hyk$ . Or  $H$  est normal dans  $G$ , donc  $y^{-1}hy \in H$  et donc  $y^{-1}hyk \in H$ . On en déduit donc que les classes de  $xy$  et de  $x'y'$  sont les mêmes, c'est-à-dire  $xyH = x'y'H$ . Donc la loi est bien définie.

- La loi est associative :  $(xH.yH).zH = xyH.zH = (xy)zH = x(yz)H = xH.(yH.zH)$  pour tout  $(x, y, z) \in G^3$  puisque la loi de  $G$  est associative.
- Il y a un élément neutre pour la loi, qui est  $H = \pi(1)$ ; en effet,  $xH.H = (x1)H = xH = (1x)H = H.xH$  pour tout  $x \in G$ .
- Tout élément  $xH \in G/H$  avec  $x \in G$  possède un inverse dans  $G/H$ , qui est  $x^{-1}H$ .

Donc  $G/H$  est bien un groupe pour cette loi. De plus, il est clair que  $\pi$  est alors un morphisme de groupes (la loi a été construite pour cela). ✓

**Remarque.** Lorsque  $G/H$  est un groupe, la classe (à gauche) modulo  $H$  de  $x$  est souvent notée  $\bar{x}$ .

**Exemple.** Soit  $n \in \mathbb{N}^*$ . L'ensemble des classes (à gauche) modulo  $n$  dans  $\mathbb{Z}$  est  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$ . C'est un groupe d'ordre  $n$  et la loi du groupe est définie par  $\bar{k} + \bar{l} = \overline{k+l}$ , pour tout  $(k, l) \in \mathbb{Z}^2$ .

**Remarque.** Dans le théorème précédent, on a  $H = \text{Ker } \pi$ .

Il découle donc des deux derniers résultats qu'un sous-groupe  $H$  d'un groupe  $G$  est normal dans  $G$  si, et seulement si, il existe un morphisme de groupes  $f: G \rightarrow G'$  tel que  $H = \text{Ker } f$ .

**Théorème 1.14.** Soit  $f: G \rightarrow G'$  un morphisme de groupes.

- (Théorème de factorisation)** Soit  $H \triangleleft G$  tel que  $H \subset \text{Ker } f$ . Alors il existe un unique morphisme de groupes  $\bar{f}: G/H \rightarrow G'$  tel que  $\bar{f} \circ \pi = f$  (où  $\pi: G \rightarrow G/H$  est la surjection canonique).

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ & \searrow \pi \quad \nearrow \bar{f} & \\ & G/H & \end{array}$$

- (Premier théorème d'isomorphisme)** Le morphisme  $f$  induit un isomorphisme

$$\bar{f}: G / \text{Ker } f \rightarrow \text{Im } f.$$

**Démonstration.** (1) Soit  $y \in G/H$ . Puisque  $\pi$  est surjectif il existe  $x \in G$  tel que  $y = \pi(x)$ . Par hypothèse, on doit avoir  $\bar{f}(y) = \bar{f}(\pi(x)) = f(x)$ . Nous devons donc poser  $\bar{f}(y) = f(x)$  pour un  $x \in G$  tel que  $\pi(x) = y$ . On en déduit en particulier que si  $\bar{f}$  existe, il est unique. Cependant, la définition de  $\bar{f}$  semble dépendre du choix de  $x$ . Vérifions que ce n'est pas le cas. Soit  $x' \in G$  tel que  $\pi(x') = y$ . Alors  $\pi(x) = \pi(x')$  donc  $x^{-1}x' \in \text{Ker } \pi = H \subset \text{Ker } f$ , donc  $1 = f(x^{-1}x') = f(x)^{-1}f(x')$  et donc  $f(x) = f(x')$ . On a vérifié que  $\bar{f}$  est bien définie.

Vérifions que  $\bar{f}$  est un morphisme de groupes. Pour  $(x, x') \in G^2$  on a  $\bar{f}(\pi(x)\pi(x')) = \bar{f}(\pi(xx')) = f(xx') = f(x)f(x') = \bar{f}(\pi(x))\bar{f}(\pi(x'))$  donc  $\bar{f}$  est bien un morphisme de groupes.

- On applique (1) à  $H = \text{Ker } f$ . On obtient donc un morphisme  $\bar{f}: G / \text{Ker } f \rightarrow G'$ , qui est par construction à valeurs dans  $\text{Im } f$ ; de plus, pour tout  $y \in \text{Im } f$ , il existe  $x \in G$  tel que  $y = f(x) = \bar{f}(\pi(x))$  donc  $\bar{f}: G / \text{Ker } f \rightarrow \text{Im } f$  est surjective. Déterminons maintenant  $\text{Ker } \bar{f}$ . Soit  $y \in \text{Ker } \bar{f}$ , il existe  $x \in G$  tel que  $y = \pi(x)$  et on a  $1 = \bar{f}(y) = \bar{f}(\pi(x)) = f(x)$  donc  $x \in \text{Ker } f = H = \text{Ker } \pi$  et donc  $y = \pi(x) = 1$ . On a donc  $\text{Ker } \bar{f} = \{1\}$  et donc  $\bar{f}$  est injective et par conséquent c'est un isomorphisme. ✓

**Exercice.** Montrer que  $\text{GL}_n(\mathbb{C}) / \text{SL}_n(\mathbb{C}) \cong \mathbb{C}^*$ .

*Correction.* On considère le morphisme de groupes  $\det: \mathrm{GL}_n(\mathbb{C}) \rightarrow \mathbb{C}^*$ . Il est surjectif (par exemple, tout élément  $x \in \mathbb{C}^*$  est l'image de  $\begin{pmatrix} x & 0 \\ 0 & I_{n-1} \end{pmatrix}$ ). Son noyau est  $\mathrm{SL}_n(\mathbb{C})$ . On en déduit donc grâce au premier théorème d'isomorphisme que  $\det$  induit un isomorphisme  $\mathrm{GL}_n(\mathbb{C}) / \mathrm{SL}_n(\mathbb{C}) \cong \mathbb{C}^*$ . ✓

### Théorème 1.15. (Théorème de correspondance)

Soit  $G$  un groupe et soit  $H$  un sous-groupe normal de  $G$ . Alors la surjection canonique  $\pi: G \rightarrow G/H$  induit une correspondance bijective entre les sous-groupes de  $G$  contenant  $H$  (resp. les sous-groupes normaux de  $G$  contenant  $H$ ) et les sous-groupes de  $G/H$  (resp. les sous-groupes normaux de  $G/H$ ).

*Démonstration.* Soit  $K$  un sous-groupe de  $G$  avec  $H \subset K$ . Alors  $\pi(K) = K/H$  est un sous-groupe de  $G/H$ . Soit  $K^*$  un sous groupe de  $G/H$  : alors  $\pi^{-1}(K^*)$  est un sous-groupe de  $G$  qui contient  $H$  car  $H = \pi^{-1}(\{1_{G/H}\})$ .

De plus, si  $K \triangleleft G$ , alors  $\pi(K) \triangleleft \pi(G) = G/H$ , et si  $K^* \triangleleft G/H$  alors  $\pi^{-1}(K^*) \triangleleft G$ .

Nous avons donc construit deux applications :

$$\begin{array}{ccc} \{\text{sous-groupes (normaux) de } G \text{ contenant } H\} & \xrightleftharpoons[\Psi]{\Phi} & \{\text{sous-groupes (normaux) de } G/H\} \\ K & \longmapsto & \pi(K) = K/H \\ \pi^{-1}(K^*) & \longleftarrow & K^* \end{array}$$

Vérifions que ce sont des bijections réciproques.

On a  $K \subset \pi^{-1}(\pi(K)) = \Phi(\Psi(K))$ . De plus, soit  $x \in \pi^{-1}(\pi(K))$ . Alors il existe  $y \in K$  tel que  $\pi(x) = \pi(y)$ , donc  $x \in yH$ . Comme  $H \subset K$ , on a  $x \in K$  et ainsi  $K = \pi^{-1}(\pi(K))$ . Donc  $\Phi \circ \Psi = \mathrm{id}$ .

L'égalité  $K^* = \pi(\pi^{-1}(K^*))$  provient de la surjectivité de  $\pi$  (c'est purement ensembliste). On a donc  $\Psi \circ \Phi = \mathrm{id}$ .

On a bien les correspondances bijectives annoncées. ✓

**Définition 1.16.** Un groupe non trivial  $G$  est dit **simple** si ses seuls sous-groupes normaux sont  $\{1\}$  et  $G$ .

Cette notion est importante pour la raison suivante. Supposons que l'on essaie de classer les groupes finis par récurrence sur leur ordre. Si un groupe fini  $G$  n'est pas simple, il contient un sous-groupe normal  $H$  tel que  $1 < |H| < |G|$ , et on a aussi  $1 < |G/H| < |G|$ . Alors, par hypothèse de récurrence, on connaît les groupes  $H$  et  $G/H$ , et on peut espérer reconstruire  $G$  à partir de ces groupes (même si c'est souvent difficile en pratique).

Les groupes simples sont les groupes auxquels on ne peut pas appliquer cette méthode, et pour cette raison on les considère comme les « briques élémentaires » à partir desquelles on construit les autres groupes.

## IV. PARTIES GÉNÉRATRICES, GROUPES CYCLIQUES

La preuve du résultat suivant est laissée en exercice.

**Proposition 1.17.** Soit  $G$  un groupe. Une intersection de sous-groupes de  $G$  (resp. de sous-groupes normaux de  $G$ ) est un sous-groupe de  $G$  (resp. un sous-groupe normal de  $G$ ).

*Démonstration.* Exercice.

Soit  $(H_i)_{i \in I}$  une famille quelconque de sous-groupes de  $G$ . Posons  $H = \bigcap_{i \in I} H_i$ .

Puisque  $H_i$  est un sous-groupe de  $G$  pour tout  $i \in I$ , on a  $1 \in H_i$  pour tout  $i$  donc  $1 \in H$ .

Soit  $(x, y) \in H^2$ . Alors, pour tout  $i \in I$ , on a  $(x, y) \in H_i$ . Puisque  $H_i$  est un sous-groupe de  $G$ ,  $x^{-1}y \in H_i$  pour tout  $i \in I$ . Donc  $x^{-1}y \in H$  et  $H$  est bien un sous-groupe de  $G$ .

Supposons de plus que  $H_i \triangleleft G$  pour tout  $i \in I$ . Soit  $(g, h) \in G \times H$ . Alors  $h \in H_i$  pour tout  $i \in I$  donc  $ghg^{-1} \in H_i$  pour tout  $i \in I$  et donc  $ghg^{-1} \in H$ . Donc  $H$  est normal dans  $G$ . ✓

Ce résultat permet d'introduire la définition suivante.

**Définition 1.18.** Soit  $G$  un groupe et soit  $S$  une partie de  $G$ . On note  $\langle S \rangle$  l'intersection de tous les sous-groupes de  $G$  contenant  $S$ . C'est un sous-groupe de  $G$  appelé **sous-groupe de  $G$  engendré par  $S$** .

Si  $G = \langle S \rangle$ , on dit que  $G$  est engendré par  $S$ .

La terminologie utilisée dans cette définition est justifiée par le résultat suivant, dont la preuve est laissée en exercice.

**Proposition 1.19.** Le sous-groupe  $\langle S \rangle$  est le plus petit sous-groupe de  $G$  qui contient  $S$  (au sens où tout sous-groupe de  $G$  qui contient  $S$  contient  $\langle S \rangle$ ), et

$$\langle S \rangle = \{x_1 \cdots x_n \mid x_i \in S \text{ ou } x_i^{-1} \in S\}.$$

*Démonstration.* Exercice.

➤ Soit  $\{H_i \mid i \in I\}$  l'ensemble des sous-groupes de  $G$  contenant  $S$ . Alors  $\langle S \rangle = \bigcap_{i \in I} H_i$  par définition.

Soit  $H$  un sous-groupe de  $G$  contenant  $S$ . Alors  $H$  est l'un des  $H_i$  donc  $\langle S \rangle \subset H$ . Par conséquent,  $\langle S \rangle$  est bien le plus petit sous-groupe de  $G$  contenant  $S$ .

➤ Notons  $H = \{x_1 \cdots x_n \mid x_i \in S \text{ ou } x_i^{-1} \in S\}$ . C'est une partie de  $G$  qui contient  $S$  et qui en particulier n'est pas vide. Vérifions que c'est un sous-groupe de  $G$ . Soit  $(u, u') \in H^2$ . Alors on peut écrire  $u = x_1 \cdots x_n$  et  $u' = x'_1 \cdots x'_m$  avec, pour tout  $(i, j)$ ,  $x_i \in S$  ou  $x_i^{-1} \in S$  et  $x'_j \in S$  ou  $(x'_j)^{-1} \in S$ . On en déduit que  $u^{-1}u' = x_n^{-1} \cdots x_1^{-1} x'_1 \cdots x'_m \in H$  car chaque facteur ou son inverse est dans  $S$ . Donc  $H$  est un sous-groupe de  $G$ , qui contient  $S$  et d'après la première partie de la démonstration on en déduit que  $\langle S \rangle \subset H$ .

Soit maintenant  $u \in H$  et posons  $u = x_1 \cdots x_n$  avec, pour tout  $i$ ,  $x_i \in S$  ou  $x_i^{-1} \in S$ . On rappelle que  $\langle S \rangle$  est un sous-groupe de  $G$  contenant  $S$ . En particulier, pour tout  $i$  on a  $x_i \in \langle S \rangle$  (si  $x_i \in S$  c'est immédiat et si  $x_i^{-1} \in S$  alors  $x_i^{-1} \in \langle S \rangle$  donc  $x_i = (x_i^{-1})^{-1} \in \langle S \rangle$ ). On en déduit donc que  $u \in \langle S \rangle$  et donc que  $\langle S \rangle = H$ . ✓

**Exemples.** (1) Soit  $n \in \mathbb{N}^*$ . Le groupe multiplicatif  $\mu_n$  des racines  $n^{\text{ièmes}}$  de l'unité (complexes) est engendré par  $\{\omega\}$ , où  $\omega = e^{\frac{2i\pi}{n}}$ , puisque  $\mu_n = \{\omega^k \mid k \in \mathbb{Z}\}$ .

(2) On rappelle que le **groupe diédral**  $\mathcal{D}_n$  est le groupe des isométries du plan affine euclidien qui conservent un polygone régulier à  $n$  sommets. On a

$$\mathcal{D}_n = \{r^k s^\ell \mid 0 \leq k \leq n-1, 0 \leq \ell \leq 1\}$$

où  $r$  est la rotation d'angle  $\frac{2\pi}{n}$  et de centre  $O$ , l'isobarycentre des sommets du polygone, et  $s$  est la symétrie orthogonale par rapport à une droite passant par un sommet et par  $O$ . On a les relations suivantes :  $r^n = 1$ ,  $s^2 = 1$  et  $sr^k = r^{n-k}s$ .

La description des éléments de  $\mathcal{D}_n$  montre que le groupe diédral  $\mathcal{D}_n$  est engendré par  $\{r, s\}$ .

En effet, il est clair que  $\mathcal{D}_n \subset \langle \{r, s\} \rangle$ . De plus, tout élément de  $\langle \{r, s\} \rangle$  peut s'écrire sous la forme  $r^u s^v$  grâce à la relation  $sr^k = r^{n-k}s$ . On effectue les divisions euclidiennes de  $u$

par  $n$  et de  $v$  par 2, qui s'écrivent  $u = qn + k$  et  $v = 2t + \ell$  avec  $0 \leq k \leq n - 1$  et  $0 \leq \ell \leq 1$ . On en déduit que  $r^u s^v = (r^n)^q r^k (s^2)^t s^\ell = r^k s^\ell \in \mathcal{D}_n$ .

De plus,  $\mathcal{D}_n$  est d'ordre  $2n$ . En effet, l'écriture d'un élément de  $\mathcal{D}_n$  sous la forme  $r^k s^\ell$  avec  $0 \leq k < n$  et  $0 \leq \ell \leq 1$  est unique donc ces éléments sont deux à deux distincts. Supposons le contraire, il existe alors  $k' \in \llbracket 0; n - 1 \rrbracket$  et  $\ell' \in \{0, 1\}$  tels que  $r^k s^\ell = r^{k'} s^{\ell'}$ . Si  $\ell \neq \ell'$ , on peut supposer par exemple que  $\ell = 0$  et  $\ell' = 1$  et on a alors  $r^{k-k'} = s$ ; mais  $s$  est une isométrie indirecte et  $r^{k-k'}$  est une isométrie directe, on a donc obtenu une contradiction. Donc  $\ell = \ell'$  et on en déduit que  $r^k = r^{k'}$  donc  $k = k'$  car  $r$  est d'ordre  $n$ .

Le résultat suivant est souvent utile. La preuve est laissée en exercice.

**Proposition 1.20.** Soit  $f: G \rightarrow H$  un morphisme de groupes et  $S$  une partie de  $G$ . Alors  $f(\langle S \rangle) = \langle f(S) \rangle$ .

*Démonstration.* Exercice.

Puisque  $\langle S \rangle$  est un sous-groupe de  $G$ , son image  $f(\langle S \rangle)$  est un sous-groupe de  $H$ . De plus,  $S \subset \langle S \rangle$  donc  $f(S) \subset f(\langle S \rangle)$ . On en déduit que  $\langle f(S) \rangle$  est un sous-groupe de  $f(\langle S \rangle)$ .

Soit maintenant  $y \in f(\langle S \rangle)$ . Il existe  $x \in \langle S \rangle$  tel que  $y = f(x)$ . On peut donc écrire  $x = x_1 \cdots x_n$  avec, pour tout  $i$ ,  $x_i \in S$  ou  $x_i^{-1} \in S$ . On a alors  $y = f(x_1) \cdots f(x_i)$  avec, pour tout  $i$ ,  $f(x_i) \in f(S)$  ou  $f(x_i)^{-1} = f(x_i^{-1}) \in f(S)$ , donc  $y \in \langle f(S) \rangle$  et par conséquent  $f(\langle S \rangle) = \langle f(S) \rangle$ . ✓

Si  $S = \{x\}$ , on note  $\langle x \rangle = \langle \{x\} \rangle$  et on a  $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ .

**Définition 1.21.** Soit  $G$  un groupe et soit  $x \in G$ . On dit que  $x$  est d'**ordre fini** s'il existe  $n \in \mathbb{N}^*$  tel que  $x^n = 1$ . L'**ordre** de  $x$ , noté  $o(x)$ , est alors le plus petit nombre entier  $n \in \mathbb{N}^*$  tel que  $x^n = 1$ .

**Remarque.** L'élément neutre est le seul élément d'ordre 1 d'un groupe.

**Exemple.** Soit  $G$  un groupe fini et soit  $x \in G$ . Alors  $x$  est d'ordre fini avec  $o(x) \leq |G|$ . En effet si  $n = |G|$ , le sous-ensemble  $\{1, x, \dots, x^n\}$  de  $G$  possède nécessairement deux éléments égaux : il existe  $(i, j) \in \llbracket 0; n \rrbracket^2$  avec  $i > j$  tel que  $x^i = x^j$ , ce qui donne  $x^{i-j} = 1$  avec  $0 < i - j \leq n$ , d'où le résultat.

Le résultat suivant donne les principales propriétés de l'ordre d'un élément.

**Proposition 1.22.** Soit  $G$  un groupe et soit  $x \in G$ .

- (1) Soit  $m \in \mathbb{Z}^*$  tel que  $x^m = 1$ . Alors  $x$  est d'ordre fini et  $o(x) \mid m$ .
- (2) Soit  $x \in G$  un élément d'ordre fini. Alors  $x^{-1}$  est d'ordre fini et  $o(x^{-1}) = o(x)$ .
- (3) Si  $x$  est d'ordre fini, alors  $|\langle x \rangle| = o(x)$ .
- (4) Si  $G$  est fini, alors  $x^{|G|} = 1$  et  $o(x) \mid |G|$ .

*Démonstration.* (2) Notons  $d = o(x)$ . Puisque  $x$  et  $x^{-1}$  commutent,  $(x^{-1})^d = (x^{-1})^d x^d = (x^{-1}x)^d = 1$  donc  $x^{-1}$  est d'ordre fini et  $o(x^{-1}) \leq d = o(x)$  par définition. En appliquant cela à  $x^{-1}$ , on obtient  $o(x) = o((x^{-1})^{-1}) \leq o(x^{-1})$  et finalement  $o(x^{-1}) = o(x)$ .

(1) Si  $m > 0$ , alors  $x$  est d'ordre fini par définition. Si  $m < 0$ , alors  $x^{-m} x^m = x^{-m+m} = x^0 = 1$  donc  $x^{-m} = (x^m)^{-1} = 1$  avec  $-m > 0$  donc  $x$  est d'ordre fini.

On effectue la division euclidienne de  $m$  par  $o(x)$ , il existe donc des nombres entiers  $q$  et  $r$  avec  $0 \leq r < o(x)$  tels que  $m = o(x)q + r$ . Alors  $1 = x^m = (x^{o(x)})^q x^r = x^r$ , donc  $r = 0$  et on a le résultat.

- (3) Posons  $n = o(x)$ . Montrons que  $\{1, x, \dots, x^{n-1}\} = \langle x \rangle$ . L'inclusion  $\{1, x, \dots, x^{n-1}\} \subset \langle x \rangle$  est claire. Soit  $a \in \langle x \rangle$ , alors  $a = x^m$  pour  $m \in \mathbb{Z}$ . La division euclidienne de  $m$  par  $n$  dans  $\mathbb{Z}$  donne  $m = nq + r$ , avec  $0 \leq r < n$ . Donc  $a = x^{nq+r} = (x^n)^q x^r = x^r$  et  $a \in \{1, \dots, x^{n-1}\}$ . Finalement il est clair, puisque  $o(x) = n$ , que l'ensemble  $\{1, x, \dots, x^{n-1}\}$  possède bien  $n$  éléments distincts.
- (4) On sait que  $o(x) = |\langle x \rangle|$  donc le théorème de Lagrange assure que  $|G| = o(x)m$  pour un  $m \in \mathbb{N}^*$ . Alors  $x^{|G|} = (x^{o(x)})^m = 1$ . ✓

On étudie maintenant le produit d'éléments d'ordre fini. On ne peut rien dire en toute généralité, mais on a le résultat suivant.

**Proposition 1.23.** Soient  $a$  et  $b$  des éléments d'ordres finis d'un groupe  $G$  tels que  $ab = ba$ .

- (1)  $ab$  est d'ordre fini avec  $o(ab) \mid \text{ppcm}(o(a), o(b))$ .
- (2) Si  $\langle a \rangle \cap \langle b \rangle = \{1\}$ , alors  $o(ab) = \text{ppcm}(o(a), o(b))$ .
- (3) Si  $\text{pgcd}(o(a), o(b)) = 1$ , alors  $o(ab) = o(a)o(b)$ .
- (4) Soit  $r \in \mathbb{N}$ . Alors  $o(a^r) = \frac{o(a)}{\text{pgcd}(o(a), r)}$ .

*Démonstration.* Comme  $ab = ba$ , on a  $(ab)^m = a^m b^m$  pour tout nombre entier  $m$ . Notons  $p = o(a)$ ,  $q = o(b)$ .

- (1) Soit  $\mu = \text{ppcm}(p, q)$ , alors il existe des nombres entiers  $r$  et  $s$  tels que  $\mu = rp = sq$ . On a donc  $(ab)^\mu = (a^p)^r (b^q)^s = 1$ , donc  $ab$  est d'ordre fini et  $o(ab) \mid \mu$ .
- (2) Soit  $m \in \mathbb{N}^*$  tel que  $(ab)^m = 1$ . Alors  $a^m = b^{-m} \in \langle a \rangle \cap \langle b \rangle = \{1\}$ , donc  $a^m = 1$  et  $b^m = 1$  et donc  $p \mid m$  et  $q \mid m$ ; on en déduit que  $m$  est un multiple de  $p$  et de  $q$  et donc que  $\mu \mid m$ . On applique cela à  $m = o(ab)$ , et on conclut en utilisant (1).
- (3)  $\langle a \rangle \cap \langle b \rangle$  est un sous-groupe de  $\langle a \rangle$  et de  $\langle b \rangle$ , donc  $|\langle a \rangle \cap \langle b \rangle|$  divise à la fois  $|\langle a \rangle|$  et  $|\langle b \rangle|$  qui sont premiers entre eux. Ainsi  $\langle a \rangle \cap \langle b \rangle = \{1\}$  et on applique (2) (avec  $\text{ppcm}(p, q) = pq$ ).
- (4) Soit  $d = \text{pgcd}(p, r)$ . Posons  $p = dp'$  et  $r = dr'$  avec  $(p', r') \in (\mathbb{N}^*)^2$  et  $\text{pgcd}(p', r') = 1$ . On a  $(a^r)^{p'} = a^{dr'p'} = (a^p)^{r'} = 1$ , donc  $o(a^r) \mid p'$ . Soit  $m \in \mathbb{N}^*$  tel que  $(a^r)^m = 1$ . Alors  $p$  divise  $rm$ , donc en divisant par  $d$  on obtient  $p' \mid r'm$  donc d'après le lemme de Gauss,  $p'$  divise  $m$ . En appliquant cela à  $m = o(a^r)$ , on en déduit que  $p'$  divise  $o(a^r)$  et finalement que  $o(a^r) = p' = \frac{p}{d}$ . ✓

**Exercice.** Donner un exemple de groupe  $G$  contenant des éléments d'ordres finis  $a$  et  $b$  tels que  $ab$  ne soit pas d'ordre fini.

Voir travaux dirigés

*Correction.* ➤ Dans l'espace vectoriel euclidien  $\mathbb{R}^2$ , soit  $s_1$  (resp.  $s_2$ ) la symétrie orthogonale par rapport à la droite  $D_1 = \text{vect}\{u_1\}$  (resp.  $D_2 = \text{vect}\{u_2\}$ ) avec  $D_1 \neq D_2$ . Soit  $\theta = 2\pi x$  l'angle  $(\widehat{u_2, u_1})$  avec  $x \in \mathbb{R}$ . Alors  $s_1 \circ s_2$  est la rotation  $r$  d'angle  $2\theta$ .

Les symétries  $s_1$  et  $s_2$  sont d'ordre 2, fini. Cependant,  $r$  est d'ordre fini si, et seulement si,  $2\theta$  (ou, ce qui revient au même,  $\theta$ ) est un multiple rationnel de  $2\pi$  (c'est-à-dire que  $x \in \mathbb{Q}$ ).

Il suffit donc de choisir  $x \in \mathbb{R} \setminus \mathbb{Q}$ .

Remarque : on peut aussi choisir  $x \in \mathbb{Q}$  pour obtenir  $s_1 \circ s_2$  d'ordre fini mais tel que cet ordre ne soit pas un diviseur de  $\text{ppcm}(o(s_1), o(s_2)) = 2$ ; par exemple, avec  $x = \frac{1}{6}$ , soit  $\theta = \frac{\pi}{3}$ , la rotation  $r = s_1 \circ s_2$  est d'ordre 3.

➤ Autre exemple : dans  $\text{GL}_2(\mathbb{R})$ , les matrices  $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  et  $B = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$  sont d'ordre 2, mais  $AB = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}$  est d'ordre infini. ✓

On s'intéresse maintenant aux groupes dont la structure est la plus simple possible, à savoir les groupes monogènes.

**Définition 1.24.** Un groupe est dit **monogène** s'il est engendré par un de ses éléments. Il est dit **cyclique** s'il est monogène fini.

**Remarque.** Soit  $G$  un groupe monogène, posons  $G = \langle x \rangle$ . Soit  $H$  un groupe. Tout morphisme de groupes  $f: G \rightarrow H$  est entièrement déterminé par  $f(x)$ .

En effet, on sait que  $G = \{x^k \mid k \in \mathbb{Z}\}$ , et si  $f$  est un morphisme de groupes on doit avoir  $f(x^k) = f(x)^k$ , donc il suffit de connaître  $f(x)$  pour connaître  $f$ .

**Exemples.** (1) Le groupe  $(\mathbb{Z}, +)$  est monogène (de générateur 1).

(2) Pour  $n \in \mathbb{N}^*$ , le groupe  $\mathbb{Z}/n\mathbb{Z}$  est cyclique d'ordre  $n$ , engendré par  $\bar{1}$ .

(3) Pour  $n \in \mathbb{N}^*$ , le groupe  $\mu_n$  des racines  $n^{\text{ièmes}}$  de l'unité (complexes) est cyclique d'ordre  $n$ , engendré par  $\omega = e^{\frac{2i\pi}{n}}$ .

Les exemples présentés plus haut fournissent une liste complète des groupes monogènes.

**Théorème 1.25. (Classification des groupes monogènes)** Soit  $G$  un groupe monogène.

(1) Si  $G$  est infini, alors  $G$  est isomorphe à  $\mathbb{Z}$ .

(2) Si  $G$  est cyclique (fini), alors il existe  $n \in \mathbb{N}^*$  ( $n = |G|$ ) tel que  $G$  soit isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ .

**Démonstration.** Soit  $x \in G$  un générateur de  $G$  et soit  $f: \mathbb{Z} \rightarrow G$  le morphisme de groupes défini par  $f(k) = x^k$  pour tout  $k \in \mathbb{Z}$ . Alors  $f$  est surjectif. Puisque  $\text{Ker } f$  est un sous-groupe de  $\mathbb{Z}$ , il existe  $n \in \mathbb{N}$  tel que  $\text{Ker } f = n\mathbb{Z}$ . Ainsi le premier théorème d'isomorphisme assure que  $f$  induit un isomorphisme  $\mathbb{Z}/n\mathbb{Z} \cong G$ .

Par conséquent,  $G$  est fini si, et seulement si,  $n \neq 0$ , et on a le résultat voulu. ✓

**Notations.** Pour  $n \in \mathbb{N}^*$  on note  $C_n$  « le » groupe cyclique multiplicatif d'ordre  $n$  (il est donc isomorphe au groupe additif  $\mathbb{Z}/n\mathbb{Z}$ ).

Si  $x$  est un générateur de  $C_n$ , on a  $C_n = \{1, x, \dots, x^{n-1}\}$ , avec  $x^n = 1$  et  $x^i \neq 1$  pour  $1 \leq i \leq n-1$ .

**Proposition 1.26.** Soit  $n \in \mathbb{N}^*$  et soit  $C_n = \{1, x, \dots, x^{n-1}\}$  le groupe cyclique d'ordre  $n$ .

(1) Pour tout diviseur  $d$  de  $n$ , il existe un unique sous-groupe de  $C_n$  d'ordre  $d$ ; ce sous-groupe est cyclique, engendré par  $x^k$  avec  $k = \frac{n}{d}$ .

(2) Les générateurs de  $C_n$  sont les éléments  $x^k$  avec  $\text{pgcd}(k, n) = 1$ .

**Démonstration.** (1) Soit  $d$  un diviseur de  $n$  et soit  $a = x^k$  avec  $k = \frac{n}{d}$ . Alors  $o(a) = \frac{o(x)}{\text{pgcd}(o(x), k)} = \frac{n}{\text{pgcd}(n, \frac{n}{d})} = \frac{n}{\frac{n}{d}} = d$ , donc  $\langle a \rangle$  est un sous-groupe de  $C_n$  d'ordre  $d$ , et il est cyclique.

Supposons que  $H$  soit un sous-groupe de  $C_n$  d'ordre  $d$ . Soit  $m = \min\{\ell \in \llbracket 1; n-1 \rrbracket \mid x^\ell \in H\}$ . Alors  $\langle x^m \rangle \subset H$ . Soit maintenant  $x^t \in H$  un élément quelconque. Il existe des nombres entiers  $q$  et  $r$  avec  $0 \leq r < m$  tels que  $t = qm + r$ . On a alors  $x^t = (x^m)^q x^r$  donc  $x^r \in H$  et par définition de  $m$  on doit avoir  $r = 0$ . Donc  $x^t \in \langle x^m \rangle$  et donc  $H = \langle x^m \rangle$ .

En particulier,  $x^m$  est d'ordre  $d = |H|$ . On a aussi  $o(x^m) = \frac{n}{\text{pgcd}(n, m)} = \frac{dk}{\text{pgcd}(n, m)}$ , donc  $\text{pgcd}(n, m) = k$  et en particulier  $k$  divise  $m$ . On en déduit que  $x^m \in \langle x^k \rangle$ , donc  $H \subset \langle x^k \rangle$  et finalement  $H = \langle x^k \rangle$  puisque les deux groupes ont le même cardinal.

(2) Un élément  $x^k$  de  $C_n$  engendre  $C_n$  si, et seulement si,  $o(x^k) = n$ . Puisque  $o(x^k) = \frac{n}{\text{pgcd}(n,k)}$ , on en déduit que  $x^k$  engendre  $C_n$  si, et seulement si,  $\text{pgcd}(n,k) = 1$ . ✓

**Théorème 1.27. (Classification des groupes d'ordre premier)** Soit  $G$  un groupe d'ordre  $p$  premier. Alors  $G \cong \mathbb{Z}/p\mathbb{Z}$ .

*Démonstration.* Voir travaux dirigés

Par hypothèse,  $|G| = p \geq 2$ , donc il existe  $x \in G$  avec  $x \neq 1$ . Alors  $|\langle x \rangle|$  divise  $|G| = p$  par le théorème de Lagrange, donc puisque  $p$  est premier,  $|\langle x \rangle| = p = |G|$  et donc  $G = \langle x \rangle$ . Ainsi  $G$  est cyclique et le théorème précédent permet de conclure. ✓

**Théorème 1.28.** Soit  $G$  un groupe qui n'est pas trivial. Alors les assertions suivantes sont équivalentes :

- (1)  $G$  ne possède pas de sous-groupe propre.
- (2) L'ordre de  $G$  est un nombre premier.
- (3)  $G$  est cyclique d'ordre premier.

*Démonstration.* L'implication (3)  $\Rightarrow$  (2) est évidente et l'implication (2)  $\Rightarrow$  (1) est une conséquence immédiate du théorème de Lagrange.

Montrons (1)  $\Rightarrow$  (3). Puisque  $G$  n'est pas trivial, il existe  $x \in G$  avec  $x \neq 1$ . Le sous-groupe  $\langle x \rangle$  n'est pas réduit à  $\{1\}$ , donc  $\langle x \rangle = G$  par (1). Donc  $G$  est monogène. Puisque  $\mathbb{Z}$  contient des sous-groupes propres, il suit du théorème 1.25 que  $G \cong \mathbb{Z}/n\mathbb{Z}$  pour un  $n \in \mathbb{N}^*$ . Si  $n$  n'est pas premier, alors il existe  $(a, b) \in \mathbb{N}^2$  avec  $a > 1$  et  $b > 1$  tels que  $n = ab$ . Alors  $x^a \neq 1$  car  $1 < a < n$ ,  $(x^a)^b = 1$  et  $|\langle x^a \rangle| = o(x^a) \leq b < n$ , donc  $\langle x^a \rangle$  est un sous-groupe propre de  $G$ , ce qui contredit (1). Ainsi  $n$  est premier. ✓

**Corollaire 1.29.** Soit  $G$  un groupe abélien. Alors  $G$  est simple si, et seulement si, il existe un nombre premier  $p$  tel que  $G \cong \mathbb{Z}/p\mathbb{Z}$ .

*Démonstration.* Dans un groupe abélien tous les sous-groupes sont normaux donc le théorème est une conséquence directe du théorème précédent. ✓

On termine le paragraphe par un résultat très utile pour construire des morphismes de groupes.

**Théorème 1.30.** Soient  $G$  un groupe cyclique d'ordre  $n \in \mathbb{N}^*$ ,  $x$  un générateur de  $G$ ,  $H$  un groupe et  $h \in H$  tel que  $h^n = 1$ . Alors il existe un unique morphisme de groupes  $f: G \rightarrow H$  tel que  $f(x) = h$ .

*Démonstration.* Soient  $u: \mathbb{Z} \rightarrow G$  et  $v: \mathbb{Z} \rightarrow H$  les morphismes de groupes définis par  $u(k) = x^k$  et  $v(k) = h^k$  pour tout  $k \in \mathbb{Z}$ . Puisque  $x$  engendre  $G$ ,  $u$  est surjectif, et puisque  $o(x) = n$  on a  $\text{Ker } u = n\mathbb{Z}$ , donc par le premier théorème d'isomorphisme  $u$  induit un isomorphisme  $\bar{u}: \mathbb{Z}/n\mathbb{Z} \rightarrow G$  tel que  $\bar{u}(\bar{1}) = x$ .

Puisque  $h^n = 1$ , on a  $n\mathbb{Z} \subset \text{Ker } v$  donc d'après le théorème de factorisation  $v$  induit un morphisme de groupes  $\bar{v}: \mathbb{Z}/n\mathbb{Z} \rightarrow H$  tel que  $\bar{v}(\bar{1}) = h$ .

Alors  $f = \bar{v} \circ \bar{u}^{-1}: G \rightarrow H$  est un morphisme de groupes tel que  $f(x) = h$ .

L'unicité provient du fait que  $G = \langle x \rangle$  (voir la remarque page 20). ✓

Il s'agit ici de décrire une opération qui permet construire de nouveaux groupes à partir d'anciens : le produit direct de groupes.

**Définition-Proposition 1.31.** Soient  $G_1$  et  $G_2$  deux groupes. Alors l'ensemble  $G_1 \times G_2$ , muni de la loi :

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2), \quad \forall (x_1, y_1) \in G_1^2, \forall (x_2, y_2) \in G_2^2,$$

est un groupe. L'élément neutre est  $(1_{G_1}, 1_{G_2})$  et l'inverse d'un élément  $(x, y)$  est  $(x^{-1}, y^{-1})$ . Le groupe obtenu, noté  $G_1 \times G_2$ , est appelé le **produit direct** (ou tout simplement produit) de  $G_1$  par  $G_2$ .

On s'intéresse tout d'abord au produit direct de groupes cycliques.

**Théorème 1.32. (Théorème chinois)** Soient  $n, m \in \mathbb{N}^*$ . Alors

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z} \iff \text{pgcd}(n, m) = 1.$$

*Démonstration.* (Pas faite en cours.) On va utiliser les notations multiplicatives. On doit donc montrer :

$$C_n \times C_m \cong C_{nm} \iff \text{pgcd}(n, m) = 1.$$

Soient  $x$  un générateur de  $C_n$  et  $y$  un générateur de  $C_m$ . Calculons  $o((x^r, y^s))$  pour  $(r, s) \in \mathbb{N}^2$ . Soient  $a = (x, 1)$  et  $b = (y, 1)$ . On a  $(x^r, y^s) = a^r b^s$  avec  $a^r b^s = b^s a^r$  et  $\langle a^r \rangle \cap \langle b^s \rangle = \{1\}$ . On peut donc appliquer la proposition 1.23 :

$$\begin{aligned} o((x^r, y^s)) &= \text{ppcm}(o(a^r), o(b^s)) = \text{ppcm}\left(\frac{o(a)}{\text{pgcd}(o(a), r)}, \frac{o(b)}{\text{pgcd}(o(b), s)}\right) \\ &= \text{ppcm}\left(\frac{n}{\text{pgcd}(n, r)}, \frac{m}{\text{pgcd}(m, s)}\right). \end{aligned}$$

Par conséquent, si  $\text{pgcd}(n, m) = 1$  on a  $o((x, y)) = \text{ppcm}(n, m) = nm$ , et puisque  $|C_n \times C_m| = nm$ , ce groupe est cyclique (engendré par  $(x, y)$ ).

Réciproquement, si  $C_m \times C_n \cong C_{nm}$ , il contient un élément  $(x^r, y^s)$  d'ordre  $mn$ . Ainsi  $nm = \text{ppcm}\left(\frac{n}{\text{pgcd}(n, r)}, \frac{m}{\text{pgcd}(m, s)}\right) \leq \text{ppcm}(n, m) \leq nm$  et donc  $\text{ppcm}(n, m) = nm$  et enfin  $\text{pgcd}(n, m) = 1$ . ✓

**Remarque.** Supposons que  $\text{pgcd}(n, m) = 1$ . On peut donner un isomorphisme explicite  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/nm\mathbb{Z}$ .

Pour  $k \in \mathbb{Z}$ , notons  $\pi_k: \mathbb{Z} \rightarrow \mathbb{Z}/k\mathbb{Z}$  la projection canonique. Soit  $f: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  le morphisme de groupes défini par  $f(x) = (\pi_n(x), \pi_m(x))$ .

Puisque  $f(nm) = (0, 0)$ , on a  $nm\mathbb{Z} \subset \text{Ker } f$ . De plus, soit  $x \in \text{Ker } f$ , alors  $\pi_n(x) = 0$  donc  $n \mid x$  et de même  $m \mid x$ , donc puisque  $\text{pgcd}(n, m) = 1$  on en déduit que  $nm \mid x$  et donc que  $x \in nm\mathbb{Z}$ . Finalement,  $\text{Ker } f = nm\mathbb{Z}$ .

Soit maintenant  $t = (\pi_n(a), \pi_m(b)) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  un élément quelconque, avec  $(a, b) \in \mathbb{Z}^2$ . Puisque  $\text{pgcd}(n, m) = 1$ , d'après le théorème de Bézout il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $un + vm = 1$ . Soit  $x = unb + vma$ . Alors

$$\begin{aligned} x &= unb + (1 - un)a = un(b - a) + a \\ &= (1 - vm)b + vmb = vm(a - b) + b \end{aligned}$$

donc  $f(x) = (\pi_n(x), \pi_m(x)) = (\pi_n(a), \pi_m(b)) = t$ , donc  $f$  est surjectif.

Alors, par le premier théorème d'isomorphisme,  $f$  induit un isomorphisme  $\bar{f}: \mathbb{Z}/nm\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ .

Il est défini par  $\bar{f}(\pi_{nm}(x)) = (\pi_n(x), \pi_m(x))$  et sa bijection réciproque est donnée par  $\bar{f}^{-1}(\pi_n(a), \pi_m(b)) = (\pi_{nm}(unb + vma))$  où  $(u, v) \in \mathbb{Z}^2$  est tel que  $un + vm = 1$ .

On peut également démontrer la réciproque du théorème en travaillant avec les groupes additifs.

Supposons qu'il existe un isomorphisme  $\psi: \mathbb{Z}/nm\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ . On doit démontrer que  $\text{pgcd}(n, m) = 1$ .

Notons  $\alpha = \psi \circ \pi_{nm}: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ , soient  $p_1: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  et  $p_2: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  les projections sur chacune des composantes et soient  $\alpha_i = p_i \circ \alpha$  pour  $i \in \{1, 2\}$ . On vérifie facilement que

- $\text{Ker } \alpha = \text{Ker}(\pi) = nm\mathbb{Z}$  (car  $\psi$  est injectif);
- $\text{Ker}(\alpha) = \text{Ker}(\alpha_1) \cap \text{Ker}(\alpha_2)$ ;
- $\alpha_1$  est surjectif (composée de deux surjections),  $\text{Ker } \alpha_1$  est un sous-groupe de  $\mathbb{Z}$ , donc de la forme  $u\mathbb{Z}$  avec  $u \in \mathbb{Z}$ , donc grâce au premier théorème d'isomorphisme on a un isomorphisme  $\mathbb{Z}/u\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ , donc ces deux groupes ont le même ordre, c'est-à-dire que  $u = n$  et finalement  $\text{Ker}(\alpha_1) = n\mathbb{Z}$ .

On en déduit que  $nm\mathbb{Z} = \text{Ker}(\alpha) = n\mathbb{Z} \cap m\mathbb{Z}$ , donc  $\text{ppcm}(n, m) = nm$  et donc  $\text{pgcd}(n, m) = 1$ .

Soient  $G_1$  et  $G_2$  deux groupes. Alors  $G_1$  est naturellement isomorphe au sous-groupe  $G_1 \times \{1\}$  de  $G_1 \times G_2$  et  $G_2$  est naturellement isomorphe au sous-groupe  $\{1\} \times G_2$  de  $G_1 \times G_2$ .

On se pose alors naturellement la question suivante : si  $G$  est un groupe et si  $H$  et  $K$  sont des sous-groupes de  $G$ , quand a-t-on  $G \cong H \times K$ ?

La réponse sera fournie par le théorème 1.34.

**Notation.** Soit  $G$  un groupe et soient  $H$  et  $K$  des parties de  $G$ . On pose  $HK = \{hk \mid h \in H, k \in K\}$ .

**Proposition 1.33.** Soit  $G$  un groupe et soient  $H$  et  $K$  des sous-groupes de  $G$ .

- (1) Si  $H$  et  $K$  sont finis, alors  $|HK| = \frac{|H||K|}{|H \cap K|}$ .
- (2)  $HK$  est un sous-groupe de  $G$  si et seulement si  $HK = KH$ .
- (3) Si  $H \triangleleft G$  ou  $K \triangleleft G$ , alors  $HK$  est un sous-groupe de  $G$ .
- (4) Si  $H \triangleleft G$  et  $K \triangleleft G$ , alors  $HK$  est un sous-groupe normal de  $G$ .

**Démonstration.** (1) On considère l'application  $m: H \times K \rightarrow HK, (x, y) \mapsto xy$ , qui est surjective par définition de  $HK$ .

Soit  $\mathcal{R}$  la relation d'équivalence sur  $H \times K$  définie par  $(x, y)\mathcal{R}(x', y') \iff xy = x'y'$ . On note  $\text{cl}(x, y)$  la classe de  $(x, y) \in H \times K$  pour  $\mathcal{R}$ .

Puisque  $m$  est surjective, elle induit une bijection  $(H \times K)/\mathcal{R} \cong HK$  (la classe d'équivalence  $\text{cl}(x, y)$  est l'ensemble des antécédents de  $xy$ ). Soient  $(x_i, y_i)_{1 \leq i \leq r}$  les représentants distincts des diverses classes d'équivalence pour  $\mathcal{R}$ , on a donc  $H \times K = \coprod_{i=1}^r \text{cl}(x_i, y_i)$  (réunion disjointe) et  $|(H \times K)/\mathcal{R}| = |HK| = r$ .

Soit  $(x, y) \in H \times K$ , déterminons le cardinal de  $\text{cl}(x, y)$ . On construit une bijection

$$\begin{aligned} \text{cl}(x, y) &\longrightarrow H \cap K \\ (x', y') &\longmapsto x^{-1}x' = y(y')^{-1} \\ (xt, t^{-1}y) &\longleftarrow t \end{aligned}$$

Ainsi  $|H||K| = |H \times K| = r|H \cap K| = |HK||H \cap K|$ .

- (2) ♦ Supposons d'abord que  $HK$  est un sous-groupe de  $G$  et montrons que  $HK = KH$ .

Soit  $x \in HK$ , alors  $x^{-1} \in HK$  puisque  $HK$  est un sous-groupe de  $G$ . Donc il existe  $(h, k) \in H \times K$  tel que  $x^{-1} = hk$ . On en déduit que  $x = (hk)^{-1} = k^{-1}h^{-1} \in KH$ . Donc  $HK \subset KH$ .

Pour l'autre inclusion, on remarque que  $H$  et  $K$  sont contenus dans  $HK$  donc, puisque le sous-groupe  $HK$  est stable par produit,  $KH \subset HK$ .

- ♦ Supposons que  $HK = KH$  et montrons que  $HK$  est un sous-groupe de  $G$ . Soient  $x_1$  et  $x_2$  deux éléments de  $HK$ . Il existe donc  $(h_1, k_1, h_2, k_2) \in (H \times K)^2$  tel que  $x_1 = h_1 k_1$  et  $x_2 = h_2 k_2$ .

On a  $x_1^{-1} = k_1^{-1} h_1^{-1} \in KH = HK$ .

De plus,  $k_1 h_2 \in KH = HK$  donc il existe  $(h', k') \in H \times K$  tel que  $k_1 h_2 = h' k'$ , donc  $x_1 x_2 = h_1 k_1 h_2 k_2 = h_1 h' k' k_2 \in HK$ .

Donc  $HK$  est un sous-groupe de  $G$ .

- (3) Supposons que  $H \triangleleft G$ . D'après (2), on doit démontrer que  $HK = KH$ .

Soit  $x \in HK$ , il existe  $(h, k) \in H \times K$  tel que  $x = hk$ . Puisque  $H \triangleleft G$ , on sait que  $k^{-1} h k \in H$ , donc  $k^{-1} x \in H$  et donc  $x = k(k^{-1} x) \in KH$ . Donc  $HK \subset KH$ . L'autre inclusion se démontre de la même manière.

Si  $K \triangleleft G$ , en échangeant les rôles de  $H$  et  $K$  on en déduit que  $KH$  est un sous-groupe de  $G$  et d'après (2)  $HK = KH$  est donc un sous-groupe de  $G$ .

- (4) Supposons que  $H \triangleleft G$  et  $K \triangleleft G$ . On sait d'après (3) que  $HK$  est un sous-groupe de  $G$ . Soit  $x \in HK$  et soit  $g \in G$ . Il existe  $(h, k) \in H \times K$  tel que  $x = hk$ . On a alors  $g x g^{-1} = g h g^{-1} g k g^{-1} \in HK$  car  $g h g^{-1} \in H$  et  $g k g^{-1} \in K$ . Donc  $HK \triangleleft G$ . ✓

Le résultat qui suit est souvent utile dans les résultats de classification.

### **Théorème 1.34. (Caractérisation du produit direct)**

Soit  $G$  un groupe et soient  $H$  et  $K$  deux sous-groupes de  $G$ . Supposons que :

- (1)  $G = HK$ ,
- (2)  $H \cap K = \{1\}$ ,
- (3)  $H \triangleleft G$  et  $K \triangleleft G$ .

Alors  $G$  est isomorphe au produit direct  $H \times K$ .

*Démonstration.* Montrons que l'application  $m: H \times K \longrightarrow G$  définie par  $m(x, y) = xy$  pour tout  $(x, y) \in H \times K$  est un isomorphisme de groupes.

On commence par remarquer que pour tout  $(h, k) \in H \times K$  on a  $hk = kh$ . En effet,  $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$  car  $K \triangleleft G$  et  $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$  car  $H \triangleleft G$ , donc  $hkh^{-1}k^{-1} \in H \cap K = \{1\}$  et donc  $hkh^{-1}k^{-1} = 1$ .

Vérifions que  $m$  est un morphisme de groupes. Soient  $(h, k)$  et  $(h', k')$  deux éléments de  $H \times K$ . Alors en utilisant ce qui précède on a

$$m(h, k)m(h', k') = hkh'k' = hh'kk' = m(hh', kk').$$

L'application  $m$  est surjective par hypothèse (1).

Enfin, soit  $(h, k) \in \text{Ker } m$ . Alors  $hk = 1$  donc  $h = k^{-1} \in H \cap K$  et donc  $h = 1$  et  $k^{-1} = 1$  et on en déduit que  $(h, k) = (1, 1)$ . Donc  $\text{Ker } m = \{(1, 1)\}$  et donc  $m$  est injective. ✓

Voici des exemples d'application des résultats de ce paragraphe.

**Exercice.** Soit  $G$  un groupe fini contenant des sous-groupes normaux  $H$  et  $K$  tels que  $|G| = |H||K|$  et  $\text{pgcd}(|H|, |K|) = 1$ . Montrer que  $G \cong H \times K$ . Voir travaux dirigés

*Correction.* Puisque  $\text{pgcd}(|H|, |K|) = 1$ , grâce au théorème de Lagrange l'ordre du sous-groupe  $H \cap K$  de  $H$  et de  $K$  divise  $|H|$  et  $|K|$  et on obtient  $|H \cap K| = 1$  donc  $H \cap K = \{1\}$ .

On a alors  $|HK| = \frac{|H||K|}{|H \cap K|} = |H||K| = |G|$  donc  $HK = G$ .

Enfin,  $H \triangleleft G$  et  $K \triangleleft G$  par hypothèse.

Donc  $G \cong H \times K$ . ✓

**Exercice.** Montrer que si  $G$  un groupe abélien fini non trivial tel qu'il existe un nombre premier  $p$  tel que  $x^p = 1$  pour tout  $x \in G$ , alors il existe  $n \in \mathbb{N}^*$  tel que  $|G| = p^n$  et  $G \cong (\mathbb{Z}/p\mathbb{Z})^n$  (on pourra raisonner par récurrence sur  $|G|$ ).

*Remarque.* Si  $p = 2$ , et si  $G$  est un groupe fini tel que  $x^2 = 1$  pour tout  $x \in G$ , alors  $G$  est automatiquement abélien. Voir travaux dirigés

**Correction.** Remarquons que pour tout  $x \in G$  avec  $x \neq 1$ , on a  $o(x) = p$  et  $\langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$ . Nous allons démontrer les deux points séparément.

➤ Montrons que l'ordre de  $G$  est une puissance de  $p$ , par récurrence sur  $|G|$ . Notons que  $G$  n'est pas trivial donc  $|G| \geq 2$ .

◆ Initialisation. Si  $|G| = 2$ , on a  $p = 2$  et  $|G| = 2^1$ .

◆ Hérédité : soit  $d \in \mathbb{N}^*$ ,  $d \geq 3$  tel que  $|G| = d$  et tel que pour tout groupe fini abélien non trivial  $H$  tel que  $|H| < d$  et  $x^p = 1$  pour tout  $x \in H$ , il existe  $n \in \mathbb{N}^*$  tel que  $|H| = p^n$ .

Soit  $x \in G$  avec  $x \neq 1$ . Alors  $\langle x \rangle$  est normal dans  $G$  car  $G$  est abélien et la projection canonique  $\pi: G \rightarrow G/\langle x \rangle$  est un morphisme surjectif de groupes abéliens de noyau  $\langle x \rangle$ , donc  $|G| = |\langle x \rangle| |G/\langle x \rangle|$ . Or  $|\langle x \rangle| = p$  et  $|G/\langle x \rangle| < |G|$  donc soit  $G/\langle x \rangle = \{1\}$  soit, par hypothèse de récurrence, il existe  $n \in \mathbb{N}^*$  tel que  $|G/\langle x \rangle| = p^n$ . Dans les deux cas, il existe  $n \in \mathbb{N}$  tel que  $|G/\langle x \rangle| = p^n$ .

On en déduit finalement que  $|G| = p^{n+1}$  avec  $n+1 \in \mathbb{N}^*$ .

➤ Démontrons par récurrence sur  $n \in \mathbb{N}^*$  tel que  $|G| = p^n$  que  $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ .

◆ Initialisation. Si  $n = 1$ , alors  $|G| = p$  premier et on sait que  $G \cong \mathbb{Z}/p\mathbb{Z}$ .

◆ Hérédité. Soit  $n \in \mathbb{N}^*$  avec  $n \geq 2$  tel que pour tout groupe abélien  $H$  d'ordre  $p^{n-1}$  tel que  $|H| < n$  et  $x^p = 1$  pour tout  $x \in H$ , on a  $H \cong (\mathbb{Z}/p\mathbb{Z})^{n-1}$ .

Soit  $x \in G$  avec  $x \neq 1$ . Soit  $L = \langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$ . Comme  $G$  est abélien,  $L \triangleleft G$ . Alors  $|G/L| = p^{n-1}$  donc par hypothèse de récurrence il existe un isomorphisme  $\alpha: G/L \rightarrow (\mathbb{Z}/p\mathbb{Z})^{n-1}$ . Notons  $\pi: G \rightarrow G/L$  la projection canonique. Pour tout  $i$  entier avec  $1 \leq i \leq n-1$ , soit  $e_i = (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}, \dots, \bar{0}) \in (\mathbb{Z}/p\mathbb{Z})^{n-1}$  avec  $\bar{1}$  en  $i^{\text{ème}}$  position. Alors  $\{\alpha^{-1}(e_1), \dots, \alpha^{-1}(e_{n-1})\}$  engendrent  $G/L$  car  $\alpha$  est un isomorphisme. Pour tout  $i$ , choisissons  $g_i \in G$  tel que  $\pi(g_i) = \alpha^{-1}(e_i)$ , on a donc  $\pi(\langle g_1, \dots, g_{n-1} \rangle) = \langle \pi(g_1), \dots, \pi(g_{n-1}) \rangle = \langle \alpha^{-1}(e_1), \dots, \alpha^{-1}(e_{n-1}) \rangle = G/L$ .

Ainsi, comme  $\pi$  est surjectif,  $H = \langle g_1, \dots, g_{n-1} \rangle$  est un sous-groupe de  $G$  d'ordre au moins  $|\pi(H)| = |G/L| = p^{n-1}$ . De plus,  $G$  est abélien et  $z^p = 1$  pour tout  $z \in G$  donc  $H = \{g_1^{u_1} \cdots g_{n-1}^{u_{n-1}} \mid 0 \leq u_i \leq p-1\}$ , donc  $|H| \leq p^{n-1}$  donc  $|H| = p^{n-1}$ .

Montrons que  $G \cong H \times L$ . Puisque  $G$  est abélien, les sous-groupes  $H$  et  $L$  sont normaux dans  $G$ . De plus,  $x$  est d'ordre  $p$  donc  $|L| = p$  et donc  $|H||L| = p^{n-1} \cdot p = p^n = |G|$ .

Il reste donc à vérifier que  $H \cap L = \{1\}$ . Soit  $y \in H \cap L$ . Alors  $\pi(y) = 1$ . Puisque  $y \in H$  on peut écrire  $y = g_1^{u_1} \cdots g_{n-1}^{u_{n-1}}$  avec  $u_i \in \llbracket 0; p-1 \rrbracket$  pour tout  $i$ . On a donc  $0 = \alpha(1) = \alpha(\pi(y)) = \sum_{i=1}^{n-1} u_i e_i = (\bar{u}_1, \dots, \bar{u}_{n-1})$ , donc  $\bar{u}_i = \bar{0}$  dans  $\mathbb{Z}/p\mathbb{Z}$  pour tout  $i$ , donc  $p \mid u_i$  pour tout  $i$  et donc  $u_i = 0$  pour tout  $i$ . On obtient  $y = 1$ . Donc  $H \cap L = \{1\}$ .

On en déduit que  $G \cong H \times K \cong (\mathbb{Z}/p\mathbb{Z})^{n-1} \times \mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^n$ .

➤ Remarque finale : cas  $p = 2$ . Soit  $G$  un groupe fini tel que pour tout  $x \in G$  on a  $x^2 = 1$ . Notons que pour tout  $x \in G$  on a donc  $x = x^{-1}$ .

Soit  $(x, y) \in G^2$ . Alors  $xyx^{-1}y^{-1} = xyxy = (xy)^2 = 1$  donc  $xy = yx$ .

Donc  $G$  est abélien. ✓

**Exercice.** Soit  $G$  un groupe abélien d'ordre  $pq$  où  $p, q$  sont des nombres premiers distincts. Montrer que  $G \cong C_{pq}$ . Voir travaux dirigés

**Correction.** D'après le théorème de Lagrange, pour tout  $x \in G$  on a  $o(x) \in \{1, p, q, pq\}$ .

- S'il existe un élément  $x \in G$  d'ordre  $pq$ , alors  $|\langle x \rangle| = pq = |G|$  et  $\langle x \rangle \subset G$  donc  $G = \langle x \rangle$  est cyclique d'ordre  $pq$  donc  $G \cong C_{pq}$ .
- Supposons que  $G$  contienne deux éléments  $x$  et  $y$  de  $G$  tels que  $o(x) = p$  et  $o(y) = q$ . Notons  $H = \langle x \rangle$  et  $K = \langle y \rangle$ . On a  $H \cong C_p$  et  $K \cong C_q$  puisque  $p$  et  $q$  sont premiers. Puisque  $G$  est abélien,  $H$  et  $K$  sont normaux dans  $G$ . De plus,  $|G| = pq = |H||K|$  et  $\text{pgcd}(|H|, |K|) = \text{pgcd}(p, q) = 1$  donc d'après un exercice précédent, on a  $G \cong H \times K \cong C_p \times C_q$ . Finalement, d'après le théorème chinois,  $G \cong C_{pq}$ . Notons que  $G$  contient donc aussi un élément d'ordre  $pq$ . Autre méthode : on démontre directement que  $xy$  est un élément d'ordre  $pq$ . En effet,  $G$  est abélien donc  $xy = yx$  et donc  $o(xy) = \text{ppcm}(o(x), o(y)) = \text{ppcm}(p, q) = pq$  car  $p$  et  $q$  sont premiers entre eux. Donc  $G$  contient un élément d'ordre  $pq = |G|$ , donc  $G = \langle xy \rangle \cong C_{pq}$ .
- Si nous ne sommes pas dans les cas précédents, alors soit  $x^p = 1$  pour tout  $x \in G$ , soit  $x^q = 1$  pour tout  $x \in G$ . Mais alors, d'après l'exercice précédent,  $|G|$  est une puissance d'un nombre premier ( $p$  ou  $q$ ) et on a obtenu une contradiction.

Donc  $G \cong C_{pq}$ . ✓

On conclut cette partie avec des applications du premier théorème d'isomorphisme, que l'on rappelle ici car elles sont classiques.

**Théorème 1.35.** Soit  $G$  un groupe, soit  $H$  un sous-groupe normal de  $G$  et soit  $K$  un sous-groupe de  $G$ .

- (1) **(Deuxième théorème d'isomorphisme)** Alors  $H \cap K$  est un sous-groupe normal de  $K$  et  $H$  est un sous-groupe normal de  $HK$  et les groupes  $K/H \cap K$  et  $HK/H$  sont isomorphes.
- (2) **(Troisième théorème d'isomorphisme)** On suppose de plus que  $K$  est normal dans  $G$  et que  $H \subset K$ . Alors  $K/H$  est un sous-groupe normal de  $G/H$  et les groupes  $(G/H)/(K/H)$  et  $G/K$  sont isomorphes.

*Démonstration.* Voir travaux dirigés

- (1) Puisque  $H \triangleleft G$ , on sait que  $HK$  est un sous-groupe de  $G$  et que  $H \triangleleft HK$ . De plus,  $H \cap K \triangleleft K$ . Donc les quotients sont bien des groupes. On considère le morphisme de groupes naturel  $f: K \hookrightarrow HK \twoheadrightarrow HK/H$ . Alors  $f$  est surjectif, car pour tout  $(h, k) \in H \times K$  on a  $\overline{hk} = \overline{k}$  dans  $HK/H$  (on a  $k^{-1}hk \in H$  car  $H \triangleleft K$ ). De plus, il est facile de vérifier que  $\text{Ker } f = H \cap K$ . On conclut avec le premier théorème d'isomorphisme.
- (2) Soit  $\pi: G \rightarrow G/H$  la surjection canonique. Vérifions d'abord que les quotients sont bien des groupes. On a  $H \triangleleft G$  et  $K \triangleleft G$  par hypothèse. On sait que  $H \triangleleft K$ . Il reste à vérifier que  $K/H$  est normal dans  $G/H$ . Or  $K \triangleleft G$  donc  $\pi(K) \triangleleft \pi(G)$  par la proposition 1.12 et donc  $K/H \triangleleft G/H$ . Soit  $\pi': G/H \rightarrow (G/H)/(K/H)$  la surjection canonique. Alors  $\pi' \circ \pi: G \rightarrow (G/H)/(K/H)$  est un morphisme de groupes surjectif. On vérifie facilement que  $\text{Ker}(\pi' \circ \pi) = \pi^{-1}(K/H) = K$  (théorème de correspondance) et on conclut avec le premier théorème d'isomorphisme. ✓

**Définition 1.36.** Soient  $G, H$  et  $K$  trois groupes. Soient  $i: H \rightarrow G$  et  $p: G \rightarrow K$  deux morphismes de groupes. On dit que la suite de morphismes

$$1 \rightarrow H \xrightarrow{i} G \xrightarrow{p} K \rightarrow 1$$

est une **suite exacte** de groupes si les conditions suivantes sont vérifiées :

- (i)  $i$  est injectif,
- (ii)  $p$  est surjectif,
- (iii)  $\text{Im } i = \text{Ker } p$ .

**Remarque.** Le groupe  $H$  est isomorphe à  $\text{Im } i$  et  $\text{Im } i = \text{Ker } p$  est nécessairement normal dans  $G$ , donc  $H$  est isomorphe à un sous-groupe normal de  $G$ .

**Exemples.** (1) Soient  $G = C_8 = \langle g \rangle$ ,  $H = C_2 = \langle a \rangle$  avec  $a = g^4$  et  $K = C_4 = \langle k \rangle$ . Soit  $i: H \rightarrow G$  l'inclusion (on a donc  $i(a) = g^4$ ) et  $p: G \rightarrow K$  défini par  $p(g) = k$ .

Alors la suite  $1 \rightarrow H \xrightarrow{i} G \xrightarrow{p} K \rightarrow 1$  est exacte.

En effet, il est clair que  $i$  est injectif et, puisque  $k$  engendre  $K$ , que  $p$  est surjectif. On a également  $p \circ i(a) = p(g^4) = k^4 = 1$  donc  $\text{Im } i \subset \text{Ker } p$  (notons que  $\text{Im } i = \langle i(a) \rangle = \langle g^4 \rangle$ ). Enfin, soit  $x \in \text{Ker } p$ . Il existe  $n \in \mathbb{Z}$  tel que  $x = g^n$  et on a  $1 = p(x) = p(g)^n = k^n$  donc  $n = 4m$  est multiple de 4 et donc  $x = g^{4m} = i(a)^m = i(a^m) \in \text{Im } i$ . Donc  $\text{Ker } p = \text{Im } i$ .

(2) Soient  $G_1$  et  $G_2$  deux groupes. Soit  $i: G_1 \rightarrow G_1 \times G_2$  le morphisme défini par  $i(x) = (x, 1)$  pour tout  $x \in G_1$  et soit  $p: G_1 \times G_2 \rightarrow G_2$  le morphisme défini par  $p(x_1, x_2) = x_2$  pour tout  $(x_1, x_2) \in G_1 \times G_2$ .

Alors la suite  $1 \rightarrow G_1 \xrightarrow{i} G_1 \times G_2 \xrightarrow{p} G_2 \rightarrow 1$  est une suite exacte.

En effet, il est évident que  $i$  est injectif et  $p$  est surjectif, et que  $p \circ i \equiv 1$  donc  $\text{Im } i \subset \text{Ker } p$ . Enfin, soit  $(x_1, x_2) \in \text{Ker } p$ , alors  $x_2 = 1$  donc  $(x_1, x_2) = (x_1, 1) = i(x_1) \in \text{Im } i$  donc  $\text{Ker } p = \text{Im } i$ .

**Proposition 1.37.** Soit  $1 \rightarrow H \xrightarrow{i} G \xrightarrow{p} K \rightarrow 1$  une suite exacte de groupes.

Alors  $H \cong \text{Im } i$  et  $K \cong G / \text{Im } i$ . Donc si  $H$  est un sous-groupe de  $G$  et  $i$  est l'inclusion, on a  $K \cong G/H$ .

De plus,  $G$  est fini si, et seulement si,  $H$  et  $K$  sont finis et on a alors  $|G| = |H||K|$ .

**Démonstration.** En restreignant l'espace d'arrivée,  $i: H \rightarrow \text{Im } i$  est un morphisme surjectif. Il est injectif par hypothèse donc  $H \cong \text{Im } i$ .

Ensuite,  $p$  est un morphisme surjectif, dont le noyau est  $\text{Ker } p = \text{Im } i$  donc d'après le premier théorème d'isomorphisme, on a bien  $K \cong G / \text{Im } i$ . (Notons en particulier que  $\text{Im } i \triangleleft G$ .)

Si  $G$  est fini, alors  $H \cong \text{Im } i$  et  $K$  sont finis (sous-groupe et quotient de  $G$ ). Si  $H$  et  $K$  sont finis, alors  $\text{Im } i \cong H$  et  $G / \text{Im } i \cong K$  sont finis donc  $G$  est fini de cardinal  $|G| = |\text{Im } i| |G : \text{Im } i| = |H| |K|$  d'après le théorème de Lagrange. ✓

**Exemple.** On reprend la suite exacte  $1 \rightarrow G_1 \rightarrow G_1 \times G_2 \rightarrow G_2 \rightarrow 1$  de l'exemple précédent. Alors  $G_2 \cong (G_1 \times G_2) / (G_1 \times \{1\})$ .



# Groupes finis abéliens

Dans ce chapitre on décrit les groupes finis abéliens, en montrant que tout groupe fini abélien est isomorphe à un produit de groupes cycliques. L'outil essentiel pour montrer cela sera le dual du groupe.

## I. DUAL D'UN GROUPE

### A. Généralités

On cherche à imiter la construction du dual pour un espace vectoriel (rappelons que si  $E$  est un  $\mathbb{K}$ -espace vectoriel, l'espace vectoriel dual de  $E$  est  $E^* = \mathcal{L}(E, \mathbb{K})$ ; voir l'annexe A.I). Ici, le groupe multiplicatif  $\mathbb{C}^*$  joue le rôle de l'espace vectoriel standard  $\mathbb{K}$  de dimension 1.

**Définition 2.1.** Un caractère sur un groupe  $G$  est un morphisme de groupes  $\chi: G \rightarrow \mathbb{C}^*$ .

On remarque que si le groupe  $G$  est fini d'ordre  $n$ , alors pour tout caractère  $\chi: G \rightarrow \mathbb{C}^*$ , on a  $\chi(G) \subset \mu_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$ .

**Exemples.** (1) Le caractère trivial  $\mathbb{1}: G \rightarrow \mathbb{C}^*$  défini par  $g \mapsto 1$  pour tout  $g \in G$ .

(2) Pour tout  $k \in \mathbb{Z}$ , l'application  $\mu_n \rightarrow \mathbb{C}^*$  donnée par  $x \mapsto x^k$  (à valeurs dans  $\mu_n$ ) est un caractère sur  $\mu_n$ .

(3) La signature  $\varepsilon: S_n \rightarrow \mathbb{C}^*$  (à valeurs dans  $\{\pm 1\}$ ) est un caractère sur le groupe symétrique  $S_n$ . C'est le seul caractère non trivial sur  $S_n$  (Voir travaux dirigés et chapitre 5).

**Définition-Proposition 2.2.** Soit  $G$  un groupe. Notons  $\widehat{G}$  l'ensemble des caractères sur  $G$ . L'application

$$\begin{aligned} \widehat{G} \times \widehat{G} &\longrightarrow \widehat{G} \\ (\chi, \psi) &\longmapsto \chi \cdot \psi: \quad G \rightarrow \mathbb{C}^*, \\ &\quad g \mapsto \chi(g)\psi(g) \end{aligned}$$

munit  $\widehat{G}$  d'une structure de groupe dont l'élément neutre est le caractère trivial  $\mathbb{1}$  et tel que, pour tout  $\chi \in \widehat{G}$  et tout  $g \in G$  on a  $\chi^{-1}(g) = \chi(g)^{-1}$ . Le groupe  $\widehat{G}$  est abélien, et il est appelé le **groupe dual** de  $G$ .

*Démonstration.* Exercice.

Puisque  $\mathbb{C}^*$  est un groupe (muni de la multiplication), on sait que l'ensemble  $\mathcal{F}(G, \mathbb{C}^*)$  des applications de  $G$  dans  $\mathbb{C}^*$  est aussi un groupe, dont la loi est définie par :

$$\forall (\alpha, \beta) \in (\mathcal{F}(G, \mathbb{C}^*))^2, \alpha\beta: G \rightarrow \mathbb{C}^*: \forall g \in G, (\alpha\beta)(g) = \alpha(g)\beta(g)$$

et donc l'élément neutre est l'application constante égale à 1, c'est-à-dire  $\mathbb{1}$  et l'inverse de  $\alpha \in \mathcal{F}(G, \mathbb{C}^*)$  est donné par  $\alpha^{-1}: g \mapsto \alpha(g)^{-1}$  pour tout  $g \in G$ . Ce groupe est abélien car  $\mathbb{C}^*$  est abélien.

Montrons que  $\widehat{G}$  est un sous-groupe de  $\mathcal{F}(G, \mathbb{C}^*)$ .

L'ensemble  $\widehat{G}$  n'est pas vide, car il contient  $\mathbb{1}$ .

Soit  $(\chi, \psi) \in \widehat{G}^2$ . Alors  $\chi \cdot \psi \in \widehat{G}$ . En effet, pour tout  $(g, h) \in G^2$ , on a  $(\chi \cdot \psi)(gh) = \chi(gh)\psi(gh) = \chi(g)\chi(h)\psi(g)\psi(h) = \chi(g)\psi(g)\chi(h)\psi(h) = (\chi \cdot \psi)(g)(\chi \cdot \psi)(h)$  donc  $\chi \cdot \psi$  est un morphisme de groupes (on a utilisé le fait que  $\mathbb{C}^*$  est abélien).

Soit maintenant  $\chi \in \widehat{G}$ . Alors  $\chi^{-1}$  est un morphisme de groupes. En effet, si  $(g, h) \in \widehat{G}^2$ , on a  $\chi^{-1}(gh) = (\chi(gh))^{-1} = (\chi(g)\chi(h))^{-1} = \chi(g)^{-1}\chi(h)^{-1} = \chi^{-1}(g)\chi^{-1}(h)$  car  $\mathbb{C}^*$  est abélien. Donc  $\chi^{-1} \in \widehat{G}$ . ✓

La preuve est laissée en exercice, ainsi que la vérification du résultat suivant.

**Proposition 2.3.** Si  $f: G \rightarrow H$  est un morphisme de groupes, alors l'application

$$\begin{aligned}\widehat{f}: \widehat{H} &\rightarrow \widehat{G} \\ \chi &\mapsto \chi \circ f\end{aligned}$$

est un morphisme de groupes.

*Démonstration.* Exercice. Voir travaux dirigés

Tout d'abord, pour tout  $\chi \in \widehat{H}$  l'application  $\chi \circ f: G \rightarrow \mathbb{C}^*$  est un morphisme de groupes, donc un élément de  $\widehat{G}$ . Donc  $\widehat{f}$  est bien définie.

Soit  $(\chi, \psi) \in \widehat{H}^2$ . Pour tout  $g \in G$  on a

$$\widehat{f}(\chi\psi)(g) = (\chi\psi)(f(g)) = \chi(f(g))\psi(f(g)) = ((\chi \circ f)(\psi \circ f))(g) = (\widehat{f}(\chi)\widehat{f}(\psi))(g)$$

donc  $\widehat{f}(\chi\psi) = \widehat{f}(\chi)\widehat{f}(\psi)$ . Donc  $\widehat{f}$  est un morphisme de groupes. ✓

**Corollaire 2.4.** Si  $G$  et  $H$  sont des groupes, alors les groupes  $\widehat{G \times H}$  et  $\widehat{G} \times \widehat{H}$  sont isomorphes.

*Démonstration.* Considérons les morphismes de groupes

$$i: G \rightarrow G \times H, g \mapsto (g, 1), \quad j: H \rightarrow G \times H, h \mapsto (1, h)$$

Ils induisent les morphismes  $\widehat{i}: \widehat{G \times H} \rightarrow \widehat{G}$  et  $\widehat{j}: \widehat{G \times H} \rightarrow \widehat{H}$  et on peut définir l'application

$$\begin{aligned}\theta: \widehat{G \times H} &\longrightarrow \widehat{G} \times \widehat{H} \\ \chi &\longmapsto (\widehat{i}(\chi), \widehat{j}(\chi)) = (\chi \circ i, \chi \circ j)\end{aligned}$$

qui est un morphisme de groupes car  $\widehat{i}$  et  $\widehat{j}$  sont des morphismes de groupes.

Enfin, notons  $p: G \times H \rightarrow G$  et  $q: G \times H \rightarrow H$  les projections naturelles (ce sont des morphismes de groupes). On introduit l'application  $\theta': \widehat{G} \times \widehat{H} \rightarrow \widehat{G \times H}$  définie par  $\theta'(\varphi, \psi) = (\varphi \circ p)(\psi \circ q)$  (qui à  $(g, h) \in G \times H$  associe  $\varphi(g)\psi(h)$ ). Vérifions que  $\theta'$  est la bijection réciproque de  $\theta$  :

➤ Soit  $(\varphi, \psi) \in \widehat{G} \times \widehat{H}$ . Notons  $\chi = \theta'(\varphi, \psi)$ . Alors  $\theta \circ \theta'(\varphi, \psi) = (\chi \circ i, \chi \circ j)$ .

Soit  $g \in G$ . On a  $\chi \circ i(g) = \chi(g, 1) = \varphi(g)\psi(1) = \varphi(g)$  donc  $\chi \circ i = \varphi$ . De même,  $\chi \circ j = \psi$ .

Finalement,  $\theta \circ \theta'(\varphi, \psi) = (\varphi, \psi)$ .

➤ Soit  $\chi \in \widehat{G \times H}$ . Alors  $\theta' \circ \theta(\chi) = (\chi \circ i \circ p)(\chi \circ j \circ q)$ .

Soit  $(g, h) \in G \times H$ . On a  $\chi \circ i \circ p(g, h) = \chi(i(g)) = \chi(g, 1)$  et de même  $\chi \circ j \circ q(g, h) = \chi(1, h)$ . On en déduit que

$$\begin{aligned}(\theta' \circ \theta(\chi))(g, h) &= ((\chi \circ i \circ p)(\chi \circ j \circ q))(g, h) = ((\chi \circ i \circ p)(g, h))((\chi \circ j \circ q)(g, h)) \\ &= \chi(g, 1)\chi(1, h) = \chi((g, 1)(1, h)) = \chi(g, h)\end{aligned}$$

car  $\chi$  est un morphisme de groupes et finalement  $\theta' \circ \theta(\chi) = \chi$ . ✓

## B. Exemple fondamental : le cas d'un groupe cyclique

Comme premier exemple, on détermine le groupe dual d'un groupe cyclique.

