Cours de Licence 3: Structures algébriques 2

Cours de: Olivier Brinon
Rédigé par Hugo Clouet*

Année universitaire 2023 - 2024
Version: 9 novembre 2025

Table des matières

*email: hugo.clouet@etu.u-bordeaux.fr

Bibliographie sommaire

[1] O. Brinon, *Structures Algébriques 2, Cours à l'Université de Bordeaux 2023/2024*, document électronique disponible en ligne

[2] J. Calais, *Éléments de théorie des groupes*, PUF (1984)

[3] M. Demazure, *Cours d'algèbre*, Cassini (2009)

[4] D. Perrin, *Cours d'algèbre*, Ellipses (1996)

[5] J.-P. Serre, *Groupes finis, Cours à l'École Normale supérieure de Jeunes Filles 1978/1979*, document électronique disponible en ligne

1 Théorie des Groupes

1.1 Rappels

1.1.1 Relations d'équivalence et ensembles quotients

Définition 1.1.1.1. Soit X un ensemble.
(i) Une *relation d'équivalence* sur X est une relation binaire $\mathcal{R}$ sur X vérifiant les propriétés suivantes :
- $\mathcal{R}$ est *réflexive* : $(\forall x \in X)\ x\mathcal{R}x$;
- $\mathcal{R}$ est *symétrique* : $(\forall x, y \in X)\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$;
- $\mathcal{R}$ est *transitive* : $(\forall x, y, z \in X)\ (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

(ii) La *classe d'équivalence* de $x \in X$ est alors $[x] = \{y \in X;\ x\mathcal{R}y\}$. C'est une partie de X et si $x_1, x_2 \in X$, alors on a $[x_1] = [x_2]$ ou $[x_1] \cap [x_2] = \varnothing$: les classes d'équivalence forment une partition de X. Cette partition détermine entièrement $\mathcal{R}$: on a $x\mathcal{R}y \Leftrightarrow [x] = [y]$.
(iii) L'*ensemble quotient* $X/\mathcal{R}$ est la partie de $\mathcal{P}(X)$ constituée des classes d'équivalence. Si $A \in X/\mathcal{R}$, alors $A = [x]$ pour tout $x \in A$. Un tel élément x s'appelle un *représentant* de A.

Exemple 1.1.1.2. Soit $f\colon X \to Y$ une application. On définit une relation d'équivalence $\mathcal{R}_f$ sur X en posant $x_1\mathcal{R}_f x_2 \Leftrightarrow f(x_1) = f(x_2)$. Par définition, les classes d'équivalence sont les pré-images non vides des singletons *i.e.* pour $y \in f(X) \subset Y$, on a $[y] = f^{-1}(y)$.

Définition 1.1.1.3. Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble X, on dispose de la *surjection canonique* :

$$\begin{aligned} \pi_{\mathcal{R}}\colon X &\to X/\mathcal{R} \\ x &\mapsto [x] \end{aligned}$$

Un *système complet de représentants* est une partie $T \subset X$ telle que la restriction de $\pi_{\mathcal{R}}$ à T induise une bijection $T \xrightarrow{\sim} X/\mathcal{R}$. Cela signifie que pour tout $A \in X/\mathcal{R}$, il existe un unique $t \in T$ tel que $A = [t]$ *i.e.* tel que t soit un représentant de A. Dans ce cas, tout élément de X est équivalent à un unique élément de T.

Remarque 1.1.1.4. Si on accepte l'axiome du choix, il existe toujours un système de représentants.

Proposition 1.1.1.5 (Propriété universelle)**.** Soient $\mathcal{R}$ une relation d'équivalence sur un ensemble X et $f\colon X \to Y$ une application. Supposons que $x_1\mathcal{R}x_2 \Rightarrow f(x_1) = f(x_2)$. Il existe alors une unique application $\widetilde{f}\colon X/\mathcal{R} \to Y$ telle que $f = \widetilde{f} \circ \pi_{\mathcal{R}}$.

Démonstration. Pour l'existence, il suffit de vérifier que $f(x)$ ne dépend pas du choix de $x \in A$, ce qui résulte précisément de l'hypothèse sur f. Si $A \in X/\mathcal{R}$, il existe $x \in X$ tel que $A = [x] = \pi_{\mathcal{R}}(x)$, donc $\widetilde{f}(A) = \widetilde{f}(\pi_{\mathcal{R}}(x)) = f(x)$, d'où l'unicité de l'application $\widetilde{f}$. □

Corollaire 1.1.1.6 (Décomposition canonique d'une application)**.** Soit $f\colon X \to Y$ une application. Il existe une unique application $\widetilde{f}\colon X/\mathcal{R}_f \to f(X)$ telle que $f = \iota \circ \widetilde{f} \circ \pi_{\mathcal{R}_f}$ où $\iota\colon f(X) \hookrightarrow Y$ est l'inclusion. L'application $\widetilde{f}$ est alors bijective.

$$\begin{array}{ccc} X & \xrightarrow{\quad f \quad} & Y \\ {\scriptstyle \pi_{\mathcal{R}_f}}\downarrow & & \uparrow{\scriptstyle \iota} \\ X/\mathcal{R}_f & \xrightarrow[\sim]{\ \widetilde{f}\ } & f(X) \end{array}$$

Démonstration. L'application f se factorise uniquement en $f = \iota \circ g$ où $g\colon X \to f(X)$ est surjective. La proposition précédente appliquée à $\mathcal{R} = \mathcal{R}_f$ fournit alors une unique application $\widetilde{f}\colon X/\mathcal{R}_f \to f(X)$ telle que $f = \iota \circ \widetilde{f} \circ \pi_{\mathcal{R}_f}$. Si $x_1, x_2 \in X$ sont tels que $\widetilde{f}([x_1]) = \widetilde{f}([x_2])$, alors $f(x_1) = f(x_2)$ *i.e.* $x_1\mathcal{R}_f x_2$, d'où $[x_1] = [x_2]$, ce qui montre que $\widetilde{f}$ est injective. Elle est de plus surjective parce que g l'est. □

1.1.2 Groupes : définitions et propriétés de base

Définition 1.1.2.1. Un *groupe* est un couple $(G, *)$ où G est un ensemble et $*\colon G \times G \to G$ est une loi de composition interne, vérifiant les conditions suivantes :
(i) $(\forall x, y, z \in G)\ (x * y) * z = x * (y * z)$; *(associativité)*
(ii) il existe un élément $e \in G$ tel que : $(\forall x \in G)\ e * x = x * e = x$; *(élément neutre)*
(iii) pour tout $x \in G$, il existe un élément $x' \in G$ tel que : $x * x' = x' * x = e$. *(inverse)*
On dit que G est *abélien* (ou *commutatif*) lorsque : $(\forall x, y \in G)\ x * y = y * x$.

