UFR MATHÉMATIQUES
Université Clermont Auvergne

Master 1 Mathématiques

Algèbre 1

(Groupes finis et arithmétique dans les anneaux)

R. Taillefer

Rachel.Taillefer@uca.fr

2022-2023

version du 12 décembre 2022

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

Table des matières

Première partie :

Groupes

CHAPITRE 1

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 $*\colon G \times G \longrightarrow G$ 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 $E = \{1, \dots, n\} = [\![1\,;n]\!]$ est noté S_n. Si $n \geqslant 3$, alors S_n n'est pas abélien.

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

(4) $(\mathbb{C}^*, \cdot)$ $(= (\mathrm{GL}_1(\mathbb{C}), \cdot))$ est un groupe abélien.

Définition 1.2. *Soient G et G' des groupes. Un **morphisme de groupes** $f\colon G \longrightarrow G'$ 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 $\mathrm{Hom}(G, G')$.

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

*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* $\mathrm{Aut}(G)$.

On cherche à classifier 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 $\mathrm{Aut}(G)$ est un sous-groupe du groupe symétrique S_G.

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

➢ Soit $f \in \mathrm{Aut}(G)$. Il faut démontrer que la bijection réciproque f^{-1} est dans $\mathrm{Aut}(G)$; 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 $\mathrm{Aut}(G)$ alors $f \circ g \in \mathrm{End}(G)$; de plus, $f \circ g$ est une bijection donc $f \circ g \in \mathrm{Aut}(G)$. ✓

Exemple. Le déterminant, $\det\colon \mathrm{GL}_n(\mathbb{C}) \longrightarrow \mathbb{C}^*$, 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 $G \times G \to G$ induit une loi de groupe $H \times H \to H$. On en déduit que si $(x, y) \in H^2$ alors $xy \in H$.
Soit maintenant $x \in H$ et soit x^{-1} son inverse dans G. Puisque H est un groupe, il a un inverse $\overline{x} \in H$. Mais $\overline{x}$ est alors un inverse dans G. Par unicité de l'inverse d'un élément, on a $x^{-1} = \overline{x} \in H$.

➢ (2)⇒(3). 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 $(x,1) \in H$ 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}) et on obtient $xy^{-1} = (x^{-1})^{-1}y^{-1} \in H$.

➢ (4)⇒(1).

Soit $x \in H$ (H n'est pas vide). Alors $(x,x) \in H^2$ donc $1 = xx^{-1} \in H$. On en déduit que H possède un élément neutre.

Soit $x \in H$. Alors $(x,1) \in H^2$ 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, donc 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 $n\mathbb{Z} = \{na,\ a \in \mathbb{Z}\}$ 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 quite à changer son signe, 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 $0 \leqslant r < n$. 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 de l'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 $\operatorname{Im} f = f(G)$ 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 $\operatorname{Ker} f = f^{-1}(\{1_{G'}\})$ 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, $\operatorname{Im} f = f(G)$ 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 $\mathrm{Ker}\, f = f^{-1}(\{1_{G'}\})$ 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 $y = xh \in xH$.
La classe à gauche modulo H de x est souvent notée $\bar{x}$. **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 $H \to xH$ définie par $h \mapsto xh$ est une bijection, de bijection réciproque $xH \to H$ 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.*
(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 $G = \cup_{i\in I} x_iH$ et $x_iH \cap x_jH = \emptyset$ si $i \neq j$. Alors $\mathrm{card}(I) = [G : H]$ et comme $|x_iH| = |H|$ pour tout $i \in I$, on trouve bien que $|G| = \mathrm{card}(I)|H| = [G : H]|H|$. ✓

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 $G = S_4$, $K = \{\mathrm{id}\} \triangleleft S_4$, $H = \{\mathrm{id}; (1\,2)\}$.
Autre exemple : $G = S_4$, $K = V_4 = \{\mathrm{id}; (1\,2)(3\,4); (1\,3)(2\,4); (1\,4)(2\,3)\}$ 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 τ 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 $L = \{\mathrm{id}; (1\,2)\}$ 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 $K = \{\mathrm{id}; (1\,2)(3\,4)\}$. 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 $\mathrm{Ker}\, f \triangleleft G$.

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

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

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

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 π soit un morphisme de groupes.

Démonstration. Soit $x \in G$, par définition $\pi(x) = xH$. Puisque π 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 $(xy)^{-1}(x'y') = y^{-1}x^{-1}xhyk = y^{-1}hyk$. 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 : $(xH.yH).zH = xyH.zH = (xy)zH = x(yz)H = xH.(yH.zH)$ poru 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 π est alors un morphisme de groupes (la loi a été construite pour cela). ✓

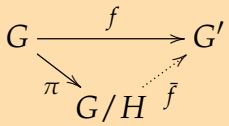
Exemple. Soit $n \in \mathbb{N}^*$. L'ensemble des classes (à gauche) modulo n dans $\mathbb{Z}$ est $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$. On a $|\mathbb{Z}/n\mathbb{Z}| = n$ et la loi du groupe est définie par $\overline{k} + \overline{l} = \overline{k+l}$, pour tout $(k,l)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

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

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 $f\colon G \to G'$ tel que $H = \operatorname{Ker} f$.

Théorème 1.14. Soit $f\colon G \longrightarrow G'$ un morphisme de groupes.

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



2. **(Premier théorème d'isomorphisme)** Le morphisme f induit un isomorphisme
$$\tilde{f}\colon G/\operatorname{Ker} f \longrightarrow \operatorname{Im} f.$$

Démonstration. (1) Soit $y \in G/H$. Puisque π 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 $x^{-1}x' \in \operatorname{Ker} \pi = H \subset \operatorname{Ker} f$, 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.

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

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

Correction. On considère le morphisme de groupes $\det\colon \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^*$. 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 $\pi : G \longrightarrow G/H$ 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 :

$$\{\text{sous-groupes (normaux) de } G \text{ contenant } H\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{sous-groupes (normaux) de } G/H\}$$

$$\begin{array}{rcl} K & \longmapsto & \pi(K) = K/H \\ \pi^{-1}(K^*) & \longmapsfrom & K^* \end{array}$$

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 π (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 classifier 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 $|G/H| < |G|$. Alors, par hypothèse de récurrence, on connait 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 $H = \{x_1 \dots x_n \mid x_i \in S \text{ ou } x_i^{-1} \in S\}$. 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 H 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 μ_n des racines n-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

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

où r est la rotation d'angle $\dfrac{2\pi}{n}$ 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 $0 \leqslant k \leqslant n-1$ et $0 \leqslant \ell \leqslant 1$. 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 $0 \leqslant k < n$ et $0 \leqslant \ell \leqslant 1$ est unique donc ces éléments sont deux à deux distincts. Supposons le contraire, il existe alors $k' \in [\![0\,;n-1]\!]$ 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 $f : G \longrightarrow H$ 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 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 $o(x) \leqslant |G|$. En effet si $n = |G|$, le sous-ensemble $\{1, x, \ldots, x^n\}$ de G possède nécessairement deux éléments égaux : il existe $(i,j) \in [\![0\,;n]\!]^2$ avec $i > j$ tel que $x^i = x^j$, ce qui donne $x^{i-j} = 1$ avec $0 < i - j \leqslant n$, 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 $m \in \mathbb{N}^*$ tel que $x^m = 1$. Alors x est d'ordre fini et $o(x) \mid m$.

(2) Si x est d'ordre fini, alors $|\langle x\rangle| = o(x)$.

(3) Si G est fini, alors $x^{|G|} = 1$ et $o(x) \mid |G|$.

Démonstration. (1) On effectue la division euclidienne de m par $o(x)$, il existe donc des entiers q et r avec $0 \leqslant r < o(x)$ 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.

(2) Posons $n = o(x)$. Montrons que $\{1, x, \ldots, x^{n-1}\} = \langle x\rangle$. L'inclusion $\{1, x, \ldots, x^{n-1}\} \subset \langle x\rangle$ 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 $0 \leqslant r < n$. Donc $a = x^{nq+r} = (x^n)^q x^r = x^r$ et $a \in \{1, \ldots, x^{n-1}\}$. Finalement il est clair, puisque $o(x) = n$, que l'ensemble $\{1, x, \ldots, x^{n-1}\}$ possède bien n éléments distincts.

(3) 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 entier m. Notons $p = o(a)$, $q = o(b)$.

(1) Soit $\mu = \text{ppcm}(p, q)$, alors il existe des 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 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. $D_2 = \text{vect}\{u_2\}$). 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 2θ.

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

➢ Exemple plus concret : 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 $f : G \to H$ 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 $\overline{1}$.

(3) Pour $n \in \mathbb{N}^*$, le groupe μ_n des racines n-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 $f : \mathbb{Z} \longrightarrow G$ le morphisme de groupes défini par $f(k) = x^k$ pour tout $k \in \mathbb{Z}$. Alors f est surjectif. Puisque $\operatorname{Ker} f$ est un sous-groupe de $\mathbb{Z}$, il existe $n \in \mathbb{N}$ tel que $\operatorname{Ker} f = n\mathbb{Z}$. Ainsi le 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 $1 \leqslant i \leqslant n-1$.

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 $\operatorname{pgcd}(k, n) = 1$.

Démonstration. (1) Soit d un diviseur de n et soit $a = x^k$ avec $k = \frac{n}{d}$. Alors $o(a) = \frac{o(x)}{\operatorname{pgcd}(o(x),k)} = \frac{n}{\operatorname{pgcd}(n,\frac{n}{d})} = \frac{n}{\frac{n}{d}} = d$, 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 $m = \min\{\ell \in [\![1\,;n-1]\!] \mid x^\ell \in H\}$. 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 $0 \leqslant r < m$ 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 $o(x^m) = \frac{n}{\operatorname{pgcd}(n,m)} = \frac{dk}{\operatorname{pgcd}(n,m)}$, donc $\operatorname{pgcd}(n, m) = k$ 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 $o(x^k) = \frac{n}{\operatorname{pgcd}(n,k)}$, on en déduit que x^k engendre C_n si, et seulement si, $\operatorname{pgcd}(n, k) = 1$. ✓

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, $|G| = p \geqslant 2$, 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 $|\langle x^a \rangle| = o(x^a) \leqslant b < n$, 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 $f : G \longrightarrow H$ tel que $f(x) = h$.

Démonstration. Soient $u : \mathbb{Z} \longrightarrow G$ et $v : \mathbb{Z} \longrightarrow H$ 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 $\operatorname{Ker} u = n\mathbb{Z}$, donc par le premier théorème d'isomorphisme u induit un isomorphisme $\bar{u} : \mathbb{Z}/n\mathbb{Z} \to G$ tel que $\bar{u}(\bar{1}) = x$.

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

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

L'unicité provient du fait que $G = \langle x \rangle$ (voir la remarque page 19). ✓

V Produit direct de groupes

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 :*

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

*est un groupe. L'élement 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 :
$$o((x^r,y^s)) = \text{ppcm}(o(a^r), o(b^s)) = \text{ppcm}\left(\frac{o(a)}{\text{pgcd}(o(a),r)}, \frac{o(b)}{\text{pgcd}(o(b),s)}\right)$$
$$= \text{ppcm}\left(\frac{n}{\text{pgcd}(n,r)}, \frac{m}{\text{pgcd}(m,s)}\right).$$
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 $nm = \text{ppcm}\left(\frac{n}{\text{pgcd}(n,r)}, \frac{m}{\text{pgcd}(m,s)}\right) \leqslant \text{ppcm}(n,m) \leqslant nm$ et donc $\text{ppcm}(n,m) = nm$ et $\text{pgcd}(n,m) = 1$. ✓

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

Pour $k \in \mathbb{Z}$, notons $\pi_k : \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ la projection canonique. Soit $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ 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
$$x = unb + (1-un)a = un(b-a) + a$$
$$= (1-vm)b + vmb = vm(a-b) + b$$
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 $\bar{f} : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

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 $\psi : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. On doit démontrer que $\text{pgcd}(n,m) = 1$.

Notons $\alpha = \psi \circ \pi_{nm} : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, soient $p_1 : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ et $p_2 : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ les projections sur chacune des composantes et soient $\alpha_1 = p_i \circ \alpha$ pour $i \in \{1,2\}$. On vérifie facilement que

- ➢ $\text{Ker}\, \alpha = \text{Ker}(\pi) = nm\mathbb{Z}$ *(car ψ est injectif)* ;
- ➢ $\text{Ker}(\alpha) = \text{Ker}(\alpha_1) \cap \text{Ker}(\alpha_2)$;
- ➢ *α_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- a-dire que $u = n$ et finalement* $\text{Ker}(\alpha_1) = n\mathbb{Z}$.

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

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 $m\colon H \times K \longrightarrow HK$, $(x,y) \mapsto xy$, 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 $\mathrm{cl}(x,y)$ 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 $\mathrm{cl}(x,y)$ est l'ensemble des antécédents de xy). Soient $(x_i,y_i)_{1 \leqslant i \leqslant r}$ les représentants distincts des diverses classes d'équivalence pour $\mathcal{R}$, on a donc $H \times K = \coprod_{i=1}^{r} \mathrm{cl}(x_i,y_i)$ (réunion disjointe) et $|(H \times K)/\mathcal{R}| = |HK| = r$.

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

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

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 $x_1 = h_1k_1$ et $x_2 = h_2k_2$.

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

De plus, $k_1h_2 \in KH = HK$ donc il existe $(h',k') \in H \times K$ tel que $k_1h_2 = h'k'$, donc $x_1x_2 = h_1k_1h_2k_2 = h_1h'k'k_2 \in HK$.

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 $k^{-1}hk \in H$, 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 $gxg^{-1} = ghg^{-1}gkg^{-1} \in HK$ car $ghg^{-1} \in H$ et $gkg^{-1} \in K$. 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 $(h,k) \in \operatorname{Ker} m$. 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 $\operatorname{Ker} m = \{(1,1)\}$ 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 $\operatorname{pgcd}(|H|,|K|) = 1$. Montrer que $G \cong H \times K$. Voir travaux dirigés

Correction. Puisque $\operatorname{pgcd}(|H|,|K|) = 1$, grâce au théorème de Lagrange on obtient $|H \cap K| = 1$ donc $H \cap K = \{1\}$.

On a alors $|HK| = \dfrac{|H||K|}{|H \cap K|} = |H||K| = |G|$ 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 $|G| \geqslant 2$.

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

✦ Hérédité : soit $d \in \mathbb{N}^*$, $d \geqslant 3$ 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 $\pi : G \to G/\langle x \rangle$ 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 $n \geqslant 2$ 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 $\alpha : G/L \to (\mathbb{Z}/p\mathbb{Z})^{n-1}$. Notons $\pi : G \to G/L$ la projection canonique. Pour tout i entier avec $1 \leqslant i \leqslant n-1$, 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 $i^{\text{ième}}$ position. Alors $\{\alpha^{-1}(e_1), \dots, \alpha^{-1}(e_{n-1})\}$ engendre G/L car α 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 π 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 $H = \{g_1^{u_1} \cdots g^{u_{n-1}} \mid 0 \leqslant u_i \leqslant p-1\}$, donc $|H| \leqslant p^{n-1}$ 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 $u_i \in [\![0; p-1]\!]$ pour tout i. On a donc $0 = \alpha(1) = \alpha(\pi(y)) = \sum_{i=1}^{n-1} u_i e_i = (\overline{u}_1, \dots, \overline{u}_{n-1})$, donc $\overline{u}_i = \overline{0}$ 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 $G = |x|$ 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 $G \cong C_{pq}$.

➢ 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 $\operatorname{Ker} f = H \cap K$. On conclut avec le premier théorème d'isomorphisme.

(2) Soit $\pi : G \to G/H$ 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 $\pi' : G/H \to (G/H)/(K/H)$ la surjection canonique. Alors $\pi' \circ \pi : G \to (G/H)/(K/H)$ est un morphisme de groupes surjectif. On vérifie facilement que $\operatorname{Ker}(\pi' \circ \pi) = \pi^{-1}(K/H) = K$ (théorème de correspondance) et on conclut avec le premier théorème d'isomorphisme. ✓

VI Suites exactes

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

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

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

(i) *i est injectif,*

(ii) *p est surjectif,*

(iii) $\operatorname{Im} i = \operatorname{Ker} p$.

Remarque. Le groupe H est isomorphe à $\operatorname{Im} i$ et $\operatorname{Im} i = \operatorname{Ker} p$ 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 $i : H \to G$ l'inclusion (on a donc $i(a) = g^4$) et $p : G \to K$ défini par $p(g) = k$.

Alors la suite $1 \to H \xrightarrow{i} G \xrightarrow{p} K \to 1$ 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 $\operatorname{Im} i \subset \operatorname{Ker} p$ (notons que $\operatorname{Im} i = \langle i(a) \rangle = \langle g^4 \rangle$). Enfin, soit $x \in \operatorname{Ker} p$. 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 $x = g^{4m} = i(a)^m = i(a^m) \in \operatorname{Im} i$. Donc $\operatorname{Ker} p = \operatorname{Im} i$.

(2) Soient G_1 et G_2 deux groupes. Soit $i \colon G_1 \to G_1 \times G_2$ le morphisme défini par $i(x) = (x, 1)$ pour tout $x \in G_1$ et soit $p \colon G_1 \times G_2 \to G_2$ 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 $1 \to G_1 \xrightarrow{i} G_1 \times G_2 \xrightarrow{p} G_2 \to 1$ 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 $\operatorname{Im} i \subset \operatorname{Ker} p$. Enfin, soit $(x_1, x_2) \in \operatorname{Ker} p$, alors $x_2 = 1$ donc $(x_1, x_2) = (x_1, 1) = i(x_1) \in \operatorname{Im} i$ donc $\operatorname{Ker} p = \operatorname{Im} i$.

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

Alors $H \cong \operatorname{Im} i$ et $K \cong G/\operatorname{Im} i$. 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, $i \colon H \to \operatorname{Im} i$ est un morphisme surjectif. Il est injectif par hypothèse donc $H \cong \operatorname{Im} i$.

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

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

Exemple. On reprend la suite exacte $1 \to G_1 \to G_1 \times G_2 \to G_2 \to 1$ de l'exemple précédent.

Alors $G_2 \cong (G_1 \times G_2)/(G_1 \times \{1\})$.

CHAPITRE 2

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 $E^* = \mathcal{L}(E, \mathbb{K})$). 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 $\chi : G \to \mathbb{C}^*$.*

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

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

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

(3) La signature $\varepsilon : S_n \to \mathbb{C}^*$ (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*

$$\begin{array}{ccc} \widehat{G} \times \widehat{G} & \longrightarrow & \widehat{G} \\ (\chi, \psi) & \longmapsto & \chi \cdot \psi : \begin{array}{l} G \to \mathbb{C}^*, \\ g \mapsto \chi(g)\psi(g) \end{array} \end{array}$$

*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 :

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

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 $\alpha^{-1} : g \to \alpha(g)^{-1}$ 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 effetm 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 χ^{-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 $f : G \to H$ est un morphisme de groupes, alors l'application

$$\widehat{f} : \widehat{H} \to \widehat{G}$$
$$\chi \mapsto \chi \circ f$$

est un morphisme de groupes.