**Proposition 2.5.** Soit  $G = \langle g \rangle$  un groupe cyclique d'ordre  $n$ . Pour tout  $\omega \in \mu_n$ , il existe un unique  $\chi_\omega \in \widehat{G}$  tel que  $\chi_\omega(g) = \omega$ . L'application

$$\begin{aligned}\mu_n &\longrightarrow \widehat{G} \\ \omega &\longmapsto \chi_\omega\end{aligned}$$

est un isomorphisme de groupes. En particulier un groupe cyclique est isomorphe à son groupe dual.

*Démonstration.* D'après le théorème 1.30, pour tout  $\omega \in \mu_n$ , il existe un unique morphisme de groupes  $\chi_\omega: G \rightarrow \mathbb{C}^*$  tel que  $\chi_\omega(g) = \omega$ .

Soit  $\psi: \widehat{G} \rightarrow \mathbb{C}^*$  l'application définie par  $\psi(\chi) = \chi(g)$  pour tout  $\chi \in \widehat{G}$ . Par définition de la structure de groupe sur  $\widehat{G}$ , c'est un morphisme de groupes.

On remarque que  $g^n = 1$  donc  $\chi(g)^n = \chi(g^1) = \chi(1) = 1$  donc  $\psi$  est à valeurs dans  $\mu_n$  et, pour tout  $\omega \in \mu_n$ , le caractère  $\chi_\omega$  est l'unique antécédent de  $\omega$  par  $\psi$ .

Donc  $\psi: \widehat{G} \rightarrow \mu_n$  est un isomorphisme de groupes, dont la réciproque  $\psi^{-1}: \mu_n \rightarrow \widehat{G}$  est donnée par  $\psi^{-1}(\omega) = \chi_\omega$ .

Enfin,  $G$  est cyclique d'ordre  $n$  donc  $G \cong C_n \cong \mu_n \cong \widehat{G}$ . ✓

**Corollaire 2.6.** Si  $G$  est isomorphe à un produit direct fini de groupes cycliques, alors les groupes  $G$  et  $\widehat{G}$  sont isomorphes.

*Démonstration.* Posons  $G = G_1 \times \cdots \times G_n$  avec  $G_1, \dots, G_n$  des groupes cycliques. Alors  $\widehat{G} \cong \widehat{G}_1 \times \cdots \times \widehat{G}_n \cong G_1 \times \cdots \times G_n \cong G$  puisque les  $G_i$  sont cycliques. ✓

## C. Le théorème de prolongement

**Théorème 2.7.** Soit  $G$  un groupe abélien fini et soit  $H \subset G$  un sous-groupe. Il existe, pour tout  $\psi \in \widehat{H}$ , un élément  $\tilde{\psi} \in \widehat{G}$  tel que  $\tilde{\psi}|_H = \psi$ .

$$\begin{array}{ccc} H & \xrightarrow{\quad} & G \\ & \searrow \psi & \swarrow \tilde{\psi} \\ & \mathbb{C}^* & \end{array}$$

*Démonstration.* Soit  $G$  un groupe abélien fini, soit  $H \subset G$  un sous-groupe de  $G$  et soit  $\psi \in \widehat{H}$ .

Considérons l'ensemble  $\mathcal{E}$  des paires  $(K, \chi)$  où  $K$  est un sous-groupe de  $G$  contenant  $H$  et  $\chi \in \widehat{K}$  est un caractère tel que  $\chi|_H = \psi$ . L'ensemble  $\mathcal{E}$  n'est pas vide puisque  $(H, \psi)$  est dans  $\mathcal{E}$ . On peut donc considérer le nombre entier

$$m = \max\{|K|, (K, \chi) \in \mathcal{E}\} \in \mathbb{N}^*.$$

Soit  $(K, \chi)$  un élément de  $\mathcal{E}$  tel que  $|K| = m$ . Montrons que  $K = G$ , ce qui donnera le résultat recherché.

Par l'absurde, si  $K \subsetneq G$ , il existe  $g \in G \setminus K$ . Considérons le sous-groupe  $N = K\langle g \rangle$ . On a  $K \subsetneq N$ . Nous allons démontrer qu'il existe  $\varphi \in \widehat{N}$  tel que  $\varphi|_K = \chi$ , on aura donc  $(N, \varphi) \in \mathcal{E}$ , ce qui contredira la maximalité de  $|K|$ .

Les éléments de  $N$  sont de la forme  $xg^k$  avec  $x \in K$  et  $k \in \mathbb{Z}$ . Cette écriture n'est pas unique.

On veut définir  $\varphi(xg^k)$ . On doit avoir  $\varphi(xg^k) = \varphi(x)\varphi(g^k) = \chi(x)\varphi(g)^k$  puisque  $\varphi$  doit être un morphisme qui prolonge  $\chi$ . Si de plus  $g^k \in K$ , alors  $\varphi(g)^k = \varphi(g^k) = \chi(g^k)$ .

L'ensemble  $\{t \in \mathbb{Z} \mid g^t \in K\}$  est un sous-groupe de  $\mathbb{Z}$ , il existe donc un unique  $d \in \mathbb{N}$  tel que  $\{t \in \mathbb{Z} \mid g^t \in K\} = d\mathbb{Z}$ . On doit avoir  $\varphi(g)^d = \chi(g^d)$  d'après ce qui précède.

Soit donc  $\omega \in \mathbb{C}^*$  tel que  $\omega^d = \chi(g^d)$  (si  $\varphi(g)$  existait,  $\omega$  serait une valeur naturelle possible pour  $\varphi(g)$ ). Si  $t = dq \in d\mathbb{Z}$  avec  $q \in \mathbb{Z}$ , on a alors  $\varphi(g^t) = \varphi(g^d)^q = (\omega^d)^q = \omega^t$ .

Il est donc naturel de poser  $\varphi(xg^k) = \chi(x)\omega^k$ .

Vérifions que  $\varphi$  est bien défini. Si  $xg^k = yg^\ell$  avec  $y \in K$  et  $\ell \in \mathbb{Z}$ , alors  $g^{\ell-k} = y^{-1}x \in K$  donc  $t := \ell - k \in d\mathbb{Z}$ . On a donc

$$\chi(y)\omega^\ell = \chi(y)\omega^{k+t} = \chi(y)\chi(g^t)\omega^k = \chi(yg^t)\omega^k = \chi(yg^{\ell-k})\omega^k = \chi(x)\omega^k.$$

Donc  $\varphi$  est bien définie.

On vérifie facilement que  $\varphi$  est un morphisme de groupes ( $G$  est abélien) et  $\varphi|_K = \chi$  par construction, donc  $\varphi|_H = \psi$  et finalement  $(N, \varphi) \in \mathcal{E}$  avec  $|N| > |K| = m$ . On a obtenu une contradiction.

Donc  $K = G$  et  $\tilde{\psi} = \chi$  convient. ✓

**Corollaire 2.8.** Si  $1 \rightarrow H \xrightarrow{i} G \xrightarrow{p} K \rightarrow 1$  est une suite exacte de groupes finis abéliens, alors la suite  $1 \rightarrow \hat{K} \xrightarrow{\hat{p}} \hat{G} \xrightarrow{\hat{i}} \hat{H} \rightarrow 1$  est exacte.

*Démonstration.* Vérifions que  $\hat{p}$  est injectif. Soit  $\chi \in \hat{K}$  tel que  $\hat{p}(\chi) = 1$ , c'est-à-dire que pour tout  $g \in G$  on a  $\chi \circ p(g) = 1$ . Donc pour tout  $k \in \text{Im } p$  on a  $\chi(k) = 1$ . Mais par hypothèse  $\text{Im } p = K$  donc  $\chi = 1$ . Donc  $\text{Ker } \hat{p} = \{1\}$  et  $\hat{p}$  est injectif.

Vérifions que  $\hat{i}$  est surjectif. Soit  $\varphi \in \hat{H}$ . (Moralement, on va prolonger  $\varphi$  à  $G$  mais il faut passer par le sous-groupe  $\text{Im}(i)$  de  $G$ .) Soit  $j: H \rightarrow \text{Im } i$  l'isomorphisme obtenu à partir de  $i$  en restreignant le groupe d'arrivée. On a donc :

$$\begin{array}{ccccc} & & i & & \\ & \nearrow & & \searrow & \\ H & \xrightarrow{j} & \text{Im } i & \hookrightarrow & G \\ & \searrow \varphi & \downarrow \varphi \circ j^{-1} & \nearrow \tilde{\varphi} & \\ & & \mathbb{C}^* & & \end{array}$$

où  $\tilde{\varphi}$  est obtenu grâce au théorème de prolongement, il vérifie donc  $\tilde{\varphi}|_{\text{Im } i} = \varphi \circ j^{-1}$ , donc  $\varphi = \tilde{\varphi} \circ i = \hat{i}(\tilde{\varphi}) \in \text{Im } \hat{i}$ . Donc  $\hat{i}$  est surjectif.

Soit maintenant  $\chi \in \hat{K}$ . Alors  $\hat{i} \circ \hat{p}(\chi) = \chi \circ p \circ i$ . Or pour tout  $h \in H$  on a  $p \circ i(h) = 1$  donc pour tout  $h \in H$  on a  $\chi \circ p \circ i(h) = 1$ . On en déduit que  $\hat{i} \circ \hat{p}(\chi) = 1$  et donc que  $\text{Im } \hat{p} \subset \text{Ker } \hat{i}$ .

Enfin, soit  $\psi \in \text{Ker } \hat{i}$ , c'est-à-dire que  $\psi \circ i = 1$ . Donc pour tout  $h \in H$  on a  $\psi(i(h)) = 1$ , c'est-à-dire que  $\text{Ker } p = \text{Im } i \subset \text{Ker } \psi$ . On cherche  $\chi \in \hat{K}$  tel que  $\psi = \hat{p}(\chi) = \chi \circ p$ . D'après le premier théorème d'isomorphisme,  $p: G \rightarrow K$  induit un isomorphisme  $\alpha: G/\text{Ker } p \rightarrow K$  tel que  $\alpha \circ \pi = p$ , où  $\pi: G \rightarrow G/\text{Ker } p$  est la projection canonique. Or  $\text{Ker } p \subset \text{Ker } \psi$  donc d'après le théorème de factorisation,  $\psi$  induit un morphisme  $\bar{\psi}: G/\text{Ker } p = G/\text{Im } i \rightarrow \mathbb{C}^*$  tel que  $\bar{\psi} \circ \pi = \psi$ . On pose  $\chi = \bar{\psi} \circ \alpha^{-1}$ . On a alors  $\hat{p}(\chi) = \chi \circ p = \bar{\psi} \circ \alpha^{-1} \circ p = \bar{\psi} \circ \pi = \psi$  donc  $\psi \in \text{Im } \hat{p}$  et donc  $\text{Ker } \hat{i} = \text{Im } \hat{p}$ .

$$\begin{array}{ccccc} G & \xrightarrow{p} & K \\ \pi \searrow & & \nearrow \alpha \\ & G/\text{Ker } p & \\ \psi \searrow & \downarrow \bar{\psi} & \nearrow ? \\ & \mathbb{C}^* & \end{array}$$

**Corollaire 2.9.** On a  $|G| = |\widehat{G}|$  pour tout groupe fini abélien  $G$ .

*Démonstration.* D'après la proposition 2.5, le résultat est vrai pour les groupes cycliques.

Nous allons démontrer le résultat par récurrence sur  $|G|$ .

➤ Initialisation. Si  $|G| \leq 3$ , alors  $G$  est cyclique (éventuellement trivial) donc  $\widehat{G} \cong G$  et donc  $|\widehat{G}| = |G|$ .

➤ Hérédité. Soit  $G$  un groupe abélien d'ordre  $n \geq 4$ . Supposons que pour tout groupe abélien  $H$  d'ordre  $\leq n-1$  on a  $|H| = |\widehat{H}|$ .

Si  $G$  est simple alors  $G$  est cyclique d'après le corollaire 1.29, donc  $|G| = |\widehat{G}|$ .

Supposons donc que  $G$  n'est pas simple, et soit  $H$  un sous-groupe propre (normal) de  $G$ .

Soit  $K = G/H$ . Alors on a une suite exacte  $1 \rightarrow H \xrightarrow{i} G \xrightarrow{\pi} K \rightarrow 1$  où  $i$  est l'inclusion et  $\pi$  est la projection canonique. On en déduit une suite exacte  $1 \rightarrow \widehat{K} \rightarrow \widehat{G} \rightarrow \widehat{H} \rightarrow 1$  d'après le corollaire 2.8.

Les groupes  $H$  et  $K$  sont abéliens finis, avec  $|H| < n$  et  $|K| < n$ , donc l'hypothèse de récurrence s'applique et on a  $|\widehat{H}| = |H|$  et  $|\widehat{K}| = |K|$ . En particulier,  $\widehat{H}$  et  $\widehat{K}$  sont finis et on a  $|\widehat{G}| = |\widehat{H}||\widehat{K}| = |H||K| = |G|$  d'après la proposition 1.37. ✓

**Remarque.** Le résultat n'est plus vrai si on ne suppose pas  $G$  abélien. Par exemple  $|\widehat{S}_3| = 2 < |S_3|$ . Voir travaux dirigés

La signature  $\varepsilon: S_3 \rightarrow \mathbb{C}^*$  est un caractère non trivial, donc  $|\widehat{S}_3| \geq 2$ .

Notons  $\tau = (12)$  la transposition qui échange 1 et 2 et  $\sigma = (123)$  le 3-cycle. Alors  $(23) = \sigma(12)\sigma^{-1}$  et  $(13) = \sigma^{-1}(12)\sigma$ . De plus,  $\sigma = (13)(12) = \sigma^{-1}(12)\sigma(12)$  et  $\sigma^{-1} = (12)\sigma^{-1}(12)\sigma$ .

Soit maintenant  $\chi: \widehat{S}_3 \rightarrow \mathbb{C}^*$  un caractère. On remarque que  $\chi((12))^2 = \chi((12)) = \chi(\text{id}) = 1$  donc  $\chi((12)) \in \{\pm 1\}$ . De plus, puisque  $\mathbb{C}^*$  est abélien et  $\chi$  est un morphisme de groupes,  $\chi((23)) = \chi((12)) = \chi((13))$  et  $\chi(\sigma) = \chi((12))^2 = 1$  et  $\chi(\sigma^{-1}) = 1$ . On en déduit que  $\chi$  est entièrement déterminé par  $\chi((12))$ .

Si  $\chi((12)) = 1$ , alors  $\chi = \mathbb{1}$ .

Si  $\chi((12)) = -1$ , alors  $\chi((23)) = -1 = \chi((13))$  donc  $\chi = \varepsilon$ .

Finalement,  $\widehat{S}_3 = \{\mathbb{1}, \varepsilon\}$ .

On remarquera plus tard que c'est vrai pour tout  $n \in \mathbb{N}, n \geq 3$  : on a  $|\widehat{S}_n| = 2$  et  $\widehat{S}_n = \{\mathbb{1}, \varepsilon\}$ .

**Théorème 2.10** (bidualité). Si  $G$  est un groupe fini abélien, le morphisme de groupes

$$\begin{aligned} G &\longrightarrow \widehat{\widehat{G}} \\ g &\longmapsto \varepsilon_g: \widehat{G} \rightarrow \mathbb{C}^* \\ &\quad \psi \mapsto \psi(g) \end{aligned}$$

est un isomorphisme.

*Démonstration.* Vérifions d'abord que  $\varepsilon_g$  est bien un élément de  $\widehat{\widehat{G}}$ . Soit  $(\psi, \varphi) \in \widehat{\widehat{G}}^2$ . Alors  $\varepsilon_g(\psi\varphi) = (\psi\varphi)(g) = \psi(g)\varphi(g) = \varepsilon_g(\psi)\varepsilon_g(\varphi)$  par définition de la loi sur  $\widehat{\widehat{G}}$ . Donc  $\varepsilon_g$  est bien un morphisme de groupes.

Notons  $f: G \rightarrow \widehat{\widehat{G}}$  l'application de l'énoncé.

Vérifions d'abord que  $f$  est un morphisme de groupes. Soit  $(g, h) \in G^2$ . Alors  $f(gh) = \varepsilon_{gh}$ . Soit  $\psi \in \widehat{\widehat{G}}$ . Alors

$$f(gh)(\psi) = \varepsilon_{gh}(\psi) = \psi(gh) = \psi(g)\psi(h) = \varepsilon_g(\psi)\varepsilon_h(\psi) = (\varepsilon_g\varepsilon_h)(\psi)$$

où la dernière égalité vient de la définition du produit dans  $\widehat{\widehat{G}}$ . On en déduit que  $f(gh) = \varepsilon_g\varepsilon_h = f(g)f(h)$ .

Montrons que  $f$  est un isomorphisme. Soit  $g \in \text{Ker } f$ , on a donc  $\varepsilon_g = 1$ , c'est-à-dire que pour tout  $\psi \in \widehat{G}$  on a  $\psi(g) = \varepsilon_g(\psi) = 1$ . Supposons que  $g \neq 1$ . Alors le sous-groupe  $H = \langle g \rangle$  de  $G$  est cyclique et d'ordre  $d > 1$  (puisque  $G$  est fini). Soit  $\omega$  une racine  $d^{\text{ième}}$  de l'unité avec  $\omega \neq 1$  (elle existe puisque  $d > 1$ ). On sait qu'il existe un unique  $\alpha \in \widehat{H}$  tel que  $\alpha(g) = \omega$  d'après le théorème 1.30. D'après le théorème de prolongement, il existe  $\psi \in \widehat{G}$  tel que  $\psi|_H = \alpha$ . En particulier,  $\psi(g) = \alpha(g) = \omega \neq 1$  : on a obtenu une contradiction. Donc  $g = 1$  et donc  $\text{Ker } f = \{1\}$ .

Enfin, puisque  $G$  est abélien fini, on a  $|G| = |\widehat{G}|$ . De plus,  $\widehat{G}$  est abélien (toujours) et fini d'après ce qui précède, donc  $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$ . On en déduit finalement que  $f$  est un isomorphisme. ✓

## II. APPLICATION À LA CLASSIFICATION DES GROUPES FINIS ABÉLIENS

**Définition 2.11.** Soit  $G$  un groupe fini. L'**exposant** de  $G$  est le nombre entier défini par

$$\exp(G) = \text{ppcm}\{o(g), g \in G\}$$

**Exemples.**  $\exp(C_n) = n$ ,  $\exp(C_2 \times C_2) = 2$ ,  $\exp(S_3) = 6$ .

On peut vérifier que  $\exp(S_n) = \text{ppcm}(1, 2, \dots, n)$ .

Il est clair que pour tout  $k$  avec  $1 \leq k \leq n$ , chaque  $k$ -cycle est d'ordre  $k$  donc  $\exp(S_n)$  est un multiple de  $\text{ppcm}(1, 2, \dots, n)$ .

Soit maintenant  $\sigma$  un élément de  $S_n$ . On sait que  $\sigma$  peut s'écrire comme un produit de cycles disjoints  $\gamma_1 \cdots \gamma_r$ . Notons  $d_i$  la longueur de  $\gamma_i$  pour tout  $i$ . Puisque les  $\gamma_i$  sont disjoints, ils commutent deux à deux, donc l'ordre de  $\sigma$  est  $\text{ppcm}(d_1, \dots, d_r)$ . Or chacun des  $d_i$  est dans  $\{1, 2, \dots, n\}$ , donc l'ordre de  $\sigma$  divise  $\text{ppcm}(1, 2, \dots, n)$ . On en déduit finalement que  $\exp(S_n)$  divise  $\text{ppcm}(1, 2, \dots, n)$  et donc qu'on a bien l'égalité.

**Lemme 2.12.** Soit  $G$  un groupe fini abélien. Il existe  $g \in G$  tel que  $o(g) = \exp(G)$ .

*Démonstration.* Voir travaux dirigés

Soit  $G$  un groupe abélien fini, et notons  $\exp(G) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  où  $p_1, \dots, p_r$  sont des nombres premiers deux à deux distincts et  $\alpha_1, \dots, \alpha_r > 0$  sont des nombres entiers. Soit  $i \in \{1, \dots, r\}$ . Par définition de  $\exp(G)$ , il existe  $y_i \in G$  tel que  $o(y_i) = p_i^{\alpha_i} q_i$  où  $q_i$  est un nombre entier premier avec  $p_i$ . D'après la proposition 1.23, l'élément  $x_i = y_i^{q_i}$  est alors un élément d'ordre  $p_i^{\alpha_i}$  de  $G$  et l'élément  $x = x_1 \cdots x_r$  est alors un élément d'ordre  $\exp(G)$  de  $G$ . ✓

**Remarque.** Attention, le résultat est faux si on retire l'hypothèse que le groupe est abélien. Par exemple,  $\exp(S_3) = 6$  mais  $S_3$  ne contient aucun élément d'ordre 6.

**Théorème 2.13.** Un groupe fini abélien est isomorphe à un produit direct de groupes cycliques.

*Démonstration.* On montre le résultat par récurrence sur  $|G|$ .

- Si  $|G| \in \{1, 2, 3\}$ , le groupe est trivial ou cyclique, le résultat est donc vrai.
- Soit  $G$  un groupe abélien d'ordre  $> 3$  et supposons le résultat montré pour tous les groupes abéliens d'ordre  $< |G|$ . Soit  $g \in G$  un élément d'ordre  $m = \exp(G) > 1$ . Soit  $\omega$  une racine primitive  $m^{\text{ième}}$  de l'unité et soit  $\chi \in \widehat{\langle g \rangle}$  l'unique caractère tel que  $\chi(g) = \omega$ . Notons que l'image de  $\chi$  est  $\mu_m$  puisque  $\chi$  est à valeurs dans  $\mu_m$  et  $\omega$  engendre  $\mu_m$ ; de

plus,  $|\langle g \rangle| = |\mu_m|$  donc  $\chi$  induit un isomorphisme de  $\langle g \rangle$  sur  $\mu_m$ . En particulier,  $\chi$  est injectif.

Il existe, par le théorème 2.7,  $\chi' \in \widehat{G}$  qui prolonge  $\chi$ . Puisque  $m = \exp(G)$ , on a  $\chi'(G) \subset \mu_m$ . Considérons alors le morphisme de groupes

$$\begin{aligned}\Phi: G &\longrightarrow \mu_m \times G/\langle g \rangle \\ x &\longmapsto (\chi'(x), \pi(x))\end{aligned}$$

où  $\pi: G \rightarrow G/\langle g \rangle$  est la surjection canonique. Le morphisme  $\Phi$  est injectif : en effet, soit  $x \in \text{Ker } \Phi$ , alors  $\pi(x) = 1$  donc  $x \in \langle g \rangle$  et donc  $1 = \chi'(x) = \chi(x)$  donc  $x = 1$  puisque  $\chi$  est injectif. De plus,  $|\mu_m||G/\langle g \rangle| = |\langle g \rangle| \frac{|G|}{|\langle g \rangle|} = |G|$  donc  $\Phi$  est un isomorphisme. L'hypothèse de récurrence, appliquée au groupe  $G/\langle g \rangle$ , permet de conclure que  $G$  est isomorphe à un produit de groupes cycliques. ✓

**Corollaire 2.14.** Si  $G$  est un groupe abélien fini, alors les groupes  $G$  et  $\widehat{G}$  sont isomorphes.

*Démonstration.* On applique le théorème 2.13 et le corollaire 2.6. ✓

*Remarque.* Il n'y a pas d'isomorphisme canonique entre  $G$  et  $\widehat{G}$ .

**Corollaire 2.15.** Soit  $G$  un groupe fini abélien avec  $|G| = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ , où  $p_1, \dots, p_t$  sont des nombres premiers deux à deux distincts et  $\alpha_1, \dots, \alpha_t$  sont dans  $\mathbb{N}^*$ . Il existe des sous-groupes  $H_1, \dots, H_t$  de  $G$ , d'ordres respectifs  $p_1^{\alpha_1}, \dots, p_t^{\alpha_t}$ , tels que

$$G \simeq H_1 \times \cdots \times H_t$$

avec pour tout  $i \in \{1, \dots, t\}$ ,  $H_i = \{g \in G \mid o(g) \text{ est une puissance de } p_i\}$ .

*Démonstration.* Puisque  $G$  est un groupe fini abélien, il existe des groupes cycliques  $K_1, \dots, K_s$  tels que  $G \cong K_1 \times \cdots \times K_s$ . On applique le théorème chinois à chacun des  $K_j$ , qui se décompose donc en produit de groupes cycliques dont les ordres sont des puissances de nombres premiers distincts. De plus, chaque  $K_j$  est isomorphe à un sous-groupe de  $G$ , donc les nombres premiers qui apparaissent dans sa décomposition sont dans  $\{p_1, \dots, p_t\}$ . On peut donc écrire, pour tout  $j$  avec  $1 \leq j \leq s$ ,  $K_j = L_{j,p_1} \times \cdots \times L_{j,p_t}$  où  $L_{j,p_i}$  est soit le groupe trivial, soit un groupe cyclique dont l'ordre est une puissance de  $p_i$  inférieure à  $p_i^{\alpha_i}$ . On pose alors  $H'_i = L_{1,p_i} \times \cdots \times L_{s,p_i}$  et on obtient un isomorphisme  $\varphi: G \xrightarrow{\sim} H'_1 \times \cdots \times H'_t$ . Pour tout  $i$  on a  $|H'_i| = p_i^{\beta_i}$  avec  $0 \leq \beta_i \leq \alpha_i$ . De plus,  $|G| = \prod_{i=1}^t |H'_i| = p_1^{\beta_1} \cdots p_t^{\beta_t}$ , donc pour tout  $i$  on a  $\beta_i = \alpha_i$  et donc  $|H'_i| = p_i^{\alpha_i}$ .

Pour tout  $i \in \llbracket 1; t \rrbracket$ , soit  $H_i = \varphi^{-1}(\{1\}^{i-1} \times H'_i \times \{1\}^{t-i}) \subset G$ . On a alors  $H_i \cong H'_i$  et  $G \cong H_1 \times \cdots \times H_t$ .

Il reste à vérifier que  $H_i = \{g \in G \mid o(g) \text{ est une puissance de } p_i\}$ . Puisque  $|H_i| = p_i^{\alpha_i}$ , il est clair que  $H_i \subset \{g \in G \mid o(g) \text{ est une puissance de } p_i\}$  d'après le théorème de Lagrange. Réciproquement, soit  $g \in G$  tel que  $o(g)$  est une puissance de  $p_i$ . Posons  $\varphi(g) = (h'_1, \dots, h'_t)$  avec  $h'_k \in H'_k$  pour tout  $k \in \llbracket 1; t \rrbracket$  et posons  $h_k = (1, \dots, 1, h'_k, 1, \dots, 1) \in \varphi(H_k)$  avec  $h'_k$  dans la  $k^{\text{ième}}$  position pour tout  $k \in \llbracket 1; t \rrbracket$ . Alors  $\varphi(g) = h_1 \cdots h_t$ . Les  $h_k$  commutent et de plus leurs ordres sont premiers entre eux deux à deux. Donc  $o(g) = o(\varphi(g)) = o(h_1 \cdots h_t) = \prod_{k=1}^t o(h_k)$ . On en déduit que pour tout  $k \neq i$  on doit avoir  $h_k = 1$  donc  $\varphi(g) = h_i \in \varphi(H_i)$  et finalement  $g \in H_i$  puisque  $\varphi$  est un isomorphisme. On a donc bien l'égalité. ✓

**Théorème 2.16.** Soit  $G$  un groupe fini abélien non trivial. Il existe un nombre entier  $r \in \mathbb{N}^*$  une suite  $(d_1, \dots, d_r)$  de nombres entiers supérieurs ou égaux à 2 tels que  $d_1 \mid d_2 \mid \dots \mid d_{r-1} \mid d_r$  et

$$G \simeq C_{d_1} \times \dots \times C_{d_r}$$

Cette suite de nombres entiers détermine uniquement le groupe  $G$  à isomorphisme près, et est appelée la suite des **facteurs invariants** de  $G$ .

**Remarque.** On a  $\exp(G) = d_r$ .

Notons que  $\exp(G) = \exp(C_{d_1} \times \dots \times C_{d_r})$ . Le générateur de  $C_{d_r}$  est d'ordre  $d_r$ , donc  $d_r \mid \exp(G)$ . Soit maintenant  $x$  un élément quelconque de  $C_{d_1} \times \dots \times C_{d_r}$ . Posons  $x = (x_1, \dots, x_r)$  avec  $x_i \in C_{d_i}$  pour tout  $i$  avec  $1 \leq i \leq r$  et soit  $y_i = (1, \dots, 1, x_i, 1, \dots, 1)$ . Alors  $x = y_1 \dots y_r$  et les  $y_i$  commutent donc  $o(x) = \text{ppcm}\{o(y_i) \mid 1 \leq i \leq r\}$ . De plus, pour tout  $i$  on a  $o(x_i) = o(y_i) \mid d_i \mid d_r$  donc  $o(x) \mid d_r$  et donc  $\exp(G) \mid d_r$ .

**Théorème 2.16, démonstration de l'existence.** Grâce au théorème précédent, on a un isomorphisme

$$G \cong \prod_{i=1}^t \left( \prod_{j=1}^{s_i} L_{j_i, p_i} \right)$$

avec  $p_1, \dots, p_t$  des nombres premiers deux à deux distincts et  $L_{j_i, p_i}$  un groupe cyclique d'ordre une puissance de  $p_i$ . Quitte à réordonner les  $L_{j_i, p_i}$ , on peut supposer que  $|L_{1, p_1}| \mid |L_{2, p_1}| \mid \dots \mid |L_{s_1, p_1}|$ .

Soit  $D_r = L_{s_1, p_1} \times \dots \times L_{s_t, p_t}$ . Alors  $D_r$  est un groupe cyclique grâce au théorème chinois. Notons  $d_r = |D_r|$ , on a donc  $D_r \cong C_{d_r}$ .

Soit ensuite  $D_{r-1} = L_{s_1-1, p_1} \times \dots \times L_{s_t-1, p_t}$ . De même,  $D_{r-1} \cong C_{d_{r-1}}$ . De plus, par construction on a  $d_{r-1} \mid d_r$ .

On continue jusqu'à avoir épuisé tous les  $L_{j, p}$  et on obtient l'isomorphisme recherché. ✓

**Remarque.** La démonstration de l'existence dans le théorème 2.16 montre comment, étant donnée une décomposition d'un groupe fini abélien  $G$  en produit de groupes cycliques dont les ordres sont des puissances de nombres premiers, trouver les facteurs invariants de  $G$ .

Le passage de la décomposition en termes de facteurs invariants à la décomposition à la décomposition du corollaire 2.15 se fait en décomposant chaque  $d_i$  en produit de facteurs premiers et en appliquant le théorème chinois à  $C_{d_i}$ .

Pour l'unicité (pas faite en cours – admise), nous aurons besoin du lemme suivant.

**Lemme.** Soit  $G$  un groupe abélien fini. Soit  $(x, y) \in G^2$  tel que  $x$  et  $y$  soient d'ordre maximal dans  $G$ . Alors il existe  $\theta \in \text{Aut}(G)$  tel que  $\theta(x) = y$ .

(Autrement dit, dans le vocabulaire du chapitre 4, le groupe  $\text{Aut}(G)$  opère transitivement sur l'ensemble des éléments d'ordre maximal de  $G$ .)

**Démonstration.** Remarquons d'abord qu'il y a bien des éléments d'ordre maximal dans  $G$ , car  $G$  est abélien fini donc d'après le lemme 2.12 on a  $\exp(G) = \max\{o(g) \mid g \in G\}$ .

➤ Premier cas : supposons que  $|G|$  soit une puissance d'un nombre premier  $p$ . D'après le théorème 2.13 et le théorème de Lagrange, on a un isomorphisme  $G \cong \prod_{i=1}^s L_i$  avec  $L_i$  cyclique d'ordre  $p^{a_i}$  pour tout  $i$ . Quitte à réordonner les  $L_i$ , on peut supposer que  $a_1 \leq a_2 \leq \dots \leq a_s$ . Les éléments d'ordre maximal de  $G$  sont donc d'ordre  $p^{a_s}$ . On note  $k = |\{i \in \llbracket 1; s \rrbracket \mid a_i = a_s\}|$ .

Soit  $x = (x_1, \dots, x_s)$  un élément d'ordre maximal dans  $G$ . Alors l'une des  $k$  dernières composantes  $x_i$  de  $x$  engendre  $L_i$  (car  $o(x) = \text{ppcm}\{o(x_i) \mid 1 \leq i \leq s\}$ ). Soit  $\alpha$  un générateur fixé de  $L_s$ . Notons que l'unique morphisme de groupes  $L_i \rightarrow L_s$  qui envoie  $x_i$  sur  $\alpha$

donné par le théorème 1.30 est un isomorphisme (surjectif car  $\alpha$  engendre  $L_s$  puis bijectif car les cardinaux sont égaux).

Soit  $x_0 = (1, 1, \dots, 1, \alpha) \in G$ . Il suffit de démontrer qu'il existe un automorphisme  $\theta$  de  $G$  tel que  $\theta(x_0) = x$  (il en existe alors également un qui envoie  $x_0$  sur  $y$  et on compose).

Soit  $H = L_1 \times \dots \times L_{i-1} \times \{1\} \times L_{i+1} \times \dots \times L_s$  et soit  $K = \langle x \rangle$ . Soit  $H' = L_1 \times \dots \times L_{s-1} \times \{1\}$  et soit  $K' = \{1\}^{s-1} \times L_s = \langle x_0 \rangle$ .

En utilisant l'isomorphisme  $L_i \cong L_s$ , on obtient un isomorphisme  $f_H: H \rightarrow H'$  défini par  $f_H(z_1, \dots, z_{i-1}, 1, z_{i+1}, \dots, \alpha^\ell) = (z_1, \dots, z_{i-1}, x_i^\ell, z_{i+1}, \dots, z_{s-1}, 1)$ .

De plus, soit  $f_K: K \rightarrow K'$  l'unique morphisme tel que  $f_K(x) = x_0$  (théorème 1.30), puisque  $x_0$  engendre  $K'$  il est surjectif et  $|K| = |K'|$  donc  $f_K$  est un isomorphisme.

De plus, on vérifie facilement que  $H' \cap K' = \{1\}$  et que  $G = H'K'$ . Comme  $G$  est abélien, tous ses sous-groupes sont normaux dans  $G$  et on a  $G \cong H' \times K'$ . Cet isomorphisme est donné par  $(z_1, \dots, z_s) \mapsto ((z_1, \dots, z_{s-1}, 1), (1, \dots, 1, z_s))$ .

On a également un isomorphisme  $H \times K \cong G$ , donné par  $(h, k) \mapsto hk$ . En effet, c'est bien un morphisme et puisque  $|H \times K| = |G|$  il suffit de vérifier qu'il est injectif. Soit donc  $(h, k)$  dans son noyau, on a donc  $h = k^{-1} \in H \cap K$ . On peut donc écrire  $h = (z_1, \dots, z_{i-1}, 1, z_{i+1}, \dots, z_s) = x^\ell = (x_1^\ell, \dots, x_s^\ell)$  pour un  $\ell \in \mathbb{Z}$ . On a donc  $x_i^\ell = 1$  mais comme  $x_i$  engendre  $L_i$ , on en déduit que  $|L_i| \mid \ell$ . Or  $|L_j| \mid |L_i| = |L_s|$  pour tout  $j$ , donc  $x^\ell = 1$  et finalement  $h = 1$  et  $k = h^{-1} = 1$ .

Enfin, en composant ces isomorphismes, on obtient un automorphisme  $\theta$  de  $G$  :

$$\theta: G \cong H' \times K' \xrightarrow{(f_H^{-1}, f_K^{-1})} H' \times K' \cong G$$

tel que  $x_0 \mapsto (1, x_0) \mapsto (1, x) \mapsto x$ .

- Cas général. Posons  $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$  où les  $p_i$  sont des nombres premiers distincts et les  $\alpha_i$  sont dans  $\mathbb{N}^*$ . On sait qu'il existe des groupes  $K_1, \dots, K_r$  tels que  $|K_i| = p_i^{\alpha_i}$  pour tout  $i$  et tels qu'on ait un isomorphisme  $\varphi: G \xrightarrow{\sim} K_1 \times \dots \times K_r$ .

Soient  $x$  et  $y$  des éléments d'ordre maximal dans  $G$ , alors  $\varphi(x) = (x_1, \dots, x_r)$  et  $\varphi(y) = (y_1, \dots, y_r)$  sont des éléments d'ordre maximal dans  $K_1 \times \dots \times K_r$ , avec  $(x_i, y_i) \in K_i^2$  pour tout  $i$ . Alors, pour tout  $i$ , les éléments  $x_i$  et  $y_i$  sont d'ordre maximal dans  $K_i$ . Grâce au premier cas, il existe un automorphisme  $\theta_i \in \text{Aut}(K_i)$  tel que  $\theta_i(x_i) = y_i$  pour tout  $i$ . On obtient alors un automorphisme  $\theta \in \text{Aut}(K_1 \times \dots \times K_r)$  en posant  $\theta(z_1, \dots, z_r) = (\theta_1(z_1), \dots, \theta_r(z_r))$  et cet automorphisme vérifie  $\theta(\varphi(x)) = \varphi(y)$ . Finalement,  $\varphi^{-1} \circ \theta \circ \varphi \in \text{Aut}(G)$  convient. ✓

**Théorème 2.16, démonstration de l'unicité.** Il faut maintenant démontrer l'unicité des « facteurs invariants ». Supposons que  $G \cong C_{d_1} \times \dots \times C_{d_r}$  et  $G \cong C_{u_1} \times \dots \times C_{u_s}$  avec  $r, n, d_1, \dots, d_r$  et  $u_1, \dots, u_s$  dans  $\mathbb{N}^*$ ,  $d_1 \mid \dots \mid d_r$  et  $u_1 \mid \dots \mid u_s$ . Notons  $a = \exp(G)$ . La remarque suivant l'énoncé du théorème montre que  $d_r = a = u_s$ .

On raisonne par récurrence sur  $r$ .

- Si  $r = 1$ , alors  $C_{d_1} = C_a \cong G \cong C_{u_1} \times \dots \times C_{u_s} = C_{u_1} \times \dots \times C_{u_{s-1}} \times C_a$ .  
En comparant les cardinaux des deux groupes, on en déduit que  $C_{u_1} \times \dots \times C_{u_{s-1}}$  est trivial, c'est-à-dire que  $s = 1 = r$  et  $u_1 = a = d_1$ .
- Soit  $r > 1$  un nombre entier tel que le résultat soit vrai au rang  $r - 1$ . Grâce aux remarques précédentes, on a un isomorphisme

$$\varphi: D := C_{d_1} \times \dots \times C_{d_{r-1}} \times C_a \cong G \cong C_{u_1} \times \dots \times C_{u_{s-1}} \times C_a =: U.$$

Soit  $\alpha$  un générateur de  $C_a$ . Soit  $g_1 = (1, \dots, 1, \alpha) \in D$  et soit  $g_2 = (1, \dots, 1, \alpha) \in U$ . Ce sont des éléments d'ordre maximal  $a$  dans leurs groupes respectifs. D'après le lemme, il existe  $\theta \in \text{Aut}(U)$  tel que  $\theta(\varphi(g_1)) = g_2$ . On a donc un isomorphisme  $\theta \circ \varphi: D \rightarrow U$  tel que  $\theta \circ \varphi(g_1) = g_2$ . On considère les surjections canoniques  $\pi_D: D \rightarrow D/\langle g_1 \rangle$  et

$\pi_U: U \rightarrow U/\langle g_2 \rangle$ . Alors  $\text{Ker}(\pi_U \circ \theta \circ \varphi) = \langle g_1 \rangle$  et par le théorème de factorisation on a un morphisme  $\psi: D/\langle g_1 \rangle \rightarrow U/\langle g_2 \rangle$ :

$$\begin{array}{ccc} D & \xrightarrow[\sim]{\theta \circ \varphi} & V \\ \pi_D \downarrow & & \downarrow \pi_U \\ D/\langle g_1 \rangle & \xrightarrow{\psi} & U/\langle g_2 \rangle, \end{array}$$

qui est un isomorphisme (exercice).

Or  $D/\langle g_1 \rangle \cong C_{d_1} \times \cdots \times C_{d_{r-1}}$ . En effet, le morphisme  $D \rightarrow C_{d_1} \times \cdots \times C_{d_{r-1}}$  de projection sur les  $r-1$  premières composantes est surjectif et son noyau est  $\{1\}^{r-1} \times C_a = \langle g_1 \rangle$  et on peut appliquer le premier théorème d'isomorphisme. De même,  $U/\langle g_2 \rangle \cong C_{u_1} \times \cdots \times C_{u_{s-1}}$ .

On a donc obtenu un isomorphisme  $C_{d_1} \times \cdots \times C_{d_{r-1}} \cong C_{u_1} \times \cdots \times C_{u_{s-1}}$  où il y a  $r-1$  facteurs cycliques à gauche. On peut donc appliquer l'hypothèse de récurrence, qui donne  $r-1 = s-1$  et  $d_i = u_i$  pour tout  $i$  avec  $1 \leq i \leq r-1$ . Finalement,  $r = s$  et puisqu'on a déjà  $d_r = u_r = a$ , on a démontré l'unicité. ✓

**Exemples.** (1) On peut donner, à isomorphisme près, tous les groupes abéliens d'ordre 36. En effet,  $36 = 2^2 \cdot 3^2$  donc les possibilités pour décomposer le groupe comme dans le corollaire 2.15 sont

$$\begin{array}{ll} C_2 \times C_2 \times C_3 \times C_3 & C_4 \times C_3 \times C_3 \\ C_2 \times C_2 \times C_9 & C_4 \times C_9. \end{array}$$

En appliquant la méthode de la démonstration du théorème 2.16, on peut trouver la décomposition en termes de facteurs invariants :

$$\begin{array}{ll} C_6 \times C_6 & C_3 \times C_{12} \\ C_2 \times C_{18} & C_{36} \end{array}$$

et on voit bien que ces groupes sont isomorphes aux précédents grâce au théorème chinois.

(2) On peut déterminer de même tous les groupes abéliens d'ordre inférieur ou égal à 16 par exemple. On trouve :

| Ordre | Groupes                                                  | Ordre | Groupes                                                                                                                      |
|-------|----------------------------------------------------------|-------|------------------------------------------------------------------------------------------------------------------------------|
| 1     | $C_1$ (groupe trivial)                                   | 9     | $C_3 \times C_3$ et $C_9$                                                                                                    |
| 2     | $C_2$                                                    | 10    | $C_2 \times C_5 \cong C_{10}$                                                                                                |
| 3     | $C_3$                                                    | 11    | $C_{11}$                                                                                                                     |
| 4     | $C_2 \times C_2$ et $C_4$                                | 12    | $C_2 \times C_2 \times C_3 \cong C_2 \times C_6$ et $C_4 \times C_3 \cong C_{12}$                                            |
| 5     | $C_5$                                                    | 13    | $C_{13}$                                                                                                                     |
| 6     | $C_2 \times C_3 \cong C_6$                               | 14    | $C_2 \times C_7 \cong C_{14}$                                                                                                |
| 7     | $C_7$                                                    | 15    | $C_3 \times C_5 \cong C_{15}$                                                                                                |
| 8     | $C_2 \times C_2 \times C_2$ et $C_2 \times C_4$ et $C_8$ | 16    | $C_2 \times C_2 \times C_2 \times C_2$ et $C_2 \times C_2 \times C_4$<br>et $C_2 \times C_8$ et $C_4 \times C_4$ et $C_{16}$ |

# Produit semi-direct de groupes

On étudie dans ce chapitre une construction qui permet de construire de nouveaux groupes à partir d'anciens : le produit semi-direct. C'est une généralisation du produit direct.

## I. CONSTRUCTION DU PRODUIT SEMI-DIRECT

**Définition 3.1.** Soient  $G$  et  $N$  deux groupes. Une *opération de  $G$  sur  $N$  par automorphismes* est la donnée d'un morphisme de groupes  $\varphi: G \longrightarrow \text{Aut}(N)$ .

**Exemple.** Soit  $N$  un groupe abélien et soit  $\theta$  l'automorphisme de  $N$  défini par  $\theta(x) = x^{-1}$  pour tout  $x \in N$ . Alors il existe un unique morphisme de groupes  $\varphi: C_2 \longrightarrow \text{Aut}(N)$  qui envoie le générateur  $g$  de  $C_2$  sur  $\theta$  d'après le théorème 1.30.

**Exemple.** Soit  $G$  un groupe et soit  $N$  un sous-groupe *normal* de  $G$ . Pour tout  $g \in G$ , l'application  $N \rightarrow G$  qui envoie  $x$  sur  $gxg^{-1}$  est à valeurs dans  $N$ , donc induit un endomorphisme  $\varphi_g$  de  $N$ , qui est un automorphisme (de réciproque  $\varphi_{g^{-1}}$ ). On obtient alors une application  $\varphi: G \rightarrow \text{Aut}(N)$  qui associe  $\varphi_g$  à  $g$  pour tout  $g \in G$ . C'est un morphisme de groupes et on dit que  $G$  *opère sur  $N$  par conjugaison*.

**Définition-Proposition 3.2.** Soient  $G$  et  $N$  deux groupes et soit  $\varphi: G \longrightarrow \text{Aut}(N)$  une opération de  $G$  sur  $N$  par automorphismes. On peut alors munir l'ensemble  $N \times G$  d'une structure de groupe pour la loi :

$$(x, g) \cdot (y, h) = (x\varphi(g)(y), gh), \text{ pour tout } (x, g, y, h) \in (N \times G)^2.$$

L'élément neutre est  $(1_N, 1_G)$  et l'inverse d'un élément  $(x, g)$  est  $(\varphi(g^{-1})(x^{-1}), g^{-1})$ . Le groupe obtenu, noté  $N \rtimes_{\varphi} G$  (ou plus simplement  $N \rtimes G$ ), est appelé le **produit semi-direct** de  $N$  par  $G$  relativement à  $\varphi$ .

**Démonstration.** L'ensemble  $N \times G$  n'est pas vide et l'expression de l'énoncé définit bien une loi sur  $N \times G$ .

Cette loi est associative. En effet, soit  $(x, g, y, h, z, k) \in (N \times G)^3$ , alors

$$\begin{aligned} ((x, g)(y, h))(z, k) &= (x\varphi(g)(y), gh)(z, k) = (x\varphi(g)(y)\varphi(gh)(z), ghk) \\ &= (x, \varphi(g)(y)(\varphi(g) \circ \varphi(h))(z), ghk) \quad (\varphi \text{ morphisme}) \\ &= (x\varphi(g)(y\varphi(h)(z)), ghk) \quad (\varphi(g) \text{ morphisme}) \\ &= (x, g)(y\varphi(h)(z), hk) \\ &= (x, g)((y, h)(z, k)). \end{aligned}$$

Pour tout  $(x, g) \in N \times G$  on a  $(x, g)(1_N, 1_G) = (x\varphi(g)(1_N), g1_G) = (x1_N, g) = (x, g)$  car  $\varphi(g)$  est un morphisme de groupes, et  $(1_N, 1_G)(x, g) = (1_N\varphi(1_G)(x), 1_Gg) = (\text{id}_N(x), g) = (x, g)$  car  $\varphi$  est un morphisme de groupes, donc  $(1_N, 1_G)$  est bien un élément neutre pour la loi.

Soit  $(x, g) \in N \times G$ . Alors

$$\begin{aligned}
 (x, g)(\varphi(g^{-1})(x^{-1}), g^{-1}) &= (x\varphi(g)(\varphi(g^{-1})(x^{-1})), gg^{-1}) = \\
 &= (x(\varphi(g) \circ \varphi(g^{-1})(x^{-1})), 1_G) \\
 &= (x(\varphi(gg^{-1})(x^{-1})), 1_G) \quad (\varphi \text{ morphisme}) \\
 &= (x\varphi(1_G)(x^{-1}), 1_G) \\
 &= (x \text{id}_N(x^{-1}), 1_G) \quad (\varphi \text{ morphisme}) \\
 &= (xx^{-1}, 1_G) = (1_N, 1_G) \\
 \text{et } (\varphi(g^{-1})(x^{-1}), g^{-1})(x, g) &= (\varphi(g^{-1})(x^{-1})\varphi(g^{-1})(x), g^{-1}g) \\
 &= (\varphi(g^{-1})(x^{-1}x), 1_G) \quad (\varphi(g^{-1}) \text{ morphisme}) \\
 &= (\varphi(g^{-1})(1_N), 1_G) \\
 &= (1_N, 1_G) \quad (\varphi(g^{-1}) \text{ morphisme})
 \end{aligned}$$

donc  $(\varphi(g^{-1})(x^{-1}), g^{-1})$  est bien l'inverse de  $(x, g)$ . ✓

**Remarque.** Si le morphisme  $\varphi$  est trivial, alors le produit semi-direct associé est le produit direct.

**Exemple.** Soit  $N$  un groupe abélien, soit  $\theta$  l'unique automorphisme de  $N$  défini par  $\theta(x) = x^{-1}$  pour tout  $x \in N$  et soit  $\varphi: C_2 \rightarrow \text{Aut}(N)$  l'unique morphisme de groupes qui envoie le générateur  $g$  de  $C_2$  sur  $\theta$ . Le groupe  $N \rtimes_{\varphi} C_2$  est noté  $\text{Di}(N)$  et s'appelle le *groupe diédral généralisé*. Lorsque  $N = C_n$ , le groupe  $\text{Di}(C_n)$  est isomorphe au groupe diédral  $\mathcal{D}_n$ .

En effet, soit  $f: \mathcal{D}_n \rightarrow \text{Di}(C_n)$  l'application définie par  $f(r^p s^k) = (u^p, g^k)$  où  $C_n = \langle u \rangle$ ,  $p \in \mathbb{Z}$  et  $k \in \mathbb{Z}$ . Vérifions d'abord que  $f$  est bien définie. Si  $r^p s^k = r^q s^{\ell}$  avec  $(p, k, q, \ell) \in \mathbb{Z}^4$ , alors  $r^{p-q} = s^{\ell-k} \in \langle r \rangle \cap \langle s \rangle = \{1\}$  donc  $n$  divise  $p - q$  et  $\ell - k$  est pair. Posons  $q = p + na$  et  $\ell = k + 2b$  avec  $(a, b) \in \mathbb{Z}^2$ . On a alors  $(u^q, g^{\ell}) = (u^p(u^n)^a, g^k(g^2)^b) = (u^p, g^k)$  car  $u$  est d'ordre  $n$  et  $g$  est d'ordre 2.

Vérifions que  $f$  est un morphisme de groupes. Soit  $(r^p s^k, r^q s^{\ell}) \in \mathcal{D}_n^2$  avec  $(p, k, q, \ell) \in \mathbb{Z}^4$ .

- Si  $k \equiv 0 \pmod{2}$ , alors  $f(r^p s^k r^q s^{\ell}) = f(r^{p+q} s^{\ell}) = (u^{p+q}, g^{\ell})$  et  $f(r^p s^k) f(r^q s^{\ell}) = (u^p, 1)(u^q, s^{\ell}) = (u^p \varphi(1)(u^q), s^{\ell}) = (u^p u^q, s^{\ell}) = f(r^p s^k r^q s^{\ell})$ .
- Si  $k \equiv 1 \pmod{2}$ , alors  $f(r^p s^k r^q s^{\ell}) = f(r^p r^{n-q} s^{\ell+1}) = (u^{p-q}, g^{\ell+1})$  et  $f(r^p s^k) f(r^q s^{\ell}) = (u^p, g)(u^q, g^{\ell}) = (u^p \theta(u^q), s^{\ell+1}) = (u^p u^{-q}, s^{\ell+1}) = f(r^p s^k r^q s^{\ell})$ .

Soit maintenant  $r^p s^k \in \text{Ker } f$ . Alors  $u^p = 1$  et  $g^k = 1$  donc  $n \mid p$  et  $2 \mid k$ . Or  $r^n = 1$  et  $s^2 = 1$  donc  $r^p s^k = 1$ . Donc  $f$  est injectif.

Enfin,  $|\text{Di}(C_n)| = |C_n \times C_2| = 2n = |\mathcal{D}_n|$  donc  $f$  est un isomorphisme.

Le produit semi-direct permet de construire très facilement des groupes non abéliens :

**Proposition 3.3.** Soient  $G$  et  $N$  deux groupes non triviaux et soit  $\varphi: G \rightarrow \text{Aut}(N)$  une opération non triviale de  $G$  sur  $N$  par automorphismes. Alors le groupe  $N \rtimes_{\varphi} G$  n'est pas abélien.

*Démonstration.* Par hypothèse, il existe  $g \in G$  tel que  $\varphi(g) \neq \text{id}_N$ , donc il existe  $y \in N$  tel que  $\varphi(g)(y) \neq y$ . On a alors, dans  $N \rtimes_{\varphi} G$ ,

$$\begin{aligned}
 (1, g)(y, 1) &= (1\varphi(g)(y), g) = (\varphi(g)(y), g) \\
 \text{et } (y, 1)(1, g) &= (y\varphi(1)(1), g) = (y, g) \neq (\varphi(g)(y), g)
 \end{aligned}$$

donc  $N \rtimes_{\varphi} G$  n'est pas abélien. ✓

**Exemple.** Soit  $N$  un groupe abélien. S'il existe  $x \in N$  tel que  $x^2 \neq 1$  alors le groupe  $\text{Di}(N)$  n'est pas abélien. En effet, il existe un automorphisme  $\theta \in \text{Aut}(N)$  d'ordre 2, car  $\theta: t \mapsto t^{-1}$  ne fixe pas  $x$  et est donc différent de  $\text{id}_N$  et par conséquent une opération par automorphismes de  $C_2$  sur  $N$  qui n'est pas triviale.

Pour construire d'autres exemples, il est important de connaître les automorphismes d'un groupe. Le résultat suivant est très utile.

**Proposition 3.4.** Soit  $G = \langle g \rangle$  un groupe cyclique d'ordre  $n$ . Pour tout  $k \in \llbracket 1; n \rrbracket$  tel que  $\text{pgcd}(k, n) = 1$ , il existe un unique automorphisme  $\theta$  de  $G$  tel que  $\theta(g) = g^k$ . Tout automorphisme de  $G$  est de cette forme.

*Démonstration.* Par hypothèse,  $G$  est cyclique engendré par  $g$  et  $(g^k)^n = (g^n)^k = 1$ , donc il existe un unique morphisme de groupes  $\theta: G \rightarrow G$  tel que  $\theta(g) = g^k$ .

Puisque  $\text{pgcd}(k, n) = 1$ , l'élément  $g^k$  de  $G$  engendre  $G$ , donc  $\theta$  est surjectif.

Enfin,  $G$  est fini, donc  $\theta$  est un automorphisme de  $G$ .

Si  $\eta$  est un autre automorphisme de  $G$ , on aura  $\eta(g) = g^q$  pour un  $q$  entier tel que  $0 \leq q \leq n-1$ . De plus,  $\eta$  est surjectif, donc  $g^q$  engendre  $G$  et donc  $\text{pgcd}(q, n) = 1$ . Donc  $\eta$  est bien de la même forme que  $\theta$ . ✓

**Remarque.** On a un isomorphisme entre  $\text{Aut}(C_n)$  et le groupe  $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$  des éléments inversibles de l'anneau  $\mathbb{Z}/n\mathbb{Z}$  (ou des générateurs du groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$ ). Il est donné par  $f: (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(C_n): f(\bar{a})(g) = g^a$  (il faut vérifier que  $f$  est bien définie et que c'est un morphisme, la proposition montre que c'est une bijection).

En particulier, si  $p$  est un nombre premier,  $\text{Aut}(C_p)$  est cyclique d'ordre  $p-1$ .

*Démonstration.* Remarquons d'abord que pour  $n \in \mathbb{N}^*$  on a  $n = \sum_{d|n} \varphi(d)$ . Cette identité découle de la proposition 1.26 (le groupe cyclique  $C_n$  est la réunion disjointe des ensembles d'éléments d'ordre  $d$ , pour  $d | n$ , et le nombre d'éléments d'ordre  $d$ , qui sont tous des générateurs de l'unique sous-groupe d'ordre  $d$  de  $C_n$ , est  $\varphi(d) = |\{k \mid \text{pgcd}(k, d) = 1\}|$ ).

Soit maintenant  $G = (\mathbb{Z}/p\mathbb{Z})^\times$ . On a  $|G| = p-1$ . Pour tout  $d \mid (p-1)$ , posons  $G^{[d]} = \{g \in G \mid g^d = 1\}$ .

Si  $x$  est un élément d'ordre  $d$  de  $G$ , alors  $G^{[d]} = \langle x \rangle$ . En effet, on a  $\langle x \rangle \subset G^{[d]}$  d'après le théorème de Lagrange. De plus, les éléments de  $G^{[d]}$  sont les racines dans  $\mathbb{Z}/p\mathbb{Z}$  du polynôme  $X^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ , qui a donc au moins  $d = |\langle x \rangle|$  racines. Mais il a au plus  $d = \deg(X^d - 1)$  racines car  $\mathbb{Z}/p\mathbb{Z}$  est un anneau intègre, donc  $|G^{[d]}| = d$  et donc  $G^{[d]} = \langle x \rangle$ .

Soit  $d$  un diviseur de  $p-1$ . S'il y a un élément d'ordre  $d$ , alors les éléments d'ordre  $d$  sont dans  $G^{[d]} = \langle x \rangle$  et sont les générateurs de  $\langle x \rangle$ , il y en a donc  $\varphi(d)$ . Donc pour tout diviseur  $d$  de  $p-1$ , le nombre  $n_d$  d'éléments d'ordre  $d$  de  $G$  est 0 ou  $\varphi(d)$ .

Le groupe  $G$  est la réunion de ses éléments d'ordre  $d$  pour  $d \mid (p-1)$ . On a donc

$$\begin{aligned} p-1 = |G| &= \sum_{d \mid (p-1)} n_d \\ &\leq \sum_{d \mid (p-1)} \varphi(d) \\ &= p-1 \end{aligned}$$

donc on doit avoir  $n_d = \varphi(d)$  pour tout  $d \mid (p-1)$ .

En particulier, pour  $d = p-1$ , on obtient  $n_{p-1} = \varphi(p-1)$  et il existe donc un élément d'ordre  $p-1 = |G|$  dans  $G$ , le groupe  $G$  est donc cyclique d'ordre  $p-1$ .

Autre démonstration. Notons  $G = (\mathbb{Z}/p\mathbb{Z})^\times$ . On sait que  $|G| = \varphi(p) = p-1$ .

Soient d'abord  $q$  un nombre premier et  $\alpha \in \mathbb{N}^*$  tels que  $q^\alpha \mid (p-1)$ . Montrons qu'il existe un élément d'ordre  $q^\alpha$  dans  $G$ . Pour tout  $x \in G$ , posons  $y_x = x^{p-1/q^\alpha}$ . D'après le petit

théorème de Fermat, on a  $y_x^{q^\alpha} = x^{p-1} = 1$  dans  $G$  donc  $o(y_x) = q^{\beta_x}$  avec  $1 \leq \beta_x \leq \alpha$ . Notons  $r = \max\{\beta_x \mid x \in G\}$  et montrons que  $r = \alpha$ . Pour tout  $x \in G$  on a  $y_x^{q^r} = 1$  c'est-à-dire que  $x^{p-1/q^{\alpha-r}} = 1$ , donc  $x$  est une racine du polynôme  $X^{p-1/q^{\alpha-r}} - 1$ , qui a donc au moins  $p-1$  racines distinctes, donc son degré est au moins  $p-1$  et donc  $\alpha - r = 0$ . Donc il existe  $x \in G$  dont l'ordre est  $q^\alpha$ .

Posons maintenant  $p-1 = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$  avec  $q_1, \dots, q_s$  des nombres premiers deux à deux distincts et  $\alpha_1, \dots, \alpha_s$  dans  $\mathbb{N}^*$ . Pour tout  $i$  il existe un élément  $x_i$  de  $G$  d'ordre  $q_i^{\alpha_i}$ . Posons  $x = x_1 \cdots x_s$ . Puisque  $G$  est abélien et les ordres des  $x_i$  sont premiers entre eux,  $o(x) = \text{ppcm}(o(x_i) \mid 1 \leq i \leq s) = \prod_{i=1}^s o(x_i) = \prod_{i=1}^s q_i^{\alpha_i} = p-1$ , donc  $G$  est cyclique d'ordre  $p-1$  (engendré par  $x$ ). ✓

**Exemple.** Il existe un groupe non abélien d'ordre 21 (on pourra démontrer, avec les outils que nous verrons plus loin, que si  $G$  est un groupe d'ordre impair qui n'est pas abélien, alors  $|G| \geq 21$  – voir page 54).

En effet, soit  $\theta$  l'unique automorphisme de  $C_7 = \langle u \rangle$  qui envoie  $u$  sur  $u^2$  (il existe bien puisque  $\text{pgcd}(2, 7) = 1$ ). On vérifie que  $\theta^3 = \theta \circ \theta \circ \theta = \text{id}_{C_7}$  (pour cela il suffit de vérifier que  $\theta^3(u) = u$ ). On en déduit qu'il existe un unique morphisme de groupes  $\varphi: C_3 = \langle g \rangle \rightarrow \text{Aut}(C_7)$  tel que  $\varphi(g) = \theta$ . Puisque l'opération  $\varphi$  n'est pas triviale, le groupe  $C_7 \rtimes_\varphi C_3$  n'est pas abélien, et il est d'ordre  $7 \cdot 3 = 21$ .

Il est possible que les produits semi-directs associés à des opérations différentes soient isomorphes. On n'a pas de résultat qui décrit les isomorphismes entre produits semi-directs en toute généralité, mais on a les résultats partiels suivants.

**Exercices.** Voir travaux dirigés

(1) Soient  $\varphi, \psi: G \rightarrow \text{Aut}(N)$  des opérations de  $G$  sur  $N$  par automorphismes. On suppose qu'il existe  $\alpha \in \text{Aut}(G)$  tel que  $\psi \circ \alpha = \varphi$ . Montrer que les produits semi-directs  $N \rtimes_\varphi G$  et  $N \rtimes_\psi G$  sont isomorphes.

L'isomorphisme est donné par  $N \rtimes_\varphi G \rightarrow N \rtimes_\psi G: (x, g) \mapsto (x, \alpha(g))$ .

(2) Soient  $\varphi, \psi: G \rightarrow \text{Aut}(N)$  des opérations de  $G$  sur  $N$  par automorphismes. On suppose qu'il existe  $\beta \in \text{Aut}(N)$  tel que

$$\forall g \in G, \varphi(g) = \beta \circ \psi(g) \circ \beta^{-1}$$

Montrer que les produits semi-directs  $N \rtimes_\varphi G$  et  $N \rtimes_\psi G$  sont isomorphes.

L'isomorphisme est donné par  $N \rtimes_\varphi G \rightarrow N \rtimes_\psi G: (x, g) \mapsto (\beta^{-1}(x), g)$ .

## II. CARACTÉRISATION DU PRODUIT SEMI-DIRECT

Le résultat suivant est très utile pour obtenir des résultats de classification.

**Théorème 3.5** (Caractérisation du produit semi-direct). Soit  $G$  un groupe et  $N$  et  $H$  deux sous-groupes. On suppose :

- (1)  $G = NH$ .
- (2)  $N \cap H = \{1\}$ .
- (3)  $N \triangleleft G$ .

Alors  $G$  est isomorphe à un produit semi-direct  $N \rtimes H$ .

**Démonstration.** On considère l'application  $m: N \times H \rightarrow G, (x, h) \mapsto xh$ , qui est surjective par hypothèse (puisque  $G = NH$ ). On a  $N \triangleleft G$ , donc  $G$  opère sur  $N$  par conjugaison, et en

restreignant cette opération à  $H$ , on obtient un morphisme de groupes

$$\begin{aligned}\varphi: H &\longrightarrow \text{Aut}(N) \\ h &\longmapsto (x \mapsto h x h^{-1})\end{aligned}$$

et on peut donc munir  $N \times H$  de la structure de produit semi-direct  $N \rtimes_{\varphi} H$ .

Montrons alors que  $m: N \rtimes_{\varphi} H \longrightarrow G$  est un morphisme de groupes. On a  $m((x, h)(y, k)) = m(x h y h^{-1}, h k) = x h y k = m(x, h) m(y, k)$ . De plus, si  $m(x, h) = 1$  alors  $x h = 1$  donc  $x = h^{-1} \in N \cap H$ , ce qui implique que  $x = 1$  et  $h = 1$  puisque  $N \cap H = \{1\}$ . Ainsi  $m$  est un isomorphisme. ✓

**Remarque.** Si on ajoute l'hypothèse  $H \triangleleft G$ , alors on obtient le produit direct  $N \times H$ .

**Remarque.** Soit  $G = N \rtimes_{\varphi} H$ , on considère  $N' = N \rtimes \{1\} = N \times \{1\} \subset G$  et  $H' = \{1\} \rtimes H = \{1\} \times H \subset G$ . Alors  $N'$  et  $H'$  sont des sous-groupes de  $G$ , avec  $N' \triangleleft G$  ([Voir travaux dirigés](#)), et il est clair que  $N' \cap H' = \{(1, 1)\}$  et que  $G = N' H'$  (car  $(x, h) = (x, 1)(1, h)$  pour tout  $(x, h) \in N \times H$ ). Ainsi, les propriétés (1) – (3) sont vérifiées pour  $N'$  et  $H'$ . On a alors  $G \cong N' \rtimes_{\varphi'} H'$  avec  $\varphi'((1, h))((x, 1)) = (1, h)(x, 1)(1, h)^{-1} = (\varphi(h)(x), h)(1, h^{-1}) = (\varphi(h)(x)\varphi(h)(1), h h^{-1}) = (\varphi(h)(x), 1)$ .

Notons que  $i: N \rightarrow N'$  et  $j: H \rightarrow H'$  définis par  $i(x) = (x, 1)$  et  $j(h) = (1, h)$  sont des isomorphismes, que  $i$  induit un isomorphisme  $c: \text{Aut}(N) \rightarrow \text{Aut}(N')$  défini pour tout  $\alpha \in \text{Aut}(N)$  par  $c(\alpha) = i \circ \alpha \circ i^{-1}$ . On a alors  $\varphi'(j(h)) = i \circ \varphi(h) \circ i^{-1} = c(\varphi(h))$  pour tout  $h \in H$  donc  $\varphi'$  correspond à  $\varphi$  via ces isomorphismes :

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \text{Aut}(N) \\ j \downarrow \sim & & \sim \downarrow c \\ H' & \xrightarrow{\varphi'} & \text{Aut}(N'). \end{array}$$

Voici un exemple d'application du produit semi-direct.

**Théorème 3.6.** Soit  $G$  un groupe d'ordre  $2p$ , où  $p \geq 3$  est un nombre premier impair. Alors  $G \cong C_{2p}$  ou  $G \cong D_p$ .

*Démonstration.* Par le théorème de Lagrange, les ordres des éléments de  $G$  sont dans  $\{1, 2, p, 2p\}$ . Démontrons qu'il existe nécessairement un élément  $g$  d'ordre 2 et un élément  $u$  d'ordre  $p$  dans  $G$ .

- S'il existe un élément  $t \in G$  d'ordre  $2p$ , alors  $u = t^2$  est d'ordre  $p$  et  $g = t^p$  est d'ordre 2.
- Si tous les éléments de  $G \setminus \{1\}$  sont d'ordre 2, on sait que  $G$  est abélien et d'ordre une puissance de 2 (exercice vers la fin du chapitre 1); on a donc une contradiction. Il y a donc au moins un élément  $u$  d'ordre  $p$  dans  $G$ .
- Soit  $N = \langle u \rangle$ . Alors  $|N| = o(u) = p$  donc  $[G : N] = 2$  et donc  $N \triangleleft G$ . Soit  $\pi: G \rightarrow G/N$  la surjection canonique. Le groupe  $N/G$  est isomorphe au groupe cyclique  $C_2$ , notons  $a$  un générateur de  $N/G$ . Puisque  $\pi$  est surjectif, il existe  $x \in G$  tel que  $\pi(x) = a$ . Supposons que  $x$  soit d'ordre  $p$ , alors on aurait  $1 = \pi(1) = \pi(x^p) = \pi(x)^p = a^p = a$  car  $p$  est impair et  $a$  est d'ordre 2, et on aurait une contradiction. Donc  $x$  est d'ordre 2 ou  $2p$  et finalement  $x$  ou  $x^p$  est d'ordre 2. Il existe donc également un élément  $g$  d'ordre 2 dans  $G$ . Posons  $H = \langle g \rangle \cong C_2$ .

On a vu que  $N \triangleleft G$ . De plus,  $|N \cap H|$  divise les ordres 2 et  $p$  de  $H$  et  $N$ , donc  $|N \cap H| = 1$  et  $N \cap H = \{1\}$ . Enfin,  $|NH| = \frac{|N||H|}{|N \cap H|} = 2p = |G|$  donc  $NH = G$ .

On en déduit que  $G \cong N \rtimes_{\varphi} H$  pour un morphisme  $\varphi: H \rightarrow \text{Aut}(N)$ . Puisque  $H \cong C_2$ , il y a deux possibilités :

- $\varphi$  est trivial, alors  $G \cong N \times H \cong C_p \times C_2 \cong C_{2p}$  par le théorème chinois ;
- $\varphi$  n'est pas trivial. Alors  $\theta = \varphi(g)$  est un élément d'ordre 2, qui d'après la proposition 3.4 est donné par  $\theta(u) = u^k$  pour un  $k$  entier tel que  $2 \leq k \leq p-1$ . L'automorphisme  $\theta$  est d'ordre 2 si, et seulement si,  $\theta^2(u) = u$  c'est-à-dire  $u^{k^2} = u$  soit  $u^{k^2-1} = 1$ . On cherche donc les  $k \in \llbracket 2; p-1 \rrbracket$  tels que  $p \mid (k^2 - 1) = (k-1)(k+1)$ . Puisque  $p$  est premier et ne divise pas  $k-1$  (qui est entre 1 et  $p-2$ ), par le lemme d'Euclide (ou le lemme de Gauss) il divise  $k+1$  donc  $k = p-1$ . On en déduit que  $\theta(u) = u^{p-1} = u^{-1}$  et grâce à un exemple page 40 que  $G \cong N \rtimes_{\varphi} H \cong \text{Di}(C_p) \cong \mathcal{D}_p$ . ✓

**Remarque.** L'existence d'éléments d'ordres 2 et  $p$  peut se démontrer à l'aide des théorèmes de Sylow du prochain chapitre.

Mais sans les théorèmes de Sylow, on peut démontrer que tout groupe d'ordre pair contient un élément d'ordre 2. Voir travaux dirigés (exercice complémentaire)

En effet, soit  $G$  un groupe d'ordre pair. Soit  $\mathcal{R}$  la relation définie sur  $G$  par :

$$\forall (x, y) \in G^2, \quad (x \mathcal{R} y \iff y \in \{x, x^{-1}\}).$$

On vérifie facilement que c'est une relation d'équivalence. Pour tout  $x \in G$ , notons  $\mathcal{C}(x)$  la classe d'équivalence de  $x$ .

Il est clair que  $\mathcal{C}(1) = \{1\}$ . De plus, pour tout  $x \in G$  on a  $|\mathcal{C}(x)| \in \{1, 2\}$  et  $|\mathcal{C}(x)| = 1$  si, et seulement si,  $x^2 = 1$ . Si on suppose que  $G$  ne contient pas d'élément d'ordre 2, alors pour tout  $x \in G \setminus \{1\}$  on a  $|\mathcal{C}(x)| = 2$ . Si le nombre de classes d'équivalence distinctes pour  $\mathcal{R}$  est  $k$  et si on note  $\{g_1 = 1, g_2, \dots, g_k\}$  un système de représentants de ces classes d'équivalence, alors  $G = \coprod_{j=1}^k \mathcal{C}(g_j)$  (union disjointe) et  $|G| = |\mathcal{C}(1)| + \sum_{j=2}^k |\mathcal{C}(g_j)| = 1 + 2(k-1)$  est à la fois pair et impair, on a une contradiction. Donc  $G$  contient un élément d'ordre 2.

# Groupes opérant sur un ensemble. Applications.

Ce chapitre est consacré à la notion de groupe opérant sur un ensemble. C'est un concept extrêmement utile pour obtenir des informations sur les groupes. Les applications que nous avons en vue sont les théorèmes de Sylow (qui permettent par exemple de démontrer que de nombreux groupes ne sont pas simples).

## I. DÉFINITIONS ET EXEMPLES

**Définition 4.1.** Soient  $G$  un groupe et  $E$  un ensemble non vide. Une **opération** (ou **action**) à gauche de  $G$  sur  $E$  est la donnée d'une application

$$\begin{aligned} G \times E &\longrightarrow E \\ (g, x) &\longmapsto g.x \end{aligned}$$

telle que

- (1)  $\forall (g_1, g_2) \in G^2, \forall x \in E, \text{ on a } (g_1 g_2).x = g_1.(g_2.x).$
- (2)  $\forall x \in E, \text{ on a } 1.x = x.$

**Exemple.** Soit  $E$  un ensemble et soit  $S_E$  le groupe des bijections de  $E$  dans lui-même. Alors  $S_E$  opère sur  $E$  :

$$\begin{aligned} S_E \times E &\longrightarrow E \\ (\sigma, x) &\longmapsto \sigma(x). \end{aligned}$$

On peut reformuler la notion d'opération de groupe sur un ensemble en termes de morphismes de groupes. Cette reformulation est souvent utile pour construire des sous-groupes normaux, et donc montrer qu'un groupe n'est pas simple.

**Proposition 4.2.** Soit  $G$  un groupe et soit  $E$  un ensemble non vide. La donnée d'une opération à gauche de  $G$  sur  $E$  est équivalente à la donnée d'un morphisme de groupes  $\alpha: G \rightarrow S_E$ .  
On appellera  $\text{Ker } \alpha$  le **noyau** de l'action.

*Démonstration.* Supposons que  $G$  opère sur  $E$ . Pour  $g \in G$ , considérons l'application  $\alpha_g: E \rightarrow E$  définie par  $\alpha_g(x) = g.x$ . On vérifie (exercice) que  $\alpha_1 = \text{id}_E$  et  $\alpha_{gh} = \alpha_g \circ \alpha_h$  pour tout  $(g, h) \in G^2$ . En particulier  $\alpha_g \circ \alpha_{g^{-1}} = \text{id}_E = \alpha_{g^{-1}} \circ \alpha_g$ . Ainsi  $\alpha_g \in S_E$ , et on obtient un morphisme de groupes

$$\begin{aligned} \alpha: G &\longrightarrow S_E \\ g &\longmapsto \alpha_g. \end{aligned}$$

Réciproquement, si  $\alpha: G \longrightarrow S_E$  est un morphisme de groupes, on vérifie (exercice) que l'application

$$\begin{aligned} G \times E &\longrightarrow E \\ (g, x) &\longmapsto g.x = \alpha(g)(x) \end{aligned}$$

définit une opération de  $G$  sur  $E$ . ✓

**Exemples.** Soit  $G$  un groupe.

(a)  $G$  opère sur lui-même par « translations » :

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto g.x = gx \end{aligned}$$

(b)  $G$  opère sur lui-même par conjugaison :

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto g.x = gxg^{-1} \end{aligned}$$

(c)  $G$  opère sur  $\mathcal{P}(G)$ , l'ensemble de ses parties, par conjugaison :

$$\begin{aligned} G \times \mathcal{P}(G) &\longrightarrow \mathcal{P}(G) \\ (g, S) &\longmapsto g.S = gSg^{-1} \end{aligned}$$

(d) Soit  $H \subset G$  un sous-groupe. Alors  $G$  opère sur l'ensemble  $G/H$  par translations :

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, xH) &\longmapsto g.(xH) = gxH \end{aligned}$$

Si  $H \subsetneq G$ , le morphisme de groupe associé  $\alpha: G \longrightarrow S_{G/H}$  est non trivial ( $\text{Ker } \alpha \neq G$ ).

(e) Soit  $N$  un sous-groupe normal de  $G$  et soit  $H$  un sous-groupe de  $G$ . Alors  $H$  opère par conjugaison sur  $N$  :

$$\begin{aligned} H \times N &\longrightarrow N \\ (h, n) &\longmapsto h.n = hnh^{-1}. \end{aligned}$$

(f) Soit  $V$  un espace vectoriel :  $\text{GL}(V)$  opère sur  $V$  :

$$\begin{aligned} \text{GL}(V) \times V &\longrightarrow V \\ (f, v) &\longmapsto f.v = f(v) \end{aligned}$$

Voici une première illustration de l'utilisation des opérations de groupes.

**Application.** Soit  $G$  un groupe fini, soit  $p$  le plus petit nombre premier qui divise l'ordre de  $G$  et soit  $H$  un sous-groupe d'indice  $p$  dans  $G$ . Alors  $H$  est normal dans  $G$ .

*Voir travaux dirigés*

$G$  agit sur l'ensemble  $G/H$  par translations. On en déduit un morphisme de groupes  $\varphi: G \rightarrow S_{G/H} \cong S_p$ .