Remarque 1.1.2.2. (1) L'élément neutre est unique. L'inverse d'un élément est unique. (exercice)
(2) Dans la pratique, on parle du groupe G en omettant la loi $*$ dans la notation.
(3) En général, on note la loi multiplicativement : si $x, y \in G$, on note souvent xy ou $x \times y$ pour $x * y$. L'inverse de x est souvent noté x^{-1}.
(4) Lorsque le groupe est abélien, la loi est souvent notée additivement, l'élément neutre 0 et l'inverse de x est donné par l'élément $-x$.

Exemple 1.1.2.3. On a $(\mathbf{Z}, +)$, $(\mathbf{Z}/n\,\mathbf{Z}, +)$ pour $n \in \mathbf{N}$, $(\mathfrak{S}_X, \circ)$ des permutations d'un ensemble X, $\mathsf{GL}(V)$ où V est un espace vectoriel, d'innombrables exemples en géométrie.

Définition 1.1.2.4. Comme pour toute « structure algébrique », on a les notions suivantes :
(i) un *morphisme* entre deux groupes $(G, *)$ et $(G', \bullet)$ est une application $f\colon G \to G'$ telle que :

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

(on a alors : $(\forall x \in G)\ f(x^{-1}) = f(x)^{-1}$ et $f(e_G) = e_{G'}$ est l'élément neutre) ;
(ii) un *sous-groupe* de G est une partie $H \subset G$ telle que l'inclusion soit un morphisme de groupes (on note alors $H \leqslant G$). On dit qu'un sous-groupe $H \leqslant G$ est *distingué* (ou *normal*) lorsque : $(\forall x \in G)\ xH = Hx$. C'est automatique lorsque G est abélien. On note alors $H \lhd G$;
(iii) le *noyau* (resp. l'*image*) d'un morphisme de groupes $f\colon G \to G'$ est $\mathsf{Ker}(f) = f^{-1}(e_{G'})$ (resp. $\mathsf{Im}(f) = f(G)$). C'est un sous-groupe distingué de G (resp. un sous-groupe de G').

Proposition 1.1.2.5. Soient G un groupe et $H \subset G$. L'ensemble H est un sous-groupe de G si et seulement si

$$H \neq \varnothing \text{ et } (x, y \in H \Rightarrow xy^{-1} \in H).$$

Démonstration. • Supposons $H \leqslant G$, alors $e \in H$, d'où $H \neq \varnothing$. Soit $x, y \in H$. Comme $y \in H$, alors $y^{-1} \in H$, donc $xy^{-1} \in H$.
• Supposons que $H \neq \varnothing$ et pour $x, y \in H$, $xy^{-1} \in H$. Il contient un élément x, donc $xx^{-1} = e \in H$. De plus, en appliquant notre hypothèse de départ, on obtient $ey^{-1} = y^{-1} \in H$. Enfin, $x(y^{-1})^{-1} = xy \in H$. Les axiomes de sous-groupes sont donc vérifiés et H est bien un sous-groupe de G. □

Exemple 1.1.2.6. Les sous-groupes de $\mathbf{Z}$ sont les parties de la forme $n\,\mathbf{Z}$ avec $n \in \mathbf{N}$.

Corollaire 1.1.2.7. Si G est un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de G, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Démonstration. Il est clair que $e \in H_i$ pour tout $i \in I$, donc $e \in \bigcap_{i \in I} H_i$. Soit $x, y \in \bigcap_{i \in I} H_i$. En particulier, $x, y \in H_i$ pour tout $i \in I$. Comme $H_i \leqslant G$, on a $xy^{-1} \in H_i$. C'est vrai pour tout $i \in I$, donc $xy^{-1} \in \bigcap_{i \in I} H_i$. □

Définition 1.1.2.8. Soit G un groupe et $X \subset G$ une partie. Le sous-groupe de G *engendré* par X est le plus petit sous-groupe de G qui contient X. Ce n'est autre que l'intersection de tous les sous-groupes de G qui contiennent X. On le note $\langle X \rangle$.

Si on pose $\mathscr{E} = \{H \leqslant G;\ X \subset H\}$, on a alors $\langle X \rangle = \bigcap_{H \in \mathscr{E}} H$.

Exemple 1.1.2.9. On a $\langle 2, 3 \rangle = \mathbf{Z}$ dans $(\mathbf{Z}, +)$ et $\langle (1,2), (1,2,3) \rangle = \mathfrak{S}_3$ dans $(\mathfrak{S}_3, \circ)$.

Définition 1.1.2.10. L'*ordre* d'un groupe G est son cardinal. Si $g \in G$, l'*ordre* de g est l'ordre du sous-groupe engendré $\langle g \rangle = \{g^n;\ n \in \mathbf{Z}\}$. C'est aussi le plus petit entier $n \in \mathbf{N}_{>0}$ tel que $g^n = e$, ou $+\infty$ si un tel entier n'existe pas.

Proposition 1.1.2.11. Soit $f\colon G \to G'$ un morphisme de groupes.
(i) L'image directe d'un sous-groupe de G est un sous-groupe de G'. En particulier, $\mathsf{Im}(f)$ est un sous-groupe de G'.
(ii) L'image réciproque $f^{-1}(H')$ d'un sous-groupe $H' \leqslant G'$ dans G est un sous-groupe de G. Il est distingué dans G lorsque H' est distingué dans G'.
(iii) L'application f est injective si et seulement si $\mathsf{Ker}(f) = \{e_G\}$.
(iv) Si f est bijective, alors l'application $f^{-1}\colon G' \to G$ est un morphisme de groupes (et f est un *isomorphisme* de groupes).