Démonstration. Exercice. Voir travaux dirigés

Tout d'abord, pour tout $\chi \in \widehat{H}$ l'application $\chi \circ f : G \to \mathbb{C}^*$ 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

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

Ils induisent les morphismes $\widehat{\imath} : \widehat{G \times H} \to \widehat{G}$ et $\widehat{\jmath} : \widehat{G \times H} \to \widehat{H}$ et on peut définir l'application

$$\theta : \widehat{G \times H} \longrightarrow \widehat{G} \times \widehat{H}$$
$$\chi \longmapsto (\widehat{\imath}(\chi), \widehat{\jmath}(\chi)) = (\chi \circ i, \chi \circ j)$$

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

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

✓

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 $\chi_\omega \colon G \to \mathbb{C}^*$ tel que $\chi_\omega(g) = \omega$.

Soit $\psi \colon \widehat{G} \to \mathbb{C}^*$ 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 ψ est à valeurs dans μ_n et, pour tout $\omega \in \mu_n$, le caractère χ_ω est l'unique antécédent de ω par ψ.

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

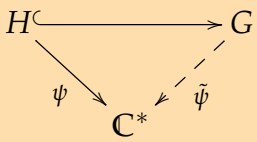
Enfin, G est cyclique d'ordre n donc $G \cong C_n \cong \mu_n \cong \widehat{G}$. ✓

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 $G_1, \ldots, G_n$ 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 $\tilde{\psi}_{|H} = \psi$.



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, χ) 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, ψ) est dans $\mathcal{E}$. On peut donc considérer le nombre entier

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

Soit (K, χ) 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 φ doit être un morphisme qui prolonge χ. 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, ω 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 φ 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 φ est bien définie.

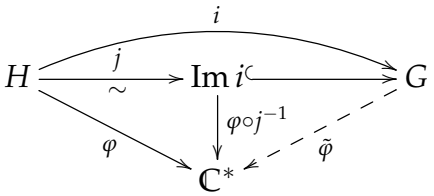
On vérifie facilement que φ est un morphisme de groupes (G est abélien) et $\varphi_{|N} = \chi$ par construction, donc $\varphi_{|H} = \psi$ et finalement $(N, \varphi) \in \mathcal{E}$ avec $|N| > |K| = m$. On a obtenu une contradiction.

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

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

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

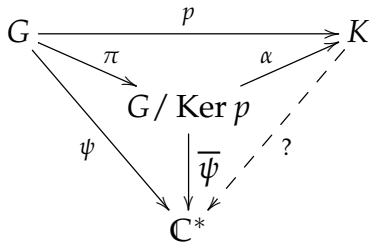
Vérifions que $\widehat{\imath}$ est surjectif. Soit $\varphi \in \widehat{H}$. *(Moralement, on va prolonger φ à G mais il faut passer par le sous-groupe $\operatorname{Im}(i)$ de G.)* Soit $j\colon H \to \operatorname{Im} i$ l'isomorphisme obtenu a partir de i en restreignant le groupe d'arrivée. On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



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

Soit maintenant $\chi \in \widehat{K}$. Alors $\widehat{\imath} \circ \widehat{p}(\chi) = \chi \circ p \circ i$. 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 $\widehat{\imath} \circ \widehat{p}(\chi) = \mathbb{1}$ et donc que $\operatorname{Im} \widehat{p} \subset \operatorname{Ker} \widehat{\imath}$.

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



✓

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

➢ Hérédité. Soit G un groupe abélien d'ordre $n \geqslant 4$. Supposons que pour tout groupe abélien H d'ordre $\leqslant n-1$ 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 $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ où i est l'inclusion et π est la projection canonique. On en déduit une suite exacte $1 \to \widehat{K} \to \widehat{G} \to \widehat{H} \to 1$ 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 $\varepsilon : S_3 \to \mathbb{C}^*$ est un caractère non trivial, donc $|\widehat{S_3}| \geqslant 2$.

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 $\chi : \widehat{S_3} \to \mathbb{C}^*$ un caractère. On remarque que $\chi((12))^2 = \chi((12)) = \chi(\mathrm{id}) = 1$ donc $\chi((12)) \in \{\pm 1\}$. De plus, puisque $\mathbb{C}^*$ est abélien et χ 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 χ 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 $n \in \mathbb{N}$, $n \geqslant 3$: on a $\left|\widehat{S_n}\right| = 2$ et $\widehat{S_n} = \{\mathbb{1}, \varepsilon\}$.

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

$$\begin{array}{ccl} G & \longrightarrow & \widehat{\widehat{G}} \\ g & \longmapsto & \varepsilon_g : \ \widehat{G} \to \mathbb{C}^* \\ & & \qquad \psi \mapsto \psi(g) \end{array}$$

est un isomorphisme.

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

Notons $f : G \to \widehat{\widehat{G}}$ 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 $\psi \in \widehat{G}$. 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 $g \in \operatorname{Ker} f$, on a donc $\varepsilon_g = \mathbb{1}$, 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 ω 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 $\operatorname{Ker} f = \{1\}$.

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 l'entier défini par*

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

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

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

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

Soit maintenant σ un élément de S_n. On sait que σ peut s'écrire comme un produit de cycles disjoints $\gamma_1 \cdots \gamma_r$. Notons d_i la longueur de γ_i pour tout i. Puisque les γ_i sont disjoints, ils commutent deux à deux, donc l'ordre de σ est $\operatorname{ppcm}(d_1, \dots, d_r)$. *Or chacun des d_i est dans $\{1, 2, \dots, n\}$, donc l'ordre de σ divise* $\operatorname{ppcm}(1, 2, \dots, n)$. *On en déduit finalement que* $\exp(S_n)$ *divise* $\operatorname{ppcm}(1, 2, \dots, n)$ *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 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 ω une racine primitive m-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 χ est μ_m puisque χ est à valeurs dans μ_m et ω engendre μ_m ; de plus, $|\langle g \rangle| = |\mu_m|$ donc χ induit un isomorphisme de $\langle g \rangle$ sur μ_m. Il existe, par le théorème 2.7, $\chi' \in \widehat{G}$ qui prolonge χ. 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 $\pi : G \to G/\langle g \rangle$ est la surjection canonique. Le morphisme Φ est injectif : en effet, soit $x \in \operatorname{Ker} \Phi$, alors $\pi(x) = 1$ donc $x \in \langle g \rangle$ et donc $1 = \chi'(x) = \chi(x)$ donc $x = 1$ puisque χ est injectif. De plus, $|\mu_m||G/\langle g \rangle| = |\langle g \rangle| \frac{|G|}{|\langle g \rangle|} = |G|$ donc Φ 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, la proposition 2.5 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 $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, où $p_1, \ldots, p_r$ sont des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_r$ sont dans $\mathbb{N}^*$. Il existe des sous-groupes $H_1, \ldots, H_r$ de G, d'ordres respectifs $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$, tels que

$$G \simeq H_1 \times \cdots \times H_r$$

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

Démonstration. Puisque G est un groupe fini abélien, il existe des groupes cycliques $K_1, \ldots, K_s$ 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 $\{p_1, \ldots, p_r\}$. On peut donc écrire, pour tout j avec $1 \leqslant j \leqslant s$, $K_j = L_{j,p_1} \times \cdots \times L_{j,p_r}$ 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 $\varphi \colon G \xrightarrow{\sim} H_1' \times \cdots \times H_r'$. Pour tout i on a $\left|H_i'\right| = p_i^{\beta_i}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$. De plus, $|G| = \prod_{i=1}^r \left|H_i'\right| = p_1^{\beta_1} \cdots p_r^{\beta_r}$, donc pour tout i on a $\beta_i = \alpha_i$ et donc $\left|H_i'\right| = p_i^{\alpha_i}$.

Pour tout $i \in [\![1\,;r]\!]$, soit $H_i = \varphi^{-1}(\{1\}^{i-1} \times H_i' \times \{1\}^{r-i}) \subset G$. On a alors $H_i \cong H_i'$ et $G \cong H_1 \times \cdots \times H_r$. De plus, $G = H_1 \cdots H_r$ (pour tout élément x de G, il existe $(h_1', \ldots, h_r') \in H_1' \times \cdots \times H_r'$ tel que $x = \varphi^{-1}(h_1', \ldots, h_r') = \varphi^{-1}\left(\prod_{i=1}^r (1, \ldots, 1, h_i', 1, \ldots, 1)\right) = \prod_{i=1}^r \varphi^{-1}(1, \ldots, 1, h_i', 1, \ldots, 1) \in H_1 \cdots H_r$).

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. Alors $g = h_1 \cdots h_r$ avec $h_k \in H_k$ pour tout $k \in [\![1\,;r]\!]$. Puisque G est commutatif, les h_k commutent et de plus leurs ordres sont premiers entre eux deux à deux. Donc $o(g) = \prod_{k=1}^r o(h_k)$. On en déduit que pour tout $k \neq i$ on doit avoir $h_k = 1$ et donc $g = h_i \in H_i$. 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 $(d_1, \ldots, d_r)$ de nombres entiers supérieurs ou égaux à 2 tels que $d_1 \mid d_2 \mid \cdots \mid d_{r-1} \mid d_r$ et

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

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 $\exp(G) = \exp(C_{d_1} \times \cdots \times C_{d_r})$. Le générateur de C_{d_r} est d'ordre d_r, donc $d_r \mid \exp(G)$. Soit maintenant x un élément quelconque de $C_{d_1} \times \cdots \times C_{d_r}$. Posons $x = (x_1, \ldots, x_r)$

avec $x_i \in C_{d_i}$ pour tout i avec $1 \leqslant i \leqslant r$ et soit $y_i = (1, \dots, 1, x_i, 1, \dots, 1)$. Alors $x = y_1 \cdots y_r$ et les y_i commutent donc $o(x) = \text{ppcm}\{o(y_i) \mid 1 \leqslant i \leqslant r\}$. 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

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

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 $\left|L_{1,p_i}\right| \mid \left|L_{2,p_i}\right| \mid \cdots \mid \left|L_{s_i,p_i}\right|$.

Soit $D_r = L_{s_1,p_1} \times \cdots \times L_{s_t,p_t}$. 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 $D_{r-1} = L_{s_1-1,p_1} \times \cdots \times L_{s_t-1,p_t}$. 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 maximaux 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 $a_1 \leqslant a_2 \leqslant \dots \leqslant a_s$. Les éléments d'ordre maximal de G sont donc d'ordre p^{a_s}. On note $k = |\{i \in [\![1\,;s]\!] \mid a_i = a_s\}|$.

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 $o(x) = \text{ppcm}\{o(x_i) \mid 1 \leqslant i \leqslant s\}$). Soit α un générateur fixé de L_s. Notons que l'unique morphisme de groupes $L_i \to L_s$ qui envoie x_i sur α donné par le théorème 1.30 est un isomorphisme (surjectif car α 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 θ de G tel que $\theta(x_0) = x$ (il en existe alors également un qui envoie x_0 sur y et on compose).

Soit $H = L_1 \times \cdots \times L_{i-1} \times \{1\} \times L_{i+1} \times \cdots \times L_s$ et soit $K = \langle x \rangle$. Soit $H' = L_1 \times \cdots \times L_{s-1} \times \{1\}$ 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 $f_H \colon H \to H'$ 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 $f_K \colon K \to K'$ 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 θ de G :

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

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

➢ Cas général. Posons $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où les p_i sont des nombres premiers distincts et les α_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 $\varphi \colon G \xrightarrow{\sim} K_1 \times \cdots \times K_r$.

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 $K_1 \times \cdots \times K_r$, 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 $\theta_i \in \mathrm{Aut}(K_i)$ tel que $\theta_i(x_i) = y_i$ pour tout i. On obtient alors un automorphisme $\theta \in \mathrm{Aut}(K_1 \times \cdots \times K_r)$ 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, $\varphi^{-1} \circ \theta \circ \varphi \in \mathrm{Aut}(G)$ convient. ✓

Théorème 2.16, démonstration de l'unicité. Il faut maintenant démontrer l'unicité des «facteurs invariants». Supposons que $G \cong C_{d_1} \times \cdots \times C_{d_r}$ et $G \cong C_{u_1} \times \cdots \times C_{u_s}$ avec r, n, $d_1, \dots, d_r$ et $u_1, \dots, u_s$ dans $\mathbb{N}^*$, $d_1 \mid \cdots \mid d_r$ et $u_1 \mid \cdots \mid u_s$. 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 $C_{d_1} = C_a \cong G \cong C_{u_1} \times \cdots \times C_{u_s} = C_{u_1} \times \cdots \times C_{u_{s-1}} \times C_a$.

En comparant les cardinaux des deux groupes, on en déduit que $C_{u_1} \times \cdots \times C_{u_{s-1}}$ est trivial, c'est-à-dire que $s = 1 = r$ et $u_1 = a = d_1$.

➢ Soit $r > 1$ un entier tel que le résultat soit vrai au rang $r - 1$. Grâce aux remarques précédentes, on a un isomorphisme

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

Soit α 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 $\theta \in \mathrm{Aut}(U)$ tel que $\theta(\varphi(g_1)) = g_2$. On a donc un isomorphisme $\theta \circ \varphi \colon D \to U$ tel que $\theta \circ \varphi(g_1) = g_2$. On considère les surjections canoniques $\pi_D \colon D \to D/\langle g_1 \rangle$ et $\pi_U \colon U \to U/\langle g_2 \rangle$. Alors $\mathrm{Ker}(\pi_U \circ \theta \circ \varphi) = \langle g_1 \rangle$ et par le théorème de factorisation on a un morphisme $\psi : D/\langle g_1 \rangle \to U/\langle g_2 \rangle$:

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

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 $D \to C_{d_1} \times \cdots \times C_{d_{r-1}}$ 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 $1 \leqslant i \leqslant r-1$. 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

$$C_2 \times C_2 \times C_3 \times C_3 \qquad C_4 \times C_3 \times C_3$$
$$C_2 \times C_2 \times C_9 \qquad C_4 \times C_9.$$

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

$$C_6 \times C_6 \qquad C_3 \times C_{12}$$
$$C_2 \times C_{18} \qquad C_{36}$$

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 $C_2 \times C_2 \times C_4$ et $C_2 \times C_8$ et $C_4 \times C_4$ et C_{16}

CHAPITRE 3

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 $\varphi\colon G \longrightarrow \mathrm{Aut}(N)$.*

Exemple. Soit N un groupe abélien et soit θ l'automorphisme de N défini par $\theta(x) = x^{-1}$ pour tout $x \in N$. Alors il existe un unique morphisme de groupes $\varphi\colon C_2 \longrightarrow \mathrm{Aut}(N)$ qui envoie le générateur g de C_2 sur θ 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 $N \to G$ qui envoie x sur gxg^{-1} est à valeurs dans N, donc induit un endomorphisme φ_g de N, qui est un automorphisme (de réciproque $\varphi_{g^{-1}}$). On obtient alors un morphisme de groupes $\varphi\colon G \to \mathrm{Aut}(N)$ qui associe φ_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 $\varphi\colon G \longrightarrow \mathrm{Aut}(N)$ 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'élement 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 φ.*

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

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

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 $(1_N,1_G)(x,g) = (1_N\varphi(1_G)(x), 1_G g) = (\mathrm{id}_N(x), g) =$

(x,g) car φ 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

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

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

Remarque. Si le morphisme φ est trivial, alors le produit semi-direct associé est le produit direct.

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

En effet, soit $f\colon \mathcal{D}_n\to \mathrm{Di}(C_n)$ l'application définie par $f(r^ps^k)=(u^p,g^k)$ où $C_n=\langle u\rangle$, $0\leqslant p\leqslant n-1$ et $0\leqslant k\leqslant 1$. Vérifions que f est un morphisme de groupes. Soit $(r^ps^k,r^qs^\ell)\in\mathcal{D}_n^2$.

➢ Si $k=0$, alors $f(r^ps^kr^qs^\ell)=f(r^{p+q}s^\ell)=(u^{p+q},g^\ell)$ et $f(r^ps^k)f(r^qs^\ell)=(u^p,1)(u^q,s^\ell)=(u^p\varphi(1)(u^q),s^\ell)=(u^pu^q,s^\ell)=f(r^ps^kr^qs^\ell)$.

➢ Si $k=1$, alors $f(r^ps^kr^qs^\ell)=f(r^pr^{n-q}s^{\ell+1})=(u^{p-q},g^{\ell+1})$ et $f(r^ps^k)f(r^qs^\ell)=(u^p,g)(u^q,g^\ell)=(u^p\theta(u^q),s^{\ell+1})=(u^pu^{-q},s^{\ell+1})=f(r^ps^kr^qs^\ell)$.

Soit maintenant $r^ps^k\in\mathrm{Ker}\,f$. 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 $r^ps^k=1$. Donc f est injectif.

Enfin, $|\mathrm{Di}(C_n)|=2n=|\mathcal{D}_n|$ 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 $\varphi\colon G\longrightarrow \mathrm{Aut}(N)$ 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 $\varphi(g)\neq \mathrm{id}_N$, 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 $\mathrm{Di}(N)$ n'est pas abélien.

Pour construire d'autres exemples, il est important de connaitre 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 $k \in [\![1\,;n]\!]$ tel que $\text{pgcd}(k,n) = 1$, il existe un unique automorphisme θ 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 $\theta\colon G \to G$ tel que $\theta(g) = g^k$.

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

Enfin, G est fini, donc θ est un automorphisme de G.

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

Remarque. On a un isomorphisme entre $\text{Aut}(C_n)$ et le groupe $(U(\mathbb{Z}/n\mathbb{Z}), \cdot)$ 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 $f\colon U(\mathbb{Z}/n\mathbb{Z}) \to \text{Aut}(C_n) : f(\bar{a})(g) = g^a$ (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 $d \mid n$, 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 $\left|G^{[d]}\right| = d$ 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

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

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^α 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 $1 \leqslant \beta_x \leqslant \alpha$. 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^α.

Posons maintenant $p-1 = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$ avec $q_1, \ldots, q_s$ des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_s$ 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, $o(x) = \mathrm{ppcm}(o(x_i) \mid 1 \leqslant i \leqslant s) = \prod_{i=1}^{s} o(x_i) = \prod_{i=1}^{s} q_i^{\alpha_i} = p-1$, 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 $|G| \geqslant 21$ – voir page 54).

En effet, soit θ l'unique automorphisme de $C_7 = \langle u \rangle$ qui envoie u sur u^2 (il existe bien puisque $\mathrm{pgcd}(2,7) = 1$). On vérifie que $\theta^3 = \theta \circ \theta \circ \theta = \mathrm{id}_{C_7}$ (pour cela il suffit de vérifier que $\theta^3(u) = u$). On en déduit qu'il existe un unique morphisme de groupes $\varphi \colon C_3 = \langle g \rangle \to \mathrm{Aut}(C_7)$ tel que $\varphi(g) = \theta$. Puisque l'opération φ 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 $\varphi, \psi \colon G \longrightarrow \mathrm{Aut}(N)$ des opérations de G sur N par automorphismes. On suppose qu'il existe $\alpha \in \mathrm{Aut}(G)$ 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 $N \rtimes_\varphi G \to N \rtimes_\psi G \colon (x,g) \mapsto (x, \alpha(g))$.

(2) Soient $\varphi, \psi \colon G \longrightarrow \mathrm{Aut}(N)$ des opérations de G sur N par automorphismes. On suppose qu'il existe $\beta \in \mathrm{Aut}(N)$ 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 $N \rtimes_\varphi G \to N \rtimes_\psi G \colon (x,g) \mapsto (\beta^{-1}(x), g)$.