Si  $g \in \text{Ker } \varphi$ , alors en particulier  $\varphi(g)(H) = H$  donc  $gH = H$  et donc  $g \in H$ . On a démontré que  $\text{Ker } \varphi \subset H$ . Montrons que  $\text{Ker } \varphi = H$ .

Par le premier théorème d'isomorphisme,  $\varphi$  induit un isomorphisme  $\overline{\varphi}: G/\text{Ker } \varphi \xrightarrow{\sim} \text{Im } \varphi \hookrightarrow S_p$ , donc  $[G : \text{Ker } \varphi] \mid p!$ . Or  $[G : \text{Ker } \varphi] = [G : H][H : \text{Ker } \varphi] = p[H : \text{Ker } \varphi]$  donc  $[H : \text{Ker } \varphi] \mid (p-1)!$ . Supposons que  $[H : \text{Ker } \varphi] > 1$ , il existe alors un diviseur premier  $q$  de  $[H : \text{Ker } \varphi]$  (qui divise donc  $|G|$  par le théorème de Lagrange), on doit donc avoir  $q \mid (p-1)!$ , donc  $q$  divise un nombre entier dans  $\llbracket 1; p-1 \rrbracket$  par le lemme d'Euclide et donc  $q < p$  : cela contredit la minimalité de  $p$  comme diviseur premier de  $|G|$ . Donc  $[H : \text{Ker } \varphi] = 1$  et donc  $H = \text{Ker } \varphi$  est le noyau d'un morphisme de groupes  $\varphi: G \rightarrow S_p$  et par conséquent  $H$  est normal dans  $G$ .

On peut aussi utiliser les actions de groupes pour caractériser les produits semi-directs à l'aide de suites exactes de groupes.

Remarquons d'abord que si  $G = N \rtimes_{\varphi} H$  est un produit semi-direct, alors on a une suite exacte

$$1 \rightarrow N \xrightarrow{f} G \xrightarrow{g} H \rightarrow 1$$

où  $f(n) = (n, 1)$  et  $g(n, h) = h$  pour tout  $(n, h) \in N \times H$ . (Voir travaux dirigés)

Dans l'autre sens, soit

$$1 \rightarrow N \xrightarrow{f} G \xrightarrow{g} K \rightarrow 1$$

une suite exacte (on rappelle que cela implique en particulier que  $f(N) \triangleleft G$  et  $K \cong G/f(N)$ ).

**Définition 4.3.** Soit  $H$  un sous-groupe de  $G$ . On dit que  $H$  est un **relèvement** de  $K$  si la restriction de  $g$  à  $H$  induit un isomorphisme  $H \cong K$ .

Si on note  $N' = f(N) \cong N$ , alors  $N' \cap H = \{1\}$  et  $G = N'H$  (exercice). Voir travaux dirigés

En effet :

- Soit  $x \in N' \cap H$ . Alors  $x \in N' = \text{Ker } g$  donc  $g(x) = 1$ . De plus,  $x \in H$  et  $g|_H$  est injectif, donc  $x = 1$ . Donc  $N' \cap H = \{1\}$ .
- Puisque  $N' = \text{Ker } g \triangleleft G$ , on sait que  $N'H$  est un sous-groupe de  $G$ . Soit maintenant  $x \in G$ . Soit  $h \in H$  l'unique antécédent dans  $H$  de  $g(x)$  par  $g$ . On a alors  $g(h) = g(x)$  donc  $xh^{-1} \in \text{Ker } g = N'$ . On en déduit que  $x = (xh^{-1})h \in N'H$  et donc que  $G = N'H$ .

**Proposition 4.4.** Soit

$$1 \rightarrow N \xrightarrow{f} G \xrightarrow{g} K \rightarrow 1$$

une suite exacte.

Si  $K$  admet un relèvement  $H$ , alors  $G$  est isomorphe à un produit semi-direct  $N \rtimes H$ .

*Démonstration.* Voir travaux dirigés

Le sous-groupe  $H$  de  $G$  agit par conjugaison sur  $N'$  (qui est normal dans  $G$ ). Cette action induit donc un morphisme de groupes  $\varphi: H \rightarrow \text{Aut}(N')$ . On considère l'application

$$\begin{aligned} \alpha: N' \rtimes_{\varphi} H &\longrightarrow G \\ (n, h) &\longmapsto nh. \end{aligned}$$

Vérifions que  $\alpha$  est un morphisme de groupes. On a

$$\alpha((n, h)(n', h')) = \alpha(n\varphi(h)(n'), hh') = \alpha(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h' = \alpha(n, h)\alpha(n', h').$$

Soit  $(n, h) \in \text{Ker } \alpha$ . Alors  $nh = 1$  dans  $G$ , donc  $n = h^{-1} \in N' \cap H = \{1\}$ , donc  $n = 1 = h$  et donc  $(n, h) = (1, 1)$ . Donc  $\alpha$  est injectif.

Enfin,  $\alpha$  est surjectif car  $G = N'H$ . On a démontré que  $\alpha$  est un isomorphisme, c'est-à-dire que  $G \cong N' \rtimes_{\varphi} H \cong N \rtimes H$ . ✓

## II. ORBITES, STABILISATEURS

Dans ce paragraphe on introduit les notions d'orbite et de stabilisateur, qui permettent d'analyser l'opération d'un groupe sur un ensemble.

**Définition 4.5.** Soit  $G$  un groupe opérant sur un ensemble  $E$  et soit  $x \in E$ . Alors l'ensemble  $\Omega(x) = \{g.x \mid g \in G\} \subset E$  est appelé **l'orbite** de  $x$  sous l'action de  $G$ .

L'orbite  $\Omega(x)$  est parfois notée  $\Omega_G(x)$ , ou encore  $G.x$ .

**Remarque.** Une orbite est stable sous l'action du groupe.

Soit  $G$  un groupe opérant sur un ensemble  $E$ . La relation  $\mathcal{R}$  sur  $E$  définie par

$$\forall (x, y) \in E^2, \quad (x \mathcal{R} y \iff \exists g \in G \text{ tq } y = g.x)$$

est une relation d'équivalence sur  $E$  (exercice). L'orbite  $\Omega(x)$  d'un élément  $x \in E$  est la classe d'équivalence de  $x$  pour la relation  $\mathcal{R}$ . Les orbites des éléments de  $E$  sous l'action de  $G$  forment donc une partition de  $E$ .

**Définition-Proposition 4.6.** Soit  $G$  un groupe opérant sur un ensemble  $E$  et soit  $x \in E$ . Alors l'ensemble  $\text{Stab}_G(x) = \{g \in G \mid g.x = x\}$  est un sous-groupe de  $G$ , appelé le **stabilisateur** de  $x$  dans  $G$ .

La vérification est laissée en exercice.

*Démonstration.* Soit  $x \in E$ . Il est clair que  $\text{Stab}_G(x)$  est une partie de  $G$ , qui contient 1 par définition d'une action.

Soit  $(g, h) \in \text{Stab}_G(x)^2$ , alors  $(gh).x = g.(h.x) = g.x = x$  donc  $gh \in \text{Stab}_G(x)$ .

De plus, puisque  $g.x = x$  on a  $g^{-1}.(g.x) = g^{-1}.x$ . Or  $g^{-1}.(g.x) = (g^{-1}g).x = 1x = x$  donc  $x = g^{-1}.x$  et donc  $g^{-1} \in \text{Stab}_G(x)$ .

Par conséquent,  $\text{Stab}_G(x)$  est un sous-groupe de  $G$ . ✓

**Définition 4.7.** Soit  $G$  un groupe opérant sur un ensemble  $E$ .

(1) On dit que  $G$  opère **transitivement** sur  $E$  si  $\forall (x, y) \in E^2, \exists g \in G$  tel que  $y = g.x$ .

(2) On dit que  $G$  opère **librement** sur  $E$  si  $\forall g \in G, \forall x \in E, g.x = x \iff g = 1$ .

Ainsi  $G$  opère transitivement sur  $E$  si, et seulement si, il n'y a qu'une seule orbite, et  $G$  opère librement sur  $E$  si et seulement si pour tout  $x \in E$  on a  $\text{Stab}_G(x) = \{1\}$ .

**Exemples.** (a) L'opération de  $G$  sur lui-même par translations est libre et transitive.

(b) On fait opérer  $G$  sur lui-même par conjugaison. Pour  $x \in G$ ,

- l'orbite de  $x$  est l'ensemble  $\{gxg^{-1} \mid g \in G\}$ , c'est la **classe de conjugaison** de  $x$ ;

- le stabilisateur de  $x$  est le sous-groupe  $Z_G(x) = \{g \in G \mid gx = xg\}$ , il est appelé **centralisateur** de  $x$ .

(c) On fait opérer  $G$  sur l'ensemble de ses parties par conjugaison. L'orbite de  $S \subset G$  est l'ensemble  $\{gSg^{-1}, g \in G\}$ .

Le stabilisateur de  $S$  est le sous-groupe  $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$ , il est appelé **normalisateur** de  $S$ . Si  $S = H$  est un sous-groupe de  $G$ , alors  $H \triangleleft N_G(H)$ .

(d) Si  $H$  est un sous-groupe de  $G$ , l'opération de  $G$  sur  $G/H$  par translations est transitive, et le stabilisateur de  $xH$  est le sous-groupe  $xHx^{-1}$ .

(e) Pour l'opération naturelle de  $\text{GL}(V)$  sur un espace vectoriel  $V$ , il y a deux orbites :  $\{0\}$  et  $V \setminus \{0\}$ .

En effet, il est clair que  $\Omega(0) = \{0\}$ . Soit  $v \in V$  un vecteur non nul fixé et montrons que  $\Omega(v) = V \setminus \{0\}$ , dans le cas où  $V$  est de dimension finie  $n$  (c'est également vrai en dimension infinie, en utilisant le théorème 7.24). Soit  $v' \in V \setminus \{0\}$  un vecteur quelconque. Les familles  $\{v\}$  et  $\{v'\}$  étant libres, il existe des bases  $\mathcal{B} = (v_1 = v, v_2, \dots, v_n)$  et  $\mathcal{B}' = (v'_1 = v', v'_2, \dots, v'_n)$  de  $V$  d'après le théorème de la base incomplète. Soit  $f: V \rightarrow V$  l'unique application linéaire définie sur la base  $\mathcal{B}$  par  $f(v_i) = v'_i$  pour tout  $i \in \llbracket 1; n \rrbracket$ . Alors l'image de la base  $\mathcal{B}$  par  $f$  est la base  $\mathcal{B}'$ , donc  $f$  est un automorphisme, c'est-à-dire que  $f \in \text{GL}(V)$ . De plus,  $v' = f(v) = f.v$  donc  $v' \in \Omega(v)$ .

**Proposition 4.8.** Soit  $G$  un groupe opérant sur un ensemble  $E$ . Soit  $(x, y) \in E^2$ . Si  $x$  et  $y$  sont dans la même orbite, c'est-à-dire s'il existe  $g \in G$  tel que  $y = g.x$ , alors les sous-groupes  $\text{Stab}_G(x)$  et  $\text{Stab}_G(y)$  sont conjugués dans  $G$ .

*Démonstration.* On vérifie que  $\text{Stab}_G(g.x) = g \text{Stab}_G(x) g^{-1}$ , ce qui donne le résultat.

En effet, soit  $h \in G$ . Alors

$$\begin{aligned} h \in g \text{Stab}_G(x) g^{-1} &\iff \exists u \in \text{Stab}_G(x), h = gu g^{-1} \\ &\iff g^{-1} h g \in \text{Stab}_G(x) \\ &\iff g^{-1} h g.x = x \\ &\iff h.(g.x) = g.x \\ &\iff h \in \text{Stab}_G(g.x). \end{aligned} \quad \checkmark$$

Le résultat suivant est le résultat clé pour décrire les ensembles sur lesquels opère un groupe.

**Théorème 4.9.** Soit  $G$  un groupe opérant sur  $E$  et soit  $x \in E$ . Alors on a une bijection :

$$G / \text{Stab}_G(x) \simeq \Omega(x).$$

En particulier,  $|\Omega(x)| = [G : \text{Stab}_G(x)]$ .

*Démonstration.* Soit  $f: G \rightarrow \Omega(x)$  l'application définie par  $f(g) = g.x$ . Elle est surjective par définition de  $\Omega(x)$ . Soit  $(g, h) \in G^2$ . Alors

$$\begin{aligned} f(g) = f(h) &\iff g.x = h.x \iff (h^{-1}g).x = x \iff h^{-1}g \in \text{Stab}_G(x) \\ &\iff g \text{Stab}_G(x) = h \text{Stab}_G(x) \\ &\quad (\text{les éléments } g \text{ et } h \text{ sont équivalents modulo } \text{Stab}_G(x)). \end{aligned}$$

On peut donc considérer l'application  $\bar{f}: G / \text{Stab}_G(x) \rightarrow \Omega(x)$  induite par  $f$ , c'est-à-dire que  $\bar{f}(g \text{Stab}_G(x)) = f(g)$ . Les équivalences ci-dessus montrent qu'elle est bien définie et qu'elle est injective.

Ainsi  $f$  induit la bijection annoncée  $\bar{f}$ .  $\checkmark$

En combinant la proposition précédente et le théorème de Lagrange, on obtient :

**Corollaire 4.10.** Soit  $G$  un groupe fini opérant sur un ensemble  $E$ . Alors le cardinal d'une orbite est fini et divise l'ordre du groupe.

**Corollaire 4.11. (Equation aux classes)**

Soit  $G$  un groupe opérant sur un ensemble fini  $E$ . Soit  $(x_i)_{1 \leq i \leq r}$  une famille de représentants des orbites distinctes. Alors

$$|E| = \sum_{i=1}^r [G : \text{Stab}_G(x_i)]$$

*Démonstration.* Les orbites forment une partition de  $E$ , donc il existe  $r \in \mathbb{N}^*$  et des éléments  $x_1, \dots, x_r$  de  $E$  tels que  $E = \coprod_{i=1}^r \Omega(x_i)$ . On en déduit que  $|E| = \sum_{i=1}^r |\Omega(x_i)| = \sum_{i=1}^r [G : \text{Stab}_G(x_i)]$ .  $\checkmark$

**Corollaire 4.12. (Equation aux classes)**

Soit  $G$  un groupe fini (opérant sur lui-même par conjugaison). Soit  $(x_i)_{1 \leq i \leq r}$  une famille de représentants des classes de conjugaison distinctes qui ne sont pas réduites à un élément. Alors

$$|G| = |Z(G)| + \sum_{i=1}^r [G : Z_G(x_i)].$$

*Démonstration.* On fait opérer  $G$  sur lui-même par conjugaison. Pour cette opération on a  $\text{Stab}_G(x_i) = Z_G(x_i)$ .

Soit  $x \in G$ . Alors  $\Omega(x)$  est réduite à un élément si, et seulement si, pour tout  $g \in G$  on a  $gxg^{-1} = g.x = x$ , c'est-à-dire  $gx = xg$ , ce qui revient à  $x \in Z(G)$ .

On en déduit que

$$G = \left( \coprod_{x \in Z(G)} \Omega(x) \right) \amalg \left( \coprod_{i=1}^r \Omega(x_i) \right) = \left( \coprod_{x \in Z(G)} \{x\} \right) \amalg \left( \coprod_{i=1}^r \Omega(x_i) \right)$$

et donc que  $|G| = \sum_{x \in Z(G)} |\{x\}| + \sum_{i=1}^r |\Omega(x_i)| = |Z(G)| + \sum_{i=1}^r [G : \text{Stab}_G(x_i)]$ . ✓

On va appliquer ces premiers résultats sur les opérations de groupes aux  $p$ -groupes.

**Définition 4.13.** Soit  $p$  un nombre premier. Un  $p$ -groupe est un groupe d'ordre  $p^n$  avec  $n \in \mathbb{N}^*$ .

On commence par deux lemmes.

**Lemme 4.14.** Soit  $p$  un nombre premier et soit  $G$  un  $p$ -groupe opérant sur un ensemble fini  $E$ .

Alors  $|E^G| \equiv |E| \pmod{p}$ , où

$$E^G = \{x \in E \mid \forall g \in G, g.x = x\}$$

est l'ensemble de points fixes de  $E$  sous l'action de  $G$ .

*Démonstration.* Les éléments de  $E^G$  sont exactement les éléments de  $E$  dont l'orbite est réduite à un point. Si  $E = E^G$ , on a le résultat. Sinon, on a

$$|E| = |E^G| + \sum_{i=1}^r [G : \text{Stab}_G(x_i)]$$

où  $x_1, \dots, x_r$  sont les représentants des orbites qui ne sont pas réduites à un point. Ainsi pour tout  $i \in \llbracket 1; r \rrbracket$  on a  $[G : \text{Stab}_G(x_i)] > 1$ . Or  $[G : \text{Stab}_G(x_i)] \mid |G| = p^n$  donc il existe, pour tout  $i$ , un nombre entier  $d_i \in \mathbb{N}^*$  tel que  $[G : \text{Stab}_G(x_i)] = p^{d_i}$ . En particulier,  $p$  divise  $[G : \text{Stab}_G(x_i)]$  pour tout  $i$  et on a donc bien  $|E^G| \equiv |E| \pmod{p}$ . ✓

**Lemme 4.15.** Soit  $G$  un groupe. Si le groupe  $G/Z(G)$  est monogène, alors  $G$  est abélien.

*Démonstration.* Voir travaux dirigés

Notons  $\pi: G \rightarrow G/Z(G)$  la projection canonique. Soit  $x = \pi(a)$  un générateur du groupe monogène  $G/Z(G)$ , avec  $a \in G$ .

Soit  $(g, h) \in G^2$ . Il existe  $(k, \ell) \in \mathbb{Z}^2$  tel que  $\pi(g) = \pi(a)^k$  et  $\pi(h) = \pi(a)^\ell$  et donc  $(z_1, z_2) \in Z(G)^2$  tel que  $g = a^k z_1$  et  $h = a^\ell z_2$ . Puisque  $z_1$  et  $z_2$  sont centraux dans  $G$  on obtient

$$gh = a^k z_1 a^\ell z_2 = a^k a^\ell z_1 z_2 = a^{k+\ell} z_1 z_2 \text{ et } hg = a^\ell z_2 a^k z_1 = a^{\ell+k} z_2 z_1 = a^{k+\ell} z_1 z_2 = gh. \quad \checkmark$$

**Théorème 4.16.** Soit  $p$  un nombre premier.

- (1) Soit  $G$  un  $p$ -groupe. Alors le centre de  $G$  n'est pas trivial.
- (2) Soit  $G$  un groupe d'ordre  $p^2$ . Alors  $G$  est abélien et  $G$  est isomorphe à  $C_{p^2}$  ou à  $C_p \times C_p$ .
- (3) Soit  $G$  un groupe d'ordre  $p^n$  avec  $n \in \mathbb{N}^*$ . Alors pour tout  $i \in \llbracket 0; n \rrbracket$  le groupe  $G$  contient un sous-groupe normal d'ordre  $p^i$ . En particulier, si  $n \geq 2$  le groupe  $G$  n'est pas simple.

*Démonstration.* (1) Le centre d'un groupe  $G$  est l'ensemble des points fixes de  $G$  pour l'opération sur lui-même par conjugaison. Ainsi le lemme 4.14 donne  $|G| \equiv |Z(G)| \pmod{p}$ , et puisque  $|Z(G)| \geq 1$ , on a bien  $|Z(G)| > 1$ .

(2) Soit  $G$  un groupe d'ordre  $p^2$ . On sait que  $|Z(G)| > 1$  et, comme  $|Z(G)|$  divise  $p^2$  (théorème de Lagrange), on a  $|Z(G)| = p$  ou  $|Z(G)| = p^2$ .

Si  $|Z(G)| = p$ , le groupe  $G/Z(G)$  est d'ordre  $p$  premier, donc il est cyclique et le lemme 4.15 affirme que  $G$  est abélien; mais  $Z(G) \neq G$  et on a une contradiction.

Ainsi,  $|Z(G)| = p^2$  donc  $Z(G) = G$  et finalement  $G$  est abélien.

Le théorème de classification des groupes abéliens finis nous permet alors d'affirmer que  $G \cong C_{p^2}$  ou  $G \cong C_p \times C_p$ .

(3) On procède par récurrence sur  $n$ .

♦ Initialisation. Si  $n = 1$ , le groupe  $G$  est d'ordre premier et le résultat est évidemment vrai.

♦ Hérédité. Soit  $n > 1$  tel que tout groupe d'ordre  $p^j$  avec  $1 \leq j < n$  possède des sous-groupes normaux de tous les ordres possibles. Soit  $G$  un groupe d'ordre  $p^n$ .

On sait que  $Z(G) \neq \{1\}$ . Si  $G$  est abélien, alors  $G$  n'est pas simple car les seuls groupes simples abéliens sont d'ordre premier. Ainsi,  $G$  contient un sous-groupe normal  $H$  avec  $\{1\} \subsetneq H \subsetneq G = Z(G)$ . Si  $G$  n'est pas abélien, alors  $H = Z(G)$  vérifie  $\{1\} \subsetneq H \subsetneq G$  et on a  $H \triangleleft G$ .

Dans tous les cas, il existe un sous-groupe normal  $H$  de  $G$ , contenu dans  $Z(G)$  et tel que  $\{1\} \subsetneq H \subsetneq G$ . Il existe alors un nombre entier  $k$  avec  $0 < k < n$  tel que  $|H| = p^k$  et  $[G : H] = p^{n-k}$ . L'hypothèse de récurrence fournit des sous-groupes de  $H$  et donc de  $G$  d'ordre  $p^i$  pour tout  $i \in \llbracket 0; k \rrbracket$ , qui sont normaux dans  $G$  car contenus dans  $Z(G)$ . L'hypothèse de récurrence fournit également pour tout  $\ell \in \llbracket 0; n - k \rrbracket$  un sous-groupe normal  $K_\ell$  de  $G/H$  d'ordre  $p^\ell$ . Soit  $\pi : G \rightarrow G/H$  la surjection canonique. Alors  $\pi^{-1}(K_\ell)$  est un sous-groupe normal de  $G$  contenant  $H$ , avec  $K_\ell \cong \pi^{-1}(K_\ell)/H$ . Ainsi  $|\pi^{-1}(K_\ell)| = |H||K_\ell| = p^{k+\ell}$ . Si  $i \in \llbracket k + 1; n \rrbracket$ , il existe  $\ell \in \llbracket 1; n - k \rrbracket$  tel que  $i = k + \ell$ , et donc il existe un sous-groupe normal  $\pi^{-1}(K_\ell)$  de  $G$  d'ordre  $p^i$ . ✓

### III. THÉORÈMES DE SYLOW

Dans ce paragraphe on énonce et démontre les théorèmes de Sylow, qui assurent l'existence de certains sous-groupes, et donnent des informations sur leur nombre.

Dans la suite,  $p$  est un nombre premier.

**Définition 4.17.** Soit  $G$  un groupe d'ordre  $p^\alpha m$  où  $\alpha \in \mathbb{N}^*$  et  $p$  ne divise pas  $m$ . Un  $p$ -sous-groupe de Sylow (ou  $p$ -Sylow) de  $G$  est un sous-groupe de  $G$  d'ordre  $p^\alpha$ .

**Remarque.** Soit  $H$  un sous-groupe de  $G$ . Alors  $H$  est un  $p$ -sous-groupe de Sylow de  $G$  si, et seulement si,  $H$  est un  $p$ -groupe et  $p$  ne divise pas  $[G : H]$ .

**Théorème 4.18 (Premier théorème de Sylow).** Soit  $G$  un groupe fini et  $p$  un diviseur premier de  $|G|$ . Alors  $G$  contient un  $p$ -sous-groupe de Sylow.

Pour démontrer ce théorème, nous utiliserons les deux lemmes qui suivent, qui concernent les groupes abéliens.

**Lemme 4.19.** Soit  $G$  un groupe abélien d'ordre  $N$ , et soit  $n \in \mathbb{N}^*$  tel que pour tout  $x \in G$  on ait  $x^n = 1$ . Alors  $N$  divise une puissance de  $n$ .

Ne sert nulle part il me semble...

*Démonstration.* On sait qu'il existe des nombres entiers  $r \in \mathbb{N}^*$  et  $d_1, \dots, d_r$  tels que  $d_1 \mid d_2 \mid \dots \mid d_r$  et  $G \cong C_{d_1} \times \dots \times C_{d_r}$  d'après le théorème 2.16. On a également  $N = d_1 \dots d_r$ . Pour tout  $i \in \llbracket 1; r \rrbracket$ , il existe un élément  $x_i$  d'ordre  $d_i$  dans  $G$  (un générateur de  $C_{d_i}$ ), qui vérifie  $x_i^n = 1$  par hypothèse, donc  $d_i$  divise  $n$ . Posons donc  $n = d_i q_i$  avec  $q_i \in \mathbb{N}^*$ . On a alors  $n^r = d_1 \dots d_r q_1 \dots q_r = N q_1 \dots q_r$  donc  $N$  divise  $n^r$ . ✓

**Lemme 4.20** (de Cauchy pour les groupes abéliens). Soit  $G$  un groupe abélien fini et soit  $p$  un diviseur premier de  $|G|$ . Alors  $G$  contient un élément d'ordre  $p$ .

*Démonstration.* Posons  $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$  avec  $p_1, \dots, p_r$  des nombres premiers deux à deux distincts et  $(\alpha_1, \dots, \alpha_r) \in (\mathbb{N}^*)^r$ . Le nombre premier  $p$  est l'un des  $p_i$ .

Grâce au corollaire 2.15, il existe des sous-groupes  $H_1, \dots, H_r$  de  $G$  tels que  $|H_i| = p_i^{\alpha_i}$  pour tout  $i \in \llbracket 1; r \rrbracket$  et  $G \cong H_1 \times \dots \times H_r$ .

Soit  $i \in \llbracket 1; r \rrbracket$ . D'après le théorème 4.16 le groupe  $H_i$ , et donc  $G$ , contient un sous-groupe d'ordre (premier)  $p_i$ , qui est cyclique, donc  $H_i$  et  $G$  contiennent un élément d'ordre  $p_i$ . ✓

*Démonstration du premier théorème de Sylow.* On procède par récurrence sur  $|G|$ .

Initialisation :  $n \leq 5$ . Si  $|G|$  est un  $p$ -groupe, le résultat est clair ( $G$  est lui-même un  $p$ -sous-groupe de Sylow de  $G$ ). Le résultat est donc vrai si  $|G| \leq 5$ .

Hérédité. Soit  $n \geq 6$  tel que le premier théorème de Sylow soit vrai pour les groupes d'ordre  $< n$ . Soit  $G$  un groupe d'ordre  $n$  et soit  $p$  un diviseur premier de  $|G|$ ; posons  $|G| = p^\alpha m$  avec  $\alpha \in \mathbb{N}^*$  et  $m \in \mathbb{N}^*$  tels que  $p \nmid m$ .

On distingue deux cas :

Cas 1. Il existe un sous-groupe propre  $H$  de  $G$  tel que  $p \nmid [G : H]$ . Alors  $p^\alpha \mid |H|$ , donc on a  $|H| = p^\alpha q$  avec  $q \mid m$ ,  $q < m$  et l'hypothèse de récurrence fournit un  $p$ -sous-groupe de Sylow de  $H$ , qui est d'ordre  $p^\alpha$ , et qui est donc un  $p$ -sous-groupe de Sylow de  $G$ , et le résultat est démontré.

Cas 2. Pour tout sous-groupe propre  $H$  de  $G$ , on a  $p \mid [G : H]$ . Montrons que  $p \mid |Z(G)|$ . Si  $G$  est abélien c'est clair puisque  $Z(G) = G$ . Sinon, l'équation aux classes donne

$$|G| = |Z(G)| + \sum_{i=1}^r [G : Z_G(x_i)]$$

où les  $x_i$  sont les représentants des classes de conjugaison qui ne sont pas réduites à un élément. On a  $1 \leq |Z(G)| < |G|$ , donc pour tout  $i$  on a  $|G| > [G : Z_G(x_i)] > 1$ . Les  $Z_G(x_i)$  sont des sous-groupes propres de  $G$  donc par hypothèse (Cas 2.)  $p \mid [G : Z_G(x_i)]$  pour tout  $i$ . On en déduit que  $p \mid |Z(G)|$ .

Puisque  $Z(G)$  est abélien, le lemme de Cauchy pour les groupes abéliens montre qu'il existe un élément  $a \in Z(G)$  d'ordre  $p$ . Soit  $H = \langle a \rangle$ . Alors  $H \triangleleft G$  car  $H \subset Z(G)$ , et  $G/H$  est un groupe d'ordre  $p^{\alpha-1}m$ . L'hypothèse de récurrence fournit un sous-groupe  $\bar{K}$  de  $G/H$  d'ordre  $p^{\alpha-1}$ , et il existe un sous-groupe  $K$  de  $G$  contenant  $H$  tel que  $\bar{K} \cong K/H$ . On a alors  $|K| = |H||\bar{K}| = p^\alpha$ , et  $K$  est donc un  $p$ -sous-groupe de Sylow de  $G$ . ✓

**Corollaire 4.21.** Soit  $G$  un groupe d'ordre  $p^\alpha m$  avec  $p \nmid m$ . Alors  $G$  possède des sous-groupes d'ordre  $p^i$  pour tout  $i$  tel que  $0 \leq i \leq \alpha$ .

*Démonstration.* Le premier théorème de Sylow fournit un  $p$ -sous-groupe de Sylow  $H$  de  $G$ , qui est d'ordre  $p^\alpha$ . D'après le théorème 4.16, le  $p$ -groupe  $H$  et donc  $G$  contient des sous-groupes d'ordre  $p^i$  pour tout  $i \in \llbracket 0; \alpha \rrbracket$ . ✓

**Conséquence 4.22** (Théorème de Cauchy). Soit  $G$  un groupe fini et soit  $p$  un diviseur premier de  $|G|$ . Alors il existe un élément d'ordre  $p$  dans  $G$ .

**Exercice.** Soit  $G$  un groupe fini non trivial et soit  $p$  un nombre premier tel que pour tout  $g \in G$ , l'ordre de  $g$  est une puissance de  $p$ . Alors  $|G|$  est une puissance de  $p$ .

**Correction.** Puisque  $G$  n'est pas trivial, il contient un élément dont l'ordre est une puissance de  $p$  différente de 1 et par conséquent  $p$  divise  $|G|$ . Posons  $|G| = p^\alpha m$  avec  $\alpha \in \mathbb{N}^*$  et  $m \in \mathbb{N}^*$  tel que  $p \nmid m$ . Si  $m \neq 1$ , il existe un diviseur premier  $q$  de  $m$ , on a donc  $q \neq p$ . D'après le théorème de Cauchy, il existe un élément de  $G$  dont l'ordre est  $q$ , ce qui contredit l'hypothèse sur  $G$ . Donc  $m = 1$  et  $|G| = p^\alpha$ . ✓

**Remarque.** Soit  $p$  un nombre premier. La définition générale d'un  $p$ -groupe est un groupe tel que les ordres de tous ses éléments sont des puissances de  $p$ .

On voit grâce à l'exercice précédent et le théorème de Lagrange que pour un groupe fini, cette définition est équivalente à la nôtre.

#### **Théorème 4.23. (Deuxième théorème de Sylow)**

Soit  $G$  un groupe d'ordre  $|G| = p^\alpha m$ , avec  $p$  premier,  $\alpha \in \mathbb{N}^*$ ,  $m \in \mathbb{N}^*$  et  $p \nmid m$ .

- (1) Si  $H$  est un  $p$ -sous-groupe de  $G$ , alors  $H$  est contenu dans un  $p$ -sous-groupe de Sylow de  $G$ .
- (2) Tous les  $p$ -sous-groupes de Sylow sont conjugués entre eux.
- (3) Le nombre de  $p$ -sous-groupes de Sylow est congru à 1 modulo  $p$  et divise  $m$ .

On commence par un lemme.

**Lemme 4.24.** Soit  $P$  un  $p$ -sous-groupe de Sylow de  $G$  et soit  $H$  un  $p$ -sous-groupe de  $G$ . Si  $H \subset N_G(P)$ , alors  $H \subset P$ .

**Démonstration.** On suppose que  $H \subset N_G(P)$ . Il est clair que  $P \subset HP$ . Montrons que  $HP \subset P$ , ce qui impliquera  $H \subset P$ .

Puisque  $H \subset N_G(P)$  et  $P \subset N_G(P)$ , on a  $HP \subset N_G(P)$ . De plus,  $P$  est normal dans  $N_G(P)$  donc  $HP$  est un sous-groupe de  $N_G(P)$  et donc de  $G$ . On a  $|HP| = \frac{|H||P|}{|H \cap P|}$ , qui est une puissance de  $p$  (car  $H$  et  $P$  sont des  $p$ -groupes). Puisque  $P$  est un  $p$ -sous-groupe de Sylow de  $G$ , on a  $|HP| \leq |P|$  et donc  $HP = P$ , d'où  $H \subset P$ . ✓

**Démonstration du deuxième théorème de Sylow.** Soit  $\mathcal{S}$  l'ensemble des  $p$ -sous-groupes de Sylow de  $G$ . On remarque que si  $P$  est un  $p$ -sous-groupe de Sylow de  $G$  et si  $g \in G$ , alors  $gPg^{-1}$  est un sous-groupe de  $G$  d'ordre  $|gPg^{-1}| = |P|$ , donc  $gPg^{-1}$  est un  $p$ -sous-groupe de Sylow de  $G$ . On peut considérer l'action de  $G$  sur  $\mathcal{S}$  par conjugaison.

Soit  $P \in \mathcal{S}$  un  $p$ -sous-groupe de Sylow fixé. Soit  $E = \Omega(P) = \{xPx^{-1} \mid x \in G\}$  la classe de conjugaison de  $P$ . On sait que  $|E| = [G : \text{Stab}_G(P)] = [G : N_G(P)]$ . De plus, puisque  $P \subset N_G(P)$ , on a  $|E| \mid [G : P] = m$ .

Soit  $H$  un  $p$ -sous-groupe de  $G$ . Alors  $H$  opère par conjugaison sur  $E$ . D'après le lemme 4.14, on a  $|E^H| \equiv |E| \pmod{p}$ . Or  $|E|$  divise  $m$  et  $p \nmid m$  donc  $|E| \not\equiv 0 \pmod{p}$ . On en déduit que  $|E^H| \not\equiv 0 \pmod{p}$  et en particulier que  $E^H \neq \emptyset$ . Soit donc  $Q \in E^H$ . Pour tout  $h \in H$  on a  $hQh^{-1} = Q$  donc  $H \subset N_G(Q)$  et donc  $H \subset Q$  d'après le lemme précédent. Nous avons donc démontré l'assertion (1).

Supposons dans la suite que  $H$  est un  $p$ -sous-groupe de Sylow de  $G$ . Alors si  $Q \in E^H$  on a  $H \subset Q$  et  $|H| = |Q|$  donc  $H = Q \in E$ . Donc  $H$  et  $P$  sont conjugués et on a démontré l'assertion (2). On a également démontré que  $E^H = \{H\}$ .

On déduit de ce qui précède que  $\mathcal{S} = E$  et donc que  $|\mathcal{S}| = |E|$ . On a donc  $|\mathcal{S}| = |E| \equiv |E^H| = 1 \pmod{p}$ . Enfin, on a remarqué plus tôt que  $|E| \mid m$  donc  $|\mathcal{S}| \mid m$  et on a démontré l'assertion (3). ✓

**Remarque.** Il découle de la démonstration précédente que le nombre de  $p$ -sous-groupes de Sylow de  $G$  est  $[G : N_G(H)]$  où  $H$  est un  $p$ -sous-groupe de Sylow de  $G$ .

**Corollaire 4.25.** Un groupe fini possède un seul  $p$ -sous-groupe de Sylow si et seulement si ce sous-groupe est normal.

*Démonstration.* Soit  $H$  un  $p$ -sous-groupe de Sylow de  $G$ . L'ensemble des  $p$ -sous-groupes de Sylow de  $G$  est

$$\mathcal{S} = \{xHx^{-1} \mid x \in G\}$$

Alors  $|\mathcal{S}| = 1 \iff \mathcal{S} = \{H\} \iff \forall x \in G, (xHx^{-1} = H) \iff H \triangleleft G.$  ✓

#### IV. APPLICATIONS À LA CLASSIFICATION DES GROUPES FINIS

On propose dans ce paragraphe des applications des théorèmes de Sylow.

**Théorème 4.26.** Soient  $p$  et  $q$  des nombres premiers distincts et soit  $G$  un groupe d'ordre  $pq$ .

- (1) Alors  $G$  n'est pas simple et si  $p > q$ , alors  $G$  est isomorphe à un produit semi-direct  $C_p \rtimes C_q$ .
- (2) Si  $p \not\equiv 1 \pmod{q}$  et  $q \not\equiv 1 \pmod{p}$ , alors  $G$  est cyclique. (exemples :  $|G| = 15, 35, \dots$ ).

*Démonstration.* (1) Soit  $H$  un  $p$ -sous-groupe de Sylow de  $G$  et soit  $K$  un  $q$ -sous-groupe de Sylow de  $G$  (qui existent par le premier théorème de Sylow). Alors  $|H| = p$  est premier donc  $H \cong C_p$  et  $|K| = q$  donc  $K \cong C_q$ . Le nombre  $n_p$  de  $p$ -sous-groupes de Sylow vérifie  $n_p \equiv 1 \pmod{p}$  et  $n_p \mid q$  d'après le deuxième théorème de Sylow. Si on pose  $n_p = 1 + kp$  avec  $k \in \mathbb{N}$ , puisque  $p > q$  et  $n_p \mid q$ , on doit avoir  $k = 0$  et donc  $n_p = 1$ . Donc  $H$  est l'unique  $p$ -sous-groupe de Sylow de  $G$  et par conséquent  $H \triangleleft G$  d'après le corollaire 4.25. En particulier,  $G$  n'est pas simple.

Puisque  $\text{pgcd}(p, q) = 1$ , grâce au théorème de Lagrange on a  $H \cap K = \{1\}$  et  $|HK| = pq = |G|$  donc  $G = HK$ . On en déduit grâce à la caractérisation du produit semi-direct du théorème 3.5 que  $G \cong H \rtimes K \cong C_p \rtimes C_q$ .

- (2) Quitte à échanger  $p$  et  $q$  on peut supposer que  $p > q$  et on reprend les notations de la première partie de la démonstration. Soit  $n_q$  le nombre de  $q$ -sous-groupes de Sylow de  $G$ . On sait que  $n_q \equiv 1 \pmod{q}$  et que  $n_q \mid p$ , donc  $n_q \in \{1, p\}$ . Si  $n_q \neq 1$ , alors  $p = n_q \equiv 1 \pmod{q}$  et on a obtenu une contradiction. Donc  $n_q = 1$ , ce qui implique que  $K \triangleleft G$  (corollaire 4.25) et donc que  $G \cong C_p \times C_q$  grâce à la caractérisation du produit direct. Enfin, d'après le théorème chinois,  $G \cong C_{pq}$  est cyclique.

*Autre méthode.* Quitte à échanger  $p$  et  $q$  on peut supposer que  $p > q$  et on sait d'après la partie (1) que  $G \cong C_p \rtimes_{\varphi} C_q$  pour une action par automorphismes  $\varphi : C_q \rightarrow \text{Aut}(C_p)$  de  $C_q$  sur  $C_p$ . Notons  $a$  un générateur de  $C_q$ . Alors  $\varphi$  est entièrement déterminé par  $\varphi(a)$ , qui doit être un élément de  $\text{Aut}(C_p)$  tel que  $\varphi(a)^q = 1$ , c'est-à-dire que l'ordre de  $\varphi(a)$  est 1 ou  $q$ . Mais puisque  $p$  est premier,  $\text{Aut}(C_p)$  est (cyclique) d'ordre  $p - 1$ . Par hypothèse,  $q$  ne divise pas  $p - 1$  donc  $\text{Aut}(C_p)$  ne contient pas d'élément d'ordre  $q$ . Ainsi,  $\varphi(a) = 1$ , l'action est triviale et  $C_p \rtimes_{\varphi} C_q \cong C_p \times C_q \cong C_{pq}$  ✓

**Exemple.** Les groupes d'ordre 15 et 35 sont cycliques.

**Exemple.** Nous pouvons maintenant compléter l'exemple page 42 : si  $G$  est un groupe qui n'est pas abélien et dont l'ordre est impair, alors  $|G| \geq 21$ .

En effet, soit  $G$  un groupe d'ordre impair tel que  $|G| < 21$ . Si  $|G|$  est premier alors  $G$  est cyclique donc abélien et si  $|G| = p^2$  avec  $p$  premier alors  $G$  est abélien d'après le théorème 4.16. Il reste le cas d'un groupe d'ordre 15, qui est abélien d'après le théorème précédent.

**Remarque.** Si  $p$  et  $q$  sont deux nombres premiers tels que  $p > q$  et  $q \mid (p-1)$ , on peut montrer qu'il y a, à isomorphisme près, deux groupes d'ordre  $pq$  : le groupe cyclique  $C_{pq}$  et un produit semi-direct non abélien  $C_p \rtimes C_q$ . (C'est le cas par exemple des groupes d'ordre 21.)

En effet, puisque  $p > q$ , nous avons vu dans la démonstration du théorème 4.26 que si  $|G| = pq$  alors  $G$  est isomorphe à un produit semi-direct  $G \cong C_p \rtimes_{\varphi} C_q$ , où  $\varphi: C_q \rightarrow \text{Aut}(C_p)$  est le morphisme d'une opération de  $C_q$  sur  $C_p$  par automorphismes.

Notons  $a$  un générateur de  $C_q$ . Alors  $\varphi$  est entièrement déterminé par  $\varphi(a) \in \text{Aut}(C_p)$ , qui doit être un élément dont l'ordre divise  $q$ , c'est-à-dire 1 ou  $q$ . Or  $\text{Aut}(C_p) \cong C_{p-1}$  et  $q \mid (p-1)$  donc il existe des éléments d'ordre  $q$  dans  $\text{Aut}(C_p)$ .

Si  $\varphi(a) = \text{id}_{C_p}$ , alors l'opération  $\varphi$  est triviale. Ainsi,  $G$  est abélien et  $G \cong C_{pq}$ .

Si  $\varphi(a)$  est d'ordre  $q$ , alors l'opération  $\varphi$  n'est pas triviale et  $G$  n'est pas abélien. Nous devons démontrer que toutes les opérations non triviales de  $C_q$  sur  $C_p$  par automorphismes induisent des produits semi-directs isomorphes.

Soient maintenant  $\varphi, \psi: C_q \rightarrow \text{Aut}(C_p)$  deux actions non triviales. Alors  $\varphi(C_q)$  et  $\psi(C_q)$  sont des sous-groupes de  $\text{Aut}(C_p)$  d'ordre  $q$ . Puisque  $\text{Aut}(C_p)$  est un cyclique d'ordre  $p-1$  et  $q$  divise  $p-1$ , il admet un unique sous-groupe cyclique  $L$  d'ordre  $q$ . On en déduit que  $\varphi(a)$  et  $\psi(a)$  sont deux générateurs de  $L = \varphi(C_q) = \psi(C_q)$  et donc qu'il existe un nombre entier  $k \in \llbracket 1; q-1 \rrbracket$  (premier à  $q$ ) tel que  $\varphi(a) = \psi(a)^k$ . Soit  $\alpha: C_q \rightarrow C_q$  l'unique automorphisme de  $C_q$  défini par  $\alpha(a) = a^k$  (voir la proposition 3.4). On a  $\psi \circ \alpha(a) = \psi(a^k) = \psi(a)^k = \varphi(a)$  donc  $\psi \circ \alpha = \varphi$  (car  $a$  engendre  $C_q$ ). On en déduit que  $C_p \rtimes_{\varphi} C_q \cong C_p \rtimes_{\psi} C_q$  grâce à un exercice page 42.

## Classification des groupes d'ordre $n \leq 15$ .

**Définition-Proposition 4.27.** Soit  $Q_8$  le sous-groupe de  $\text{GL}_2(\mathbb{C})$  engendré par les éléments  $a, b$  et  $c$  donnés par

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, c = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = ab.$$

C'est un groupe d'ordre 8 qui n'est pas abélien et dont tous les sous-groupes sont normaux dans  $Q_8$  (en particulier,  $Q_8$  n'est pas isomorphe à  $\mathcal{D}_4$ ). Il est appelé **groupe quaternionique**.

*Démonstration.* Voir travaux dirigés

On vérifie que  $a^2 = b^2 = c^2 = -1$ ,  $ab = c = -ba$  (donc  $Q_8$  est engendré par  $\{a, b\}$ ),  $bc = a = -cb$  et  $ca = b = -ac$ . En particulier,  $Q_8$  n'est pas abélien.

Les éléments de  $Q_8$  sont des produits de puissances de  $a$  et de  $b$ ; comme  $ba = -ab = a^3b$  et  $a^4 = 1 = b^4$ , on en déduit que les éléments de  $Q_8$  sont tous de la forme  $a^k b^{\ell}$  avec  $(k, \ell) \in \mathbb{Z}^2$ ,  $0 \leq k, \ell \leq 4$  et donc, puisque  $a^2 = -1 = b^2$ , de la forme  $\pm a^k b^{\ell}$  avec  $(k, \ell) \in \mathbb{Z}^2$ ,  $0 \leq k, \ell \leq 1$ , ce qui donne

$$Q_8 = \{\pm 1, \pm a, \pm b, \pm ab = \pm c\}.$$

Donc  $Q_8$  est d'ordre 8.

Les sous-groupes de  $Q_8$  doivent donc être d'ordre 1, 2, 4 ou 8.

Le seul élément d'ordre 2 de  $Q_8$  est  $-1$ , donc le seul sous-groupe d'ordre 2 est  $\{\pm 1\}$ .

Les autres éléments de  $Q_8$  distincts de l'élément neutre sont tous d'ordre 4. Puisque  $\langle -a \rangle = \langle a^3 \rangle = \langle a \rangle$  (et de même avec les autres éléments), on en déduit qu'il y a trois sous-groupes d'ordre 4, qui sont  $\langle a \rangle$ ,  $\langle b \rangle$  et  $\langle c \rangle$ . Ils sont tous normaux dans  $Q_8$  car ils sont d'indice 2 dans  $Q_8$ .

Il est évident que le groupe trivial et le groupe  $Q_8$  sont les seuls autres sous-groupes de  $Q_8$  et qu'ils sont normaux dans  $Q_8$ .

Vérifions donc que  $\{\pm 1\}$  est normal dans  $Q_8$ . Pour tout  $x \in Q_8$  on a  $x(-1)x^{-1} = -xx^{-1} = -1 \in \{\pm 1\}$  (et bien sûr  $x1x^{-1} = 1 \in \{\pm 1\}$ ). Donc  $\{\pm 1\}$  est un sous-groupe normal de  $Q_8$ .

Enfin, il reste à vérifier que  $Q_8$  n'est pas isomorphe à  $\mathcal{D}_4$ . Cela découle du fait que le sous-groupe de  $\mathcal{D}_4$  engendré par  $s$  n'est pas normal dans  $\mathcal{D}_4$ . En effet,  $rsr^{-1} = r^2s \notin \langle s \rangle$ . ✓

**Définition-Proposition 4.28.** Le groupe dicyclique  $\text{Dic}_n$  d'ordre  $4n$  est le sous-groupe de  $\text{GL}_2(\mathbb{C})$  engendré par les matrices  $a$  et  $b$  données par

$$a = \begin{pmatrix} e^{i\pi/n} & 0 \\ 0 & e^{-i\pi/n} \end{pmatrix} \quad \text{et} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Ces éléments vérifient les relations  $a^{2n} = 1$ ,  $b^2 = a^n$ ,  $ba = a^{-1}b$  et on a

$$\text{Dic}_n = \{a^k b^l \mid 0 \leq k \leq 2n-1, 0 \leq l \leq 1\}.$$

On a  $\text{Dic}_2 \cong Q_8$  et  $\text{Dic}_3 \cong C_3 \rtimes_\varphi C_4$  pour l'opération  $\varphi: C_4 = \langle g \rangle \rightarrow \text{Aut}(C_3)$  définie par  $\varphi(g)(x) = x^{-1}$  pour tout  $x \in C_3$ .

*Démonstration.* Voir travaux dirigés

On vérifie facilement les relations. On peut même préciser que  $a$  est d'ordre  $2n$  et que  $b$  est d'ordre 4. De plus, les relations  $ba = a^{-1}b$  et  $b^2 = a^n$  permettent d'affirmer que  $b^3 = a^n b$  puis que

$$\text{Dic}_n = \{a^u b^l \mid u \in \mathbb{Z}, 0 \leq l \leq 1\}.$$

Effectuons la division euclidienne de  $u$  par  $2n$ , qui s'écrit  $u = q2n + k$  avec  $0 \leq k \leq 2n-1$ . Alors  $a^u b^l = (a^{2n})^q a^k b^l = a^k b^l$ . Donc les éléments de  $\text{Dic}_n$  sont bien ceux de l'énoncé.

On en déduit que  $|\text{Dic}_n| \leq 2n \cdot 2 = 4n$ . Soit maintenant  $(k, l, u, v) \in \mathbb{Z}^4$  avec  $0 \leq k, u \leq 2n-1$  et  $0 \leq l, v \leq 1$  tel que  $a^k b^l = a^u b^v$ . Alors  $a^{-u} a^k = b^v b^{-l}$ .

Si  $v \neq l$ , alors  $a^{k-u} = b^{\pm 1} = \pm b$ . Mais  $a^{k-u}$  est diagonale alors que  $\pm b$  ne l'est pas, c'est donc impossible. On en déduit que  $v = l$ . Alors  $a^{k-u} = I_2$  donc  $2n$  (l'ordre de  $a$ ) divise  $k-u$ . Or  $-2n+1 \leq k-u \leq 2n-1$  donc  $k-u = 0$  et on a  $k = u$ . Ainsi,  $\text{Dic}_n$  a exactement  $4n$  éléments.

Il nous faut maintenant vérifier les isomorphismes.

➤ **Cas  $n = 2$ .** Alors on a  $a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$  et par conséquent  $ab = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ . Le groupe  $\text{Dic}_2$  est le sous-groupe de  $\text{GL}_2(\mathbb{C})$  engendré par  $a$  et  $b$ , donc par  $a$ ,  $b$  et  $ab$ . Il s'agit bien de  $Q_8$  (par définition de  $Q_8$ ).

➤ **Cas  $n = 3$ .** On a alors  $a^3 = -I_2 = b^2$ .

Soit  $N$  le sous-groupe de  $\text{Dic}_3$  engendré par  $a^2$ , il est isomorphe à  $C_3$ . Alors  $N$  est normal dans  $\text{Dic}_3$ ; en effet,  $a \cdot a^2 \cdot a^{-1} = a^2 \in N$  et  $ba^2b^{-1} = a^{-1}bab^{-1} = a^{-2}bb^{-1} = a^{-2} \in N$ .

Soit  $H$  le sous-groupe de  $\text{Dic}_3$  engendré par  $b$ . Il est isomorphe à  $C_4$ . On a donc  $N \cap H = \{1\}$  puisque  $\text{pgcd}(|N|, |H|) = 1$ .

De plus,  $|NH| = \frac{|N||H|}{|N \cap H|} = \frac{3 \cdot 4}{1} = 12 = |\text{Dic}_3|$  donc  $\text{Dic}_3 = NH$ .

On en déduit que  $\text{Dic}_3 \cong N \rtimes_\varphi H \cong C_3 \rtimes_\varphi C_4$  pour un morphisme  $\varphi: C_4 \rightarrow \text{Aut}(C_3)$ .

Le groupe  $\text{Dic}_3$  n'est pas abélien (par exemple, en utilisant les calculs ci-dessus,  $a^{-1}b = a^{-2}ba^{-1} = a^2ba^{-1} \neq ba^{-1}$  car  $a^2 = \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix} \neq I_2$ ), donc le produit ne peut pas être direct et donc  $\varphi$  n'est pas trivial. Le seul automorphisme de  $C_3$  différent de  $\text{id}_{C_3}$  est l'automorphisme  $\theta$  défini par  $\theta(x) = x^{-1}$ ; de plus, il existe bien un morphisme  $\varphi: C_4 \rightarrow \text{Aut}(C_3)$  tel que  $\varphi(b) = \theta$  car  $\theta^4 = \text{id}$  (théorème 1.30). On a donc obtenu le résultat cherché. ✓

**Théorème 4.29.** Tous les groupes d'ordre  $n \leq 15$  sont donnés, à isomorphisme près, dans le tableau suivant.

| ordre du groupe | groupes abéliens                                                                  | groupes non abéliens                       |
|-----------------|-----------------------------------------------------------------------------------|--------------------------------------------|
| 1               | $C_1 = \{1\}$                                                                     |                                            |
| 2               | $C_2$                                                                             |                                            |
| 3               | $C_3$                                                                             |                                            |
| 4               | $C_4$<br>$C_2 \times C_2 \cong \mathcal{D}_2$                                     |                                            |
| 5               | $C_5$                                                                             |                                            |
| 6               | $C_6 \cong C_2 \times C_3$                                                        | $\mathcal{D}_3 \cong S_3$                  |
| 7               | $C_7$                                                                             |                                            |
| 8               | $C_8$<br>$C_4 \times C_2$<br>$C_2 \times C_2 \times C_2$                          | $\mathcal{D}_4$<br>$Q_8$                   |
| 9               | $C_9$                                                                             |                                            |
|                 | $C_3 \times C_3$                                                                  |                                            |
| 10              | $C_{10} \cong C_2 \times C_5$                                                     | $\mathcal{D}_5$                            |
| 11              | $C_{11}$                                                                          |                                            |
| 12              | $C_{12} \cong C_4 \times C_3$<br>$C_2 \times C_6 \cong C_2 \times C_2 \times C_3$ | $\mathcal{D}_6$<br>$A_4$<br>$\text{Dic}_3$ |
| 13              | $C_{13}$                                                                          |                                            |
| 14              | $C_{14} \cong C_2 \times C_7$                                                     | $\mathcal{D}_7$                            |
| 15              | $C_{15} \cong C_3 \times C_5$                                                     |                                            |

*Démonstration.* Pour tous les groupes abéliens et pour les groupes d'ordre  $p$ ,  $p^2$  ou  $2p$  avec  $p$  premier, cela découle des théorèmes 2.16, 1.27, 4.16 et 3.6. Pour les groupes d'ordre 15, c'est le théorème précédent. Il reste les groupes d'ordres 8 et 12, qui seront traités en TD et en DM. ✓



# Groupes symétriques et alternés

Soit  $n \in \mathbb{N}^*$ . On considère le groupe symétrique  $S_n$  des bijections de  $\llbracket 1; n \rrbracket$  dans  $\llbracket 1; n \rrbracket$  (la loi de groupe est la composition des bijections). C'est un groupe d'ordre  $n!$ , qui n'est pas abélien si  $n \geq 3$  (nous verrons même que son centre est trivial si  $n \geq 3$ ).

Ce chapitre est consacré à une étude détaillée des groupes symétriques et de sous-groupes remarquables, les groupes alternés. Du point de vue des groupes abstraits, la motivation est fournie par le théorème suivant.

**Théorème 5.1** (Théorème de Cayley). Soit  $G$  un groupe fini d'ordre  $n$ . Alors  $G$  est isomorphe à un sous-groupe de  $S_n$ .

*Démonstration.* Le groupe  $G$  opère sur lui-même par translations (multiplication à gauche), cela induit un morphisme de groupes  $\varphi: G \rightarrow S_G \cong S_n$  défini par  $\varphi(g)(x) = g.x = gx$ . Il est facile de vérifier que  $\varphi$  est injectif, donc  $\varphi$  induit un isomorphisme  $G \cong \text{Im } \varphi$  et  $\text{Im } \varphi$  est un sous-groupe de  $S_n$ . ✓

Nous rappelons également des définitions et résultats vus en L3 (sans démonstration).

## I. GÉNÉRATEURS DU GROUPE SYMÉTRIQUE

Soient  $k \geq 2$  et  $i_1, \dots, i_k$  dans  $\llbracket 1; n \rrbracket$  deux à deux distincts. On note  $(i_1 \ i_2 \ \dots \ i_k)$  la permutation définie par

$$(i_1 \ i_2 \ \dots \ i_k)(l) = \begin{cases} l & \text{si } l \notin \{i_1, \dots, i_k\} \\ i_{r+1} & \text{si } l = i_r \in \{i_1, \dots, i_{k-1}\} \\ i_1 & \text{si } l = i_k \end{cases}$$

Une permutation de ce type est appelée un  **$k$ -cycle**.

On a le résultat suivant, extrêmement utile pour faire des calculs.

**Lemme 5.2.** Soient  $\sigma \in S_n$  et  $(i_1 \ i_2 \ \dots \ i_k)$  est un  $k$ -cycle. On a

$$\sigma(i_1 \ i_2 \ \dots \ i_k)\sigma^{-1} = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_k))$$

*Démonstration.* Exercice.

Notons  $c = (i_1 \ i_2 \ \dots \ i_k)$  et  $\gamma = (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_k))$ . Soit  $j \in \llbracket 1; n \rrbracket$ .

Supposons que  $\sigma^{-1}(j) \notin \{i_1, \dots, i_k\}$ . Alors  $\sigma c \sigma^{-1}(j) = \sigma(\sigma^{-1}(j)) = j = \gamma(j)$  car, par hypothèse,  $j$  n'est pas dans le support de  $\gamma$ .

Supposons maintenant qu'il existe  $q \in \llbracket 1; k \rrbracket$  tel que  $\sigma^{-1}(j) = i_q$ . Alors  $\sigma c \sigma^{-1}(j) = \sigma c(i_q) = \sigma(i_{q+1}) = \gamma(\sigma(i_q)) = \gamma(j)$  si  $q < k$  et  $\sigma c \sigma^{-1}(j) = \sigma c(i_k) = \sigma(i_1) = \gamma(\sigma(i_k)) = \gamma(j)$  si  $q = k$ .

On en déduit que  $\sigma c \sigma^{-1}(j) = \gamma(j)$  pour tout  $j \in \llbracket 1; n \rrbracket$  et donc que  $\sigma c \sigma^{-1} = \gamma$ . ✓

**Définition 5.3.** Le **support** d'une permutation  $\sigma \in S_n$  est l'ensemble  $\text{Supp}(\sigma) = \{i \in \llbracket 1; n \rrbracket \mid \sigma(i) \neq i\}$ . Par exemple, si  $\sigma = (i_1 \dots i_k)$  est un  $k$ -cycle, le support de  $\sigma$  est  $\{i_1, \dots, i_k\}$ .

On peut vérifier que deux permutations à supports disjoints commutent.  
On ne démontrera pas le théorème (bien connu) suivant.

**Théorème 5.4.** Soit  $\sigma \in S_n \setminus \{\text{id}\}$ . Alors :

- (1) La permutation  $\sigma$  s'écrit comme un produit de cycles à supports disjoints.
- (2) La décomposition de  $\sigma$  en produit de cycles à supports disjoints est unique à l'ordre près des cycles. En particulier, le nombre  $r$  et les longueurs  $\ell_1, \dots, \ell_r$  des cycles non triviaux à supports disjoints dont le produit est égal à  $\sigma$  est entièrement déterminé par  $\sigma$ , et la suite  $[\ell_1, \dots, \ell_r]$  rangée dans l'ordre croissant est appelée le **type** de  $\sigma$ .
- (3) Deux permutations sont conjuguées si, et seulement si, elles ont le même type.

*Démonstration.* Voir cours de L3.

Etant donné un cycle  $c$ , on notera  $\ell(c) = |\text{Supp}(c)|$  sa longueur.

- (1) Soit  $\sigma \in S_n \setminus \{\text{id}\}$ . Le groupe  $S_n$  agit naturellement sur  $\llbracket 1; n \rrbracket$  (le morphisme de groupes correspondant étant  $\text{id}: S_n \rightarrow S_n$ ). On restreint cette action au sous-groupe  $H = \langle \sigma \rangle$  de  $S_n$ .

Les orbites sous l'action de  $H$  forment une partition de  $\llbracket 1; n \rrbracket$ ; notons-les  $X_1, \dots, X_r$ . Pour tout  $k \in \llbracket 1; r \rrbracket$ , on choisit un  $i_k \in X_k$ , on a donc  $X_k = \Omega_H(i_k) = \{\gamma(i_k) \mid \gamma \in H\} = \{\sigma^j(i_k) \mid j \in \mathbb{Z}\}$ .

Pour tout  $i \in \llbracket 1; n \rrbracket$ , l'ensemble  $\{k \in \mathbb{N}^* \mid \sigma^k(i) = i\}$  n'est pas vide car  $\sigma$  est d'ordre fini, on peut donc considérer  $m_i = \min\{k \in \mathbb{N}^* \mid \sigma^k(i) = i\}$ . Vérifions que  $\Omega_H(i) = \{\sigma^j(i) \mid 0 \leq j < m_i\}$ . Il est clair que  $\{\sigma^j(i) \mid 0 \leq j < m_i\} \subset \Omega_H(i)$ . Soit donc  $u \in \Omega_H(i)$ , il existe  $j \in \mathbb{Z}$  tel que  $u = \sigma^j(i)$ . Effectuons la division euclidienne de  $j$  par  $m_i$ , il existe donc  $(q, s) \in \mathbb{Z}^2$  tel que  $j = qm_i + s$  et  $0 \leq s < m_i$ . On a alors  $u = \sigma^j(i) = \sigma^s \circ (\sigma^{m_i})^q(i) = \sigma^s(i)$  car  $\sigma^{m_i}(i) = i$ . On en déduit que  $u \in \{\sigma^j(i) \mid 0 \leq j < m_i\}$  et donc que  $\Omega_H(i) = \{\sigma^j(i) \mid 0 \leq j < m_i\}$ . De plus, si  $(j, j') \in \llbracket 0; m_i - 1 \rrbracket^2$  avec  $j \neq j'$ , on peut supposer sans perte de généralité que  $j < j'$  et on a alors  $0 < j' - j < m_i$  et donc  $\sigma^{j'-j}(i) \neq i$  par définition de  $m_i$  et finalement  $\sigma^{j'}(i) \neq \sigma^j(i)$ .

En particulier, pour  $k \in \llbracket 1; r \rrbracket$ , on a  $X_k = \{\sigma^j(i_k) \mid 0 \leq j < m_{i_k}\}$  et les  $\sigma^j(i_k)$  avec  $0 \leq j < m_{i_k}$  sont deux à deux distincts.

On a donc un  $m_{i_k}$ -cycle  $c_k = (i_k \ \sigma(i_k) \ \dots \ \sigma^{m_{i_k}-1}(i_k))$  et  $\text{Supp}(c_k) = X_k$ .

On a construit ainsi  $r$  cycles à supports disjoints  $c_1, \dots, c_r$ , qui commutent donc deux à deux. Montrons que  $\sigma = c_1 \cdots c_r$ . Soit  $i \in \llbracket 1; n \rrbracket$ . Puisque les  $X_k$  forment une partition de  $\llbracket 1; n \rrbracket$ , il existe un unique  $k \in \llbracket 1; r \rrbracket$  tel que  $i \in X_k = \text{Supp}(c_k)$ . Pour tout  $j \in \llbracket 1; r \rrbracket$  avec  $j \neq k$ , on a  $c_j(i) = i$ , donc  $c_1 \cdots c_r(i) = c_k c_1 \cdots c_{k-1} c_{k+1} \cdots c_r(i) = c_k(i) = \sigma(i)$  et finalement  $c_1 \cdots c_r = \sigma$ .

- (2) Nous allons démontrer, par récurrence sur  $r \in \mathbb{N}^*$ , la proposition  $\mathcal{P}_r$  suivante :

$\mathcal{P}_r$  : « Soient  $c_1, \dots, c_r$  des cycles de longueurs au moins 2 à supports disjoints, soit  $q \in \mathbb{N}$  avec  $q \geq r$  et soient  $c'_1, \dots, c'_q$  des cycles de longueurs au moins 2 à supports disjoints tels que  $c_1 \cdots c_r = c'_1 \cdots c'_q$ . Alors  $q = r$  et il existe  $\tau \in S_r$  tel que  $c'_{\tau(i)} = c_i$  pour tout  $i \in \llbracket 1; r \rrbracket$ . »

Notons que sous les hypothèses de  $\mathcal{P}_r$ , on a  $\bigcup_{i=1}^r \text{Supp}(c_i) = \bigcup_{j=1}^q \text{Supp}(c'_j)$  (unions disjointes) d'après la démonstration de (1). De plus, si  $c$  est un cycle, pour tout  $i \in \text{Supp}(c)$  on a  $\text{Supp}(c) = \{c^j(i) \mid j \in \mathbb{N}\}$  et  $c = (i \ c(i) \ \dots \ c^{m-1}(i))$  avec  $m = |\text{Supp}(c)|$ .

- Initialisation ( $r = 1$ ). Soit  $i \in \text{Supp}(c_1) = \bigcup_{j=1}^q \text{Supp}(c'_j)$ . Alors il existe un unique  $k \in \llbracket 1; q \rrbracket$  tel que  $i \in \text{Supp}(c'_k)$ . On a donc  $c_1(i) = c_1 \cdots c_q(i) = c'_k(i)$  et, pour tout  $j \in \mathbb{N}$ ,  $c_1^j(i) = c'^j_k(i)$  donc  $\text{Supp}(c_1) = \text{Supp}(c'_k)$  et  $c_1 = c'_k$ . Donc nécessairement  $q = 1, k = 1$  et  $c_1 = c'_1$ . La proposition  $\mathcal{P}_1$  est donc vérifiée.
- Hérédité. Soit maintenant  $r \geq 2$  tel que  $\mathcal{P}_{r-1}$  est vraie.  
Soient  $c_1 \cdots c_r = c'_1 \cdots c'_q$  deux décompositions en produits de cycles à supports disjoints non réduits à un point avec  $r \leq q$ .  
Soit  $i \in \text{Supp}(c_1) \subset \bigcup_{j=1}^q \text{Supp}(c'_j)$ . Il existe un unique  $k \in \llbracket 1; q \rrbracket$  tel que  $i \in \text{Supp}(c'_k)$  et le même raisonnement que pour l'initialisation montre que  $c_1 = c'_k$ . On a alors  $c_2 \cdots c_r = c'_1 \cdots c'_{k-1} c'_{k+1} \cdots c'_q$ . Comme  $r - 1 \leq q - 1$ , par hypothèse de récurrence il existe une bijection  $\hat{\tau} : \llbracket 2; r \rrbracket \rightarrow \llbracket 1; q \rrbracket \setminus \{k\}$  telle que pour tout  $j \in \llbracket 2; r \rrbracket$  on a  $c_j = c'_{\hat{\tau}(j)}$ . On définit  $\tau \in S_r$  par  $\tau(j) = \begin{cases} k & \text{si } j = 1 \\ \hat{\tau}(j) & \text{si } j \in \llbracket 2; r \rrbracket. \end{cases}$   
Alors, pour tout  $j \in \llbracket 1; r \rrbracket$  on a  $c_j = c'_{\tau(j)}$ . La proposition  $\mathcal{P}_r$  est donc vérifiée.

(3) Soient  $\sigma$  et  $\sigma'$  deux permutations de  $S_n$ .

- Supposons que  $\sigma$  et  $\sigma'$  sont conjuguées : il existe  $\tau \in S_n$  tel que  $\sigma' = \tau \sigma \tau^{-1}$ . Posons  $\sigma = c_1 \cdots c_r$  avec  $c_1, \dots, c_r$  des cycles de longueurs au moins 2 à supports disjoints. Alors  $\sigma' = c'_1 \cdots c'_r$  avec  $c'_i = \tau c_i \tau^{-1}$  pour tout  $i \in \llbracket 1; r \rrbracket$ . De plus, on sait d'après le lemme 5.2 que  $c'_i$  est un cycle de même longueur que  $c_i$  et de support  $\tau(\text{Supp}(c_i))$ . Comme  $\tau$  est une bijection de  $\llbracket 1; n \rrbracket$  dans  $\llbracket 1; n \rrbracket$ , on en déduit que les  $c'_i$  sont des cycles à supports disjoints et que  $\ell(c_i) = \ell(c'_i)$  pour tout  $i \in \llbracket 1; r \rrbracket$ . Ainsi,  $\sigma$  et  $\sigma'$  ont le même type.
- Supposons que  $\sigma$  et  $\sigma'$  ont le même type. On peut donc écrire  $\sigma = c_1 \cdots c_r$  et  $\sigma' = c'_1 \cdots c'_r$  avec  $c_1, \dots, c_r$  des cycles à supports disjoints,  $c'_1, \dots, c'_r$  des cycles à supports disjoints, et  $\ell(c_i) = \ell(c'_i) \geq 2$  pour tout  $i \in \llbracket 1; r \rrbracket$ .  
On définit une permutation  $\tau \in S_n$  de la façon suivante. Pour tout  $i \in \llbracket 1; n \rrbracket$ , notons  $c_i = (a_{i,1} \dots a_{i,m_i})$  et  $c'_i = (a'_{i,1} \dots a'_{i,m_i})$ ; on pose, pour tout  $i \in \llbracket 1; n \rrbracket$  et tout  $j \in \llbracket 1; m_i \rrbracket$ ,  $\tau(a_{i,j}) = a'_{i,j}$ . De plus, comme  $\text{Supp}(\sigma)$  et  $\text{Supp}(\sigma')$  ont le même cardinal, il existe une bijection  $E := \llbracket 1; n \rrbracket \setminus \text{Supp}(\sigma) \rightarrow \llbracket 1; n \rrbracket \setminus \text{Supp}(\sigma') =: E'$ ; on en choisit une pour définir  $\tau|_E : E \rightarrow E'$ . Ainsi,  $\tau \in S_n$ . De plus, pour tout  $i \in \llbracket 1; r \rrbracket$  on a  $c'_i = (a'_{i,1} \dots a'_{i,m_i}) = (\tau(a_{i,1}) \dots \tau(a_{i,m_i})) = \tau c_i \tau^{-1}$  d'après le lemme 5.2 et finalement  $\sigma' = \tau c_1 \tau^{-1} \cdots \tau c_r \tau^{-1} = \tau \sigma \tau^{-1}$  : les permutations  $\sigma$  et  $\sigma'$  sont bien conjuguées. ✓

Ainsi les cycles engendrent le groupe symétrique. Le lemme suivant va être utile pour trouver des familles plus petites de générateurs.

**Lemme 5.5.** (1) Soient  $i_1, \dots, i_k$  des éléments de  $\llbracket 1; n \rrbracket$  deux à deux distincts. Alors on a  $(i_1 \dots i_k) = (i_1 \ i_2)(i_2 \ i_3) \cdots (i_{k-1} \ i_k)$ .  
(2) Soient  $i, j \geq 2$  avec  $i < j - 1$ . On a  $(i \ j) = (j - 1 \ j)(i \ j - 1)(j - 1 \ i)$ .  
(3) Soient  $1 \leq i < j \leq n$ . On a  $(i \ j) = (1 \ i)(1 \ j)(1 \ i)$ .  
(4) Soit  $\sigma = (1 \ 2 \ \dots \ n)$ . Pour  $i \leq n - 1$ , on a  $(i \ i + 1) = \sigma^{i-1}(1 \ 2)\sigma^{1-i}$ .

*Démonstration.* Ce sont des calculs immédiats. ✓

**Théorème 5.6.** Soit  $n \geq 2$ . Le groupe  $S_n$  est engendré par l'une quelconque des familles suivantes.

- (1) Les transpositions.
- (2) Les transpositions  $(i \ i+1)$  avec  $1 \leq i \leq n-1$ .
- (3) Les transpositions  $(1 \ i)$  avec  $2 \leq i \leq n$ .
- (4) La transposition  $(1 \ 2)$  et le  $n$ -cycle  $\sigma = (1 \ 2 \ \dots \ n)$ .
- (5) Une transposition  $(i \ i+1)$  avec  $1 \leq i \leq n-1$  et le  $n$ -cycle  $\sigma = (1 \ 2 \ \dots \ n)$ .

*Démonstration.* Les points (1) à (4) découlent des points correspondants du lemme précédent (en répétant le point (2) autant de fois que nécessaire).

Le point (5) découle du point (4) en utilisant  $(1 \ 2) = \sigma^{1-i}(i \ i+1)\sigma^{i-1}$ . ✓

Le résultat suivant sera probablement utile pour l'étude de la résolubilité des polynômes (Semestre 2).

**Proposition 5.7.** Soit  $p$  un nombre premier et soit  $G$  un sous-groupe de  $S_p$ . Supposons que  $p \mid |G|$  et que  $G$  contient une transposition. Alors  $G = S_p$ .

*Démonstration.* Il suffit de montrer que  $G$  contient un  $p$ -cycle  $(1 \ 2 \ \dots \ p)$  et une transposition  $(i \ i+1)$ . Tout d'abord on sait que  $G$  contient un élément  $\sigma$  d'ordre  $p$  (conséquence du premier théorème de Sylow), et un élément d'ordre  $p$  de  $S_p$  est nécessairement un  $p$ -cycle car  $p$  est premier. En effet, si  $\sigma$  est un élément d'ordre  $p$ , soit  $\sigma = \gamma_1 \cdots \gamma_r$  sa décomposition en produit de cycles à supports disjoints. Alors les  $\gamma_i$  commutent deux à deux donc  $o(\sigma) = \text{ppcm}(o(\gamma_i) \mid 1 \leq i \leq r)$ . Or  $o(\gamma_i) > 1$  pour tout  $i$  et  $p$  est premier donc  $o(\gamma_i) = p$  pour tout  $i$ . Mais ce sont des cycles de  $S_p$ , leur support est donc  $\llbracket 1; p \rrbracket$  donc  $r = 1$  et  $\sigma = \gamma_1$  est un  $p$ -cycle.

Ecrivons  $\sigma = (i_1 \ \dots \ i_p)$  et soit  $\nu \in S_p$  la permutation définie par  $\nu(i_k) = k$ , on a  $\nu \circ \sigma \circ \nu^{-1} = (1 \ 2 \ \dots \ p) \in \nu G \nu^{-1}$ . On a  $|\nu G \nu^{-1}| = |G|$ , et comme pour montrer que  $G = S_p$  il suffit de voir que  $|G| = |S_p|$ , on peut remplacer  $G$  par  $\nu G \nu^{-1}$  et donc supposer sans perte de généralité que  $(1 \ 2 \ \dots \ p) \in G$ . Notons  $\sigma = (1 \ 2 \ \dots \ p)$ .

A ce stade il est commode de changer de notation : on remplace  $\llbracket 1; p \rrbracket$  par  $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \dots, \overline{p-1}\}$ , et  $G$  est un sous-groupe du groupe des permutations de  $\mathbb{Z}/p\mathbb{Z}$  contenant  $\sigma = (\bar{0} \ \bar{1} \ \dots \ \overline{p-1})$  et une transposition  $\tau = (\bar{i} \ \bar{j})$  avec  $i, j$  dans  $\{0, \dots, p-1\}$  et  $i < j$ . On peut alors écrire, pour tout  $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ ,  $\sigma(\bar{k}) = \bar{k} + 1$ . Montrons, par récurrence sur  $k$ , que

$$\forall k \in \llbracket 1; p-1 \rrbracket, \text{ on a } (\bar{0} \ \overline{k(j-i)}) \in G.$$

➤ Initialisation. Si  $k = 1$ , on a  $\sigma^{-i}(\bar{i} \ \bar{j})\sigma^i = (\bar{0} \ \overline{j-i}) \in G$ .

➤ Hérédité. Soit maintenant  $k \in \llbracket 1; p-2 \rrbracket$  tel que  $(\bar{0} \ \overline{s(j-i)}) \in G$  pour tout  $s \in \llbracket 1; k \rrbracket$  on doit démontrer que  $(\bar{0} \ \overline{(k+1)(j-i)}) \in G$ . On a

$$\sigma^j(\bar{0} \ \overline{k(j-i)})\sigma^{-j} = (\bar{j} \ \overline{j(k+1)-ki}) \in G$$

et on a  $\overline{j(k+1)-ki} = \overline{(j-i)(k+1)} + \bar{i} = \overline{(j-i)k} + \bar{j} \notin \{\bar{i}; \bar{j}\}$  car  $\bar{k} \neq \bar{0}$ ,  $\bar{k}+1 \neq \bar{0}$ ,  $\bar{j}-\bar{i} \neq \bar{0}$  et  $\mathbb{Z}/p\mathbb{Z}$  est un corps. Donc

$$(\bar{i} \ \bar{j})(\bar{j} \ \overline{j(k+1)-ki})(\bar{i} \ \bar{j}) = (\bar{i} \ \overline{j(k+1)-ki}) \in G$$

et

$$\sigma^{-i}(\bar{i} \ \overline{j(k+1)-ki})\sigma^i = (\bar{0} \ \overline{(k+1)(j-i)}) \in G$$

et on a bien le résultat désiré.

Comme  $\mathbb{Z}/p\mathbb{Z}$  est un corps, il existe  $k \in \llbracket 1; p-1 \rrbracket$  tel que  $\overline{k(j-i)} = \overline{1}$ , et ainsi  $(\overline{0} \ \overline{1}) \in G$ , et on conclut bien que  $G = S_p$ . ✓

**Remarque.** Le résultat est faux en général si  $n$  n'est pas premier. Par exemple le groupe  $S_4$  n'est pas engendré par  $(1 \ 2 \ 3 \ 4)$  et  $(1 \ 3)$ .