Démonstration. (i) Soit $H \leqslant G$. Posons $f(H) = \{f(x);\ x \in H\}$. Soient $y_1, y_2 \in f(H)$, il existe $x_1, x_2 \in H$ tel que $f(x_1) = y_1$ et $f(x_2) = y_2$. On a alors :

$$y_1 y_2^{-1} = f(x_1)f(x_2)^{-1} = f(x_1 x_2^{-1})$$

et $x_1 x_2^{-1} \in H$ puisque $H \leqslant G$. On en déduit donc que $y_1 y_2^{-1} \in f(H)$. Pour montrer que $\mathsf{Im}(f) \leqslant G'$, il suffit de poser $H = G$.
(ii) Soient $x_1, x_2 \in f^{-1}(H')$. On a alors $f(x_1), f(x_2) \in H'$ et comme $H' \leqslant G'$:

$$f(x_1)f(x_2)^{-1} = f(x_1 x_2^{-1}) \in H'$$

d'où $x_1 x_2^{-1} \in f^{-1}(H')$. Montrons maintenant que $f^{-1}(H') \lhd G$. Soit $h \in f^{-1}(H')$ et $g \in G$. On a $f(h) \in H'$ et

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1}$$

alors comme $H' \lhd G'$, on a $f(ghg^{-1}) \in H'$ *i.e.* $ghg^{-1} \in f^{-1}(H')$.
(iii) Supposons f injective. Si $x \in \mathsf{Ker}(f)$, alors $f(x) = e_{G'} = f(e_G)$, d'où $x = e_G$ et par suite, $\mathsf{Ker}(f) = \{e_G\}$. Réciproquement, supposons $\mathsf{Ker}(f) = \{e_G\}$. Soient $x, x' \in G$ tel que $f(x) = f(x')$. On a :

$$e_{G'} = f(x)^{-1}f(x') = f(x^{-1}x')$$

i.e. $x^{-1}x' \in \mathsf{Ker}(f)$. En outre,

$$\mathsf{Ker}(f) = \{e_G\} \Rightarrow x^{-1}x' = e_G \Leftrightarrow x = x'$$

d'où l'injectivité de f.
(iv) Par définition, f admet une application réciproque f^{-1}. Soient $y_1, y_2 \in G'$, posons $x = f^{-1}(y_1 y_2)$. On a donc $f(x) = y_1 y_2$. De plus, il existe $x_1, x_2 \in G$ uniques tel que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. Comme f est bijective, elle est injective, donc $x = x_1 x_2$. Or, $x_1 = f^{-1}(y_1)$ et $x_2 = f^{-1}(y_2)$, donc

$$f^{-1}(y_1 y_2) = f^{-1}(y_1)f^{-1}(y_2).$$

L'application $f^{-1}\colon G' \to G$ est donc un morphisme de groupes. □

Remarque 1.1.2.12. (1) Si $H \leqslant G$ est un sous-groupe distingué, l'image directe $f(H)$ n'est pas distinguée dans G' en général.
(2) On retrouve le fait que $\mathsf{Ker}(f) = f^{-1}(e_{G'})$ est un sous-groupe distingué de G.
(3) Lorsque H n'est pas distingué dans G, les relations d'équivalence (et donc les partitions) associées ne coïncident pas.

Définition 1.1.2.13. Les *automorphismes* d'un groupe G sont les isomorphismes de G dans lui-même. Ils forment un groupe pour la composition, qu'on note $\mathsf{Aut}(G)$.

On peut raffiner la proposition 1.1.2.11 de la façon suivante.

Proposition 1.1.2.14. Soit $f\colon G \to G'$ un morphisme de groupes. L'application $H \mapsto f(H)$ induit une bijection de l'ensemble des sous-groupes de G qui contiennent $\mathsf{Ker}(f)$ et l'ensemble des sous-groupes de $\mathsf{Im}(f)$ *i.e.*

$$\{H \leqslant G;\ \mathsf{Ker}(f) \subset H\} \xrightarrow{\sim} \{H' \leqslant G';\ H' \leqslant \mathsf{Im}(f)\}.$$

Démonstration. • D'après la proposition 1.1.2.11, l'application est bien définie. Si $H \leqslant G$ est un sous-groupe de G tel que $\mathsf{Ker}(f) \subset H$, on a bien sûr $H \subset f^{-1}(f(H))$. Si $g \in f^{-1}(f(H))$, on a $f(g) \in f(H)$: il existe $h \in H$ tel que $f(g) = f(h)$, *i.e.* $f(gh^{-1}) = e_{G'}$, soit $gh^{-1} \in \mathsf{Ker}(f) \subset H$ et donc $g \in hH = H$. Cela montre que $f^{-1}(f(H)) = H$.
• Si maintenant H' est un sous-groupe de $\mathsf{Im}(f)$, posons $H = f^{-1}(H')$: c'est un sous-groupe de G qui contient $\mathsf{Ker}(f)$. On a $f(H) \subset H'$. Réciproquement, si $\gamma \in H'$, il existe $g \in G$ tel que $\gamma = f(g)$ (parce que $H' \subset \mathsf{Im}(f)$) et comme $f(g) \in H'$, on a $g \in H$, de sorte que $\gamma \in f(H)$. Cela montre que $f(f^{-1}(H')) = H'$.
• On a donc montré que l'application $H \mapsto f(H)$ induit une bijection de l'ensemble des sous-groupes de G qui contiennent $\mathsf{Ker}(f)$ et l'ensemble des sous-groupes de $\mathsf{Im}(f)$. En particulier, on a donc montré que l'application réciproque est $H' \mapsto f^{-1}(H')$. □

1.1.3 Classes modulo un sous-groupe

Définition 1.1.3.1. Soient G un groupe et $H \leqslant G$ un sous-groupe. On définit une relation d'équivalence sur G en posant : $g_1 \mathcal{R}_H g_2 \Leftrightarrow g_1^{-1} g_2 \in H$. Les classes d'équivalence sont les *classes à gauche* modulo H : ce sont les parties de la forme gH. Elles forment une partition de G. On définit de façon analogue les *classes à droite*. On note G/H (resp. $H\backslash G$) l'ensemble des classes à gauche (resp. à droite).