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) $N \lhd G$.

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

Démonstration. On considère l'application $m \colon N \times H \longrightarrow G$, $(x,h) \longmapsto xh$, qui est surjective par hypothèse (puisque $G = NH$). On a $N \lhd G$, donc G opère sur N par conjugaison, et en restreignant cette opération à H, on obtient un morphisme de groupes

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

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

Montrons alors que $m\colon N \rtimes_\varphi H \longrightarrow G$ est un morphisme de groupes. On a $m((x,h)(y,k)) = m(xhyh^{-1},hk) = xhyk = m(x,h)m(y,k)$. De plus, si $m(x,h) = 1$ alors $xh = 1$ donc $x = h^{-1} \in N \cap H$, ce qui implique que $x = 1$ 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 $\varphi'((1,h))((x,1)) = (1,h)(x,1)(1,h)^{-1} = (\varphi(h)(x),h)(1,h^{-1}) = (\varphi(h)(x)\varphi(h)(1),hh^{-1}) = (\varphi(h)(x),1)$.

Notons que $i\colon N \to N'$ et $j\colon H \to H'$ définis par $i(x) = (x,1)$ et $j(h) = (1,h)$ sont des isomorphismes, que i induit un isomorphisme $c\colon \mathrm{Aut}(N) \to \mathrm{Aut}(N')$ défini pour tout $\alpha \in \mathrm{Aut}(N)$ 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 φ' correspond à φ via ces isomorphismes :

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \mathrm{Aut}(N) \\ {\scriptstyle j}\downarrow\wr & & \wr\downarrow{\scriptstyle c} \\ H' & \xrightarrow[\varphi']{} & \mathrm{Aut}(N'). \end{array}$$

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

Théorème 3.6. Soit G un groupe d'ordre $2p$, où $p \geqslant 3$ est un nombre premier impair. Alors $G \cong C_{2p}$ ou $G \cong \mathcal{D}_p$.

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.

➢ Il reste le cas où tous les éléments de $G \setminus \{1\}$ sont d'ordre p. Soit $x \in G \setminus \{1\}$ et soit $K = \langle x \rangle$. Alors $|K| = o(x) = p$ donc $[G : K] = 2$ et donc $K \triangleleft G$. Soit $\pi\colon G \to G/K$ la surjection canonique. Le groupe K/G est isomorphe au groupe cyclique C_2, notons a un générateur de K/G. Puisque π est surjectif, il existe $y \in G$ tel que $\pi(y) = a$. On a alors $y^p = 1$ donc $\pi(y^p) = \pi(1) = 1$ mais aussi $\pi(y^p) = \pi(y)^p = a^p = a$ car p est impair et a est d'ordre 2. On a donc une contradiction. Il existe donc également un élément g d'ordre 2 dans G.

Posons $H = \langle g \rangle \cong C_2$ et $N = \langle u \rangle \cong C_p$.

On a $[G : N] = 2$ donc $N \triangleleft G$. 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 $\varphi\colon H \to \mathrm{Aut}(N)$. Puisque $H \cong C_2$, il y a deux possibilités :

➢ φ est trivial, alors $G \cong N \times H \cong C_p \times C_2 \cong C_{2p}$ par le théorème chinois ;

➢ φ 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 $2 \leqslant k \leqslant p-1$. L'automorphisme θ 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 $k \in [\![2\,;p-1]\!]$ 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 $G \cong N \rtimes_\varphi H \cong \mathrm{Di}(C_p) \cong \mathcal{D}_p$. ✓

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.

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

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

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 $\{g_1 = 1, g_2, \ldots, g_k\}$ 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.

CHAPITRE 4

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) $\forall (g_1, g_2) \in G^2, \forall x \in E$, *on a* $(g_1 g_2).x = g_1.(g_2.x)$.

(2) $\forall x \in E$, *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 $\alpha : G \to S_E$.
On appelera $\operatorname{Ker} \alpha$ le **noyau** de l'action.

Démonstration. Supposons que G opère sur E. Pour $g \in G$, considérons l'application $\alpha_g : E \to E$ définie par $\sigma_g(x) = g.x$. On vérifie (exercice) que $\alpha_1 = \mathrm{id}_E$ et $\alpha_{gh} = \alpha_g \circ \alpha_h$ pour tout $(g, h) \in G^2$. En particulier $\alpha_g \circ \alpha_{g^{-1}} = \mathrm{id}_E = \alpha_{g^{-1}} \circ \alpha_g$. 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 $\alpha\colon G \longrightarrow S_E$ 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 $\alpha\colon G \longrightarrow S_{G/H}$ est non trivial ($\operatorname{Ker}\alpha \neq G$).

(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 : $\mathrm{GL}(V)$ opère sur V :

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

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 $\varphi\colon G \to S_{G/H} \cong S_p$.

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

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

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

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

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

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 $x \in N' = \operatorname{Ker} g$ donc $g(x) = 1$. De plus, $x \in H$ et $g_{|H}$ est injectif, donc $x = 1$. Donc $N' \cap H = \{1\}$.
- Puisque $N' = \operatorname{Ker} g \triangleleft G$, 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 $xh^{-1} \in \operatorname{Ker} g = N'$. On en déduit que $x = (xh^{-1})h \in N'H$ et donc que $G = N'H$.

Proposition 4.4. Soit

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

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 $\varphi \colon H \to \operatorname{Aut}(N')$. On considère l'application

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

Vérifions que α 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 $(n, h) \in \operatorname{Ker} \alpha$. 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 α est injectif.

Enfin, α est surjectif car $G = N'H$. On a démontré que α 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 $\mathrm{Stab}_G(x) = \{g \in G \mid g.x = x\}$ est un sous-groupe de G, appelé le **stabilisateur** de x dans G.*

La vérification est laissée en exercice.

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 $\forall g \in G$, $\forall x \in E$, $g.x = x \Leftrightarrow g = 1$.*

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 $\mathrm{Stab}_G(x) = \{1\}$.

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 $\{gxg^{-1}, g \in G\}$, c'est la **classe de conjugaison de** x. Le stabilisateur de x est le sous-groupe $Z_G(x) = \{g \in G \mid gx = xg\}$, c'est le **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 $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$, c'est le **normalisateur** de S. Si $S = H$ est un sous-groupe de G, alors $H \lhd N_G(H)$.

(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 $\mathrm{GL}(V)$ 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 7.23). Soit $v' \in V \setminus \{0\}$ un vecteur quelconque. Les familles $\{v\}$ et $\{v'\}$ étant libres, il existe des bases $\mathcal{B} = (v_1 = v, v_2, \ldots, v_n)$ et $\mathcal{B}' = (v'_1 = v', v'_2, \ldots, v'_n)$ de V d'après le théorème de la base incomplète. Soit $f : V \to V$ l'unique application linéaire définie sur la base $\mathcal{B}$ par $f(v_i) = v'_i$ pour tout $i \in [\![1\,;n]\!]$. 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 $f \in \mathrm{GL}(V)$. 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 $\mathrm{Stab}_G(x)$ et $\mathrm{Stab}_G(y)$ sont conjugués dans G.

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

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 :

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

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

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

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

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

Ainsi f induit la bijection annoncée $\overline{f}$. ✓

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 $(x_i)_{1\leqslant i\leqslant r}$ une famille de représentants des orbites distinctes. Alors

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

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

Corollaire 4.12. (Equation aux classes)
Soit G un groupe fini (opérant sur lui-même par conjugaison). Soit $(x_i)_{1\leqslant i\leqslant r}$ 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 $\operatorname{Stab}_G(x_i) = Z_G(x_i)$.

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

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
$$E^G = \{x \in E \mid g.x = x,\ \forall g \in G\}$$
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
$$|E| = |E^G| + \sum_{i=1}^{r} [G : \mathrm{Stab}_G(x_i)]$$
où $x_1, \dots, x_r$ sont les représentants des orbites qui ne sont pas réduites à un point. Ainsi pour tout $i \in [\![1\,;r]\!]$ on a $[G : \mathrm{Stab}_G(x_i)] > 1$. Or $[G : \mathrm{Stab}_G(x_i)] \mid |G| = p^n$ donc il existe, pour tout i, un entier $d_i \in \mathbb{N}^*$ tel que $[G : Z_G(x_i)] = p^{d_i}$. En particulier, p divise $[G : Z_G(x_i)]$ 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 $\pi : G \to G/Z(G)$ 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
$$gh = a^k z_1 a^\ell z_2 = a^k a^\ell z_1 z_2 = a^{k+\ell} z_1 z_2 \text{ et } hg = a^\ell z_2 a^k z_1 = a^{\ell+k} z_2 z_1 = z^{k+\ell} z_1 z_2 = gh. \quad ✓$$

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 $i \in [\![0\,;n]\!]$ le groupe G contient un sous-groupe normal d'ordre p^i. En particulier, si $n \geqslant 2$ 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 $|Z(G)| \geqslant 1$, 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, on a $|Z(G)| = p$ ou $|Z(G)| = p^2$. Si $|Z(G)| = p^2$, alors G est abélien. Sinon $|Z(G)| = p$, le groupe $G/Z(G)$ est d'ordre p premier, donc il est cyclique et le lemme 4.15 permet de conclure encore que 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. Si $n = 1$, le groupe G est cyclique et le résultat est évidemment vrai. Soit donc $n > 1$ tel que le résultat soit vrai pour les groupes d'ordre p^j, $1 \leqslant j < n$. 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 $\{1\} \subsetneqq H \subsetneqq G = Z(G)$. Si G n'est pas abélien, alors $H = Z(G)$ vérifie $\{1\} \subsetneqq H \subsetneqq G$ 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 $\{1\} \subsetneqq H \subsetneqq G$. 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 $i \in [\![0\,;k]\!]$, qui sont normaux dans G car contenus dans $Z(G)$. L'hypothèse de récurrence fournit également pour tout $\ell \in [\![0\,;n-k]\!]$ un sous-groupe normal K_ℓ de G/H d'ordre p^ℓ. Soit $\pi\colon G \longrightarrow G/H$ 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 $i \in [\![k+1\,;n]\!]$, il existe $\ell \in [\![1\,;n-k]\!]$ 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^α.*

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 $d_1, \ldots, d_r$ tels que $d_1 \mid d_2 \mid \cdots \mid d_r$ et $G \cong C_{d_1} \times \cdots \cong C_{d_r}$ d'après le théorème 2.16. On a également $N = d_1 \cdots d_r$. Pour tout $i \in [\![1\,;r]\!]$, 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 $n^r = d_1 \cdots d_r q_1 \cdots q_r = N q_1 \cdots q_r$ 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 $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1, \ldots, p_r$ des nombres premiers deux à deux distincts et $(\alpha_1, \ldots, \alpha_r) \in (\mathbb{N}^*)^r$. Le nombre premier p est l'un des p_i.

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

Soit $i \in [\![1\,;r]\!]$. 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 $|G|$.

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 $|G| \leqslant 5$.

Soit $n \geqslant 6$ 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^α, 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 $1 \leqslant |Z(G)| < |G|$, 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 $\overline{K}$ de G/H d'ordre $p^{\alpha-1}$, et il existe un sous-groupe K de G contenant H tel que $\overline{K} \cong K/H$. On a alors $|K| = |H||\overline{K}| = p^\alpha$, 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 $0 \leqslant i \leqslant \alpha$.

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

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.

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, $m \in \mathbb{N}^*$ 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 $|HP| \leqslant |P|$ 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 $\left|gPg^{-1}\right| = |P|$, 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 $E = \Omega(P) = \left\{xPx^{-1} \mid x \in G\right\}$ la classe de conjugaison de P. On sait que $|E| = [G : \mathrm{Stab}_G(P)] = [G : N_G(P)]$. 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 $\left|E^H\right| \not\equiv 0 \pmod{p}$ et en particulier que $E^H \neq \varnothing$. 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 $|\mathcal{S}| = |E| \equiv \left|E^H\right| = 1 \pmod{p}$. 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

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

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

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 : $|G| = 15, 35...$).

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. ✓

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 $|G| \geqslant 21$.

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 $C_p \rtimes C_q$.

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 $\varphi : C_q \to \text{Aut}(C_p)$ est le morphisme d'une opération de C_q sur C_p par automorphismes.

Si l'opération φ est triviale, alors G est abélien et $G \cong C_{pq}$.

Si l'opération φ n'est pas triviale, alors G est n'est pas abélien. Vérifions qu'il en existe bien. Soit a un générateur de C_q. Alors tout morphisme $\varphi : C_q \to \text{Aut}(C_p)$ est entièrement déterminé par $\varphi(a)$, qui doit être un élément dont l'ordre divise $o(a) = q$; comme q est premier, l'action n'est pas triviale si, et seulement si, l'ordre de $\varphi(a)$ est égal à q. D'après une remarque page 41, $\text{Aut}(C_p)$ est cyclique d'ordre $p-1$. Puisque q divise $p-1$, il existe bien des éléments d'ordre q dans $\text{Aut}(C_p)$ et donc des opérations non-triviales.

Montrons enfin que toutes les opérations non triviales donnent des produits semi-directs isomorphes. Soient $\varphi, \psi : C_q \to \text{Aut}(C_p)$ 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 q est premier. Mais on sait que $\text{Aut}(C_p)$ est un groupe cyclique d'ordre $p-1$, donc 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 $k \in [\![1\,;q-1]\!]$ tel que $\varphi(a) = \psi(a)^k$. Soit $\alpha\colon C_q \to C_q$ l'unique endomorphisme de C_q défini par $\alpha(a) = a^k$. C'est un automorphisme car a^k engendre C_q, donc α est surjectif, et c'est un endomorphisme d'un groupe fini et donc un automorphisme. De plus, $\psi \circ \alpha(a) = \psi(a^k) = \psi(a)^k = \varphi(a)$ donc $\psi \circ \alpha = \varphi$ (car a engendre C_q). On en déduit que $C_p \rtimes_\varphi C_q \cong C_p \rtimes_\psi C_q$ via l'isomorphisme donné par $(x,y) \mapsto (x, \alpha(y))$ (voir page 42).

Classification des groupes d'ordre $n \leqslant 15$.

Définition-Proposition 4.27. *Soit Q_8 le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ 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 donc tous de la forme $a^k b^\ell$ avec $(k,\ell) \in \mathbb{Z}^2$, $0 \leqslant k, \ell \leqslant 4$ et donc, puisque $a^2 = -1 = b^2$, de la forme $\pm a^k b^\ell$ avec $(k,\ell) \in \mathbb{Z}^2$, $0 \leqslant k, \ell \leqslant 1$, 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, $rsr^{-1} = r^2 s \notin \langle s\rangle$. ✓

Définition-Proposition 4.28. *Le **groupe dicyclique** Dic_n d'ordre $4n$ est le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ 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

$$\mathrm{Dic}_n = \left\{ a^k b^l \mid 0 \leqslant k \leqslant 2n-1,\ 0 \leqslant l \leqslant 1 \right\}.$$

On a $\mathrm{Dic}_2 \cong Q_8$ et $\mathrm{Dic}_3 \cong C_3 \rtimes_\varphi C_4$ pour l'opération $\varphi\colon C_4 = \langle g\rangle \to \mathrm{Aut}(C_3)$ 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

$$\mathrm{Dic}_n = \left\{ a^u b^l \mid u \in \mathbb{Z},\ 0 \leqslant l \leqslant 1 \right\}.$$

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

On en déduit que $|\mathrm{Dic}_3| \leqslant 2n \cdot 2 = 4n$. Soit maintenant $(k,l,u,v) \in \mathbb{Z}^4$ avec $0 \leqslant k,u \leqslant 2n-1$ et $0 \leqslant l,v \leqslant 1$ 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 deduit que $v = l$. Alors $a^{k-u} = I_2$ donc $2n$ (l'ordre de a) divise $k-u$. Or $-2n+1 \leqslant k-u \leqslant 2n-1$ donc $k-u = 0$ et on a $k = u$. Ainsi, 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 Dic_2 est le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ 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 Dic_3 engendré par a^2, il est isomorphe à C_3. Alors N est normal dans 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 Dic_3 engendré par b. Il est isomorphe à C_4. On a donc $N \cap H = \{1\}$ puisque $\mathrm{pgcd}(|N|,|H|) = 1$.

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

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

Le groupe 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 φ n'est pas trivial. Le seul automorphisme de C_3 différent de id_{C_3} est l'automorphisme θ défini par $\theta(x) = x^{-1}$; de plus, il existe bien un morphisme $\varphi \colon C_4 \to \mathrm{Aut}(C_3)$ tel que $\varphi(b) = \theta$ car $\theta^4 = \mathrm{id}$ (théorème 1.30). On a donc obtenu le résultat cherché. ✓

Théorème 4.29. Tous les groupes d'ordre $n \leqslant 15$ 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 $C_2 \times C_2 \cong \mathcal{D}_2$	
5	C_5	
6	$C_6 \cong C_2 \times C_3$	$\mathcal{D}_3 \cong S_3$
7	C_7	
8	C_8 $C_4 \times C_2$ $C_2 \times C_2 \times C_2$	$\mathcal{D}_4$ 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	$C_{12} \cong C_4 \times C_3$ $C_2 \times C_6 \cong C_2 \times C_2 \times C_3$	$\mathcal{D}_6$ A_4 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. ✓

CHAPITRE 5

Groupes symétriques et alternés

Soit $n \in \mathbb{N}^*$. On considère le groupe symétrique S_n des bijections de $[\![1\,;n]\!]$ dans $[\![1\,;n]\!]$ (la loi de groupe est la composition des bijections). C'est un groupe d'ordre $n!$, qui n'est pas abélien si $n \geqslant 3$ (nous verrons même que son centre est trivial si $n \geqslant 3$).

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 $\varphi\colon G \to S_G \cong S_n$ défini par $\varphi(g)(x) = g.x = gx$. Il est facile de vérifier que φ est injectif, donc φ induit un isomorphisme $G \cong \operatorname{Im}\varphi$ et $\operatorname{Im}\varphi$ 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 $k \geqslant 2$ et $i_1, \dots, i_k$ dans $[\![1\,;n]\!]$ deux à deux distincts. On note $\begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix}$ la permutation définie par

$$\begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix}(l) = \begin{cases} l & \text{si } l \notin \{i_1, \dots, i_k\} \\ i_{r+1} & \text{si } l = i_r \in \{i_1, \dots, i_{k-1}\} \\ i_1 & \text{si } l = i_k \end{cases}$$

Une permutation de ce type est appelée un **k-cycle**.

On a le résultat suivant, extrèmement utile pour faire des calculs.

Lemme 5.2. Soient $\sigma \in S_n$ et $\begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix}$ est un k-cycle. On a

$$\sigma \begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_k) \end{pmatrix}$$

Définition 5.3. *Le **support** d'une permutation $\sigma \in S_n$ est l'ensemble* $\operatorname{Supp}(\sigma) = \{i \in [\![1\,;n]\!] \mid \sigma(i) \neq i\}$. *Par exemple, si $\sigma = \begin{pmatrix} i_1 & \dots & i_k \end{pmatrix}$ est un k-cycle, le support de σ 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 $\sigma \in S_n \setminus \{\mathrm{id}\}$.