En effet, on a  $\tau\sigma = \sigma^{-1}\tau$  donc

$$\begin{aligned} \langle \sigma, \tau \rangle &= \left\{ \sigma^k \tau^\ell \mid (k, \ell) \in \mathbb{Z}^2 \right\} = \left\{ \sigma^k \tau^\ell \mid 0 \leq k \leq 3, 0 \leq \ell \leq 1 \right\} \\ &= \{ \text{id}, \tau, (1 \ 4)(2 \ 3), (2 \ 4), (1 \ 2)(3 \ 4), \sigma, (1 \ 3)(2 \ 4), (1 \ 4 \ 3 \ 2) \} \\ &\neq S_4. \end{aligned}$$

## II. LE GROUPE ALTERNÉ

**Définition-Proposition 5.8.** Soit  $n \geq 2$ . Il existe unique morphisme de groupes surjectif

$$\varepsilon: S_n \longrightarrow \{\pm 1\}$$

tel que pour tout  $k$ -cycle  $\sigma$ , on ait  $\varepsilon(\sigma) = (-1)^{k-1}$ . Le morphisme  $\varepsilon$  est appelé la **signature**, et le **groupe alterné**  $A_n$  est défini comme le noyau de  $\varepsilon$ . On a  $A_n \triangleleft S_n$  (puisque  $A_n$  est le noyau du morphisme  $\varepsilon$ , ou parce qu'il est d'indice 2 dans  $S_n$ ) et  $|A_n| = \frac{n!}{2}$ .

*Démonstration.* L'existence a été démontrée en L3. Pour l'unicité, soit  $\varphi: S_n \rightarrow \{\pm 1\}$  un autre morphisme surjectif. On sait que les transpositions engendrent  $S_n$  donc il suffit de vérifier que  $\varphi(\tau) = \varepsilon(\tau)$  pour toute transposition  $\tau$ . Notons que les transpositions sont toutes conjuguées dans  $S_n$  et que tout morphisme défini sur  $S_n$  prendra donc la même valeur sur toutes les transpositions. Il y a donc deux cas :

Cas 1 : pour toute transposition  $\tau$  on a  $\varphi(\tau) = 1$ . Mais alors  $\varphi \equiv 1$  donc  $\varphi$  n'est pas surjectif ; on a obtenu une contradiction.

Cas 2 : pour toute transposition  $\tau$  on a  $\varphi(\tau) = -1$ . On a alors  $\varphi(\tau) = \varepsilon(\tau)$  pour toute transposition  $\tau$  et donc  $\varphi = \varepsilon$ . ✓

*Pour compléter : une démonstration de l'existence de  $\varepsilon$ .* Soit  $\sigma \in S_n$ . Nous savons qu'il existe des transpositions  $\tau_1, \dots, \tau_p$  telles que  $\sigma = \tau_1 \cdots \tau_p$ . Si  $\varepsilon$  existe, la démonstration de l'unicité nous impose  $\varepsilon(\sigma) = \varepsilon(\tau_1) \cdots \varepsilon(\tau_p) = (-1)^p$ . Mais l'écriture de  $\sigma$  comme produit de transpositions n'est pas unique, il faut donc démontrer que la parité du nombre de transpositions dans l'écriture de  $\sigma$  ne dépend que de  $\sigma$ .

**Etape 1.** On suppose que  $n \geq 3$ . Soient  $p \in \mathbb{N}^*$ ,  $\tau_1, \dots, \tau_p$  des transpositions et  $i \in \llbracket 1; n \rrbracket$  fixé. Montrons qu'il existe alors  $q \in \mathbb{N}$  et des transpositions  $\tau'_1, \dots, \tau'_q$  telles que

- ♦  $\tau_1 \cdots \tau_p = \tau'_1 \cdots \tau'_q$  (lorsque  $q = 0$  le produit de droite est id, de support vide);
- ♦  $p + q$  est pair;
- ♦  $i \notin \bigcup_{j=1}^{q-1} \text{Supp}(\tau'_j)$  (attention,  $i$  peut être dans le support de  $\tau'_q$ ).

On raisonne par récurrence à deux pas sur  $p$ .

- Initialisation : si  $p = 1$ , on choisit une transposition quelconque  $\tau$  telle que  $i \notin \text{Supp}(\tau)$  (c'est possible car  $n \geq 3$ ). On a alors  $\tau_1 = \tau^2 \tau_1$  donc en posant  $\tau'_1 = \tau'_2 = \tau$  et  $\tau'_3 = \tau_1$  on a démontré le résultat. Si  $p = 2$ , posons  $\tau_1 = (i \ j)$ ; on distingue quatre cas :

Cas 1.  $\tau_1$  et  $\tau_2$  sont à supports disjoints. Alors on pose  $\tau'_1 = \tau_2$  et  $\tau'_2 = \tau_1$ .

Cas 2.  $\tau_1 = \tau_2$ . Soit  $\tau$  une transposition telle que  $i \notin \text{Supp}(\tau)$  (il en existe car  $n \geq 3$ ). Alors on a  $\tau_1 \tau_2 = \text{id} = \tau^2$  et on pose  $\tau'_1 = \tau'_2 = \tau$ .

Cas 3.  $\tau_2 = (i \ k)$  avec  $k \notin \{i, j\}$ . Alors on pose  $\tau'_1 = (k \ j)$  et  $\tau'_2 = (i \ j)$ .

Cas 4.  $\tau_2 = (j \ k)$  avec  $k \notin \{i, j\}$ . Alors on pose  $\tau'_1 = (k \ j)$  et  $\tau'_2 = (i \ k)$ .

- Soit  $p \geq 3$  tel que le résultat soit vrai aux rangs  $p - 2$  et  $p - 1$ . Soient  $\tau_1, \dots, \tau_p$  des transpositions.

Si  $\tau_1 = \tau_2$  alors  $\tau_1 \cdots \tau_p = \tau_3 \cdots \tau_p$  et on utilise l'hypothèse de récurrence au rang  $p - 2$  (cela fonctionne car  $p$  et  $p - 2$  ont la même parité).

Si  $\tau_1 \neq \tau_2$ , on sait par le cas  $p = 2$  qu'il existe des transpositions  $\tau''_1$  et  $\tau''_2$  telles que  $\tau''_1 \tau''_2 = \tau_1 \tau_2$  et  $i \notin \text{Supp}(\tau'_1)$ . On a  $\tau_1 \cdots \tau_p = \tau''_1 \tau''_2 \tau_3 \cdots \tau_p$ . On applique l'hypothèse de récurrence au rang  $p - 2$  à  $\tau''_2 \tau_3 \cdots \tau_p$ , cela fournit des transpositions  $\tau'_1, \dots, \tau'_q$  telles que  $\tau''_2 \tau_3 \cdots \tau_p = \tau'_1 \cdots \tau'_q$ ,  $p - 1 + q$  est pair et  $i$  n'est pas dans les supports de  $\tau'_1, \dots, \tau'_q$ . On en déduit que  $\tau_1 \cdots \tau_p = \tau''_1 \tau'_1 \cdots \tau'_q$  avec  $p + q + 1$  pair et  $i$  n'est pas dans le support de  $\tau''_1, \tau'_1, \dots, \tau'_q$ . Donc la propriété est vraie au rang  $p$ .

**Etape 2.** Montrons, par récurrence sur  $n \geq 2$ , que la permutation  $\text{id}_{[1,n]}$  ne peut s'écrire que comme un nombre pair de transpositions de  $S_n$ .

- ♦ Initialisation. Si  $n = 2$ , la seule transposition est  $\tau = (1 \ 2)$ , et on a  $\tau^k = \text{id}$  si, et seulement si,  $k$  est pair. Donc la propriété est vraie au rang 2.
- ♦ Soit  $n > 2$  tel que la propriété soit vraie au rang  $n - 1$ . Soient  $\tau_1, \dots, \tau_p$  des transpositions telles que  $\text{id}_{[1,n]} = \tau_1 \cdots \tau_p$ . D'après l'étape 1, il existe  $q \in \mathbb{N}$  avec  $p + q$  pair et des transpositions  $\tau'_1, \dots, \tau'_q$  telles que  $\text{id}_{[1,n]} = \tau'_1 \cdots \tau'_q$  et  $n$  n'est pas dans le support de  $\tau'_1, \dots, \tau'_{q-1}$ . Supposons par l'absurde que  $n$  soit dans  $\text{Supp}(\tau'_q)$ . Alors  $n = \text{id}(n) = \tau'_q(n) \neq n$  et on a une contradiction. Donc  $n$  n'est pas dans  $\text{Supp}(\tau'_q)$ . Mais alors  $\text{id}_{[1,n]}$  est un produit de  $q$  transpositions de  $S_{n-1}$ , donc  $\text{id}_{[1,n-1]}$  aussi. On peut donc appliquer l'hypothèse de récurrence pour déduire que  $q$  est pair et par conséquent que  $p$ , qui a la même parité que  $q$ , est pair.

**Etape 3.** Conclusion. Soit  $\sigma \in S_n$  et supposons qu'il existe des transpositions  $\tau_1, \dots, \tau_p, \tau'_1, \dots, \tau'_q$  telles que  $\sigma = \tau_1 \cdots \tau_p = \tau'_1 \cdots \tau'_q$ . Alors  $\text{id} = \tau_1 \cdots \tau_p \tau'_1 \cdots \tau'_q$  donc  $p + q$  est pair. Finalement on a bien  $(-1)^p = (-1)^q$ .

Nous avons donc défini une application  $\varepsilon : S_n \rightarrow \{\pm 1\}$  qui n'est pas constante et qui est donc surjective. De plus, si  $(\sigma, \sigma') \in S_n^2$ , il existe des transpositions  $\tau_1, \dots, \tau_p, \tau'_1, \dots, \tau'_q$  telles que  $\sigma = \tau_1 \cdots \tau_p$  et  $\sigma' = \tau'_1 \cdots \tau'_q$  et on a alors

$$\varepsilon(\sigma)\varepsilon(\sigma') = (-1)^p(-1)^q = (-1)^{p+q} = \varepsilon(\tau_1 \cdots \tau_p \tau'_1 \cdots \tau'_q) = \varepsilon(\sigma\sigma')$$

donc  $\varepsilon$  est bien un morphisme de groupes. ✓

**Remarque.** On en déduit que  $\widehat{S}_n = \{1, \varepsilon\}$ .

**Proposition 5.9.** Soit  $n \geq 3$ . Le groupe  $A_n$  est engendré par les 3-cycles  $(1 \ 2 \ i)$  pour  $i \geq 3$ .

*Démonstration.* On sait que  $S_n$  est engendré par les cycles  $(1 \ i)$ ,  $i \geq 2$ . Ainsi si  $\sigma \in A_n$ , on a

$$\sigma = (1 \ i_1) \cdots (1 \ i_m)$$

avec, pour tout  $k$ ,  $i_k \geq 2$  et  $m$  pair. Donc  $A_n$  est engendré par les éléments  $(1 \ i)(1 \ j)$ , avec  $i, j \geq 2$  et  $i \neq j$ . On a

$$\begin{aligned} (1 \ i)(1 \ j) &= (1 \ j \ i) \text{ si } 2 \leq i \neq j \leq n, \\ (1 \ j \ i) &= (1 \ 2 \ i)(1 \ 2 \ j)^2 \text{ si } 3 \leq i \neq j \leq n \\ (1 \ i \ 2) &= (1 \ 2 \ i)^2 \text{ si } i \geq 3 \end{aligned}$$

On a donc le résultat. ✓

**Lemme 5.10.** Pour  $n \geq 3$ , le groupe  $A_n$  opère  $(n - 2)$  fois transitivement sur  $\llbracket 1; n \rrbracket$ , c'est-à-dire que pour tout  $((a_1, \dots, a_{n-2}), (b_1, \dots, b_{n-2})) \in (\llbracket 1; n \rrbracket^{n-2})^2$  avec les  $a_i$  deux à deux distincts et les  $b_i$  deux à deux distincts, il existe  $\sigma \in A_n$  tel que pour tout  $i \in \llbracket 1; n - 2 \rrbracket$  on a  $\sigma(a_i) = b_i$ .

*Démonstration.* On complète les ensembles de  $a_i$  et  $b_i$  de façon à avoir  $\{a_1, \dots, a_{n-2}, a_{n-1}, a_n\} = \llbracket 1; n \rrbracket = \{b_1, \dots, b_{n-2}, b_{n-1}, b_n\}$ . Il est clair qu'il existe une (unique) bijection  $f: \llbracket 1; n \rrbracket \rightarrow \llbracket 1; n \rrbracket$  qui envoie  $i$  sur  $a_i$  pour tout  $i$  et une (unique) bijection  $g: \llbracket 1; n \rrbracket \rightarrow \llbracket 1; n \rrbracket$  qui envoie  $i$  sur  $b_i$  pour tout  $i$ . En les composant, on obtient  $\gamma = g \circ f^{-1} \in S_n$  telle que  $\gamma(a_i) = b_i$  pour tout  $i$ .

Si  $\gamma \in A_n$ , c'est terminé. Sinon,  $\sigma = \gamma(a_{n-1} \ a_n) \in A_n$  et vérifie  $\sigma(a_i) = b_i$  pour tout  $i$  avec  $1 \leq i \leq n - 2$ . ✓

**Proposition 5.11.** Soit  $n \geq 5$ . Les 3-cycles sont conjugués dans  $A_n$ .

*Démonstration.* Voir travaux dirigés.

Soient  $\gamma_a = (a_1 \ a_2 \ a_3)$  et  $\gamma_b = (b_1 \ b_2 \ b_3)$  deux 3-cycles. Puisque  $n \geq 5$ , on peut compléter en des ensembles  $\{a_1, \dots, a_{n-2}\}$  et  $\{b_1, \dots, b_{n-2}\}$  à  $n - 2$  éléments. Puisque l'action de  $A_n$  sur  $\llbracket 1; n \rrbracket$  est  $(n - 2)$ -transitive, il existe  $\sigma \in A_n$  tel que  $\sigma(a_i) = b_i$  pour tout  $i$  avec  $1 \leq i \leq n - 2$ . On a alors  $\gamma_b = \sigma \gamma_a \sigma^{-1}$ . ✓

**Remarque.** C'est faux si  $n = 3$  ou  $n = 4$ . Voir travaux dirigés

En effet, si  $n = 3$  alors  $A_3$  est abélien donc les classes de conjugaison sont des singletons. Si  $n = 4$  il y a 8 cycles d'ordre 3; s'ils formaient une seule orbite pour l'opération de conjugaison de  $A_4$  sur lui-même, elle serait donc de cardinal 8. Mais le cardinal d'une orbite divise l'ordre du groupe et ici  $|A_4| = 12$  n'est pas multiple de 8, on a obtenu une contradiction.

**Théorème 5.12.** Soit  $n \geq 5$ . Le groupe  $A_n$  est simple.

*Démonstration.* Soit  $H \neq \{\text{id}\}$  un sous-groupe normal de  $A_n$ . On veut démontrer que  $H = A_n$ . Il suffit de démontrer que  $H$  contient un 3-cycle. En effet, si  $H$  contient un 3-cycle, il contient tous ses conjugués (car  $H \triangleleft A_n$ ) et donc tous les 3-cycles (proposition précédente), qui engendrent  $A_n$ , donc  $A_n \subset H$  et puisque  $H$  est un sous-groupe de  $A_n$ , on aura bien  $H = A_n$ .

Soit  $\sigma \in H \setminus \{\text{id}\}$ . On remarque que pour tout  $\tau \in A_n$ , on a  $\sigma \tau \sigma^{-1} \tau^{-1} = \sigma(\tau \sigma^{-1} \tau^{-1}) \in H$  car  $\sigma \in H$ ,  $\sigma^{-1} \in H$  et  $H \triangleleft A_n$ , et de même  $\tau^{-1} \sigma \tau \sigma^{-1} \in H$ .

Notons  $\sigma = \gamma_1 \cdots \gamma_r$  la décomposition de  $\sigma$  en produit de cycles à supports disjoints. En particulier, ces cycles  $\gamma_1, \dots, \gamma_r$  commutent deux à deux, donc on peut supposer qu'ils sont ordonnés par longueur décroissante. On distingue quatre cas.

**Cas 1.**  $\ell(\gamma_1) \geq 4$ . Posons  $\gamma_1 = (i_1 \ i_2 \ \dots \ i_t)$  avec  $t \geq 4$ . Soit  $\tau = (i_1 \ i_2 \ i_3)$ . Les supports de  $\tau$ ,  $\gamma_2, \dots, \gamma_r$  sont disjoints, donc ces cycles commutent et on a

$$\begin{aligned} \sigma \tau \sigma^{-1} \tau^{-1} &= \gamma_1 \cdots \gamma_r \gamma_r^{-1} \cdots \gamma_2^{-1} \tau \gamma_1^{-1} \tau^{-1} \\ &= \gamma_1 \tau \gamma_1^{-1} \tau^{-1} = (i_2 \ i_3 \ i_4) \tau^{-1} = (i_2 \ i_3 \ i_4)(i_1 \ i_3 \ i_2) = (i_1 \ i_4 \ i_2) \end{aligned}$$

et c'est un élément de  $H$ , donc  $H$  contient un 3-cycle.

**Cas 2.**  $\ell(\gamma_1) = 3$ . Alors  $\sigma^2 \in H$  et  $\sigma^2 = \gamma_1^2 \cdots \gamma_r^2$  est un produit de 3-cycles disjoints car pour tout  $i$ , soit  $\gamma_i$  est un 3-cycle et  $\gamma_i^2$  aussi, soit  $\gamma_i$  est une transposition et  $\gamma_i^2 = \text{id}$ . Ainsi, quitte à remplacer  $\sigma$  par  $\sigma^2$ , on peut supposer que la décomposition de  $\sigma$  en produit de cycles disjoints ne contient pas de transposition, c'est-à-dire que  $\ell(\gamma_i) = 3$  pour tout  $i$ . Si  $r = 1$  c'est terminé, supposons donc que  $r > 1$ .

Alors  $\sigma = \gamma_1 \gamma_2 \sigma'$  avec  $\gamma_1 = (i_1 \ i_2 \ i_3)$ ,  $\gamma_2 = (i_4 \ i_5 \ i_6)$  et  $\sigma' = \gamma_3 \cdots \gamma_r$ . Soit  $\tau = (i_1 \ i_4 \ i_5)$ . Alors comme ci-dessus,  $\sigma \tau \sigma^{-1} \tau^{-1}$  est un élément de  $H$  et il est égal à  $(i_2 \ i_5 \ i_6)(i_1 \ i_5 \ i_4) = (i_1 \ i_6 \ i_2 \ i_5 \ i_4)$ . On est donc ramenés au cas 1 et  $H$  doit donc contenir un 3-cycle.

**Cas 3.**  $\ell(\gamma_1) = 2$  et  $r = 2$ . Posons  $\gamma_1 = (i_1 \ i_2)$  et  $\gamma_2 = (i_3 \ i_4)$ . Puisque  $n \geq 5$  il existe  $i_5 \in \llbracket 1; n \rrbracket \setminus \{i_1; i_2; i_3; i_4\}$ . Posons  $\tau = (i_3 \ i_4 \ i_5)$ . Alors  $\tau^{-1} \sigma \tau \sigma^{-1} \in H$  et  $\tau^{-1} \sigma \tau \sigma^{-1} = (i_3 \ i_5 \ i_4)(i_4 \ i_3 \ i_5) = (i_3 \ i_4 \ i_5)$ . Donc  $H$  contient un 3-cycle.

**Cas 4.**  $\ell(\gamma_1) = 2$  et  $r > 2$ . Alors  $\sigma = \gamma_1 \gamma_2 \sigma'$  avec  $\gamma_1 = (i_1 \ i_2)$ ,  $\gamma_2 = (i_3 \ i_4)$  et  $\sigma' = \gamma_3 \cdots \gamma_r$ . Posons  $\tau = (i_1 \ i_2 \ i_3)$ . Alors  $\tau^{-1} \sigma \tau \sigma^{-1}$  est un élément de  $H$  et puisque  $\tau$  commute avec  $\sigma'$  on a à  $\tau^{-1} \sigma \tau \sigma^{-1} = \tau^{-1} \gamma_1 \gamma_2 \tau (\gamma_1 \gamma_2)^{-1} = (i_1 \ i_3 \ i_2)(i_2 \ i_1 \ i_4) = (i_1 \ i_4)(i_2 \ i_3)$  et on est ramenés au cas 3. Donc  $H$  contient un 3-cycle. ✓

### III. QUELQUES RÉSULTATS SUR LES SOUS-GROUPES DE $S_n$

**Proposition 5.13.** Si  $n \geq 3$ , alors  $Z(S_n) = \{\text{id}\}$ .

*Démonstration.* Voir travaux dirigés.

Soit  $\sigma \in Z(S_n)$ . Supposons que  $\sigma \neq \text{id}$ . Soit  $i \in \text{Supp}(\sigma)$ , on a donc  $\sigma(i) \neq i$ . Puisque  $n \geq 3$ , il existe  $j \in \llbracket 1; n \rrbracket$  tel que  $j \notin \{i, \sigma(i)\}$ . Soit  $\tau = (i \ j)$ . Alors  $\tau \sigma \tau(j) = \tau \sigma(i) = \sigma(i)$  car  $\sigma(i) \notin \{i, j\}$ , et  $\sigma(i) \neq \sigma(j)$  car  $i \neq j$  et  $\sigma$  est injective, donc  $\tau \sigma \tau \neq \sigma$  et donc  $\tau \sigma \neq \sigma \tau$  : on a obtenu une contradiction. Donc  $\sigma = \text{id}$  et on a bien  $Z(S_n) = \{\text{id}\}$ . ✓

**Théorème 5.14.** Pour  $n \neq 4$ , les seuls sous-groupes normaux de  $S_n$  sont  $\{\text{id}\}$ ,  $A_n$  et  $S_n$ .

*Démonstration.* Si  $n = 2$ , alors  $S_2 \cong C_2$  et ses seuls sous-groupes (nécessairement normaux) sont  $\{\text{id}\} = A_2$  et  $S_2$ .

Traisons le cas  $n = 3$ . Soit  $H$  un sous-groupe normal de  $S_3$ , avec  $\{\text{id}\} \subsetneq H \subsetneq S_3$ . Alors  $|H| = 2$  ou  $|H| = 3$ . Si  $|H| = 2$ , posons  $H = \{\text{id}, \sigma\}$  avec  $\sigma$  un élément d'ordre 2. Les seuls éléments d'ordre 2 de  $S_3$  sont les transpositions. qui sont toutes conjuguées donc, puisque  $H \triangleleft S_3$  doivent toutes être dans  $H$  : on a obtenu une contradiction. Si  $|H| = 3$ , alors  $H = \{\text{id}, \sigma_1, \sigma_2\}$  avec  $\sigma_i$  d'ordre 3. Il y a exactement deux éléments d'ordre 3 dans  $S_3$ , qui sont les 3-cycles. On en déduit que  $H = A_3$ .

Supposons maintenant que  $n \geq 5$ . Soit  $H$  un sous-groupe normal de  $S_n$  avec  $\{\text{id}\} \subsetneq H \subsetneq S_n$ . Alors  $H \cap A_n \triangleleft A_n$ . Mais  $A_n$  est simple donc  $H \cap A_n = \{\text{id}\}$  ou  $H \cap A_n = A_n$ .

Si  $H \cap A_n = \{\text{id}\}$ , alors toutes les permutations non triviales de  $H$  sont impaires. On en déduit en particulier que pour tout  $\sigma \in H$  on a  $\sigma^2 = \text{id}$  (puisque  $\sigma^2$  est paire et dans  $H$ ). Fixons  $\sigma \in H \setminus \{\text{id}\}$ . Alors pour tout  $\tau \in H \setminus \{\text{id}\}$  on a  $\sigma \tau = \text{id}$  (pour les mêmes raisons) donc  $\tau = \sigma^{-1} = \sigma$ . Donc  $H = \{\text{id}, \sigma\}$ . Mais si  $\gamma \in S_n$  est du même type que  $\sigma$ , alors  $\gamma$  et  $\sigma$  sont conjuguées, donc puisque  $H \triangleleft S_n$  on doit avoir  $\gamma \in H$  et on a une contradiction.

Donc  $H \cap A_n = A_n$ , on a alors  $A_n \subset H$  et  $[S_n : A_n] = 2$  donc  $H = A_n$ . ✓

**Remarque.** C'est faux si  $n = 4$ ; en effet, le sous-groupe

$$V_4 = \{\text{id}, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\}$$

est normal dans  $S_4$ .

**Théorème 5.15.** Soit  $n \geq 2$  et  $H$  un sous-groupe de  $S_n$ .

(1) Si  $[S_n : H] = 2$ , on a  $H = A_n$ .

(2) Si  $[S_n : H] = n$ , on a  $H \cong S_{n-1}$ .

*Démonstration.* (1) Puisque  $H$  est d'indice 2 dans  $S_n$ , il est normal dans  $S_n$  donc si  $n \neq 4$  on a  $H = A_n$ .

Si  $n = 4$ , le sous-groupe  $H$  de  $S_4$  est toujours un sous-groupe normal de  $S_4$ , d'ordre 12. Par le théorème de Cauchy, il contient un élément d'ordre 3, qui est dans  $S_4$  et qui est donc un 3-cycle. De plus, puisque  $H \triangleleft S_4$ , il suit que tous les 3-cycles sont dans  $H$  car ils sont conjugués dans  $S_4$ . Or les 3-cycles engendrent  $A_4$ , donc  $A_4 \subset H$  et finalement  $H = A_4$ .

(2) Si  $n = 2$  le résultat est trivial.

Si  $n = 4$ , alors  $H$  est un sous-groupe de  $S_4$  d'ordre 6. D'après le théorème 3.6,  $H$  est donc isomorphe à  $C_6$  ou à  $S_3$ . Or  $S_4$ , donc en particulier  $H$ , ne contient aucun élément d'ordre 6, donc  $H \not\cong C_6$  et finalement  $H \cong S_3$ .

Si  $n \neq 4$  et  $n > 2$ , on considère l'opération de  $S_n$  sur l'ensemble  $E = S_n/H$  par translations à gauche, elle induit donc un morphisme de groupes  $\varphi: S_n \rightarrow S_E$  défini par  $\varphi(\sigma)(\tau H) = (\sigma\tau H)$ , où  $(\sigma, \tau) \in S_n^2$ . Puisque  $|E| = n$  on a  $S_E \cong S_n$ .

Le noyau de  $\varphi$  est un sous-groupe normal de  $S_n$ . De plus, il est contenu dans  $H$  (si  $\sigma \in \text{Ker } \varphi$ , en particulier  $\varphi(\sigma)(H) = H$ , c'est-à-dire que  $\sigma H = H$  donc  $\sigma \in H$ ), qui est d'indice  $n > 2$ , donc  $\text{Ker } \varphi = \{\text{id}\}$  d'après le théorème 5.14. Donc  $\varphi$  est un isomorphisme.

On remarque que  $\varphi(H) \subset \text{Stab}_{S_n}(H)$ . De plus, il est clair que  $\text{Stab}_{S_n}(H)$ , qui est l'ensemble des permutations de  $E = S_n/H$  qui fixent le point  $H$ , s'identifie à  $S_{E \setminus \{H\}}$ , qui est isomorphe à  $S_{n-1}$  (via l'identification  $S_E \cong S_n$ ). Puisque  $|H| = (n-1)!$ , on obtient  $H \cong \varphi(H) = \text{Stab}_{S_n}(H) \cong S_{n-1}$ . ✓

**Exercice.** Soit  $G$  un groupe d'ordre 12 qui n'est pas abélien et qui contient un sous-groupe normal  $H$  d'ordre 4. Alors  $G \cong A_4$ . Voir travaux dirigés

*Correction.* Notons que  $H$  est un 4-sous-groupe de Sylow de  $G$  (et, puisque  $H \triangleleft G$ , c'est le seul). On considère l'ensemble  $E$  des 3-sous-groupes de Sylow de  $G$ . Alors  $|E| \equiv 1 \pmod{3}$  et  $|E| \mid 4$ . Si  $|E| = 1$ , alors il y a un unique 3-sous-groupe de Sylow  $L$ , qui est normal dans  $G$  et on en déduit par des méthodes déjà vues précédemment que  $G \cong H \times K$ . Mais  $H$  et  $K$  sont abéliens (d'ordres 3 premier et 4 carré d'un nombre premier) donc  $G$  est abélien : on a obtenu une contradiction.

Donc  $|E| = 4$ . Puisque tous les 3-sous-groupes de Sylow sont conjugués, on peut considérer l'opération de  $G$  sur  $E$  par conjugaison. On obtient donc un morphisme de groupes  $\varphi: G \rightarrow S_E \cong S_4$ . Soit  $K = \text{Ker } \varphi$ .

Soit  $g \in K$ . Alors, pour tout  $L \in E$ , on a  $gLg^{-1} = L$  donc  $g \in N_G(L)$ . On a donc  $K \subset \bigcap_{L \in E} N_G(L)$ . L'autre inclusion est facile à vérifier, donc  $K = \bigcap_{L \in E} N_G(L)$ . De plus,  $L \subset N_G(L)$  et on sait que  $[G : N_G(L)] = |E| = 4$  pour tout  $L \in E$ , donc  $|N_G(L)| = 3 = |L|$  et donc  $L = N_G(L)$ . On a donc  $K = \bigcap_{L \in E} L$ .

Soient maintenant  $L$  et  $L'$  deux 3-sous-groupes de Sylow de  $G$  (des éléments de  $E$ ) et soit  $x \in L \cap L'$ . Si  $x \neq 1$ , alors  $o(x) = 3$  et on a  $L = \{1, x, x^2\} = L'$ , donc  $K = \bigcap_{L \in E} L = \{1\}$ . On a démontré que  $\varphi$  est injectif et donc que  $\varphi(G)$  est un sous-groupe de  $S_4$  d'ordre 12, donc d'indice 2. D'après le théorème 5.15, on a  $\varphi(G) = A_4$  et donc  $G \cong \varphi(G) = A_4$ . ✓



# Groupes résolubles

On étudie dans ce chapitre une classe de groupes que l'on peut « approximer » par des groupes abéliens : les groupes résolubles. Cette notion sera utilisée plus tard (Semestre 2) pour étudier la « résolubilité » par radicaux des équations polynomiales (c'est de là que provient la terminologie).

## I. DÉFINITION ET EXEMPLES

**Définition 6.1.** Soit  $G$  un groupe. On dit que  $G$  est **résoluble** s'il existe une suite croissante de sous-groupes

$$G_0 = \{1\} \subset G_1 \subset \cdots \subset G_m = G$$

tels que pour tout  $i \in \llbracket 0; m-1 \rrbracket$ , on a  $G_i \triangleleft G_{i+1}$  et le groupe quotient  $G_{i+1}/G_i$  est abélien. Une telle suite est appelée **suite de résolubilité** pour  $G$ .

**Exemples.** (1) Un groupe abélien est résoluble.

(2) Le groupe  $S_3$  est résoluble, avec suite de résolubilité

$$\{\text{id}\} \subset A_3 \subset S_3.$$

En effet, on a bien  $\{\text{id}\} \triangleleft A_3 \triangleleft S_3$  et les quotients  $S_3/A_3 \cong C_2$  et  $A_3/\{\text{id}\} \cong C_3$  sont abéliens.

**Lemme 6.2.** Soit  $G$  un groupe et soit  $H$  un sous-groupe normal de  $G$ . On note  $\pi: G \rightarrow G/H$  la surjection canonique.

- (1) Soient  $K$  et  $L$  deux sous-groupes de  $G$  avec  $K \triangleleft L$ . Alors les sous-groupes  $HK$  et  $HL$  de  $G$  vérifient  $HK \triangleleft HL$  et  $HK/H \triangleleft HL/H$ . De plus, on a un morphisme surjectif  $L/K \rightarrow HL/HK$ .
- (2) Soient  $K'$  et  $L'$  deux sous-groupes de  $G/H$  avec  $K' \triangleleft L'$ . Alors  $\pi^{-1}(K') \triangleleft \pi^{-1}(L')$  et  $\pi^{-1}(L')/\pi^{-1}(K') \cong L'/K'$ .

**Démonstration.** (1) Puisque  $H \triangleleft G$ , on sait que  $HK$  et  $HL$  sont des sous-groupes de  $G$  et que  $HK = KH$ . Soit  $(x, y) \in HK \times HL$ . Posons  $x = hk$  et  $y = h'\ell$  avec  $(h, k, h', \ell) \in H \times K \times H \times L$ . Alors

$$yxy^{-1} = h'\ell h k \ell^{-1} h'^{-1} = h'\ell h \ell^{-1} \ell k \ell^{-1} h'^{-1}.$$

Or  $K \triangleleft L$  donc  $\ell k \ell^{-1} \in K$  et donc  $\ell k \ell^{-1} (h')^{-1} \in KH = HK$ . De plus,  $H \triangleleft G$  donc  $\ell h \ell^{-1} \in H$ . On en déduit que  $yxy^{-1} \in HK$  et donc que  $HK \triangleleft HL$ .

Le fait que  $HK/H \triangleleft HL/H$  découle de la correspondance entre les sous-groupes normaux de  $HL$  contenant  $H$  et les sous-groupes normaux de  $HL/H$ .

Enfin, soit  $L \rightarrow HL$  l'injection naturelle, on compose avec la surjection canonique  $HL \rightarrow HL/HK$  pour obtenir un morphisme de groupes  $\varphi$ . Il est clair que  $K \subset \text{Ker } \varphi$  donc  $\varphi$  induit un morphisme  $\bar{\varphi}: L/K \rightarrow HL/HK$  tel que  $\bar{\varphi}(\bar{\ell}) = \varphi(\ell)$  pour tout  $\ell \in L$ .

Soit  $y \in HL/HK$ . Il existe  $x \in HL$  tel que  $y = \bar{x}$  et il existe donc  $(h, \ell) \in H \times L$  tel que  $x = h\ell$ . Alors, dans  $HL/HK$ , on a  $y = \bar{x} = \bar{\ell}$ ; en effet, on a  $h \in HK$  donc  $\bar{h} = \bar{1}$ . On en déduit donc que  $y = \bar{x} = \varphi(\ell) = \bar{\varphi}(\bar{\ell})$  et donc que  $\bar{\varphi}$  est surjectif.

- (2) Puisque  $\pi$  est surjective, on a  $\pi(\pi^{-1}(L')) = L'$ . On considère le morphisme surjectif  $\pi^{-1}(L') \xrightarrow{\pi} L' \rightarrow L'/K'$ . Son noyau est  $\pi^{-1}(K')$  et on applique le premier théorème d'isomorphisme pour conclure.  $\checkmark$

**Proposition 6.3.** Soient  $G$  un groupe et  $H \subset G$  un sous-groupe.

- (1) Si  $G$  est résoluble, alors  $H$  est résoluble.  
(2) Si  $H \triangleleft G$ , alors  $G$  est résoluble  $\iff H$  et  $G/H$  sont résolubles.

*Démonstration.* (1) Supposons  $G$  résoluble et soit

$$G_0 = \{1\} \triangleleft G_1 \triangleleft \cdots \triangleleft G_m = G$$

une suite de résolubilité. Posons, pour  $i \in \llbracket 0; m \rrbracket$ ,  $H_i = H \cap G_i$ . Alors on a

$$H_0 = \{1\} \subset H_1 \subset \cdots \subset H_m = H$$

et  $H_i = H \cap G_i \triangleleft H \cap G_{i+1} = H_{i+1}$  pour  $i \in \llbracket 0; m-1 \rrbracket$ . Le morphisme naturel  $H \cap G_{i+1} \hookrightarrow G_{i+1} \twoheadrightarrow G_{i+1}/G_i$  a pour noyau  $H \cap G_i$  donc il induit un morphisme injectif

$$H_{i+1}/H_i = (H \cap G_{i+1})/(H \cap G_i) \longrightarrow G_{i+1}/G_i$$

et ainsi  $H_{i+1}/H_i$  est isomorphe à un sous-groupe du groupe abélien  $G_{i+1}/G_i$ , et par conséquent  $H_{i+1}/H_i$  est abélien.

Donc  $H_0 = \{1\} \subset H_1 \subset \cdots \subset H_m = H$  est une suite de résolubilité et  $H$  est résoluble.

- (2) Supposons d'abord que  $G$  est résoluble et reprenons la suite de résolubilité précédente pour  $G$ . On sait déjà que  $H$  est résoluble.

Le sous-groupe  $H$  est normal dans  $G$  donc  $HG_i$  est un sous-groupe de  $G$  pour tout  $i$ . On considère les sous-groupes  $HG_i/H$  de  $G/H$ , on obtient la suite de sous-groupes

$$HG_0/H = \{1\} \subset HG_1/H \subset \cdots \subset HG_m/H = G/H$$

On a  $H \triangleleft G$  et  $G_i \triangleleft G_{i+1}$ , donc  $HG_i \triangleleft HG_{i+1}$  et  $HG_i/H \triangleleft HG_{i+1}/H$  d'après le lemme précédent. Toujours d'après ce lemme, on a un morphisme surjectif  $G_{i+1}/G_i \longrightarrow HG_{i+1}/HG_i$  avec  $G_{i+1}/G_i$  abélien. On en déduit que  $(HG_{i+1}/H)/(HG_i/H)$ , qui est isomorphe à  $HG_{i+1}/HG_i$  par le troisième théorème d'isomorphisme, est abélien. On a démontré que  $G/H$  est résoluble.

Réciproquement, supposons que  $H$  et  $G/H$  sont résolubles, et considérons des suites de résolubilité

$$H_0 = \{1\} \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = H \quad \text{et}$$

$$K_0 = \{1\} \triangleleft K_1 \triangleleft \cdots \triangleleft K_n = G/H$$

Notons  $\pi: G \longrightarrow G/H$  la surjection canonique. Alors

$$H_0 = \{1\} \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = H = \pi^{-1}(K_0) \triangleleft \pi^{-1}(K_1) \triangleleft \cdots \triangleleft \pi^{-1}(K_n) = G$$

est une suite de résolubilité pour  $G$ . En effet, d'après le lemme précédent, les groupes  $\pi^{-1}(K_{i+1})/\pi^{-1}(K_i) \cong K_{i+1}/K_i$  sont abéliens.  $\checkmark$

**Remarque.** On peut reformuler le point (2) de la proposition de la façon suivante.

Soit  $1 \rightarrow H \rightarrow G \rightarrow K \rightarrow 1$  une suite exacte de groupes. Alors  $G$  est résoluble si, et seulement si,  $H$  et  $K$  sont résolubles.

On peut maintenant donner de larges classes d'exemples de groupes résolubles et non résolubles.

**Théorème 6.4.** Soit  $G$  un groupe fini.

- (1) Si  $|G| = p^n$ , pour  $p$  premier, alors  $G$  est résoluble.
- (2) Si  $|G| = pq$ , pour  $p, q$  premiers, alors  $G$  est résoluble.
- (3) Si  $|G| < 60$ , alors  $G$  est résoluble.

*Démonstration.* (1) On raisonne par récurrence sur  $n$ .

- ◆ Initialisation. Si  $n = 0$  le résultat est clair, si  $n = 1$  alors  $G$  est cyclique donc abélien et donc résoluble.
- ◆ Hérédité. Soit donc  $n > 1$  tel que tous les groupes d'ordre  $p^i$  avec  $i \leq n - 1$  sont résolubles. Soit  $G$  un groupe d'ordre  $p^n$ . Le théorème 4.16 montre l'existence d'un sous-groupe normal  $H$  de  $G$  d'ordre  $p^{n-1}$ . Le quotient  $G/H$  est d'ordre  $p$  donc cyclique et donc résoluble, et  $H$  est résoluble par hypothèse de récurrence, donc  $G$  est résoluble.

(2) Si  $p = q$ , on est dans le cadre du (1).

Supposons donc que  $p > q$ . Alors grâce au théorème 4.26, on peut supposer que  $G = C_p \rtimes C_q$ . On a une suite exacte  $1 \rightarrow C_p \rightarrow G = C_p \rtimes C_q \rightarrow C_q \rightarrow 1$  avec  $C_p$  et  $C_q$  abéliens, donc résolubles. Donc  $G$  est également résoluble.

(3) Le 3 est à titre culturel. Voir l'annexe sur les groupes? ✓

**Théorème 6.5.** Un groupe simple non abélien n'est pas résoluble.

En particulier, si  $n \geq 5$  alors  $A_n$  n'est pas résoluble.

*Démonstration.* Soit  $G$  un groupe simple qui n'est pas abélien. Puisque  $G$  est simple, la seule suite de résolubilité possible est  $\{1\} \subset G$ , mais  $G$  n'est pas abélien donc ce n'est pas une suite de résolubilité. ✓

**Théorème 6.6.** Soit  $n \in \mathbb{N}^*$ . Le groupe  $S_n$  est résoluble si et seulement si  $n \leq 4$ .

*Démonstration.* Si  $n \leq 2$ , alors  $S_n$  est abélien donc résoluble.

Si  $n = 3$ , alors  $\{\text{id}\} \subset A_3 \subset S_3$  est une suite de résolubilité.

Si  $n = 4$ , alors  $\{\text{id}\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$  est une suite de résolubilité. En effet,  $A_4 \triangleleft S_4$  car  $A_4$  est d'indice 2 dans  $S_4$ , et  $V_4$  est normal dans  $S_4$  et donc dans  $A_4$  car la conjugaison préserve le type d'une permutation et les éléments de  $V_4$  sont id et tous les produits de deux transpositions disjointes. De plus,  $V_4 \cong C_2 \times C_2$  est abélien (tous ses éléments  $\sigma$  vérifient  $\sigma^2 = \text{id}$ ) et les deux autres quotients sont d'ordres premiers donc sont cycliques et donc abéliens.

Enfin, si  $n \geq 5$ , on sait que  $A_n$ , qui est un sous-groupe normal de  $S_n$  n'est pas résoluble, donc  $S_n$  ne peut pas être résoluble d'après la proposition 6.3. ✓

## II. GROUPE DÉRIVÉ

On propose dans ce paragraphe une nouvelle caractérisation des groupes résolubles.

**Définition 6.7.** Soit  $G$  un groupe. Le **groupe dérivé** de  $G$ , noté  $D(G)$  ou encore  $[G, G]$ , est le sous-groupe de  $G$  engendré par les **commutateurs** de  $G$ , c'est-à-dire les éléments de la forme

$$[x, y] := xyx^{-1}y^{-1} \text{ pour } (x, y) \in G^2.$$

Pour  $(x, y) \in G^2$  on a  $[x, y]^{-1} = [y, x]$  et donc l'inverse d'un commutateur est encore un commutateur. Ainsi un élément arbitraire de  $D(G)$  est un produit fini de commutateurs.

**Définition 6.8.** Soient  $G$  un groupe et  $n \in \mathbb{N}^*$ . Le  $n^{\text{ième}}$  **groupe dérivé** de  $G$ , noté  $D^n(G)$ , est défini la manière suivante :

$$D^1(G) = D(G), D^2(G) = D(D(G)), \dots, D^n(G) = D(D^{n-1}(G)), \dots$$

**Remarques.** (1) On a  $D^{n+1}(G) \subset D^n(G)$  pour tout  $n \in \mathbb{N}^*$ .

(2) Si  $H$  et  $K$  sont des sous-groupes de  $G$  avec  $H \subset K$ , alors  $D(H) \subset D(K)$ .

(3)  $G$  est abélien si et seulement si  $D(G) = \{1\}$ .

**Proposition 6.9.** Pour tout  $n \in \mathbb{N}^*$ , le groupe  $D^n(G)$  est un sous-groupe normal de  $G$ .

*Démonstration.* On raisonne par récurrence sur  $n$ .

➤ Initialisation. Si  $n = 1$ , soit  $(x, y, g) \in G^3$ , on a  $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}] \in D(G)$ . Puisque les commutateurs engendrent  $D(G)$ , on en déduit que  $D(G) \triangleleft G$ . Voir travaux dirigés.

➤ Hérédité. Soit  $n \geq 1$  tel que  $D^i(G) \triangleleft G$  pour tout  $i \leq n$ . Démontrons que  $D^{n+1}(G)$  est normal dans  $G$ . Rappelons que  $D^{n+1}(G) = D(D^n(G))$  est engendré par les  $[x, y]$  avec  $(x, y) \in D^n(G)^2$ . Soit  $(x, y, g) \in D^n(G)^2 \times G$ , on a  $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$ . De plus, par hypothèse de récurrence,  $D^n(G) \triangleleft G$  donc  $gxg^{-1}$  et  $gyg^{-1}$  sont dans  $D^n(G)$  et donc  $g[x, y]g^{-1} \in D^{n+1}(G)$ . Puisque les commutateurs d'éléments de  $D^n(G)$  engendrent  $D^{n+1}(G)$ , on en déduit que  $D^{n+1}(G) \triangleleft G$ . ✓

**Définition-Proposition 6.10.** Soit  $G$  un groupe. Le groupe  $G/D(G)$  est abélien. On dit que  $G/D(G)$  est l'**abélianisé** de  $G$ , on le note souvent  $G_{\text{ab}}$ .

*Démonstration.* Soit  $(u, v) \in (G/D(G))^2$ ; il existe  $(x, y) \in G^2$  tel que  $u = \bar{x}$  et  $v = \bar{y}$ . Alors  $[u, v] = [\bar{x}, \bar{y}] = \overline{[x, y]} = \bar{1}$  dans  $G/D(G)$ , donc  $\bar{x}$  et  $\bar{y}$  commutent. ✓

**Proposition 6.11.** Soit  $G$  un groupe et soit  $H \triangleleft G$  un sous-groupe normal de  $G$ . Alors le groupe  $G/H$  est abélien si, et seulement si,  $D(G) \subset H$ .

*Démonstration.* Voir travaux dirigés

Supposons que  $G/H$  soit abélien. Soit  $(x, y) \in G^2$ . On a  $\overline{[x, y]} = [\bar{x}, \bar{y}] = \bar{1}$  car  $G/H$  est abélien. On en déduit que pour tout  $(x, y) \in G^2$ , on a  $[x, y] \in H$ . Puisque les commutateurs engendrent  $D(H)$ , on en déduit que  $D(G) \subset H$ .

Réciproquement, supposons que  $D(G) \subset H$ . Soit  $(u, v) \in (G/H)^2$ ; il existe  $(x, y) \in G^2$  tel que  $u = \bar{x}$  et  $v = \bar{y}$ . Alors  $[u, v] = [\bar{x}, \bar{y}] = \overline{[x, y]}$  et  $[x, y] \in D(G) \subset H$  donc  $[u, v] = \bar{1}$ . Puisque les commutateurs d'éléments de  $G/H$  engendrent  $D(G/H)$ , on en déduit que  $D(G/H) = \{\bar{1}\}$  et donc que  $G/H$  est abélien. ✓

**Exemples.** (1) Pour  $n \geq 3$ , on a  $D(S_n) = A_n$ . Voir travaux dirigés

Puisque  $S_n$  n'est pas abélien, on a  $D(S_n) \neq \{\text{id}\}$ . De plus  $A_n \triangleleft S_n$  et  $S_n/A_n \cong C_2$  est abélien donc  $D(S_n) \subset A_n$ .

Démontrons l'autre inclusion. Soit  $\sigma$  un 3-cycle. Alors  $\sigma^2$  est aussi un 3-cycle donc d'après le théorème 5.4 (3)  $\sigma$  et  $\sigma^2$  sont conjugués dans  $S_n$ . Il existe donc  $\gamma \in S_n$  tel que  $\sigma^2 = \gamma\sigma\gamma^{-1}$ . On en déduit que  $\sigma = \gamma\sigma\gamma^{-1}\sigma^{-1} = [\gamma, \sigma] \in D(S_n)$ . Puisque les 3-cycles engendrent  $A_n$ , on en déduit que  $A_n = D(S_n)$ .

*Remarque.* Pour  $n \neq 4$ , on peut aussi utiliser le fait que  $D(S_n) \triangleleft S_n$  pour déduire que  $D(S_n) = A_n$ , après avoir précisé que  $\{\text{id}\} \subsetneq D(S_n) \subset A_n$ .

(2) Pour  $n \geq 5$ , on a  $D(A_n) = A_n$ . Voir travaux dirigés

On a  $D(A_n) \triangleleft A_n$ . Pour  $n \geq 5$ , le groupe  $A_n$  est simple donc  $D(A_n) = \{\text{id}\}$  ou  $D(A_n) = A_n$ . Mais si on avait  $D(A_n) = \{\text{id}\}$  alors  $A_n \cong A_n / \{\text{id}\} = A_n / D(A_n)$  serait abélien, ce qui n'est pas le cas. Donc  $D(A_n) = A_n$ .

(3) On a  $D(A_4) = V_4$ . Voir travaux dirigés

On a  $V_4 \triangleleft A_4$  et  $A_4 / V_4 \cong C_3$  abélien, donc  $D(A_4) \subset V_4$ . De plus, si  $(i, j, k, l) \in \llbracket 1; 4 \rrbracket^4$  avec  $i, j, k, l$  deux à deux distincts, on a  $(i \ j)(k \ l) = [(i \ j \ k), (i \ j \ l)] \in D(A_4)$  donc  $V_4 = D(A_4)$ .

**Théorème 6.12.** Soit  $G$  un groupe. Alors  $G$  est résoluble si, et seulement si, il existe  $n \in \mathbb{N}^*$  tel que  $D^n(G) = \{1\}$ .

*Démonstration.* ➤ Supposons que  $G$  soit résoluble et soit

$$G_m = \{1\} \subset G_{m-1} \subset \cdots \subset G_0 = G$$

une suite de résolubilité. Montrons, par récurrence sur  $i$ , que pour tout  $i \in \llbracket 1; m \rrbracket$ , on a  $D^i(G) \subset G_i$ . On en déduira que  $D^m(G) \subset G_m = \{1\}$  et donc que  $D^m(G) = \{1\}$ .

- Initialisation. Si  $i = 1$ , le groupe  $G/G_1 = G_0/G_1$  est abélien donc  $D(G) \subset G_1$  d'après la proposition 6.11.
- Hérédité. Soit donc  $i \geq 2$  tel que  $D^{i-1}(G) \subset G_{i-1}$ . Le groupe  $G_{i-1}/G_i$  est abélien, donc  $D(G_{i-1}) \subset G_i$ . Ainsi  $D^i(G) = D(D^{i-1}(G)) \subset D(G_{i-1}) \subset G_i$ , et on a le résultat.

➤ Réciproquement, la suite  $D^n(G) = \{1\} \subset D^{n-1}(G) \subset \cdots \subset D^1(G) \subset D^0(G) := G$  est une suite de résolubilité pour  $G$ . En effet, on a  $D^{i+1}(G) \triangleleft G$  donc  $D^{i+1}(G) \triangleleft D^i(G)$  et  $D^i(G)/D^{i+1}(G) = D^i(G)/D(D^i(G))$  est abélien pour tout  $i \in \llbracket 0; n-1 \rrbracket$ . ✓

Le résultat précédent permet une nouvelle formulation pour la résolubilité.

**Définition 6.13.** Soit  $G$  un groupe. Une suite **normale** pour  $G$  est une suite croissante de sous-groupes normaux de  $G$

$$G_0 = \{1\} \subset G_1 \subset \cdots \subset G_m = G.$$

**Corollaire 6.14.** Soit  $G$  un groupe non trivial. Alors  $G$  est résoluble si et seulement si  $G$  possède une suite normale  $G_0 = \{1\} \subset G_1 \subset \cdots \subset G_m = G$  telle que pour tout  $i \in \llbracket 1; m \rrbracket$  le groupe  $G_i/G_{i-1}$  soit abélien.

*Démonstration.* Soit  $G$  un groupe possédant une suite normale dont tous les quotients sont abéliens. C'est alors une suite de résolubilité pour  $G$ , donc  $G$  est résoluble.

Réciproquement, supposons que  $G$  soit résoluble et soit  $n \in \mathbb{N}^*$  tel que  $D^n(G) = \{1\}$ . Alors on a vu dans la démonstration précédente que la suite  $D^n(G) = \{1\} \subset D^{n-1}(G) \subset \cdots \subset D^1(G) \subset G$  est une suite de résolubilité pour  $G$ . De plus, pour tout  $i \in \llbracket 1; n \rrbracket$  on a  $D^i(G) \triangleleft G$  donc c'est une suite normale pour  $G$  dont tous les quotients sont abéliens. ✓

**Exemple.** On a vu que le groupe  $S_4$  est résoluble. La suite  $\{\text{id}\} \subset V_4 \subset A_4 \subset S_4$  est une suite normale pour  $S_4$  dont tous les quotients sont abéliens.

La suite  $\{\text{id}\} \triangleleft \langle (1 \ 2)(3 \ 4) \rangle \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$  est une suite de résolubilité pour  $S_4$ , mais ce n'est pas une suite normale pour  $S_4$  car  $\langle (1 \ 2)(3 \ 4) \rangle$  n'est pas un sous-groupe normal de  $S_4$ .



# Annexes sur les groupes

## I. RAPPELS ET COMPLÉMENTS SUR LA DUALITÉ (ESPACES VECTORIELS)

Soit  $K$  un corps.

**Définition A.1.** Soit  $V$  un  $K$ -espace vectoriel. L'espace vectoriel dual  $V^*$  de  $V$  est l'espace vectoriel  $\text{Hom}(V, K)$  des formes linéaires sur  $V$ .

**Proposition A.2.** Soit  $V$  un espace vectoriel de dimension finie  $n$ . Soit  $\mathcal{B} = \{e_1, \dots, e_n\}$  une base de  $V$ .

On définit une base  $\mathcal{B}^* = \{e_1^*, \dots, e_n^*\}$  de  $V^*$  en posant

$$e_i^*(e_j) = \delta_{ij} = \begin{cases} 1 & \text{si } j = i \\ 0 & \text{si } j \neq i. \end{cases}$$

Cette base  $\mathcal{B}^*$  est appelée **base duale** de  $\mathcal{B}$ .

En particulier, on a  $\dim(V^*) = \dim(V)$ .

*Démonstration.* Soit  $\alpha \in V^*$  une forme linéaire sur  $V$ .

Supposons que  $\alpha = \sum_{i=1}^n \lambda_i e_i^*$  avec  $(\lambda_1, \dots, \lambda_n) \in K^n$ . Alors, pour tout  $j \in \{1, \dots, n\}$  on a  $\alpha(e_j) = \sum_{i=1}^n \lambda_i e_i^*(e_j) = \sum_{i=1}^n \lambda_i \delta_{ij} = \lambda_j$ . Donc  $\alpha = \sum_{i=1}^n \alpha(e_i) e_i^*$  et l'écriture de  $\alpha$  comme combinaison linéaire des  $e_i^*$  est unique.

Soit maintenant  $\alpha \in V^*$  soit quelconque. Posons  $\beta = \sum_{i=1}^n \alpha(e_i) e_i^* \in V^*$ . Alors pour tout  $j \in \{1, \dots, n\}$  on a  $\beta(e_j) = \sum_{i=1}^n \alpha(e_i) e_i^*(e_j) = \sum_{i=1}^n \alpha(e_i) \delta_{ij} = \alpha(e_j)$ , donc  $\beta$  et  $\alpha$  coïncident sur une base et donc  $\alpha = \beta \in \text{vect}\{\mathcal{B}^*\}$ .

Finalement, on a démontré que  $\alpha$  s'écrit de manière unique comme combinaison linéaire des  $e_i^*$  et donc que  $\mathcal{B}^*$  est une base de  $V^*$ . ✓

**Remarque.** Soit  $V$  un espace vectoriel de dimension finie  $n$ , soit  $\mathcal{B} = \{e_1, \dots, e_n\}$  une base de  $V$  et soit  $\mathcal{B}^* = \{e_1^*, \dots, e_n^*\}$  sa base duale. Pour tout  $\alpha \in V^*$ , on a

$$\alpha = \sum_{i=1}^n \alpha(e_i) e_i^*.$$

**Remarque.** Soit  $V$  un espace vectoriel de dimension finie. Alors  $V$  et  $V^*$  sont isomorphes : il suffit de fixer une base  $\mathcal{B} = \{e_1, \dots, e_n\}$  de  $V$  et sa base duale  $\mathcal{B}^* = \{e_1^*, \dots, e_n^*\}$ , et on définit un isomorphisme  $f: V \rightarrow V^*$  par  $f(e_i) = e_i^*$  pour tout  $i \in \{1, \dots, n\}$ .

Cet isomorphisme dépend de la base choisie de  $V$ .

**Remarque.** Vous verrez probablement au S2 que, dans le cas où  $V$  est muni d'une forme bilinéaire non dégénérée  $b$ , on peut définir un isomorphisme  $V \cong V^*$  qui ne dépend pas des bases (mais qui dépend de  $b$ ) :

$$\begin{aligned} \Psi_b: V &\longrightarrow V^* \\ v &\longmapsto \Psi_b(v) = b(-, v): \quad \begin{array}{ccc} V & \rightarrow & K \\ w & \mapsto & b(w, v) \end{array} \end{aligned}$$

(cf. cours S2 Théorie des corps et algèbre bilinéaire).

**Proposition A.3.** Soit  $V$  un espace vectoriel de dimension finie sur  $K$ . Alors

$$\begin{aligned} \varphi: V &\rightarrow V^{**} \\ v &\mapsto \varphi(v): V^* \rightarrow V \\ &\alpha \mapsto \alpha(v) \end{aligned}$$

est un isomorphisme naturel (il est indépendant de toutes bases de  $V$  que l'on pourrait fixer).

*Démonstration.* Puisque  $\dim(V^{**}) = \dim(V^*) = \dim(V)$ , d'après le théorème du rang il suffit de vérifier que  $\varphi$  est injective.

Soit donc  $v \in \text{Ker}(\varphi)$  avec  $v \neq 0$ . On a donc  $\varphi(v) = 0$ , c'est-à-dire que pour toute forme linéaire  $\alpha \in V^*$  on a  $\varphi(v)(\alpha) = 0$ , autrement dit  $\alpha(v) = 0$ .

Supposons que  $v$  ne soit pas nul. On peut donc compléter  $\{v\}$  en une base  $\mathcal{B} = \{e_1 = v, e_2, \dots, e_n\}$  de  $V$ . Soit  $\mathcal{B}^* = \{e_1^*, \dots, e_n^*\}$  sa base duale. Alors  $e_1^* \in V^*$  mais  $e_1^*(v) = e_1^*(e_1) = 1 \neq 0$  : on a obtenu une contradiction. Donc  $v = 0$ .

On a démontré que  $\varphi$  est injective et donc un isomorphisme de  $V$  dans  $V^{**}$ . ✓

**Définition-Proposition A.4.** Soient  $V$  et  $W$  deux espaces vectoriels sur  $K$ . Soit  $f: V \rightarrow W$  une application linéaire.

Alors on définit une application linéaire  $\tilde{f}: W^* \rightarrow V^*$  par

$$\forall \alpha \in W^*, \tilde{f}(\alpha) = \alpha \circ f.$$

L'application linéaire  $\tilde{f}$  est appelée **transposée** de  $f$ .

Le résultat suivant justifie le nom de la transposée.

**Proposition A.5.** Soient  $V$  et  $W$  deux espaces vectoriels de dimensions finies sur  $K$ . Soit  $\mathcal{B}_V = \{v_1, \dots, v_n\}$  une base de  $V$  et soit  $\mathcal{B}_W = \{w_1, \dots, w_p\}$  une base de  $W$ . On note  $\mathcal{B}_V^*$  et  $\mathcal{B}_W^*$  leurs bases duales. Alors

$$M_{\mathcal{B}_W^*, \mathcal{B}_V^*}(\tilde{f}) = {}^t M_{\mathcal{B}_V, \mathcal{B}_W}(f).$$

*Démonstration.* Notons  $A = M_{\mathcal{B}_V, \mathcal{B}_W}(f) = (a_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$ . Par définition de la matrice de  $f$  dans les bases

$\mathcal{B}_V$  et  $\mathcal{B}_W$  on a, pour tout  $j \in \{1, \dots, n\}$ ,  $f(v_j) = \sum_{i=1}^p a_{ij} w_i$ . On doit démontrer que la matrice de  $\tilde{f}$  dans

les bases  $\mathcal{B}_W^*$  et  $\mathcal{B}_V^*$  est  ${}^t A$ , c'est-à-dire que pour tout  $\ell \in \{1, \dots, p\}$ , on a  $\tilde{f}(w_\ell^*) = \sum_{k=1}^n a_{\ell,k} v_k^*$ .

Puisque  $\tilde{f}(w_\ell^*)$  est une forme linéaire sur  $V$ , on sait que  $\tilde{f}(w_\ell^*) = \sum_{k=1}^n \tilde{f}(w_\ell^*)(v_k) v_k^*$ . Or

$$\tilde{f}(w_\ell^*)(v_k) = w_\ell^*(f(v_k)) = w_\ell^*\left(\sum_{i=1}^p a_{ik} w_i\right) = \sum_{i=1}^p a_{ik} w_\ell^*(w_i) = \sum_{i=1}^p a_{ik} \delta_{\ell,i} = a_{\ell,k}.$$

On en déduit donc que  $\tilde{f}(w_\ell^*) = \sum_{k=1}^n a_{\ell,k} v_k^*$ , ce que l'on voulait. ✓

## II. GROUPES D'ORDRE $n$ AVEC $n < 60$

Le but de cette section est de démontrer le résultat suivant.

**Proposition A.6.** Soit  $G$  un groupe d'ordre  $n$  avec  $n < 60$ .  
Si  $n$  n'est pas premier, alors  $G$  n'est pas simple.

Supposons ce résultat démontré. Nous pouvons alors en déduire le résultat suivant.

**Corollaire A.7.** Soit  $G$  un groupe d'ordre  $n$  avec  $n < 60$ . Alors  $G$  est résoluble.

*Démonstration.* On le démontre par récurrence sur  $n$  avec  $1 \leq n \leq 59$ .

Si  $n$  est premier ou de la forme  $p^r$  avec  $p$  premier et  $r \in \mathbb{N}^*$ , alors  $G$  est résoluble.

Soit maintenant  $n \geq 6$  tel que tout groupe d'ordre  $< n$  soit résoluble. Soit  $G$  un groupe d'ordre  $n$ . Les groupes cycliques étant résolubles (car abéliens), nous pouvons supposer que  $n$  n'est pas premier. D'après la proposition,  $G$  n'est donc pas simple : soit  $H$  un sous-groupe normal propre de  $G$ . Alors  $|H| < n$  et  $|G/H| < n$  donc  $H$  et  $G/H$  sont résolubles et donc  $G$  est résoluble. ✓

Soit maintenant  $G$  un groupe d'ordre  $n$  avec  $n < 60$  et  $n$  pas premier.

On traite les cas suivants, en utilisant les résultats du cours :

- $n = p^r$  avec  $r \geq 2$ ;
- $n = pq$  avec  $p$  et  $q$  premiers ;
- $n = p^\alpha m$  avec  $p$  premier,  $p \nmid m$ ,  $p > m$  et  $\alpha > 1$  ;
- $n = 2^\alpha p$  avec  $p \in \{5, 11, 13\}$  et  $\alpha \in \{2, 3\}$  ou  $p = 7$  et  $\alpha = 2$  ;
- $n = 45$ .

Si  $n = p^r$  avec  $r \geq 2$  ou si  $n = pq$  avec  $p$  et  $q$  premiers, alors  $G$  n'est pas simple (théorèmes 4.16 et 4.26).

Il nous reste donc à considérer les groupes d'ordres 12, 18, 20, 24, 28, 30, 36, 40, 42, 44, 45, 48, 50, 52, 54 et 56.

Commençons par les cas les plus rapides.

- Si  $n = p^\alpha m$  avec  $p$  premier,  $p \nmid m$ ,  $p > m$  et  $\alpha > 1$ , alors le nombre  $n_p$  de  $p$ -Sylow de  $G$  vérifie :  $n_p \equiv 1 \pmod{p}$  et  $n_p \mid m$ . En particulier,  $n_p < p$  donc  $n_p = 1$ . Donc  $G$  ne contient qu'un  $p$ -Sylow, qui est donc normal dans  $G$ , donc  $G$  n'est pas simple.  
Cela s'applique pour  $n = 18, n = 50$  et  $n = 54$ .
- Si  $n = 2^\alpha p$  avec  $p \in \{5, 11, 13\}$  et  $\alpha \in \{2, 3\}$  ou  $p = 7$  et  $\alpha = 2$ . Alors  $n_p \equiv 1 \pmod{p}$  et  $n_p$  divise  $2^\alpha$  et on en déduit dans chaque cas que  $n_p = 1$ . On conclut comme dans le cas précédent.  
Cela s'applique pour  $n \in \{20, 28, 40, 44, 52\}$ .
- Si  $n = 45 = 3^2 \cdot 5$ , on applique le même type d'argument (il n'y a qu'un 5-Sylow dans  $G$ ) pour démontrer que  $G$  n'est pas simple.

**Lemme A.8.** Soit  $G$  un groupe d'ordre  $n = pqr$  avec  $p, q, r$  des nombres premiers,  $p < q < r$ . Alors  $G$  n'est pas simple.

*Démonstration.* Supposons par l'absurde que  $G$  soit simple. Si on note  $n_p$  (resp.  $n_q$ , resp.  $n_r$ ) le nombre de  $p$ -Sylow (resp.  $q$ -Sylow, resp.  $r$ -Sylow), alors  $n_p \neq 1$ ,  $n_q \neq 1$  et  $n_r \neq 1$ .

On sait que  $n_r \equiv 1 \pmod{r}$  donc  $n_r \geq r + 1$ . De plus,  $n_r$  divise  $pq$  donc, puisque  $p < r$  et  $q < r$  on doit avoir  $n_r = pq$ .

On sait que  $n_q \equiv 1 \pmod{q}$  donc  $n_q > q$ . De plus,  $n_q \mid pr$  donc  $n_q \in \{p, r, pr\}$ . On en déduit que  $n_q \geq r$ . De même,  $n_p \geq q$ .

De plus, tous les sous-groupes de Sylow de  $G$  sont d'ordres premiers. Grâce au théorème de Lagrange, l'intersection de deux quelconques des sous-groupes de Sylow d'ordres différents est  $\{1\}$ . De plus, l'intersection de deux sous-groupes de Sylow distincts de même ordre est également  $\{1\}$  car tout élément différent de l'élément neutre engendre le groupe. On peut donc minimiser le nombre d'éléments de  $G$  (en comptant les éléments non triviaux de chaque sous-groupe de Sylow et en ajoutant l'élément neutre) : il y a au moins

$$\begin{aligned} n_r(r-1) + n_q(q-1) + n_p(p-1) + 1 &\geq pq(r-1) + r(q-1) + q(p-1) + 1 \\ &= pqr + r(q-1) - q + 1 \end{aligned}$$

éléments dans  $G$ . Or  $q \geq 3$  et  $r > q$  donc  $r(q-1) - q + 1 \geq r^2 - r + 1 = r + 1 > 0$  donc il y a plus de  $pqr$  éléments dans  $G$  et on a obtenu une contradiction.

Donc  $G$  n'est pas simple. ✓

Ce lemme s'applique pour  $n = 30$  et pour  $n = 42$ .

Un argument de comptage similaire permet de traiter le cas  $n = 56 = 2^3 \cdot 7$ . Le nombre  $n_7$  de 7-Sylow vérifie  $n_7 \equiv 1 \pmod{7}$  et  $n_7 \mid 8$ , donc  $n_7 \in \{1, 8\}$ . Si  $n_7 = 1$  alors le 7-Sylow est normal dans  $G$  et  $G$  n'est donc pas simple. Supposons donc que  $n_7 = 8$ . L'intersection de deux quelconques des 7-sous-groupes de Sylow, qui sont cycliques d'ordre premier 7, est  $\{1\}$ , donc il y a  $8 \cdot (7 - 1) = 48$  éléments d'ordre 7 dans  $G$ . Ces éléments ne sont pas dans les 2-Sylow (d'ordre 8), il reste 8 éléments dans  $G$ , donc il y a un unique 2-Sylow, qui est donc normal dans  $G$  et donc  $G$  n'est pas simple.

Pour les cas qui restent, nous utiliserons le lemme suivant.

**Lemme A.9.** Soit  $G$  un groupe d'ordre  $n$ , soit  $p$  un diviseur premier de  $n$ , soit  $n_p$  le nombre de  $p$ -Sylow de  $G$ . On suppose que  $n \nmid n_p!$ . Alors  $G$  n'est pas simple.

*Démonstration.* Supposons par l'absurde que  $G$  soit simple. En particulier,  $n_p > 1$ . Soit  $E$  l'ensemble des  $p$ -Sylow de  $G$ . Le groupe  $G$  opère par conjugaison sur  $E$  (la conjugaison préserve les cardinaux). On en déduit un morphisme de groupes  $\varphi: G \rightarrow S_E \cong S_{n_p}$ . On sait que les  $p$ -Sylow sont tous conjugués, donc l'action est transitive et par conséquent le morphisme  $\varphi$  n'est pas trivial. Puisque  $\varphi$  n'est pas trivial,  $\text{Ker } \varphi \neq G$ . Or  $G$  est simple et  $\text{Ker } \varphi \triangleleft G$ , donc  $\text{Ker } \varphi = \{1\}$ . Donc  $G \cong \varphi(G)$  et  $\varphi(G)$  est un sous-groupe de  $S_{n_p}$  donc  $n$  divise  $|S_{n_p}| = n_p!$ . On a obtenu une contradiction, donc  $G$  n'est pas simple. ✓

**Corollaire A.10.** Soit  $G$  un groupe d'ordre  $n = p^\alpha q^\beta$  avec  $p$  et  $q$  deux nombres premiers distincts,  $(\alpha, \beta) \in (\mathbb{N}^*)^2$ . On suppose que  $n \nmid p^\alpha!$  ou  $n \nmid q^\beta!$ . Alors  $G$  n'est pas simple.

*Démonstration.* Supposons par exemple que  $n \nmid q^\beta!$ . Le nombre  $n_p$  de  $p$ -Sylow de  $G$  divise  $q^\beta$  donc en particulier  $n_p \leq q^\beta$ . Mais alors  $n \nmid n_p!$  et on peut appliquer le lemme. ✓

Ce corollaire s'applique directement pour  $n \in \{12, 24, 48, 36\}$ .

Nous avons donc traité tous les cas et démontré dans chacun des cas que  $G$  n'est pas simple.

### III. GROUPES D'ORDRE 8

Voir travaux dirigés

Soit  $G$  un groupe d'ordre 8.

- (1) Caractériser  $G$  à isomorphisme près s'il contient un élément d'ordre 8 ou si tous ses éléments distincts de l'élément neutre sont d'ordre 2.

Dans la suite on suppose qu'on n'est pas dans un de ces deux cas.

- (2) Démontrer que  $G$  contient un élément d'ordre 4, que l'on notera  $a$ .
- (3) En déduire qu'il existe un élément  $b$  de  $G$ , qui n'est pas dans  $\langle a \rangle$ , et tel que  $G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ .
- (4) Démontrer alors que  $ba \in \{ab, a^3b\}$  (on pourra calculer  $ba^2$  pour éliminer une des possibilités).
- (5) On suppose que  $ba = ab$ . Démontrer que  $G$  est commutatif et isomorphe à  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
- (6) On suppose que  $ba = a^3b$ . Démontrer que l'on ne peut pas construire entièrement la table de multiplication de  $G$  avec cette information, puis démontrer que si  $b^2 = 1$  alors  $G \cong \mathcal{D}_4$  à l'aide d'un produit semi-direct. Enfin, démontrer que si  $b^2 = a^2$  alors  $G \cong Q_8$  (on pourra écrire les tables de multiplication des deux groupes).
- (7) En déduire qu'il n'existe que cinq groupes d'ordre 8 à isomorphisme près :

$$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathcal{D}_4, Q_8.$$

*Correction.* (1) On sait que si  $G$  contient un élément  $x$  d'ordre 8, alors  $G = \langle x \rangle \cong \mathbb{Z}/8\mathbb{Z}$ . On a également vu que si  $x^2 = 1$  pour tout  $x \in G$  alors  $G$  est abélien et  $G \cong (\mathbb{Z}/2\mathbb{Z})^3$ .

(2) Les ordres possibles d'éléments de  $G$  sont les diviseurs de 8, c'est-à-dire 1, 2, 4 ou 8. On a supposé qu'ils ne sont pas tous d'ordre 2, qu'il n'y a pas d'élément d'ordre 8 et ils ne peuvent pas y avoir d'autre élément que le neutre d'ordre 1, il y a donc nécessairement un élément  $a$  d'ordre 4 dans  $G$ .

(3) L'élément  $a$  engendre un sous-groupe d'ordre 4 de  $G$ , donc  $\langle a \rangle \subsetneq G$ . Soit donc  $b \in G \setminus \langle a \rangle$ . Notons  $H = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ . Bien sûr on a  $H \subset G$ . Pour montrer que  $H = G$ , il suffit de vérifier que  $|H| = |G| = 8$ .

On a choisi  $b \notin \langle a \rangle = \{1, a, a^2, a^3\}$ . On en déduit que pour tout  $k$  avec  $0 \leq k \leq 3$ , on a  $a^k b \notin \{1, a, a^2, a^3\}$  (sinon  $b = a^{-k}(a^k b)$  serait dans  $\langle a \rangle$ ). De plus, si  $a^k b = a^\ell b$  avec  $0 \leq k, \ell \leq 3$ , alors  $a^k = a^\ell$  donc  $k = \ell$ . Donc les éléments de  $H$  sont deux à deux distincts, on a  $|H| = 8$  et  $G = H$ .

(4) Si  $ba \in \langle a \rangle$ , alors  $b = (ba)a^{-1} \in \langle a \rangle$  et on a obtenu une contradiction. Si  $ba = b$  alors  $a = 1$ , une contradiction. Enfin, si  $ba = a^2b$ , alors  $ba^2 = (ba)a = (a^2b)a = a^2(ba) = a^4b = b$ , donc  $a^2 = 1$ , une contradiction. Donc  $ba \in \{ab, a^3b\}$ .

(5) Cas où  $ba = ab$ . La description des éléments de  $G$  montre que  $G$  est engendré par  $a$  et  $b$ . Comme ils commutent, le groupe  $G$  est abélien.

D'après la classification des groupes abéliens finis (théorème 2.16) et la question (1), on sait alors que  $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ .

**Autre méthode, si on ne connaît pas encore la classification des groupes abéliens finis :** On considère les sous-groupes (forcément normaux)  $\langle a \rangle$  et  $\langle b \rangle$  de  $G$ . On a toujours  $\langle a \rangle \langle b \rangle \subset G$ . De plus,  $G$  est abélien donc  $\langle a \rangle \langle b \rangle = \langle b \rangle \langle a \rangle = \langle a, b \rangle = G$ .

L'ordre de  $b$  est 2 ou 4 (car il n'y a pas d'élément d'ordre 8).

Si  $o(b) = 2$ , alors  $|\langle a \rangle \cap \langle b \rangle| = \frac{|\langle a \rangle| |\langle b \rangle|}{|\langle a, b \rangle|} = 1$  donc  $\langle a \rangle \cap \langle b \rangle = \{1\}$ . On en déduit alors que  $G \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

Si  $o(b) = 4$ , alors  $b^2 \neq 1$  et  $b^2 \notin \{b, ab, a^2b, a^3b\}$  (sinon  $b$  serait dans  $\langle a \rangle$ ), donc  $b^2 \in \langle a \rangle$  et  $o(b^2) = 2$  donc  $b^2 = a^2$ . On en déduit que  $(ab)^2 = a^2b^2 = a^4 = 1$  donc  $ab$  est un élément d'ordre 2. De plus,  $ab \notin \langle a \rangle$  donc  $\langle a \rangle \cap \langle ab \rangle = \{1\}$ . En calculant les cardinaux on voit que  $G = \langle a \rangle \langle ab \rangle$  et on conclut que  $G \cong \langle a \rangle \times \langle ab \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

(6) Cas où  $ba = a^3b = a^{-1}b$ . L'ordre de  $b$  est 2 ou 4 (car il n'y a pas d'élément d'ordre 8).

♦ Supposons que l'ordre de  $b$  soit 2, c'est-à-dire que  $b^2 = 1$ . On a donc  $a^4 = 1$ ,  $b^2 = 1$ ,  $ba = a^{-1}b$  (qui sont les relations vérifiées par les générateurs de  $\mathcal{D}_4$ ).

Soit  $K = \langle a \rangle$  et  $L = \langle b \rangle$ . Alors  $|K| = 4$ ,  $|L| = 2$  et  $G = KL$ . On en déduit grâce aux cardinaux que  $K \cap L = \{1\}$ . De plus,  $K$  est d'indice 2 donc normal dans  $G$ .

On en déduit que  $G \cong K \rtimes_\varphi L$  avec  $\varphi: L \rightarrow \text{Aut}(K)$ . Notons que  $K \cong C_4$  et  $L \cong C_2$ . On sait que  $\text{Aut}(C_4)$  a deux éléments, l'automorphisme identité et l'unique automorphisme  $\alpha$  qui envoie le générateur  $a$  de  $C_4$  sur  $a^3 = a^{-1}$ . Dans le premier cas on obtient un produit direct, qui est donc abélien, donc ce n'est pas  $G$ . Ainsi,  $\varphi$  est défini par  $\varphi(b) = \alpha$ , qui n'est pas trivial, et on a vu en cours que dans ce cas  $K \rtimes_\varphi L = \text{Di}(C_4) \cong \mathcal{D}_4$ .