Remarque 1.1.3.2. (1) Dans la pratique, on note $\overline{g}$ la classe gH, lorsque cela ne prête pas à confusion.
(2) Si G est un groupe et H un sous-groupe de G, on a l'équivalence « $g_1 H = g_2 H \Leftrightarrow H g_1^{-1} = H g_2^{-1}$ », pour tous $g_1, g_2 \in G$. Cela implique que l'application $gH \mapsto Hg^{-1}$ induit une bijection de l'ensemble G/H sur $H\backslash G$.

Définition 1.1.3.3. Soient G un groupe et $H \leqslant G$ un sous-groupe. L'*indice* de H dans G est le cardinal de l'ensemble quotient G/H (et donc aussi celui de $H\backslash G$ en vertu de la remarque qui précède). On le note $(G : H) \in \mathbf{N} \cup \{\infty\}$.

Théorème 1.1.3.4 (Lagrange)**.** Si G est un groupe fini et H un sous-groupe de G, alors

$$\#G = (G : H)\#H.$$

On a donc $\#H \mid \#G$. En particulier, l'ordre d'un élément $g \in G$ divise $\#G$.

Démonstration. Les classes à gauche modulo H forment une partition : $G = \bigsqcup_{g \in T} gH$ (où T est un système complet de représentants de G/H). Comme $\#gH = \#H$ pour tout $g \in T$, on a $\#G = \#T\#H = (G : H)\#H$ (puisqu'on a une bijection $T \xrightarrow{\sim} G/H$ et donc $\#T = \#G/H = (G : H)$). La dernière assertion correspond au cas $H = \langle g \rangle$. □

Remarque 1.1.3.5. Il faut prendre garde que le théorème de Lagrange ne dit pas que réciproquement, si d est un diviseur de $\#G$, alors G contient un sous-groupe ou un élément d'ordre d. Par exemple, le groupe alterné $\mathfrak{A}_4$ est d'ordre 12, mais ne contient pas de sous-groupe d'ordre 6. Cela dit, on verra plus loin des réciproques partielles : le théorème de Cauchy et les théorèmes de Sylow.

Proposition 1.1.3.6. Soit G un groupe. Les relations d'équivalence sur G qui sont compatibles avec la loi de groupe sont les relations modulo un sous-groupe distingué.

Démonstration. Soit $\mathcal{R}$ une relation d'équivalence sur G. Notons H la classe d'équivalence de l'élément neutre et $\pi \colon G \to G/\mathcal{R}$ la surjection canonique. Supposons $\mathcal{R}$ compatible à la loi de groupe : cela implique que si $x_1, x_2 \in G$, la classe $[x_1 x_2]$ ne dépend que des classes $[x_1]$ et $[x_2]$, donc pas des représentants x_1 et x_2. On peut donc poser $[x_1] \cdot [x_2] = [x_1 x_2]$. Cela munit l'ensemble quotient d'une loi de composition interne et les axiomes de groupe « passent au quotient » : c'est une loi de groupe sur $G/\mathcal{R}$. En outre, l'égalité $[x_1] \cdot [x_2] = [x_1 x_2]$ peut s'écrire $\pi(x_1) \cdot \pi(x_2) = \pi(x_1 x_2)$: la surjection canonique est un morphisme de groupes. Cela implique que $H = \mathsf{Ker}(\pi)$ est un sous-groupe distingué de G. Si $g_1, g_2 \in G$, on a alors

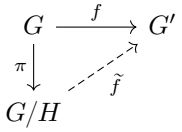
$$g_1 \mathcal{R} g_2 \Leftrightarrow \pi(g_1) = \pi(g_2) \Leftrightarrow g_1^{-1} g_2 \in \mathsf{Ker}(\pi) = H$$

ce qui montre que $\mathcal{R}$ coïncide avec la relation modulo H (à gauche ou à droite, c'est la même chose). □

Ce qui précède montre en particulier que si H est distingué dans G, l'ensemble quotient G/H est naturellement muni d'une structure de groupe. La loi de groupe est la suivante : si $g_1, g_2 \in G$, on a $(g_1 H)(g_2 H) = g_1 g_2 H$ et $(gH)^{-1} = g^{-1} H$ (l'élément neutre est la classe « triviale » $eH = H$).

Exemple 1.1.3.7. Si $n \in \mathbf{N}$, on dispose du groupe quotient $\mathbf{Z}/n\mathbf{Z}$.

Corollaire 1.1.3.8 (Propriété universelle : Cas des groupes)**.** Soient $f \colon G \to G'$ un morphisme de groupes et $H \leqslant G$ un sous-groupe distingué tel que $H \subset \mathsf{Ker}(f)$. Il existe alors un morphisme de groupes $\widetilde{f} \colon G/H \to G'$ unique tel que $f = \widetilde{f} \circ \pi$, où $\pi \colon G \to G/H$ est la surjection canonique.



Démonstration. C'est un cas particulier de la proposition 1.1.1.5. □

Exemple 1.1.3.9. (1) Si $f\colon G \to G'$ est un morphisme de groupes, alors f induit un isomorphisme :

$$G/\operatorname{Ker}(f) \xrightarrow{\sim} \operatorname{Im}(f).$$

Lorsque G est fini, cela implique en particulier que $(G : \operatorname{Ker}(f)) = \#\operatorname{Im}(f)$ et donc $\#G = \#\operatorname{Ker}(f)\#\operatorname{Im}(f)$, égalité qui n'est pas sans rappeler le théorème du rang.
(2) Rappelons que le *centre* d'un groupe G est le sous-groupe

$$\mathsf{Z}(G) = \{g \in G;\ (\forall x \in G)\ gx = xg\}.$$

Si $g \in G$, posons :

$$\begin{aligned} \varphi_g\colon G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$$

On a $\varphi_e = \mathsf{Id}_G$ et $\varphi_{g_1g_2} = \varphi_{g_1} \circ \varphi_{g_2}$ pour tous $g_1, g_2 \in G$. Cela implique que $\varphi_g \in \operatorname{Aut}(G)$ et $\varphi_g^{-1} = \varphi_{g^{-1}}$ pour tout $g \in G$. En outre, l'application $\varphi\colon G \to \operatorname{Aut}(G)$ est un morphisme de groupes. Par définition, on a $\mathsf{Z}(G) = \operatorname{Ker}(\varphi)$. En passant au quotient, le morphisme φ induit un morphisme de groupes injectif

$$G/\mathsf{Z}(G) \hookrightarrow \operatorname{Aut}(G).$$

On note $\operatorname{Int}(G)$ son image : ses éléments s'appellent les *automorphismes intérieurs* de G. On a alors un isomorphisme

$$G/\mathsf{Z}(G) \xrightarrow{\sim} \operatorname{Int}(G).$$

En général, l'inclusion $\operatorname{Int}(G) \subset \operatorname{Aut}(G)$ est stricte.