(1) Alors σ s'écrit comme un produit de cycles à supports disjoints.

(2) Le nombre r et les longueurs $\ell_1, \dots, \ell_r$ des cycles non triviaux à supports disjoints dont le produit est égal à σ est entièrement déterminé par σ, et la suite $[\ell_1, \dots, \ell_r]$ rangée dans l'ordre croissant est appelée le **type** de σ.

(3) Deux permutations sont conjuguées si, et seulement si, elles ont le même type.

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 $[\![1\,;n]\!]$ deux à deux distincts. Alors on a $(i_1 \quad \dots \quad i_k) = (i_1 \quad i_2)(i_2 \quad i_3)\cdots(i_{k-1} \quad i_k)$.

(2) Soient $i, j \geqslant 2$ avec $i < j-1$. On a $(i \quad j) = (j-1 \quad j)(i \quad j-1)(j-1 \quad j)$.

(3) Soient $1 \leqslant i < j \leqslant n$. On a $(i \quad j) = (1 \quad i)(1 \quad j)(1 \quad i)$.

(4) Soit $\sigma = (1 \quad 2 \quad \dots \quad n)$. Pour $i \leqslant n-1$, on a $(i \quad i+1) = \sigma^{i-1}(1 \quad 2)\sigma^{1-i}$.

Démonstration. Ce sont des calculs immédiats. ✓

Théorème 5.6. Soit $n \geqslant 2$. Le groupe S_n est engendré par l'une quelconque des familles suivantes.

(1) Les transpositions.

(2) Les transpositions $(i \quad i+1)$ avec $1 \leqslant i \leqslant n-1$.

(3) Les transpositions $(1 \quad i)$ avec $2 \leqslant i \leqslant n$.

(4) La transposition $(1 \quad 2)$ et le n-cycle $(1 \quad 2 \quad \dots \quad n)$.

(5) Une transposition $(i \quad i+1)$ avec $1 \leqslant i \leqslant n-1$ et le n-cycle $(1 \quad 2 \quad \dots \quad n)$.

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 $(1 \quad 2) = \sigma^{1-i}(i \quad i+1)\sigma^{i-1}$. ✓

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 $(1 \quad 2 \quad \dots \quad p)$ et une transposition $(i \quad i+1)$. Tout d'abord on sait que G contient un élément σ 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 σ est un élément d'ordre p, soit $\sigma = \gamma_1 \cdots \gamma_r$ sa décomposition en produit de cycles à supports disjoints. Alors les γ_i commutent deux à deux donc $o(\sigma) = \mathrm{ppcm}(o(\gamma_i) \mid 1 \leqslant i \leqslant r)$. Or $o(\gamma_i) > 1$ pour tout i et p est premier donc $o(\gamma_i) = p$ pour tout i. Mais ce sont des permutations de $[\![1\,;p]\!]$ donc $r = 1$ et $\sigma = \gamma_1$ est un p-cycle.

Soit $\tau \in G$ une transposition. Ecrivons $\sigma = (i_1 \quad \dots \quad i_p)$ et soit $\nu \in S_p$ la permutation définie par $\nu(i_k) = k$, on a $\nu \circ \sigma \circ \nu^{-1} = (1 \quad 2 \quad \dots \quad p) \in \nu G \nu^{-1}$. 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 $(1 \quad 2 \quad \dots \quad p) \in G$. Notons $\sigma = (1 \quad 2 \quad \dots \quad p)$.

A ce stade il est commode de changer de notation : on remplace $[\![1\,;p]\!]$ par $\mathbb{Z}/p\mathbb{Z} = \{\overline{0},\dots,\overline{p-1}\}$, et G est un sous-groupe du groupe des permutations de $\mathbb{Z}/p\mathbb{Z}$ contenant $\sigma = \begin{pmatrix}\overline{0} & \overline{1} & \dots & \overline{p-1}\end{pmatrix}$ et $\tau = \begin{pmatrix}\overline{i} & \overline{j}\end{pmatrix}$ avec i,j dans $\{0,\dots,p-1\}$ et $i<j$. On peut alors écrire, pour tout $\overline{k}\in\mathbb{Z}/p\mathbb{Z}$, $\sigma(\overline{k}) = \overline{k+1}$. Montrons, par récurrence sur k, que

$$\forall k\in\{\overline{1},\dots,\overline{p-1}\},\ \text{on a } \begin{pmatrix}\overline{0} & \overline{k(j-i)}\end{pmatrix}\in G.$$

Si $k=1$, on a $\sigma^{-i}\begin{pmatrix}\overline{i} & \overline{j}\end{pmatrix}\sigma^{i} = \begin{pmatrix}\overline{0} & \overline{j-i}\end{pmatrix}\in G$.

Soit maintenant $k\in[\![1\,;p-2]\!]$ tel que $\begin{pmatrix}\overline{0} & \overline{s(j-i)}\end{pmatrix}\in G$ pour tout $s\in[\![1\,;k]\!]$ on doit démontrer que $\begin{pmatrix}\overline{0} & \overline{(k+1)(j-i)}\end{pmatrix}\in G$. On a

$$\sigma^{j}\begin{pmatrix}\overline{0} & \overline{k(j-i)}\end{pmatrix}\sigma^{-j} = \begin{pmatrix}\overline{j} & \overline{j(k+1)-ki}\end{pmatrix}\in G$$

et on a $\overline{j(k+1)-ki} = \overline{(j-i)(k+1)}+\overline{i} = \overline{(j-i)k}+\overline{j}\notin\{\overline{i};\overline{j}\}$ car $\overline{k}\neq\overline{0}$, $\overline{k+1}\neq\overline{0}$, $\overline{j-i}\neq\overline{0}$ et $\mathbb{Z}/p\mathbb{Z}$ est un corps. Donc

$$\begin{pmatrix}\overline{i} & \overline{j}\end{pmatrix}\begin{pmatrix}\overline{j} & \overline{j(k+1)-ki}\end{pmatrix}\begin{pmatrix}\overline{i} & \overline{j}\end{pmatrix} = \begin{pmatrix}\overline{i} & \overline{j(k+1)-ki}\end{pmatrix}\in G$$

et

$$\sigma^{-i}\begin{pmatrix}\overline{i} & \overline{j(k+1)-ki}\end{pmatrix}\sigma^{i} = \begin{pmatrix}\overline{0} & \overline{(k+1)(j-i)}\end{pmatrix}\in G$$

et on a bien le résultat désiré. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, il existe $k\in[\![1\,;p-1]\!]$ tel que $\overline{k(j-i)} = \overline{1}$, et ainsi $\begin{pmatrix}\overline{0} & \overline{1}\end{pmatrix}\in G$, 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 $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}$ et $\begin{pmatrix}1 & 3\end{pmatrix}$.

En effet, on a $\tau\sigma = \sigma^{-1}\tau$ donc

$$\begin{aligned}\langle\sigma,\tau\rangle &= \left\{\sigma^k\tau^\ell \mid (k,\ell)\in\mathbb{Z}^2\right\} = \left\{\sigma^k\tau^\ell \mid 0\leqslant k\leqslant 3,\ 0\leqslant\ell\leqslant 1\right\}\\ &= \left\{\mathrm{id},\tau,\begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix},\begin{pmatrix}2 & 4\end{pmatrix},\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix},\sigma,\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix},\begin{pmatrix}1 & 4 & 3 & 2\end{pmatrix}\right\}\\ &\neq S_4.\end{aligned}$$

II Le groupe alterné

Définition-Proposition 5.8. *Soit $n\geqslant 2$. Il existe unique morphisme de groupes surjectif*

$$\varepsilon\colon S_n\longrightarrow\{\pm 1\}$$

*tel que pour tout k-cycle σ, on ait $\varepsilon(\sigma) = (-1)^{k-1}$. Le morphisme ε est appelé la **signature**, et le **groupe alterné** A_n est défini comme le noyau de ε. On a $A_n\triangleleft S_n$ (puisque A_n est le noyau du morphisme ε, ou parce qu'il est d'indice 2 dans S_n) et $|A_n| = \frac{n!}{2}$.*

Démonstration. L'existence a été démontrée L3. Pour l'unicité, soit $\varphi\colon S_n\to\{\pm1\}$ 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 τ. 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 τ on a $\varphi(\tau) = 1$. Mais alors $\varphi\equiv 1$ donc φ n'est pas surjectif ; on a obtenu une contradiction.

Cas 2 : pour toute transposition τ on a $\varphi(\tau) = -1$. On a alors $\varphi(\tau) = \varepsilon(\tau)$ pour toute transposition τ et donc $\varphi = \varepsilon$. ✓

Remarque. On en déduit que $\widehat{S_n} = \{\mathbb{1},\varepsilon\}$.

Proposition 5.9. Soit $n \geqslant 3$. Le groupe A_n est engendré par les 3-cycles $(1 \quad 2 \quad i)$ pour $i \geqslant 3$.

Démonstration. On sait que S_n est engendré par les cycles $(1 \quad i)$, $i \geqslant 2$. Ainsi si $\sigma \in A_n$, on a

$$\sigma = (1 \quad i_1) \cdots (1 \quad i_m)$$

avec, pour tout k, $i_k \geqslant 2$ et m pair. Donc A_n est engendré par les éléments $(1 \quad i)(1 \quad j)$, avec $i, j \geqslant 2$ et $i \neq j$. On a

$$\begin{aligned}(1 \quad i)(1 \quad j) &= (1 \quad j \quad i) \text{ si } 2 \leqslant i \neq j \leqslant n,\\ (1 \quad j \quad i) &= (1 \quad 2 \quad i)(1 \quad 2 \quad j)^2 \text{ si } 3 \leqslant i \neq j \leqslant n\\ (1 \quad i \quad 2) &= (1 \quad 2 \quad i)^2 \text{ si } i \geqslant 3\end{aligned}$$

On a donc le résultat. ✓

Lemme 5.10. Pour $n \geqslant 3$, le groupe A_n opère $(n-2)$ fois transitivement sur $[\![1\,;n]\!]$, c'est-à-dire que pour tout $((a_1, \ldots, a_{n-2}), (b_1, \ldots, b_{n-2})) \in ([\![1\,;n]\!]^{n-2})^2$ 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 $i \in [\![1\,;n-2]\!]$ on a $\sigma(a_i) = b_i$.

Démonstration. On complète les ensembles de a_i et b_i de façon à avoir $\{a_1, \ldots, a_{n-2}, a_{n-1}, a_n\} = [\![1\,;n]\!] = \{b_1, \ldots, b_{n-2}, b_{n-1}, b_n\}$. Il est clair qu'il existe une (unique) bijection $[\![1\,;n]\!] \to [\![1\,;n]\!]$ qui envoie i sur a_i pour tout i et une (unique) bijection $[\![1\,;n]\!] \to [\![1\,;n]\!]$ qui envoie i sur b_i pour tout i. En les composant, on obtient $\gamma \in S_n$ telle que $\gamma(a_i) = b_i$ pour tout i.

Si $\gamma \in A_n$, c'est terminé. Sinon, $\sigma = \gamma(a_{n-1} \quad a_n) \in A_n$ et vérifie $\sigma(a_i) = b_i$ pour tout i avec $1 \leqslant i \leqslant n-2$. ✓

Proposition 5.11. Soit $n \geqslant 5$. Les 3-cycles sont conjugués dans A_n.

Démonstration. Voir travaux dirigés.

Soient $\gamma_a = (a_1 \quad a_2 \quad a_3)$ et $\gamma_b = (b_1 \quad b_2 \quad b_3)$ deux 3-cycles. Puisque $n \geqslant 5$, on peut compléter en des ensembles $\{a_1, \ldots, a_{n-2}\}$ et $\{b_1, \ldots, b_{n-2}\}$ à $n-2$ éléments. Puisque l'action de A_n sur $[\![1\,;n]\!]$ est $(n-2)$-transitive, il existe $\sigma \in A_n$ tel que $\sigma(a_i) = b_i$ pour tout i avec $1 \leqslant i \leqslant n-2$. 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 $n \geqslant 5$. Le groupe A_n est simple.

Démonstration. Soit $H \neq \{\mathrm{id}\}$ 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 $\sigma \in H \setminus \{\mathrm{id}\}$. 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 σ en produit de cycles à supports disjoints. En particulier, ces cycles $\gamma_1, \ldots, \gamma_r$ commutent deux à deux, donc on peut supposer qu'ils sont ordonnés par longueur décroissante. On distingue quatre cas.

Cas 1. $\ell(\gamma_1) \geqslant 4$. Posons $\gamma_1 = (i_1\ i_2\ \ldots\ i_t)$ avec $t \geqslant 4$. Soit $\tau = (i_1\ i_2\ i_3)$. Les supports de τ, $\gamma_2, \ldots, \gamma_r$ 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 γ_i est un 3-cycle et γ_i^2 aussi, soit γ_i est une transposition et $\gamma_i^2 = \mathrm{id}$. Ainsi, quitte à remplacer σ par σ^2, on peut supposer que la décomposition de σ 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 $n \geqslant 5$ il existe $i_5 \in [\![1\,;n]\!] \setminus \{i_1;i_2;i_3;i_4\}$. 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 τ commute avec σ' 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 $n \geqslant 3$, alors $Z(S_n) = \{\mathrm{id}\}$.

Démonstration. Voir travaux dirigés.

Soit $\sigma \in Z(S_n)$. Supposons que $\sigma \neq \mathrm{id}$. Soit $i \in \mathrm{Supp}(\sigma)$, on a donc $\sigma(i) \neq i$. Puisque $n \geqslant 3$, il existe $j \in [\![1\,;n]\!]$ 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 σ est injective, donc $\tau\sigma\tau \neq \sigma$ et donc $\tau\sigma \neq \sigma\tau$: on a obtenu une contradiction. Donc $\sigma = \mathrm{id}$ et on a bien $Z(S_n) = \{\mathrm{id}\}$. ✓

Théorème 5.14. Pour $n \neq 4$, les seuls sous-groupes normaux de S_n sont $\{\mathrm{id}\}$, A_n et S_n.

Démonstration. Si $n = 2$, alors $S_2 \cong C_2$ et ses seuls sous-groupes (nécessairement normaux) sont $\{\mathrm{id}\} = A_2$ et S_2.

Traitons le cas $n = 3$. Soit H un sous-groupe normal de S_3, avec $\{1\} \subsetneqq H \subsetneqq S_3$. Alors $|H| = 2$ ou $|H| = 3$. Si $|H| = 2$, posons $H = \{\mathrm{id}, \sigma\}$ avec σ 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 $H = \{\mathrm{id}, \sigma_1, \sigma_2\}$ avec σ_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 $n \geqslant 5$. Soit H un sous-groupe normal de S_n avec $\{1\} \subsetneqq H \subsetneqq S_n$. Alors $H \cap A_n \triangleleft A_n$. Mais A_n est simple donc $H \cap A_n = \{\mathrm{id}\}$ ou $H \cap A_n = A_n$.

Si $H \cap A_n = \{1\}$, alors toutes les permutations non triviales de H sont impaires. On en déduit en particulier que pour tout $\sigma \in H$ on a $\sigma^2 = \mathrm{id}$ (puisque σ^2 est paire et dans H). Fixons $\sigma \in H \setminus \{\mathrm{id}\}$. Alors pour tout $\tau \in H \setminus \{\mathrm{id}\}$ on a $\sigma\tau = \mathrm{id}$ (pour les mêmes raisons) donc $\tau = \sigma^{-1} = \sigma$. Donc $H = \{\mathrm{id}, \sigma\}$. Mais si $\gamma \in S_n$ est du même type que σ, alors γ et σ 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

$$V_4 = \{\mathrm{id}, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$$

est normal dans S_4.

Théorème 5.15. Soit $n \geqslant 2$ 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 $H \ncong C_6$ 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 $\varphi \colon S_n \to S_E \cong S_n$ 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 φ est un sous-groupe normal de S_n. De plus, il est contenu dans H (si $\sigma \in \operatorname{Ker}\varphi$, 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 $\operatorname{Ker}\varphi = \{\mathrm{id}\}$ d'après le théorème 5.14. Donc φ est un isomorphisme.

On remarque que $\varphi(H) \subset \operatorname{Stab}_{S_n}(H)$. De plus, il est clair que $\operatorname{Stab}_{S_n}(H)$, 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 $H \cong \varphi(H) = \operatorname{Stab}_{S_n}(H) \cong S_{n-1}$. ✓

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 $H \cong A_4$. 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 $\varphi \colon G \to S_E \cong S_4$. Soit $K = \operatorname{Ker}\varphi$.

Soit $g \in K$. Alors, pour tout $L \in E$, on a $gLg^{-1} = L$ donc $g \in N_G(L)$. On a donc $K \subset \cap_{L\in E} N_G(L)$. L'autre inclusion est facile à vérifier, donc $K = \cap_{L\in E} N_G(L)$. 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 $K = \cap_{L\in E} L$.

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 $K = \cap_{L\in E} L = \{1\}$. On a démontré que φ 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 $G \cong \varphi(G) = A_4$. ✓

CHAPITRE 6

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» 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 $i \in [\![0\,;m-1]\!]$, 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

$$\{\mathrm{id}\} \subset A_3 \subset S_3.$$

En effet, on a bien $\{\mathrm{id}\} \triangleleft A_3 \triangleleft S_3$ et les quotients $S_3/A_3 \cong C_2$ et $A_3/\{\mathrm{id}\} \cong C_3$ sont abéliens.

Lemme 6.2. Soit G un groupe. Soient H, K et L trois sous-groupes de G avec $H \triangleleft G$ et $K \triangleleft L$.

(1) 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 $L/K \to HL/HK$.

(2) Si on suppose de plus que $H \subset K$ et si on note $\pi\colon G \to G/H$ la surjection canonique, 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

$$yxy^{-1} = h'\ell hk\ell^{-1}h'^{-1} = h'\ell h\ell^{-1}\ell k\ell^{-1}h'^{-1}.$$

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 $L \to HL$ l'injection naturelle, on compose avec la surjection canonique $HL \to HL/HK$ pour obtenir un morphisme de groupes φ. Il est clair que $K \subset \operatorname{Ker}\varphi$ donc φ induit un morphisme $\overline{\varphi}\colon L/K \to HL/HK$ tel que $\overline{\varphi}(\overline{\ell}) = \varphi(\ell)$.

Soit $y \in HL/HK$. Il existe $x \in HL$ tel que $y = \overline{x}$ et il existe donc $(k, \ell) \in H \times L$ tel que $x = hl$. Alors, dans HL/HK, on a $y = \overline{x} = \overline{\ell}$; en effet, on a $\ell^{-1}x = \ell^{-1}h\ell \in H \subset HK$ car $H \triangleleft G$ donc $\overline{\ell^{-1}x} = \overline{1}$ et donc $\overline{\ell}^{-1}\overline{x} = \overline{1}$. On en déduit donc que $y = \overline{x} = \varphi(\ell) = \overline{\varphi}(\overline{\ell})$ et donc que $\overline{\varphi}$ est surjectif.