♦ Supposons que l'ordre de  $b$  soit 4. Alors  $b^2 \neq 1$  et  $b^2 \notin \{b, ab, a^2b, a^3b\}$  (sinon  $b$  serait dans  $\langle a \rangle$ ), donc  $b^2 \in \langle a \rangle$  et  $o(b^2) = 2$  donc  $b^2 = a^2$ . Dans ce cas,  $a$  et  $b$  sont d'ordre 4 et on a  $(ab)^2 = a^2b^2 = a^4 = 1$ .

Posons  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  et  $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$  dans  $\text{GL}_2(\mathbb{C})$ , ils engendrent  $Q_8$ . Posons également  $C = AB$ .

Les tables de  $G$  et de  $Q_8$  sont les mêmes si on fait correspondre  $a$  et  $A$  d'une part, et  $b$  et  $B$  d'autre part.

| G                | 1                | a                | a <sup>2</sup>   | a <sup>3</sup>   | b                | ab               | a <sup>2</sup> b | a <sup>3</sup> b |
|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| 1                | 1                | a                | a <sup>2</sup>   | a <sup>3</sup>   | b                | ab               | a <sup>2</sup> b | a <sup>3</sup> b |
| a                | a                | a <sup>2</sup>   | a <sup>3</sup>   | 1                | ab               | a <sup>2</sup> b | a <sup>3</sup> b | b                |
| a <sup>2</sup>   | a <sup>2</sup>   | a <sup>3</sup>   | 1                | a                | a <sup>2</sup> b | a <sup>3</sup> b | b                | ab               |
| a <sup>3</sup>   | a <sup>3</sup>   | 1                | a                | a <sup>2</sup>   | a <sup>3</sup> b | b                | ab               | a <sup>2</sup> b |
| b                | b                | a <sup>3</sup> b | a <sup>2</sup> b | ab               | a <sup>2</sup>   | a                | 1                | a <sup>3</sup>   |
| ab               | ab               | b                | a <sup>3</sup> b | a <sup>2</sup> b | a <sup>3</sup>   | a <sup>2</sup>   | a                | 1                |
| a <sup>2</sup> b | a <sup>2</sup> b | ab               | b                | a <sup>3</sup> b | 1                | a <sup>3</sup>   | a <sup>2</sup>   | a                |
| a <sup>3</sup> b | a <sup>3</sup> b | a <sup>2</sup> b | ab               | b                | a                | 1                | a <sup>3</sup>   | a <sup>2</sup>   |

| Q <sub>8</sub> | 1  | A  | -1 | -A | B  | C  | -B | -C |
|----------------|----|----|----|----|----|----|----|----|
| 1              | 1  | A  | -1 | -A | B  | C  | -B | -C |
| A              | A  | -1 | -A | 1  | C  | -A | -C | B  |
| -1             | -1 | -A | 1  | A  | -B | -C | B  | C  |
| -A             | -A | 1  | A  | -1 | -C | A  | C  | -B |
| B              | B  | -C | -B | C  | -1 | A  | 1  | -A |
| C              | C  | B  | -C | -B | -A | -1 | A  | 1  |
| -B             | -B | C  | B  | -C | 1  | -A | -1 | A  |
| -C             | -C | -B | C  | B  | A  | 1  | -A | -1 |

(7) Les questions précédentes montrent qu'il y a au plus les cinq possibilités de l'énoncé. Il faut vérifier qu'il n'y a aucun isomorphisme entre ces groupes.

Les groupes  $\mathcal{D}_4$  et  $Q_8$  ne sont pas abéliens, donc ne sont pas isomorphes à l'un des trois autres groupes.

On a vu que tous les sous-groupes de  $Q_8$  sont normaux dans  $Q_8$ . En revanche, le sous-groupe  $\langle s \rangle$  de  $\mathcal{D}_4$  n'est pas normal dans  $\mathcal{D}_4$ , car  $rsr^{-1} = r^2s \notin \langle s \rangle$ . Donc  $Q_8$  et  $\mathcal{D}_4$  ne sont pas isomorphes.

Enfin, les groupes abéliens ne sont pas isomorphes entre eux grâce au théorème de classification 2.16. ✓

#### IV. GROUPES D'ORDRE 12

En devoir à la maison.

Nous aurons besoin du lemme suivant :

**Lemme A.11.**  $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$ .

*Démonstration.* Notons  $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  et  $E = V \setminus \{(\bar{0}, \bar{0})\} = \{a, b, c\}$ . Posons  $0 = (\bar{0}, \bar{0})$ . On a  $a + b = c$ ,  $b + c = a$  et  $a + c = b$ . Tout automorphisme  $\alpha$  de  $V$  vérifie  $\alpha(0) = 0$  donc induit une permutation de  $E$  (c'est-à-dire que  $\alpha(E) \subset E$ ). On a donc un morphisme de groupes  $\varphi: \text{Aut}(V) \hookrightarrow S_E \cong S_3$  défini par  $\varphi(\alpha) = \alpha|_E$ . Démontrons que  $\varphi$  est un isomorphisme. Il est clair qu'il est injectif.

Les transpositions engendrent  $S_3$ , donc il suffit de vérifier que les transpositions de  $S_E$  définissent des automorphismes de  $V$  (en posant  $\alpha(0) = 0$ ).

Soit  $\alpha_1 = (a\ b)$ , c'est-à-dire que  $\alpha_1(0) = 0$ ,  $\alpha_1(a) = b$ ,  $\alpha_1(b) = a$  et  $\alpha_1(c) = c$ . Il est clair que  $\alpha_1$  est une bijection. De plus,

$$\begin{aligned}\alpha_1(a+b) &= \alpha_1(c) = c = b+a = \alpha_1(a) + \alpha_1(b) \\ \alpha_1(a+c) &= \alpha_1(b) = a = b+c = \alpha_1(a) + \alpha_1(c) \\ \alpha_1(b+c) &= \alpha_1(a) = b = a+c = \alpha_1(b) + \alpha_1(c) \\ \forall x \in V, \quad \alpha_1(0+x) &= \alpha_1(x) = \alpha_1(0) + \alpha_1(x) \\ \forall x \in V, \quad \alpha_1(x+x) &= \alpha_1(0) = 0 = \alpha_1(x) + \alpha_1(x)\end{aligned}$$

donc  $\alpha_1$  est bien un morphisme de groupes et donc un automorphisme de  $V$ .

De même,  $\alpha_2 = (a\ c)$  et  $\alpha_3 = (b\ c)$  définissent des automorphismes de  $V$ . Donc  $S_3 = \langle \alpha_1, \alpha_2, \alpha_3 \rangle \subset \text{Im } \varphi$  et donc  $\varphi$  est surjectif.

Donc  $\text{Aut}(V) \cong S_E \cong S_3$ . ✓

Nous pourrions aussi utiliser le lemme suivant.

**Lemme A.12.** Il existe des produits semi-directs  $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$  qui ne sont pas directs. De plus, ces produits semi-directs sont tous isomorphes.

*Démonstration.* Il faut trouver les morphismes de groupes  $\varphi: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(V)$  non triviaux, c'est-à-dire des éléments d'ordre 3 de  $\text{Aut}(V)$  (puisque l'image d'un élément de  $\mathbb{Z}/3\mathbb{Z}$  est nécessairement d'ordre 1 ou 3). On reprend les notations de la démonstration du lemme A.11.

Puisque  $\text{Aut}(V) \cong S_E$ , il y a exactement deux éléments d'ordre 3 dans  $\text{Aut}(V)$ , qui sont  $\sigma = (a \ b \ c)$  et  $\sigma^2 = (a \ c \ b)$ .

Il y a donc deux morphismes non triviaux  $\varphi, \psi: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(V)$ , définis par  $\varphi(\bar{1}) = \sigma$  et  $\psi(\bar{1}) = \sigma^2$ .

Or  $\psi(\bar{1}) = \sigma^2 = \alpha_1 \circ \sigma \circ \alpha_1^{-1} = \alpha_1 \circ \varphi(\bar{1}) \circ \alpha_1^{-1}$  donc, puisque  $\bar{1}$  engendre  $\mathbb{Z}/3\mathbb{Z}$ , on a  $\psi(g) = \alpha_1 \circ \varphi(g) \circ \alpha_1^{-1}$  pour tout  $g \in \mathbb{Z}/3\mathbb{Z}$ . En effet, si  $g \in \mathbb{Z}/3\mathbb{Z}$  il existe  $x \in \mathbb{Z}$  tel que  $g = \bar{x}$  et on a  $\psi(g) = \psi(x \cdot \bar{1}) = \psi(\bar{1})^x = (\alpha_1 \circ \varphi(\bar{1}) \circ \alpha_1^{-1})^x = \alpha_1 \circ \varphi(\bar{1})^x \circ \alpha_1^{-1} = \alpha_1 \circ \varphi(x \cdot \bar{1}) \circ \alpha_1^{-1} = \alpha_1 \circ \varphi(g) \circ \alpha_1^{-1}$ . On en déduit que  $V \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z} \cong V \rtimes_{\psi} \mathbb{Z}/3\mathbb{Z}$  grâce aux exercices page 42. ✓

**Soit maintenant  $G$  un groupe d'ordre 12.**

**Théorème A.13.** Soit  $G$  un groupe d'ordre 12. Alors  $G$  est isomorphe à exactement un des groupes suivants :

- $C_{12}$ ;
- $C_2 \times C_6$ ;
- $C_2^2 \rtimes C_3 \cong A_4$ ;
- $C_3 \rtimes C_4 \cong \text{Dic}_3$ ;
- $C_3 \rtimes C_2^2 \cong \mathcal{D}_6$ .

En particulier, les groupes  $A_4$ ,  $\mathcal{D}_6$  et  $\text{Dic}_3$  ne sont pas isomorphes.

*Démonstration.* Si  $G$  est abélien, en utilisant la classification des groupes abéliens finis on sait qu'il est isomorphe à  $C_2 \times C_6$  ou à  $C_{12}$ .

On suppose dans la suite que  $G$  n'est pas abélien.

Soit  $n_3$  le nombre de 3-sous-groupes de Sylow de  $G$ . Alors  $n_3 \equiv 1 \pmod{3}$  et  $n_3 \mid 4$  donc  $n_3 \in \{1, 4\}$ .

- Supposons que  $n_3 = 4$ . Il y a donc quatre 3-sous-groupes de Sylow, qui sont cycliques d'ordre premier 3. En particulier, si  $S$  et  $T$  sont deux 3-sous-groupes de Sylow, on a  $S \cap T = \{1\}$ . On en déduit que dans les 3-sous-groupes de Sylow il y a  $1 + 4 \cdot 2 = 9$  éléments (l'élément neutre et deux éléments d'ordre 3 par 3-sous-groupe de Sylow).

Il reste donc 3 éléments dans  $G$ , qui sont nécessairement dans les 2-sous-groupes de Sylow. Mais dans un 2-sous-groupe de Sylow, qui est d'ordre 4, il y a 3 éléments distincts de l'élément neutre. On en déduit qu'il y a un seul 2-sous-groupe de Sylow. Soit  $H$  ce 2-sous-groupe de Sylow. On a donc  $H \triangleleft G$ .

◆ Première méthode : avec l'exercice 4 de la feuille 5. Le groupe  $G$  est d'ordre 12 et il a un sous-groupe normal d'ordre 4, donc  $G$  est isomorphe à  $A_4$ .

◆ Deuxième méthode : avec les lemmes. Soit  $S$  un 3-sous-groupe de Sylow. Alors  $H \cap S = \{1\}$  car  $\text{pgcd}(|H|, |S|) = 1$  et  $|HS| = \frac{|H||S|}{|H \cap S|} = 12 = |G|$  donc  $HS = G$ . On en déduit donc que  $G \cong H \rtimes_{\alpha} S$  pour un morphisme  $\alpha: S \rightarrow \text{Aut}(H)$ .

On remarque que  $H$  et  $K$  sont abéliens ( $S$  est d'ordre 3 donc il est cyclique et  $K$  est d'ordre  $4 = 2^2$  donc il est abélien, isomorphe à  $C_4$  ou à  $C_2 \times C_2$ ). Le morphisme  $\varphi$  ne peut donc pas être trivial car sinon le produit serait direct et comme  $S$  et  $H$  sont abéliens,  $G$  serait également abélien.

◆ Si  $H \cong C_4$ , alors  $|\text{Aut}(H)| = 2$  et il n'y a donc pas de morphisme non trivial  $\alpha: C_3 \rightarrow \text{Aut}(C_4)$  (il faudrait avoir un automorphisme d'ordre 3).

◆ Donc  $H \cong C_2 \times C_2$ . Le lemme A.12 nous permet de dire que  $G \cong H \rtimes_{\alpha} S$  avec  $\alpha: S \rightarrow \text{Aut}(H) \cong S_3$  défini par  $\alpha(\bar{1}) = (1 \ 2 \ 3)$ .

➤ Supposons maintenant que  $n_3 = 1$ . Alors l'unique 3-sous-groupe de Sylow  $S$  de  $G$  est normal dans  $G$ . Soit  $H$  un 2-sous-groupe de Sylow de  $G$ . Alors comme dans l'autre cas on a  $S \cap H = \{1\}$ ,  $G = SH$  et  $S \triangleleft G$  donc  $G \cong S \rtimes H \cong C_3 \rtimes_{\varphi} H$  pour un morphisme  $\varphi: H \rightarrow \text{Aut}(C_3)$ . Ici encore,  $\varphi$  n'est pas trivial.

On sait que  $\text{Aut}(C_3) = \{1, \theta\}$  avec  $\theta$  défini par  $\theta(x) = x^{-1}$  pour tout  $x \in C_3$ ; on a en particulier  $\theta^2 = \text{id}_{C_3}$ .

◆ Premier cas :  $H \cong \mathbb{Z}/4\mathbb{Z}$ . Puisque  $\theta^4 = \text{id}_{C_3}$ , il existe un unique morphisme non trivial  $\varphi: H \rightarrow \text{Aut}(C_3)$ , qui vérifie  $\varphi(\bar{1}) = \theta$ . Donc il y a un unique produit semi-direct  $\mathbb{Z}/4\mathbb{Z} \rtimes_{\varphi} C_3$ .

◆ Deuxième cas :  $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . On reprend les notations de la démonstration du lemme A.11. Puisque  $\varphi: H \rightarrow \text{Aut}(C_3)$  n'est pas trivial,  $\theta$  est dans  $\text{Im } \varphi$ . On a donc par exemple  $\varphi(a) = \theta$ . De plus,  $\theta = \varphi(a) = \varphi(b+c) = \varphi(b) \circ \varphi(c)$  donc on doit avoir par exemple  $\varphi(b) = \theta$  et  $\varphi(c) = \text{id}$ . Ceci définit bien un morphisme de groupes :

$$\begin{aligned}\varphi(a+b) &= \varphi(c) = \text{id} = \theta^2 = \varphi(a)\varphi(b) \\ \varphi(a+c) &= \varphi(b) = \theta = \theta \circ \text{id} = \varphi(a)\varphi(c) \\ \varphi(b+c) &= \varphi(a) = \theta = \theta \circ \text{id} = \varphi(b)\varphi(c) \\ \forall x \in H, \varphi(0+x) &= \varphi(x) = \text{id} \circ \varphi(x) = \varphi(0)\varphi(x) \\ \forall x \in H, \varphi(x+x) &= \varphi(0) = \text{id} = \varphi(x)^2.\end{aligned}$$

Soit maintenant  $\psi: H \rightarrow \text{Aut}(C_3)$  un autre morphisme de groupes qui n'est pas trivial. Alors en raisonnant comme pour  $\varphi$ , on constate qu'il existe nécessairement une permutation de  $\{a, b, c\}$ , c'est-à-dire un automorphisme  $\sigma$  de  $H$  d'après le lemme A.11, tel que  $\psi = \varphi \circ \sigma$ . On en déduit grâce aux exercices page 42 que  $H \rtimes_{\psi} C_3 \cong H \rtimes_{\varphi} C_3$ . Il y a donc un unique produit semi-direct  $H \rtimes C_3$  à isomorphisme près.

Nous avons épuisé toutes les possibilités, et nous avons obtenu que  $G$  est isomorphe à l'un des groupes suivants :

- $C_{12}$ ;
- $C_2 \times C_6$ ;
- $C_2^2 \rtimes C_3$  ou  $A_4$ ;
- $C_3 \rtimes C_4$ ;
- $C_3 \rtimes C_2^2$ .

Or nous connaissons déjà des groupes non abéliens d'ordre 12, qui sont  $A_4$ ,  $\mathcal{D}_6$  et  $\text{Dic}_3$ . Il faut donc les identifier aux produits semi-directs ci-dessus.

- Si nous avons appliqué la deuxième méthode pour obtenir  $C_2^2 \rtimes C_3$ , nous pouvons observer à ce stade que  $G$  est un groupe d'ordre 12 qui contient un sous-groupe normal  $C_2^2$  d'ordre 4, donc  $G$  est isomorphe à  $A_4$  (exercice 4 de la feuille 5). On peut aussi, si on veut éviter d'utiliser l'exercice 4 de la feuille 5, remarquer que  $A_4$  contient quatre 3-sous-groupes de Sylow, et  $C_2^2 \rtimes C_3$  est le seul produit semi-direct ci-dessus qui contienne quatre 3-sous-groupes de Sylow.
- Nous avons déjà vu que  $\text{Dic}_3$  est isomorphe à  $C_3 \rtimes C_4$  (exercice 6 de la feuille 3 et définition-proposition 4.28).
- On remarque que le sous-groupe de  $\mathcal{D}_6$  engendré par  $r^2$  est normal dans  $\mathcal{D}_6$  et d'ordre 3 donc  $\mathcal{D}_6$  contient un unique 3-Sylow; de plus, il ne contient pas d'élément d'ordre 4 donc il ne peut pas être isomorphe à  $C_3 \rtimes C_4$  et finalement  $C_3 \rtimes C_2^2 \cong \mathcal{D}_6$ . ✓

## V. GROUPES DICYCLIQUES

On reprend les notations de la définition-proposition 4.28.

**Proposition A.14.** Soit  $n$  un nombre entier impair. Alors  $\text{Dic}_n \cong C_n \rtimes_{\varphi} C_4$  via  $\varphi: C_4 = \langle b \rangle \rightarrow \text{Aut}(C_n)$  défini par  $\varphi(b): x \rightarrow x^{-1}$ .

*Démonstration.* Soient  $N = \langle a^2 \rangle$  et  $H = \langle b \rangle$ . Alors  $N$  est cyclique d'ordre  $n$  et  $H$  est cyclique d'ordre 4. De plus,

➤  $|N \cap H|$  divise  $\text{pgcd}(n, 4) = 1$  par le théorème de Lagrange donc  $N \cap H = \{1\}$ ;

➤  $NH \subset \text{Dic}_n$  et  $|NH| = \frac{|N||H|}{|N \cap H|} = 4n = |\text{Dic}_n|$  donc  $NH = \text{Dic}_n$ ;

➤  $N$  est normal dans  $\text{Dic}_n$ ; en effet, soit  $x \in N$ , alors il existe  $k \in \mathbb{Z}$  tel que  $x = a^{2k}$ , on a alors  $axa^{-1} = a^{2k} \in N$  et  $bx b^{-1} = a^{-2k} \in N$  donc, puisque  $a$  et  $b$  engendrent  $\text{Dic}_n$ , on a  $g x g^{-1} \in N$  pour tout  $g \in \text{Dic}_n$ .

Par la caractérisation du produit semi-direct de sous-groupes, il existe un morphisme  $\varphi: H \rightarrow \text{Aut}(N)$  tel que  $\text{Dic}_n \cong N \rtimes_{\varphi} H$ .

Précisons  $\varphi$ ; pour cela, il suffit de donner  $\varphi(b)$  puisque  $H$  est cyclique engendré par  $b$ . La démonstration du théorème 3.5 donne  $\varphi(b)(x) = b x b^{-1}$  pour tout  $x \in N$ . On a donc  $\varphi(b)(a^2) = b a^2 b^{-1} = a^{-2} = (a^2)^{-1}$  et, comme  $a^2$  engendre  $N$  on en déduit que  $\varphi(b)(x) = x^{-1}$  pour tout  $x \in N$ . ✓

**Proposition A.15.** Pour tout  $r \in \mathbb{N}^*$  et tout  $s \in \mathbb{N}$  impair, on a  $\text{Dic}_{2^r s} \cong C_s \rtimes \text{Dic}_{2^r}$ . En particulier,  $\text{Dic}_6 \cong C_3 \rtimes Q_8$ .

*Démonstration.* Soient  $N = \langle a^{2^{r+1}} \rangle$  et  $H = \langle a^s, b \rangle$ . Alors  $N$  est cyclique d'ordre  $s$ . De plus,  $a^s = \begin{pmatrix} e^{i\pi/2^r} & 0 \\ 0 & -e^{i\pi/2^r} \end{pmatrix}$  donc par définition de  $\text{Dic}_{2^r}$  on a  $H = \text{Dic}_{2^r}$ .

➤  $|N \cap H|$  divise  $\text{pgcd}(s, 2^{r+2}) = 1$  par le théorème de Lagrange donc  $N \cap H = \{1\}$ ;

➤  $NH \subset \text{Dic}_n$  et  $|NH| = \frac{|N||H|}{|N \cap H|} = 2^{r+2}s = |\text{Dic}_{2^r s}|$  donc  $NH = \text{Dic}_{2^r s}$ ;

➤  $N$  est normal dans  $\text{Dic}_{2^r s}$ ; en effet, soit  $x \in N$ , alors il existe  $k \in \mathbb{Z}$  tel que  $x = a^{2^{r+1}k}$ , on a alors  $axa^{-1} = x \in N$  et  $bx b^{-1} = x^{-1} \in N$  donc, puisque  $a$  et  $b$  engendrent  $\text{Dic}_{2^r s}$ , on a  $g x g^{-1} \in N$  pour tout  $g \in \text{Dic}_{2^r s}$ .

Par la caractérisation du produit semi-direct de sous-groupes, il existe un morphisme  $\varphi: H \rightarrow \text{Aut}(N)$  tel que  $\text{Dic}_{2^r s} \cong N \rtimes_{\varphi} H \cong C_s \rtimes \text{Dic}_{2^r}$ .

Précisons  $\varphi$ ; pour cela, il suffit de donner  $\varphi(a^s)$  et  $\varphi(b)$  puisque  $H$  est engendré par  $a^s$  et  $b$ . La démonstration du théorème 3.5 donne  $\varphi(a^s)(x) = a^s x a^{-s}$  et  $\varphi(b)(x) = b x b^{-1}$  pour tout  $x \in N$ . On a donc  $\varphi(a^s)(a^{2^{r+1}}) = a^{2^{r+1}}$  et  $\varphi(b)(a^{2^{r+1}}) = b a^{2^{r+1}} b^{-1} = a^{-2^{r+1}} = (a^{2^{r+1}})^{-1}$  et, comme  $a^{2^{r+1}}$  engendre  $N$  on en déduit que  $\varphi(a^s)(x) = x$  et  $\varphi(b)(x) = x^{-1}$  pour tout  $x \in N$ . ✓

**Définition-Proposition A.16.** Pour tout  $r \in \mathbb{N}$  avec  $r \geq 3$ , on note  $Q_{2^r} = \text{Dic}_{2^{r-2}}$  et on l'appelle le **groupe quaternionique généralisé**. C'est un groupe d'ordre  $2^r$ . En particulier, pour  $r = 3$  on obtient le groupe quaternionique  $Q_8$ .

Les groupes quaternioniques généralisés ne sont pas isomorphes à des produits semi-directs.

*Démonstration.* Supposons par l'absurde que l'on ait un isomorphisme  $Q_{2^r} \cong N \rtimes H$ . Puisque  $Q_{2^r}$  est un 2-groupe,  $N$  et  $H$  le sont aussi. Par le théorème de Cauchy,  $N$  et  $H$  contiennent chacun au moins un élément d'ordre 2 donc  $Q_{2^r}$  contient au moins deux éléments d'ordre 2.

Déterminons les ordres des éléments de  $Q_{2^r} = \{a^k b^{\ell} \mid k \in \llbracket 0; 2^{r-1} - 1 \rrbracket, \ell \in \llbracket 0; 1 \rrbracket\}$ .

Puisque  $a$  est d'ordre  $2^{r-1}$ , on sait que  $o(a^k) = \frac{2^{r-1}}{\text{pgcd}(2^{r-1}, k)}$  donc  $o(a^k) = 2$  si, et seulement si,  $k = 2^{r-2}$ .

D'autre part,  $(a^k b)^2 = a^k b a^k b = a^k a^{-k} b^2 = b^2 = a^{2^{r-2}}$  est d'ordre 2 donc  $a^k b$  est d'ordre 4 pour tout  $k$ .

Finalement, le seul élément d'ordre 2 de  $Q_{2^r}$  est  $a^{2^{r-2}} = -I_2$  et on a obtenu une contradiction.

Donc  $Q_{2^r}$  n'est pas isomorphe à un produit semi-direct. ✓

**Remarque.** Pour  $Q_8$  on peut utiliser un autre argument. Supposons par l'absurde que l'on ait un isomorphisme  $Q_8 \cong N \rtimes H$ . Tous les sous-groupes de  $Q_8$  sont normaux dans  $Q_8$  donc en particulier  $\{1\} \times H$  est normal dans  $N \rtimes H$ . Grâce à un exercice de TD, on en déduit que  $Q_8 = N \times H$  (produit

direct). Mais tous les sous-groupes de  $Q_8$  sont abéliens (et même cycliques), donc  $Q_8$  est abélien et on a obtenu une contradiction.

Donc  $Q_8$  n'est pas isomorphe à un produit semi-direct.

Cet argument ne se généralise pas à  $Q_{2^r}$  si  $r > 3$ . En effet, le sous-groupe  $\langle b \rangle$  n'est pas normal dans  $Q_{2^r}$  dans ce cas. Vérifions-le.

On rappelle que  $Q_{2^r} = \{a^k b^\ell \mid k \in \llbracket 0; 2^{r-1} - 1 \rrbracket, \ell \in \llbracket 0; 1 \rrbracket\}$  (tous les éléments de cette liste sont distincts). On a  $aba^{-1} = a^2 b$ , qui n'est pas égal à  $1 = a^0 b^0$ , à  $b = a^0 b^1$ , à  $b^2 = a^{2^{r-2}} b^0$  ou à  $b^3 = a^{2^{r-2}} b$ , donc  $aba^{-1} \notin \langle b \rangle$ .

Pour  $Q_8$ , on peut aussi démontrer que les suites exactes  $1 \rightarrow N \rightarrow Q_8 \rightarrow H \rightarrow 1$  ne peuvent pas être scindées. Voir travaux dirigés.

## VI. CARACTÈRES

On a vu le théorème de prolongement 2.7, qui s'applique aux groupes abéliens finis. On peut se demander si on peut supprimer ou relâcher les hypothèses sur le groupe  $G$ .

La réponse est oui, mais il y a des limites, le théorème de prolongement n'est pas vrai sans hypothèse.

**Exemple.** Soit  $\zeta = e^{2i\pi/3}$ , notons  $\sigma = (1 \ 2 \ 3) \in S_3$  et soit  $\chi: A_3 = \langle \sigma \rangle \rightarrow \mathbb{C}^*$  l'unique caractère défini par  $\chi(\sigma) = \zeta$ . Ce caractère ne se prolonge pas à  $S_3$ . En effet, supposons qu'il existe  $\hat{\chi}: S_3 \rightarrow \mathbb{C}^*$  tel que  $\hat{\chi}|_{A_3} = \chi$ . Soit  $\tau \in S_3$  une transposition. Alors l'ordre de  $\hat{\chi}(\tau)$  divise 2 (l'ordre de  $\tau$ ) donc  $\hat{\chi}(\tau) \in \{\pm 1\}$ . Mais alors

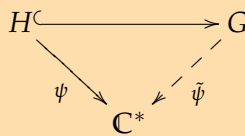
$$\zeta = \chi(\sigma) = \hat{\chi}(\sigma) = \hat{\chi}((1 \ 2)(2 \ 3)) = \hat{\chi}((1 \ 2))\hat{\chi}((2 \ 3)) = 1$$

et on a obtenu une contradiction.

### a) Groupes abéliens quelconques

Une hypothèse que l'on peut enlever est celle que les groupes sont finis : le théorème de prolongement est vrai pour tous les groupes abéliens.

**Théorème A.17.** Soit  $G$  un groupe abélien et soit  $H \subset G$  un sous-groupe. Il existe, pour tout  $\psi \in \hat{H}$ , un élément  $\tilde{\psi} \in \hat{G}$  tel que  $\tilde{\psi}|_H = \psi$ .



**Démonstration.** ➤ Commençons par démontrer que pour tout  $n \in \mathbb{Z}$ , tout caractère sur  $n\mathbb{Z}$  se prolonge en un caractère sur  $\mathbb{Z}$ .

Soit  $n \in \mathbb{Z}$  et soit  $\chi: n\mathbb{Z} \rightarrow \mathbb{C}^*$  un caractère. Si  $n = 0$  alors le caractère trivial sur  $\mathbb{Z}$  prolonge  $\chi$ . Supposons donc que  $n \in \mathbb{Z}^*$ . On cherche un morphisme  $\hat{\chi}: \mathbb{Z} \rightarrow \mathbb{C}^*$ , qui sera entièrement déterminé par  $\hat{\chi}(1)$  puisque  $\mathbb{Z}$  est monogène. On doit avoir  $\chi(n) = \hat{\chi}(n) = n\hat{\chi}(1)$  donc  $\hat{\chi}(1) = \frac{1}{n}\chi(n)$ .

Soit donc  $\hat{\chi}$  le caractère sur  $\mathbb{Z}$  déterminé par  $\hat{\chi}(1) = \frac{1}{n}\chi(n)$ , il prolonge bien  $\chi$ .

➤ Démontrons maintenant le cas général. Soit  $G$  un groupe abélien, soit  $H$  un sous-groupe de  $G$  et soit  $\chi: H \rightarrow \mathbb{C}^*$  un caractère sur  $H$ . Nous allons utiliser le lemme de Zorn (voir la section III du chapitre 7).

Considérons l'ensemble  $\mathcal{S}$  formé des couples  $(\chi', H')$  où  $H'$  est un sous-groupe de  $G$  contenant  $H$  et  $\chi' \in \hat{H}'$  prolonge  $\chi$ . Il est clair que  $\mathcal{S}$  n'est pas vide (il contient  $(\chi, H)$ ) et qu'il est partiellement ordonné par la relation

$$(\chi', H') \leq (\chi'', H'') \iff H' \subset H'' \text{ et } \chi'|_{H'} = \chi'.$$

De plus, l'ensemble ordonné  $(\mathcal{S}, \leq)$  est inductif. En effet, si  $(\chi'_i, H'_i)_{i \in I}$  est une partie totalement ordonnée de  $\mathcal{S}$ , elle admet un élément maximal  $(\tilde{\chi}, \tilde{H} = \cup_{i \in I} H'_i)$  où  $\tilde{\chi}$  est défini de la façon suivante; soit  $x \in \tilde{H}$ , il existe  $i$  tel que  $x \in H'_i$ , on pose  $\tilde{\chi}(x) = \chi'_i(x)$ ; de plus, si  $j \in I$  est tel que  $x \in H'_j$ , on a par exemple  $(\chi'_i, H'_i) \leq (\chi'_j, H'_j)$  donc  $\chi'_{j|H'_i} = \chi'_i$  et donc  $\chi'_j(x) = \chi'_i(x)$  et finalement  $\tilde{\chi}$  est bien défini. Il reste à vérifier que  $\tilde{H}$  est un sous-groupe de  $G$ , que  $\tilde{\chi}$  est un morphisme de groupes et que  $(\tilde{\chi}, \tilde{H})$  est bien un majorant de  $(\chi'_i, H'_i)_{i \in I}$  dans  $\mathcal{S}$  (exercice).

D'après le lemme de Zorn, l'ensemble  $\mathcal{S}$  admet donc un élément maximal,  $(\chi_0, H_0)$ . Il suffit pour conclure de démontrer que  $H_0 = H$  et de poser  $\hat{\chi} = \chi_0$ .

Supposons par l'absurde que  $H_0 \subsetneq H$  et soit donc  $x \in H \setminus H_0$ . L'ensemble  $I := \{a \in \mathbb{Z} \mid ax \in H_0\}$  est un idéal de  $\mathbb{Z}$ , il existe donc  $n \in \mathbb{Z}$  tel que  $I = n\mathbb{Z}$ . On considère le morphisme de groupes  $f: I = n\mathbb{Z} \rightarrow \mathbb{C}^*$  défini par  $f(a) = \chi_0(ax)$ . D'après la première partie de la démonstration, on peut prolonger  $f$  en un morphisme  $\hat{f}: \mathbb{Z} \rightarrow \mathbb{C}^*$ . Posons  $X = H_0 + \mathbb{Z}x$  (le sous-groupe de  $G$  engendré par  $H_0 \cup \{x\}$ ) et soit  $F: X \rightarrow \mathbb{C}^*$  le morphisme de groupes défini par  $F(y + ax) = \chi_0(y) + \hat{f}(a)$  où  $(y, a) \in H_0 \times \mathbb{Z}$ . Vérifions qu'il est bien défini. Si  $y + ax = y_1 + a_1x$  avec  $(y_1, a_1) \in H_0 \times \mathbb{Z}$ , alors  $(a - a_1)x = y_1 - y \in H_0$  donc  $a - a_1 \in I = n\mathbb{Z}$  et  $\hat{f}(a) - \hat{f}(a_1) = \hat{f}(a - a_1) = f(a - a_1) = \chi_0((a - a_1)x) = \chi_0(y_1 - y) = \chi_0(y_1) - \chi_0(y)$  donc  $\chi_0(y) + \hat{f}(a) = \chi_0(y_1) + \hat{f}(a_1)$ . On vérifie facilement que  $F$  est un morphisme de groupes. De plus,  $F|_{H_0} = \chi_0$  donc  $(F, X) \in \mathcal{S}$  et  $(\chi_0, H_0) < (F, X)$ , ce qui contredit la maximalité de  $(\chi_0, H_0)$ .

Finalement  $H_0 = H$  et  $\hat{\chi} = \chi_0$  convient. ✓

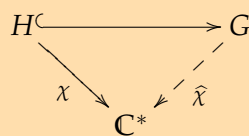
## b) Prolongement de certains caractères dans le cas de groupes quelconques

Enfin, on peut étendre cela à certains caractères sur des groupes qui ne sont pas abéliens.

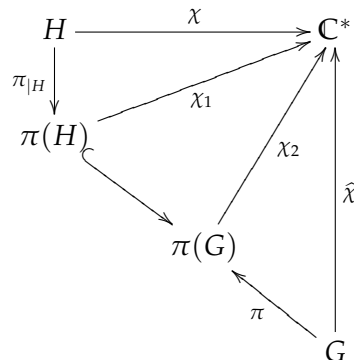
**Remarque.** Soit  $G$  un groupe, soit  $H$  un sous-groupe de  $G$  et soit  $\chi: H \rightarrow \mathbb{C}^*$  un caractère sur  $H$ . Supposons qu'il existe un prolongement  $\hat{\chi}: G \rightarrow \mathbb{C}^*$  de  $\chi$  à  $G$ . Alors  $D(G) \subset \text{Ker } \hat{\chi}$  car  $\mathbb{C}^*$  est abélien, donc  $H \cap D(G) \subset \text{Ker } \chi$ , autrement dit,  $\chi|_{H \cap D(G)}$  est le caractère trivial sur  $H \cap D(G)$ .

Cette remarque impose l'hypothèse que nous mettons sur le caractère sur  $H$  dans le résultat suivant.

**Théorème A.18.** Soit  $G$  un groupe, soit  $H$  un sous-groupe de  $G$  et soit  $\chi: H \rightarrow \mathbb{C}^*$  un caractère sur  $H$  tel que  $\chi|_{H \cap D(G)}$  est le caractère trivial sur  $H \cap D(G)$ . Alors il existe un prolongement  $\hat{\chi}$  de  $\chi$  à  $G$  :



**Démonstration.** Notons  $\pi: G \rightarrow G/D(G)$  la surjection canonique. Le schéma suivant illustre la démonstration :



On a  $\text{Ker}(\pi|_H) = H \cap D(G) \subset \text{Ker } \chi$  donc par factorisation on obtient un morphisme  $\chi_1: \pi(H) \rightarrow \mathbb{C}^*$  tel que  $\chi_1 \circ \pi|_H = \chi$ .

Ensuite,  $\pi(H)$  est un sous-groupe du groupe abélien  $\pi(G) = G/D(G)$  et  $\chi_1$  est un caractère sur  $\pi(H)$  donc d'après le théorème de prolongement A.17, il existe un caractère  $\chi_2: \pi(G) \rightarrow \mathbb{C}^*$  tel que  $\chi_2|_{\pi(H)} = \chi_1$ .  
Enfin, posons  $\hat{\chi} = \chi_2 \circ \pi: G \rightarrow \mathbb{C}^*$ , c'est bien un caractère sur  $G$  qui prolonge  $\chi$ . ✓

**Deuxième partie :**

**Anneaux**



# Rappels et compléments sur les anneaux

## I. RAPPELS DE BASE

On rappelle un certain nombre de définitions et propriétés de base sur les anneaux. Pour plus de détails, on renvoie au cours de L3.

**Définition 7.1.** Un **anneau** est un groupe abélien  $(A, +)$  muni d'une deuxième loi interne, la **multiplication** ou le **produit**  $\cdot : A \times A \rightarrow A$ , tel que :

- le produit est associatif :  $\forall (a, b, c) \in A^3, (ab)c = a(bc)$ ;
- le produit est distributif par rapport à l'addition :  $\forall (a, b, c) \in A^3, a(b + c) = ab + ac$  et  $(a + b)c = ac + bc$ .

Si de plus le produit possède un élément neutre 1, on dit que l'anneau  $A$  est **unitaire** et 1 est appelé **élément unité** de  $A$ . Il vérifie  $1a = a = a1$  pour tout  $a \in A$ .

Enfin, si le produit est commutatif, c'est-à-dire que  $ab = ba$  pour tout  $(a, b) \in A^2$ , on dit que l'anneau  $A$  est commutatif.

Pour mémoire, un groupe abélien est un ensemble non vide  $A$  muni d'une loi interne  $+: A \times A \rightarrow A$  qui est associative ( $\forall (a, b, c) \in A^3, (a + b) + c = a + (b + c)$ ), possède un élément neutre noté 0 ( $\forall a \in A, a + 0 = a = 0 + a$ ), est telle que tout élément  $a \in A$  possède un inverse  $-a$  appelé opposé ( $\forall a \in A, \exists b \in A$  tq.  $a + b = 0 = b + a$ ;  $b = -a$ ) et qui est commutative ( $\forall (a, b) \in A^2, a + b = b + a$ ).

**Dans tout ce cours, anneau signifie anneau commutatif unitaire, sauf mention expresse du contraire.**

**Définition 7.2.** Un **corps** est un anneau (commutatif unitaire) tel que tout élément non nul possède un inverse :  $\forall a \in A \setminus \{0\}, \exists b \in A$  tel que  $ab = 1$ .

**Définition 7.3.** Un **sous-anneau**  $B$  d'un anneau  $A$  est une partie non vide  $B$  de  $A$  qui, munie des opérations de  $A$ , est un anneau. Cela sous-entend en particulier que l'élément unité de  $A$  est dans  $B$ .

On peut vérifier que  $B$  est un sous-anneau de  $A$  si, et seulement si,

- $(B \neq \emptyset)$ ;
- $\forall (a, b) \in B^2$ , on a  $a - b \in B$  (ou  $a + b \in B$  et  $-a \in B$ ) – d'où  $B$  est un sous-groupe (abélien) de  $(A, +)$ ;
- $1 \in B$ ;
- $\forall (a, b) \in B^2$ , on a  $ab \in B$ .

**Remarque.** On doit vérifier que  $1 \in B$ , cela n'est pas automatique.

**Définition 7.4.** Un **morphisme d'anneaux** d'un anneau  $A$  vers un anneau  $B$  est une application  $f: A \rightarrow B$  vérifiant, pour tout  $(a, b) \in A^2$ ,

- $f(a + b) = f(a) + f(b)$ ,
- $f(ab) = f(a)f(b)$  et
- $f(1) = 1$ .

On peut vérifier que si un morphisme d'anneaux  $f$  est bijectif, alors l'application réciproque  $f^{-1}$  est aussi un morphisme d'anneaux. On dit alors que  $f$  est un **isomorphisme** d'anneaux.

**Définition 7.5.** Soit  $A$  un anneau.

- Un élément  $a \in A$  est dit **inversible** s'il possède un inverse, noté  $a^{-1}$ , pour le produit. On note  $A^\times$  l'ensemble des éléments inversibles de  $A$ .
- Un élément  $a \in A$  est un **diviseur de zéro** si  $a \neq 0$  s'il existe  $b \in A$  avec  $b \neq 0$  tel que  $ab = 0$ .
- Un anneau  $A$  est dit **intègre** si  $A \neq \{0\}$  et s'il ne contient pas de diviseur de zéro.

Un anneau intègre n'est pas nul.

Un corps est en particulier un anneau intègre.

**Définition 7.6.** Soit  $A$  un anneau. Un **idéal** de  $A$  est un sous-groupe abélien  $I$  de  $A$  qui vérifie

$$\forall a \in A, \forall x \in I, \text{ on a } ax \in I.$$

Une partie  $I$  de  $A$  est un idéal de  $A$  si, et seulement si,

- $I \neq \emptyset$ ;
- $\forall (x, y) \in I^2, x + y \in I$  et
- $\forall (a, x) \in A \times I, ax \in I$ .

**Propriétés 7.7.** ➤ Un idéal  $I$  de  $A$  est égal à  $A$  si, et seulement si,  $1 \in I$ .

➤ Un idéal  $I$  de  $A$  est égal à  $A$  si, et seulement si, il contient un élément inversible de  $A$ .

➤ Une intersection d'idéaux est un idéal.

➤ Soit  $f: A \rightarrow B$  un morphisme d'anneaux.

- ◆ Si  $C$  est un sous-anneau de  $A$ , alors  $f(C)$  est un sous-anneau de  $B$ . En particulier,  $\text{Im } f = f(A)$  est un sous-anneau de  $B$ .
- ◆ Si  $D$  est un sous-anneau de  $B$ , alors  $f^{-1}(D)$  est un sous-anneau de  $A$ .
- ◆ Si  $I$  est un idéal de  $B$ , alors  $f^{-1}(I)$  est un idéal de  $A$ . En particulier,  $\text{Ker } f = f^{-1}(\{0\})$  est un idéal de  $A$ .
- ◆ Si  $f$  est surjectif et si  $J$  est un idéal de  $A$ , alors  $f(J)$  est un idéal de  $B$ .

**Définition-Proposition 7.8.** Soit  $A$  un anneau et soit  $X$  une partie de  $A$ . L'**idéal de  $A$  engendré par  $X$**  est le plus petit idéal de  $A$  contenant  $X$ . Celui-ci existe et il est égal à l'intersection de tous les idéaux de  $A$  contenant  $X$ . On le note  $(X)$  ou  $(x_1, \dots, x_n)$  si  $X = \{x_1, \dots, x_n\}$ .

**Théorème 7.9.** Soit  $A$  un anneau et soit  $I$  un idéal de  $A$ . On définit une relation d'équivalence  $\sim$  sur  $A$  en posant

$$a \sim b \iff a - b \in I.$$

L'ensemble quotient  $A/\sim$  est alors un anneau pour les lois

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a+b}; \\ \bar{a}\bar{b} &= \overline{ab}\end{aligned}$$

où  $\bar{a}$  désigne la classe d'équivalence de  $a$  dans  $A/\sim$  (celle-ci est parfois notée  $a + I$ ). Cet anneau est appelé **anneau quotient** de  $A$  par  $I$  et noté  $A/I$ .

L'application  $\pi: A \rightarrow A/I$  définie par  $\pi(a) = \bar{a}$  est un morphisme d'anneaux surjectif, appelé **projection canonique**.

**Théorème 7.10** (Théorème de passage au quotient). Soit  $f: A \rightarrow B$  un morphisme d'anneaux. Soit  $I$  un idéal de  $A$  et soit  $J$  un idéal de  $B$  tel que  $f(I) \subset J$ . On note  $\pi_A: A \rightarrow A/I$  et  $\pi_B: B \rightarrow B/J$  les projections canoniques.

Alors il existe un unique morphisme d'anneaux  $\bar{f}: A/I \rightarrow B/J$  tel que  $\bar{f} \circ \pi_A = \pi_B \circ f$  (on a donc  $\bar{f}(\bar{a}) = \overline{f(a)}$ ).

Schématiquement, on a

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi_A \downarrow & & \downarrow \pi_B \\ A/I & \xrightarrow{\bar{f}} & B/J. \end{array}$$

Réciproquement, si un tel  $\bar{f}$  existe, alors  $f(I) \subset J$ .

*Démonstration.* ➤ Supposons que  $\bar{f}$  existe. Soit  $b \in f(I)$ . Alors il existe  $a \in I$  tel que  $b = f(a)$ . On a alors  $\pi_B(b) = \pi_B(f(a)) = \bar{f}(\pi_A(a)) = \bar{f}(0) = 0$  donc  $b \in \text{Ker } \pi_B = J$ . Donc  $f(I) \subset J$ .

➤ Réciproquement, supposons que  $f(I) \subset J$ . On doit avoir  $\bar{f}(\pi_A(a)) = \pi_B(f(a))$  pour tout  $a \in A$ . Soit  $x \in A/I$ . Il existe  $a \in A$  tel que  $\pi_A(a) = x$ . Posons donc  $\bar{f}(x) = \pi_B(f(a))$ .

Il faut vérifier que  $\bar{f}$  est bien définie, c'est-à-dire que si on choisit un autre représentant  $a'$  de  $x$  dans  $A$ , on a bien  $\pi_B(f(a')) = \pi_B(f(a))$ . Puisque  $a$  et  $a'$  sont deux représentants de  $x$  dans  $A$ , on a  $a' - a \in \text{Ker } \pi_A = I$ , donc  $f(a' - a) \in J$  et donc  $\pi_B(f(a' - a)) = 0$ . Or  $\pi_B$  et  $f$  sont des morphismes d'anneaux donc  $\pi_B(f(a')) - \pi_B(f(a)) = 0$ . On a donc bien défini une application  $\bar{f}$ .

De plus,  $\bar{f}$  est un morphisme d'anneaux. Soit  $(x, y) \in (A/I)^2$  et soit  $(a, b) \in A^2$  tel que  $x = \pi_A(a)$  et  $y = \pi_A(b)$ . Alors

- ♦  $\bar{f}(x + y) = \bar{f}(\pi_A(a + b)) = \pi_B(f(a + b)) = \pi_B(f(a)) + \pi_B(f(b)) = \bar{f}(x) + \bar{f}(y);$
- ♦  $\bar{f}(xy) = \bar{f}(\pi_A(ab)) = \pi_B(f(ab)) = \pi_B(f(a))\pi_B(f(b)) = \bar{f}(x)\bar{f}(y);$
- ♦  $\bar{f}(1) = \bar{f}(\pi_A(1)) = \pi_B(f(1)) = 1.$

Enfin, la condition  $\bar{f} \circ \pi_A = \pi_B \circ f$  nous a imposé la définition de  $\bar{f}$ , donc un tel morphisme d'anneaux est unique. ✓

**Remarque.** Dans le cas particulier où  $J = \{0\}$ , la condition «  $f(I) \subset J$  » devient «  $I \subset \text{Ker } f$  ». Ainsi, si  $f: A \rightarrow B$  est un morphisme d'anneaux et si  $I$  est un idéal de  $A$  tel que  $I \subset \text{Ker } f$ , alors  $f$  induit un unique morphisme d'anneaux  $\bar{f}: A/I \rightarrow B$  tel que  $f = \bar{f} \circ \pi_A$  (c'est-à-dire que  $\bar{f}(\bar{a}) = f(a)$ ).

**Théorème 7.11** (Premier théorème d'isomorphisme). Soit  $f: A \rightarrow B$  un morphisme d'anneaux. Le morphisme  $f$  induit un isomorphisme d'anneaux

$$\bar{f}: A / \text{Ker } f \rightarrow \text{Im } f.$$

**Théorème 7.12** (Deuxième théorème d'isomorphisme). Soit  $A$  un anneau, soit  $B$  un sous-anneau de  $A$  et soit  $I$  un idéal de  $A$ . Alors l'ensemble  $B + I = \{b + x; (b, x) \in B \times I\}$  est un sous-anneau de  $A$ , l'idéal  $I$  est un idéal de  $B + I$ , l'ensemble  $B \cap I$  est un idéal de  $B$  et on a un isomorphisme d'anneaux

$$(B + I) / I \cong B / (B \cap I).$$

**Théorème 7.13** (Troisième théorème d'isomorphisme). Soit  $A$  un anneau. Soit  $I$  un idéal de  $A$ . Notons  $\pi: A \rightarrow A/I$  la projection canonique. Soit  $J$  un idéal de  $A$  contenant  $I$  ( $I \subset J$ ). Alors on a un isomorphisme d'anneaux

$$(A/I) / \pi(J) \cong A/J$$

ce que l'on peut également écrire  $(A/I) / (J/I) \cong A/J$ .

**Définition-Proposition 7.14.** Soit  $A$  un anneau. Soient  $I$  et  $J$  deux idéaux de  $A$ . On note  $IJ$  l'idéal engendré par les produits  $xy$  avec  $(x, y) \in I \times J$  et  $I + J$  l'idéal engendré par  $I \cup J$ . On a donc

$$IJ = \left\{ \sum_{k=1}^n x_k y_k \mid n \in \mathbb{N}, (x_k, y_k) \in I \times J \right\}$$

$$I + J = \left\{ \sum_{k=1}^n a_k x_k \mid n \in \mathbb{N}, x_k \in I \cup J, a_k \in A \right\} = \{x + y \mid (x, y) \in I \times J\}.$$

*Démonstration.* Notons  $Z = \{xy \mid (x, y) \in I \times J\}$  et  $K = \{\sum_{k=1}^n x_k y_k \mid n \in \mathbb{N}, (x_k, y_k) \in I \times J\}$ . On vérifie facilement que  $K$  est un idéal de  $A$ , qui contient  $Z$ . Donc  $IJ \subset K$ . Soit  $K'$  un idéal de  $A$  qui contient  $Z$ . Alors, puisque  $K'$  est stable par somme, il contient tous les éléments de  $K$ , donc  $K \subset K'$ . Ainsi,  $K$  est le plus petit idéal de  $A$  qui contient  $Z$ , c'est-à-dire que  $K = (Z) = IJ$ .

Notons  $L = \{x + y \mid (x, y) \in I \times J\}$ . On sait déjà que c'est un sous-groupe de  $(A, +)$  (proposition 1.33). Soit  $(a, x, y) \in A \times I \times J$ . Alors  $a(x + y) = ax + ay \in L$ . Donc  $L$  est un idéal de  $A$ , qui contient  $I \cup J$ . Donc  $I + J \subset L$ . Soit  $L'$  un idéal de  $A$  contenant  $I \cup J$ . Alors  $L'$  contient  $I$  et  $J$  donc, puisqu'il est stable par somme, il contient  $L$ . Ainsi,  $L$  est le plus petit idéal de  $A$  qui contient  $I \cup J$  et finalement  $L = (I \cup J) = I + J$ . ✓

**Théorème 7.15** (Théorème Chinois). Soit  $A$  un anneau. Soient  $I$  et  $J$  deux idéaux de  $A$  tels que  $I + J = A$ . Alors

- (a)  $IJ = I \cap J$ ;
- (b) les anneaux  $A/IJ$  et  $A/I \times A/J$  sont isomorphes.

*Démonstration.* (a) Il est clair que  $IJ \subset I \cap J$  (sans hypothèse sur les idéaux  $I$  et  $J$ ).

Réciproquement, soit  $x \in I \cap J$ . Puisque  $I + J = A$  il existe  $a \in I$  et  $b \in J$  tels que  $1 = a + b$ . On a alors  $x = ax + bx$  et  $ax \in IJ$  puisque  $(a, x) \in I \times J$  et  $bx \in IJ$  puisque  $(b, x) \in J \times I$ . Donc  $x \in IJ$ .

On a bien  $I \cap J = IJ$ .

(b) Notons  $\pi_I: A \rightarrow I$  et  $\pi_J: A \rightarrow A/J$  les projections canoniques (morphisms d'anneaux) et considérons  $\varphi: A \rightarrow A/I \times A/J$  définie par  $\varphi(x) = (\pi_I(x), \pi_J(x))$  pour tout  $x \in A$ . C'est un morphisme d'anneaux.

Il est clair que  $\text{Ker } \varphi = I \cap J = IJ$ .

Démontrons que  $\varphi$  est surjective. Soit  $(u, v) \in A/I \times A/J$ , il existe  $(y, z) \in A^2$  tel que  $(u, v) = (\pi_I(y), \pi_J(z))$ . On cherche  $x \in A$  tel que  $\varphi(x) = (u, v)$ , c'est-à-dire tel que  $\pi_I(x) = \pi_I(y)$  et  $\pi_J(x) = \pi_J(z)$ .

Comme dans la première partie, il existe  $a \in I$  et  $b \in J$  tels que  $1 = a + b$ . Posons  $x = yb + za$ . Alors  $\pi_I(x) = \pi_I(yb) = \pi_I(y(1 - a)) = \pi_I(y - ya) = \pi_I(y) = u$  et  $\pi_J(x) = \pi_J(za) = \pi_J(z - zb) = \pi_J(z) = v$  donc  $\varphi(x) = (u, v)$ .

Finalement, d'après le premier théorème d'isomorphisme,  $\varphi$  induit un isomorphisme  $\bar{\varphi}: A/IJ \rightarrow A/I \times A/J$  (donné par  $\bar{\varphi}(\bar{x}) = (\pi_I(x), \pi_J(x))$ ). ✓

**Conséquence 7.16.** Soit  $A$  un anneau principal. Soient  $m$  et  $n$  deux éléments de  $A$  premiers entre eux. Alors les anneaux  $A/(m) \times A/(n)$  et  $A/(mn)$  sont isomorphes.

**Remarque.** L'isomorphisme est donné par  $\bar{\varphi}(\bar{x}) = (\pi_m(x), \pi_n(x))$  où  $\pi_m: A \rightarrow A/(m)$  et  $\pi_n: A \rightarrow A/(n)$  sont les projections canoniques. Pour exprimer  $\bar{\varphi}^{-1}$ , on applique la propriété de Bézout, qui donne  $(u, v) \in A^2$  tel que  $mu + nv = 1$ . Alors  $\bar{\varphi}^{-1}(\pi_m(y), \pi_n(z)) = \overline{zmu + ynv}$ .

Ceci permet, dans le cas où  $A = \mathbb{Z}$ , de résoudre des systèmes de congruences du type

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

avec  $m$  et  $n$  deux entiers premiers entre eux.

## II. IDÉAUX PREMIERS ET MAXIMAUX.

**Définition 7.17.** Soient  $A$  un anneau et  $I$  un idéal de  $A$ .

- (1) L'idéal  $I$  est dit **premier** s'il est distinct de  $A$  et vérifie la condition suivante : pour tous  $a, b \in A$ ,  $ab \in I \implies a \in I$  ou  $b \in I$ .
- (2) L'idéal  $I$  est dit **maximal** s'il est distinct de  $A$  et vérifie la condition suivante : pour tout idéal  $J$  de  $A$ ,  $I \subset J \subset A \implies J = I$  ou  $J = A$ .

On peut caractériser la primalité ou la maximalité de l'idéal  $I$  d'un anneau  $A$  à l'aide de l'anneau quotient  $A/I$ .

**Proposition 7.18.** Soient  $A$  un anneau et  $I$  un idéal de  $A$ .

- (1) L'idéal  $I$  est premier si et seulement si l'anneau  $A/I$  est intègre.
- (2) L'idéal  $I$  est maximal si et seulement si l'anneau  $A/I$  est un corps.

*Démonstration.* Exercice (L3). ✓

**Remarque.** ➤ Il est clair d'après la proposition 7.18 que tout idéal maximal est premier.

➤ Par contre, il est facile de démontrer que  $\{0\}$  est un idéal premier et non maximal de l'anneau  $\mathbb{Z}$ . (En effet,  $\mathbb{Z}/\{0\} \cong \mathbb{Z}$  est intègre mais n'est pas un corps).

**Proposition 7.19.** Soient  $A$  un anneau,  $I$  un idéal de  $A$  et  $\pi: A \longrightarrow A/I$  la projection canonique. On note  $\mathbf{I}_{A/I}$  l'ensemble de tous les idéaux de  $A/I$  et  $\mathbf{J}_{A,I}$  l'ensemble de tous les idéaux de  $A$  contenant  $I$ . Alors :

(1) les applications

$$\begin{array}{ccc} \mathbf{J}_{A,I} & \xrightarrow{\alpha} & \mathbf{I}_{A/I} \\ K & \mapsto & \pi(K) \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbf{I}_{A/I} & \xrightarrow{\beta} & \mathbf{J}_{A,I} \\ L & \mapsto & \pi^{-1}(L) \end{array}$$

sont des bijections réciproques l'une de l'autre. Elles établissent donc une correspondance bijective entre idéaux de  $A/I$  et idéaux de  $A$  contenant  $I$ .

(2) la correspondance bijective ci-dessus induit des correspondances bijectives entre les idéaux premiers (resp. maximaux) de  $A/I$  et les idéaux premiers (resp. maximaux) de  $A$  contenant  $I$ .

*Démonstration.* (1) Puisque  $\pi$  est un morphisme d'anneaux,  $\pi^{-1}(L)$  est un idéal de  $A$  pour tout idéal  $L$  de  $A/I$ . De plus,  $0$  est dans  $L$  donc  $I = \pi^{-1}(\{0\}) \subset \pi^{-1}(L)$ .

Puisque  $\pi$  est un morphisme d'anneaux surjectif,  $\pi(K)$  est un idéal de  $A/I$  pour tout idéal  $K$  de  $A$ .

On a  $\alpha \circ \beta = \text{id}_{\mathbf{I}_{A/I}}$  car  $\pi \circ \pi^{-1}(L) = L$  pour tout idéal  $L$  de  $A/I$ .

Il reste à vérifier que  $\beta \circ \alpha = \text{id}_{\mathbf{J}_{A,I}}$  pour tout idéal  $K$  de  $A$  contenant  $I$ . Soit  $K$  un tel idéal.

On a toujours  $\pi^{-1}(\pi(K)) \supset K$ . Soit maintenant  $x \in \pi^{-1}(\pi(K))$ . Alors  $\pi(x) \in \pi(K)$  donc il existe  $a \in K$  tel que  $\pi(x) = \pi(a)$ . Mais alors  $x - a \in I \subset K$  donc  $x \in K$ . On a donc bien  $\pi^{-1}(\pi(K)) = K$ .

Ainsi,  $\alpha$  et  $\beta$  sont des bijections réciproques.

(2) Le troisième théorème d'isomorphisme précise que pour tout idéal  $K$  de  $A$  contenant  $I$ , on a un isomorphisme d'anneaux

$$A/K \cong (A/I)/\pi(K).$$

Ainsi, d'après la proposition 7.18, pour tout idéal  $K$  de  $A$  contenant  $I$ ,  $K$  est premier (resp. maximal) dans  $A$  si et seulement si  $\pi(K)$  est premier (resp. maximal) dans  $A/I$ . ✓

Il est clair par définition que l'anneau nul ne contient pas d'idéaux premiers (et donc pas d'idéaux maximaux). La première question légitime est alors la suivante : étant donné un anneau non nul  $A$ , existe-t-il toujours des idéaux premiers, des idéaux maximaux, dans  $A$  ? La réponse est donnée par le *théorème de Krull*.

### III. ENSEMBLES ORDONNÉS ET LEMME DE ZORN

Ce lemme est utilisé pour faire certaines démonstrations où une récurrence est impossible (si l'ensemble d'indices n'est pas dénombrable). Il est équivalent à l'axiome du choix (indépendant des autres axiomes, Cohen 1963). Vous le verrez également dans le cours de topologie.

**Axiome du choix.** Le produit d'une famille non vide d'ensembles non vides n'est pas vide.

Autrement dit, si  $(A_i)_{i \in I}$  est une famille non vide d'ensembles non vides, on peut choisir simultanément  $x_i \in A_i$  pour tout  $i \in I$ .

Nous nous contenterons d'énoncer le lemme de Zorn, et admettrons qu'il est équivalent à l'axiome du choix.

## A. Lemme de Zorn

**Définition 7.20.** Soit  $E$  un ensemble. Un **ordre** sur  $E$  est une relation binaire  $\preceq$ , réflexive, anti-symétrique et transitive, c'est-à-dire telle que :

- $\forall x \in E, x \preceq x$ ;
- $\forall (x, y) \in E^2$ , si  $x \preceq y$  et  $y \preceq x$ , alors  $x = y$ ;
- $\forall (x, y, z) \in E^3$ , si  $x \preceq y$  et  $y \preceq z$  alors  $x \preceq z$ .

On dit alors que l'ensemble  $(E, \preceq)$  est un **ensemble ordonné**.

**Remarque.** Il est clair que, si  $F$  est un sous-ensemble de l'ensemble  $E$  et si  $\preceq$  est un ordre sur  $E$ , alors  $\preceq$  induit un ordre sur  $F$ .

**Exemples.**  $(\mathbb{R}, \leq)$ ,  $(\mathbb{Q}, \leq)$ ,  $(\mathbb{N}^*, |)$  et  $(\mathcal{P}(\mathbb{C}), \subset)$  sont des ensembles ordonnés.

**Définition 7.21.** Si  $(E, \preceq)$  est un ensemble ordonné et si, pour tous  $(x, y) \in E^2$ , on a  $x \preceq y$  ou  $y \preceq x$ , on dit que  $\preceq$  est un **ordre total** ou que  $(E, \preceq)$  est un **ensemble totalement ordonné**. Dans le cas contraire, on dit que  $\preceq$  est un **ordre partiel** ou que  $(E, \preceq)$  est un **ensemble partiellement ordonné**.

**Exemples.** Dans les exemples précédents,  $(\mathbb{R}, \leq)$  et  $(\mathbb{Q}, \leq)$  sont totalement ordonnés alors que  $(\mathbb{N}^*, |)$  et  $(\mathcal{P}(\mathbb{C}), \subset)$  sont partiellement ordonnés.

**Définition 7.22.** Soit  $(E, \preceq)$  un ensemble ordonné.

- Un **élément maximal** de  $(E, \preceq)$  est un élément  $x \in E$  tel que, pour tout  $y \in E$ , si  $x \preceq y$ , alors  $x = y$ .
- Soit  $F$  un sous-ensemble de  $E$ . Un **majorant** de  $F$  dans  $E$  est un élément  $m$  de  $E$  tel que pour tout  $x \in F$ ,  $x \preceq m$ .
- On dit que  $(E, \preceq)$  est un **ensemble inductif** si tout sous-ensemble non-vide  $F$  de  $E$  tel que  $(F, \preceq)$  soit totalement ordonné admet un majorant dans  $E$ .

**Remarque.** Soient  $A$  un anneau et  $\mathcal{E}$  l'ensemble de tous les idéaux de  $A$  distincts de  $A$ . L'inclusion définit une relation d'ordre (partiel) sur  $\mathcal{E}$  et on note  $(\mathcal{E}, \subset)$  l'ensemble ordonné ainsi obtenu. Alors,  $I$  est un idéal maximal de  $A$  si et seulement si  $I$  est un élément maximal de  $(\mathcal{E}, \subset)$ .

**Théorème 7.23** (Lemme de Zorn). Soit  $(E, \preceq)$  un ensemble ordonné, inductif et non vide. Alors il existe un élément maximal dans  $E$ .

*Démonstration.* (admis)

✓

## B. Applications

**Théorème 7.24** (Théorème de la base incomplète). Soit  $\mathbb{K}$  un corps. Toute famille libre d'un espace vectoriel non nul  $E$  sur  $\mathbb{K}$  est contenu dans une base de  $E$ .

*Démonstration.* Soit  $E$  un espace vectoriel sur  $\mathbb{K}$  et soit  $\mathcal{L}$  une famille libre de  $E$ . Soit  $\mathcal{S}$  l'ensemble des parties libres de  $E$  qui contiennent  $\mathcal{L}$ , muni de l'ordre fourni par l'inclusion. Comme  $\mathcal{L} \in \mathcal{S}$ , on a  $\mathcal{S} \neq \emptyset$ .

$S$  muni de cet ordre est inductif : soit  $F = (S_i)_{i \in I}$  une partie totalement ordonnée de  $S$ . Alors  $K = \cup_{i \in I} S_i$  contient  $\mathcal{L}$  et tous les  $S_i$  pour  $i \in I$ . Il reste à vérifier que c'est un élément de  $S$ , c'est-à-dire une famille libre, pour démontrer que  $K$  est un majorant de  $F$  dans  $S$ . Soit  $\sum_{j \in J} \lambda_j x_j = 0$  une relation de dépendance avec  $J$  une partie finie de  $I$ ,  $x_j \in S_j$  et  $\lambda_j \in \mathbb{K}$  pour tout  $j \in J$ . Puisque  $J$  est fini et  $F$  est totalement ordonnée, on peut choisir  $i_0 \in J$  tel que  $S_j \subset S_{i_0}$  pour tout  $j \in J$ . Alors  $x_j \in S_{i_0}$  pour tout  $j \in J$ . Or  $S_{i_0}$  est libre, donc  $\lambda_j = 0$  pour tout  $j \in J$ . Donc  $K$  est libre.

D'après le lemme de Zorn, il existe une partie libre maximale dans  $S$ , notons-la  $B$ . La famille  $B$  contient  $\mathcal{L}$ . Il reste à démontrer que  $B$  est un système générateur : sinon, il existe  $y \in E$  tel que  $y \notin \text{vect}\{B\}$ , donc  $\{y\} \cup B$  est libre, ce qui contredit la maximalité de  $B$ . ✓

**Théorème 7.25** (Théorème de Krull). Soit  $A$  un anneau unitaire. Alors tout idéal de  $A$  distinct de  $A$  est contenu dans un idéal maximal.

*Démonstration.* Soit  $I$  un idéal de  $A$  distinct de  $A$ . Soit  $\mathcal{S}$  l'ensemble des idéaux de  $A$  qui contiennent  $I$  et qui sont distincts de  $A$ , ordonné par l'inclusion. Puisque  $I \in \mathcal{S}$ , cet ensemble n'est pas vide. De plus,  $\mathcal{S}$  muni de cet ordre est inductif : soit  $F = (I_j)_{j \in J}$  une famille totalement ordonnée d'idéaux qui contiennent  $I$  et qui sont distincts de  $A$ . Alors  $K = \cup_{j \in J} I_j$  contient tous les  $I_j$  pour  $j \in J$ , donc si c'est un élément de  $\mathcal{S}$ , c'est-à-dire un idéal distinct de  $A$  et contenant  $I$ , alors c'est un majorant de  $F$  dans  $\mathcal{S}$ .

Vérifions donc que  $K \in \mathcal{S}$ . Tout d'abord,  $1 \notin \cup_{j \in J} I_j$  donc  $K \neq A$ . Il est clair que  $I \subset \cup_{j \in J} I_j = K$ . De plus, si  $x$  et  $y$  sont dans  $K$  il existe  $j_0$  tel que  $x$  et  $y$  soient dans  $I_{j_0}$  (puisque la famille des  $I_j$  est totalement ordonnée). Alors  $x + y \in I_{j_0} \subset K$  et  $ax \in I_{j_0} \subset K$  pour tout  $a \in A$ , donc c'est bien un idéal de  $A$ . On en déduit que  $K$  est dans  $\mathcal{S}$ .

D'après le lemme de Zorn,  $\mathcal{S}$  contient un élément maximal. C'est un idéal maximal de  $A$  contenant  $I$ . ✓

*Remarque.* Vous verrez également le théorème de Hahn-Banach qui se démontre à l'aide du lemme de Zorn.

#### IV. CORPS DES FRACTIONS D'UN ANNEAU INTÈGRE

Soit  $A$  un anneau *intègre*. Notons  $S = A \setminus \{0\}$ .

On veut construire un corps  $K$  contenant  $A$  comme sous-anneau (d'où la nécessité d'avoir un anneau intègre) et qui soit minimal pour cette propriété. La construction est la même que celle de  $\mathbb{Q}$  à partir de  $\mathbb{Z}$  : on va considérer un ensemble de quotients de la forme  $\frac{a}{s}$  avec  $(a, s) \in A^2$  et  $s \neq 0$ , et le munir d'une structure d'anneau (qui se trouvera être un corps).

On définit une relation d'équivalence sur  $A \times S$  par

$$(a, s) \sim (a', s') \iff as' - a's = 0.$$

C'est bien une relation d'équivalence :

- $(a, s) \sim (a, s)$  car  $as - sa = 0$ .
- Si  $(a, s) \sim (a', s')$ , alors  $as' - a's = 0$ , donc  $a's - as' = 0$  et donc  $(a', s') \sim (a, s)$ .
- Si  $(a, s) \sim (a', s')$  et  $(a', s') \sim (a'', s'')$ , alors  $as' - a's = 0$  et  $a's'' - a''s' = 0$ . Donc  $(as' - a's)s'' + (a's'' - a''s')s = as's'' - a''s's = 0$  et donc  $as'' - a''s = 0$  car  $A$  est intègre et  $s' \neq 0$ . Donc  $(a, s) \sim (a'', s'')$ .

On forme le quotient  $A \times S / \sim$ , dont les éléments sont notés  $\frac{a}{s}$ . On note ce quotient  $\text{Frac}(A)$ .

**Définition-Proposition 7.26.**  $\text{Frac}(A)$  est un corps (commutatif), dit *corps des fractions* de  $A$ , pour les opérations suivantes :

$$\triangleright \frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$$

$$\triangleright \frac{a}{s} \frac{a'}{s'} = \frac{aa'}{ss'}.$$

L'unité est  $\frac{1}{1}$  et l'élément nul est  $\frac{0}{1}$ .

*Démonstration.* Les opérations sont bien définies : si  $\frac{a}{s} = \frac{a_1}{s_1}$  et  $\frac{a'}{s'} = \frac{a'_1}{s'_1}$ , on doit vérifier que

$$\frac{a_1s'_1 + a'_1s_1}{s_1s'_1} = \frac{as' + a's}{ss'} \quad (\text{IV.1}) \quad \text{et que} \quad \frac{aa'}{ss'} = \frac{a_1a'_1}{s_1s'_1}. \quad (\text{IV.2})$$

Par hypothèse, on a  $a_1s - as_1 = 0$  et  $a'_1s' - a's'_1 = 0$ . On a donc  $0 = (a_1s - as_1)s'_1 + (a'_1s' - a's'_1)ss_1 = ss'(s'_1a_1 + s_1a'_1) - s_1s'_1(as' + sa')$ , ce qui démontre (IV.1), et  $0 = (a_1s - as_1)a'_1s'_1 + (a'_1s' - a's'_1)as_1 = a_1a'_1ss'_1 - aa's_1s'_1$ , ce qui démontre (IV.2).

Il reste à vérifier que  $A$  est bien un anneau, commutatif et unitaire, et que tout élément non nul est inversible (exercice). ✓

**Remarque.** L'application  $\varphi: A \rightarrow \text{Frac}(A)$  définie par  $\varphi(a) = \frac{a}{1}$  est un morphisme d'anneaux injectif. Ainsi  $A$  peut être identifié à un sous-anneau de  $\text{Frac}(A)$ .

**Proposition 7.27.** Soit  $A$  un anneau intègre et soit  $\varphi: A \rightarrow \text{Frac}(A)$  le morphisme d'anneaux ci-dessus. Pour tout anneau  $B$  et pour tout morphisme d'anneaux  $f: A \rightarrow B$  tel que pour tout  $s \in S$ ,  $f(s)$  est inversible dans  $B$  (autrement dit,  $f(S) \subset B^\times$ ), il existe un unique morphisme d'anneaux  $g: \text{Frac}(A) \rightarrow B$  tel que  $g \circ \varphi = f$ .

*Démonstration.* Commençons par démontrer l'unicité. Supposons que  $g$  existe. Alors on doit avoir  $f(a) = g(\varphi(a)) = g\left(\frac{a}{1}\right) = g\left(\frac{a}{s} \frac{s}{1}\right) = g\left(\frac{a}{s}\right)g\left(\frac{s}{1}\right) = g\left(\frac{a}{s}\right)g(\varphi(s)) = g\left(\frac{a}{s}\right)f(s)$ , d'où l'unicité pour  $g\left(\frac{a}{s}\right)$ .

Maintenant, posons  $g\left(\frac{a}{s}\right) = (f(s))^{-1}f(a)$ . Alors

➤  $g$  est bien défini : si  $\frac{a}{s} = \frac{a'}{s'}$ , alors  $as' - a's = 0$ , d'où  $f(a')f(s) - f(a)f(s') = 0$ . En multipliant par  $f(s)^{-1}f(s')^{-1}$ , on obtient  $f(s)^{-1}f(a) = f(s')^{-1}f(a')$ .

➤  $g$  est un morphisme. En effet, on a

$$\begin{aligned} \blacklozenge g\left(\frac{a}{s} + \frac{a'}{s'}\right) &= g\left(\frac{as' + a's}{ss'}\right) = f(as' + a's)f(ss')^{-1} \\ &= f(a)f(s')f(s)^{-1}f(s')^{-1} + f(a')f(s)f(s)^{-1}f(s')^{-1} \\ &= f(a)f(s)^{-1} + f(a')f(s')^{-1} = g\left(\frac{a}{s}\right) + g\left(\frac{a'}{s'}\right); \end{aligned}$$

$$\begin{aligned} \blacklozenge g\left(\frac{a}{s} \frac{a'}{s'}\right) &= g\left(\frac{aa'}{ss'}\right) = f(aa')f(ss')^{-1} = f(a)f(a')f(s)^{-1}f(s')^{-1} \\ &= f(a)f(s)^{-1}f(a')f(s')^{-1} = g\left(\frac{a}{s}\right)g\left(\frac{a'}{s'}\right); \end{aligned}$$

$$\blacklozenge g\left(\frac{1}{1}\right) = f(1)f(1)^{-1} = 1.$$

➤  $g \circ \varphi = f$  :  $g \circ \varphi(a) = g\left(\frac{a}{1}\right) = f(1)^{-1}f(a) = f(a)$ . ✓

*Remarque.* Le morphisme  $g$  est nécessairement injectif.

**Conséquence 7.28** (« Minimalité » du corps des fractions). Soit  $K$  un corps contenant  $A$  comme sous-anneau. Alors  $\text{Frac}(A)$  est (s'identifie à) un sous-corps de  $K$ .

Autrement dit,  $\text{Frac}(A)$  est le plus petit corps contenant  $A$ .

Pour vérifier cela, il suffit d'appliquer la proposition avec  $f$  l'inclusion de  $A$  dans  $K$ .

*Exemple.* Si  $A = \mathbb{Z}$  on obtient  $\text{Frac}(A) = \mathbb{Q}$ .

*Exemple.* Soit  $K$  un corps. Le corps des fractions de l'anneau de polynômes  $K[X]$  est le corps des fractions rationnelles  $K(X)$ .

# Arithmétique dans les anneaux

## I. RAPPELS D'ARITHMÉTIQUE.

Dans cette partie, on étudie et rappelle des propriétés arithmétiques des anneaux, c'est-à-dire des propriétés des anneaux liées à la divisibilité.

Dans toute cette partie, sauf mention expresse du contraire,  $A$  désigne un anneau (commutatif, unitaire) intègre (et donc non nul). On note alors  $A^\times$  le groupe des éléments inversibles de  $A$ .

**Définition 8.1.** Soit  $(a, b) \in A^2$ .

- (1) On dit que  $a$  **divise**  $b$ , et on note  $a \mid b$ , s'il existe un élément  $c$  de  $A$  tel que  $b = ac$ .
- (2) On dit que  $a$  et  $b$  sont **associés** si  $a \mid b$  et  $b \mid a$ . On note  $a \sim b$ .

**Remarque.** Soit  $(a, b) \in A^2$ . Les points suivants sont clairs :

- (1)  $a$  divise  $b$  si et seulement si  $(b) \subset (a)$ ;
- (2)  $a$  et  $b$  sont associés si et seulement si  $(a) = (b)$ ;
- (3)  $a$  et  $b$  sont associés si et seulement s'il existe  $u \in A^\times$  tel que  $a = ub$ .

**Définition 8.2.** Soit  $p$  un élément de  $A$ .

- On dit que  $p$  est **irréductible** (dans  $A$ ) s'il satisfait aux conditions suivantes :
  - (i)  $p \notin A^\times$ ;
  - (ii)  $p = ab$  avec  $(a, b) \in A^2$  entraîne que  $a$  ou  $b$  est un élément inversible de  $A$ .
- On dit que  $p$  est **premier** (dans  $A$ ) s'il n'est pas nul et si l'idéal engendré  $(p)$  de  $A$  est premier.

**Remarques.** (1) Le produit d'un élément irréductible de  $A$  par un élément inversible de  $A$  est un élément irréductible de  $A$ .

(2) L'élément 0 n'est pas irréductible car  $0 = 0 \cdot 0$ . Ainsi, un corps n'a pas d'éléments irréductibles.