Théorème 1.1.3.10 (D'ISOMORPHISME)**.** Soit G un groupe.
(i) Si $H \leqslant G$ et $N \lhd G$, alors $HN = \{hn\}_{\substack{h\in H\\ n\in N}}$ est un sous-groupe de G. De plus, $N \cap H \lhd H$ et on a un isomorphisme :

$$H/(N \cap H) \xrightarrow{\sim} HN/N.$$

(ii) Soient H et K deux sous-groupes distingués de G. Si $K \leqslant H$, alors $H/K \lhd G/K$ et on a un isomorphisme :

$$(G/K)/(H/K) \xrightarrow{\sim} G/H.$$

Démonstration. (i) On a $HN \neq \varnothing$ puisque $e \in HN$. Pour $g_1, g_2 \in HN$, écrivons $g_1 = h_1n_1$ et $g_2 = h_2n_2$ avec $h_1, h_2 \in H$ et $n_1, n_2 \in N$. On a alors

$$\begin{aligned} g_1g_2^{-1} &= h_1n_1(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1(h_2^{-1}h_2)n_1n_2^{-1}h_2^{-1} \\ &= (h_1h_2^{-1})(h_2n_1n_2^{-1}h_2^{-1}) \in HN \end{aligned}$$

puisque $n_1n_2^{-1} \in N$, donc $h_2(n_1n_2^{-1})h_2^{-1} \in N$ vu que $N \lhd G$, ce qui prouve que HN est un sous-groupe de G. Il est clair que $H \leqslant HN$ et $N \leqslant HN$ et comme $N \lhd G$, alors $N \lhd HN$. On dispose de l'inclusion $i\colon H \to HN$ et de la surjection canonique $\pi\colon HN \to HN/N$. Le composé $\pi \circ i$ est surjectif : si $h \in H$ et $n \in N$, on a $(hn)N = hN = \pi(i(h))$. Par ailleurs, on a $\operatorname{Ker}(\pi \circ i) = \{h \in H;\ \pi(i(h)) = N\} = \{h \in H;\ hN = N\}$. Finalement, on a $\operatorname{Ker}(\pi \circ i) = \{h \in H;\ h \in N\} = N \cap H$ et par définition du noyau, $N \cap H \lhd H$. En passant au quotient, le morphisme $\pi \circ i$ induit un isomorphisme $H/(N \cap H) \xrightarrow{\sim} HN/N$.
(ii) Comme $K \leqslant H$, la surjection canonique $\pi_H\colon G \to G/H$ se factorise en un morphisme surjectif $\pi_{H,K}\colon G/K \to G/H$. On a $\operatorname{Ker}(\pi_{H,K}) = H/K$, ce qui montre que $H/K \lhd G/K$ et en passant au quotient, $\pi_{H,K}$ induit un isomorphisme $(G/K)/(H/K) \xrightarrow{\sim} G/H$. □

Proposition 1.1.3.11. Soit $n \in \mathbf{N}_{>0}$. Pour tout diviseur d de n, il existe un seul sous-groupe d'ordre d dans $\mathbf{Z}/n\mathbf{Z}$: c'est le sous-groupe engendré par $\frac{n}{d}$.

Démonstration. On dispose de la surjection canonique $\pi\colon \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. Les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont précisément les parties de la forme $\pi(H)$ où H est un sous-groupe de $\mathbf{Z}$ contenant $\operatorname{Ker}(\pi) = n\mathbf{Z}$ (*cf.* proposition 1.1.2.14), *i.e.* de la forme $m\mathbf{Z}$ avec $m \mid n$. Le groupe $\pi(m\mathbf{Z}) = m\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/(n/m)\mathbf{Z}$ est d'ordre $d = \frac{n}{m}$. □

1.2 Le groupe symétrique

1.2.1 Généralités, décomposition en produit de cycles à supports disjoints

Définition 1.2.1.1. Si E est un ensemble, on note $\mathfrak{S}_E$ l'ensemble des *permutations* de E *i.e.* des bijections de E dans lui-même. C'est un groupe pour la composition. Si $n \in \mathbf{N}_{>0}$, on note $\mathfrak{S}_n$ le *groupe des permutations* de $\{1, \dots, n\}$.

Remarque 1.2.1.2. Une bijection $f\colon E \to E'$ induit l'isomorphisme :

$$\begin{aligned} \mathfrak{S}_E &\xrightarrow{\sim} \mathfrak{S}_{E'} \\ \sigma &\mapsto f \circ \sigma \circ f^{-1} \end{aligned}$$

En particulier, si E est un ensemble de cardinal $n \in \mathbf{N}_{>0}$, le choix d'une numérotation des éléments de E fournit un isomorphisme $\mathfrak{S}_E \xrightarrow{\sim} \mathfrak{S}_n$. Pour cette raison, on va se concentrer sur l'étude de $\mathfrak{S}_n$ dans ce qui suit.

Soit $n \in \mathbf{N}_{>0}$.

Proposition 1.2.1.3. On a $\#\mathfrak{S}_n = n!$.