(2) Puisque π est surjective, on a $\pi(\pi^{-1}(L)) = L$. On considère le morphisme surjectif $\pi^{-1}(L) \xrightarrow{\pi} L \twoheadrightarrow L/K$. Son noyau est $\pi^{-1}(K)$ et on applique le premier théorème d'isomorphisme pour conclure. ✓

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 $i \in [\![0\,;m]\!]$, $H_i = H \cap G_i$. 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 $i \in [\![0\,;m-1]\!]$. 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 $\pi\colon G \longrightarrow G/H$ 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 groupe s $\pi^{-1}(K_{i+1})/\pi^{-1}(K_i) \cong K_{i+1}/K_i$ sont abéliens. ✓

Remarque. On peut reformuler le point (2) de la proposition de la façon suivante.

Soit $1 \to H \to G \to K \to 1$ 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.

Si $n = 0$ le résultat est clair, si $n = 1$ alors G est cyclique donc abélien et donc résoluble.

Soit donc $n > 1$ tel que tous les groupes d'ordre p^i avec $i \leqslant n-1$ 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 $1 \to C_p \to G = C_p \rtimes C_q \to C_q \to 1$ 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 fini simple non abélien n'est pas résoluble.
En particulier, si $n \geqslant 5$ 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 $n \leqslant 4$.

Démonstration. Si $n \leqslant 2$, alors S_n est abélien donc résoluble.

Si $n = 3$, alors $\{\mathrm{id}\} \subset A_3 \subset S_3$ est une suite de résolubilité.

Si $n = 4$, alors $\{\mathrm{id}\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$ 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 σ vérifient $\sigma^2 = \mathrm{id}$) et les deux autres quotients sont d'ordres premiers donc cycliques et donc abéliens.

Enfin, si $n \geqslant 5$, 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-ième groupe dérivé** de G, noté $D^n(G)$, est défini la manière suivante :*

$$D^1(G) = D(G),\ D^2(G) = D(D(G)),\ \ldots,\quad D^n(G) = D(D^{n-1}(G)),\ \ldots$$

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.

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 $D(G) \triangleleft G$.

Soit $n \geqslant 1$ tel que $D^i(G) \triangleleft G$ pour tout $i \leqslant n$. 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_{ab}.*

Démonstration. Soit $(x, y) \in G^2$. Alors $[\overline{x}, \overline{y}] = \overline{[x, y]} = \overline{1}$ dans $G/D(G)$, donc $\overline{x}$ et $\overline{y}$ 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 $\overline{[x, y]} = [\overline{x}, \overline{y}] = \overline{1}$ 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 $(\overline{x}, \overline{y}) \in (G/H)^2$. Alors $[\overline{x}, \overline{y}] = \overline{[x, y]}$ et $[x, y] \in D(G) \subset H$ donc $[\overline{x}, \overline{y}] = \{\overline{1}\}$. Puisque les commutateurs d'élements de G/H engendrent $D(G/H)$, on en déduit que $D(G/H) = \{\overline{1}\}$ et donc que G/H est abélien. ✓

Exemples. (1) Pour $n \geqslant 3$, on a $D(S_n) = A_n$. Voir travaux dirigés

Puisque S_n n'est pas abélien, on a $D(S_n) \neq \{\mathrm{id}\}$. 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 σ un 3-cycle. Alors σ^2 est aussi un 3-cycle donc d'après le théorème 5.4 (3) σ et σ^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_4, on en déduit que $A_4 = D(S_4)$.

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 $\{\mathrm{id}\} \subsetneq D(S_n) \subset A_n$.

(2) Pour $n \geqslant 5$, on a $D(A_n) = A_n$. Voir travaux dirigés

On a $D(A_n) \triangleleft A_n$. Pour $n \geqslant 5$, le groupe A_n est simple donc $D(A_n) = \{\mathrm{id}\}$ ou $D(A_n) = A_n$. Mais si on avait $D(A_n) = \{\mathrm{id}\}$ alors $A_n \cong A_n/\{\mathrm{id}\} = A_n/D(A_n)$ 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 $(i,j,k,l) \in [\![1\,;4]\!]^4$ avec i,j,k,l deux à deux distincts, on a $\begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} k & l \end{pmatrix} = [\begin{pmatrix} i & j & k \end{pmatrix}, \begin{pmatrix} i & j & l \end{pmatrix}] \in D(A_4)$ 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 $i \in [\![1\,;m]\!]$, on a $D^i(G) \subset G_i$. On en déduira que $D^m(G) = \{1\}$.

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.

Soit donc $i \geqslant 2$ 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 $i \in [\![0\,;n-1]\!]$. ✓

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 dont tous les quotients sont abéliens.

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 $i \in [\![1\,;n]\!]$ 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 $\{\mathrm{id}\} \subset V_4 \subset A_4 \subset S_4$ est une suite normale pour S_4 dont tous les quotients sont abéliens.

La suite $\{\mathrm{id}\} \triangleleft \langle \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} \rangle \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$ est une suite de résolubilité pour S_4, mais ce n'est pas une suite normale pour S_4 car $\langle \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} \rangle$ n'est pas un sous-groupe normal de S_4.

Deuxième partie :

Anneaux

CHAPITRE 7

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** $\cdot : A \times A \to A$, 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 $+ : A \times A \to A$ 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.*

On peut vérifier que B est un sous-anneau de A si, et seulement si,

- *$(B \neq \varnothing)$;*
- *$\forall (a,b) \in B^2$, 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 $ab \in B$.*

Définition 7.4. *Un **morphisme d'anneaux** d'un anneau A vers un anneau B est une application $f : A \to B$ 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,

- ✦ $I \neq \varnothing$;
- ✦ $\forall (x, y) \in I^2,\ x + y \in I$ *et*
- ✦ $\forall (a, x) \in A \times I,\ ax \in I$.

Propriétés. ✦ 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 s'il contient un élément inversible de A.
- ✦ Une intersection d'idéaux est un idéal.
- ✦ Soit $f : A \to B$ un morphisme d'anneaux.
  - ✧ Si C est un sous-anneau de A, alors $f(C)$ est un sous-anneau de B. En particulier, $\operatorname{Im} f = f(A)$ 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, $\operatorname{Ker} f = f^{-1}(\{0\})$ 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 7.7. *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.*

Théorème 7.8. 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

$$\overline{a} + \overline{b} = \overline{a+b};$$
$$\overline{a}\,\overline{b} = \overline{ab}$$

où $\overline{a}$ 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 $\pi\colon A \to A/I$ définie par $\pi(a) = \overline{a}$ est un morphisme d'anneaux surjectif, appelé **projection canonique**.

Théorème 7.9 (Théorème de passage au quotient)**.** Soit $f\colon A \to B$ 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 $\pi_A\colon A \to A/I$ et $\pi_B\colon B \to B/J$ les projections canoniques.

Alors il existe un unique morphisme d'anneaux $\bar{f} : A/I \to B/J$ tel que $\bar{f} \circ \pi_A = \pi_B \circ f$ (on a donc $\bar{f}(\overline{a}) = \overline{f(a)}$).

Schématiquement, on a

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_B} \\ A/I & \xrightarrow[\bar{f}]{} & B/J. \end{array}$$

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 $b \in \operatorname{Ker} \pi_B = J$. 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 $a' - a \in \operatorname{Ker} \pi_A = I$, donc $f(a' - a) \in J$ et donc $\pi_B(f(a' - a)) = 0$. Or π_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 $y = \pi_B(b)$. 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 "$I \subset \operatorname{Ker} f$". Ainsi, si $f : A \to B$ est un morphisme d'anneaux et si I est un idéal de A tel que $I \subset \operatorname{Ker} f$, alors f induit un unique morphisme d'anneaux $\bar{f} : A/I \to B$ tel que $f = \bar{f} \circ \pi_A$ (c'est-à-dire que $\bar{f}(\overline{a}) = f(a)$).

Théorème 7.10 (Premier théorème d'isomorphisme)**.** Soit $f\colon A \to B$ un morphisme d'anneaux. Le morphisme f induit un isomorphisme d'anneaux

$$\overline{f}\colon A/\operatorname{Ker} f \to \operatorname{Im} f.$$

Théorème 7.11 (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'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 7.12 (Troisième théorème d'isomorphisme)**.** Soit A un anneau. Soit I un idéal de A. Notons $\pi : A \to A/I$ 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 7.13. *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*

$$IJ = \left\{ \sum_{k=1}^{n} x_k y_k;\ n \in \mathbb{N},\ (x_k, y_k) \in I \times J \right\}$$

$$I+J = \left\{ \sum_{k=1}^{n} a_k x_k;\ n \in \mathbb{N},\ x_k \in I \cup J,\ a_k \in A \right\} = \{x+y;\ (x,y) \in I \times J\}.$$

Théorème 7.14 (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 $\pi_I\colon A \to I$ et $\pi_J\colon A \to A/J$ les projections canoniques (morphismes d'anneaux) et considérons $\varphi : A \to A/I \times A/J$ 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 $\operatorname{Ker}\varphi = I \cap J = IJ$.

Démontrons que φ est surjective. Soit $(\overline{y}, \overline{z}) \in A/I \times A/J$, avec $(y,z) \in A^2$ tel que $\overline{y} = \pi_I(y)$ et $\overline{z} = \pi_J(z)$. On cherche $x \in A$ tel que $\varphi(x) = (\overline{y}, \overline{z})$.

Comme dans la première partie, il existe $a \in I$ et $b \in J$ tels que $1 = a+b$. Posons $x = yb + za$. Alors $\pi_I(x) = \pi_I(yb) = \pi_I(y(1-a)) = \pi_I(y - ya) = \pi_I(y) = \overline{y}$ et $\pi_J(x) = \pi_J(za) = \pi_J(z - zb) = \pi_J(z) = \overline{z}$ donc $\varphi(x) = (\overline{y}, \overline{z})$.

Finalement, d'après le premier théorème d'isomorphisme, φ induit un isomorphisme $\overline{\varphi} : A/IJ \to A/I \times A/J$ (donné par $\overline{\varphi}(\overline{x}) = (\pi_I(x), \pi_J(x))$). ✓

Conséquence 7.15. 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 $\overline{\varphi}(\overline{x}) = (\pi_m(x), \pi_n(x))$ où $\pi_m : A \to A/(m)$ et $\pi_n : A \to A/(n)$ sont les projections canoniques. Pour exprimer $\overline{\varphi}^{-1}$, on applique la propriété de Bézout, qui donne $(u, v) \in A^2$ tel que $mu + nv = 1$. Alors $\overline{\varphi}^{-1}(\pi_m(y), \pi_n(z)) = \overline{znu + ymv}$.

Ceci permet, dans le cas où $A = \mathbb{Z}$, de résoudre des systèmes de congruences du type

$$\begin{cases} x \equiv a \pmod{m} \\ y \equiv b \pmod{n} \end{cases}$$

avec m et n deux entiers premiers entre eux.

II Idéaux premiers et maximaux.

Définition 7.16. *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 $a, b \in A$, $ab \in I \Longrightarrow a \in I$ 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, $I \subset J \subset A \Longrightarrow J = I$ 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 7.17. 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 7.17 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 7.18. 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 idéaux premiers (resp. maximaux) de A/I et idéaux premiers (resp. maximaux) de A contenant I.

Démonstration. **(1)** Puisque π 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 π est un morphisme d'anneaux surjectif, $\pi(K)$ est un idéal de A/I pour tout idéal K de A.
On a $\alpha \circ \beta = \mathrm{id}_{\mathbf{I}_{A/I}}$ car $\pi \circ \pi^{-1}(L) = L$ pour tout idéal L de A/I.
Il reste à vérifier que $\beta \circ \alpha = \mathrm{id}_{\mathbf{J}_{A,I}}$ 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, α et β 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 7.17, 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.*** Un produit d'une famille non vide d'ensembles non vides est non 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 7.19. *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 7.20. *Si $(E, \preccurlyeq)$ est un ensemble ordonné et si, pour tous $(x,y) \in E^2$, on a $x \preccurlyeq y$ 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, un dit que $\preccurlyeq$ est un **ordre partiel** ou que $(E, \preccurlyeq)$ est un **ensemble partiellement ordonné**.*

Définition 7.21. *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 de E. Un **majorant** de F dans E est un élément m de E tel que pour tout $x \in F$, $x \preccurlyeq m$.*
- ✦ *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.*

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 7.22 (Lemme de Zorn)**.** Soit $(E, \preccurlyeq)$ un ensemble ordonné, inductif et non vide. Alors il existe un élément maximal dans E.

Démonstration. (admis) ✓

B. Applications

Théorème 7.23 (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 $\mathcal{S} \neq \varnothing$.

$\mathcal{S}$ muni de cet ordre est inductif : soit $(S_i)_{i\in I}$ une partie totalement ordonnée de $\mathcal{S}$. Alors $\cup_{i\in I} S_i$ contient $\mathcal{L}$ et tous les S_i pour $i \in I$. Il reste à vérifier que c'est un élément de $\mathcal{S}$, c'est-à-dire une famille libre, pour démontrer que $\cup_{i\in I} S_i$ est un majorant de $(S_i)_{i\in I}$ dans $\mathcal{S}$. 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 $(S_i)_{i\in I}$ 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 $j \in J$.

D'après le lemme de Zorn, il existe une partie libre maximale dans $\mathcal{S}$, 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 7.24 (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 $(I_j)_{j\in J}$ une famille totalement ordonnée d'idéaux qui contiennent I et qui sont distincts de A. Alors $\cup_{j\in J} I_j$ 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 $(I_j)_{j\in J}$ dans $\mathcal{S}$.

Vérifions donc que $\cup_{j\in J} I_j \in \mathcal{S}$. Tout d'abord, $1 \notin \cup_{j\in J} I_j$ donc $\cup_{j\in J} I_j \neq A$. Il est clair que $I \subset \cup_{j\in J} I_j$. De plus, si x et y sont dans $\cup_{j\in J} I_j$, il existe j_0 tel que x et y soient dans I_{j_0} (puisque la famille des I_j est totalement ordonnée). Alors $x + y \in I_{j_0} \subset \cup_{j\in J} I_j$ et $ax \in I_{j_0} \subset \cup_{j\in J} I_j$ pour tout $a \in A$, donc c'est bien un idéal. On en déduit que $\cup_{j\in J} I_j$ 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 $\mathrm{Frac}(A)$.

Définition-Proposition 7.25. $\mathrm{Frac}(A)$ *est un corps (commutatif), dit* ***corps des fractions*** *de A, pour les opérations suivantes :*

- ✦ $\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$
- ✦ $\frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}$.

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

$$\frac{a_1 s'_1 + a'_1 s_1}{s_1 s'_1} = \frac{as' + a's}{ss'} \qquad \text{(IV.1)} \qquad \text{et que} \qquad \frac{aa'}{ss'} = \frac{a_1 a'_1}{s_1 s'_1}. \qquad \text{(IV.2)}$$

Par hypothèse, on a $a_1 s - a s_1 = 0$ et $a'_1 s' - a' s'_1 = 0$. On a donc $0 = (a_1 s - a s_1)s' s'_1 + (a'_1 s' - a' s'_1)ss_1 = ss'(s'_1 a_1 + s_1 a'_1) - s_1 s'_1(as' + sa')$, ce qui démontre (IV.1), et $0 = (a_1 s - a s_1)a'_1 s' + (a'_1 s' - a' s'_1)as_1 = a_1 a'_1 ss' - aa' s_1 s'_1$, 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 $\varphi : A \to \mathrm{Frac}(A)$ définie par $\varphi(a) = \frac{a}{1}$ est un morphisme d'anneaux injectif. Ainsi A peut être identifié à un sous-anneau de $\mathrm{Frac}(A)$.

Proposition 7.26. Soit A un anneau intègre et soit $\varphi : A \to \mathrm{Frac}(A)$ le morphisme d'anneaux ci-dessus. Pour tout anneau B et pour tout morphisme d'anneaux $f : A \to B$ 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 $g : \mathrm{Frac}(A) \to B$ 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
  - ✧ $g\left(\frac{a}{s} + \frac{a'}{s'}\right) = g\left(\frac{as' + a's}{ss'}\right) = f(as' + a's)f(ss')^{-1}$
    $= f(a)f(s')f(s)^{-1}f(s')^{-1} + f(a')f(s)f(s)^{-1}f(s')^{-1}$
    $= f(a)f(s)^{-1} + f(a')f(s')^{-1} = g\left(\frac{a}{s}\right) + g\left(\frac{a'}{s'}\right)$;
  - ✧ $g\left(\frac{a}{s}\frac{a'}{s'}\right) = g\left(\frac{aa'}{ss'}\right) = f(aa')f(ss')^{-1} = f(a)f(a')f(s)^{-1}f(s')^{-1}$
    $= f(a)f(s)^{-1}f(a')f(s')^{-1} = g\left(\frac{a}{s}\right)g\left(\frac{a'}{s'}\right)$;
  - ✧ $g\left(\frac{1}{1}\right) = f(1)f(1)^{-1} = 1$.
- ✦ $g \circ \varphi = f : g \circ \varphi(a) = g\left(\frac{a}{1}\right) = f(1)^{-1}f(a) = f(a)$. ✓

Remarque. Le morphisme g est nécessairement injectif.

Conséquence 7.27 («Minimalité» du corps des fractions)**.** Soit K un corps contenant A comme sous-anneau. Alors $\mathrm{Frac}(A)$ est (s'identifie à) un sous-corps de K.

Autrement dit, $\mathrm{Frac}(A)$ 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 $\mathrm{Frac}(A) = \mathbb{Q}$.

Exemple. Soit K un corps. Le corps des fractions de l'anneau de polynômes $K[X]$ est le corps des fractions rationnelles $K(X)$.

CHAPITRE 8

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** 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.*

➢ *On dit que p est **premier** s'il n'est pas nul et si l'idéal engendré (p) est premier.*

Remarques. **(1)** Le produit d'un élément irréductible par un élément inversible est un élément irréductible.

(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 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 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. ✓

(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 $(a, b) \in A^2$, $p \mid ab \Rightarrow (p \mid a$ 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. ✓

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 $i \in I$, $a|a_i$ (resp. $a_i|a$).*

(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 $a \in A \setminus \{0\}$; a et 0 sont premiers entre eux si et seulement si a est un élément inversible de A.

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. En particulier, 1 n'est pas un pgcd de a et b car sinon a diviserait 1 et serait donc inversible. Donc a et b ne sont pas premiers entre eux.

Réciproquement, supposons que a ne divise pas b. L'élément 1 est un diviseur commun de a et b. Soit x un autre 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 donc divise 1. Par définition, 1 est donc un pgcd de a et b, 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 $p_1, \dots, p_r$ 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 $1 \leqslant i \leqslant r$, 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 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 ;*

➢ *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 s'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 $p \in \mathcal{P}$, l'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. 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, $v_p(a) \leqslant v_p(b)$ 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. **(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 $v_p(a) \leqslant v_p(b)$ pour tout i, alors $b = au_a^{-1}u_b \prod_{p\in\mathcal{P}} p^{v_p(b)-v_p(a)}$ donc a divise b. *[Les hypothèses sur A ne servent pas ici.]*

($\Rightarrow$) Si $b = ac$, alors pour tout $p \in \mathcal{P}$ on a $v_p(b) = v_p(a) + v_p(c) \geqslant v_p(a)$.