(3) Soit  $p$  un élément de  $A$ ;  $p$  est irréductible dans  $A$  si et seulement si :

- (i)  $p \notin A^\times$ ;
- (ii)  $p \neq 0$  et les seuls diviseurs de  $p$  sont les éléments inversibles de  $A$  et les éléments de  $A$  associés à  $p$ .

*Démonstration.* Supposons que  $p$  est un élément irréductible de  $A$  et soit  $a$  un diviseur de  $p$ . Alors il existe  $b \in A \setminus \{0\}$  tel que  $p = ab$ . On en déduit que  $a$  ou  $b$  est inversible. Si  $b$  est inversible, alors  $a$  est associé à  $p$ . Ainsi,  $a$  est inversible ou associé à  $p$ .

Réciproquement, soit  $p \in A \setminus A^\times$  et supposons que les seuls diviseurs de  $p$  sont les éléments inversibles de  $A$  et les éléments de  $A$  associés à  $p$ . On suppose que  $p = ab$  avec

$(a, b) \in A^2$ . Alors  $a$  divise  $p$  donc  $a$  est inversible ou associé à  $p$ . Si  $a$  est associé à  $p$  alors il existe  $u \in A^\times$  tel que  $a = up$ , donc  $p = upb$  et donc, puisque  $A$  est intègre,  $1 = ub$  donc  $b$  est inversible. Donc  $a$  ou  $b$  est inversible et  $p$  est bien irréductible dans  $A$ . ✓

(4) Soit  $p \in A$  un élément non nul. Alors  $p$  est premier si et seulement s'il n'est pas inversible et si pour tout  $(a, b) \in A^2$ ,  $p \mid ab \Rightarrow (p \mid a \text{ ou } p \mid b)$ .

(5) Soit  $p \in A$ ; si  $p$  est premier, alors  $p$  est irréductible.

*Démonstration.* Soit  $p \in A$  un élément premier. En particulier,  $p$  n'est pas inversible (sinon  $(p) = A$  n'est pas premier). Supposons que  $p = ab$  avec  $(a, b) \in A^2$ . Alors  $p$  divise  $ab$  donc  $p$  divise  $a$  ou  $p$  divise  $b$ ; par exemple,  $p$  divise  $a$ . Alors il existe  $c \in A$  tel que  $a = pc$  donc  $p = pcb$  et donc, puisque  $A$  est intègre,  $1 = cb$ . Donc  $b$  est inversible. On en déduit que  $p$  est irréductible. ✓

(6) **Attention!** Les notions d'irréductibilité et de primalité dépendent de l'anneau ambiant. Par exemple, le polynôme  $2X$  est irréductible et premier dans  $\mathbb{Q}[X]$  (voir chapitre suivant) mais n'est ni irréductible, ni premier dans  $\mathbb{Z}[X]$ . Dans l'autre sens, le nombre entier 2 est irréductible (et premier) dans  $\mathbb{Z}$  mais pas dans  $\mathbb{Q}$  puisqu'il est inversible dans  $\mathbb{Q}$ . Ainsi, sauf s'il n'y a pas de confusion possible, on précise toujours irréductible (ou premier) dans  $A$ .

**Définition 8.3.** Soient  $I$  un ensemble non vide et  $(a_i)_{i \in I}$  une famille d'éléments de  $A$ .

(1) On dit que  $a \in A$  est un **diviseur** (resp. **multiple**) **commun** de  $(a_i)_{i \in I}$  si, pour tout  $i \in I$ ,  $a \mid a_i$  (resp.  $a_i \mid a$ ).

(2) On suppose que les  $a_i$ ,  $i \in I$ , ne sont pas tous nuls. On dit que  $d \in A$  est un **plus grand commun diviseur** (en abrégé pgcd) de  $(a_i)_{i \in I}$  si c'est un diviseur commun de  $(a_i)_{i \in I}$  et si tout diviseur commun de  $(a_i)_{i \in I}$  divise  $d$ .

(3) On suppose que tous les  $a_i$ ,  $i \in I$ , sont non nuls. On dit que  $m \in A$  est un **plus petit commun multiple** (en abrégé ppcm) de  $(a_i)_{i \in I}$  si c'est un multiple commun de  $(a_i)_{i \in I}$  qui divise tout multiple commun de  $(a_i)_{i \in I}$ .

(4) On dit que les  $a_i$ ,  $i \in I$ , sont **premiers entre eux** si 1 est un pgcd de  $(a_i)_{i \in I}$ .

**Remarque.** Soit  $I$  un ensemble non vide et soit  $\mathcal{A} = (a_i)_{i \in I}$  une famille d'éléments de  $A$ . On suppose que les  $a_i$ ,  $i \in I$ , ne sont pas tous nuls (resp. sont tous non nuls). On démontre facilement que si  $a \in A$  est un pgcd (resp. ppcm) de  $\mathcal{A}$ , un élément  $b$  est un pgcd (resp. ppcm) de  $\mathcal{A}$  si et seulement s'il est associé à  $a$ .

On notera donc  $d \sim \text{pgcd}(a_i, i \in I)$  (resp.  $m \sim \text{ppcm}(a_i, i \in I)$ ) si  $d$  (resp.  $m$ ) est un pgcd (resp. ppcm) de  $(a_i)_{i \in I}$ .

**Remarque.** Soit  $a \in A \setminus \{0\}$  et soit  $b \in A$ . Alors  $a$  et  $b$  sont premiers entre eux si, et seulement si, les seuls diviseurs communs à  $a$  et  $b$  sont les éléments inversibles de  $A$ .

En particulier, puisque  $a$  divise 0,  $a$  et 0 sont premiers entre eux si et seulement si  $a$  est un élément inversible de  $A$ .

*Démonstration.* Supposons que  $a$  et  $b$  sont premiers entre eux et soit  $c$  un diviseur commun à  $a$  et  $b$ . Par hypothèse,  $a$  et  $b$  admettent 1 comme pgcd donc  $c$  divise 1 et donc  $c$  est inversible.

Réciproquement, supposons que les seuls diviseurs communs à  $a$  et  $b$  sont les éléments inversibles de  $A$ . Il est clair que 1 est un diviseur commun à  $a$  et  $b$ . Soit maintenant  $c$  un diviseur commun à  $a$  et  $b$ . Par hypothèse  $c$  est inversible donc  $c$  divise 1. On en déduit que 1 est un pgcd de  $a$  et  $b$ , c'est-à-dire que  $a$  et  $b$  sont premiers entre eux. ✓

**Proposition 8.4.** Soit  $(a, b) \in A^2$ ,  $ab \neq 0$ . Soit  $d$  un pgcd de  $a$  et  $b$  et soit  $m$  un ppcm de  $a$  et  $b$ . Alors  $ab$  et  $dm$  sont associés.

*Démonstration.* Puisque  $a$  et  $b$  divisent  $ab$ , leur ppcm  $m$  divise  $ab$ . Posons  $ab = me$  pour un  $e \in A$ . Pour conclure, il suffit de démontrer que  $e$  est associé à  $d$ .

Posons  $a = da'$ ,  $b = db'$ , et  $m = aa'' = bb''$ .

On a  $ab = me = aa''e$  donc  $b = a''e$  et donc  $e$  divise  $b$ . De même,  $e$  divise  $a$ , donc  $e$  divise  $d$  qui est un pgcd de  $a$  et  $b$ .

Puisque  $d$  divise  $a$  et  $b$ , il divise  $ab$ , posons  $ab = dx$ . On a alors  $dx = ab = da'b = dab'$  donc  $x = ab' = a'b$  et donc  $a$  et  $b$  divisent tous deux  $x$ , donc  $m$  divise  $x$ . Posons  $x = my$ . On a alors  $me = ab = dx = dmy$  donc  $e = dy$  est un multiple de  $d$ .

On en déduit finalement que  $d$  est associé à  $e$  et donc que  $ab = me$  est associé à  $md$ . ✓

**Proposition 8.5.** Soit  $a$  un élément irréductible de  $A$  et  $b$  un élément de  $A$ . Alors,  $a$  et  $b$  sont premiers entre eux si et seulement si  $a$  ne divise pas  $b$ .

*Démonstration.* Supposons que  $a$  divise  $b$ . Alors  $a$  est un diviseur commun à  $a$  et  $b$  qui n'est pas inversible. D'après la remarque plus haut, on en déduit que  $a$  et  $b$  ne sont pas premiers entre eux.

Réciproquement, supposons que  $a$  ne divise pas  $b$ . Soit  $x$  un diviseur commun de  $a$  et  $b$ . Il existe  $a' \in A$  tel que  $a = xa'$ . Comme  $a$  est irréductible,  $x$  ou  $a'$  est inversible et puisque  $a$  ne divise pas  $b$ , on en déduit que  $x$  est inversible. Donc tout diviseur commun de  $a$  et  $b$  est inversible, c'est-à-dire que  $a$  et  $b$  sont premiers entre eux. ✓

## II. ANNEAUX FACTORIELS

### A. Anneaux factoriels.

**Définition 8.6. (1)** On dit que  $A$  satisfait la condition (E) si tout élément non nul et non inversible  $a \in A$  admet une décomposition en produit d'éléments irréductibles, c'est-à-dire qu'il existe  $r \in \mathbb{N}^*$  et des éléments irréductibles  $p_1, \dots, p_r$  de  $A$  tels que  $a = p_1 \dots p_r$ .

**(2)** On dit que  $A$  satisfait la condition (U) si pour tout élément non nul et non inversible de  $A$ , une décomposition en produit d'éléments irréductibles (si elle existe) est essentiellement unique, c'est-à-dire que, si  $a = p_1 \dots p_r = q_1 \dots q_s$  où  $(r, s) \in \mathbb{N}^* \times \mathbb{N}^*$  et  $p_1, \dots, p_r, q_1, \dots, q_s$  sont des éléments irréductibles de  $A$ , alors  $r = s$  et il existe  $\sigma \in S_r$  tel que, pour  $1 \leq i \leq r$ ,  $p_i$  et  $q_{\sigma(i)}$  soient associés.

**(3)** On dit que  $A$  est **factoriel** s'il est intègre et s'il satisfait aux conditions (E) et (U).

*Exemple.* Tout corps est un anneau factoriel.

On va donner une définition équivalente d'un anneau factoriel, dans laquelle on a vraiment unicité de la décomposition. Pour cela on introduit la définition suivante.

**Définition 8.7.** Soit  $A$  un anneau. Une partie  $\mathcal{P}$  de  $A$  est un **système de représentants des éléments irréductibles** de  $A$  si c'est un système de représentants des classes d'équivalence des éléments irréductibles de  $A$  pour la relation  $\sim$  (association), autrement dit,

- tout élément de  $\mathcal{P}$  est irréductible dans  $A$ ;
- si  $a \in A$  est irréductible alors il existe  $p \in \mathcal{P}$  tel que  $a \sim p$ ;
- deux éléments distincts de  $\mathcal{P}$  ne sont pas associés.

**Définition-Proposition 8.8.** Un anneau  $A$  est factoriel si, et seulement si, il est intègre et si tout élément non nul  $a \in A$  se décompose de manière unique sous la forme  $a = u_a \prod_{p \in \mathcal{P}} p^{v_p(a)}$  avec  $u_a \in A^\times$ ,  $v_p(a) \in \mathbb{N}$  pour tout  $p \in \mathcal{P}$  et les  $v_p(a)$  sont nuls sauf pour un nombre fini de  $p \in \mathcal{P}$ . Pour  $p \in \mathcal{P}$ , le nombre entier  $v_p(a)$  est appelé **valuation  $p$ -adique** de  $a$ .

*Démonstration.* C'est clair. ✓

**Exemple.** L'anneau  $\mathbb{Z}$  est factoriel (les éléments irréductibles de  $\mathbb{Z}$  sont les nombres premiers et leurs opposés). Si  $A = \mathbb{Z}$ , on peut prendre l'ensemble des nombres premiers (positifs) pour  $\mathcal{P}$ , ou bien l'ensemble des opposés de nombres premiers.

**Propriétés 8.9.** Soit  $A$  un anneau factoriel et soient  $a$  et  $b$  deux éléments non nuls de  $A$ . Alors

- (1) pour tout  $p \in \mathcal{P}$  on a  $v_p(ab) = v_p(a) + v_p(b)$ .
- (2)  $a$  divise  $b$  si, et seulement si,  $v_p(a) \leq v_p(b)$  pour tout  $p \in \mathcal{P}$ .
- (3)  $a$  et  $b$  sont premiers entre eux si, et seulement si,  $v_p(a)v_p(b) = 0$  pour tout  $p \in \mathcal{P}$ .

*Démonstration.* Pour tout  $x \in A \setminus \{0\}$ , on note  $x = u_x \prod_{p \in \mathcal{P}} p^{v_p(x)}$  comme dans la définition-proposition 8.8.

- (1) On a  $ab = \left(u_a \prod_{p \in \mathcal{P}} p^{v_p(a)}\right) \left(u_b \prod_{p \in \mathcal{P}} p^{v_p(b)}\right) = u_a u_b \prod_{p \in \mathcal{P}} p^{v_p(a) + v_p(b)} = u_{ab} \prod_{p \in \mathcal{P}} p^{v_p(ab)}$ . Par unicité de la décomposition on en déduit que  $u_{ab} = u_a u_b$  et  $v_p(ab) = v_p(a) + v_p(b)$  pour tout  $p \in \mathcal{P}$ .
- (2) ( $\Leftarrow$ ) Si  $v_p(a) \leq v_p(b)$  pour tout  $i$ , alors  $b = a u_a^{-1} u_b \prod_{p \in \mathcal{P}} p^{v_p(b) - v_p(a)}$  donc  $a$  divise  $b$ . [Les hypothèses sur  $A$  ne servent pas ici.]  
 ( $\Rightarrow$ ) S'il existe  $c \in A$  tel que  $b = ac$ , alors pour tout  $p \in \mathcal{P}$  on a  $v_p(b) = v_p(a) + v_p(c) \geq v_p(a)$ .
- (3) ( $\Rightarrow$ ) S'il existe  $p$  tel que  $v_p(a)v_p(b) \neq 0$ , alors  $p$  divise  $a$  et  $b$  donc, comme  $p$  n'est pas inversible,  $a$  et  $b$  ne sont pas premiers entre eux. [Les hypothèses sur  $A$  ne servent pas ici.]  
 ( $\Leftarrow$ ) Supposons que l'on ait, pour tout  $p \in \mathcal{P}$ ,  $v_p(a)v_p(b) = 0$ . Soit  $c$  un diviseur commun de  $a$  et  $b$ . On a donc  $0 \leq v_p(c) \leq \min(v_p(a), v_p(b)) = 0$  pour tout  $p \in \mathcal{P}$  donc  $v_p(c) = 0$  pour tout  $p \in \mathcal{P}$  et donc  $c = u_c \in A^\times$ . D'après une remarque page 100,  $a$  et  $b$  sont premiers entre eux. ✓

Dans un anneau intègre quelconque, les pgcd et ppcm n'existent pas toujours. Cependant, dans un anneau factoriel, ils existent toujours.

**Proposition 8.10.** Supposons  $A$  factoriel. Si  $a_1, \dots, a_r$  ( $r \in \mathbb{N}^*$ ) sont des éléments non nuls de  $A$ , alors ils admettent un pgcd et un ppcm.

*Démonstration.* Posons  $a_i = u_{a_i} \prod_{p \in \mathcal{P}} p^{v_p(a_i)}$  pour tout  $i$ .

Pour tout  $p \in \mathcal{P}$ , posons  $\delta_p = \min\{v_p(a_i) \mid i \in \llbracket 1; r \rrbracket\}$  et considérons  $d = \prod_{p \in \mathcal{P}} p^{\delta_p}$  (notons que c'est bien le produit d'un nombre fini d'éléments distincts de 1).

- Il est clair que  $d$  est un diviseur de chacun des  $a_i$  (pour tout  $p \in \mathcal{P}$  on a  $v_p(d) = \delta_p \leq v_p(a_i)$ ).
- Soit  $x \in A$  un diviseur commun des  $a_i$ . Puisque  $x$  divise tous les  $a_i$ , on a  $v_p(x) \leq \min\{v_p(a_i) \mid i \in \llbracket 1; r \rrbracket\} = \delta_p = v_p(d)$  pour tout  $p \in \mathcal{P}$ , donc  $x$  divise  $d$ .

L'élément  $d$  est donc bien un pgcd des  $a_i$ .

Pour le ppcm on fait un raisonnement similaire.

Pour tout  $p \in \mathcal{P}$ , posons  $\mu_p = \max\{v_p(a_i) \mid i \in \llbracket 1; r \rrbracket\}$  et considérons  $m = \prod_{p \in \mathcal{P}} p^{\mu_p}$ .

- Il est clair que  $m$  est un multiple de tous les  $a_i$ .
- Soit  $y \in A$  un multiple commun des  $a_i$ . Puisque  $a_i$  divise  $y$  pour tout  $i$ , on a  $v_p(y) \geq \max\{v_p(a_i) \mid i \in \llbracket 1; r \rrbracket\} = \mu_p = v_p(m)$  pour tout  $p \in \mathcal{P}$ , donc  $m$  divise  $y$ .
- L'élément  $m$  est donc bien un ppcm de  $a$  et  $b$ . ✓

**Lemme 8.11.** Soit  $A$  un anneau (intègre) dans lequel tout  $(a, b) \in A^2 \setminus \{(0, 0)\}$  admet un pgcd (par exemple un anneau factoriel), soit  $\{a_i \mid i \in I\}$  une famille finie d'éléments non tous nuls de  $A$  et soit  $b \in A, b \neq 0$ .

- (1) Soit  $d$  un pgcd des  $a_i$ . Alors  $bd$  est un pgcd des  $ba_i, i \in I$ .
- (2) Si  $d$  est un pgcd des  $a_i$  alors pour tout  $i \in I$  il existe  $a'_i \in A$  tel que  $a_i = da'_i$ , et les  $a'_i, i \in I$ , sont premiers entre eux.

*Démonstration.* (1) Soit  $c$  un pgcd des  $ba_i$ . Il est clair que  $bd$  est un diviseur commun des  $ba_i$  donc  $bd$  divise  $c$ . Réciproquement, puisque  $b \mid ba_i$  pour tout  $i \in I$ , on en déduit que  $b \mid c$  donc  $c = bc'$  avec  $c' \in A$ . Puisque  $c = bc' \mid ba_i$  pour tout  $i \in I$ , on a  $c' \mid a_i$  pour tout  $i$  et donc  $c' \mid d$ . Finalement,  $c = bc'$  divise  $bd$ . Donc  $bd \sim c$  est un pgcd des  $ba_i$ .

*On peut aussi utiliser les décompositions en produits de facteurs irréductibles pour démontrer ce résultat, mais alors il faut supposer que  $A$  est factoriel.*

- (2) Puisque  $d$  est un diviseur commun des  $a_i$ , il existe  $a'_i$  tel que  $a_i = da'_i$  pour tout  $i \in I$ . D'après ce qui précède, si  $d'$  est un pgcd des  $a'_i$  (qui existe car  $A$  est factoriel), alors  $dd'$  est un pgcd des  $a_i$  donc il est associé à  $d$  et donc  $d'$  est inversible. ✓

**Proposition 8.12.** Soit  $A$  un anneau (intègre) dans lequel tout  $(a, b) \in A^2$  avec  $ab \neq 0$  admet un ppcm (par exemple un anneau factoriel). Soient  $a_1, \dots, a_r$  ( $r \in \mathbb{N}^*$ ) des éléments de  $A$  qui sont tous non nuls.

Alors un élément de  $A$  est un ppcm de  $\{a_1, \dots, a_r\}$  si et seulement s'il engendre l'idéal  $a_1A \cap \dots \cap a_rA = (a_1) \cap \dots \cap (a_r)$ .

*Démonstration.* Notons  $I = \llbracket 1; r \rrbracket$ .

Soit  $m$  un ppcm de  $\{a_1, \dots, a_r\}$ . Alors pour tout  $i \in I$  on a  $(m) \subset (a_i)$ , donc  $(m) \subset (a_1) \cap \dots \cap (a_r)$ .

Soit maintenant  $x \in (a_1) \cap \dots \cap (a_r)$ . Alors, pour tout  $i$ , on a  $a_i \mid x$  donc, par définition du ppcm, on a  $m \mid x$  et donc  $x \in (m)$ . Par conséquent,  $(a_1) \cap \dots \cap (a_r) \subset (m)$  et finalement  $(a_1) \cap \dots \cap (a_r) = (m)$ .

Réciproquement, si  $m \in A$  est tel que  $(m) = (a_1) \cap \dots \cap (a_r)$ , alors  $m$  est un multiple commun des  $a_i, i \in I$ , et pour tout autre multiple commun  $c$  des  $a_i, i \in I$ , on a  $(m) = (a_1) \cap \dots \cap (a_r) \supset (c)$  donc  $m$  divise  $c$  et donc  $m$  est un ppcm des  $a_i, i \in I$ . ✓

**Théorème 8.13.** Soit  $A$  un anneau intègre satisfaisant la condition (E). Alors les assertions suivantes sont équivalentes :

- (a)  $A$  est factoriel
- (b)  $A$  satisfait la condition (U).
- (c) Pour tout triplet  $(a, b, c)$  d'éléments de  $A$  tel que  $a \neq 0$ , si  $a$  et  $b$  sont premiers entre eux et si  $a \mid bc$ , alors  $a \mid c$  (condition de Gauss).
- (d) Pour tout triplet  $(a, b, c)$  d'éléments de  $A$ , si  $a$  est irréductible et divise  $bc$ , alors  $a$  divise  $b$  ou  $a$  divise  $c$  (condition d'Euclide).
- (e) Pour  $p$  dans  $A$ ,  $p$  est premier si et seulement si  $p$  est irréductible (condition de primalité).

*Démonstration.* (a)  $\Leftrightarrow$  (b) par définition d'un anneau factoriel.

(a)⇒(c) On suppose que  $A$  est factoriel. Soient  $a$  et  $b$  premiers entre eux divisant  $bc$ .

- Si  $b = 0$ , puisque  $a$  et  $b$  sont premiers entre eux on en déduit que  $a$  est inversible (voir remarque page 100) donc  $a$  divise  $c$ .
- Si  $c = 0$ , alors  $a$  divise  $c$ .
- Supposons donc que  $a$ ,  $b$  et  $c$  ne sont pas nuls. Puisque  $A$  est factoriel, on peut décomposer  $a$ ,  $b$  et  $c$  de manière unique sous la forme  $a = u_a \prod_{p \in \mathcal{P}} p^{v_p(a)}$ ,  $b = u_b \prod_{p \in \mathcal{P}} p^{v_p(b)}$  et  $c = u_c \prod_{p \in \mathcal{P}} p^{v_p(c)}$  avec les notations de la définition-proposition 8.8. Alors, puisque  $a$  et  $b$  sont premiers entre eux, on a  $v_p(a)v_p(b) = 0$  pour tout  $p \in \mathcal{P}$ . Puisque  $a$  divise  $bc$  on a  $v_p(a) \leq v_p(b) + v_p(c)$  pour tout  $p \in \mathcal{P}$ . On en déduit facilement que  $v_p(a) \leq v_p(c)$  pour tout  $p \in \mathcal{P}$  et donc que  $a$  divise  $c$ .

(c)⇒(d) On suppose que la condition de Gauss est vérifiée. Soit  $a$  un élément irréductible divisant  $bc$ . Si  $a$  ne divise pas  $b$ , alors d'après la proposition 8.5  $a$  et  $b$  sont premiers entre eux, donc d'après la condition de Gauss  $a$  divise  $c$ .

(d)⇒(e) On suppose que la condition d'Euclide est vérifiée. On sait déjà que si  $p$  est premier alors  $p$  est irréductible. Soit  $p$  un élément irréductible. Il n'est pas nul et il n'est pas inversible. Supposons que  $p$  divise  $ab$  avec  $(a, b) \in A^2$ . Si  $p$  ne divise pas  $a$ , alors  $p$  et  $a$  sont premiers entre eux d'après la proposition 8.5 donc d'après l'hypothèse (d) on en déduit que  $p$  divise  $b$ . Donc  $p$  divise  $a$  ou  $p$  divise  $b$ . Finalement,  $p$  est premier.

(e)⇒(b) On suppose que la condition de primalité est vérifiée. Soit  $a \in A$  et supposons que  $a = p_1 \dots p_m = q_1 \dots q_n$  avec  $p_1, \dots, p_m, q_1, \dots, q_n$  irréductibles et  $m \leq n$ . On raisonne par récurrence sur  $m$ .

- Initialisation. Si  $m = 1$ , on a  $a = p_1 = q_1 \dots q_n$ . Donc  $q_1 \mid p_1$ ,  $p_1$  est irréductible et  $q_1 \notin A^\times$ , donc  $q_1 = up_1$  avec  $u \in A^\times$ . Donc  $uq_2 \dots q_n \in A^\times$  et donc  $n = 1$ .
- Hérédité. Soit  $m > 1$  tel que le résultat soit vrai jusqu'au rang  $m - 1$ ; démontrons-le au rang  $m$ . On a  $p_1(p_2 \dots p_m) = q_1 \dots q_n$ . Puisque  $p_1$  est irréductible,  $p_1$  est premier d'après (e), et il divise  $q_1 \dots q_n$ , donc il existe  $i$  tel que  $p_1 \mid q_i$  : on a  $q_i = u_1 p_1$  avec  $u_1 \in A$ . Puisque  $q_i$  est irréductible,  $u_1 \in A^\times$ .  
On a donc  $p_1(p_2 \dots p_m) = u_1 p_1(q_1 \dots q_{i-1} q_{i+1} \dots q_n)$ , donc  $p_2 \dots p_m = u_1 q_1 \dots q_{i-1} q_{i+1} \dots q_n$  et par hypothèse de récurrence on a  $m - 1 = n - 1$ , donc  $m = n$ , et il existe une bijection  $\tau: \{2, \dots, m\} \rightarrow \{1, \dots, m\} \setminus \{i\}$  telle que  $p_j \sim q_{\tau(j)}$  pour tout  $j = 2, \dots, m$ . On conclut en définissant  $\sigma \in S_m$  par  $\sigma(1) = i$  et  $\sigma(j) = \tau(j)$  pour  $j = 2, \dots, m$ . ✓

## B. Exemples d'anneaux factoriels.

Dans cette partie, on étudie les anneaux principaux et les anneaux euclidiens. Ce sont des exemples d'anneaux factoriels.

On commence par l'étude des anneaux principaux. On rappelle qu'un idéal  $I$  d'un anneau  $A$  est dit **principal** s'il existe  $a \in A$  tel que  $I = (a)$  et qu'un anneau  $A$  est dit **principal** s'il est intègre et si tout idéal de  $A$  est principal.

**Lemme 8.14.** Soit  $A$  un anneau principal et soit  $I_1 \subset I_2 \subset \dots \subset I_n \subset \dots \subset A$  une suite croissante d'idéaux de  $A$ . Alors cette suite stationne, c'est-à-dire qu'il existe  $N \in \mathbb{N}^*$  tel que pour tout  $n \geq N$  on ait  $I_n = I_N$ .

*Démonstration.* Posons  $I = \bigcup_{n \in \mathbb{N}^*} I_n$ . Alors  $I$  est un idéal de  $A$  (exercice), donc comme  $A$  est principal il existe  $a \in A$  tel que  $I = (a)$ . Alors  $a \in \bigcup_{n \in \mathbb{N}^*} I_n$ , donc il existe  $N \in \mathbb{N}^*$  tel que  $a \in I_N$ . Par conséquent,  $(a) \subset I_N \subset I = (a)$ , donc  $I = I_N$ . De plus, pour tout  $n \geq N$ , on a  $I_N \subset I_n \subset I = I_N$  donc  $I_n = I_N$ . ✓

**Proposition 8.15.** Soit  $A$  un anneau principal qui n'est pas un corps. Soit  $a \in A$ . Alors  $a$  est irréductible si et seulement si  $(a)$  est maximal.

En particulier, un anneau principal satisfait la condition de primalité. De plus, les idéaux premiers non nuls d'un anneau principal sont maximaux.

*Démonstration.* On sait déjà que l'on a les implications suivantes pour tout  $a \in A \setminus \{0\}$  :

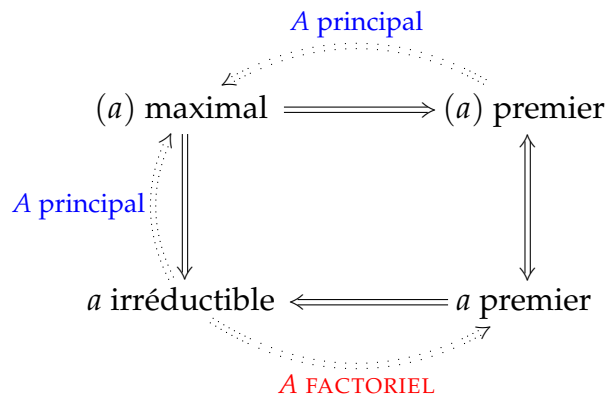
$$(a) \text{ maximal} \implies (a) \text{ premier} \xLeftrightarrow{\text{déf.}} a \text{ premier} \xRightarrow{\text{p. 99}} a \text{ irréductible}$$

Il suffit donc de démontrer que si  $a$  est irréductible alors  $(a)$  est maximal.

Supposons donc  $a$  irréductible. Soit  $I$  un idéal de  $A$  tel que  $(a) \subsetneq I \subset A$ . Puisque  $A$  est principal, il existe  $b \in A$  tel que  $I = (b)$ . Donc  $b \mid a$  et comme  $a$  est irréductible et que  $b$  n'est pas associé à  $a$  (puisque  $(a) \neq (b)$ ),  $b$  est inversible et donc  $I = (b) = A$ . Donc  $(a)$  est maximal.

Le reste est clair. ✓

*Remarque.* Soit  $A$  un anneau intègre et soit  $a \in A$  un élément non nul. On a les implications suivantes :



**Théorème 8.16.** Si  $A$  est principal, alors il est factoriel.

*Démonstration.* Soit  $A$  un anneau principal. On sait déjà que  $A$  est intègre.

Si  $A$  est un corps, il est factoriel (voir p. 101). Supposons donc que  $A$  n'est pas un corps.

D'après la proposition 8.15, la condition de primalité est satisfaite par  $A$ . Pour démontrer que  $A$  est factoriel, il suffit donc d'après le théorème 8.13 de démontrer qu'il satisfait à la condition (E), c'est-à-dire que tout élément non nul et non inversible de  $A$  est un produit d'éléments irréductibles.

Soit  $\mathcal{S}$  l'ensemble des idéaux  $(a)$  engendrés par les éléments  $a$  non nuls, non inversibles et n'admettant pas de factorisation en produit d'éléments irréductibles. Supposons par l'absurde que  $\mathcal{S} \neq \emptyset$ .

Démontrons que  $\mathcal{S}$  admet un élément maximal. Si ce n'est pas le cas, soit  $(a_1) \in \mathcal{S}$ . Alors  $(a_1)$  n'est pas maximal dans  $\mathcal{S}$  donc il existe  $(a_2) \in \mathcal{S}$  tel que  $(a_1) \subsetneq (a_2)$ . De même,  $(a_2)$  n'est pas maximal donc il existe  $(a_3) \in \mathcal{S}$  tel que  $(a_2) \subsetneq (a_3)$ . En procédant ainsi, on construit une suite strictement croissante d'idéaux dans  $A$ , contredisant ainsi le lemme 8.14.

Donc  $\mathcal{S}$  admet un élément maximal, notons-le  $(a_0)$ . En particulier, comme  $(a_0) \in \mathcal{S}$ , l'élément  $a_0$  n'est pas irréductible, donc on peut écrire  $a_0 = bc$  avec  $b$  et  $c$  non nuls et non inversibles. On a alors  $(a_0) \subsetneq (b)$  et  $(a_0) \subsetneq (c)$  donc par maximalité de  $(a_0)$  dans  $\mathcal{S}$ , on a  $(b) \notin \mathcal{S}$  et  $(c) \notin \mathcal{S}$ . Par définition de  $\mathcal{S}$  il existe donc des éléments irréductibles  $p_1, \dots, p_r$  et  $q_1, \dots, q_s$  tels que  $b = p_1 \cdots p_r$  et  $c = q_1 \cdots q_s$ . Mais alors  $a_0 = p_1 \cdots p_r q_1 \cdots q_s$  ce qui contredit le fait que  $(a_0) \in \mathcal{S}$ .

Finalement,  $\mathcal{S} = \emptyset$  et donc la propriété (E) est bien vérifiée. ✓

**Remarque.** On suppose que  $A$  est principal.

(1) Si  $A$  est un corps, son unique idéal premier est  $\{0\}$ .

(2) Si  $A$  n'est pas un corps, ses idéaux premiers sont  $\{0\}$  (qui n'est pas maximal) et les idéaux  $(p)$  où  $p$  est irréductible (et un tel idéal est maximal d'après la proposition 8.15).

Le théorème 8.16 montre que toute famille finie d'éléments non tous nuls (respectivement tous non nuls) d'un anneau principal admet un pgcd (respectivement un ppcm) grâce à la proposition 8.10; on peut les caractériser au moyen d'idéaux.

**Proposition 8.17.** Soit  $A$  un anneau principal et soient  $a_1, \dots, a_r$  ( $r \in \mathbb{N}^*$ ) des éléments de  $A$ . On suppose que les  $a_1, \dots, a_r$  ne sont pas tous nuls. Alors un élément de  $A$  est un pgcd de  $\{a_1, \dots, a_r\}$  si et seulement s'il engendre l'idéal  $a_1A + \dots + a_rA = (a_1, \dots, a_r)$ .

*Démonstration.* Notons  $I = \llbracket 1; r \rrbracket$ .

Soit  $d$  un pgcd de  $\{a_1, \dots, a_r\}$ . Alors pour tout  $i \in I$  on a  $a_i \in (d)$ , donc  $(a_1, \dots, a_r) = (a_1) + \dots + (a_r) \subset (d)$ .

Puisque  $A$  est principal, il existe  $b \in A$  tel que  $(a_1, \dots, a_r) = (b)$ . Pour tout  $i \in I$ , on a  $(a_i) \subset (b)$  donc  $b$  divise  $a_i$  pour tout  $i \in I$  et donc  $b$  divise  $d$  qui est un pgcd des  $a_i$ . Par conséquent,  $(d) \subset (b)$  et finalement  $(a_1, \dots, a_r) = (b) = (d)$ .

Réciproquement, si  $d \in A$  est tel que  $(d) = (a_1, \dots, a_r)$ , alors  $d$  est un diviseur commun des  $a_i$ , et pour tout autre diviseur commun  $b$  des  $a_i$ ,  $i \in I$ , on a  $(d) = (a_1, \dots, a_r) \subset (b)$  donc  $b$  divise  $d$  et donc  $d$  est un pgcd des  $a_i$ ,  $i \in I$ . ✓

**Remarque.** La proposition 8.17 est fausse si on suppose que  $A$  est factoriel et pas principal. Par exemple, dans l'anneau  $\mathbb{Z}[X]$ , qui est factoriel mais pas principal (voir chapitre 9) on a  $(2, X) \neq (1)$  alors que  $\text{pgcd}(2, X) \sim 1$  (exercice).

**Corollaire 8.18** (Propriété de Bézout). Supposons  $A$  principal et soient  $a_1, \dots, a_r$  ( $r \in \mathbb{N}^*$ ) des éléments non tous nuls de  $A$ . Alors, les éléments  $a_1, \dots, a_r$  sont premiers entre eux si et seulement s'il existe  $x_1, \dots, x_r \in A$  tels que  $a_1x_1 + \dots + a_rx_r = 1$ .

*Démonstration.* C'est une conséquence immédiate de la proposition 8.17. ✓

On passe maintenant au cas des anneaux euclidiens. Ce sont des exemples d'anneaux principaux.

**Définition 8.19.** L'anneau  $A$  est dit **euclidien** s'il est intègre et s'il existe une application  $v: A \setminus \{0\} \rightarrow \mathbb{N}$  vérifiant : pour tout couple  $(a, b)$  d'éléments de  $A$  tel que  $b \neq 0$ , il existe un couple  $(q, r)$  d'éléments de  $A$  tel que  $a = bq + r$  et ou bien  $r = 0$ , ou bien  $v(r) < v(b)$ .

L'application  $v$  s'appelle un **stathme euclidien**.

**Remarque.** Dans la littérature, un tel  $v$  s'appelle parfois un *pré-stathme euclidien*, et il faut ajouter la condition que pour tout  $(a, b) \in A^2$  avec  $ab \neq 0$ , on a  $v(a) \leq v(ab)$  pour avoir un *stathme euclidien*. Mais on peut démontrer que si un pré-stathme existe, il existe aussi un stathme, donc les deux définitions d'anneau euclidien sont équivalentes.

**Théorème 8.20.** Si  $A$  est euclidien, il est principal.

*Démonstration.* cf. cours de L3.

Soit  $A$  un anneau euclidien. Il est intègre.

Soit  $I$  un idéal de  $A$ . Si  $I = \{0\} = (0)$ , il est principal. Sinon, l'ensemble  $I \setminus \{0\}$  n'est pas vide et par suite l'ensemble  $\{\nu(a) \mid a \in I \setminus \{0\}\}$  est une partie non vide de  $\mathbb{N}$  qui admet donc un plus petit élément  $m$ . Soit alors  $a \in I \setminus \{0\}$  tel que  $\nu(a) = m$ . Pour tout  $b \in I$ , il existe  $(q, r) \in A^2$  tel que  $b = aq + r$  avec  $r = 0$  ou  $\nu(r) < \nu(a)$ . Si l'on suppose que  $r \neq 0$ , alors  $r = b - aq$  est un élément non nul de  $I$  tel que  $\nu(r) < \nu(a)$ . Ceci contredit la définition de  $a$  et, par suite, on doit avoir  $r = 0$  et donc  $b = aq \in (a)$  donc  $I \subset (a)$ . Puisque  $a \in I$ , on a  $(a) \subset I$  et on a donc démontré que  $I = (a)$ . Tous les idéaux de  $A$  sont principaux.

Donc  $A$  est un anneau principal. ✓

**Exemples.** L'anneau  $\mathbb{Z}$  est euclidien (considérer l'application  $\nu: \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$  définie par  $\nu(n) = |n|$ ).

Si  $K$  est un corps, l'anneau  $K[X]$  est euclidien (considérer l'application  $\nu: K[X] \setminus \{0\} \rightarrow \mathbb{N}$  définie par  $\nu(P) = \deg P$ ).

**Corollaire 8.21.** Soit  $A$  un anneau commutatif unitaire quelconque (ie. qui n'est pas nécessairement intègre). On a les équivalences :

$$A[X] \text{ est principal} \iff A \text{ est un corps} \iff A[X] \text{ est euclidien.}$$

*Démonstration.* D'après le théorème 8.20 et l'exemple ci-dessus, si  $A$  est un corps, alors  $A[X]$  est principal.

Réciproquement, supposons que  $A[X]$  est principal. Alors  $A$  est intègre car c'est un sous-anneau de  $A[X]$  qui est principal donc intègre.

L'application  $\varphi: A[X] \rightarrow A$  définie par  $\varphi(P) = P(0)$  est un morphisme d'anneaux surjectif et de noyau  $(X)$ , donc d'après le premier théorème d'isomorphisme on a  $A[X]/(X) \cong A$ . Or  $A$  est intègre, donc  $A[X]/(X)$  est intègre, donc  $(X)$  est un idéal premier et non nul, donc maximal puisque  $A[X]$  est principal, et donc  $A \cong A[X]/(X)$  est un corps. ✓

Enfin, bien que  $A[X]$  ne soit pas euclidien en général, on peut faire certaines divisions euclidiennes dans  $A[X]$ .

**Proposition 8.22** (Un résultat utile : division euclidienne dans les anneaux de polynômes.). Soit  $A$  un anneau, soit  $F \in A[X]$  et soit  $G \in A[X]$  un polynôme non nul. On suppose que le coefficient dominant de  $G$  est inversible dans  $A$ . Alors il existe un unique couple  $(Q, R) \in A[X] \times A[X]$  tel que  $F = GQ + R$  et  $\deg R < \deg G$  (convention :  $\deg 0 = -\infty$ ).

*Démonstration.* Voir travaux dirigés Existence :

➤ Si  $\deg F < \deg G$ , il suffit de prendre  $Q = 0$  et  $R = F$ .

➤ Si  $m = \deg F \geq \deg G = n$ , raisonnons par récurrence sur  $m \geq n$ .

◆ Initialisation. Si  $m = n$ , notons  $F(X) = aX^m + H(X)$  et soit  $u$  le coefficient dominant de  $G$ . Posons  $a = ub$  avec  $b \in A$ . Il suffit alors de prendre  $Q = b$  et  $R = F - QG$  est de degré  $< m$ .

◆ Soit  $m > n$  tel que le résultat soit vrai en degré  $\leq m - 1$ . Notons  $m = \deg F$ ,  $n = \deg G$ ,  $u$  le coefficient dominant de  $G$  et  $a$  le coefficient dominant de  $F$ .

Le degré du polynôme  $F - u^{-1}aX^{m-n}G$  est  $\leq m - 1$ , donc par hypothèse de récurrence il existe  $Q_1$  et  $R_1$  tels que  $F - u^{-1}aX^{m-n}G = Q_1G + R_1$  et  $\deg R_1 < \deg G$ . On a donc  $F = (u^{-1}aX^{m-n} + Q_1)G + R_1$ , d'où l'existence.

Pour l'unicité : Supposons que  $F = QG + R = Q'G + R'$  avec  $\deg R < \deg G$  et  $\deg R' < \deg G$ . Alors  $G(Q - Q') = R' - R$ . Puisque  $u$  est inversible, on a  $\deg(R' - R) = \deg(Q - Q') + \deg G \geq \deg G$ , ce qui est impossible si  $Q - Q' \neq 0$  et  $R' - R \neq 0$ . Donc  $(Q', R') = (Q, R)$ . ✓



# Anneaux de polynômes

Dans tout ce chapitre,  $A$  désigne un anneau (commutatif unitaire).

## I. ANNEAUX DE POLYNÔMES EN PLUSIEURS INDÉTERMINÉES

Vous avez défini en L3 l'anneau de polynômes  $A[X]$  en une indéterminée. Pour mémoire, il s'agit de l'ensemble des suites  $(a_n)_{n \in \mathbb{N}}$  finies d'éléments de  $A$ , muni de l'addition composante à composante et du produit défini par  $(a_n) \cdot (b_n) = (c_n)$  avec  $c_n = \sum_{k=0}^n a_k b_{n-k}$ . On note  $(a_n)_{n \in \mathbb{N}} = \sum_{k=0}^d a_k X^k$  où  $d \geq \max\{k \mid a_k \neq 0\}$  et  $\max\{k \mid a_k \neq 0\} = \deg\left(\sum_{k=0}^d a_k X^k\right)$  est le degré du polynôme  $\sum_{k=0}^d a_k X^k$  (par convention,  $\deg(0) = -\infty$ ).

On définit alors récursivement les anneaux de polynômes en plusieurs indéterminées.

**Définition 9.1.** Soit  $n \in \mathbb{N}$  un nombre entier avec  $n > 1$ . L'anneau de polynômes en  $n$  indéterminées  $X_1, \dots, X_n$ , noté  $A[X_1, \dots, X_n]$ , est défini récursivement par

$$A[X_1, \dots, X_n] := A[X_1, \dots, X_{n-1}][X_n].$$

**Remarque.** On a une inclusion naturelle  $A \rightarrow A[X]$  qui à un élément  $a \in A$  associe le polynôme  $a$ . C'est un morphisme d'anneaux. Il découle de la définition qu'il existe des morphismes injectifs d'anneaux naturels

- $A \hookrightarrow A[X_1, \dots, X_n]$  et
- $A[X_1, \dots, X_p] \hookrightarrow A[X_1, \dots, X_n]$  pour tout  $p \leq n$  tel que  $X_i$  a pour image  $X_i$  pour tout  $i \in \llbracket 1; p \rrbracket$ .

**Proposition 9.2.** Tout élément de  $A[X_1, \dots, X_n]$  s'écrit, de façon unique, sous la forme

$$\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n},$$

où  $a_{(i_1, \dots, i_n)} \in A$ , pour tout  $(i_1, \dots, i_n) \in \mathbb{N}^n$  (somme finie).

**Démonstration.** On raisonne par récurrence sur  $n$ .

- Initialisation. C'est vrai pour  $n = 1$  (L3 – écriture unique d'une suite  $(a_n)_{n \in \mathbb{N}}$  dont toutes les composantes sont nulles sauf un nombre fini d'entre elles sous la forme d'une somme finie  $\sum_{k \in \mathbb{N}} a_k X^k$ ).
- Hérédité. Soit  $n \geq 1$  tel que le résultat soit vrai pour l'anneau de polynômes en  $n$  indéterminées. Soit  $P \in A[X_1, \dots, X_n, X_{n+1}]$ ,  $P \neq 0$ . Posons  $B = A[X_1, \dots, X_n]$ . Alors, puisque  $A[X_1, \dots, X_n, X_{n+1}] = B[X_{n+1}]$ , le résultat au rang 1 nous permet d'écrire  $P = \sum_{i=0}^d Q_i X_{n+1}^i$  avec  $d \in \mathbb{N}$  et  $Q_i \in B$ ,  $Q_d \neq 0$ . Par hypothèse de récurrence, on a, pour tout  $j$ ,  $Q_j = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)}^{(j)} \cdot X_1^{i_1} \dots X_n^{i_n}$  avec où  $a_{(i_1, \dots, i_n)}^{(j)} \in A$  (somme finie). On en déduit

que

$$P = \sum_{j=0}^d \sum_{(i_1, \dots, i_n)} a_{(i_1, \dots, i_n)}^{(j)} \cdot X_1^{i_1} \dots X_n^{i_n} X_{n+1}^j = \sum_{(i_1, \dots, i_n, i_{n+1})} b_{(i_1, \dots, i_n, i_{n+1})} \cdot X_1^{i_1} \dots X_n^{i_n} X_{n+1}^{i_{n+1}}$$

où  $b_{(i_1, \dots, i_n, i_{n+1})} = a_{(i_1, \dots, i_n)}^{(j)}$ . On a démontré l'existence. Démontrons maintenant l'unicité.

Il suffit pour cela de démontrer que si  $P = \sum_{(i_1, \dots, i_n, i_{n+1})} a_{(i_1, \dots, i_n, i_{n+1})} \cdot X_1^{i_1} \dots X_n^{i_n} X_{n+1}^{i_{n+1}}$  est le polynôme nul, alors tous les coefficients  $a_{(i_1, \dots, i_n, i_{n+1})}$  sont nuls.

On peut écrire  $0 = \sum_{i_{n+1} \in \mathbb{N}} \left( \sum_{(i_1, \dots, i_n)} a_{(i_1, \dots, i_n, i_{n+1})} \cdot X_1^{i_1} \dots X_n^{i_n} \right) X_{n+1}^{i_{n+1}} = \sum_{i_{n+1} \in \mathbb{N}} Q_{i_{n+1}} X_{n+1}^{i_{n+1}}$  avec  $Q_{i_{n+1}} \in B$ . Le résultat au rang 1 donne  $Q_j = 0$  pour tout  $j$ . L'hypothèse de récurrence implique que tous les coefficients de tous les  $Q_j$  sont nuls, c'est-à-dire que tous les coefficients de  $P$  sont nuls. ✓

**Définition 9.3.** ➤ Un élément de  $A[X_1, \dots, X_n]$  de la forme  $X_1^{i_1} \dots X_n^{i_n}$ , avec  $(i_1, \dots, i_n) \in \mathbb{N}^n$  s'appelle un **monôme** de  $A[X_1, \dots, X_n]$  (en  $X_1, \dots, X_n$ ).

➤ Soit  $P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n}$ . Alors  $a_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n}$  est le **terme monomial** correspondant au monôme  $X_1^{i_1} \dots X_n^{i_n}$ .

La proposition ci-dessus dit que tout polynôme de  $A[X_1, \dots, X_n]$  s'écrit de manière unique comme somme finie de termes monomiaux.

➤ Le **degré**, ou **degré total**, du monôme  $X_1^{i_1} \dots X_n^{i_n}$  ou du terme monomial  $a_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n}$  (avec  $a_{(i_1, \dots, i_n)} \neq 0$ ) est  $\sum_{k=1}^n i_k$ .

Le **degré**, ou **degré total**, du polynôme  $P$  est le maximum des degrés des termes monomiaux non nuls qui constituent  $P$  :

$$\deg P := \max \left\{ \sum_{k=1}^n i_k \mid a_{(i_1, \dots, i_n)} \neq 0 \right\}.$$

**Proposition 9.4.** Soit  $A$  un anneau intègre et  $n \in \mathbb{N}^*$ . L'anneau de polynômes  $A[X_1, \dots, X_n]$  en  $n$  indéterminées est intègre.

*Démonstration.* On procède par récurrence sur  $n$ .

➤ Le résultat est connu si  $n = 1$ . Pour mémoire, si  $P = \sum_{i=0}^d a_i X^i$  et  $Q = \sum_{j=0}^t b_j X^j$  ne sont pas nuls, avec  $a_d \neq 0$  et  $b_t \neq 0$ , alors  $PQ = a_d b_t X^{d+t} + R$  avec  $\deg R < d + t$ . Puisque  $A$  est intègre,  $a_d b_t \neq 0$  et donc  $PQ \neq 0$ .

➤ Hérédité. Soit  $n \geq 1$  tel que  $B = A[X_1, \dots, X_n]$  soit intègre. Alors  $A[X_1, \dots, X_{n+1}] = B[X_{n+1}]$  est intègre d'après le résultat au rang 1. ✓

**Théorème 9.5** (Propriété universelle des anneaux de polynômes). Soient  $B$  un anneau,  $f: A \rightarrow B$  un morphisme d'anneaux et  $b_1, \dots, b_n \in B$ . On note  $\sigma: A \rightarrow A[X_1, \dots, X_n]$  l'inclusion naturelle.

Alors il existe un morphisme d'anneaux  $g: A[X_1, \dots, X_n] \rightarrow B$  et un seul tel que, pour  $1 \leq j \leq n$ ,  $g(X_j) = b_j$  et tel que  $g \circ \sigma = f$ , c'est-à-dire que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & A[X_1, \dots, X_n] \\ & \searrow f & \downarrow g \\ & & B \end{array}$$

**Remarque.** La condition  $g \circ \sigma = f$  s'écrit  $g|_A = f$  lorsqu'on identifie  $A$  et  $\sigma(A)$ . Autrement dit,  $g$  est un prolongement de  $f$  à  $A[X_1, \dots, X_n]$ .

*Démonstration.* Si  $g$  existe, on doit avoir

$$\begin{aligned} g\left(\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n}\right) &= \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} g\left(a_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n}\right) \\ &= \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} f(a_{(i_1, \dots, i_n)}) \cdot g(X_1)^{i_1} \dots g(X_n)^{i_n} \\ &= \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} f(a_{(i_1, \dots, i_n)}) b_1^{i_1} \dots b_n^{i_n} \end{aligned}$$

donc  $g$  est nécessairement unique.

Vérifions que l'application  $g: A[X_1, \dots, X_n] \rightarrow B$  définie par

$$g\left(\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n}\right) = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} f(a_{(i_1, \dots, i_n)}) b_1^{i_1} \dots b_n^{i_n}$$

vérifie les propriétés requises. En effet :

- Il est clair que  $g(\sigma(a)) = g(a) = f(a)$  pour tout  $a \in A$  (prendre  $(i_1, \dots, i_n) = (0, \dots, 0)$ ).
- Il est clair que  $g(X_k) = b_k$  pour tout  $k \in \llbracket 1; n \rrbracket$  (prendre  $(i_1, \dots, i_n) = (0, \dots, 0, 1, 0, \dots, 0)$  avec le 1 en  $k^{\text{ième}}$  position).
- Il reste à vérifier que  $g$  est bien un morphisme d'anneaux.

◆  $g(1) = f(1) = 1$ .

◆ Posons  $P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n}$  et  $Q = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a'_{(i_1, \dots, i_n)} \cdot X_1^{i_1} \dots X_n^{i_n}$ . Alors

$$\begin{aligned} g(P + Q) &= g\left(\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} (a_{(i_1, \dots, i_n)} + a'_{(i_1, \dots, i_n)}) \cdot X_1^{i_1} \dots X_n^{i_n}\right) \\ &= \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} f(a_{(i_1, \dots, i_n)} + a'_{(i_1, \dots, i_n)}) \cdot b_1^{i_1} \dots b_n^{i_n} \\ &= \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} (f(a_{(i_1, \dots, i_n)}) + f(a'_{(i_1, \dots, i_n)})) \cdot b_1^{i_1} \dots b_n^{i_n} \\ &= \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} f(a_{(i_1, \dots, i_n)}) \cdot b_1^{i_1} \dots b_n^{i_n} + \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} f(a'_{(i_1, \dots, i_n)}) \cdot b_1^{i_1} \dots b_n^{i_n} \\ &= g(P) + g(Q). \end{aligned}$$

◆ ✧ Soient  $P = a \cdot X_1^{i_1} \dots X_n^{i_n}$  et  $Q = a' \cdot X_1^{j_1} \dots X_n^{j_n}$  des termes monomiaux. Alors

$$\begin{aligned} g(PQ) &= g(aa' \cdot X_1^{i_1+j_1} \dots X_n^{i_n+j_n}) = f(aa') \cdot b_1^{i_1+j_1} \dots b_n^{i_n+j_n} \\ &= f(a) \cdot b_1^{i_1} \dots b_n^{i_n} \cdot f(a') \cdot b_1^{j_1} \dots b_n^{j_n} = g(P)g(Q). \end{aligned}$$

✧ Soient  $P$  et  $Q$  quelconques dans  $A[X_1, \dots, X_n]$ . Alors  $P = \sum_{k=1}^p T_k$  et  $Q = \sum_{\ell=1}^q S_\ell$  où les  $T_k$  et les  $S_\ell$  sont des termes monomiaux. En utilisant ce que nous avons déjà démontré, on a

$$\begin{aligned} g(PQ) &= g\left(\sum_{k=1}^p \sum_{\ell=1}^q T_k S_\ell\right) = \sum_{k=1}^p \sum_{\ell=1}^q g(T_k S_\ell) = \sum_{k=1}^p \sum_{\ell=1}^q g(T_k) g(S_\ell) \\ &= \left(\sum_{k=1}^p g(T_k)\right) \left(\sum_{\ell=1}^q g(S_\ell)\right) = g\left(\sum_{k=1}^p T_k\right) g\left(\sum_{\ell=1}^q S_\ell\right) = g(P)g(Q). \quad \checkmark \end{aligned}$$

**Exemple.** Soit  $A$  un anneau et soit  $I$  un idéal de  $A$ . Le morphisme d'anneaux  $f: A \rightarrow (A/I)[X]$  obtenu par composition de la projection canonique  $\pi: A \rightarrow A/I$  et de l'inclusion  $A/I \rightarrow (A/I)[X]$  induit donc grâce au théorème 9.5 un morphisme d'anneaux  $\varphi_I: A[X] \rightarrow (A/I)[X]$  qui prolonge  $f$  et tel que  $\varphi_I(X) = X$  (c'est-à-dire que  $\varphi_I(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n \pi(a_i) X^i$ ). Il est clair que  $\varphi_I$  est surjectif.

De même, si  $f: A \rightarrow (A/I)[X_1, \dots, X_n]$  est la composée de la projection canonique  $\pi: A \rightarrow A/I$  et de l'inclusion  $A/I \rightarrow (A/I)[X_1, \dots, X_n]$ , il existe un morphisme d'anneaux surjectif  $\varphi_I: A[X_1, \dots, X_n] \rightarrow (A/I)[X_1, \dots, X_n]$  qui prolonge  $f$  et tel que  $\varphi_I(X_i) = X_i$  pour tout  $i$  (c'est-à-dire que  $\varphi_I(\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)} X_1^{i_1} \cdots X_n^{i_n}) = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} \pi(a_{(i_1, \dots, i_n)}) X_1^{i_1} \cdots X_n^{i_n}$ ).

**Cas particulier.** Soit  $p \in \mathbb{N}$  un nombre premier et soit  $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$  la projection canonique. On pose  $\pi(n) = \bar{n}$ . Le morphisme  $\varphi_{(p)}: \mathbb{Z}[X] \rightarrow (\mathbb{Z}/p\mathbb{Z})[X]$  consiste à réduire les coefficients des polynôme modulo  $p$  :  $\varphi_{(p)}(\sum_{k=0}^n a_k X^k) = \sum_{k=0}^n \bar{a}_k X^k$ . On appelle  $\varphi_{(p)}$  le **morphisme de réduction modulo  $p$** .

**Corollaire 9.6.** Soit  $\sigma \in S_n$ . On a un isomorphisme d'anneaux  $A[X_1, \dots, X_n] \cong A[X_{\sigma(1)}, \dots, X_{\sigma(n)}]$ .

En particulier, on en déduit que pour tout  $i \in \llbracket 1; n \rrbracket$ , on peut identifier les anneaux  $A[X_1, \dots, X_n]$  et  $A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X_i]$ .

*Démonstration.* On applique la propriété universelle des anneaux de polynômes avec  $B = A[X_{\sigma(1)}, \dots, X_{\sigma(n)}]$ ,  $f: A \rightarrow B$  l'inclusion et  $b_i = X_{\sigma(i)}$  pour obtenir un morphisme d'anneaux  $\varphi: A[X_1, \dots, X_n] \rightarrow A[X_{\sigma(1)}, \dots, X_{\sigma(n)}]$  qui fixe les éléments de  $A$  et envoie chaque  $X_i$  sur  $X_{\sigma(i)}$ .

On applique à nouveau la propriété universelle des anneaux de polynômes avec  $B = A[X_1, \dots, X_n]$  et  $b_i = X_i$  (avec au départ l'anneau  $A[X_{\sigma(1)}, \dots, X_{\sigma(n)}]$ ) pour obtenir un morphisme d'anneaux  $\psi: A[X_{\sigma(1)}, \dots, X_{\sigma(n)}] \rightarrow A[X_1, \dots, X_n]$  qui fixe les éléments de  $A$  et envoie chaque  $X_{\sigma(i)}$  sur  $X_i$ .

Alors  $\psi \circ \varphi$  est un endomorphisme d'anneaux de  $A[X_1, \dots, X_n]$  qui fixe les éléments de  $A$  et les  $X_i$ ; or  $\text{id}_{A[X_1, \dots, X_n]}$  est également un tel endomorphisme, donc par unicité on a  $\psi \circ \varphi = \text{id}_{A[X_1, \dots, X_n]}$ .

De même,  $\varphi \circ \psi = \text{id}_{A[X_{\sigma(1)}, \dots, X_{\sigma(n)}]}$  donc  $\varphi$  et  $\psi$  sont des isomorphismes réciproques. ✓

**Définition 9.7.** ➤ Le **degré partiel** du monôme  $X_1^{i_1} \cdots X_n^{i_n}$  (ou du terme monomial  $a_{(i_1, \dots, i_n)} X_1^{i_1} \cdots X_n^{i_n}$  avec  $a_{(i_1, \dots, i_n)} \neq 0$ ) en l'indéterminée  $X_k$  est  $i_k$ . Il s'agit du degré de ce monôme vu dans l'anneau  $A[X_1, \dots, X_{k-1}, X_{k+1}, \dots, X_n][X_k]$ , c'est-à-dire un polynôme en l'indéterminée  $X_k$  et à coefficients dans  $A[X_1, \dots, X_{k-1}, X_{k+1}, \dots, X_n]$ .

➤ Le **degré partiel** du polynôme  $P$  en l'indéterminée  $X_k$  est le maximum des degrés partiels en  $X_k$  des termes monomiaux non nuls qui constituent  $P$  :

$$\deg_{X_k} P := \max \{ i_k \mid a_{(i_1, \dots, i_n)} \neq 0 \}.$$

C'est le degré de  $P$  vu comme polynôme dans  $A[X_1, \dots, X_{k-1}, X_{k+1}, \dots, X_n][X_k]$ .

**Exemples.** Le degré partiel en  $X_2$  du polynôme  $2X_1^2 X_2 X_3^3 - 4X_2^2 X_3 \in \mathbb{Z}[X_1, X_2, X_3]$  est 2 et le degré partiel en  $Y$  du polynôme  $X^2 Z^3 + X^3 Z - 3XZ \in \mathbb{R}[X, Y, Z]$  est 0.

## II. FONCTIONS POLYNOMIALES.

Dans toute cette section,  $A$  est un anneau (commutatif unitaire).

Si  $n \in \mathbb{N}^*$ , on note  $\mathcal{F}(A^n, A)$  l'ensemble des applications de  $A^n$  dans  $A$ . Il est bien connu que  $\mathcal{F}(A^n, A)$  est un anneau commutatif, pour les opérations suivantes : si  $f$  et  $g$  sont dans  $\mathcal{F}(A^n, A)$ ,

$$\begin{aligned}(f + g)(x) &= f(x) + g(x) \quad \text{pour tout } x \in A^n \\ (fg)(x) &= f(x)g(x) \quad \text{pour tout } x \in A^n.\end{aligned}$$

L'élément neutre est l'application constante égale à 0, l'élément unité est l'application constante égale à 1.

**Définition 9.8.** Soit  $P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)} X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$ , où  $a_{(i_1, \dots, i_n)} \in A$  pour tout  $(i_1, \dots, i_n) \in \mathbb{N}^n$ . On associe à  $P$  l'application  $\tilde{P} \in \mathcal{F}(A^n, A)$  définie par

$$\begin{aligned}\tilde{P} : \quad A^n &\longrightarrow A \\ (\alpha_1, \dots, \alpha_n) &\mapsto \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{(i_1, \dots, i_n)} \alpha_1^{i_1} \dots \alpha_n^{i_n}.\end{aligned}$$

Cette application s'appelle la **fonction polynomiale** associée à  $P$ . Par abus de notation, pour  $(\alpha_1, \dots, \alpha_n) \in A^n$ , on écrira souvent  $P(\alpha_1, \dots, \alpha_n)$  au lieu de  $\tilde{P}(\alpha_1, \dots, \alpha_n)$ .

**Proposition 9.9.** Soit  $n \in \mathbb{N}^*$ . L'application  $A[X_1, \dots, X_n] \longrightarrow \mathcal{F}(A^n, A)$ ,  $P \mapsto \tilde{P}$  est un morphisme d'anneaux. Son image est notée  $\mathcal{F}_{\text{pol}}(A^n, A)$  et elle est appelée l'**anneau des fonctions polynomiales** sur  $A^n$ .

*Démonstration.* C'est une simple vérification.

On peut également, pour éviter des calculs techniques, utiliser la propriété universelle des anneaux de polynômes (théorème 9.5). Pour tout  $i \in \llbracket 1; n \rrbracket$ , soit  $\pi_i \in \mathcal{F}(A^n, A)$  l'application définie par  $\pi_i(\alpha_1, \dots, \alpha_n) = \alpha_i$  (la projection sur la  $i^{\text{me}}$  composante). Soit  $f: A \rightarrow \mathcal{F}(A^n, A)$  l'application qui à  $x \in A$  associe l'application constante égale à  $x$ ; c'est un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux  $A[X_1, \dots, X_n] \rightarrow \mathcal{F}(A^n, A)$  qui prolonge  $f$  et qui associe  $\pi_i$  à  $X_i$ . On constate qu'il s'agit bien de l'application  $P \mapsto \tilde{P}$ . ✓

Soit  $n \in \mathbb{N}^*$ . La proposition 9.9 montre que l'on dispose d'un morphisme d'anneaux surjectif

$$\begin{array}{ccc} \varphi_n : & A[X_1, \dots, X_n] & \longrightarrow \mathcal{F}_{\text{pol}}(A^n, A) \\ & P & \longmapsto \tilde{P} \end{array}.$$

**Remarque.** Soit  $A$  un anneau intègre. On sait que  $\varphi_1: A[X] \rightarrow \mathcal{F}_{\text{pol}}(A, A)$  est injectif si, et seulement si,  $A$  est infini.

En effet, si  $A$  est fini, posons  $A = \{t_1, \dots, t_s\}$ . Alors le polynôme  $P = \prod_{i=1}^s (X - t_i)$  n'est pas nul (il est de degré  $s$ ) mais la fonction polynomiale  $\tilde{P}: A \rightarrow A$  est nulle.

D'autre part, si  $A$  est infini, puisqu'il est intègre tout polynôme non nul de  $A[X]$  a un nombre fini de racines (voir par exemple page 117), donc la fonction polynomiale associée ne peut pas être nulle.

Ce résultat est encore vrai pour les polynômes en plusieurs indéterminées.

**Théorème 9.10.** Soit  $A$  un anneau intègre et soit  $n \in \mathbb{N}^*$ . Le morphisme  $\varphi_n$  d'anneaux est un isomorphisme si, et seulement si,  $A$  est infini.

*Démonstration.* ➤ Supposons que  $A$  est infini. Il suffit de démontrer que, pour tout  $n \in \mathbb{N}^*$ ,  $\varphi_n$  est injectif (puisque'il est surjectif par construction). On raisonne par récurrence sur  $n$ .

♦ Le cas  $n = 1$  est connu.

♦ Soit  $s \in \mathbb{N}^*$  tel que  $\varphi_n$  est injectif pour tout  $n \leq s$ . Soit  $P \in A[X_1, \dots, X_{s+1}]$  un polynôme non nul ; il existe une famille finie  $\{P_i\}_{i \in \mathbb{N}}$  d'éléments de  $A[X_1, \dots, X_s]$  telle que  $P = \sum_{i \in \mathbb{N}} P_i X_{s+1}^i$ . Comme  $P$  n'est pas nul, il existe  $i_0 \in \mathbb{N}$  tel que  $P_{i_0} \neq 0$ . Par hypothèse de récurrence, on en déduit l'existence de  $(a_1, \dots, a_s) \in A^s$  tel que  $\varphi_s(\tilde{P}_{i_0})(a_1, \dots, a_s) = \tilde{P}_{i_0}(a_1, \dots, a_s) \neq 0$ . Soit enfin  $\psi: A[X_1, \dots, X_{s+1}] \rightarrow A[X_{s+1}]$  le morphisme d'anneaux tel que  $\psi|_A = \text{id}_A$ ,  $\psi(X_i) = a_i$  pour  $1 \leq i \leq s$  et  $\psi(X_{s+1}) = X_{s+1}$ . Alors le polynôme  $\psi(P) = \sum_{i \in \mathbb{N}} \tilde{P}_i(a_1, \dots, a_s) X_{s+1}^i$  de  $A[X_{s+1}]$  n'est pas nul puisque  $\tilde{P}_{i_0}(a_1, \dots, a_s) \neq 0$ . Il existe donc  $a \in A$  tel que  $\varphi_1(\psi(P)) = \widetilde{\psi(P)}(a) \neq 0$ . On en déduit aussitôt que  $\varphi_{s+1}(P) = \tilde{P}$  ne s'annule pas en  $(a_1, \dots, a_s, a)$ , donc la fonction polynomiale  $\varphi_{s+1}(P)$  associée à  $P$  n'est pas nulle.

➤ Supposons que  $A$  est fini. On sait qu'il existe un polynôme non nul  $P \in A[X_1]$  dont la fonction polynomiale associée  $\tilde{P}: A \rightarrow A$  est nulle. Posons  $P = \sum_{i=0}^d a_i X_1^i$ .

On dispose d'un morphisme d'anneaux injectif  $\sigma: A[X_1] \rightarrow A[X_1, \dots, X_n]$  qui envoie  $X_1$  sur  $X_1$  et fixe les éléments de  $A$ . Il est clair que  $\sigma(P) \neq 0$ . Mais on a

$$\varphi_n(\sigma(P))(\alpha_1, \dots, \alpha_n) = \widetilde{\sigma(P)}(\alpha_1, \dots, \alpha_n) = \sum_{i=0}^d a_i \alpha_1^i = \tilde{P}(\alpha_1) = 0$$

donc la fonction polynomiale associée au polynôme non nul  $\sigma(P)$  est nulle. Ainsi,  $\varphi_n$  n'est pas injective. ✓

### III. ARITHMÉTIQUE DANS LES ANNEAUX DE POLYNÔMES

#### A. Théorèmes de transfert.

On a vu dans le corollaire 9.4 que la propriété d'être intègre se transfère de l'anneau  $A$  à l'anneau  $A[X_1, \dots, X_n]$ . On peut remarquer que, comme l'indique le corollaire 8.21, la propriété d'un anneau d'être principal ne se transfère pas de l'anneau  $A$  à l'anneau  $A[X]$ . Il résulte aussi du corollaire 8.21 que la propriété d'un anneau d'être euclidien ne se transfère pas de l'anneau  $A$  à l'anneau  $A[X]$ .

Dans cette section, on étudie le transfert de la propriété d'être factoriel de l'anneau  $A$  à l'anneau  $A[X_1, \dots, X_n]$ . Pour ce faire, il faut introduire la notion de contenu d'un polynôme.

**Définition 9.11.** On suppose que  $A$  est un anneau factoriel.

(1) Si  $P \in A[X] \setminus \{0\}$ , un élément de  $A$  est appelé un **contenu** de  $P$  si c'est un pgcd des coefficients de  $P$ .

(2) Un polynôme  $P \in A[X] \setminus \{0\}$  est dit **primitif** si 1 est un pgcd de ses coefficients.

On notera  $c \sim c(P)$  si  $c$  est un contenu de  $P$ .

**Remarque.** Le fait que  $A$  soit un anneau factoriel assure l'existence de pgcd dans  $A$  et donc la notion de contenu a bien un sens pour les polynômes à coefficients dans  $A$ .

**Exemple.** Les polynômes  $2X^2 + 3X + 4$  et  $X^3 + X + 1$  de  $\mathbb{Z}[X]$  sont primitifs, le polynôme  $2X^2 + 6X + 4$  admet 2 comme contenu. Notons que  $2X^2 + 6X + 4 = 2 \cdot (X^2 + 3X + 2)$  avec  $X^2 + 3X + 2$  primitif.

**Lemme 9.12.** Soit  $A$  un anneau factoriel. Soit  $P \in A[X] \setminus \{0\}$ . Alors  $p \in A$  est un contenu de  $P$  si et seulement s'il existe  $P_1 \in A[X]$  primitif tel que  $P = pP_1$ .

*Démonstration.* ( $\Rightarrow$ ) Notons  $P = \sum_{i=0}^n a_i X^i$ . Soit  $p$  un contenu de  $P$ . Alors pour tout  $i$  il existe  $a'_i \in A$  tel que  $a_i = pa'_i$  et 1 est un pgcd des  $a'_i$  d'après le lemme 8.11. On a alors  $P = pP_1$  avec  $P_1 = \sum_{i=0}^n a'_i X^i \in A[X]$  primitif.

( $\Leftarrow$ ) Supposons que  $P = pP_1$  avec  $P_1$  primitif. Posons  $P_1 = \sum_{i=0}^n a_i X^i$ . Alors  $P = \sum_{i=0}^n pa_i X^i$  et  $p = p \cdot 1$  est un pgcd des coefficients  $pa_i$  d'après le lemme 8.11 et donc  $p$  est un contenu de  $P$ .  $\checkmark$

**Lemme 9.13** (Lemme de Gauss). On suppose  $A$  factoriel. Soient  $P$  et  $Q$  des polynômes non nuls de  $A[X]$ .

(1) Si  $P$  et  $Q$  sont primitifs, alors  $PQ$  est primitif.

(2) Si  $p$  et  $q$  sont des contenus de  $P$  et  $Q$  respectivement, alors  $pq$  est un contenu de  $PQ$ .

*Démonstration.* (1) On raisonne par l'absurde. Supposons que 1 ne soit pas un contenu de  $PQ$ . Alors, puisque  $A$  est factoriel, il existe un contenu de  $PQ$  et un diviseur irréductible  $\pi \in A$  de ce contenu; il divise donc tous les coefficients de  $PQ$ . Soient  $d, e$  les degrés respectifs de  $P$  et  $Q$ ; comme  $P$  et  $Q$  sont primitifs, il existe au moins un coefficient de  $P$  et un coefficient de  $Q$  qui ne sont pas divisibles par  $\pi$ . Posons  $P = \sum_{i=0}^d a_i X^i$ ,  $Q = \sum_{j=0}^e b_j X^j$ ,  $i_0 = \min\{i \in \llbracket 0; d \rrbracket \mid \pi \nmid a_i\}$  et  $j_0 = \min\{j \in \llbracket 0; e \rrbracket \mid \pi \nmid b_j\}$ . Le coefficient d'indice  $i_0 + j_0$  de  $PQ$  est

$$\sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i < i_0 \text{ ou } j < j_0}} a_i b_j.$$

Mais alors, par définition de  $\pi$ ,  $\pi$  divise le membre de gauche et le second terme du membre de droite dans l'équation ci-dessus, donc  $\pi \mid a_{i_0} b_{j_0}$ . Comme  $A$  est factoriel et  $\pi$  est irréductible, il s'ensuit (condition d'Euclide) que  $\pi$  divise  $a_{i_0}$  ou  $b_{j_0}$ , ce qui constitue une contradiction. Ainsi 1 est un contenu de  $PQ$ , qui est donc primitif.

(2) On utilise le lemme 9.12. Il existe des polynômes primitifs  $P_1, Q_1$  dans  $A[X]$  tels que  $P = pP_1$  et  $Q = qQ_1$ . Alors  $PQ = pqP_1Q_1$  avec  $P_1Q_1$  primitif d'après (1), donc  $pq$  est un contenu de  $PQ$  d'après le lemme 9.12.  $\checkmark$

**Remarque.** Soit  $A$  un anneau factoriel. Alors  $A$  est intègre, donc son corps des fractions  $K$  existe et  $A$  peut être identifié à un sous-anneau de  $K$ . On a alors une injection  $A \rightarrow K \rightarrow K[X]$  qui est un morphisme d'anneaux. On en déduit donc grâce à la propriété universelle des anneaux de polynômes un morphisme d'anneaux  $A[X] \rightarrow K[X]$  qui prolonge cette injection  $A \hookrightarrow K[X]$  et qui à  $X$  associe  $X$ . Il est facile de voir que ce morphisme est injectif, et donc que  $A[X]$  peut être identifié à un sous-anneau de  $K[X]$ .

**Lemme 9.14.** Soit  $A$  un anneau factoriel et soit  $K$  son corps des fractions. Soit  $P \in A[X]$ . On suppose qu'il existe  $Q, R$  dans  $K[X]$  tels que  $P = QR$ . Alors il existe  $Q_1, R_1$  dans  $A[X]$  et  $\alpha, \beta$  dans  $K \setminus \{0\}$  tels que  $P = Q_1 R_1$ ,  $Q_1 = \alpha Q$ , et  $R_1 = \beta R$ .

*Démonstration.* En réduisant tous les coefficients de  $Q$  et  $R$  aux mêmes dénominateurs, on voit qu'il existe  $(q, r) \in A^2$  et  $Q_0, R_0$  dans  $A[X]$  tels que  $qQ = Q_0$  et  $rR = R_0$ . On a alors  $Q_0 R_0 = qrP$ .

Soient  $c$  un contenu de  $Q_0$  et  $d$  un contenu de  $R_0$ . On peut donc écrire  $Q_0 = cQ_2$  et  $R_0 = dR_2$  avec  $Q_2$  et  $R_2$  dans  $A[X]$  primitifs d'après le lemme 9.12. On a donc  $qrP = cdQ_2R_2$  avec  $Q_2R_2$  primitif (lemme de Gauss), donc à l'aide du lemme 9.12 on en déduit que  $cd$  est un contenu de  $qrP$  et donc que  $qr$  divise  $cd$  : il existe  $\lambda \in A$  tel que  $cd = \lambda qr$  d'où  $P = \lambda Q_2 R_2$ . Finalement on pose  $\alpha = \lambda c^{-1} q \in K \setminus \{0\}$ ,  $\beta = d^{-1} r \in K \setminus \{0\}$ ,  $Q_1 = \alpha Q$  et  $R_1 = \beta R$ .  $\checkmark$

**Théorème 9.15.** Soit  $A$  un anneau factoriel et soit  $K$  son corps des fractions.

Les éléments irréductibles de  $A[X]$  sont

- les éléments irréductibles de  $A$  et
- les polynômes non constants et primitifs de  $A[X]$  qui sont irréductibles dans  $K[X]$ .

*Démonstration.* On rappelle que  $A[X]^\times = A^\times$  ( $A$  est intègre).

(1) Soit  $a \in A$ . Montrons que  $a$  est irréductible dans  $A[X]$  si et seulement s'il est irréductible dans  $A$ .

- ◆ Si  $a$  est irréductible dans  $A$ , il n'est ni nul ni inversible dans  $A$  et donc il n'est ni nul ni inversible dans  $A[X]$ . De plus, si  $a = PQ$  avec  $P, Q$  dans  $A[X]$ , alors  $P$  et  $Q$  sont de degré 0 donc ils sont dans  $A$  et par conséquent  $P$  ou  $Q$  est un élément inversible de  $A$  donc de  $A[X]$ .
- ◆ Réciproquement, si  $a$  est irréductible dans  $A[X]$ , il n'est ni nul ni inversible dans  $A[X]$  et donc il n'est ni nul ni inversible dans  $A$  et si  $a = bc$  avec  $b, c$  dans  $A$ , alors  $b$  ou  $c$  est inversible dans  $A[X]$  et donc dans  $A$ .