Démonstration. Il est clair que le nombre de permutations d'un ensemble à n éléments est $n!$. □

Définition 1.2.1.4. (i) Si $\sigma \in \mathfrak{S}_n$, on note :

$$\mathsf{Fix}(\sigma) = \{i \in \{1, \dots, n\};\ \sigma(i) = i\}$$

l'ensemble des points fixes. L'ensemble $\mathsf{supp}(\sigma) := \{1, \dots, n\} \setminus \mathsf{Fix}(\sigma)$ s'appelle le *support* de σ.
(ii) Soient $\ell \in \mathbf{N}_{>1}$ et $i_1, \dots, i_\ell$ des éléments distincts de $\{1, \dots, n\}$. On note $(i_1, \dots, i_\ell)$ l'élément de $\mathfrak{S}_n$ qui envoi i_ℓ sur i_1, i_k sur i_{k+1} pour tout $k \in \{1, \dots, \ell-1\}$ et laisse fixe tous les éléments de $\{1, \dots, n\} \setminus \{i_1, \dots, i_\ell\}$ (on a donc $\mathsf{supp}(i_1, \dots, i_\ell) = \{i_1, \dots, i_\ell\}$). Une permutation de ce type est appelés *cycle* de longueur ℓ ou ℓ-cycle. Un 2-cycle s'appelle une *transposition*.

Remarque 1.2.1.5. (1) Un ℓ-cycle est d'ordre ℓ.
(2) Il y a $\frac{n(n-1)\cdots(n-\ell+1)}{\ell} = \binom{n}{\ell}(\ell-1)!$ cycles de longueur ℓ.
(3) On a $(i_1, i_2, \dots, i_\ell) = (i_2, \dots, i_\ell, i_1)$: un ℓ-cycle admet ℓ écritures comme ci-dessus, qui s'obtiennent les unes des autres par permutation circulaire des indices.

Lemme 1.2.1.6. Soient $\sigma_1, \sigma_2 \in \mathfrak{S}_n$. On a $\mathsf{supp}(\sigma_1\sigma_2) \subset \mathsf{supp}(\sigma_1) \cup \mathsf{supp}(\sigma_2)$. Si en outre on a $\mathsf{supp}(\sigma_1) \cap \mathsf{supp}(\sigma_2) = \varnothing$, alors $\mathsf{supp}(\sigma_1\sigma_2) = \mathsf{supp}(\sigma_1) \cup \mathsf{supp}(\sigma_2)$, les permutations σ_1 et σ_2 commutent et on a l'implication : « $\sigma_1\sigma_2 = \mathsf{Id} \Rightarrow \sigma_1 = \sigma_2 = \mathsf{Id}$ ».

Démonstration. Soit σ_1 une permutation de support S_1 et σ_2 une permutation de support S_2, telle que $S_1 \cap S_2 = \varnothing$. Montrons que $\sigma_1\sigma_2 = \sigma_2\sigma_1$. On peut distinguer trois cas :
• Si $i \notin S_1 \cup S_2$, alors $\sigma_1\sigma_2(i) = i$ et de même $\sigma_2\sigma_1(i) = i$.
• Si $i \in S_1$, alors $i \notin S_2$, donc $\sigma_1\sigma_2(i) = \sigma_1(i)$. De plus, $\sigma_1(i) \in S_1$, donc $\sigma_1(i) \notin S_2$ et $\sigma_2(\sigma_1(i)) = \sigma_1(i)$.
• Si $i \in S_2$, le cas est analogue au précédent. □

Théorème 1.2.1.7. Soit $\sigma \in \mathfrak{S}_n$. Il existe $c_1, \dots, c_r \in \mathfrak{S}_n$ des cycles à supports deux à deux disjoints tel que $\sigma = c_1 \cdots c_r$. Une telle décomposition est unique à l'ordre des facteurs près.

Démonstration. Existence : On munit $\{1, \dots, n\}$ de la relation d'équivalence définie par

$$i \sim j \Leftrightarrow (\exists m \in \mathbf{Z})\ j = \sigma^m(i).$$

Soient $A_1, \dots, A_r$ les classes d'équivalence associées, on a alors : $\{1, \dots, n\} = \bigsqcup_{k=1}^{r} A_k$. Pour $k \in \{1, \dots, r\}$, on pose

$$c_k(i) = \begin{cases} i & \text{si } i \notin A_k \\ \sigma(i) & \text{si } i \in A_k \end{cases}$$

Si $i_1 \in A_k$, alors $A_k = \{\sigma^m(i_1)\}_{0 \leqslant m \leqslant \ell_k}$ où $\ell_k = \#A_k = \min\{m \in \mathbf{N}_{>0} \mid \sigma^m(i_1) = i_1\}$ et

$$c_k = (i_1, \sigma(i_1), \dots, \sigma^{\ell_k - 1}(i_1))$$

est un ℓ_k-cycle tel que $\mathsf{supp}(c_k) = A_k$. Cela implique déjà que $c_1, \dots, c_r$ commutent deux à deux (en vertu du lemme précédent). Par construction, on a $\sigma = c_1 \cdots c_r$ (vérification sur chaque A_k pour $1 \leqslant k \leqslant r$).
Unicité : Soient $c_1, \dots, c_r$ (resp. $\gamma_1, \dots, \gamma_s$) des cycles à supports deux à deux disjoints, tels que $\sigma = c_1 \cdots c_r =$

$\gamma_1 \cdots \gamma_s$. Montrons par récurrence sur r que $r = s$ et qu'à permutation des facteurs près, on a $c_k = \gamma_k$ pour tout $k \in \{1, \ldots, r\}$. Si $r = 0$, on a

$$\varnothing = \mathsf{supp}(\gamma_1 \cdots \gamma_s) = \bigsqcup_{k=1}^{s} \mathsf{supp}(\gamma_k)$$

(en vertu du lemme qui précède) et donc $s = 0$. Supposons $r > 0$ et soit $i_1 \in \mathsf{supp}(c_r)$: on a $\sigma(i_1) \neq i_1$: il existe $k \in \{1, \ldots, s\}$ tel que $i_1 \in \mathsf{supp}(\gamma_k)$. Quitte à renuméroter, on peut supposer que $i_1 \in \mathsf{supp}(\gamma_s)$. On a alors $\mathsf{supp}(c_r) = \{\sigma^m(i_1)\}_{m \in \mathbf{Z}} = \mathsf{supp}(\gamma_s)$ et pour tout $i \in \mathsf{supp}(c_r)$, on a $c_r(i) = \sigma(i) = \gamma_s(i)$, ce qui montre que $c_r = \gamma_s$. L'égalité $c_1 \cdots c_r = \gamma_1 \cdots \gamma_s$ implique alors $c_1 \cdots c_{r-1} = \gamma_1 \cdots \gamma_{s-1}$. L'hypothèse de récurrence s'applique : on a $r - 1 = s - 1$ (d'où $r = s$) et quitte à renuméroter, $c_k = \gamma_k$ pour tout $k \in \{1, \ldots, r-1\}$, ce qui achève la preuve. □