(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 $p \in \mathcal{P}$, $v_p(a)v_p(b) = 0$. Il est clair que 1 est un diviseur commun de a et b. Soit c un diviseur commun de a et b. On a donc $0 \leqslant v_p(c) \leqslant \min(v_p(a), v_p(b)) = 0$ pour tout $p \in \mathcal{P}$ donc $v_p(c) = 0$ pour tout $p \in \mathcal{P}$ et donc $c = u_c \in A^\times$, donc c divise 1. Ainsi, 1 est un pgcd de a et b. ✓

Dans un anneau intègre quelconque, les pgcd et ppcm n'existent pas toujours. Cependant, dans un anneau factoriel, c'est le cas.

Proposition 8.9. Supposons A factoriel. Si $a_1, \ldots, a_r$ ($r \in \mathbb{N}^*$) 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 $\delta_p = \min\{v_p(a_i) \mid i \in [\![1\,;r]\!]\}$ 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 $v_p(d) = \delta_p \leqslant v_p(a_i)$).

➢ Soit $x \in A$ un diviseur commun des a_i. Puisque x divise tous les a_i, on a $v_p(x) \leqslant \min\{v_p(a_i) \mid i \in [\![1\,;r]\!]\} = \delta_p = v_p(d)$ 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 $\mu_p = \max\{v_p(a_i) \mid i \in [\![1\,;r]\!]\}$ 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 $v_p(y) \geqslant \max\{v_p(a_i) \mid i \in [\![1\,;r]\!]\} = \mu_p = v_p(m)$ pour tout $p \in \mathcal{P}$, donc m divise y.

L'élément m est donc bien un ppcm de a et b. ✓

Lemme 8.10. Soit A 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.

Remarquons qu'on n'utilise le fait que A est factoriel que pour justifier de l'existence de pgcd ; l'hypothèse que les a_i, $i \in I$, et les ba_i, $i \in I$, admettent des pgcd aurait suffi. Mais on peut aussi utiliser les décompositions en produits de facteurs irréductibles pour démontrer ce résultat, on utilise alors vraiment le fait 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 dc est un pgcd des a_i donc il est associé à d et donc c est inversible. ✓

Théorème 8.11. 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)⇔(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 84) 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 $v_p(a) \leqslant v_p(b) + v_p(c)$ pour tout $p \in \mathcal{P}$. On en déduit facilement que $v_p(a) \leqslant v_p(c)$ 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 $m \leqslant n$. On raisonne par récurrence sur m.

- ➢ 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 $n = 1$.

➢ Supposons que le résultat soit vrai jusqu'au rang $m-1$ et 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 **(d)**, 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 $\tau : \{2, \dots, m\} \to \{1, \dots, m\} \setminus \{i\}$ 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 8.12. 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 $n \geqslant N$ on ait $I_n = I_N$.

Démonstration. Posons $I = \cup_{n \in \mathbb{N}^*} I_n$. Alors I est un idéal de A (exercice), donc comme A est principal il existe $a \in A$ tel que $I = (a)$. Alors $a \in \cup_{n \in \mathbb{N}^*} I_n$, 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 $n \geqslant N$, on a $I_N \subset I_n \subset I = I_N$ donc $I_n = I_N$. ✓

Proposition 8.13. 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 :

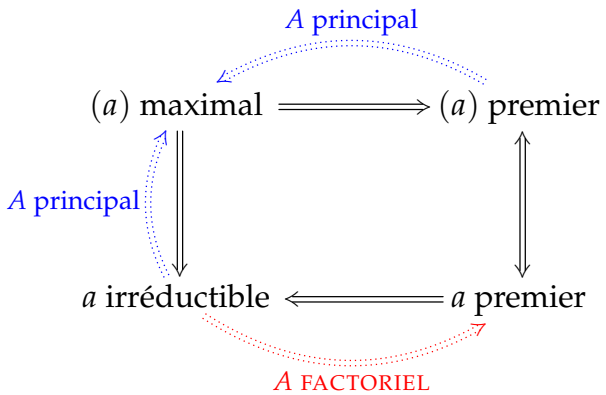
$$(a) \text{ maximal} \implies (a) \text{ premier} \overset{\text{def}}{\iff} a \text{ premier} \overset{\text{p. 83}}{\implies} a \text{ irréductible}$$

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 8.14. 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. 85). Supposons donc que A n'est pas un corps.

D'après la proposition 8.13, la condition de primalité est satisfaite par A. Pour démontrer que A est factoriel, il suffit donc d'après le théorème 8.11 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 $\mathcal{S} \neq \varnothing$.

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 8.12.

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, $\mathcal{S} = \varnothing$ 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 8.13).

Le théorème 8.14 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 8.9 ; on peut les caractériser au moyen d'idéaux.

Proposition 8.15. Supposons A principal et soient $a_1, \dots, a_r$ ($r \in \mathbb{N}^*$) des éléments de A.

➢ Si 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 $a_1A + \cdots + a_rA = (a_1, \dots, a_r)$.

➢ Si les $a_1, \dots, a_r$ 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 $a_1A \cap \cdots \cap a_rA = (a_1) \cap \ldots \cap (a_r)$.

Démonstration. ➢ Soit d un pgcd de $\{a_1, \dots, a_n\}$. Alors pour tout i on a $(a_i) \subset (d)$, donc $(a_1, \dots, a_n) = (a_1) + \cdots + (a_n) \subset (d)$.

Puisque A est principal, il existe $b \in A$ tel que $(a_1, \dots, a_n) = (b)$. Pour tout i, on a $(a_i) \subset (b)$ donc b divise a_i pour tout i et donc b divise d qui est un pgcd des a_i. Par conséquent, $(d) \subset (b)$ et finalement $(a_1, \dots, a_n) = (b) = (d)$.

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, on a $(d) = (a_1, \dots, a_r) \subset (b)$ donc b divise d et donc d est un pgcd des a_i.

➢ Soit m un ppcm de $\{a_1, \dots, a_n\}$. Alors pour tout i on a $(m) \subset (a_i)$, donc $(m) \subset (a_1) \cap \cdots \cap (a_n)$.

Puisque A est principal, il existe $b \in A$ tel que $(a_1) \cap \cdots \cap (a_n) = (b)$. Pour tout i, on a $(b) \subset (a_i)$ donc a_i divise b pour tout i et donc m, qui est un ppcm des a_i, divise b. Par conséquent, $(b) \subset (m)$ et finalement $(a_1) \cap \cdots \cap (a_n) = (b) = (m)$.

Réciproquement, si $m \in A$ est tel que $(m) = (a_1) \cap \cdots \cap (a_r)$, alors m est un multiple commun des a_i, et pour tout autre multiple commun c des a_i, on a $(m) = (a_1) \cap \cdots \cap (a_r) \supset (c)$ donc m divise c et donc m est un ppcm des a_i. ✓

Corollaire 8.16 (Propriété de Bézout)**.** Supposons A principal et soient $a_1, \ldots, a_r$ ($r \in \mathbb{N}^*$) des éléments non tous nuls de A. Alors, les éléments $a_1, \ldots, a_r$ sont premiers entre eux si et seulement s'il existe $x_1, \ldots, x_r \in A$ tels que $a_1x_1 + \cdots + a_rx_r = 1$.

Démonstration. C'est une conséquence immédiate de la proposition 8.15. ✓

On passe maintenant au cas des anneaux euclidiens. Ce sont des exemples d'anneaux principaux.

Définition 8.17. *L'anneau A est dit **euclidien** s'il est intègre et s'il existe une application $\nu : A \setminus \{0\} \longrightarrow \mathbb{N}$ 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 $\nu(r) < \nu(b)$.*
*L'application ν s'appelle un **stathme euclidien**.*

Remarque. Dans la littérature, un tel ν 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 $\nu(a) \leqslant \nu(ab)$ 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 8.18. 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 $= qa \in (a)$ 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 $\nu : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$ définie par $\nu(n) = |n|$).
Si K est un corps, l'anneau $K[X]$ est euclidien (considérer l'application $\nu : K[X] \setminus \{0\} \longrightarrow \mathbb{N}$ définie par $\nu(P) = \deg P$).

Corollaire 8.19. Soit A un anneau commutatif unitaire quelconque (*ie.* qui n'est pas nécessairement intègre). L'anneau $A[X]$ est principal si et seulement si A est un corps.

Démonstration. D'après le théorème 8.18 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 $\varphi : A[X] \to A$ 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. ✓

CHAPITRE 9

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 $d \geqslant \max\{k \mid a_k \neq 0\}$ et $\max\{k \mid a_k \neq 0\} = \deg\left(\sum_{k=0}^{d} a_k X^k\right)$ est le degré du polynôme $\sum_{k=0}^{d} a_k X^k$.

On définit alors récursivement les anneaux de polynômes en plusieurs indéterminées.

Définition 9.1. *Soit $n \in \mathbb{N}$ un 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 $A \to A[X]$ 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 $p \leqslant n$ tel que X_i a pour image X_i pour tout $i \in [\![1\,;p]\!]$.

Proposition 9.2. Tout élément de $A[X_1, \dots, X_n]$ s'écrit, de façon unique, sous la forme

$$\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)} . X_1^{i_1} \dots X_n^{i_n},$$

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.

- 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 $\sum_{n\in\mathbb{N}} a_n X^n$).
- Soit $n \geqslant 1$ tel que le résultat soit vrai pour l'anneau de polynômes en n indéterminées. Soit $P \in A[X_1, \dots, X_n, X_{n+1}]$. 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, $Q_j = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a^{(j)}_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$ avec où $a^{(j)}_{(i_1,\dots,i_n)} \in A$ (somme finie). On en déduit que

$$P = \sum_{j=0}^{d} \sum_{(i_1,\dots,i_n)} a^{(j)}_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}X_{n+1}^{j} = \sum_{(i_1,\dots,i_n,i_{n+1})} b_{(i_1,\dots,i_n,i_{n+1})}.X_1^{i_1}\dots X_n^{i_n}X_{n+1}^{i_{n+1}}$$

où $b_{(i_1,\dots,i_n,i_{n+1})} = a^{(j)}_{(i_1,\dots,i_n)}$. On a démontré l'existence. Démontrons maintenant l'unicité. Il suffit pour cela de démontrer que si $P = \sum_{(i_1,\dots,i_n,i_{n+1})} a_{(i_1,\dots,i_n,i_{n+1})}.X_1^{i_1}\dots X_n^{i_n}X_{n+1}^{i_{n+1}}$ est le polynôme nul, alors tous les coefficients $a_{(i_1,\dots,i_n,i_{n+1})}$ sont nuls.

On peut écrire $0 = \sum_{i_{n+1}\in\mathbb{N}} \left(\sum_{(i_1,\dots,i_n)} a_{(i_1,\dots,i_n,i_{n+1})}.X_1^{i_1}\dots X_n^{i_n}\right) X_{n+1}^{i_{n+1}} = \sum_{i_{n+1}\in\mathbb{N}} Q_{i_{n+1}} X_{n+1}^{i_{n+1}}$ 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 $P = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$. Alors $a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$ 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 $a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$ (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.

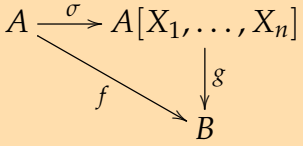
Démonstration. On procède par récurrence sur n.

➢ 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 $PQ \neq 0$.

➢ Supposons que $B = A[X_1,\dots,X_n]$ est intègre pour un $n \geqslant 1$. 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, $f : A \longrightarrow B$ un morphisme d'anneaux et $b_1,\dots,b_n \in B$. On note $\sigma : A \to A[X_1,\dots,X_n]$ l'inclusion naturelle.

Alors il existe un morphisme d'anneaux $g : A[X_1,\dots,X_n] \longrightarrow B$ et un seul tel que, pour $1 \leqslant j \leqslant n$, $g(X_j) = b_j$ et tel que $g\circ\sigma = f$, c'est-à-dire que le diagramme suivant soit commutatif :



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

$$\begin{aligned} g\left(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}\right) &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} g\left(a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}\right) \\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)}).g(X_1)^{i_1}\dots g(X_n)^{i_n} \\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)})b_1^{i_1}\dots b_n^{i_n} \end{aligned}$$

donc g est nécessairement unique.

De plus, on vérifie facilement que l'application $g\colon A[X_1, \dots, X_n] \longrightarrow B$ définie par

$$g\left(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}\right) = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)})b_1^{i_1}\dots b_n^{i_n}$$

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 $k \in [\![1\,;n]\!]$ (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 $P = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$ et $Q = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a'_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$. Alors

$$\begin{aligned} g(P+Q) &= g\left(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} (a_{(i_1,\dots,i_n)} + a'_{(i_1,\dots,i_n)}).X_1^{i_1}\dots X_n^{i_n}\right) \\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)} + a'_{(i_1,\dots,i_n)}).b_1^{i_1}\dots b_n^{i_n} \\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} (f(a_{(i_1,\dots,i_n)}) + f(a'_{(i_1,\dots,i_n)})).b_1^{i_1}\dots b_n^{i_n} \\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)}).b_1^{i_1}\dots b_n^{i_n} + \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a'_{(i_1,\dots,i_n)}).b_1^{i_1}\dots b_n^{i_n} \\ &= g(P) + g(Q). \end{aligned}$$

✦ ✧ Soient $P = a.X_1^{i_1}\dots X_n^{i_n}$ et $Q = a'.X_1^{j_1}\dots X_n^{j_n}$ des termes monomiaux. Alors

$$\begin{aligned} g(PQ) = g(aa'.X_1^{i_1+j_1}\dots X_n^{i_n+j_n}) &= f(aa').b_1^{i_1+j_1}\dots b_n^{i_n+j_n} \\ &= f(a).b_1^{i_1}\dots b_n^{i_n}\cdot f(a').b_1^{j_1}\dots b_n^{j_n} = g(P)g(Q). \end{aligned}$$

✧ 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_ℓ sont des termes monomiaux. En utilisant ce que nous avons déjà démontré, on a

$$\begin{aligned} g(PQ) = g(\sum_{k=1}^{p}\sum_{\ell=1}^{q} T_kS_\ell) &= \sum_{k=1}^{p}\sum_{\ell=1}^{q} g(T_kS_\ell) = \sum_{k=1}^{p}\sum_{\ell=1}^{q} g(T_k)g(S_\ell) \\ &= \left(\sum_{k=1}^{p} g(T_k)\right)\left(\sum_{\ell=1}^{q} g(S_\ell)\right) = g\left(\sum_{k=1}^{p} T_k\right)g\left(\sum_{\ell=1}^{q} S_\ell\right) = g(P)g(Q). \qquad \checkmark \end{aligned}$$

Exemple. Soit A un anneau et soit I un idéal de A. Le morphisme d'anneaux $f : A \to (A/I)[X]$ obtenu par composition de la projection canonique $\pi : A \to A/I$ et de l'inclusion $A/I \to (A/I)[X]$ induit donc grâce au théorème 9.5 un morphisme d'anneaux $\varphi_I : A[X] \to (A/I)[X]$ 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 φ_I est surjectif.

De même, si $f : A \to (A/I)[X_1, \dots, X_n]$ est la composée de la projection canonique $\pi : A \to A/I$ et de l'inclusion $A/I \to (A/I)[X_1, \dots, X_n]$, il existe un morphisme d'anneaux surjectif $\varphi_I : A[X_1, \dots, X_n] \to (A/I)[X_1, \dots, X_n]$ 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 $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la projection canonique. On pose $\pi(n) = \overline{n}$. Le morphisme $\varphi_{(p)} : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ consiste à réduire les coefficients des polynôme modulo p : $\varphi_{(p)}(\sum_{k=0}^n a_k X^k) = \sum_{k=0}^n \overline{a}_k X^k$. 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 $i \in [\![1\,;n]\!]$, 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 $B = A[X_{\sigma(1)}, \dots, X_{\sigma(n)}]$, $f\colon A \to B$ l'inclusion et $b_i = X_{\sigma(i)}$ pour obtenir un morphisme d'anneaux $\varphi : A[X_1, \dots, X_n] \to A[X_{\sigma(1)}, \dots, X_{\sigma(n)}]$ 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 $\psi : A[X_{\sigma(1)}, \dots, X_{\sigma(n)}] \to A[X_1, \dots, X_n]$ 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 $\mathrm{id}_{A[X_1,\dots,X_n]}$ est également un tel endomorphisme, donc par unicité on a $\psi \circ \varphi = \mathrm{id}_{A[X_1,\dots,X_n]}$.

De même, $\varphi \circ \psi = \mathrm{id}_{A[X_{\sigma(1)},\dots,X_{\sigma(n)}]}$ donc φ et ψ 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 :*

$$\deg_{X_k} P := \max\Big\{ i_k \mid a_{(i_1,\dots,i_n)} \neq 0 \Big\}.$$

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 $2X_1^2X_2X_3^3 - 4X_2^2X_3 \in \mathbb{Z}[X_1, X_2, X_3]$ est 3 et le degré partiel en Y du polynôme $X^2Z^3 + X^3Z - 3XZ \in \mathbb{R}[X, Y, Z]$ 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 $\mathcal{F}(A^n, A)$,

$$(f+g)(x) = f(x) + g(x) \quad \text{pour tout } x \in A^n$$
$$(fg)(x) = f(x)g(x) \quad \text{pour tout } x \in A^n.$$

L'élément neutre (resp. unité) est l'application constante égale à 0 (resp. 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 $\widetilde{P} \in \mathcal{F}(A^n, A)$ définie par*

$$\begin{array}{rccc} \widetilde{P} & : & A^n & \longrightarrow & A \\ & & (\alpha_1, \dots, \alpha_n) & \mapsto & \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)} \alpha_1^{i_1} \dots \alpha_n^{i_n} \end{array} .$$

*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 $\widetilde{P}(\alpha_1, \dots, \alpha_n)$.*

Proposition 9.9. Soit $n \in \mathbb{N}^*$. L'application $A[X_1, \dots, X_n] \longrightarrow \mathcal{F}(A^n, A)$, $P \mapsto \widetilde{P}$ 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 $i \in [\![1\,;n]\!]$, 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^{me} composante). Soit $f : A \to \mathcal{F}(A^n, A)$ 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 $A[X_1, \dots, X_n] \to \mathcal{F}(A^n, A)$ qui prolonge f et qui associe π_i à X_i. On constate qu'il s'agit bien de l'application $P \mapsto \widetilde{P}$. ✓

Soit $n \in \mathbb{N}^*$. La proposition 9.9 montre que l'on dispose d'un morphisme d'anneaux surjectif

$$\begin{array}{rccc} \varphi_n & : & A[X_1, \dots, X_n] & \longrightarrow & \mathcal{F}_{\text{pol}}(A^n, A) \\ & & P & \mapsto & \widetilde{P} \end{array} .$$

Remarque. Soit A un anneau intègre. On sait que $\varphi_1 : A[X] \to \mathcal{F}_{\text{pol}}(A, A)$ 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 $\widetilde{P} : A \to A$ 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, 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 φ_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 $n \in \mathbb{N}^*$, φ_n est injectif (puisqu'il est surjectif par construction). On raisonne par récurrence sur n.

Le cas $n = 1$ est connu.