(2) Soit  $P$  dans  $A[X]$  de degré supérieur ou égal à 1. Alors  $P$  n'est ni nul ni inversible dans  $A[X]$ .

- ◆ Supposons que  $P$  est primitif dans  $A[X]$  et irréductible dans  $K[X]$ . Si  $P = QR$  avec  $Q, R$  dans  $A[X]$ , l'irréductibilité de  $P$  dans  $K[X]$  assure que  $Q$ , par exemple, est un élément inversible de  $K[X]$ . Donc,  $Q = a$  avec  $a \in A \setminus \{0\}$ . L'égalité  $P = aR$  assure que si  $d$  est un contenu de  $P$ , alors  $a \mid d$ . Mais  $P$  est primitif, donc  $a = Q$  est inversible. Ainsi,  $P$  est irréductible dans  $A[X]$ .
- ◆ Réciproquement, supposons que  $P$  est irréductible dans  $A[X]$ . Si  $d$  est un contenu de  $P$ , alors  $P = dP_1$  avec  $P_1 \in A[X]$  primitif et de degré  $\geq 1$  donc non inversible. Par conséquent,  $d$  est inversible dans  $A[X]$  donc dans  $A$  et donc  $P$  est primitif.  
Démontrons que  $P$  est irréductible dans  $K[X]$ . Il n'est pas inversible dans  $K[X]$  (de degré  $\geq 1$ ). Si  $P = QR$  dans  $K[X]$ , grâce au lemme 9.14 on peut supposer que  $Q$  et  $R$  sont dans  $A[X]$ . Or  $P$  est irréductible dans  $A[X]$  donc par exemple  $Q$  est inversible dans  $A[X]$  et donc  $Q$  est inversible dans  $K[X]$ . ✓

**Remarque.** Soit  $A$  un anneau factoriel et soit  $K$  son corps des fractions. Soit  $P \in A[X]$  de contenu  $c \in A$  et tel que  $P = QR$  dans  $K[X]$ . Alors il existe des polynômes  $\tilde{Q}$  et  $\tilde{R}$  dans  $A[X]$  qui sont primitifs, tels que  $\tilde{Q} \sim Q$  et  $\tilde{R} \sim R$  dans  $K[X]$  et qui vérifient  $P = c\tilde{Q}\tilde{R}$ .

En effet, il suffit de combiner le lemme 9.12, le lemme de Gauss et le lemme 9.14.

En particulier, si  $P \in A[X]$  est primitif et tel que  $P = QR$  dans  $K[X]$ , alors il existe des polynômes  $\tilde{Q}$  et  $\tilde{R}$  dans  $A[X]$  qui sont primitifs, tels que  $\tilde{Q} \sim Q$  et  $\tilde{R} \sim R$  dans  $K[X]$  et qui vérifient  $P = \tilde{Q}\tilde{R}$ .

**Remarque.** Soit  $A$  un anneau factoriel et soit  $K$  son corps des fractions. Soit  $P \in A[X]$ .

On a vu dans la démonstration du théorème si  $P$  est irréductible dans  $A[X]$  alors il est irréductible dans  $K[X]$  (inutile de supposer que  $P$  est primitif, il l'est nécessairement).

Pour la réciproque, l'hypothèse que  $P$  est primitif est indispensable. En effet, soit  $P = 2X \in \mathbb{Z}[X]$ . Alors  $P$  est irréductible dans  $\mathbb{Q}[X]$  (car il est de degré 1) mais il n'est pas irréductible dans  $\mathbb{Z}[X]$  (car 2 et  $X$  ne sont pas inversibles dans  $\mathbb{Z}[X]$ ).

**Théorème 9.16** (Théorème de Gauss). Si  $A$  est factoriel, alors  $A[X]$  est factoriel.

*Démonstration.* Notons  $K = \text{Frac } A$ .

- On sait déjà que  $A[X]$  est intègre puisque  $A$  est intègre.
- On commence par démontrer que l'anneau  $A[X]$  satisfait la condition (E). Soit  $P \in A[X]$ , non nul et non inversible dans  $A[X]$ .
  - ◆ Si  $P$  est de degré 0, il s'écrit comme produit d'éléments irréductibles de  $A$  (et donc de  $A[X]$  d'après le théorème 9.15) et c'est terminé.
  - ◆ Supposons donc que  $P$  est de degré  $\geq 1$ . En particulier,  $P$  n'est ni nul ni inversible dans  $K[X]$ . Notons  $c$  un contenu de  $P$ .  
Comme  $K[X]$  est principal ( $K$  est un corps) et donc factoriel, il existe  $r \in \mathbb{N}^*$  et  $P_1, \dots, P_r$  des polynômes irréductibles de  $K[X]$  tels que  $P = P_1 \dots P_r$ . D'après la remarque précédente, il existe pour tout  $i \in \llbracket 1; r \rrbracket$  des polynômes primitifs  $\tilde{P}_i \in A[X]$  tels que  $\tilde{P}_i \sim P_i$  dans  $K[X]$  vérifiant  $P = c\tilde{P}_1 \dots \tilde{P}_r$ . Puisque  $A$  est factoriel, on peut écrire  $c = q_1 \dots q_s$  où les  $q_j$  sont des éléments irréductibles de  $A$ . On a alors  $P = q_1 \dots q_s \tilde{P}_1 \dots \tilde{P}_r$  et d'après le théorème précédent, les  $q_j$  sont irréductibles dans  $A[X]$  et les  $\tilde{P}_i$  aussi puisqu'ils ne sont pas constants, ils sont primitifs et ils sont irréductibles dans  $K[X]$  (associés aux  $P_i$ ).
- Pour démontrer que  $A[X]$  est factoriel, c'est-à-dire que la condition (U) est vérifiée, il suffit grâce au théorème 8.13 de démontrer que  $A[X]$  satisfait la condition de primalité, c'est-à-dire de démontrer qu'un élément irréductible de  $A[X]$  engendre un idéal premier de  $A[X]$ . Soit  $P$  un polynôme irréductible de  $A[X]$ .
  - ◆ Si  $P = a \in A$ , alors  $a$  est un élément irréductible de  $A$ . On a un morphisme surjectif d'anneaux  $A[X] \rightarrow (A/(a))[X]$  (cf. exemple page 111), et il est facile de voir qu'il induit un isomorphisme  $A[X]/(aA[X]) \cong (A/(a))[X]$  par le premier théorème d'isomorphisme. Or  $A$  est factoriel et  $a$  est irréductible dans  $A$ , donc  $A/(a)$  est intègre, donc  $A[X]/(aA[X]) \cong (A/(a))[X]$  est intègre, et donc  $aA[X]$  est un idéal premier de  $A[X]$ .
  - ◆ Si maintenant  $\deg P \geq 1$ , alors  $P$  est primitif et irréductible dans  $K[X]$  d'après le théorème 9.15. Comme  $P$  est irréductible dans l'anneau factoriel  $K[X]$ , l'idéal  $PK[X]$  est premier dans  $K[X]$ . Il suffit donc de démontrer que  $PA[X] = PK[X] \cap A[X]$  pour conclure que  $PA[X]$  est premier dans  $A[X]$  puisque  $PA[X] \neq A[X]$  (Voir travaux dirigés). Il est clair que  $PA[X] \subset PK[X] \cap A[X]$ . Démontrons l'autre inclusion : soit  $PQ \in PK[X] \cap A[X]$ , avec  $Q \in K[X]$  et  $PQ \in A[X]$ . Nous allons démontrer que  $Q \in A[X]$ . En réduisant les coefficients de  $Q$  au même dénominateur, on peut écrire  $dQ = Q_1$  avec  $d \in A$  et  $Q_1 \in A[X]$ . Notons  $c$  un contenu de  $Q_1$ . Puisque  $P$  est primitif,  $c$  est un contenu de  $PQ_1$ . Or  $PQ_1 = dPQ$  avec  $PQ \in A[X]$ , donc  $d$  divise  $c$ . Posons  $c = da$  avec  $a \in A$ . On sait qu'il existe un polynôme primitif  $Q_2 \in A[X]$  tel que  $Q_1 = cQ_2 = daQ_2$ . On en déduit que  $PQ = aPQ_2$  et donc que  $Q = aQ_2 \in A[X]$ . ✓

**Théorème 9.17.** Si  $A$  est factoriel et  $n \in \mathbb{N}^*$ , alors  $A[X_1, \dots, X_n]$  est factoriel.

*Démonstration.* Par récurrence sur  $n$  à l'aide du théorème 9.16. ✓

**Remarque.** On vérifie facilement que si  $A$  est un anneau tel que  $A[X_1, \dots, X_n]$  est factoriel, alors  $A$  est factoriel.

Cependant, en général, un sous-anneau ou un anneau quotient d'un anneau factoriel n'est pas factoriel. Voir travaux dirigés. Par exemple,  $\mathbb{Z}[i\sqrt{3}]$  n'est pas factoriel mais c'est un sous-anneau de  $\mathbb{C}$  qui est factoriel et il est isomorphe au quotient  $\mathbb{Z}[X]/(X^2 + 3)$  de  $\mathbb{Z}[X]$  qui est factoriel.

## B. Tests d'irréductibilité.

**Rappel.** Un élément  $a \in A$  est une racine d'un polynôme  $f$  de  $A[X]$  si et seulement si le polynôme  $X - a$  divise  $f$  dans  $A[X]$ . Il en découle que si  $A$  est intègre et  $f \neq 0$ , le nombre de racines de  $f$  dans  $A$  est au plus  $\deg(f)$ .

*Démonstration.* En effet, il est clair que si  $X - a$  divise  $f$  dans  $A[X]$  alors  $a$  est une racine de  $f$ . Réciproquement, supposons que  $a$  soit une racine de  $f$ . Effectuons la division euclidienne de  $f$  par le polynôme unitaire  $X - a$  dans  $A[X]$  (Voir travaux dirigés) : il existe  $(q, r) \in A[X]^2$  tel que  $f = (X - a)q + r$  et  $\deg(r) < \deg(X - a) = 1$ . Ainsi,  $r$  est constant et on a  $0 = f(a) = r(a)$  donc  $r = 0$  et finalement  $X - a$  divise  $f$  dans  $A[X]$ .

Vérifions le deuxième point par récurrence sur le degré de  $f$  dans  $\mathbb{N}$ . L'initialisation ( $f$  constant) est claire.

Soit  $n \in \mathbb{N}^*$  tel que tout polynôme de degré strictement inférieur à  $n$  admet un nombre de racines inférieur à son degré. Soit  $f \in A[X]$  un polynôme de degré  $n$ . Si  $f$  n'a pas de racine, le résultat est vrai pour  $f$ . Supposons donc que  $f$  a au moins une racine dans  $A$ , notons-la  $a$ . D'après ce qui précède, il existe  $g \in A[X]$  tel que  $f = (X - a)g$ . Comme  $X - a$  est unitaire,  $\deg(g) = n - 1$  donc par hypothèse de récurrence,  $g$  a au plus  $n - 1$  racines. De plus,  $A$  est intègre donc une racine de  $f$  est nécessairement égale à  $a$  ou est une racine de  $g$ , il y en a donc au plus  $n$ . ✓

**Proposition 9.18.** Soit  $A$  un anneau.

- (1) Soit  $a \in A$  et soit  $f \in A[X]$ . Alors  $f$  est irréductible dans  $A[X]$  si, et seulement si,  $f(X - a)$  est irréductible dans  $A[X]$ .
- (2) On suppose que  $A$  est intègre. Alors pour tout  $a \in A$  le polynôme  $X - a$  est irréductible dans  $A[X]$ . Si de plus  $A$  est un corps, tout polynôme de degré 1 est irréductible dans  $A[X]$ .
- (3) On suppose que  $A$  est intègre. Soit  $f \in A[X]$  un polynôme de degré  $\deg(f) \geq 2$ . Si  $f$  est irréductible dans  $A[X]$ , alors  $f$  n'a pas de racine dans  $A$ .
- (4) Soit  $K$  un corps. Soit  $f \in K[X]$  un polynôme de degré 2 ou 3. Alors  $f$  est irréductible dans  $K[X]$  si, et seulement si,  $f$  n'a pas de racine dans  $K$ .

*Démonstration.* (1) Vérifions d'abord que  $P \in A[X]$  est inversible si, et seulement si,  $P(X + a)$  est inversible. Il suffit de démontrer une implication, l'autre se fait en remplaçant  $a$  par  $-a$ . Supposons donc que  $P$  est inversible. Alors il existe  $Q \in A[X]$  tel que  $P(X)Q(X) = 1$ . On en déduit que  $P(X + a)Q(X + a) = 1$  donc que  $P(X + a)$  est inversible.

Soit maintenant  $f \in A[X]$ , non nul et non inversible. Alors  $f(X - a)$  n'est ni nul, ni inversible. De plus,

$$f(X - a) = P(X)Q(X) \text{ avec } P(X) \text{ et } Q(X) \text{ non inversibles}$$

$$\iff f(X) = P(X + a)Q(X + a) \text{ avec } P(X + a) \text{ et } Q(X + a) \text{ non inversibles}$$

donc  $f(X)$  est irréductible si, et seulement si,  $f(X - a)$  est irréductible.

- (2) On rappelle que  $A[X]^\times = A^\times$  lorsque  $A$  est intègre. Notons que  $X - a$  n'est pas nul et n'est pas inversible. Si  $X - a = PQ$  alors  $P$  et  $Q$  ne sont pas nuls et donc  $\deg P \geq 0$ ,  $\deg Q \geq 0$  et  $\deg P + \deg Q = \deg(X - a) = 1$  (puisque  $A$  est intègre), et finalement on doit avoir  $\deg P = 0$  ou  $\deg Q = 0$  c'est-à-dire que  $P$  ou  $Q$  est constant, par exemple  $P$ . Si on pose  $P = b$  et  $Q = cX + d$ , on a alors  $ac = 1$  (en identifiant) et donc  $P = a$  est inversible dans  $A$  donc dans  $A[X]$ .

Finalement,  $X - a$  est irréductible.

Si  $A$  est un corps et  $f$  est un polynôme de degré 1, alors  $f$  est associé à un polynôme de la forme  $X - a$  qui est irréductible dans  $A[X]$ .

- (3) Si  $f$  a une racine  $a$  dans  $A$ , alors  $X - a$  divise  $f$  donc  $f = (X - a)P$  et on a  $\deg P = \deg f - 1 \geq 1$  (car  $A$  est intègre). Puisque  $A$  est intègre, les polynômes non constants ne sont pas inversibles donc  $f$  n'est pas irréductible.

- (4) Voir travaux dirigés

Puisque  $K$  est intègre et que  $\deg f \geq 2$ , on a déjà vu que si  $f$  est irréductible alors  $f$  n'a pas de racine dans  $A$ .

Réciproquement, supposons que  $f$  est réductible. Alors il existe  $P$  et  $Q$  non constants tels que  $f = PQ$ . On a  $\deg P + \deg Q \in \{2; 3\}$  et  $\deg P \geq 1$ ,  $\deg Q \geq 1$ , donc  $\deg P = 1$  ou  $\deg Q = 1$ . Or un polynôme de degré 1 à coefficients dans un corps  $K$  a nécessairement une racine, donc  $f$  aussi. ✓

**Remarque.** Notons que si  $A$  n'est pas intègre, les éléments inversibles de  $A[X]$  ne sont pas tous de degré 0. Par exemple, dans  $\mathbb{Z}/4\mathbb{Z}[X]$  on a  $(2X + 1)^2 = 1$  donc  $2X + 1$  est inversible mais n'est pas constant. Il faut donc faire attention dans la démonstration de l'affirmation (1).

**Remarque.** Les affirmations (2) et (3) sont fausses si  $A$  n'est pas intègre.

Exercice : rechercher des contre-exemples.

➤ Pour (2) : dans  $\mathbb{Z}/6\mathbb{Z}[X]$  on a  $X - 1 = (2X + 1)(3X - 1)$  avec  $2X + 1$  et  $3X - 1$  non inversibles. En effet, si  $(2X + 1)P = 1$  avec  $P = \sum_{i=0}^d a_i X^i$  et  $a_d \neq 0$ , alors  $a_0 = 1$ ,  $2a_d = 0$  et  $a_{i+1} = 4a_i$  pour tout  $i$  avec  $0 \leq i \leq d-1$ , d'où  $a_i = 4$  pour tout  $i \in \llbracket 1; d \rrbracket$ , mais alors  $0 = 2a_d = 2 \cdot 4 = 2$  (ou  $0 = 2a_0 = 2$  si  $d = 0$ ), une contradiction ; pour  $3X - 1$  on peut raisonner de la même façon.

Autre contre-exemple : notons  $e = (1, 0) \in \mathbb{Z}^2$  ; dans  $\mathbb{Z}^2[X]$ , on a  $X = (eX + (1 - e))((1 - e)X + e)$  avec  $eX + (1 - e)$  et  $(1 - e)X + e$  non inversibles car leurs coefficients constants  $e$  et  $1 - e$  ne sont pas inversibles.

➤ Pour (3),  $2X^2 + X \in \mathbb{Z}/4\mathbb{Z}[X]$  est de degré 2, il admet 0 comme racine, mais il est irréductible. En effet,  $2X^2 + X = (2X + 1)X$  avec  $2X + 1$  inversible (cf. remarque précédente), donc il suffit de démontrer que  $X$  est irréductible. Supposons donc que  $X = PQ$  avec  $P = \sum_{i=0}^d a_i X^i$  et  $Q = \sum_{i=0}^e b_i X^i$ . Alors  $a_0 b_0 = 0$  et  $a_0 b_1 + a_1 b_0 = 1$ . Dans  $\mathbb{Z}/4\mathbb{Z}$ ,  $a_0 b_0 = 0$  implique  $a_0 = 0$  ou  $b_0 = 0$  ou  $(a_0, b_0) = (2, 2)$ , mais si  $a_0 = 2 = b_0$  alors  $2(b_1 + a_1) = 1$  et donc 2 est inversible, une contradiction. Donc  $a_0$  ou  $b_0$  est nul, par exemple  $a_0$ . Écrivons  $P = XP_1$ . On a donc  $X(P_1 Q - 1) = 0$ . Mais si  $XR = 0$ , on vérifie facilement que  $R = 0$  donc  $P_1 Q = 1$  et donc  $Q$  est inversible.

**Remarque.** L'affirmation (4) est fausse si on remplace  $K$  par un anneau (même intègre).

Exercice : rechercher des contre-exemples.

Dans  $\mathbb{Z}[X]$ , le polynôme  $2(X^2 + 1)$  est de degré 2 et sans racine mais il n'est pas irréductible ( $2$  et  $X^2 + 1$  ne sont pas inversibles).

**Proposition 9.19** (Test des racines entières). Soit  $A$  un anneau factoriel et soit  $K$  son corps des fractions. Soit  $P = \sum_{i=0}^n a_i X^i \in A[X]$  avec  $a_n \neq 0$ ,  $n \geq 1$ , et soit  $\alpha = \frac{p}{q} \in K$  une racine de  $P$  dans  $K$  avec  $p$  et  $q$  deux éléments premiers entre eux de  $A$ . Alors  $q$  divise  $a_n$  et  $p$  divise  $a_0$ .

*Démonstration.* Voir travaux dirigés

Dans  $K$  on a  $\sum_{i=0}^n a_i \frac{p^i}{q^i} = 0$  d'où, en multipliant par  $q^n$ , on a  $\sum_{i=0}^n a_i p^i q^{n-i} = 0$ . On a donc

➤  $a_0 q^n = -p \sum_{i=1}^n a_i p^{i-1} q^{n-i}$  d'où  $p \mid a_0 q^n$ . Or  $p$  et  $q$  sont premiers entre eux donc  $p$  et  $q^n$  aussi : en effet, si  $t$  est un élément irréductible de  $A$  qui divise  $p$  et  $q^n$ , alors  $t$  divise  $q$  d'après la condition d'Euclide, et  $t$  divise  $p$  donc  $t$  est inversible et on a une contradiction. D'après la condition de Gauss,  $p \mid a_0$ .

➤  $a_n p^n = \sum_{i=0}^{n-1} a_i p^i q^{n-i-1}$  d'où  $q \mid a_n p^n$  avec  $p$  et  $q$  premiers entre eux, donc  $a \mid a_n$ . ✓

**Exemple.** Soit  $P = X^3 - X + 1 \in \mathbb{Z}[X]$ . Si  $P$  a une racine  $\alpha = \frac{p}{q}$  dans  $\mathbb{Q}$  avec  $(p, q) \in \mathbb{Z}^2$  et  $\text{pgcd}(p, q) = 1$ , alors  $p \mid 1$  et  $q \mid 1$  donc  $\alpha = \pm 1$ . Mais 1 et  $-1$  ne sont pas racines de  $P$  donc  $P$  n'a pas de racine dans  $\mathbb{Q}$ . Comme  $\mathbb{Q}$  est un corps et  $\deg P = 3$ , on en déduit que  $P$  est irréductible dans  $\mathbb{Q}[X]$ . Enfin, puisque  $P$  est primitif, il est irréductible dans  $\mathbb{Z}[X]$ .

**Exemple.** Soit  $P = 5Y^3 - 2Y + X \in \mathbb{Q}[X, Y]$ . On le considère comme un polynôme de  $\mathbb{Q}[X][Y]$ . L'anneau  $\mathbb{Q}[X]$  est factoriel, de corps des fractions  $\mathbb{Q}(X)$ . Supposons que  $P$  ait une racine dans  $\mathbb{Q}(X)$ , écrite sous forme irréductible  $\frac{Q}{R}$  avec  $Q, R$  dans  $\mathbb{Q}[X]$ . Grâce au critère des racines entières, on sait que  $Q$  divise  $X$  et que  $R$  divise 5 dans  $\mathbb{Q}[X]$ . Ainsi,  $R$  est inversible dans  $\mathbb{Q}[X]$  et c'est donc une constante non nulle de  $\mathbb{Q}$ . De plus,  $X$  est irréductible dans  $\mathbb{Q}[X]$  donc  $Q$  est soit inversible, soit associé à  $X$ , c'est-à-dire que  $Q$  est soit une constante non nulle, soit le produit de  $X$  et d'une constante non nulle. Finalement,  $\frac{Q}{R}$  est dans  $\{\lambda, \lambda X \mid \lambda \in \mathbb{Q}^*\}$ . Or  $P(\lambda) = 5\lambda^3 - 2\lambda + X \neq 0$  et  $P(\lambda X) = 5\lambda^3 X^3 + (1 - 2\lambda)X \neq 0$ . Donc  $P$  n'a pas de racine dans  $\mathbb{Q}(X)$ .

On en déduit que  $P$  est un polynôme à coefficients dans le corps  $\mathbb{Q}(X)$ , de degré 3 et sans racine dans  $\mathbb{Q}(X)$ , donc  $P$  est irréductible dans  $\mathbb{Q}(X)[Y]$ . Comme il est primitif, il est également irréductible dans  $\mathbb{Q}[X][Y] = \mathbb{Q}[X, Y]$ .

On peut remarquer que  $P$  est en fait dans  $\mathbb{Z}[X, Y] = \mathbb{Z}[X][Y]$ , que l'anneau  $\mathbb{Z}[X]$  est factoriel de corps des fractions  $\mathbb{Q}(X)$ , que  $P$  est primitif et irréductible dans  $\mathbb{Q}(X)[Y]$ , donc il est également irréductible dans  $\mathbb{Z}[X][Y] = \mathbb{Z}[X, Y]$ .

Soit  $I$  un idéal de l'anneau  $A$ . On note  $\varphi_I: A[X] \rightarrow (A/I)[X]$  le morphisme d'anneaux de l'exemple page 111.

**Proposition 9.20** (Critère de réduction). Soient  $A$  un anneau factoriel et  $I$  un idéal premier de  $A$ . Soit  $P = \sum_{i=0}^n a_i X^i \in A[X]$  avec  $a_n \notin I, n \geq 1$ ; si  $\varphi_I(P)$  est irréductible dans  $(A/I)[X]$  ou dans  $(\text{Frac}(A/I))[X]$ , alors  $P$  est irréductible dans  $(\text{Frac } A)[X]$ .

*Démonstration.* Notons  $K = \text{Frac } A$ . On peut remarquer que  $I$  est premier donc  $A/I$  est intègre, il a donc bien un corps des fractions.

Les hypothèses impliquent que  $P$  n'est pas nul ( $a_n \neq 0$  en particulier) et n'est pas inversible ( $\deg P \geq 1$ ).

Supposons que  $P = QR$  avec  $Q, R$  dans  $K[X]$ . Grâce au lemme 9.14, on peut supposer que  $Q$  et  $R$  sont dans  $A[X]$ . Posons  $Q = \sum_{i=0}^q b_i X^i$  et  $R = \sum_{i=0}^r c_i X^i$  avec  $a_n = b_q c_r \notin I$ . On a  $\varphi_I(P) = \varphi_I(Q)\varphi_I(R)$ . Puisque  $\varphi_I(P)$  est irréductible dans  $(A/I)[X]$  ou dans  $(\text{Frac}(A/I))[X]$ , par exemple  $\varphi_I(Q)$  est inversible dans  $(A/I)[X]$  ou dans  $(\text{Frac}(A/I))[X]$ , donc dans les deux cas c'est un élément non nul de  $\text{Frac}(A/I)$ . Donc  $\deg \varphi_I(Q) = 0$ . Mais  $0 \neq \bar{a}_n = \bar{b}_q \bar{c}_r$ , donc  $\bar{b}_q \neq 0$ , et donc  $\deg \varphi_I(Q) = q$ . Donc  $\deg Q = q = 0$  et  $Q$  est une constante non nulle de  $K$ , donc inversible dans  $K$  et donc dans  $K[X]$ . Donc  $P$  est irréductible dans  $K[X]$ . ✓

**Exemple.** Soit  $P = 7X^3 - 3X + 75 \in \mathbb{Z}[X]$ . L'anneau  $\mathbb{Z}$  est factoriel et l'idéal  $(2) = 2\mathbb{Z}$  est premier. On réduit modulo 2 et on obtient  $\varphi_{(2)}(P) = X^3 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ . On vérifie facilement que  $\varphi_{(2)}(P)$  n'a pas de racine dans  $\mathbb{Z}/2\mathbb{Z}$ . Puisque  $\mathbb{Z}/2\mathbb{Z}$  est un corps et  $\deg \varphi_{(2)}(P) = 3$ , le polynôme  $\varphi_{(2)}(P)$  est irréductible dans  $(\mathbb{Z}/2\mathbb{Z})[X]$ . On en déduit que  $P$  est irréductible dans  $\mathbb{Q}[X]$ . De plus, puisqu'il est primitif,  $P$  est irréductible dans  $\mathbb{Z}[X]$ .

**Exemple.** Soit  $P = X^2 Y^2 + Y^2 + 2XY + Y + 1 = (X^2 + 1)Y^2 + (2X + 1)Y + 1 \in \mathbb{R}[X, Y] = \mathbb{R}[X][Y]$ . L'anneau  $\mathbb{R}[X]$  est factoriel de corps des fractions  $\mathbb{R}(X)$ . L'idéal  $(X)$  de  $\mathbb{R}[X]$  est premier car  $X$  est irréductible dans  $\mathbb{R}[X]$ . Notons que  $\varphi_{(X)}$  est à valeurs dans  $(\mathbb{R}[X]/(X))[Y] \cong \mathbb{R}[Y]$ . Dans  $\mathbb{R}[Y]$ , le polynôme  $\varphi_{(X)}(P) = Y^2 + Y + 1$  est irréductible car il est de degré 2 à coefficients dans le corps  $\mathbb{R}$  et sans racine dans  $\mathbb{R}$  donc, par le critère de réduction,  $P$  est irréductible dans  $\mathbb{R}(X)[Y]$ . De plus,  $P$  est primitif donc il est irréductible dans  $\mathbb{R}[X, Y]$ .

**Proposition 9.21** (Critère d'Eisenstein). Supposons  $A$  factoriel et considérons  $P = \sum_{i=0}^n a_i X^i \in A[X]$  avec  $n = \deg P \geq 1$ . S'il existe un élément irréductible  $p$  de  $A$  tel que  $p \nmid a_n, p \mid a_i$  pour  $0 \leq i \leq n-1$  et  $p^2 \nmid a_0$ , alors  $P$  est irréductible dans  $(\text{Frac } A)[X]$ .

*Démonstration.* Notons  $K = \text{Frac } A$ . Puisque  $\deg P \geq 1$ , le polynôme  $P$  n'est pas inversible dans  $K[X]$ . Supposons que  $P$  ne soit pas irréductible dans  $K[X]$ . Alors, il existe  $(Q, R)$  dans  $K[X]^2$  tel que  $P = QR$  et  $0 < q = \deg Q < \deg P$  et  $0 < r = \deg R < \deg P$ . D'après le lemme 9.14, on peut supposer que  $Q$  et  $R$  sont dans  $A[X]$  (avec les mêmes degrés). Posons  $Q = \sum_{j=0}^q b_j X^j$  et  $R = \sum_{k=0}^r c_k X^k$ . Comme  $p$  ne divise pas  $a_n = b_q c_r$ ,  $p$  ne divise ni  $b_q$  ni  $c_r$ . Comme  $p$  divise  $a_0$  et  $p^2$  ne divise pas  $a_0$ , l'égalité  $a_0 = b_0 c_0$  assure que  $p$  divise  $b_0$  ou  $c_0$  (car  $A$  satisfait la condition d'Euclide) mais pas les deux. Quitte à échanger  $Q$  et  $R$ , on peut supposer que  $p$  divise  $c_0$  et pas  $b_0$ . Soit donc  $\ell = \min\{i \in \llbracket 1; r \rrbracket \text{ tel que } p \nmid c_i\}$ ; comme  $\ell \leq r < n$ ,  $p$  divise  $a_\ell$  et par définition de  $\ell$ ,  $p$  divise  $c_j$  pour tout  $j \in \llbracket 0; \ell - 1 \rrbracket$ , donc l'égalité  $a_\ell = b_0 c_\ell + (b_1 c_{\ell-1} + \cdots + b_\ell c_0)$  montre que  $b_0 c_\ell$  est divisible par  $p$  et donc que  $c_\ell$  est divisible par  $p$ . Ceci constitue une contradiction. ✓

*Exemple.* Soit  $P(X) = 2X^5 - 28X^3 + 98X^2 - 14 \in \mathbb{Z}[X]$ . L'anneau  $\mathbb{Z}$  est factoriel. On applique le critère d'Eisenstein avec  $p = 7$  qui est bien irréductible dans  $\mathbb{Z}$ . En effet,  $7 \nmid 2$ ,  $7$  divise  $-28$ ,  $98$  et  $-14$  mais  $7^2 \nmid -14$ . On en déduit que  $P$  est irréductible dans  $\mathbb{Q}[X]$ .

Cependant, il n'est pas irréductible dans  $\mathbb{Z}[X]$  car  $P = 2Q$  avec  $Q(X) = X^5 - 14X^3 + 49X^2 - 7$  et ni  $2$  ni  $Q$  ne sont inversibles dans  $\mathbb{Z}[X]$ . Mais  $Q \in \mathbb{Z}[X]$  est irréductible dans  $\mathbb{Z}[X]$  car, dans  $\mathbb{Q}[X]$  il est associé à  $P$  donc il est irréductible, et il est primitif dans  $\mathbb{Z}[X]$ .

*Exemple.* Soit  $P = Y^5 + X^2 Y + X - Y + 1 \in \mathbb{C}[X, Y]$ . On a  $P = Y^5 + (X^2 - 1)Y + X + 1 \in \mathbb{C}[X][Y]$ . L'anneau  $\mathbb{C}[X]$  est factoriel, de corps des fractions  $\mathbb{C}(X)$ . L'élément  $X + 1$  est irréductible dans  $\mathbb{C}[X]$ , il divise tous les coefficients de  $P$  sauf le coefficient dominant et  $(X + 1)^2$  ne divise pas le coefficient constant  $X + 1$ . On peut donc appliquer le critère d'Eisenstein avec  $p = X + 1$  pour en déduire que  $P$  est irréductible dans  $\mathbb{C}(X)[Y]$ , et aussi dans  $\mathbb{C}[X][Y] = \mathbb{C}[X, Y]$  car il est primitif.



# Polynômes symétriques

## I. L'ANNEAU DES POLYNÔMES SYMÉTRIQUES

Soit  $A$  un anneau quelconque (commutatif et unitaire).

**Définition-Proposition 10.1.** Soit  $n \in \mathbb{N}^*$ . On définit une action de  $S_n$  sur  $A[X_1, \dots, X_n]$  par

$$\begin{aligned} S_n \times A[X_1, \dots, X_n] &\longrightarrow A[X_1, \dots, X_n] \\ (\sigma, f) &\longmapsto {}^\sigma f = f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \end{aligned}$$

pour tout  $\sigma \in S_n$  et tout  $f \in A[X_1, \dots, X_n]$ .

**Définition 10.2.** Un polynôme  $f \in A[X_1, \dots, X_n]$  est dit **symétrique** si pour tout  $\sigma \in S_n$  on a  ${}^\sigma f = f$  (autrement dit,  $f \in A[X_1, \dots, X_n]^{S_n}$ ).

**Exemples.**  $\triangleright X^2 + Y^2 + Z^2$  est un polynôme symétrique de  $\mathbb{Z}[X, Y, Z]$  (mais pas de  $\mathbb{Z}[X, Y, Z, T]$ ).

$\triangleright X_1 X_2 + X_2 X_3 + X_3 X_1$  est un polynôme symétrique de  $\mathbb{Z}[X_1, X_2, X_3]$ .

$\triangleright X^3 Y + Y^3 Z + Z^3 X$  n'est pas un polynôme symétrique de  $\mathbb{Z}[X, Y, Z]$ .

**Remarque.** Si  $f$  est un polynôme symétrique, alors le degré partiel de  $f$  par rapport à chacune de ses variables est le même, et on l'appelle **degré partiel** de  $f$ .

**Lemme 10.3.** Soit  $\varphi: A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_{n-1}]$  l'unique morphisme d'anneaux qui fixe les éléments de  $A$  ainsi que  $X_1, \dots, X_{n-1}$  et qui vérifie  $\varphi(X_n) = 0$ , obtenu grâce à la propriété universelle des anneaux de polynômes. On a  $\varphi(P) = P(X_1, \dots, X_{n-1}, 0)$ .

Soit  $f \in A[X_1, \dots, X_n]$  un polynôme symétrique. Alors  $\varphi(f)$  est un polynôme symétrique de  $A[X_1, \dots, X_{n-1}]$ .

**Démonstration.** Soit  $\gamma \in S_{n-1}$  et soit  $\gamma' \in S_n$  la permutation définie par  $\gamma'_{[1, n-1]} = \gamma$  et  $\gamma'(n) = n$ . Alors  $\gamma\varphi(f) = \varphi(\gamma'f) = \varphi(f)$ , ce que l'on voulait. ✓

**Lemme 10.4.** Soit  $\gamma \in S_n$ . Soit  $\theta_\gamma: A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n]$  l'application définie par  $\theta_\gamma(P) = \gamma P$ . Alors  $\theta_\gamma$  est un automorphisme d'anneaux qui fixe les éléments de  $A$ .

**Démonstration.** Notons que  $\theta_\gamma$  est l'unique morphisme d'anneaux qui fixe les éléments de  $A$  et qui vérifie  $\theta_\gamma(X_i) = X_{\gamma(i)}$  pour tout  $i$ . Il admet comme réciproque  $\theta_{\gamma^{-1}}$ , qui est l'unique morphisme d'anneaux qui fixe les éléments de  $A$  et qui vérifie  $\theta_\gamma(X_i) = X_{\gamma^{-1}(i)}$  pour tout  $i$ . En effet,  $\theta_\gamma \circ \theta_{\gamma^{-1}}$  et  $\text{id}_{A[X_1, \dots, X_n]}$  sont deux morphismes d'anneaux qui prolongent  $A \hookrightarrow A[X_1, \dots, X_n]$  et qui fixent tous les  $X_i$ , donc par l'unicité dans la propriété universelle 9.5 ils sont égaux. De même,  $\theta_{\gamma^{-1}} \circ \theta_\gamma = \text{id}_{A[X_1, \dots, X_n]}$ , donc  $\theta_\gamma$  est bien un automorphisme d'anneaux. ✓

**Conséquence 10.5.** L'ensemble  $A[X_1, \dots, X_n]^{S_n}$  des polynômes symétriques est un sous-anneau de  $A[X_1, \dots, X_n]$ .

En effet, on a  $\gamma(f - g) = \gamma f - \gamma g$ ,  $\gamma(fg) = (\gamma f)(\gamma g)$  et  $\gamma 1 = 1$  puisque  $\theta_\gamma$  est un morphisme d'anneaux. En particulier, la somme et le produit de polynômes symétriques sont des polynômes symétriques.

**Remarque.** L'action de  $S_n$  sur  $A[X_1, \dots, X_n]$  induit donc un morphisme de groupes  $\theta: S_n \rightarrow \text{Aut}(A[X_1, \dots, X_n])$  qui à  $\gamma$  associe  $\theta_\gamma$ .

## II. POLYNÔMES SYMÉTRIQUES ÉLÉMENTAIRES

**Définition 10.6.** Soit  $k \in \llbracket 1; n \rrbracket$ . Le polynôme  $\sigma_k = \sum_{\substack{H \subset \llbracket 1; n \rrbracket \\ |H|=k}} \left( \prod_{i \in H} X_i \right)$  de  $A[X_1, \dots, X_n]$  est un polynôme symétrique, appelé *k-ième polynôme symétrique élémentaire*. On pose  $\sigma_0 = 1$ .

**Remarque.** On a  $\deg \sigma_k = k$  (où  $\deg$  désigne le degré total).

On peut écrire  $\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_k}$ .

**Notation.** Lorsqu'il peut y avoir ambiguïté, on écrira  $\sigma_{n,k}$  pour le *k-ième polynôme symétrique élémentaire* en  $X_1, \dots, X_n$  (on précise le nombre d'indéterminées dans la notation).

**Exemples.**  $\triangleright \sigma_1 = X_1 + \dots + X_n$ .

$\triangleright \sigma_2 = X_1 X_2 + X_1 X_3 + \dots + X_1 X_n + X_2 X_3 + \dots + X_{n-1} X_n$ .

$\triangleright \sigma_n = X_1 X_2 \dots X_n$ .

**Lemme 10.7.** Les polynômes symétriques élémentaires sont symétriques.

**Démonstration.** Soit  $\gamma \in S_n$ . Alors

$$\gamma \sigma_k = \sum_{\substack{H \subset \llbracket 1; n \rrbracket \\ |H|=k}} \left( \prod_{i \in H} X_{\gamma(i)} \right) \stackrel{j=\gamma(i)}{=} \sum_{\substack{H \subset \llbracket 1; n \rrbracket \\ |H|=k}} \left( \prod_{j \in \gamma(H)} X_j \right) \stackrel{H'=\gamma^{-1}(H)}{=} \sum_{\substack{H' \subset \llbracket 1; n \rrbracket \\ |H'|=k}} \left( \prod_{j \in H'} X_j \right) = \sigma_k$$

en utilisant la bijection de l'ensemble  $\mathcal{P}_k(\llbracket 1; n \rrbracket)$  des parties de  $\llbracket 1; n \rrbracket$  à *k* éléments dans lui-même définie par  $H \mapsto \gamma(H)$ .  $\checkmark$

**Lemme 10.8.**  $\triangleright$  Soit  $\varphi: A[X_1, \dots, X_{n+1}] \rightarrow A[X_1, \dots, X_n]$  le morphisme du lemme 10.3, défini par  $\varphi(P) = P(X_1, \dots, X_n, 0)$ . Alors  $\varphi(\sigma_{n+1,k}) = \sigma_{n,k}$  pour tout  $k \in \llbracket 0; n \rrbracket$ , autrement dit,  $\sigma_{n,k} = \sigma_{n+1,k}(X_1, \dots, X_n, 0)$ .

$\triangleright$  On a  $\sigma_{n+1,0} = 1$ ,  $\sigma_{n+1,n+1} = \sigma_{n,n} X_{n+1}$  et  $\sigma_{n+1,k} = \sigma_{n,k} + \sigma_{n,k-1} X_{n+1}$  pour tout  $k \in \llbracket 1; n \rrbracket$ .

**Démonstration.** La première partie est évidente (ou se déduit de la deuxième). Pour la deuxième,

on a, pour tout  $k \in \llbracket 1; n \rrbracket$ ,

$$\begin{aligned}
\sigma_{n,k} + \sigma_{n,k-1} X_{n+1} &= \sum_{\substack{H \subset \llbracket 1;n \rrbracket \\ |H|=k}} \left( \prod_{i \in H} X_i \right) + \sum_{\substack{H' \subset \llbracket 1;n \rrbracket \\ |H'|=k-1}} \left( \prod_{i \in H'} X_i \right) X_{n+1} \\
&= \sum_{\substack{H \subset \llbracket 1;n+1 \rrbracket \\ |H|=k \text{ et } n+1 \notin H}} \left( \prod_{i \in H} X_i \right) + \sum_{\substack{H \subset \llbracket 1;n+1 \rrbracket \\ |H|=k \text{ et } n+1 \in H}} \left( \prod_{i \in H} X_i \right) \\
&= \sum_{\substack{H \subset \llbracket 1;n+1 \rrbracket \\ |H|=k}} \left( \prod_{i \in H} X_i \right) = \sigma_{n+1,k}. \quad \checkmark
\end{aligned}$$

### III. STRUCTURE DES POLYNÔMES SYMÉTRIQUES

**Lemme 10.9.** Soit  $P \in A[X_1, \dots, X_n]$  un polynôme symétrique et supposons que  $X_i$  divise  $P$  pour un  $i \in \llbracket 1; n \rrbracket$ . Alors  $\sigma_n$  divise  $P$ .

*Démonstration.* Quitte à permuter les indéterminées (ce qui ne change pas  $P$ ), on peut supposer que  $i = n$ . On raisonne par récurrence sur  $n$ .

➤ Si  $n = 1$ , c'est clair car  $\sigma_{1,1} = X_1$ .

➤ Soit  $n \in \mathbb{N}$ ,  $n > 1$  un entier tel que le résultat est vrai au rang  $n - 1$ . Soit  $P \in A[X_1, \dots, X_n]$  un polynôme symétrique multiple de  $X_n$ . Posons

$$P = P_0 + P_1 X_n + P_2 X_n^2 + \dots + P_d X_n^d$$

avec  $P_i \in A[X_1, \dots, X_{n-1}]$  pour tout  $i$ . Puisque  $P(X_1, \dots, X_{n-1}, 0) = 0$  par hypothèse, on a  $P_0 = 0$ .

Vérifions que les  $P_i$  sont des polynômes symétriques de  $A[X_1, \dots, X_{n-1}]$ . Soit donc  $\gamma \in S_{n-1}$  et soit  $\gamma' \in S_n$  défini par  $\gamma'_{\llbracket 1;n-1 \rrbracket} = \gamma$  et  $\gamma'(n) = n$ . On a alors

$$P = \gamma' P = \sum_{i=1}^d \gamma' P_i (\gamma' X_n)^i = \sum_{i=1}^d \gamma P_i X_n^i$$

donc en identifiant,  $\gamma P_i = P_i$  pour tout  $i$ . Donc  $P_i$  est symétrique.

Soit maintenant  $\tau = (n-1 \ n) \in S_n$ . Alors  $P = {}^\tau P = P(X_1, \dots, X_{n-2}, X_n, X_{n-1})$ . On applique le morphisme  $\varphi$  du lemme 10.3 (ie.  $X_n \mapsto 0$ ). On obtient donc

$$0 = \varphi(P) = P(X_1, \dots, X_{n-2}, 0, X_{n-1}) = \sum_{i=1}^d P_i(X_1, \dots, X_{n-2}, 0) X_{n-1}^i.$$

On en déduit par identification que pour tout  $i \in \llbracket 1; d \rrbracket$  on a  $P_i(X_1, \dots, X_{n-2}, 0) = 0$  dans  $A[X_1, \dots, X_{n-1}]$ . Par hypothèse de récurrence, on sait que  $\sigma_{n-1,n-1} = X_1 \cdots X_{n-1}$  divise  $P_i$  pour tout  $i$ , posons  $P_i = Q_i X_1 \cdots X_{n-1}$  avec  $Q_i \in A[X_1, \dots, X_{n-1}]$ . Alors  $P = \sum_{i=1}^d P_i X_n^i = \sum_{i=1}^d Q_i X_1 \cdots X_{n-1} X_n^i$  est un multiple de  $X_1 \cdots X_n = \sigma_{n,n}$ .  $\checkmark$

**Remarque.** Pour tout polynôme  $P \in A[X_1, \dots, X_n]$ , on a  $\deg(P\sigma_n) = \deg P + n$  (où  $\deg$  désigne le degré total). En particulier, si  $P\sigma_n = 0$  alors  $P = 0$ .

En effet, posons  $P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \cdots X_n^{i_n}$  et  $\deg P = \max\{\sum_{k=1}^n i_k; a_i \neq 0\}$ . On a alors  $P\sigma_n = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1+1} \cdots X_n^{i_n+1}$  donc  $\deg(P\sigma_n) = \max\{\sum_{k=1}^n (i_k + 1); a_i \neq 0\} = \max\{\sum_{k=1}^n i_k + n; a_i \neq 0\} = \deg P + n$ .

Pour tout  $n \in \mathbb{N}^*$ , soit  $\psi_n: A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n]$  le morphisme d'anneaux qui prolonge l'inclusion  $A \hookrightarrow A[X_1, \dots, X_n]$  et tel que  $\psi_n(X_i) = \sigma_i$  pour tout  $i \in \llbracket 1; n \rrbracket$ .

**Proposition 10.10.** Soit  $P \in A[X_1, \dots, X_n]$  un polynôme tel que  $P(\sigma_1, \dots, \sigma_n) = 0$ . Alors  $P = 0$ . Autrement dit,  $\psi_n$  est injectif.

*Démonstration.* On raisonne par récurrence sur  $n$ .

➤ Si  $n = 1$ , le résultat est clair ( $\sigma_1 = X_1$  et  $\psi_1 = \text{id}_{A[X_1]}$ ).  
 ➤ Soit  $n \geq 2$  tel que le résultat soit vrai au rang  $n - 1$ , c'est-à-dire que  $\psi_{n-1}$  est injectif. Supposons par l'absurde que  $\text{Ker}(\psi_n) \neq \{0\}$ . Alors l'ensemble  $\{\deg f \mid f \in \text{Ker}(\psi_n) \setminus \{0\}\}$  est une partie non vide de  $\mathbb{N}$  donc elle admet un minimum  $d_0$ . Soit  $P \in \text{Ker}(\psi_n) \setminus \{0\}$  de degré  $d_0$ . Posons  $P = \sum_{i=0}^d P_i X_n^i$  avec  $P_i \in A[X_1, \dots, X_{n-1}]$ .

Si  $P_0 = 0$  alors  $P = X_n Q$  pour un  $Q \in A[X_1, \dots, X_n]$ . Notons que  $Q \neq 0$ . On a dans ce cas  $0 = P(\sigma_{n,1}, \dots, \sigma_{n,n}) = \sigma_{n,n} Q(\sigma_{n,1}, \dots, \sigma_{n,n})$ . On en déduit que  $\psi_n(Q) = Q(\sigma_{n,1}, \dots, \sigma_{n,n}) = 0$  d'après la remarque précédente. Mais  $\deg Q < d_0$  et  $Q \in \text{Ker}(\psi_n) \setminus \{0\}$ , donc on a obtenu une contradiction.

Par conséquent,  $P_0 \neq 0$  et donc  $P(X_1, \dots, X_{n-1}, 0) = P_0(X_1, \dots, X_{n-1}) \neq 0$ . Par hypothèse de récurrence, on en déduit que  $P_0(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1}) = \psi_{n-1}(P_0) \neq 0$ . Mais en utilisant le lemme 10.8 avec le morphisme  $\varphi: A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_{n-1}]$  défini par  $\varphi(f) = f(X_1, \dots, X_{n-1}, 0)$ , on a

$$\begin{aligned} \psi_{n-1}(P_0) &= P_0(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1}) = P(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1}, 0) \\ &= P(\varphi(\sigma_{n,1}), \dots, \varphi(\sigma_{n,n})) = \varphi(P(\sigma_{n,1}, \dots, \sigma_{n,n})) \quad (\varphi \text{ morphisme d'anneaux}) \\ &= \varphi(\psi_n(P)) = \varphi(0) = 0. \end{aligned}$$

On a donc bien une contradiction, donc  $\text{Ker}(\psi_n) = \{0\}$ . ✓

**Définition 10.11.** Le **poids** d'un monôme  $X_1^{i_1} \cdots X_n^{i_n}$  est l'entier  $i_1 + 2i_2 + 3i_3 + \cdots + ni_n$ .

Le **poids** d'un polynôme est le maximum des poids des monômes qui le constituent : si  $P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \cdots X_n^{i_n}$ , le poids de  $P$  est  $\max\{\text{poids}(X_1^{i_1} \cdots X_n^{i_n}) \mid a_i \neq 0\} = \max\{i_1 + 2i_2 + 3i_3 + \cdots + ni_n \mid a_i \neq 0\}$ .

**Exemple.** Le polynôme  $P = X_1 + X_1 X_2^2 + X_1 X_3$  est de poids  $\max(1, 5, 4) = 5$ .

**Remarque.** Le degré de  $P(\sigma_1, \dots, \sigma_n)$  est inférieur ou égal au poids de  $P$ , soit  $\deg(\psi_n(P)) \leq \text{poids}(P)$ .

Vérifions d'abord cela dans le cas où  $P = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$  est un monôme. On a  $\deg P(\sigma_1, \dots, \sigma_n) = \alpha_1 \deg \sigma_1 + \cdots + \alpha_n \deg \sigma_n = \sum_{i=1}^n \alpha_i i$  qui est bien le poids de  $P$  (on a égalité car tous les coefficients des polynômes  $\sigma_k$  sont inversibles).

Soit maintenant  $P = \sum_{j=1}^r a_j M_j$  un polynôme non nul où les  $M_j$  sont des monômes et les  $a_j$  sont des éléments non nuls de  $A$ . Par définition,  $\text{poids}(P) = \max\{\text{poids}(M_j) \mid 1 \leq j \leq r\}$ . On a alors

$$\begin{aligned} \deg P(\sigma_1, \dots, \sigma_n) &= \deg \left( \sum_{j=1}^r a_j M_j(\sigma_1, \dots, \sigma_n) \right) \leq \max\{\deg M_j(\sigma_1, \dots, \sigma_n) \mid 1 \leq j \leq r\} \\ &= \max\{\text{poids}(M_j) \mid 1 \leq j \leq r\} \\ &= \text{poids}(P). \end{aligned}$$

**Remarque.** Pour tout  $P \in A[X_1, \dots, X_n]$  et tout  $\lambda \in S_n$ , on a  $\theta_\lambda(\psi_n(P)) = P(\theta_\lambda(\sigma_1), \dots, \theta_\lambda(\sigma_n)) = P(\sigma_1, \dots, \sigma_n) = \psi_n(P)$ , donc  $\text{Im}(\psi_n) \subset A[X_1, \dots, X_n]^{S_n}$ .

Nous allons voir qu'il y a égalité.

**Théorème 10.12.** Soit  $A$  un anneau. Soit  $P \in A[X_1, \dots, X_n]$  un polynôme symétrique. Alors il existe un unique polynôme  $T \in A[Y_1, \dots, Y_n]$  tel que  $T(\sigma_1, \dots, \sigma_n) = P$ , autrement dit,  $\psi_n: A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n]^{S_n}$  est un isomorphisme d'anneaux. Ce polynôme  $T$  est de poids  $d = \deg(P)$ .

**Exemple.** ➤ Si  $P = X_1^2 + X_2^2 \in \mathbb{Z}[X_1, X_2]$ , on a  $P = (X_1 + X_2)^2 - 2X_1X_2 = \sigma_1^2 - 2\sigma_2$ . Le polynôme  $T$  est donc  $T = Y_1^2 - 2Y_2$ .

➤ Si  $P = X_1^3X_2 + X_1X_2^3 \in \mathbb{Z}[X_1, X_2]$ , on a  $P = X_1X_2(X_1^2 + X_2^2) = \sigma_2(\sigma_1^2 - 2\sigma_2)$  et  $T = Y_1^2Y_2 - 2Y_2^2$ .

*Démonstration.* Admise en 2022-2023 et en 2023-2024.

L'unicité de  $T$  (ou l'injectivité de  $\psi_n$ ) découle de la proposition 10.10.

Démontrons l'existence (ou  $A[X_1, \dots, X_n]^{S_n} \subset \text{Im}(\psi_n)$ ).

On raisonne par récurrence sur  $n$  (le nombre d'indéterminées).

➤ Si  $n = 1$ , le résultat est évident, car  $\psi_1 = \text{id}_{A[X_1]}$  et  $A[X_1]^{S_1} = A[X_1]$ .

➤ Soit  $n > 1$  tel que  $\text{Im}(\psi_{n-1}) = A[X_1, \dots, X_{n-1}]^{S_{n-1}}$ .

On fait maintenant un raisonnement par récurrence sur le degré total  $d$  des polynômes.

➤ Si  $P$  est un polynôme (symétrique) de degré total  $d = 0$ , il est évident que  $P \in \text{Im}(\psi_n)$  (car  $P$  est constant).

➤ Soit  $d > 0$  tel que tous les polynômes de  $A[X_1, \dots, X_n]^{S_n}$  de degré total inférieur ou égal à  $(d-1)$  soient dans  $\text{Im}(\psi_n)$ .

Soit  $P \in A[X_1, \dots, X_n]$  un polynôme symétrique de degré total  $d \in \mathbb{N}$ .

Soit  $\varphi$  le morphisme du lemme 10.3. Puisque le polynôme  $\varphi(P)$  est un polynôme symétrique de  $A[X_1, \dots, X_{n-1}]$ , par hypothèse de récurrence (sur  $n$ ), il existe un unique polynôme  $V \in A[Y_1, \dots, Y_{n-1}]$  de poids inférieur ou égal à  $d$  tel que  $\varphi(P) = \psi_{n-1}(V) = V(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1})$ .

Posons  $\tilde{P} = V(\sigma_{n,1}, \dots, \sigma_{n,n-1})$  (on a remplacé les  $\sigma_{n-1,k}$  par les  $\sigma_{n,k}$  correspondant). Notons que  $\deg \tilde{P} \leq \text{poids}(V) \leq d$ . Alors  $\tilde{P}$  est un polynôme symétrique de  $A[X_1, \dots, X_n]$  et on a  $\varphi(P - \tilde{P}) = 0$  donc  $X_n$  divise  $P - \tilde{P}$  dans  $A[X_1, \dots, X_n]$ . On en déduit grâce au lemme 10.9 que  $\sigma_{n,n}$  divise  $P - \tilde{P}$ .

Posons  $P - \tilde{P} = Q\sigma_{n,n}$ . Alors  $Q$  est symétrique; en effet, si  $\gamma \in S_n$ , alors  $({}^\gamma Q)\sigma_{n,n} = {}^\gamma(Q\sigma_{n,n}) = {}^\gamma(P - \tilde{P}) = P - \tilde{P} = Q\sigma_{n,n}$  et on en déduit que  ${}^\gamma Q = Q$  (cf. remarque p. 125).

De plus,  $\deg Q = \deg(Q\sigma_{n,n}) - n = \deg(P - \tilde{P}) - n \leq d - n < d$  donc, par hypothèse de récurrence (sur  $d$ ), il existe un unique polynôme  $W \in A[Y_1, \dots, Y_n]$  tel que  $Q = \psi_n(W) = W(\sigma_{n,1}, \dots, \sigma_{n,n})$  et le poids de  $W$  est  $\deg Q$ .

Posons enfin  $T = V + WY_n$ . On a  $\psi_n(T) = T(\sigma_{n,1}, \dots, \sigma_{n,n}) = V(\sigma_{n,1}, \dots, \sigma_{n,n}) + W(\sigma_{n,1}, \dots, \sigma_{n,n})\sigma_{n,n} = \tilde{P} + Q\sigma_{n,n} = P$ . On a donc démontré l'existence.

On a de plus  $\text{poids}(T) \leq \max(\text{poids}(V), n + \text{poids}(W)) \leq d$  et si  $\text{poids}(T) < d$  alors  $d = \deg P = \deg(\psi_n(T)) \leq \text{poids}(T) < d$ , une contradiction. On en déduit donc que  $\text{poids}(T) = d = \deg P$ . ✓

**Définition 10.13.** Un polynôme  $f \in A[X_1, \dots, X_n]$  est dit **homogène** si tous ses monômes sont de même degré. Ce degré commun est nécessairement le degré total de  $f$ , on l'appelle **degré** du polynôme homogène  $f$ .

**Remarques.** ➤ Tout polynôme  $f$  s'écrit de manière unique comme somme de polynômes homogènes, que l'on appelle **composantes homogènes** de  $f$ .

En effet, soit  $f_i$  la somme de tous les termes monomiaux de  $f$  de degré total  $i$ . Alors  $f_i$  est homogène de degré  $i$  ou nul et  $f = \sum_{i \in \mathbb{N}} f_i$  (somme finie). De plus, s'il existe des

polynômes homogènes  $g_i$ ,  $i \in \mathbb{N}$ , qui sont tous nuls sauf un nombre fini d'entre eux, avec  $\deg g_i = i$  et  $f = \sum_{i \in \mathbb{N}} g_i$ , alors  $\sum_{i \in \mathbb{N}} (f_i - g_i) = 0$  avec  $f_i - g_i$  homogène de degré  $i$ . Si  $i \neq j$ , les termes monomiaux qui apparaissent dans  $f_i - g_i$  ne sont pas dans  $f_j - g_j$  (puisqu'ils sont de degrés différents). Par unicité de l'écriture d'un polynôme comme somme de termes monomiaux, on en déduit que  $f_i - g_i = 0$  pour tout  $i$ .

- Si  $f$  est un polynôme symétrique, alors ses composantes homogènes sont symétriques.  
En effet, posons  $f = \sum_{i=1}^r f_i$  avec  $f_i$  homogènes de degrés deux à deux distincts. Soit  $\gamma \in S_n$ . Alors  $\sum_{i=1}^r f_i = f = \gamma f = \sum_{i=1}^r \gamma f_i$  avec  $\gamma f_i$  homogène de degré  $i$ , donc pour tout  $i$  on a  $\gamma f_i = f_i$  par unicité des composantes homogènes de  $f$ .
- Pour tout  $k$ , le polynôme  $\sigma_k$  est homogène de degré  $k$  et de degré partiel 1.

**Remarque.** Dans la pratique, afin de simplifier les calculs, avant d'appliquer la méthode de la démonstration pour trouver  $T$ , on écrit  $P$  comme somme de polynômes homogènes et on applique la méthode à chaque composante homogène.

On suit alors la procédure suivante pour un polynôme homogène  $P$  :

- (i) On calcule  $\varphi(P)$  et on trouve  $V \in A[Y_1, \dots, Y_{n-1}]$  tel que  $\varphi(P) = V(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1})$  en suivant la procédure récursive (on recommence jusqu'à n'avoir qu'une indéterminée ou avoir une expression en les polynômes symétriques élémentaires).
- (ii) On détermine  $Q \in A[X_1, \dots, X_n]$  symétrique tel que  $P - V(\sigma_{n,1}, \dots, \sigma_{n,n-1}) = Q\sigma_{n,n}$ .
- (iii) On trouve  $W \in A[Y_1, \dots, Y_n]$  tel que  $Q = W(\sigma_{n,1}, \dots, \sigma_{n,n})$  par la procédure récursive.
- (iv) On pose  $T = V + WY_n$ .

**Exemples. (1)**  $P = XYZ + X^2Y + X^2Z + Y^2Z + XY^2 + XZ^2 + YZ^2$ . Soit  $\varphi_Z: A[X, Y, Z] \rightarrow A[X, Y]$  le morphisme d'anneaux donné par  $\varphi_Z(P) = P(X, Y, 0)$ .

- ◆ On a  $\varphi_Z(P) = X^2Y + XY^2 = XY(X + Y) = \sigma_{2,2}\sigma_{2,1}$  (autrement dit,  $V = XY$ ).
- ◆ On considère  $P - V(\sigma_{3,1}, \sigma_{3,2}) = P - (X + Y + Z)(XY + XZ + YZ) = -2XYZ = -2\sigma_{3,3}$  (autrement dit,  $Q = -2$ ).
- ◆ On pose  $T = V + QZ$  et on a bien  $P = T(\sigma_{3,1}, \sigma_{3,2}, \sigma_{3,3}) = \sigma_{3,1}\sigma_{3,2} - 2\sigma_{3,3}$ .

**(2)**  $P = X_1^3 + X_2^3 + X_3^3$ . On note  $\varphi_3: A[X_1, X_2, X_3] \rightarrow A[X_1, X_2]$  et  $\varphi_2: A[X_1, X_2] \rightarrow A[X_1]$  les morphismes d'anneaux du lemme 10.3.

- ◆ On a  $\varphi_3(P) = X_1^3 + X_2^3$ .
  - ✧ On a  $\varphi_2(\varphi_3(P)) = X_1^3 = \sigma_{1,1}^3$ .
  - ✧  $\varphi_3(P) - \sigma_{2,1}^3 = (X_1^3 + X_2^3) - (X_1 + X_2)^3 = -3X_1^2X_2 - 3X_1X_2^2 = -3(X_1 + X_2)\sigma_{2,2} = -3\sigma_{2,1}\sigma_{2,2}$  donc  $\varphi_3(P) = \sigma_{2,1}^3 - 3\sigma_{2,1}\sigma_{2,2}$ .
  - ✧  $P - (\sigma_{3,1}^3 - 3\sigma_{3,1}\sigma_{3,2}) = 3X_1X_2X_3 = 3\sigma_{3,3}$  (d'où  $Q = 3$ ).
- ◆ Donc  $P = \sigma_{3,1}^3 - 3\sigma_{3,1}\sigma_{3,2} + 3\sigma_{3,3} = T(\sigma_{3,1}, \sigma_{3,2}, \sigma_{3,3})$  avec  $T = X_1^3 - 3X_1X_2 + 3X_3$ .

Notons que le poids de  $T$  est bien  $3 = \deg P$ .

On peut résumer nos résultats.

**Théorème 10.14.** L'endomorphisme d'anneaux  $\psi_n$  de  $A[X_1, \dots, X_n]$  qui à  $P$  associe  $P(\sigma_1, \dots, \sigma_n)$  obtenu grâce à la propriété universelle des anneaux de polynômes est injectif et a pour image le sous-anneau des polynômes symétriques.

## A. Racines dans un sur-corps

Nous aurons besoin du résultat suivant, dont vous verrez des versions plus précises si vous suivez l'option Théorie des corps au S2.

**Proposition 10.15.** Soit  $K$  un corps et soit  $P \in K[X]$  un polynôme non constant. Alors

- (1) Il existe un corps  $L$  dont  $K$  est un sous-corps et tel que  $P$  a une racine dans  $L$ .
- (2) Il existe un corps  $L$  dont  $K$  est un sous-corps et tel que  $P$  est scindé dans  $L[X]$ , c'est-à-dire qu'il peut s'écrire comme un produit de polynômes de degré 1 de  $L[X]$ .

*Remarque.* Notons que si  $A$  est intègre, on sait qu'il a un corps des fractions. Comme  $P \in \text{Frac}(A)[X]$ , on a vu dans la proposition [?] qu'il existe un corps  $K$ , contenant  $\text{Frac}(A)$  et donc  $A$ , sur lequel  $P$  est scindé.

*Démonstration.* (1) Supposons dans un premier temps que  $P$  est irréductible dans  $K[X]$ .

Puisque  $K[X]$  est un anneau principal, l'idéal  $(P)$  est maximal, donc  $L := K[X]/(P)$  est un corps. De plus,  $K$  s'identifie à un sous-corps de  $L$  par le biais du morphisme d'anneaux  $K \hookrightarrow K[X] \twoheadrightarrow L$  composé de l'injection naturelle et de la projection canonique sur le quotient; ce morphisme est nécessairement injectif car il n'est pas nul ( $P$  n'est pas constant) et son noyau est un idéal du corps  $K$ . Enfin, notons  $x$  la classe de  $X$  dans  $L$ . Alors  $P(x) = \overline{P(X)} = 0$  donc  $x$  est une racine de  $P$  dans  $L$ .

Si maintenant  $P$  n'est pas irréductible dans  $K[X]$ , soit  $Q$  un facteur irréductible de  $P$ . Il existe alors un corps  $L$  dont  $K$  est un sous-corps dans lequel  $Q$  a une racine  $\alpha$ . Puisque  $\alpha$  est aussi une racine de  $P$ , on a le résultat.

- (2) On raisonne par récurrence sur le degré  $d > 0$  de  $P$ . Si  $d = 1$ , il suffit de prendre  $L = K$ .

Soit donc  $d > 1$  tel que le résultat est vrai pour les polynômes à coefficients dans un corps quelconque et de degré au plus  $d - 1$ . Soit  $P \in K[X]$  un polynôme de degré  $d$ . D'après la première partie, il existe un corps  $K'$  dont  $K$  est un sous-corps et dans lequel  $P$  a une racine  $\alpha$ . Ainsi, dans  $K'[X]$  on a  $P = (X - \alpha)Q$ . Or  $Q \in K'[X]$  est de degré  $d - 1$  donc il existe un corps  $L$  dont  $K'$  est un sous-corps et tel que  $Q$  est scindé dans  $L[X]$ . Mais alors  $K$  est un sous-corps de  $L$  et  $P = (X - \alpha)Q$  est scindé dans  $L[X]$ . Donc le résultat est vrai pour les polynômes de degré  $d$ . ✓

## B. Relation coefficients-racines

**Théorème 10.16.** Dans l'anneau  $A[X_1, \dots, X_n, T]$  on a

$$\prod_{i=1}^n (T - X_i) = \sum_{k=0}^n (-1)^{n-k} \sigma_{n-k} T^k.$$

*Démonstration.* On raisonne par récurrence sur  $n$ .

➤ Pour  $n = 1$ , on a  $P = (T - X_1) = \sigma_{1,0}T + (-1)^1\sigma_{1,1}$ .

➤ Soit  $n \in \mathbb{N}^*$  tel que le résultat soit vrai au rang  $n$ . Soit  $P = \prod_{i=1}^{n+1} (T - X_i)$ . Par hypothèse

de récurrence, on a

$$\begin{aligned}
P &= \left( \prod_{i=1}^n (T - X_i) \right) (T - X_{n+1}) = \left( \sum_{k=0}^n (-1)^{n-k} \sigma_{n,n-k} T^k \right) (T - X_{n+1}) \\
&= \sum_{k=0}^n (-1)^{n-k} \sigma_{n,n-k} T^{k+1} - \sum_{k=0}^n (-1)^{n-k} \sigma_{n,n-k} X_{n+1} T^k \\
&= \sum_{k=1}^{n+1} (-1)^{n+1-k} \sigma_{n,n+1-k} T^k + \sum_{k=0}^n (-1)^{n+1-k} \sigma_{n,n-k} X_{n+1} T^k \\
&= \sigma_{n,0} T^{n+1} + \sum_{k=1}^n (-1)^{n+1-k} (\sigma_{n,n+1-k} + \sigma_{n,n-k} X_{n+1}) T^k + (-1)^{n+1} \sigma_{n,n} X_{n+1} \\
&= \sum_{k=0}^{n+1} (-1)^{n+1-k} \sigma_{n+1,n+1-k} T^k
\end{aligned}$$

en utilisant le lemme 10.8 pour la dernière ligne. ✓

**Corollaire 10.17** (Relations coefficients/racines). Soit  $P = \sum_{i=0}^n a_i X^i \in A[X]$  un polynôme avec  $a_n \in A^\times$ , et soient  $\beta_1, \dots, \beta_n$  les racines de  $P$ , dans  $A$  ou dans un corps  $K$  contenant  $A$  (dans le cas où  $A$  est intègre). Alors, pour tout  $k \in \llbracket 0; n \rrbracket$ , on a

$$\sigma_k(\beta_1, \dots, \beta_n) = (-1)^k a_{n-k} a_n^{-1}.$$

En particulier,  $\sigma_k(\beta_1, \dots, \beta_n) \in A$ .

*Démonstration.* On a  $a_n^{-1} P = (X - \beta_1) \cdots (X - \beta_n) = X^n - \tilde{\sigma}_1 X^{n-1} + \tilde{\sigma}_2 X^{n-2} + \cdots + (-1)^n \tilde{\sigma}_n$  d'après le théorème, où  $\tilde{\sigma}_k = \sigma_k(\beta_1, \dots, \beta_n)$ . Le résultat s'en déduit par identification. ✓

**Remarque.** Pour  $n = 2$ , on retrouve le résultat très classique  $(X - \beta_1)(X - \beta_2) = X^2 - \sigma_1 X + \sigma_2$  où  $\sigma_1$  est la somme des racines et  $\sigma_2$  est leur produit.

**Exemple.** Soit  $P = X^4 + 12X - 5$ . Déterminons ses racines dans  $\mathbb{C}$ , sachant que la somme de deux d'entre elles est égale à 2.

Notons  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  les racines de  $P$  dans  $\mathbb{C}$ , avec par exemple  $\alpha_1 + \alpha_2 = 2$ . On a alors

$$\begin{cases} 0 = \sigma_1 = 2 + \alpha_3 + \alpha_4 \\ 0 = \sigma_2 = \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_1 \alpha_4 + \alpha_2 \alpha_3 + \alpha_2 \alpha_4 + \alpha_3 \alpha_4 \\ -12 = \sigma_3 = \alpha_1 \alpha_2 \alpha_3 + \alpha_1 \alpha_2 \alpha_4 + \alpha_1 \alpha_3 \alpha_4 + \alpha_2 \alpha_3 \alpha_4 \\ -5 = \sigma_4 = \alpha_1 \alpha_2 \alpha_3 \alpha_4 \end{cases}$$

où  $\sigma_k$  désigne le  $k^{\text{ième}}$  polynôme symétrique élémentaire en les  $\alpha_i$ .

Posons  $p = \alpha_1 \alpha_2$ ,  $s = \alpha_1 + \alpha_2 = 2$ ,  $q = \alpha_3 \alpha_4$  et  $t = \alpha_3 + \alpha_4$ . On a alors

$$\begin{cases} s = 2 \\ s + t = 0 \\ p + \alpha_1 t + \alpha_2 t + q = 0 \\ pt + sq = -12 \\ pq = -5 \end{cases} \iff \begin{cases} s = 2 \\ t = -2 \\ p + st + q = 0 \\ 2(q - p) = -12 \\ pq = -5 \end{cases} \iff \begin{cases} s = 2 \\ t = -2 \\ p + q = 4 \\ p - q = 6 \\ pq = -5 \end{cases} \iff \begin{cases} s = 2 \\ t = -2 \\ p = 5 \\ q = -1. \end{cases}$$

Or  $\alpha_1$  et  $\alpha_2$  sont les deux racines de  $X^2 - sX + p = X^2 - 2X + 5$  et  $\alpha_3$  et  $\alpha_4$  sont les deux racines de  $X^2 - tX + q = X^2 + 2X - 1$ .

On en déduit finalement que les racines de  $P$  sont  $1 \pm 2i$  et  $-1 \pm \sqrt{2}$ .

## C. Application : Théorème de d'Alembert-Gauss

Nous allons utiliser les polynômes symétriques pour démontrer le théorème de d'Alembert-Gauss.

**Théorème 10.18** (Théorème de d'Alembert-Gauss). Soit  $P \in \mathbb{C}[X]$  un polynôme non constant. Alors  $P$  a une racine dans  $\mathbb{C}$ .

*Démonstration.* Soit  $P \in \mathbb{C}[X]$  un polynôme non constant. Nous devons démontrer que  $P$  a une racine dans  $\mathbb{C}$ .

Remarquons que  $\overline{P}P \in \mathbb{R}[X]$  (où  $\overline{P}$  désigne le conjugué de  $P$ ). De plus, si  $P$  a une racine dans  $\mathbb{C}$  alors  $\overline{P}P$  aussi et si  $\overline{P}P$  a une racine dans  $\mathbb{C}$ , alors soit  $P$  a une racine dans  $\mathbb{C}$  soit  $\overline{P}$  a une racine  $\alpha \in \mathbb{C}$  mais alors  $\overline{\alpha} \in \mathbb{C}$  est une racine de  $P$ . Ainsi,  $P$  a une racine complexe si, et seulement si,  $\overline{P}P$  a une racine complexe et on peut donc supposer que  $P \in \mathbb{R}[X]$ . De plus, quitte à multiplier par l'inverse du coefficient dominant, on peut supposer que  $P$  est unitaire.

Posons  $\deg P = d = 2^n q$  avec  $q$  impair. On va raisonner par récurrence sur  $n \in \mathbb{N}$ .

➤ Si  $n = 0$ , alors  $P$  est de degré impair et il a une racine réelle d'après le théorème des valeurs intermédiaires.

➤ Soit  $n \geq 1$  tel que le résultat est vrai pour les polynômes de degré  $2^{n-1}q'$  avec  $q'$  impair. Soit  $P$  un polynôme unitaire de  $\mathbb{R}[X]$  de degré  $2^n q$  avec  $q$  impair.

Il existe un corps  $L$  dont  $\mathbb{C}$  est un sous-corps et sur lequel  $P$  est scindé : on a donc  $P = (X - \alpha_1) \cdots (X - \alpha_d)$  avec  $\alpha_j \in L$  pour tout  $j \in \llbracket 1; d \rrbracket$ . On doit démontrer que l'un au moins des  $\alpha_j$  est dans  $\mathbb{C}$ .

Notons  $\sigma_1, \dots, \sigma_d$  les polynômes symétriques élémentaires en  $X_1, \dots, X_d$  et posons  $\tilde{\sigma}_k = \sigma_k(\alpha_1, \dots, \alpha_d)$ . D'après les relations coefficients-racines, pour tout  $k$  on a  $\tilde{\sigma}_k \in \mathbb{R}$ .

Pour tout  $(i, j) \in \llbracket 1; n \rrbracket$  et tout  $c \in \mathbb{R}$ , on pose  $\beta_{ij}^{(c)} = \alpha_i + \alpha_j + c\alpha_i\alpha_j \in L$ ; nous allons démontrer que pour tout  $c \in \mathbb{R}$ , l'un des  $\beta_{ij}^{(c)}$  est dans  $\mathbb{C}$ . Pour cela, on considère les polynômes

$$\tilde{Q}_c = \prod_{1 \leq i < j \leq d} (X - \beta_{ij}^{(c)}) \in L[X], \quad c \in \mathbb{R}.$$

On a  $\tilde{Q}_c = Q_c(\alpha_1, \dots, \alpha_d)$  où  $Q_c = \prod_{1 \leq i < j \leq d} (X - X_i - X_j - cX_iX_j) \in \mathbb{R}[X][X_1, \dots, X_d]$ . Le polynôme  $Q_c$  est un polynôme symétrique en  $X_1, \dots, X_d$ , donc il existe un polynôme  $T \in \mathbb{R}[X][X_1, \dots, X_d]$  tel que  $Q_c = T(\sigma_1, \dots, \sigma_d)$ . On en déduit que  $\tilde{Q}_c = T(\tilde{\sigma}_1, \dots, \tilde{\sigma}_d) \in \mathbb{R}[X]$  puisque les  $\tilde{\sigma}_k$  sont réels.

De plus,  $\deg \tilde{Q}_c = |\{(i, j) \in \llbracket 1; d \rrbracket^2 \mid i < j\}| = \sum_{i=1}^{d-1} (d-i) = \frac{d(d-1)}{2} = 2^{n-1}q'$  avec  $q' = q(d-1)$  impair. Donc d'après l'hypothèse de récurrence  $\tilde{Q}_c$  a une racine  $\gamma_c$  dans  $\mathbb{C}$ .

Par conséquent, pour tout  $c \in \mathbb{R}$ , il existe  $(i(c), j(c)) \in \llbracket 1; d \rrbracket^2$  tel que  $\gamma_c = \beta_{i(c)j(c)}^{(c)} = \alpha_{i(c)} + \alpha_{j(c)} + c\alpha_{i(c)}\alpha_{j(c)} \in \mathbb{C}$ .

Puisque  $\mathbb{R}$  est infini et que les indices  $(i(c), j(c))$  parcourent un ensemble fini, il existe des nombres réels  $c_1 \neq c_2$  tels que  $(i(c_1), j(c_1)) = (i(c_2), j(c_2))$ . Notons  $r = i(c_1) = i(c_2)$  et  $s = j(c_1) = j(c_2)$ . Alors  $\gamma_{c_1} = \alpha_r + \alpha_s + c_1\alpha_r\alpha_s \in \mathbb{C}$  et  $\gamma_{c_2} = \alpha_r + \alpha_s + c_2\alpha_r\alpha_s \in \mathbb{C}$ . Posons  $u = \alpha_r + \alpha_s$  et  $v = \alpha_r\alpha_s$ . Alors  $(c_1 - c_2)v = \gamma_{c_1} - \gamma_{c_2} \in \mathbb{C}$  donc  $v \in \mathbb{C}$  et  $u = \gamma_{c_1} - c_1v \in \mathbb{C}$ . De plus,  $\alpha_r$  et  $\alpha_s$  sont les racines de  $X^2 - uX + v \in \mathbb{C}[X]$ , et l'on sait que ces racines sont complexes.