Remarque 1.2.1.8. (1) On a l'équivalence : « $r = 0 \Leftrightarrow \sigma = \mathsf{Id}$ ».
(2) Les supports des cycles $c_1, \ldots, c_r$ ne sont rien d'autres que les orbites non ponctuelles de l'action du groupe $\langle \sigma \rangle$ sur $\{1, \ldots, n\}$ (*cf.* plus bas).

Corollaire 1.2.1.9. Le groupe $\mathfrak{S}_n$ admet les parties génératrices suivantes :
(i) les transpositions ;
(ii) $\{(1, i)\}_{2 \leqslant i \leqslant n}$;
(iii) $\{(i, i+1)\}_{1 \leqslant i \leqslant n-1}$;
(iv) $\{(1, 2), (1, \ldots, n)\}$.

Démonstration. (i) On a $(i_1, i_2, \ldots, i_\ell) = (i_1, i_2)(i_2, i_3) \cdots (i_{\ell-1}, i_\ell)$: comme les cycles engendrent $\mathfrak{S}_n$, il en est de même des transpositions.
(ii) Si $i, j \in \{2, \ldots, n\}$ sont distincts, on a $(1, j)(1, i)(1, j) = (i, j)$: le point précédent permet de conclure.
(iii) Si $2 \leqslant i \leqslant n-1$, on a $(i, i+1)(1, i)(i, i+1) = (1, i+1)$: une récurrence immédiate montre que pour tout $i \in \{2, \ldots, n\}$, la transposition $(1, i)$ appartient au sous-groupe engendré par $\{(k, k+1)\}_{1 \leqslant k \leqslant n-1}$ et le point précédent permet de conclure.
(iv) Pour tout $i \in \{1, \ldots, n-1\}$, on a $(i, i+1) = (1, 2, \ldots, n)^{i-1}(1, 2)(1, 2, \ldots, n)^{1-i}$ et le point précédent permet de conclure. □

Définition 1.2.1.10. (i) Le *type* de $\sigma \in \mathfrak{S}_n$ est la suite $\underline{\ell} = (\ell_1, \ldots, \ell_r)$ (ordonné dans l'ordre décroissant) des longueurs des cycles apparaissant dans la décomposition de σ en produit de cycles à support disjoints, auxquelles on adjoint une suite de 1 correspondant aux points fixes. C'est une partition de n (*i.e.* $\ell_1 + \cdots + \ell_r = n$).
(ii) L'ensemble des partitions de n est en bijection avec les *diagrammes de Young* : un diagramme de Young est une collection finie de cases, organisée en lignes justifiées à gauche et telle que les longueurs des lignes décroissent au sens large.
(iii) Un *tableau de Young* est un diagramme de Young rempli avec les entiers de 1 à n. Un tel tableau correspond à une décomposition d'un élément de $\mathfrak{S}_n$ en produit de cycles à supports disjoints. Un *tableau de Young standard* (de type $\underline{\ell}$) est celui dont les cases sont remplies dans l'ordre.

Par exemple, le diagramme de Young associé à la partition $(4, 3, 1)$ de l'entier 8 est  .

Lemme 1.2.1.11. Soient $c = (i_1, \ldots, i_\ell)$ un cycle de longueur ℓ et $\sigma \in \mathfrak{S}_n$. On a :

$$\sigma c \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_\ell)).$$

Démonstration. Pour $\sigma(i_1, \ldots, i_\ell)\sigma^{-1}$, notons $S = \{i_1, \ldots, i_\ell\}$. On a :

$$\sigma(i) \xrightarrow{\sigma^{-1}} i \xrightarrow{(i_1, \ldots, i_\ell)} \begin{cases} i & \text{si } i \notin S \\ i_{k+1} & \text{si } i = i_k \end{cases} \xrightarrow{\sigma} \begin{cases} \sigma(i) & \text{si } i \notin S \\ \sigma(i_{k+1}) & \text{si } i = i_k \end{cases}$$

□

Cela montre que $\mathfrak{S}_n$ agit transitivement par conjugaison sur l'ensemble des ℓ-cycles. Plus généralement :

Théorème 1.2.1.12. Deux éléments de $\mathfrak{S}_n$ sont conjugués dans $\mathfrak{S}_n$ si et seulement s'ils ont même type.

Démonstration. • Si $\gamma, \sigma \in \mathfrak{S}_n$, soit $\sigma = c_1 \cdots c_r$ une décomposition de σ en produit de cycles à supports disjoints, alors $\gamma\sigma\gamma^{-1} = (\gamma c_1 \gamma^{-1}) \cdots (\gamma c_r \gamma^{-1})$ est une décomposition de $\gamma\sigma\gamma^{-1}$ en produit de cycles à supports disjoints : sont type est le même que celui de σ.
• Pour montrer la réciproque, il suffit de montrer que toute permutation σ de type $\underline{\ell} = (\ell_1, \ldots, \ell_r)$ est conjuguée à la permutation σ_0 associée au tableau de Young standard de type $\underline{\ell}$. □

Remarque 1.2.1.13. Cela montre en particulier que les classes de conjugaison dans $\mathfrak{S}_n$ sont en bijection avec les partitions de l'entier n, soit encore avec les diagrammes de Young.

Théorème 1.2.1.14. Si $n \geqslant 3$, le centre de $\mathfrak{S}_n$ est trivial.