Soit $s \in \mathbb{N}^*$ tel que φ_n est injectif pour tout $n \leqslant s$. 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 $\widetilde{P_{i_0}}(a_1,\dots,a_s) \neq 0$. Soit enfin $\psi\colon A[X_1,\dots,X_{s+1}] \longrightarrow A[X_{s+1}]$ le morphisme d'anneaux tel que $\psi_{|A} = \mathrm{id}_A$, $\psi(X_i) = a_i$ pour $1 \leqslant i \leqslant s$ et $\psi(X_{s+1}) = X_{s+1}$. Alors le polynôme $\psi(P) = \sum_{i\in\mathbb{N}} \widetilde{P_i}(a_1,\dots,a_s)X_{s+1}^i$ de $A[X_{s+1}]$ n'est pas nul puisque $\widetilde{P_{i_0}}(a_1,\dots,a_s) \neq 0$. Il existe donc $a \in A$ tel que $\widetilde{\psi(P)}(a) \neq 0$. On en déduit aussitôt que $\widetilde{P}$ ne s'annule pas en $(a_1,\dots,a_s,a)$, donc la fonction polynomiale 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 polynômiale associée $\widetilde{P} : A \to A$ est nulle. Posons $P = \sum_{i=0}^d a_i X_1^i$.
On dispose d'un morphisme d'anneaux injectif $\sigma : A[X_1] \to A[X_1,\dots,X_n]$ qui envoie X_1 sur X_1 et fixe les éléments de A. Il est clair que $\sigma(P) \neq 0$. Mais on a

$$\widetilde{\sigma(P)}(\alpha_1,\dots,\alpha_n) = \sum_{i=0}^{d} a_i\alpha_1^i = \widetilde{P}(\alpha_1) = 0$$

donc la fonction polynomiale associée au polynôme non nul $\sigma(P)$ est nulle. Ainsi, φ_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 8.19, 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 8.19 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 8.10. 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 8.10 et donc p est un contenu de P. ✓

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 pgcd des coefficients de PQ. Alors, puisque A est factoriel, il existe un pgcd des coefficients de PQ. Soit $\pi \in A$ un diviseur irréductible de ce pgcd ; 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 π. Posons $P = \sum_{i=0}^{d} a_i X^i$, $Q = \sum_{j=0}^{e} b_j X^j$, $i_0 = \min\{i \in [\![0\,;d]\!] \mid \pi \nmid a_i\}$ et $j_0 = \min\{j \in [\![0\,;e]\!] \mid \pi \nmid b_j\}$. 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 π, π 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 π irréductible, il s'ensuit (condition d'Euclide) que π divise a_{i_0} ou b_{j_0}, ce qui constitue une contradiction. Ainsi 1 est un pgcd des coefficients de PQ.

(2) On utilise le lemme 9.12. Il existe des polynômes primitifs $P_1, Q_1 \in A[X]$ 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. ✓

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 $A \to K \to K[X]$ qui est un morphisme d'anneaux. On en déduit donc grâce à la propriété universelle des anneaux de polynômes un morphisme d'anneaux $A[X] \to K[X]$ 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 α, β dans $K \setminus \{0\}$ tels que $P = Q_1R_1$, $Q_1 = \alpha Q$, et $R_1 = \beta R$.

Démonstration. En réduisant tous les coefficients de Q et R aux mêmes dénominateurs, on voit qu'il existe $q, r \in A$ et $Q_0, R_0 \in A[X]$ tels que $qQ = Q_0$ et $rR = R_0$. On a alors $Q_0R_0 = qrP$.

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 $P = \lambda Q_2R_2$. 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 $R_1 = \beta R$. ✓

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 $a \in A$. Démontrons 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 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 $\geqslant 1$ 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 $\geqslant 1$). 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 $\widetilde{Q}$ et $\widetilde{R}$ dans $A[X]$ qui sont primitifs, tels que $\widetilde{Q} \sim Q$ et $\widetilde{R} \sim R$ dans $K[X]$ et qui vérifient $P = c\widetilde{Q}\widetilde{R}$.

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 $\widetilde{Q}$ et $\widetilde{R}$ dans $A[X]$ qui sont primitifs, tels que $\widetilde{Q} \sim Q$ et $\widetilde{R} \sim R$ dans $K[X]$ et qui vérifient $P = \widetilde{Q}\widetilde{R}$.

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 $K = \operatorname{Frac} A$.

➢ 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 $\geqslant 1$. 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 $i \in [\![1\,;r]\!]$ des polynômes primitifs $P_i' \in A[X]$ tels que $P_i' \sim P_i$ dans $K[X]$ vérifiant $P = cP_1' \cdots P_r'$. 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 $P = q_1 \dots q_s P_1' \dots P_r'$ et d'après le théorème précédent, les q_j sont irréductibles dans $A[X]$ et les 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 8.11 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 $A[X] \to (A/(a))[X]$ (*cf.* exemple page 93), 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 $\deg P \geqslant 1$, 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. Par exemple, $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel (Voir travaux dirigés) 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, le nombre de racines de f dans A est au plus $\deg(f)$.

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.

(2) On suppose que A est intègre. Alors pour tout $a \in A$ le polynôme $X-a$ est irréductible.

(3) On suppose que A est intègre. Soit $f \in K[X]$ un polynôme de degré $\deg(f) \geqslant 2$. Si f est irréductible, 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 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 $\deg P \geqslant 0$, $\deg Q \geqslant 0$ 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.

(3) Si f a une racine a dans A, alors $X-a$ divise f donc $f = (X-a)P$ et on a $\deg P = \deg f - 1 \geqslant 1$ (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 $\deg f \geqslant 2$, 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 $\deg P \geqslant 1$, $\deg Q \geqslant 1$, 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* $0 \leqslant i \leqslant d-1$*, d'où* $a_i = 4$ *pour tout* $i \in [\![1\,;d]\!]$*, 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*. Ecrivons* $P = XP_1$*. 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 $a_n \neq 0$, $n \geqslant 1$, 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 $\alpha = \dfrac{p}{q}$ dans $\mathbb{Q}$ avec $(p,q) \in \mathbb{Z}^2$ et $\operatorname{pgcd}(p,q) = 1$, 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 $\mathbb{Z}[X]$.

Soit I un idéal de l'anneau A. On note $\varphi_I : A[X] \to (A/I)[X]$ le morphisme d'anneaux de l'exemple page 93.

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 $a_n \notin I$, $n \geqslant 1$; si $\varphi_I(P)$ est irréductible dans $(A/I)[X]$ ou dans $(\operatorname{Frac}(A/I))[X]$, alors P est irréductible dans $(\operatorname{Frac} A)[X]$.

Démonstration. Notons $K = \operatorname{Frac} A$. 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 ($\deg P \geqslant 1$).

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 $(\operatorname{Frac}(A/I))[X]$, par exemple $\varphi_I(Q)$ est inversible dans $(A/I)[X]$ ou dans $(\operatorname{Frac}(A/I))[X]$, donc dans les deux cas c'est un élément non nul de $\operatorname{Frac}(A/I)$. Donc $\deg \varphi_I(Q) = 0$. Mais $0 \neq \overline{a}_n = \overline{b}_q \overline{c}_r$, donc $\overline{b}_q \neq 0$, 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 $P = 7X^3 - 3X + 75 \in \mathbb{Z}[X]$. 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 $\mathbb{Z}[X]$.

Proposition 9.21 (Critère d'Eisenstein)**.** Supposons A factoriel et considérons $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ avec $n = \deg P \geqslant 1$. S'il existe un élément irréductible p de A tel que $p \nmid a_n$, $p \mid a_i$ pour $0 \leqslant i \leqslant n-1$ et $p^2 \nmid a_0$, alors P est irréductible dans $(\operatorname{Frac} A)[X]$.

Démonstration. Notons $K = \operatorname{Frac} A$. Puisque $\deg P \geqslant 1$, 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 $\ell = \min\{i \in [\![1\,;r]\!] \text{ tel que } p \nmid c_i\}$; comme $\ell \leqslant r < n$, p divise a_ℓ et par définition de ℓ, p divise c_j pour tout $j \in [\![0\,;\ell-1]\!]$, 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_ℓ est divisible par p. Ceci constitue une contradiction. ✓

Exemple. Soit $P(X) = 2X^5 - 28X^3 + 98X^2 - 14 \in \mathbb{Z}[X]$. On applique le critère d'Eisenstein avec $p = 7$. 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 $\mathbb{Z}[X]$.

CHAPITRE 10

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*

$$\begin{array}{ccc} S_n \times A[X_1, \dots, X_n] & \longrightarrow & A[X_1, \dots, X_n] \\ (\sigma, f) & \longmapsto & {}^{\sigma}f = f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \end{array}$$

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. ✦ $X^2 + Y^2 + Z^2$ est un polynôme symétrique de $\mathbb{Z}[X, Y, Z]$ (mais pas de $\mathbb{Z}[X, Y, Z, T]$).
✦ $X_1X_2 + X_2X_3 + X_3X_1$ est un polynôme symétrique de $\mathbb{Z}[X_1, X_2, X_3]$.
✦ $X^3Y + Y^3Z + Z^3X$ 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 $\varphi : A[X_1, \dots, X_n] \to A[X_1, \dots, X_{n-1}]$ 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 $\psi_\gamma : A[X_1, \dots, X_n] \to A[X_1, \dots, X_n]$ l'application définie par $\psi_\gamma(P) = {}^{\gamma}P$. Alors ψ_γ est un automorphisme d'anneaux qui fixe les éléments de A.

Démonstration. Notons que ψ_γ est l'unique morphisme d'anneaux qui fixe les éléments de A et qui vérifie $\psi_\gamma(X_i) = X_{\gamma(i)}$ pour tout i. Il admet comme réciproque $\psi_{\gamma^{-1}}$, qui est l'unique morphisme d'anneaux qui fixe les éléments de A et qui vérifie $\psi_\gamma(X_i) = X_{\gamma^{-1}(i)}$ pour tout

i. En effet, $\psi_\gamma \circ \psi_{\gamma^{-1}}$ et $\mathrm{id}_{A[X_1,\dots,X_n]}$ 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, $\psi_{\gamma^{-1}} \circ \psi_\gamma = \mathrm{id}_{A[X_1,\dots,X_n]}$, donc ψ_γ est bien un automorphisme d'anneaux. ✓

Conséquence 10.5. L'ensemble 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 ψ_γ 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 $\psi : S_n \to \mathrm{Aut}(A[X_1,\dots,X_n])$ qui à γ associe ψ_γ.

II Polynômes symétriques élémentaires

Définition 10.6. *Soit $k \in [\![1\,;n]\!]$. Le polynôme $\sigma_k = \sum_{\substack{H\subset[\![1;n]\!]\\|H|=k}} \left(\prod_{i\in H} X_i\right)$ 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 $\sigma_k = \sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} X_{i_1}X_{i_2}\cdots X_{i_k}$.

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. ✦ $\sigma_1 = X_1 + \cdots + X_n$.

✦ $\sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_{n-1}X_n$.

✦ $\sigma_n = X_1X_2\cdots X_n$.

Lemme 10.7. Les polynômes symétriques élémentaires sont symétriques.

Démonstration. Soit $\gamma \in S_n$. Alors

$$ {}^\gamma\sigma_k = \sum_{\substack{H\subset[\![1;n]\!]\\|H|=k}} \left(\prod_{i\in H} X_{\gamma(i)}\right) \overset{j=\gamma(i)}{=} \sum_{\substack{H\subset[\![1;n]\!]\\|H|=k}} \left(\prod_{j\in\gamma^{-1}(H)} X_j\right) \overset{H'=\gamma^{-1}(H)}{=} \sum_{\substack{H'\subset[\![1;n]\!]\\|H'|=k}} \left(\prod_{j\in H'} X_j\right) = \sigma_k $$

en utilisant la bijection de l'ensemble $\mathcal{P}_k([\![1\,;n]\!])$ des parties de $[\![1\,;n]\!]$ à k éléments dans lui-même définie par $H \mapsto \gamma^{-1}(H)$. ✓

Lemme 10.8. ✦ Soit $\varphi : A[X_1,\dots,X_{n+1}] \to A[X_1,\dots,X_n]$ 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 $k \in [\![0\,;n]\!]$, autrement dit, $\sigma_{n,k} = \sigma_{n+1,k}(X_1,\dots,X_n,0)$.

✦ 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 $k \in [\![1\,;n]\!]$.

Démonstration. La première partie est évidente (ou se déduit de la deuxième). Pour la deuxième,

on a, pour tout $k \in [\![1\,;n]\!]$,

$$\begin{aligned}\sigma_{n,k} + \sigma_{n,k-1}X_{n+1} &= \sum_{\substack{H\subset[\![1;n]\!]\\|H|=k}} \left(\prod_{i\in H} X_i\right) + \sum_{\substack{H'\subset[\![1;n]\!]\\|H'|=k-1}} \left(\prod_{i\in H'} X_i\right) X_{n+1} \\ &= \sum_{\substack{H\subset[\![1;n+1]\!]\\|H|=k \text{ et } n+1\notin H}} \left(\prod_{i\in H} X_i\right) + \sum_{\substack{H\subset[\![1;n+1]\!]\\|H|=k \text{ et } n+1\in H}} \left(\prod_{i\in H} X_i\right) \\ &= \sum_{\substack{H\subset[\![1;n+1]\!]\\|H|=k}} \left(\prod_{i\in H} X_i\right) = \sigma_{n+1,k}. \qquad \checkmark\end{aligned}$$

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 $i \in [\![1\,;n]\!]$. Alors σ_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

  $$P = P_0 + P_1X_n + P_2X_n^2 + \cdots + P_dX_n^d$$

  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 $\gamma'_{|[\![1;n-1]\!]} = \gamma$ et $\gamma'(n) = n$. On a alors

  $$P = {}^{\gamma'}P = \sum_{i=1}^{d} {}^{\gamma'}P_i({}^{\gamma'}X_n)^i = \sum_{i=1}^{d} {}^{\gamma}P_iX_n^i$$

  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 φ 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 $i \in [\![1\,;d]\!]$ 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 $P_i = Q_iX_1\cdots X_{n-1}$ avec $Q_i \in A[X_1,\dots,X_{n-1}]$. Alors $P = \sum_{i=1}^{d} P_iX_n^i = \sum_{i=1}^{d} Q_iX_1\cdots X_{n-1}X_n^i$ 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 $P = \sum_{\underline{i}\in\mathbb{N}^n} a_{\underline{i}}X_1^{i_1}\cdots X_n^{i_n}$ et $\deg P = \max\{\sum_{k=1}^{n} i_k;\ a_{\underline{i}} \neq 0\}$. On a alors $P\sigma_n = \sum_{\underline{i}\in\mathbb{N}^n} a_{\underline{i}}X_1^{i_1+1}\cdots X_n^{i_n+1}$ donc $\deg(P\sigma_n) = \max\{\sum_{k=1}^{n}(i_k+1);\ a_{\underline{i}} \neq 0\} = \max\{(\sum_{k=1}^{n} i_k)+n;\ a_{\underline{i}} \neq 0\} = \deg P + n$.

Proposition 10.10. Soit P un polynôme tel que $P(\sigma_1,\dots,\sigma_n) = 0$. Alors $P = 0$.

Démonstration. Pour tout $n \in \mathbb{N}^*$, soit $\psi_n \colon A[X_1,\dots,X_n] \to A[X_1,\dots,X_n]$ 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 $i \in [\![1\,;n]\!]$. Il s'agit de démontrer que ψ_n est injectif.

On raisonne par récurrence sur n.

✦ Si $n = 1$, le résultat est clair ($\sigma_1 = X_1$ et $\psi_1 = \mathrm{id}_{A[X_1]}$).

✦ Soit $n \geqslant 2$ tel que le résultat soit vrai au rang $n-1$, c'est-à-dire que ψ_{n-1} est injectif. Supposons par l'absurde que $\mathrm{Ker}(\psi_n) \neq \{0\}$. Alors l'ensemble $\{\deg f \mid f \in \mathrm{Ker}(\psi_n) \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$ donc elle admet un minimum d_0. Soit $P \in \mathrm{Ker}(\psi_n) \setminus \{0\}$ 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 $\deg Q < d_0$ (on peut raisonner comme dans la remarque) et $Q \in \mathrm{Ker}(\psi_n) \setminus \{0\}$, 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 $\varphi \colon A[X_1,\dots,X_n] \to A[X_1,\dots,X_{n-1})]$ défini par $\varphi(f) = f(X_1,\dots,X_{n-1},0)$, on a

$$\begin{aligned}\psi_{n-1}(P_0) &= P_0(\sigma_{n-1,1},\dots,\sigma_{n-1,n-1}) = P(\sigma_{n-1,1},\dots,\sigma_{n-1,n-1},0)\\ &= P(\varphi(\sigma_{n,1}),\dots,\varphi(\sigma_{n,n})) = \varphi(P(\sigma_{n,1},\dots,\sigma_{n,n})) \qquad (\varphi \text{ morphisme d'anneaux})\\ &= \varphi(\psi_n(P)) = \varphi(0) = 0.\end{aligned}$$

On a donc bien une contradiction, donc $\mathrm{Ker}(\psi_n) = \{0\}$. ✓

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 $P = \sum_{\underline{i}\in\mathbb{N}^n} a_{\underline{i}} X_1^{i_1}\cdots X_n^{i_n}$, le poids de P est $\max\Big\{\mathrm{poids}(X_1^{i_1}\cdots X_n^{i_n}) \mid a_{\underline{i}} \neq 0\Big\} = \max\{i_1 + 2i_2 + 3i_3 + \cdots + ni_n \mid a_{\underline{i}} \neq 0\}$.*

Exemple. Le polynôme $P = X_1 + X_1X_2^2 + X_1X_3$ 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.

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 σ_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, $\mathrm{poids}(P) = \max\{\mathrm{poids}(M_j) \mid 1 \leqslant j \leqslant r\}$. On a alors

$$\begin{aligned}\deg P(\sigma_1,\dots,\sigma_n) = \deg\left(\sum_{j=1}^{r} a_j M_j(\sigma_1,\dots,\sigma_n)\right) &\leqslant \max\{\deg M_j(\sigma_1,\dots,\sigma_n) \mid 1 \leqslant j \leqslant r\}\\ &= \max\{\mathrm{poids}(M_j) \mid 1 \leqslant j \leqslant r\}\\ &= \mathrm{poids}(P).\end{aligned}$$

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 $T(\sigma_1,\dots,\sigma_n) = P$. Ce polynôme 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.
L'unicité découle de la proposition 10.10. Démontrons l'existence.
On raisonne par récurrence sur n (le nombre d'indéterminées).

✦ Si $n = 1$, le résultat est évident, car $\sigma_{1,1} = X_1$.

✦ Soit $n > 1$ tel que le résultat soit vrai pour les polynômes symétriques de $A[X_1, \dots, X_{n-1}]$.
Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique de degré total $d \in \mathbb{N}$. On fait maintenant un raisonnement par récurrence sur d.

✧ Si $d = 0$, c'est évident (P est constant).