On a donc démontré que les racines  $\alpha_r$  et  $\alpha_s$  de  $P$  sont dans  $\mathbb{C}$ , donc  $P$  a bien une racine complexe. ✓

Soit  $K$  un corps. Soit  $(t_1, \dots, t_n) \in K^n$ . Soit  $P = (X - t_1)(X - t_2) \cdots (X - t_n) \in K[X]$ .

**Définition 10.19.** On appelle **discriminant** de  $P$  le produit  $\text{Disc}(P) = \prod_{1 \leq i < j \leq n} (t_i - t_j)^2$ .

$\text{Disc}(P)$  est un polynôme symétrique en  $t_1, \dots, t_n$  car tout  $\gamma \in S_n$  agit sur  $\prod_{i < j} (t_i - t_j)$  en multipliant par  $\pm 1$ . C'est donc un polynôme en les  $\sigma_i$ , où on note  $\sigma_i = \sigma_i(t_1, \dots, t_n)$ .

**Exemples. (1)** Pour  $\deg P = 2$ , si  $P = X^2 + bX + c$  alors  $\text{Disc}(P) = (t_1 - t_2)^2 = (t_1 + t_2)^2 - 4t_1t_2 = \sigma_1^2 - 4\sigma_2 = b^2 - 4c$ .

En effet, le lien coefficients-racines nous permet de dire que  $\sigma_1 = -b$  et  $\sigma_2 = c$ .

**(2)** Pour  $\deg P = 3$  et  $P = X^3 + aX + b$ , on a  $\text{Disc}(P) = -4a^3 - 27b^2$ .

*Démonstration.* On peut raisonner comme pour les polynômes de degré 2 (mais les calculs sont bien plus longs et compliqués). On peut aussi raisonner de façon plus théorique.

Notons  $P = (X - t_1)(X - t_2)(X - t_3)$ . On a  $\sigma_1 = \sigma_1(t_1, t_2, t_3) = 0$ ,  $\sigma_2 = \sigma_2(t_1, t_2, t_3) = a$  et  $\sigma_3 = \sigma_3(t_1, t_2, t_3) = -b$ . Le polynôme  $\text{Disc}(P) \in K[t_1, t_2, t_3]$  est homogène de degré 6, donc il existe un polynôme  $T \in K[Y_1, Y_2, Y_3]$  de poids 6 tel que  $\text{Disc}(P) = T(\sigma_1, \sigma_2, \sigma_3)$ . Puisque  $\sigma_1 = 0$ , on cherche  $T \in K[Y_2, Y_3]$ .

Un monôme  $Y_2^m Y_3^n$  est de poids  $2m + 3n$ , donc il est de poids 6 si et seulement si  $(m, n) \in \{(0, 2), (3, 0)\}$ . Ainsi,  $T = \lambda Y_2^3 + \mu Y_3^2$  et  $\text{Disc}(P) = T(\sigma_1, \sigma_2, \sigma_3) = \lambda \sigma_2^3 + \mu \sigma_3^2 = \lambda a^3 + \mu b^2$ .

Ceci est vrai pour tout polynôme  $P$  de la forme  $P = X^3 + aX + b$ , c'est-à-dire que  $\lambda$  et  $\mu$  ne dépendent pas de  $a$  et  $b$  (on n'a utilisé que le fait que  $\sigma_1 = 0$  pour donner  $T$ , pas les valeurs de  $\sigma_2$  et  $\sigma_3$ ). On va donc spécialiser à des polynômes particuliers.

♦ Soit  $P = X^3 - X = X(X - 1)(X + 1)$ . On a alors  $\text{Disc}(P) = ((0 - (-1))(0 - 1)(-1 - (-1)))^2 = 4$  donc, puisqu'ici  $a = -1$  et  $b = 0$ , on a  $-\lambda = 4$  d'où  $\lambda = -4$ .

♦ Soit  $P = X^3 - 1 = (X - 1)(X - j)(X - j^2)$  avec  $j = e^{2i\pi/3}$ . On a alors  $\text{Disc}(P) = ((1 - j)(1 - j^2)(j - j^2))^2 = -27$  donc, puisqu'ici  $a = 0$  et  $b = -1$ , on a  $\mu = -27$ .

Finalement,  $\text{Disc}(P) = -4a^3 - 27b^2$ . ✓

**Exercice 10.20.** Faire le cas  $\deg P = 3$  en général. [Indication : Si  $P = X^3 + aX^2 + bX + c$ , faire le changement d'indéterminée  $Y = X + \frac{a}{3}$ .]

*Correction.* Notons que le changement d'indéterminée  $Y = X + \frac{a}{3}$  ne change pas le discriminant; en effet, si  $P = \prod_{i=1}^3 (X - t_i)$  il a pour discriminant  $\prod_{1 \leq i < j \leq 3} (t_i - t_j)^2$  et alors  $P(X) = \prod_{i=1}^3 (Y - (t_i + \frac{a}{3}))$  a pour discriminant  $\prod_{1 \leq i < j \leq 3} ((t_i + \frac{a}{3}) - (t_j + \frac{a}{3}))^2 = \prod_{1 \leq i < j \leq 3} (t_i - t_j)^2$ .

De plus,  $P(X) = (Y - \frac{a}{3})^3 + a(Y - \frac{a}{3})Y^2 + b(Y - \frac{a}{3}) + c = Y^3 + pY + q$  avec  $p = b - \frac{a^2}{3}$  et  $q = c - \frac{ab}{3} + \frac{2a^3}{27}$ . On a retrouvé la forme précédente, donc le discriminant est  $-4p^3 - 27q^2 = a^2b^2 - 4b^3 - 4a^3c - 27c^3 + 18abc$ . ✓

**Proposition 10.21.** Si  $P$  est scindé dans  $K[X]$ , alors  $P$  n'a que des racines simples si, et seulement si,  $\text{Disc}(P) \neq 0$ .

*Démonstration.* Evident. ✓

# Annexes sur les anneaux

## I. COMPLÉMENT SUR LE LEMME DE ZORN

Le lemme de Zorn est utilisé pour faire certaines démonstrations où une récurrence est impossible (si l'ensemble d'indices n'est pas dénombrable). Il est équivalent à l'axiome du choix (indépendant des autres axiomes, Cohen 1963). Vous le verrez également dans le cours de topologie.

Nous allons démontrer que l'axiome du choix est équivalent au lemme de Zorn et au théorème de Zermelo.

### a Définitions, notations, énoncés

**Axiome du choix** (Formulation 1). Le produit d'une famille non vide d'ensembles non vides n'est pas vide.

Autrement dit, si  $(A_i)_{i \in I}$  est une famille non vide d'ensembles non vides, on peut choisir simultanément  $x_i \in A_i$  pour tout  $i \in I$ .

**Axiome du choix** (Formulation 2). Soit  $E$  un ensemble non vide et soit  $\mathcal{P}^*(E)$  l'ensemble des parties non vides de  $E$ . Alors il existe une **fonction de choix** sur  $E$ , c'est-à-dire une application  $\tau: \mathcal{P}^*(E) \rightarrow E$  telle que, pour tout  $X \in \mathcal{P}^*(E)$  on ait  $\tau(X) \in X$ .

**Axiome du choix** (Formulation 3). Soient  $E$  et  $F$  deux ensembles avec  $F \neq \emptyset$  et soit  $f: E \rightarrow F$  une application surjective. Alors il existe une application  $s: F \rightarrow E$  telle que  $f \circ s = \text{id}_F$  (appelée **section** de  $f$ ).

### Equivalence des trois versions.

- (Formulation 1  $\Rightarrow$  Formulation 2). On suppose que tout produit d'une famille non vide d'ensembles non vides n'est pas vide. Soit  $E$  un ensemble non vide et soit  $A = \prod_{X \in \mathcal{P}^*(E)} X$ . Par hypothèse,  $A$  n'est pas vide donc il existe  $(a_X)_{X \in \mathcal{P}^*(E)} \in A$ , où  $a_X \in X$  pour tout  $X \in \mathcal{P}^*(E)$ . On définit alors  $\tau: \mathcal{P}^*(E) \rightarrow E$  par  $\tau(X) = a_X \in X \subset E$  pour tout  $X \in \mathcal{P}^*(E)$ .
- (Formulation 2  $\Rightarrow$  Formulation 3). On suppose que pour tout ensemble non vide  $G$ , il existe une fonction de choix sur  $G$ . Soit  $f: E \rightarrow F$  une surjection entre deux ensembles non vides. Pour tout  $y \in F$ , l'ensemble  $f^{-1}(\{y\})$  n'est pas vide car  $f$  est surjective. Soit  $G$  la réunion des  $f^{-1}(\{y\})$  pour  $y \in F$  et soit  $\tau$  une fonction de choix sur  $G$ . Alors, pour tout  $y \in F$ , on a  $\tau(f^{-1}(\{y\})) \in f^{-1}(\{y\})$ . On définit  $s: F \rightarrow E$  par  $s(y) = \tau(f^{-1}(\{y\}))$  pour tout  $y \in F$ . Alors, pour tout  $y \in F$ , on a  $f \circ s(y) = f(\tau(f^{-1}(\{y\}))) \in f(f^{-1}(\{y\})) = \{y\}$  donc  $f \circ s(y) = y$  et finalement  $f \circ s = \text{id}_F$ .
- (Formulation 3  $\Rightarrow$  Formulation 1). On suppose que toute surjection à valeurs dans un ensemble non vide admet une section. Soit  $(A_i)_{i \in I}$  une famille non vide d'ensembles non vides. Soient  $F = I$ ,  $E = \{(i, a_i) \mid i \in I, a_i \in A_i\}$  et  $f: E \rightarrow F$  l'application définie par  $(i, a_i) \mapsto i$  pour tout  $i \in I$  et  $a_i \in A_i$ . Comme chaque  $A_i$  est non vide, l'application  $f$  est surjective. Par hypothèse, il existe  $s: F \rightarrow E$  telle que  $f \circ s = \text{id}_F$ . On en déduit que pour tout  $i \in I$ , il existe  $\alpha_i \in A_i$  tel que  $s(i) = (i, \alpha_i)$  (pour que  $f(s(i, \alpha_i)) = i$ ). Alors  $(\alpha_i)_{i \in I} \in \prod_{i \in I} A_i$  donc  $\prod_{i \in I} A_i$  n'est pas vide.

**Définition B.1.** Soit  $E$  un ensemble. Un **ordre** sur  $E$  est une relation binaire  $\preccurlyeq$ , réflexive, antisymétrique et transitive, c'est-à-dire telle que :

- $\forall x \in E, x \preccurlyeq x$ ;
- $\forall (x, y) \in E^2$ , si  $x \preccurlyeq y$  et  $y \preccurlyeq x$ , alors  $x = y$ ;
- $\forall (x, y, z) \in E^3$ , si  $x \preccurlyeq y$  et  $y \preccurlyeq z$  alors  $x \preccurlyeq z$ .

On dit alors que l'ensemble  $(E, \preccurlyeq)$  est un **ensemble ordonné**.

**Remarque.** Il est clair que, si  $F$  est un sous-ensemble de l'ensemble  $E$  et si  $\preccurlyeq$  est un ordre sur  $E$ , alors  $\preccurlyeq$  induit un ordre sur  $F$ .

**Définition B.2.** Si  $(E, \preccurlyeq)$  est un ensemble ordonné et si, pour tous  $(x, y) \in E^2$ ,  $x$  et  $y$  sont **comparables**, c'est-à-dire que  $x \preccurlyeq y$  ou  $y \preccurlyeq x$ , on dit que  $\preccurlyeq$  est un **ordre total** ou que  $(E, \preccurlyeq)$  est un **ensemble totalement ordonné**. Dans le cas contraire, on dit que  $\preccurlyeq$  est un **ordre partiel** ou que  $(E, \preccurlyeq)$  est un **ensemble partiellement ordonné**.

Une partie totalement ordonnée d'un ensemble ordonné  $E$  sera aussi appelée une **chaîne** de  $E$ .

**Définition B.3.** Soit  $(E, \preccurlyeq)$  un ensemble ordonné.

- Un **élément maximal** de  $(E, \preccurlyeq)$  est un élément  $x \in E$  tel que, pour tout  $y \in E$ , si  $x \preccurlyeq y$ , alors  $x = y$ .
- Soit  $F$  un sous-ensemble non vide de  $E$ . Un **majorant** de  $F$  dans  $E$  est un élément  $m$  de  $E$  tel que pour tout  $x \in F$ ,  $x \preccurlyeq m$ . Ce majorant est dit **strict** si, pour tout  $x \in F$ , on a  $x \prec m$ .
- On dit que  $(E, \preccurlyeq)$  est un **ensemble inductif** si tout sous-ensemble non-vide  $F$  de  $E$  tel que  $(F, \preccurlyeq)$  soit totalement ordonné admet un majorant dans  $E$ .

**Théorème B.4** (Lemme de Zorn). Soit  $(E, \preccurlyeq)$  un ensemble ordonné, inductif et non vide. Alors il existe un élément maximal dans  $E$ .

**Définition B.5.** Soit  $(E, \preccurlyeq)$  un ensemble ordonné.

- Soit  $F$  une partie non vide de  $E$ . Un **minorant** de  $F$  dans  $E$  est un élément  $m$  de  $E$  tel que pour tout  $x \in F$ ,  $m \preccurlyeq x$ .
- Soit  $F$  une partie non vide de  $E$ . On dit que  $m$  est un **plus petit élément** de  $F$  si  $m$  est un minorant de  $F$  et si  $m \in F$ .
- On dit que  $\preccurlyeq$  est un **bon ordre** ou que  $(E, \preccurlyeq)$  est **bien ordonné** si toute partie non vide de  $E$  admet un plus petit élément.

**Remarque.** Un ensemble bien ordonné est en particulier totalement ordonné.

En effet, si  $(x, y) \in E^2$ , alors la partie  $\{x, y\}$  admet un plus petit élément, par exemple  $x$ , et on a alors  $x \preccurlyeq y$ .

Nous pouvons alors énoncer le théorème suivant.

**Théorème B.6** (Théorème de Zermelo). Tout ensemble non vide peut être bien ordonné.

## b Le lemme de Zorn implique le théorème de Zermelo

On suppose que le lemme de Zorn est vrai.

Soit  $E$  un ensemble non vide. On veut démontrer que toute partie non vide de  $E$  a un plus petit élément.

On considère l'ensemble  $\mathcal{F}$  des couples  $(F, \leq_F)$  où  $F$  est une partie de  $E$  et  $\leq_F$  est un bon ordre sur  $F$ .

Soit  $x \in E$ , alors  $\{x\}$  muni de l'ordre évident ( $x = x$ ) est bien ordonné, donc  $\mathcal{F}$  n'est pas vide. Nous allons munir  $\mathcal{F}$  d'un ordre inductif de façon à pouvoir lui appliquer le lemme de Zorn :

$$\forall ((F, \leq_F), (G, \leq_G)) \in \mathcal{F}^2,$$

$$(F, \leq_F) \preceq (G, \leq_G) \iff \begin{cases} \text{(o1)} & F \subset G \\ \text{(o2)} & \leq_F \text{ est la restriction de } \leq_G \text{ à } F \\ \text{(o3)} & \text{si } (y, x) \in F \times G \text{ est tel que } x \leq_G y, \text{ alors } x \in F. \end{cases}$$

On vérifie facilement qu'il s'agit bien d'une relation d'ordre :

- Il est clair que  $\preceq$  est réflexive.
- On suppose que  $(F, \leq_F) \preceq (G, \leq_G)$  et que  $(G, \leq_G) \preceq (F, \leq_F)$ . Alors  $F \subset G$  et  $G \subset F$  donc  $F = G$ . Par (o2) les ordres  $\leq_F$  et  $\leq_G$  sur  $F = G$  sont les mêmes donc  $(F, \leq_F) = (G, \leq_G)$ . Ainsi,  $\preceq$  est anti-symétrique.
- Enfin,  $\preceq$  est transitive. On suppose que  $(F, \leq_F) \preceq (G, \leq_G)$  et que  $(G, \leq_G) \preceq (H, \leq_H)$ . Il est clair que  $F \subset H$  et que la restriction de  $\leq_H$  à  $F$  est  $\leq_F$ . Vérifions (o3). Soit  $(z, x) \in F \times H$  tel que  $x \leq_H z$ . On a en particulier  $(z, x) \in G \times H$  et  $x \leq_H z$  donc par (o3) pour  $(G, \leq_G)$  et  $(H, \leq_H)$  on a  $x \in G$ . Mais alors  $x \leq_G z$  avec  $(z, x) \in F \times G$  donc par (o3) pour  $(F, \leq_F)$  et  $(G, \leq_G)$  on a  $x \in F$ , ce que l'on voulait.

Pour démontrer que cet ordre est inductif, pour toute partie totalement ordonnée  $\mathcal{T}$  de  $\mathcal{F}$  nous devons trouver un majorant de  $\mathcal{T}$  dans  $\mathcal{F}$ .

Soit  $\mathcal{T} = \{(F_i, \leq_{F_i}) \mid i \in I\}$  une partie totalement ordonnée de  $\mathcal{F}$ . Soit  $G = \bigcup_{i \in I} F_i$ , on a  $F_i \subset G$  pour tout  $i \in I$ .

- Munissons  $G$  d'un ordre  $\leq_G$ . Soit  $(x, y) \in G^2$ , alors il existe  $i \in I$  tel que  $(x, y) \in F_i^2$  puisque  $\mathcal{T}$  est totalement ordonnée. On peut donc poser  $x \leq_G y \iff x \leq_{F_i} y$ . De plus, si  $j \in I$  est tel que  $(x, y) \in F_j^2$ , on peut supposer par exemple que  $(F_i, \leq_{F_i}) \preceq (F_j, \leq_{F_j})$  donc  $F_i \subset F_j$  et  $\leq_{F_i}$  est la restriction de  $\leq_{F_j}$  à  $F_i$  et on a bien  $x \leq_{F_i} y \iff x \leq_{F_j} y$ . Ainsi la relation définie sur  $G$  ne dépend pas du choix de  $i \in I$ .
- La relation  $\leq_G$  est bien une relation d'ordre.
  - Si  $x \in G$ , soit  $i \in I$  tel que  $x \in F_i$ , alors  $x \leq_{F_i} x$  donc  $x \leq_G x$  par définition de  $\leq_G$ .
  - Soit  $(x, y) \in G^2$  tel que  $x \leq_G y$  et  $y \leq_G x$ . Soit  $i \in I$  tel que  $(x, y) \in F_i^2$ . Par définition de  $\leq_G$ , on a  $x \leq_{F_i} y$  et  $y \leq_{F_i} x$  donc  $x = y$ .
  - Soit  $(x, y, z) \in G^3$  tel que  $x \leq_G y$  et  $y \leq_G z$ . Soit  $i \in I$  tel que  $(x, y, z) \in F_i^3$ . Alors  $x \leq_{F_i} y$  et  $y \leq_{F_i} z$  donc  $x \leq_{F_i} z$  et finalement  $x \leq_G z$ .
- Vérifions que  $\leq_G$  est un bon ordre.

Soit  $H$  une partie non vide de  $G$ . Soit  $i \in I$  tel que  $H \cap F_i \neq \emptyset$ . Alors  $H \cap F_i$  est une partie de  $F_i$  et  $\leq_{F_i}$  est un bon ordre donc  $F_i \cap H$  admet un plus petit élément,  $m_i \in H \cap F_i$ . Montrons que  $m_i$  ne dépend pas de  $i$  : soit  $j \in I$  tel que  $H \cap F_j \neq \emptyset$  et soit  $m_j$  le plus petit élément de  $H \cap F_j$ . On peut supposer par exemple que  $(F_i, \leq_{F_i}) \preceq (F_j, \leq_{F_j})$ . On a alors  $F_i \cap H \subset F_j \cap H$  donc  $m_j \leq_{F_j} m_i$ . D'après (o3), on a  $m_j \in F_i$ , donc  $m_j \in H \cap F_i$  et donc  $m_i \leq m_j$  et finalement  $m_j = m_i$ .

Soit  $x \in H$  et soit  $j \in I$  tel que  $m_i \in F_j$  et  $x \in F_j$ ; on a donc  $(m_i, x) \in (F_j \cap H)^2$  donc  $m_i = m_j \leq_{F_j} x$  et donc  $m_i \leq_G x$ . Ainsi,  $m_i$  est le plus petit élément de  $H$ .

Par conséquent,  $(G, \leq_G) \in \mathcal{F}$ .

- Enfin, soit  $(F_i, \leq_{F_i}) \in \mathcal{T}$ , nous devons vérifier que  $(F_i, \leq_{F_i}) \preceq (G, \leq_G)$ . Il est clair que  $F_i \subset G$  et que  $\leq_{F_i}$  est la restriction de  $\leq_G$  à  $F_i$  par construction. Soit  $(y, x) \in F_i \times G$  tel que  $x \leq_G y$ ; soit  $j \in J$  tel que  $F_i \subset F_j$  et  $x \in F_j$ . Alors  $x \leq_{F_j} y$  et comme  $(F_i, \leq_{F_i}) \preceq (F_j, \leq_{F_j})$  on en déduit que  $x \in F_i$  d'après (o3) pour  $F_i$  et  $F_j$ . Donc (o3) est vérifiée pour  $F_i$  et  $G$  et finalement  $(F_i, \leq_{F_i}) \preceq (G, \leq_G)$ .

Ainsi,  $(G, \leq_G) \in \mathcal{F}$  qui majore  $\mathcal{T}$ .

Nous avons donc démontré que  $\mathcal{F}$  est inductif. Nous pouvons par conséquent appliquer le lemme de Zorn : il existe un élément maximal  $(F, \leq_F)$  dans  $\mathcal{F}$ .

Montrons que  $F = E$ . Pour cela, supposons par l'absurde que  $F \subsetneq E$  et soit  $y \in E \setminus F$ . Soit  $K = F \cup \{y\}$ , muni du bon ordre  $\leq_K$  dont la restriction à  $F$  est  $\leq_F$  et tel que pour tout  $x \in F$  on ait  $x \leq_K y$ . Alors  $(K, \leq_K) \in \mathcal{F}$  et  $(F, \leq_F) \prec (K, \leq_K)$ , ce qui contredit la maximalité de  $(F, \leq_F)$ .

Donc  $E = F \in \mathcal{F}$  et donc  $E$  est bien ordonné.

### c) Le théorème de Zermelo implique l'axiome du choix

On suppose que le théorème de Zermelo est vrai.

Soit  $\{A_i \mid i \in I\}$  une famille non vide d'ensembles non vides. D'après le théorème de Zermelo, l'ensemble  $A = \bigcup_{i \in I} A_i$  peut être muni d'un bon ordre. Chaque partie (non vide)  $A_i$  de  $A$  admet donc un plus petit élément  $x_i \in A_i$ . On en déduit un élément  $(x_i)_{i \in I} \in \prod_{i \in I} A_i$ .

### d) L'axiome du choix implique le lemme de Zorn

On suppose l'axiome du choix.

Soit  $(E, \preceq)$  un ensemble inductif non vide. Nous devons démontrer qu'il a un élément maximal. Supposons par l'absurde qu'il n'a pas d'élément maximal.

Pour toute chaîne  $C$  de  $E$ , on note  $\mathcal{M}_C = \{x \in E \mid \forall y \in C, y \prec x\}$  l'ensemble des majorants stricts de  $C$ . On a  $\mathcal{M}_C \subset E \setminus C$ .

Soit  $C$  une chaîne de  $E$ . Alors  $\mathcal{M}_C$  n'est pas vide. En effet, puisque  $E$  est inductif,  $C$  a un majorant  $M$ . Par hypothèse,  $M$  n'est pas un élément maximal de  $E$ , donc il existe  $x \in E$  tel que  $M \prec x$ . En particulier, pour tout  $y \in C$  on a  $y \preceq M \prec x$  donc  $x \in \mathcal{M}_C$ .

L'axiome du choix fournit une fonction de choix  $\tau: \mathcal{P}^*(E) \rightarrow E$  sur  $E$  qui vérifie, en particulier, que pour toute chaîne  $C$  de  $E$ , on a  $\tau(\mathcal{M}_C) \in \mathcal{M}_C$ .

On note :

$$\begin{aligned}\mathcal{E}_0 &= \{C \text{ chaîne de } E \mid \text{pour toute chaîne } S \text{ de } C \text{ avec } \mathcal{M}_S \not\subset \mathcal{M}_C, \text{ on a } \tau(\mathcal{M}_S) \in C\} \\ \mathcal{E} &= \{C \in \mathcal{E}_0 \mid \forall C' \in \mathcal{E}_0, C \setminus C' \subset \mathcal{M}_{C'}\} \\ C^* &= \bigcup_{C \in \mathcal{E}} C.\end{aligned}$$

Nous allons :

- (1) démontrer que  $C^* \in \mathcal{E}$ ;
- (2) poser  $u = \tau(\mathcal{M}_{C^*})$  et  $C^{**} = C^* \cup \{u\} \supsetneq C^*$  et démontrer que  $C^{**} \in \mathcal{E}$ .

Ce dernier point implique en particulier que  $C^{**} \subset C^*$ , par définition de  $C^*$ , ce qui donne une contradiction car  $C^{**} \supsetneq C^*$ . On en déduit donc que  $E$  admet un élément maximal.

Démontrons donc (1), c'est-à-dire que  $C^* \in \mathcal{E}$ .

- Soit  $C' \in \mathcal{E}_0$ . Alors  $C^* \setminus C' \subset \bigcup_{C \in \mathcal{E}} (C \setminus C') \subset \mathcal{M}_{C'}$ . Donc si  $C^* \in \mathcal{E}_0$ , alors  $C^* \in \mathcal{E}$ .
- Montrons que  $C^*$  est une chaîne de  $E$ . Soit  $(x, y) \in C^* \times C^*$ . Il existe  $C \in \mathcal{E}$  tel que  $x \in C$ . Si  $y \in C$  alors  $x$  et  $y$  sont comparables car  $C$  est totalement ordonné. Sinon,  $y \in C^* \setminus C \subset \mathcal{M}_C$  d'après ce qui précède, donc  $x \prec y$  et  $x$  et  $y$  sont bien comparables.
- Soit  $S$  une chaîne de  $C^*$  telle que  $\mathcal{M}_S \not\subset \mathcal{M}_{C^*} = \bigcap_{C \in \mathcal{E}} \mathcal{M}_C$ , alors il existe  $C \in \mathcal{E}$  tel que  $\mathcal{M}_S \not\subset \mathcal{M}_C$ . Montrons que  $S \subset C$  pour pouvoir utiliser le fait que  $C \in \mathcal{E}_0$ .  
Supposons par l'absurde que  $S \not\subset C$ , alors en utilisant le premier point, il existe  $y \in (S \setminus C) \subset (C^* \setminus C) \subset \mathcal{M}_C$ .  
Puisque  $\mathcal{M}_S \not\subset \mathcal{M}_C$ , il existe  $x \in \mathcal{M}_S$  tel que  $x \notin \mathcal{M}_C$ . On a  $y \in S$  et  $x \in \mathcal{M}_S$  donc  $y \prec x$ . Comme  $y \in \mathcal{M}_C$ , pour tout  $z \in C$  on a  $z \prec y \prec x$ , donc  $x \in \mathcal{M}_C$ , une contradiction.  
Donc  $S \subset C$  et comme  $C \in \mathcal{E} \subset \mathcal{E}_0$ , on en déduit que  $\tau(\mathcal{M}_S) \in C$ . Or  $C \subset C^*$  donc  $\tau(\mathcal{M}_S) \in C^*$ .  
Ainsi,  $C^* \in \mathcal{E}_0$  et par le premier point,  $C^* \in \mathcal{E}$ .

Soit  $u = \tau(\mathcal{M}_{C^*}) \in \mathcal{M}_{C^*} \subset (E \setminus C^*)$  et posons  $C^{**} = C^* \cup \{u\} \supsetneq C^*$ .

Pour tout  $x \in C^*$  on a  $x \prec u$  donc  $C^{**}$  est bien une chaîne de  $E$ .

Montrons enfin (2), c'est-à-dire que  $C^{**} \in \mathcal{E}$ .

- Soit  $S \subset C^{**}$  une chaîne de  $C^{**}$  telle que  $\mathcal{M}_S \not\subset \mathcal{M}_{C^{**}}$ . Supposons que  $u \in S$  et soit  $m \in \mathcal{M}_S$ . Alors  $u \prec m$  et donc, pour tout  $x \in C^{**}$ , on a  $x \prec u \prec m$  et par conséquent  $m \in \mathcal{M}_{C^{**}}$ . Ainsi,  $\mathcal{M}_S \subset \mathcal{M}_{C^{**}}$  et on a obtenu une contradiction.  
Donc  $u \notin S$ , ce qui, avec  $S \subset C^{**} = C^* \cup \{u\}$ , implique que  $S \subset C^*$  et donc  $\mathcal{M}_{C^*} \subset \mathcal{M}_S$ . Vérifions que  $\tau(\mathcal{M}_S) \in C^{**}$ .  
➤ Si  $\mathcal{M}_S \subset \mathcal{M}_{C^*}$  alors  $\mathcal{M}_S = \mathcal{M}_{C^*}$  donc  $\tau(\mathcal{M}_S) = \tau(\mathcal{M}_{C^*}) = u \in C^{**}$ .

➤ Si  $\mathcal{M}_S \notin \mathcal{M}_{C^*}$ , alors  $\tau(\mathcal{M}_S) \in C^* \subset C^{**}$  car  $C^* \in \mathcal{E}_0$ .

Dans les deux cas, on a bien  $\tau(\mathcal{M}_S) \in C^{**}$ .

On a donc démontré que  $C^{**} \in \mathcal{E}_0$ .

➤ Soit  $C' \in \mathcal{E}_0$ . Nous devons démontrer que  $C^{**} \setminus C' \subset \mathcal{M}_{C'}$ .

➤ Supposons que  $C^* \setminus C' \neq \emptyset$ . Il existe donc  $x \in C^* \setminus C'$ . Comme  $C^* \in \mathcal{E}$ , on a  $x \in \mathcal{M}_{C'}$ . Or  $x \in C^*$  donc  $x \prec u$ , donc  $u \in \mathcal{M}_{C'}$  et on a  $(C^{**} \setminus C') \subset ((C^* \setminus C') \cup \{u\}) \subset \mathcal{M}_{C'}$ .

➤ Supposons que  $C^* \setminus C' = \emptyset$ , c'est-à-dire que  $C^* \subset C'$ . Si  $\mathcal{M}_{C^*} \subset \mathcal{M}_{C'}$ , alors  $u \in \mathcal{M}_{C^*} \subset \mathcal{M}_{C'}$  et  $C^{**} \setminus C' \subset \{u\} \subset \mathcal{M}_{C'}$ . Si  $\mathcal{M}_{C^*} \not\subset \mathcal{M}_{C'}$ , alors  $u = \tau(\mathcal{M}_{C^*}) \in C'$  car  $C' \in \mathcal{E}_0$  et  $C^* \subset C'$ , donc  $C^{**} \setminus C' = \emptyset \subset \mathcal{M}_{C'}$ .

## Référence

[1] K. NUIDA, *A Simple and Elementary Proof of Zorns Lemma*, arXiv :2305.10258v2.

## II. FORMULE DES DEGRÉS POUR LES POLYNÔMES EN PLUSIEURS INDÉTERMINÉES

Nous voulons démontrer le résultat suivant.

**Proposition B.7.** Soit  $A$  un anneau intègre et soit  $n \in \mathbb{N}^*$ . Si  $f$  et  $g$  sont deux polynômes non nuls de  $A[X_1, \dots, X_n]$ , alors  $\deg(fg) = \deg(f) + \deg(g)$  (où  $\deg$  désigne le degré total).

On vérifie facilement que si  $f$  et  $g$  sont des monômes, la formule est satisfaite.

Pour la démontrer dans le cas général, nous allons :

- (1) définir une relation d'ordre  $\preceq$  sur l'ensemble  $\mathcal{M}$  des monômes de  $A[X_1, \dots, X_n]$ ;
- (2) vérifier que c'est une relation d'ordre total;
- (3) vérifier que si  $(P, Q, R, S) \in \mathcal{M}^4$  sont tels que  $P \preceq Q$  et  $R \preceq S$  avec au moins une des deux inégalités stricte, alors  $PR \prec QS$ ;
- (4) utiliser ce qui précède pour démontrer le résultat.

**(1) Relation d'ordre.** Soient  $P$  et  $Q$  dans  $\mathcal{M}$ , notons-les  $P = X_1^{i_1} \dots X_n^{i_n}$  et  $Q = X_1^{j_1} \dots X_n^{j_n}$ . On dit que  $P \preceq Q$  si l'une des conditions suivantes est satisfaite :

- (i)  $P = Q$ ;
- (ii)  $\deg P < \deg Q$ ;
- (iii)  $\deg P = \deg Q$ ,  $P \neq Q$  et, si  $r = \min\{k \in \llbracket 1; n \rrbracket \mid i_k \neq j_k\}$ , alors  $i_r < j_r$  (ordre lexicographique sur les monômes de même degré).

Notons que si  $P \preceq Q$  alors on a nécessairement  $\deg P \leq \deg Q$ .

Vérifions que c'est bien une relation d'ordre.

♦ La réflexivité est évidente par (i).

♦ Soit  $(P, Q) \in \mathcal{M}^2$  avec les notations ci-dessus tel que  $P \preceq Q$  et  $Q \preceq P$ . Alors  $\deg P \leq \deg Q$  et  $\deg Q \leq \deg P$  donc  $\deg P = \deg Q$ . Supposons que  $P \neq Q$ . Alors il existe  $r$  tel que  $i_r \neq j_r$  et si on choisit un tel  $r$  minimal, on doit avoir (par définition de la relation  $\preceq$ ) à la fois  $i_r < j_r$  et  $i_r > j_r$ , ce qui est impossible. Donc  $P = Q$ . La relation  $\preceq$  est donc anti-symétrique.

♦ Soit  $(P, Q, R) \in \mathcal{M}^3$  tel que  $P \preceq Q$  et  $Q \preceq R$ . Si  $P = Q$  ou si  $Q = R$  alors  $P \preceq R$ . On peut donc supposer que les trois monômes sont distincts. Si  $\deg P < \deg Q$ , comme  $\deg Q \leq \deg R$  on a  $\deg P < \deg R$  et donc  $P \preceq R$ . De même si  $\deg Q < \deg R$ . Il reste donc le cas où  $\deg P = \deg Q = \deg R$ .

Posons  $P = X_1^{i_1} \dots X_n^{i_n}$ ,  $Q = X_1^{j_1} \dots X_n^{j_n}$  et  $R = X_1^{k_1} \dots X_n^{k_n}$ . Soit  $r = \min\{q \in \llbracket 1; n \rrbracket \mid i_q \neq j_q\}$  et  $s = \min\{q \in \llbracket 1; n \rrbracket \mid j_q \neq k_q\}$ . Si  $r \leq s$  alors pour tout  $q < r$  on a  $i_q = j_q = k_q$  et  $i_r < j_r \leq k_r$ , donc  $i_r < k_r$  et donc  $P \preceq R$ . Si  $r > s$ , alors pour tout  $q < s$  on a  $i_q = j_q = k_q$  et  $i_s = j_s < k_s$ , donc  $i_s < k_s$  et donc  $P \preceq R$ .

Dans tous les cas,  $P \preceq R$ . Donc la relation  $\preceq$  est transitive.

(2) **Relation d'ordre total et conséquence.** De plus, cette relation d'ordre est totale. En effet, si  $(P, Q) \in \mathcal{M}^2$ , soit  $P$  et  $Q$  sont égaux donc comparables, soit ils ont des degrés différents, ils sont alors comparables, soit ils ne sont pas égaux et ont même degré, mais alors  $\{k \in \llbracket 1; n \rrbracket \mid i_k \neq j_k\}$  n'est pas vide, il existe  $r = \min\{k \in \llbracket 1; n \rrbracket \mid i_k \neq j_k\}$  et on a nécessairement  $i_r < j_r$  ou  $j_r < i_r$ , c'est-à-dire  $P \prec Q$  ou  $Q \prec P$ .

Par conséquent, pour tout polynôme non nul  $f$ , il existe un unique terme monomial  $aP$  de  $f$  avec  $a \in A \setminus \{0\}$  et  $P \in \mathcal{M}$  tel que  $P$  soit le plus grand élément parmi les monômes qui apparaissent dans  $f$  avec coefficient non nul.

(3) **Propriété.**

Soit  $(P, Q, R, S) \in \mathcal{M}^4$  tel que  $P \preceq Q$  et  $R \prec S$  et montrons que  $PR \prec QS$ . Notons que  $\deg P \leq \deg Q$  et  $\deg R \leq \deg S$ .

Si  $\deg R < \deg S$  alors  $\deg(PR) = \deg P + \deg R < \deg Q + \deg S = \deg(QS)$  car la formule est vraie pour les monômes, donc  $PR \prec QS$ . De même, si  $\deg P < \deg Q$  on a  $PR \prec QS$ .

Supposons donc que  $\deg P = \deg Q$  et  $\deg R = \deg S$ . Notons  $P = X_1^{i_1} \cdots X_n^{i_n}$ ,  $Q = X_1^{j_1} \cdots X_n^{j_n}$ ,  $R = X_1^{k_1} \cdots X_n^{k_n}$  et  $S = X_1^{\ell_1} \cdots X_n^{\ell_n}$ . Comme  $R \neq S$ , il existe  $s = \min\{q \in \llbracket 1; n \rrbracket \mid k_q \neq \ell_q\}$ . Si  $P = Q$  alors pour tout  $q \in \llbracket 1; n \rrbracket$  on a  $i_q = j_q$ , sinon soit  $r = \min\{q \in \llbracket 1; n \rrbracket \mid i_q \neq j_q\}$  et soit  $t = \min(r, s)$ . Alors, pour tout  $q < t$  on a  $i_q = j_q$  et  $k_q = \ell_q$  donc  $i_q + k_q = j_q + \ell_q$  et, pour  $q = t$ , on a  $i_t \leq j_t$  et  $k_t \leq \ell_t$  avec au moins une des deux inégalités stricte, donc  $i_t + k_t < j_t + \ell_t$  et finalement  $PR \prec QS$ .

Le cas où  $P \prec Q$  et  $R \preceq S$  se traite de même.

(4) **Formule des degrés.** Soient maintenant  $f$  et  $g$  deux polynômes non nuls de  $A[X_1, \dots, X_n]$ . Notons  $aP$  le terme monomial de  $f$  avec  $a \in A \setminus \{0\}$  tel que  $P \in \mathcal{M}$  soit le plus grand élément parmi les monômes qui apparaissent dans  $f$  et  $bQ$  avec  $b \in A \setminus \{0\}$  le terme monomial de  $g$  tel que  $Q \in \mathcal{M}$  soit le plus grand élément parmi les monômes qui apparaissent dans  $g$ . On peut donc écrire  $f = aP + f_1$  et  $g = bQ + g_1$  avec  $f_1$  et  $g_1$  dans  $A[X_1, \dots, X_n]$  tels que tous les monômes  $P_1$  qui apparaissent dans  $f_1$  vérifient  $P_1 \prec P$  et tous les monômes  $Q_1$  qui apparaissent dans  $g_1$  vérifient  $Q_1 \prec Q$ . Notons que l'on a aussi  $\deg P_1 \leq \deg P$  et  $\deg Q_1 \leq \deg Q$  pour tous ces monômes. En particulier,  $\deg f = \deg P$  et  $\deg g = \deg Q$ .

On a alors  $fg = abPQ + aPg_1 + bQf_1 + f_1g_1$ . Grâce au point (3) précédent, tous les monômes qui apparaissent dans  $aPg_1 + bQf_1 + f_1g_1$  sont strictement inférieurs à  $PQ$  pour la relation  $\prec$  et en particulier différents de  $PQ$ . Il ne peut donc pas y avoir de compensation avec le terme  $abPQ$ . De plus, ils sont tous de degré inférieur ou égal à  $\deg(PQ)$ . Donc  $\deg(fg) = \deg(PQ) = \deg P + \deg Q = \deg f + \deg g$ , ce que l'on voulait.

### III. RACINES ET FACTEURS IRRÉDUCTIBLES DE POLYNÔMES ET POLYNÔMES DÉRIVÉS

Soit  $A$  un anneau et soit  $f \in A[X]$ .

**Définition B.8.** On dit que  $\alpha$  est une racine **multiple** de  $f$  si  $(X - \alpha)^2$  divise  $f$ .

On dit que  $\alpha$  est une racine de **multiplicité**  $m \in \mathbb{N}^*$  de  $f$  si  $(X - \alpha)^m$  divise  $f$  mais  $(X - \alpha)^{m+1}$  ne divise pas  $f$ , autrement dit, s'il existe  $g \in A[X]$  tel que  $f(X) = (X - \alpha)^m g(X)$  et  $g(\alpha) \neq 0$ .

**Exemple.** (Pour illustrer certaines particularités quand  $A$  n'est pas intègre.) Soit  $A = \mathbb{Z}/12\mathbb{Z}$  et soit  $f(X) = X^3 + X^2 - X - \bar{1}$ . Alors  $-\bar{1}$  et  $\bar{5}$  sont des racines de  $f$  de multiplicité 2. En effet,  $f(X) = (X + \bar{1})^2(X - \bar{1}) = (X - \bar{5})^2(X - \bar{1})$  et  $-\bar{1}$  et  $\bar{5}$  ne sont pas racines de  $(X - \bar{1})$ .

**Proposition B.9.** Soit  $\alpha \in A$  une racine de  $f$ . Alors  $\alpha$  est une racine multiple de  $f$  si, et seulement si,  $\alpha$  est une racine de  $f'$ .

**Démonstration.** Supposons que  $\alpha$  soit une racine multiple de  $f$ . Alors il existe  $g \in A[X]$  tel que  $f(X) = (X - \alpha)^2 g(X)$ . On a alors  $f'(X) = (X - \alpha)(2g(X) + (X - \alpha)g'(X))$ , donc  $\alpha$  est racine de  $f'$ .

Réciproquement, supposons que  $\alpha$  soit une racine simple de  $f$ . Alors il existe  $g \in A[X]$  tel que  $f(X) = (X - \alpha)g(X)$  et  $g(\alpha) \neq 0$ . On a alors  $f'(X) = g(X) + (X - \alpha)g'(X)$  donc  $f'(\alpha) = g(\alpha) \neq 0$ . ✓

**Exemple.** Si on reprend l'exemple précédent,  $f'(X) = \bar{3}X^2 + \bar{2}X - \bar{1} = (X + \bar{1})(\bar{3}X - \bar{1}) = (X - \bar{5})(\bar{3}X + \bar{5})$ .

**Proposition B.10.** Soit  $\alpha$  une racine de  $f$  de multiplicité  $m \geq 2$ . On suppose que, dans  $A$ ,  $m!1_A \neq 0$  et  $m!1_A$  n'est pas un diviseur de zéro. Alors  $\alpha$  est une racine de  $f'$  de multiplicité  $m - 1$ .

*Démonstration.* Soit  $g \in A[X]$  tel que  $f(X) = (X - \alpha)^m g(X)$  avec  $g(\alpha) \neq 0$ . Alors  $f'(X) = (X - \alpha)^{m-1} h(X)$  avec  $h(X) = mg(X) + (X - \alpha)g'(X)$ . On a alors  $h(\alpha) = mg(\alpha) \neq 0$  car  $g(\alpha) \neq 0$  et  $m!1_A$  n'est pas nul et n'est pas un diviseur de zéro. Donc  $\alpha$  est une racine de  $f'$  de multiplicité  $m - 1$ . ✓

**Exemple.** Même si  $A$  est un corps, il faut l'hypothèse  $m!1_A \neq 0$ . En effet, soit  $p$  un nombre premier, soit  $A = \mathbb{Z}/p\mathbb{Z}$  et soit  $f(X) = X^p \in A[X]$ . Alors 0 est racine de  $f$  de multiplicité  $p$ , mais  $f'(X) = \bar{p}X^{p-1} = 0$  donc 0 n'est pas de multiplicité  $p - 1$  comme racine de  $f'$ .

**Lemme B.11.** Soit  $m \in \mathbb{N}^*$  tel que, dans  $A$ ,  $m!1_A \neq 0$  et  $m!1_A$  n'est pas un diviseur de zéro et soit  $r$  un polynôme de degré au plus  $m$ . Si  $r' = 0$  alors  $r$  est constant.

*Démonstration.* Posons  $r = \sum_{i=0}^m a_i X^i$  avec  $a_i \in A$  pour tout  $i \in \llbracket 0; m \rrbracket$ . Alors  $r' = \sum_{i=1}^m i a_i X^{i-1}$ .

Par hypothèse,  $r' = 0$  donc pour tout  $i \in \llbracket 1; m \rrbracket$  on a  $i a_i = 0$ , c'est-à-dire que  $i!1_A a_i = 0$ . Or par hypothèse  $i!1_A$  n'est ni nul, ni un diviseur de zéro dans  $A$  donc  $a_i = 0$ . On en déduit donc que  $r = a_0$  est constant. ✓

**Proposition B.12.** Soit  $\alpha$  une racine de  $f$  et soit  $m \in \mathbb{N}^*$  tel que, dans  $A$ ,  $m!1_A \neq 0$  et  $m!1_A$  n'est pas un diviseur de zéro. Alors  $\alpha$  est une racine de  $f$  de multiplicité  $m$  si, et seulement si,  $f^{(k)}(\alpha) = 0$  pour tout  $k \in \llbracket 0; m - 1 \rrbracket$  et  $f^{(m)}(\alpha) \neq 0$ .

*Démonstration.* Raisonnons par récurrence sur  $m$ .

➤ Si  $m = 1$ , c'est la première proposition.

➤ Soit  $m > 1$  tel que le résultat soit vrai au rang  $m - 1$ . Notons  $g = f'$ .

Si  $\alpha$  est racine de  $f$  de multiplicité  $m$  alors, d'après la deuxième proposition,  $\alpha$  est racine de  $g = f'$  de multiplicité  $m - 1$ . Par hypothèse de récurrence on a  $f^{(k)}(\alpha) = g^{(k-1)}(\alpha) = 0$  pour tout  $k \in \llbracket 1; m - 1 \rrbracket$  et  $f^{(m)}(\alpha) = g^{(m-1)}(\alpha) \neq 0$ . Comme  $f(\alpha) = 0$  on a bien le résultat voulu pour  $f$ .

Réciproquement, supposons que  $f^{(k)}(\alpha) = 0$  pour tout  $k \in \llbracket 0; m - 1 \rrbracket$  et  $f^{(m)}(\alpha) \neq 0$ . Alors  $g^{(k)}(\alpha) = f^{(k+1)}(\alpha) = 0$  pour tout  $k \in \llbracket 0; m - 2 \rrbracket$  et  $g^{(m-1)}(\alpha) = f^{(m)}(\alpha) \neq 0$ . Par hypothèse de récurrence,  $\alpha$  est racine de  $g$  de multiplicité  $m - 1$ . Il existe donc  $h \in A[X]$  tel que  $f'(X) = g(X) = (X - \alpha)^{m-1} h(X)$  et  $h(\alpha) \neq 0$ . D'autre part, le polynôme  $(X - \alpha)^m$  est unitaire donc on peut effectuer la division euclidienne de  $f$  par  $(X - \alpha)^m$  : il existe un unique  $(q, r) \in (A[X])^2$  tel que  $f(X) = (X - \alpha)^m q(X) + r(X)$  et  $\deg(r) < m$ . Alors  $f'(X) = (X - \alpha)^{m-1} (mq(X) + (X - \alpha)q'(X)) + r'(X)$ . Par unicité de la division euclidienne par un polynôme unitaire, on a  $r' = 0$  et  $mq(X) + (X - \alpha)q'(X) = h(X)$ . En particulier,  $mq(\alpha) = h(\alpha) \neq 0$  donc  $q(\alpha) \neq 0$  et, d'après le lemme,  $r$  est constant. Mais  $r(\alpha) = f(\alpha) = 0$  donc  $r = 0$  et finalement  $f(X) = (X - \alpha)^m q(X)$  avec  $q(\alpha) \neq 0$  et  $\alpha$  est bien une racine de  $f$  de multiplicité  $m$ . ✓

Si on veut pouvoir appliquer ces résultats à tous les polynômes, il faut imposer des conditions sur l'anneau  $A$ . Pour s'assurer que pour tout  $m \in \mathbb{N}^*$ , ni  $m!1_A$  ni  $m!1_A$  ne sont des diviseurs de zéro, on peut supposer que  $A$  est intègre (condition suffisante).

Ensuite, on considère le morphisme d'anneaux  $\varphi: \mathbb{Z} \rightarrow A$  défini par  $\varphi(n) = n!1_A$ . Pour s'assurer que pour tout  $m \in \mathbb{N}^*$ , ni  $m!1_A$  ni  $m!1_A$  ne sont nuls, on doit supposer que  $\varphi$  est injectif et cette condition est également suffisante. On dit alors que  $A$  est de **caractéristique nulle**. Plus généralement, en remarquant que le noyau de  $\varphi$  est un idéal de  $\mathbb{Z}$ , donc de la forme  $n\mathbb{Z}$ , on introduit la définition suivante :

**Définition B.13.** La *caractéristique* de  $A$  est le nombre  $n \in \mathbb{N}$  tel que  $\text{Ker } \varphi = n\mathbb{Z}$ .

On peut noter que si  $A$  est intègre, sa caractéristique est soit 0, soit un nombre premier. En effet, par le premier théorème d'isomorphisme,  $\mathbb{Z}/n\mathbb{Z} \cong \text{Im } \varphi$  et  $\text{Im } \varphi$  est un sous-anneau de l'anneau intègre  $A$ , donc il est intègre et donc  $n = 0$  ou  $n$  est premier.

Finalement, si  $A$  est intègre de caractéristique nulle, alors les résultats précédents sont vrais sans hypothèse sur  $m$  (les hypothèses sont automatiquement vérifiées).

Dans la suite, on suppose que  $A$  est [factoriel de caractéristique nulle](#).

Soit  $k \in A[X]$  un polynôme irréductible non constant. On note  $v_k(f)$  la valuation de  $k$  comme facteur irréductible de  $f$  (cette valuation existe grâce à l'hypothèse que  $A$ , et donc  $A[X]$ , est factoriel).

Notons que le fait que  $A$  soit intègre de caractéristique nulle implique en particulier que si  $f$  n'est pas constant alors  $\deg f' = \deg f - 1$  (exercice). En particulier, si  $f$  n'est pas constant,  $f' \neq 0$  et on peut considérer  $v_k(f')$ .

**Exemple.** C'est faux si  $A$  n'est pas de caractéristique nulle, même si  $A$  est un corps. En effet, soit  $A = \mathbb{Z}/2\mathbb{Z}$ . Soit  $f(X) = X^2 + \bar{1}$ , alors  $f' = \bar{0}$ . Soit  $f(X) = X^4 + X$ , alors  $f'(X) = \bar{1}$  et  $\deg(f') = 0$  alors que  $\deg(f) = 4$ .

**Proposition B.14.** Soit  $k \in A[X]$  un facteur irréductible non constant de  $f$ . Alors  $v_k(f) \geq 2$  si, et seulement si,  $v_k(f') \geq 1$ .

*Démonstration.* Notons que  $k$  n'est pas constant donc  $f$  non plus et on a  $k' \neq 0$  et  $f' \neq 0$  ( $A$  est intègre de caractéristique nulle).

Supposons que  $k^2$  divise  $f$ . Alors il existe  $g \in A[X]$  tel que  $f = k^2g$ . On a alors  $f' = k(2k'g + kg')$ , donc  $k$  divise  $f'$ .

Réciproquement, supposons que  $k^2$  ne divise pas  $f$ . Alors il existe  $g \in A[X]$  tel que  $f = kg$  et  $k \nmid g$ . On a alors  $f' = k'g + kg'$ . Or  $k$  divise  $kg'$  mais  $k$  est irréductible, donc premier (car  $A[X]$  est factoriel),  $k$  ne divise pas  $k'$  (car  $\deg k' < \deg k$ ) et ne divise pas  $g$ , donc  $k$  ne divise pas  $k'g$  et finalement  $k$  ne divise pas  $f'$ . ✓

**Exemple.** Ce résultat est faux si  $A$  n'est pas de caractéristique nulle, même s'il est formulé sans valuations, c'est-à-dire :

Soit  $k \in A[X]$  un facteur irréductible non constant de  $f$ .  
Alors  $k^2$  divise  $f$  si, et seulement si,  $k$  divise  $f'$ .

En effet, soit  $A = (\mathbb{Z}/2\mathbb{Z})[T]$ , c'est un anneau factoriel. Soit  $f(X) = (X^2 + T)(TX^2 + \bar{1}) \in A[X]$ . On vérifie facilement que les deux facteurs de  $f$  n'ont pas de racine dans le corps  $\text{Frac}(A) = (\mathbb{Z}/2\mathbb{Z})(T)$  (on écrit une racine  $\alpha$  sous la forme  $\alpha = \frac{P(T)}{Q(T)}$  avec  $P$  et  $Q$  dans  $A$  premiers entre eux) et sont de degré 2 donc sont irréductibles dans  $\text{Frac}(A)[X]$  et donc dans  $A[X]$  car ils sont primitifs. Le seul élément inversible de  $A[X] = (\mathbb{Z}/2\mathbb{Z})[T, X]$  est  $\bar{1}$ , il est donc clair que ces deux facteurs ne sont pas associés. Ainsi,  $k(X) = X^2 + T$  divise  $f$  mais  $k^2$  ne divise pas  $f$ . Mais  $f' = \bar{0}$  donc  $k$  divise  $f'$ .

**Proposition B.15.** Soit  $k$  un facteur irréductible non constant de  $f$ . Alors  $v_k(f') = v_k(f) - 1$ .

*Démonstration.* Notons  $m = v_k(f) \geq 1$ . Soit  $g \in A[X]$  tel que  $f = k^m g$  avec  $k \nmid g$ . Alors  $f' = k^{m-1}h$  avec  $h = mk'g + kg'$ . Comme dans la démonstration précédente,  $k$  divise  $kg'$  mais  $k$  ne divise pas  $k'g$  donc  $k$  ne divise pas  $h$  et finalement  $v_k(f') = m - 1$ . ✓

**Exemple.** Ce résultat est faux si  $A$  n'est pas de caractéristique nulle. Soit  $f(X) = X^2(X^3 + X^2 + \bar{1}) \in (\mathbb{Z}/2\mathbb{Z})[X]$ . L'anneau  $(\mathbb{Z}/2\mathbb{Z})[X]$  est factoriel,  $X^3 + X^2 + \bar{1}$  est irréductible dans  $(\mathbb{Z}/2\mathbb{Z})[X]$  car il est de degré 3, à coefficients dans le corps  $\mathbb{Z}/2\mathbb{Z}$  et sans racine dans  $\mathbb{Z}/2\mathbb{Z}$ . Le facteur  $X$  est irréductible dans  $(\mathbb{Z}/2\mathbb{Z})[X]$  car il est de degré 1 et unitaire. Ces deux éléments irréductibles ne sont pas associés ( $A[X]^\times = \{\bar{1}\}$ ). Ainsi,  $v_X(f) = 2$ . Mais  $f'(X) = X^4$  donc  $v_X(f') = 4$ . Ici, la dérivée de  $k(X) = X^2$  est nulle.

**Proposition B.16.** Soit  $m \in \mathbb{N}^*$  et soit  $k$  un facteur irréductible de  $f$ . Les assertions suivantes sont équivalentes :

- (i)  $v_k(f) = m$ ;
- (ii)  $k$  divise  $f^{(j)}$  pour tout  $j \in \llbracket 0; m-1 \rrbracket$  et  $k$  ne divise pas  $f^{(m)}$ , autrement dit,  $v_k(f^{(j)}) \neq 0$  pour tout  $j \in \llbracket 0; m-1 \rrbracket$  et  $v_k(f^{(m)}) = 0$ .

*Démonstration.* Par récurrence sur  $m$ .

➤ Si  $m = 1$ , c'est une proposition précédente.

➤ Soit  $m > 1$  tel que l'équivalence soit vraie au rang  $m-1$ . Vérifions l'équivalence au rang  $m$ . Notons  $g = f'$ .

Nous avons vu dans la proposition précédente que (i) au rang  $m$  pour  $f$  est équivalente à (i) au rang  $m-1$  pour  $f'$ , qui est elle-même équivalente par hypothèse de récurrence à (ii) au rang  $m-1$  pour  $f'$ . Il reste à démontrer que (ii) au rang  $m-1$  pour  $f'$  est équivalente à (ii) au rang  $m$  pour  $f$ .

On a, pour tout  $j \in \llbracket 0; m-1 \rrbracket$ ,  $v_k(g^{(j)}) = v_k(f^{(j+1)})$ . De plus,  $v_k(f^{(0)}) = v_k(f) \neq 0$ . Ainsi,

$$(\forall j \in \llbracket 0; m-1 \rrbracket, v_k(f^{(j)}) \neq 0) \iff (\forall j \in \llbracket 0; m-2 \rrbracket, v_k(g^{(j)}) \neq 0),$$

$$\text{et } v_k(f^{(m)}) = 0 \iff v_k(g^{(m-1)}) = 0. \quad \checkmark$$

#### IV. COMPLÉMENT : RÉSULTANT DE DEUX POLYNÔMES

Le résultant, qui est un polynôme associé à un couple de polynômes, permet de généraliser la notion de discriminant et fournit des méthodes de calcul plus efficaces. Il permet aussi de définir le discriminant d'un polynôme qui n'est pas scindé.

Soit  $K$  un corps. Notons  $K_n[X]$  l'espace vectoriel des polynômes de degré au plus  $n$ . Par convention on pose  $K_{-1}[X] = \{0\}$ .

**Définition B.17.** Soit  $(P, Q) \in K[X]^2$  avec  $p = \deg P \geq 1$  et  $q = \deg Q \geq 1$ . Soit  $\varphi: K_{q-1}[X] \times K_{p-1}[X] \rightarrow K_{p+q-1}[X]$  l'application linéaire définie par  $\varphi(U, V) = UP + VQ$ .

On appelle **résultant de  $P$  et  $Q$**  et on note  $\text{Res}(P, Q) \in K$  le déterminant de  $\varphi$ .

**Remarque.** On munit  $K_{q-1}[X] \times K_{p-1}[X]$  de la base  $\mathcal{E} = \{(X^{q-1}, 0), \dots, (X, 0), (1, 0), (0, X^{p-1}), \dots, (0, X), (0, 1)\}$  et  $K_{p+q-1}[X]$  de la base  $\mathcal{F} = \{X^{p+q-1}, \dots, X, 1\}$ . Posons  $P = \sum_{i=0}^p a_i X^i$  et  $Q = \sum_{i=0}^q b_i X^i$  avec

$a_p b_q \neq 0$ . Notons  $C_P$  la matrice colonne à  $(p+1)$  lignes  $C_P = \begin{pmatrix} a_p \\ a_{p-1} \\ \vdots \\ a_0 \end{pmatrix}$  et, de la même façon, soit  $C_Q$

la matrice colonne à  $(q+1)$  lignes  $C_Q = \begin{pmatrix} b_q \\ b_{q-1} \\ \vdots \\ b_0 \end{pmatrix}$ . Soient  $A$  et  $B$  les matrices de taille respectivement  $q \times (p+q)$  et  $p \times (p+q)$  suivantes

$$A = \begin{pmatrix} C_P & 0 & \cdots & 0_{q-1} \\ & C_P & & \\ & & \ddots & \\ 0_{q-1} & 0_{q-2} & \cdots & C_P \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} C_Q & 0 & \cdots & 0_{p-1} \\ & C_Q & & \\ & & \ddots & \\ 0_{p-1} & 0_{p-2} & \cdots & C_Q \end{pmatrix}.$$

Alors  $\text{Res}(P, Q)$  est le déterminant de la matrice par blocs  $\begin{pmatrix} A & B \end{pmatrix}$ .

En effet, la colonne  ${}^t(0_i, {}^tC_P, 0_{q-1-i})$  pour  $0 \leq i \leq q-1$  est la matrice de  $X^{q-1-i}P$  dans la base  $\mathcal{F}$  et de même pour les autres colonnes.

Pour la même raison, on peut aussi remarquer que  $\text{Res}(P, Q)$  est le déterminant dans la base  $\mathcal{F}$  du système de vecteurs  $(X^{q-1}P, X^{q-2}P, \dots, XP, P, X^{p-1}Q, X^{p-2}Q, \dots, XQ, Q)$ .

**Exemple.** Par exemple si  $P = a_3X^3 + a_2X^2 + a_1X + a_0$  et  $Q = b_2X^2 + b_1X + b_0$  on a

$$\text{Res}(P, Q) = \begin{vmatrix} a_3 & 0 & b_2 & 0 & 0 \\ a_2 & a_3 & b_1 & b_2 & 0 \\ a_1 & a_2 & b_0 & b_1 & b_2 \\ a_0 & a_1 & 0 & b_0 & b_1 \\ 0 & a_0 & 0 & 0 & b_0 \end{vmatrix}.$$

**Définition B.18.** Soit  $P$  un polynôme de degré  $p \geq 1$  et soit  $a$  une constante.

On appelle **résultant** de  $P$  et  $a$  et on note  $\text{Res}(P, a)$  le déterminant de l'application linéaire  $\varphi: K_{p-1}[X] \rightarrow K_{p-1}[X]$  définie par  $\varphi(U) = aU$ . Autrement dit,  $\text{Res}(P, a) = a^p$ .

On appelle **résultant** de  $a$  et  $P$  et on note  $\text{Res}(a, P)$  le déterminant de l'application linéaire  $\varphi: K_{p-1}[X] \rightarrow K_{p-1}[X]$  définie par  $\varphi(U) = aU$ . Autrement dit,  $\text{Res}(a, P) = a^p$ .

**Remarque.** Avec la convention  $K_{-1}[X] = \{0\}$ , cette définition coïncide avec la définition précédente pour les polynômes non constants.

**Proposition B.19.** Soient  $P$  et  $Q$  deux polynômes non nuls dont l'un au moins n'est pas constant. On note  $p = \deg P$  et  $q = \deg Q$ . Alors

(1)  $\text{Res}(P, Q) = (-1)^{pq} \text{Res}(Q, P)$ .

(2)  $\text{Res}(\lambda P, \mu Q) = \lambda^q \mu^p \text{Res}(P, Q)$ .

**Démonstration.** Si  $P$  ou  $Q$  est constant, le résultat est évident. Supposons donc que  $P$  et  $Q$  ne sont pas constants.

(1) Rappelons que si on applique une permutation  $\gamma \in S_n$  aux colonnes (ou lignes) d'une matrice  $M$  de taille  $n \times n$  pour obtenir la matrice  $N$ , alors  $\det(N) = \varepsilon(\gamma) \det(M)$  où  $\varepsilon$  désigne la signature.

Soit  $\gamma = (p+q \ p+q-1 \ \dots \ 3 \ 2 \ 1) \in S_{p+q}$  la permutation circulaire. Notons que  $\varepsilon(\gamma) = (-1)^{p+q-1}$  car  $\gamma = (p+q-1 \ p+q-2)(p+q-2 \ p+q-3) \dots (3 \ 2)(2 \ 1)(1 \ p+q)$  est un produit de  $p+q-1$  transpositions. Si on permute les colonnes de  $\begin{pmatrix} A & B \end{pmatrix}$  avec  $\gamma$ , cela revient à décaler chaque colonne d'un cran vers la gauche et la première colonne devient la dernière.

Pour passer de la matrice  $\begin{pmatrix} A & B \end{pmatrix}$  à la matrice  $\begin{pmatrix} B & A \end{pmatrix}$ , on doit donc appliquer la permutation  $\gamma^q$  aux colonnes. Puisque  $\varepsilon$  est un morphisme de groupes,  $\varepsilon(\gamma^q) = \varepsilon(\gamma)^q = (-1)^{q(p+q-1)} = (-1)^{pq+q^2-q} = (-1)^{pq}$  car  $q^2 - q$  est pair. On en déduit que  $\text{Res}(P, Q) = (-1)^{pq} \text{Res}(Q, P)$ .

(2) Cela découle de la multilinéarité du déterminant (chacune des  $q$  colonnes  $C_P$  de  $A$  est multipliée par  $\lambda$  et chacune des  $p$  colonnes  $C_Q$  de  $B$  est multipliée par  $\mu$ ). ✓

**Proposition B.20.** Soient  $P$  et  $Q$  deux polynômes non nuls dont l'un au moins n'est pas constant. On note  $p = \deg P$  et  $q = \deg Q$ . Les assertions suivantes sont équivalentes.

(i)  $P$  et  $Q$  ont un facteur commun non-constant.

(ii)  $\text{Res}(P, Q) = 0$ .

(iii) Il existe  $U \in K_{q-1}[X]$  et  $V \in K_{p-1}[X]$  tels que  $UP + VQ = 0$ .

**Démonstration.** Si  $P$  ou  $Q$  est constant, il est facile de vérifier qu'aucune des trois assertions n'est vraie. Supposons donc que  $P$  et  $Q$  ne sont pas constants.

➤ (i)⇒(ii). Soit  $R$  un diviseur commun de  $P$  et  $Q$ . Alors pour tout  $(U, V)$  le polynôme  $R$  divise  $\varphi(U, V) = UP + VQ$ . En particulier,  $\varphi$  n'est pas surjective et donc  $\text{Res}(P, Q) = \det \varphi = 0$ .

➤ (ii)⇒(iii). Puisque  $\det \varphi = \text{Res}(P, Q) = 0$ , l'application linéaire  $\varphi$  n'est pas injective. Soit  $(U, V) \in \text{Ker } \varphi$ . Alors  $UP + VQ = \varphi(U, V) = 0$ .

➤ (iii)⇒(i). Supposons que (iii) est vérifiée et que  $P$  et  $Q$  soient premiers entre eux. Le polynôme  $P$  divise  $VQ = -UP$  donc par la condition de Gauss ( $K[X]$  est factoriel) le polynôme  $P$  divise  $V$  donc  $p = \deg P \leq \deg V \leq p-1$  donc on a obtenu une contradiction. ✓

Dans la suite, on fixe un polynôme  $P$  de degré  $p \geq 1$  et de coefficient dominant  $a_p$ . On note  $E = K[X]/(P)$ .

**Lemme B.21.** Notons  $x$  la classe de  $X$  dans  $E$ . Alors  $E$  est un  $K$ -espace vectoriel de dimension  $p$  et de base  $\mathcal{B} = \{x^{p-1}, x^{p-2}, \dots, x, 1\}$ .

*Démonstration.* Pour vérifier que  $E$  est bien un  $K$ -espace vectoriel, il suffit de vérifier que  $(P) = \{PQ \mid Q \in K[X]\}$  est un sous- $K$ -espace vectoriel de  $K[X]$  (exercice). Nous allons vérifier que  $\mathcal{B}$  est une base de  $E$ .

Soit  $u \in E$ . Alors il existe  $Q \in K[X]$  tel que  $u = \overline{Q} = Q(x)$ . La division euclidienne de  $Q$  par  $P$  donne  $Q = AP + R$  avec  $\deg R < p$ . On a alors  $u = Q(x) = A(x)P(x) + R(x) = R(x) \in \text{vect}\{\mathcal{B}\}$ . Donc  $\mathcal{B}$  est une famille génératrice de  $E$ .

Supposons maintenant que  $\sum_{i=0}^{p-1} \lambda_i x^i = 0$  avec  $(\lambda_0, \dots, \lambda_{p-1}) \in K^p$ . Posons  $Q = \sum_{i=0}^{p-1} \lambda_i X^i$ . Alors  $Q(x) = 0$  donc  $Q \in (P)$  et donc  $P$  divise  $Q$ . Mais  $\deg Q < p = \deg P$  donc  $Q = 0$  et donc  $\lambda_i = 0$  pour tout  $i$ . Donc  $\mathcal{B}$  est libre et c'est bien une base de  $E$ . ✓

**Lemme B.22.** Soit  $Q \in K[X] \setminus \{0\}$ . L'application  $\theta_Q: E \rightarrow E$  qui à un vecteur  $u$  associe  $Q(x)u$  est une application linéaire.

De plus, si pour  $i \in \llbracket 0; p-1 \rrbracket$  on note  $R_i$  le reste de la division euclidienne de  $X^i Q$  par  $P$ , alors la matrice de  $\theta_Q$  dans  $\mathcal{B}$  est la matrice du système de vecteurs  $\{R_{p-1}, \dots, R_0\}$  dans la base  $\mathcal{F}$  de  $K_{p+q-1}[X]$ .

*Démonstration.* Il est facile de vérifier que  $\theta_Q$  est une application linéaire.

De plus, on a  $\theta_Q(x^i) = Q(x)x^i = R_i(x)$  comme dans la démonstration du lemme précédent. Donc la  $j^{\text{me}}$  colonne de la matrice de  $\theta_Q$  est obtenue en écrivant les coefficients de  $R_j(x)$  dans la base  $\mathcal{B}$ . Puisque  $\deg R_j < p$ , ceci revient à écrire les coefficients de  $R_j$  dans la base  $\{X^{p-1}, \dots, X, 1\}$  de  $K_{p-1}[X]$  ou dans la base  $\mathcal{F}$  de  $K_{p+q-1}[X]$ . ✓

**Lemme B.23.** Soit  $Q \in K[X] \setminus \{0\}$  et soit  $q = \deg Q$ . Alors  $\text{Res}(P, Q) = a_p^q \det(\theta_Q)$ .

*Démonstration.* Si  $q = 0$  alors  $Q = b_0 \in K$  et on a  $\det(\theta_Q) = b_0^p = \text{Res}(P, b_0)$ . Supposons donc que  $q > 0$ .

On rappelle que  $\text{Res}(P, Q)$  est le déterminant dans la base  $\mathcal{F}$  du système de vecteurs  $(X^{q-1}P, X^{q-2}P, \dots, XP, P, X^{p-1}Q, X^{p-2}Q, \dots, XQ, Q)$ . Avec les notations des lemmes précédents, puisque  $P$  est un des vecteurs de la famille et que  $X^i Q = A_i P + R_i$  pour des polynômes  $A_i$ , il s'agit du déterminant dans la base  $\mathcal{F}$  du système de vecteurs  $(X^{q-1}P, X^{q-2}P, \dots, XP, P, R_{p-1}, \dots, R_0)$ . La matrice dans la base  $\mathcal{F}$  de ce système de vecteurs s'écrit  $\begin{pmatrix} T & 0 \\ N & M \end{pmatrix}$  où  $M$  est la matrice  $p \times p$  de  $\{R_{p-1}, \dots, R_0\}$  dans  $\mathcal{F}$  et donc de  $\theta_Q$  dans  $\mathcal{B}$ , et où la matrice  $T$  est triangulaire inférieure  $q \times q$  de termes diagonaux tous égaux à  $a_p$ . Ainsi,  $\text{Res}(P, Q) = \begin{vmatrix} T & 0 \\ N & M \end{vmatrix} = a_p^q \det(M) = a_p^q \det(\theta_Q)$ . ✓

**Proposition B.24.** Soit  $\alpha \in K$  et soient  $P, Q, R$  des polynômes de  $K[X]$ . Alors

- (i)  $\text{Res}(X - \alpha, Q) = Q(\alpha)$ ,
- (ii)  $\text{Res}(P, QR) = \text{Res}(P, Q) \text{Res}(P, R)$  et  $\text{Res}(PR, Q) = \text{Res}(P, Q) \text{Res}(R, Q)$ ,
- (iii) Si  $R$  est le reste de la division euclidienne de  $Q$  par  $P$  et si  $\deg R = r \geq 0$  alors  $\text{Res}(P, Q) = a_p^{q-r} \text{Res}(P, R)$ .

*Démonstration.* (i) Ici  $p = 1$ ,  $a_p = 1$  et  $R_0 = Q(\alpha)$  donc  $\theta_Q = Q(\alpha) \text{id}_K$  et finalement  $\text{Res}(X - \alpha, Q) = \det(Q(\alpha)) = Q(\alpha)$ .

Une autre démonstration ne faisant pas intervenir les lemmes précédents mais seulement les propriétés du déterminant.

Posons  $Q = \sum_{i=0}^q b_i X^i$ . Alors  $\text{Res}(X - \alpha, Q)$  est le déterminant  $(q+1) \times (q+1)$  suivant :

$$\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & b_q \\ -\alpha & 1 & 0 & \cdots & 0 & b_{q-1} \\ \vdots & & & \cdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_1 \\ 0 & 0 & 0 & \cdots & -\alpha & b_0 \end{vmatrix}.$$

On effectue l'opération suivante sur les lignes :

$$L_{q+1} \leftarrow L_{q+1} + \alpha L_q + \alpha^2 L_{q-1} + \cdots + \alpha^q L_1 = \sum_{i=0}^q \alpha^i L_{q+1-i}.$$

On a alors

$$\text{Res}(P, Q) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & b_q \\ -\alpha & 1 & 0 & \cdots & 0 & b_{q-1} \\ \vdots & & & \cdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_1 \\ 0 & 0 & 0 & \cdots & 0 & Q(\alpha) \end{vmatrix} = Q(\alpha) \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ -\alpha & 1 & 0 & \cdots & 0 \\ \vdots & & & \cdots & \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = Q(\alpha)$$

en développant suivant la dernière ligne pour obtenir le déterminant d'une matrice triangulaire avec des 1 sur la diagonale.

- (ii) Notons  $r = \deg R$ . D'après le lemme précédent, on a  $\text{Res}(P, QR) = a_p^{q+r} \det(\theta_{QR})$ . Mais il est facile de vérifier que  $\theta_{QR} = \theta_R \circ \theta_Q$  donc

$$\text{Res}(P, QR) = a_p^{q+r} \det(\theta_{QR}) = a_p^q a_p^r \det(\theta_R) \det(\theta_Q) = \text{Res}(P, Q) \text{Res}(P, R)$$

en utilisant à nouveau le lemme précédent.

La deuxième partie découle de la première et de la proposition B.19.

- (iii) Dans  $E$  on a  $Q(x) = R(x)$  et on en déduit que  $\theta_Q = \theta_R$ . Le résultat découle alors du lemme précédent. ✓

**Théorème B.25.** Si  $P \in K[X]$  est scindé sur  $K$  de racines  $\alpha_1, \dots, \alpha_p$ , alors

$$\text{Res}(P, Q) = a_p^q Q(\alpha_1) \cdots Q(\alpha_p).$$

Si de plus  $Q \in K[X]$  est scindé sur  $K$  de racines  $\beta_1, \dots, \beta_q$ , alors

$$\text{Res}(P, Q) = a_p^q b_q^p \prod_{i=1}^p \prod_{j=1}^q (\alpha_i - \beta_j).$$

*Démonstration.* On a  $P = a_p(X - \alpha_1) \cdots (X - \alpha_p)$  donc d'après la proposition B.19 on a  $\text{Res}(P, Q) = a_p^q \text{Res}((X - \alpha_1) \cdots (X - \alpha_p), Q)$ . On peut donc dans la suite supposer que  $a_p = 1$ .

Démontrons la première formule par récurrence sur  $p$ . On a déjà démontré dans la proposition précédente que le résultat est vrai pour  $p = 1$ . Supposons donc le résultat vrai pour les polynômes scindés de degré au plus  $p - 1$ . Soit  $P$  un polynôme scindé unitaire de racines  $\alpha_1, \dots, \alpha_p$ , il s'écrit  $P = R(X - \alpha_p)$  avec  $R = (X - \alpha_1) \cdots (X - \alpha_{p-1})$  scindé de degré  $p - 1$ . On a donc d'après la proposition précédente  $\text{Res}(P, Q) = \text{Res}(R(X - \alpha_p), Q) = \text{Res}(R, Q) \text{Res}(X - \alpha_p, Q) = (Q(\alpha_1) \cdots Q(\alpha_{p-1})) Q(\alpha_p)$  en utilisant l'hypothèse de récurrence.

Donc la première formule est vraie.

Si de plus  $Q = b_q \prod_{j=1}^q (X - \beta_j)$  alors  $\text{Res}(P, Q) = a_p^q \prod_{i=1}^p Q(\alpha_i) = a_p^q \prod_{i=1}^p b_q \prod_{j=1}^q (\alpha_i - \beta_j) = a_p^q b_q^p \prod_{i=1}^p \prod_{j=1}^q (\alpha_i - \beta_j)$ . ✓

On peut généraliser la définition de discriminant comme suit.

**Définition B.26.** Soit  $P \in K[X]$ . On définit le *discriminant* de  $P$  par

$$\text{Disc}(P) = (-1)^{p(p-1)/2} a_p^{-1} \text{Res}(P, P').$$

**Remarque.** Si  $P$  est scindé de racines  $\alpha_1, \dots, \alpha_p$  dans  $K$ , alors

$$\text{Disc}(P) = (-1)^{p(p-1)/2} a_p^{2p-2} \prod_{i \neq j} (\alpha_i - \alpha_j) = a_p^{2p-2} \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

On constate que pour  $a_p = 1$  on retrouve la définition précédente du discriminant.

**Corollaire B.27.** Soit  $P \in K[X]$ . Les polynômes  $P$  et  $P'$  sont premiers entre eux si, et seulement si,  $\text{Disc}(P) \neq 0$ .

En particulier, si  $P$  est scindé sur  $K$ , alors  $P$  n'a que des racines simples si, et seulement si,  $\text{Disc}(P) \neq 0$ .