✧ Soit $d > 0$ tel que le résultat est vrai pour les polynômes symétriques de $A[X_1, \dots, X_n]$ de degré total inférieur ou égal à $(d-1)$.
Soit φ 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 $\varphi(P) = V(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1})$.
Posons $\widetilde{P} = V(\sigma_{n,1}, \dots, \sigma_{n,n-1})$ (on a remplacé les $\sigma_{n-1,k}$ par les $\sigma_{n,k}$ correspondant). Notons que $\deg \widetilde{P} \leqslant \text{poids}(V) \leqslant d$. Alors $\widetilde{P}$ est un polynôme symétrique de $A[X_1, \dots, X_n]$ et on a $\varphi(P - \widetilde{P}) = 0$ donc X_n divise $P - \widetilde{P}$ dans $A[X_1, \dots, X_n]$. On en déduit grâce au lemme 10.9 que $\sigma_{n,n}$ divise $P - \widetilde{P}$.
Posons $P - \widetilde{P} = Q\sigma_{n,n}$. Alors Q est symétrique ; en effet, si $\gamma \in S_n$, alors $({}^\gamma Q)\sigma_{n,n} = {}^\gamma(Q\sigma_{n,n}) = {}^\gamma(P - \widetilde{P}) = P - \widetilde{P} = Q\sigma_{n,n}$ et on en déduit que ${}^\gamma Q = Q$ (cf. remarque p. 105).
De plus, $\deg Q = \deg(Q\sigma_{n,n}) - n = \deg(P - \widetilde{P}) - n \leqslant d - n < d$ donc, par hypothèse de récurrence, on peut écrire $Q = W(\sigma_{n,1}, \dots, \sigma_{n,n})$ pour un unique polynôme $W \in A[Y_1, \dots, Y_n]$ de poids $\deg Q$.
Posons enfin $T = V + WY_n$. On a $T(\sigma_{n,1} \dots, \sigma_{n,n}) = V(\sigma_{n,1} \dots, \sigma_{n,n}) + W(\sigma_{n,1} \dots, \sigma_{n,n})\sigma_{n,n} = \widetilde{P} + Q\sigma_{n,n} = P$. On a donc démontré l'existence.
On a de plus $\text{poids}(T) \leqslant \max(\text{poids}(V), n + \text{poids}(W)) \leqslant d$ et si $\text{poids}(T) < d$ alors $d = \deg P = \deg T(\sigma_{n,1}, \dots, \sigma_{n,n}) \leqslant \text{poids}(T) < d$, 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 σ_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 $\varphi_Z : A[X, Y, Z] \to A[X, Y]$ 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 $\varphi_3 \colon A[X_1, X_2, X_3] \to A[X_1, X_2]$ et $\varphi_2 \colon A[X_1, X_2] \to A[X_1]$ 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 ψ_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.

IV Coefficients et racines de polynômes

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 $L[X]$.

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 α. Puisque α 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 $d-1$. D'après la première partie, il existe un corps K' dont K est un sous-corps et dans lequel P a une racine α. 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 degre 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 $k \in [\![0\,;n]\!]$, 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 $a_n^{-1}P = (X-\beta_1)\cdots(X-\beta_n) = X^n - \widetilde{\sigma}_1 X^{n-1} + \widetilde{\sigma}_2 X^{n-2} + \cdots + (-1)^n \widetilde{\sigma}_n$ d'après le théorème, où $\widetilde{\sigma}_k = \sigma_k(\beta_1, \ldots, \beta_n)$. 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 σ_1 est la somme des racines et σ_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 σ_k désigne le $k^{\text{ième}}$ polynôme symétrique élémentaire en les α_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 α_1 et α_2 sont les deux racines de $X^2 - sX + p = X^2 - 2X + 5$ et α_3 et α_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 $n \geqslant 1$ 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 $j \in [\![1\,;d]\!]$. On doit démontrer que l'un au moins des α_j est dans $\mathbb{C}$.

Notons $\sigma_1, \dots, \sigma_d$ les polynômes symétriques élémentaires en $X_1, \dots, X_d$ et posons $\widetilde{\sigma}_k = \sigma_k(\alpha_1, \dots, \alpha_d)$. D'après les relations coefficients-racines, pour tout k on a $\widetilde{\sigma}_k \in \mathbb{R}$.

Pour tout $(i,j) \in \mathbb{N}^2$ avec $1 \leqslant i, j \leqslant d$ et tout $c \in \mathbb{R}$, on pose $\beta_{ij}^{(c)} = \alpha_i + \alpha_j + c\alpha_i\alpha_j$; 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

$$\widetilde{Q}_c = \prod_{1 \leqslant i < j \leqslant d} (X - \beta_{ij}^{(c)}) \in L[X],\ c \in \mathbb{R}.$$

On a $\widetilde{Q}_c = Q_c(\alpha_1, \dots, \alpha_d)$ où $Q_c = \prod_{1 \leqslant i < j \leqslant d}(X - X_i - X_j - cX_iX_j) \in \mathbb{R}[X][X_1, \dots, X_d]$. 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 $\widetilde{Q}_c = T(\widetilde{\sigma}_1, \dots, \widetilde{\sigma}_d) \in \mathbb{R}[X]$ puisque les $\widetilde{\sigma}_k$ sont réels.

De plus, $\deg \widetilde{Q}_c = \left|\left\{(i,j) \in [\![1\,;d]\!]^2 \mid i < j\right\}\right| = \sum_{i=1}^{d-1}(d-i) = \frac{d(d-1)}{2} = 2^{n-1}q'$ avec $q' = q(d-1)$ impair. Donc d'après l'hypothèse de récurrence $\widetilde{Q}_c$ a une racine γ_c dans $\mathbb{C}$.

Par conséquent, pour tout $c \in \mathbb{R}$, il existe $(i(c), j(c)) \in [\![1\,;d]\!]^2$ 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 $u = \gamma_{c_1} - c_1 v \in \mathbb{C}$. De plus, α_r et α_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 α_r et α_s de P sont dans $\mathbb{C}$, donc P a bien une racine complexe. ✓

V Exemple : le discriminant

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* $\mathrm{Disc}(P) = \prod_{i<j}(t_i - t_j)^2$.

$\mathrm{Disc}(P)$ 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 ± 1. C'est donc un polynôme en les σ_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 $\mathrm{Disc}(P) = (t_1 - t_2)^2 = (t_1 + t_2)^2 - 4t_1t_2 = \sigma_1^2 - 4\sigma_2 = b^2 - 4c$.

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 $\mathrm{Disc}(P) = -4a^3 - 27b^2$.

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 $\mathrm{Disc}(P) \in K[t_1, t_2, t_3]$ est homogène de degré 6, donc il existe un polynôme $T \in K[Y_1, Y_2, Y_3]$ de poids 6 tel que $\mathrm{Disc}(P) = T(\sigma_1, \sigma_2, \sigma_3)$. 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 $\mathrm{Disc}(P) = T(\sigma_1, \sigma_2, \sigma_3) = \lambda\sigma_2^3 + \mu\sigma_3^2 = \lambda a^3 + \mu b^2$. Ceci est vrai pour tout polynôme P de la forme $P = X^3 + aX + b$, c'est-à-dire que λ et μ ne dépendent pas de a et b (le polynôme $T = \in K[Y_2, Y_3]$ ne dépend pas des σ_i). On va donc spécialiser à des polynômes particuliers.

✦ Soit $P = X^3 - X = X(X-1)(X+1)$. On a alors $\mathrm{Disc}(P) = ((0-(-1))(0-1)(-1-(-1)))^2 = 4$ 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 $\mathrm{Disc}(P) = \big((1-j)(1-j^2)(j-j^2)\big)^2 = -27$ donc, puisqu'ici $a = 0$ et $b = -1$, on a $\mu = -27$.

Finalement, $\mathrm{Disc}(P) = -4a^3 - 27b^2$. ✓

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 $\prod_{1\leqslant i<j\leqslant 3}(t_i - t_j)^2$ et alors $P(X) = \prod_{i=1}^{3}(Y - (t_i + \frac{a}{3}))$ a pour discriminant $\prod_{1\leqslant i<j\leqslant 3}\big((t_i + \frac{a}{3}) - (t_j + \frac{a}{3})\big)^2 = \prod_{1\leqslant i<j\leqslant 3}(t_i - t_j)^2$.

De plus, $P(X) = \big(Y - \frac{a}{3}\big)^3 + a\big(Y - \frac{a}{3}\big)Y^2 + b\big(Y - \frac{a}{3}\big) + c = Y^3 + pY + q$ 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, $\mathrm{Disc}(P) \neq 0$.

Démonstration. Evident. ✓

Fin du cours.

VI 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 10.22. *Soit $(P,Q) \in K[X]^2$ avec $p = \deg P \geqslant 1$ et $q = \deg Q \geqslant 1$. Soit $\varphi : K_{q-1}[X] \times K_{p-1}[X] \to K_{p+q-1}[X]$ l'application linéaire définie par $\varphi(U,V) = UP + VQ$.*
*On appelle **résultant de P et Q** et on note $\mathrm{Res}(P,Q) \in K$ le déterminant de φ.*

Remarque. On munit $K_{q-1}[X] \times K_{p-1}[X]$ de la base $\mathcal{E} = \big\{(X^{q-1},0),\dots,(X,0),(1,0),(0,X^{p-1}),\dots,(0,X),(0,1)\big\}$ et $K_{p+q-1}[X]$ de la base $\mathcal{F} = \big\{X^{p+q-1},\dots,X,1\big\}$. 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 $\mathrm{Res}(P,Q)$ 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 $0 \leqslant i \leqslant q-1$ 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 $\mathrm{Res}(P,Q)$ 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 $Q = b_2X^2 + b_1X^1 + b_0$ on a

$$\mathrm{Res}(P,Q) = \begin{vmatrix} a_3 & 0 & b_2 & 0 & 0 \\ a_2 & a_3 & b_1 & b_2 & 0 \\ a_1 & a_2 & b_0 & b_1 & b_2 \\ a_0 & a_1 & 0 & b_0 & b_1 \\ 0 & a_0 & 0 & 0 & b_0 \end{vmatrix}.$$

Définition 10.23. *Soit P un polynôme de degré $p \geqslant 1$ et soit a une constante.*

*On appelle **résultant** de P et a et on note $\mathrm{Res}(P,a)$ le déterminant de l'application linéaire $\varphi : K_{p-1}[X] \to K_{p-1}[X]$ définie par $\varphi(U) = aU$. Autrement dit, $\mathrm{Res}(P,a) = a^p$.*

*On appelle **résultant** de a et P et on note $\mathrm{Res}(a,P)$ le déterminant de l'application linéaire $\varphi : K_{p-1}[X] \to K_{p-1}[X]$ définie par $\varphi(U) = aU$. Autrement dit, $\mathrm{Res}(a,P) = a^p$.*

Remarque. Avec la convention $K_{-1}[X] = \{0\}$, cette définition coïncide avec la définition précédente pour les polynômes non constants.

Proposition 10.24. 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) $\mathrm{Res}(P,Q) = (-1)^{pq}\,\mathrm{Res}(Q,P)$.

(2) $\mathrm{Res}(\lambda P, \mu Q) = \lambda^q \mu^p\,\mathrm{Res}(P,Q)$.

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 ε désigne la signature.

Soit $\gamma = \begin{pmatrix} p+q & p+q-1 & \cdots & 3 & 2 & 1 \end{pmatrix} \in S_{p+q}$ la permutation circulaire. Notons que $\varepsilon(\gamma) = (-1)^{p+q-1}$ car $\gamma = \begin{pmatrix} p+q-1 & p+q-2 \end{pmatrix}\begin{pmatrix} p+q-2 & p+q-3 \end{pmatrix}\cdots\begin{pmatrix} 3 & 2 \end{pmatrix}\begin{pmatrix} 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & p+q \end{pmatrix}$ est un produit de $p+q-1$ transpositions. Si on permute les colonnes de $\begin{pmatrix} A & B \end{pmatrix}$ avec γ, 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 γ^q aux colonnes. Puisque ε 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 $\mathrm{Res}(P,Q) = (-1)^{pq}\,\mathrm{Res}(Q,P)$.

(2) Cela découle de la multilinéarité du déterminant (chacune des q colonnes C_P de A est multipliée par λ et chacune des p colonnes C_Q de B est multipliée par μ). ✓

Proposition 10.25. 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) $\mathrm{Res}(P, Q) = 0$.

(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, φ n'est pas surjective et donc $\mathrm{Res}(P, Q) = \det \varphi = 0$.
- (ii)⇒(iii). Puisque $\det \varphi = \mathrm{Res}(P, Q) = 0$, l'application linéaire φ n'est pas injective. Soit $(U, V) \in \mathrm{Ker}\, \varphi$. Alors $UP + VQ = \varphi(U, V) = 0$.
- (iii)⇒(ii). 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 $p = \deg P \leqslant \deg V \leqslant p - 1$ donc on a obtenu une contradiction. ✓

Dans la suite, on fixe un polynôme P de degré $p \geqslant 1$ et de coefficient dominant a_p. On note $E = K[X]/(P)$.

Lemme 10.26. Notons x la classe de X dans E. Alors E est un K-espace vectoriel de dimension p et de base $\mathcal{B} = \left\{x^{p-1}, x^{p-2}, \ldots, x, 1\right\}$.

Démonstration. Pour vérifier que E est bien un K-espace vectoriel, il suffit de vérifier que $(P) = \{PQ; Q \in K[X]\}$ 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 $u = Q(x) = A(x)P(x) + R(x) = R(x) \in \mathrm{vect}\{\mathcal{B}\}$. Donc $\mathcal{B}$ est une famille génératrice de E.

Supposons maintenant que $\sum_{i=0}^{p-1} \lambda_i x^i = 0$ avec $(\lambda_0, \ldots, \lambda_{p-1}) \in K^p$. 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 10.27. Soit $Q \in K[X] \setminus \{0\}$. L'application $\theta_Q : E \to E$ qui à un vecteur u associe $Q(x)u$ est une application linéaire.

De plus, si pour $i \in [\![0\,;p-1]\!]$ on note R_i le reste de la division euclidienne de $X^i Q$ par P, alors la matrice de θ_Q dans $\mathcal{B}$ est la matrice du système de vecteurs $\left\{R_{p-1}, \ldots, R_0\right\}$ dans la base $\mathcal{F}$ de $K_{p+q-1}[X]$.

Démonstration. Il est facile de vérifier que θ_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^{me} colonne de la matrice de θ_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 $\left\{X^{p-1}, \ldots, X, 1\right\}$ de $K_{p-1}[X]$ ou dans la base $\mathcal{F}$ de $K_{p+q-1}[X]$. ✓

Lemme 10.28. Soit $Q \in K[X] \setminus \{0\}$ et soit $q = \deg Q$. Alors $\mathrm{Res}(P, Q) = a_p^q \det(\theta_Q)$.

Démonstration. Si $q = 0$ alors $Q = b_0 \in K$ et on a $\det(\theta_Q) = b_0^p = \mathrm{Res}(P, b_0)$. Supposons donc que $q > 0$.

On rappelle que $\mathrm{Res}(P, Q)$ 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 $X^iQ = A_iP + R_i$ 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 θ_Q dans $\mathcal{B}$, et où la matrice T est triangulaire inférieure $q \times q$ de termes diagonaux tous égaux à a_p. Ainsi, $\mathrm{Res}(P, Q) = \begin{vmatrix} T & 0 \\ N & M \end{vmatrix} = a_p^q \det(M) = a_p^q \det(\theta_Q)$. ✓

Proposition 10.29. Soit $\alpha \in K$ et soient P, Q, R des polynômes de $K[X]$. Alors

(i) $\mathrm{Res}(X - \alpha, Q) = Q(\alpha)$,

(ii) $\mathrm{Res}(P, QR) = \mathrm{Res}(P, Q)\,\mathrm{Res}(P, R)$ et $\mathrm{Res}(PR, Q) = \mathrm{Res}(P, Q)\,\mathrm{Res}(R, Q)$,

(iii) Si R est le reste de la division euclidienne de Q par P et si $\deg R = r \geqslant 0$ alors $\mathrm{Res}(P, Q) = a_p^{q-r}\,\mathrm{Res}(P, R)$.

Démonstration. (i) Ici $p = 1$, $a_p = 1$ et $R_0 = Q(\alpha)$ donc $\theta_Q = Q(\alpha)\,\mathrm{id}_K$ et finalement $\mathrm{Res}(X - \alpha, Q) = \det(Q(\alpha)) = Q(\alpha)$.

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* $\mathrm{Res}(X - \alpha, Q)$ *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 :

$$L_{q+1} \longleftarrow L_{q+1} + \alpha L_q + \alpha^2 L_{q-1} + \cdots + \alpha^q L_1 = \sum_{i=0}^{q} \alpha^i L_{q+1-i}.$$

On a alors

$$\mathrm{Res}(P, Q) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & b_q \\ -\alpha & 1 & 0 & \cdots & 0 & b_{q-1} \\ \vdots & & & \cdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_1 \\ 0 & 0 & 0 & \cdots & 0 & Q(\alpha) \end{vmatrix} = Q(\alpha) \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ -\alpha & 1 & 0 & \cdots & 0 \\ \vdots & & & \cdots & \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = Q(\alpha)$$

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 $\mathrm{Res}(P, QR) = a_p^{q+r} \det(\theta_{QR})$. Mais il est facile de vérifier que $\theta_{QR} = \theta_R \circ \theta_Q$ donc

$$\mathrm{Res}(P, QR) = a_p^{q+r} \det(\theta_{QR}) = a_p^q a_p^r \det(\theta_R) \det(\theta_Q) = \mathrm{Res}(P, Q)\,\mathrm{Res}(P, R)$$

en utilisant à nouveau le lemme précédent.

La deuxième partie découle de la première et de la proposition 10.24.

(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 10.30. Si $P \in K[X]$ est scindé sur K de racines $\alpha_1, \dots, \alpha_p$, alors

$$\operatorname{Res}(P, Q) = a_p^q Q(\alpha_1) \cdots Q(\alpha_p).$$

Si de plus $Q \in K[X]$ est scindé sur K de racines $\beta_1, \dots, \beta_q$, alors

$$\operatorname{Res}(P, Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j).$$

Démonstration. On a $P = a_p(X - \alpha_1) \cdots (X - \alpha_p)$ donc d'après la proposition 10.24 on a $\operatorname{Res}(P, Q) = a_p^q \operatorname{Res}((X - \alpha_1) \cdots (X - \alpha_p), Q)$. 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 $\operatorname{Res}(P, Q) = \operatorname{Res}(R(X - \alpha_p), Q) = \operatorname{Res}(R, Q) \operatorname{Res}(X - \alpha_n, Q) = \big(Q(\alpha_1) \cdots Q(\alpha_{p-1})\big) Q(\alpha_p)$ 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 $\operatorname{Res}(P, Q) = a_p^q \prod i = 1^p Q(\alpha_i) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j)$. ✓

On peut généraliser la définition de discriminant comme suit.

Définition 10.31. *Soit $P \in K[X]$. On définit le **discriminant** de P par*

$$\operatorname{Disc}(P) = (-1)^{p(p-1)/2} a_p^{-1} \operatorname{Res}(P, P').$$

Remarque. Si P est scindé de racines $\alpha_1, \dots, \alpha_p$ dans K, alors

$$\operatorname{Disc}(P) = (-1)^{p(p-1)/2} a_p^{2p-2} \prod_{i \neq j} (\alpha_i - \alpha_j) = a_p^{2p-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

On constate que pour $a_p = 1$ on retrouve la définition précédente du discriminant.

Corollaire 10.32. Soit $P \in K[X]$. Les polynômes P et P' sont premiers entre eux si, et seulement si, $\operatorname{Disc}(P) \neq 0$.

En particulier, si P est scindé sur K, alors P n'a que des racines simples si, et seulement si, $\operatorname{Disc}(P) \neq 0$.