Démonstration. Soit $\sigma \in \mathsf{Z}(\mathfrak{S}_n)$. Si $i, j \in \{1, \dots, n\}$ sont distincts, $\sigma(i,j)\sigma^{-1} = (\sigma(i), \sigma(j))$ mais comme $\sigma \in \mathsf{Z}(\mathfrak{S}_n)$, alors $\sigma(i,j)\sigma^{-1} = (i,j)$, donc $\{\sigma(i), \sigma(j)\} = \{i,j\}$. Comme $n \geqslant 3$, il existe $k \in \{1, \dots, n\} \backslash \{i,j\}$. De même, $\sigma(i) \in \{i,k\}$, donc $\sigma(i) \in \{i,j\} \cap \{i,k\} = \{i\}$ *i.e.* $\sigma(i) = i$, d'où $\sigma = \mathsf{Id}_{\{1,\dots,n\}}$. □

Exercice 1.2.1.15. Montrer que $\mathfrak{S}_9$ contient un élément d'ordre 20, mais pas d'élément d'ordre 18.

Solution : L'élément $(1,2,3,4,5)(6,7,8,9) \in \mathfrak{S}_9$ est d'ordre $5 \times 4 = 20$. Supposons que $\mathfrak{S}_9$ contienne un élément σ d'ordre $18 = 2 \times 3^2$. Cela implique que la décomposition de σ en produit de cycles disjoints fait intervenir au moins une transposition et un 9-cycle, donc que σ a un support de cardinal au moins 11, ce qui est impossible.

1.2.2 Signature et groupe alterné

Définition 1.2.2.1. Si $\sigma \in \mathfrak{S}_n$, on pose $\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$ que l'on appelle la *signature* d'une permutation σ.

Remarque 1.2.2.2. Un élément $\sigma \in \mathfrak{S}_n$ permute les parties à 2 éléments de $\{1, \dots, n\}$. Cela implique que $\varepsilon(\sigma) \in \{\pm 1\}$.

Lemme 1.2.2.3. Si $c \in \mathfrak{S}_n$ est un ℓ-cycle, on a $\varepsilon(c) = (-1)^{\ell - 1}$. En particulier, on a $\varepsilon(\tau) = -1$ pour toute transposition $\tau \in \mathfrak{S}_n$.

Démonstration. Quitte à renuméroter, on peut supposer que $c = (1, \dots, \ell)$. On a alors

$$\begin{aligned} \varepsilon(c) &= \left(\prod_{1 \leqslant i < j \leqslant \ell} \frac{c(j) - c(i)}{j - i} \right) \left(\prod_{j=\ell+1}^{n} \prod_{i=1}^{\ell} \frac{j - c(i)}{j - i} \right) \\ &= \left(\prod_{i=1}^{\ell-1} \frac{1 - (i+1)}{\ell - i} \right) \prod_{j=\ell+1}^{n} \left(\frac{j-1}{j-\ell} \prod_{i=1}^{\ell-1} \frac{j - (i+1)}{j - i} \right) = (-1)^{\ell - 1} \end{aligned}$$

puisque $\frac{j-1}{j-\ell} \prod_{i=1}^{\ell-1} \frac{j-(i+1)}{j-i} = 1$. □

Théorème 1.2.2.4. L'application ε définit un morphisme de groupes $\varepsilon \colon \mathfrak{S}_n \to \{\pm 1\}$. Il est surjectif lorsque $n \geqslant 2$.

Démonstration. Pour $\sigma, \gamma \in \mathfrak{S}_n$, on a :

$$\begin{aligned} \varepsilon(\sigma\gamma) &= \prod_{i,j} \frac{\sigma\gamma(i) - \sigma\gamma(j)}{i - j} = \prod_{i,j} \frac{\sigma\gamma(i) - \sigma\gamma(j)}{\gamma(i) - \gamma(j)} \prod_{i,j} \frac{\gamma(i) - \gamma(j)}{i - j} \\ &= \prod_{i,j} \frac{\sigma(i) - \sigma(j)}{i - j} \prod_{i,j} \frac{\gamma(i) - \gamma(j)}{i - j} = \varepsilon(\sigma)\varepsilon(\gamma). \end{aligned}$$

On a bien sûr $\varepsilon(\mathsf{Id}) = 1$: cela montre que ε induit un morphisme de groupes $\mathfrak{S}_n \to \{\pm 1\}$. La surjectivité est claire par cardinalité. □

Définition 1.2.2.5. Le *groupe alterné* est $\mathfrak{A}_n = \mathsf{Ker}(\varepsilon)$. Il est distingué dans $\mathfrak{S}_n$, d'indice 2 lorsque $n \geqslant 2$.

Proposition 1.2.2.6. Le groupe $\mathfrak{A}_n$ admet les parties génératrices suivantes :
(i) $\{(1,i)(1,j)\}_{2 \leqslant i < j \leqslant n}$;
(ii) $\{(1,2,i)\}_{3 \leqslant i \leqslant n}$;
(iii) $\{\sigma^2\}_{\sigma \in \mathfrak{S}_n}$.

Démonstration. (i) Comme $\mathfrak{S}_n$ est engendré par les transpositions de la forme $(1,i)$, tout élément de $\mathfrak{A}_n$ peut s'écrire comme un produit d'un nombre pair de telles transpositions, ce qui conclut.
(ii) Si $i > 2$, on a $(1,2,i) = (1,i)(1,2)$. Si $j > 2$ et $i \neq j$, on a $(1,2,j)^{-1}(1,2,i)(1,2,j) = (1,i,j) = (1,j)(1,i)$. Le point précédent montre que la famille $\{(1,2,i)\}_{3 \leqslant i \leqslant n}$ est génératrice.
(iii) Pour tout $i \in \{3, \dots, n\}$, on a $(1,2,i) = (1,i,2)^2$: comme $\{(1,2,i)\}_{3 \leqslant i \leqslant n}$ engendre $\mathfrak{A}_n$, il en est de même de $\{\sigma^2\}_{\sigma \in \mathfrak{S}_n}$. □

Remarque 1.2.2.7. Les classes de conjugaison de $\mathfrak{A}_n$ sont un peu plus compliquées que celles de $\mathfrak{S}_n$. Si deux permutations paires sont conjuguées dans $\mathfrak{A}_n$, alors elles le sont à fortiori dans $\mathfrak{S}_n$: elles ont même type. Par contre, deux permutations paires de même type peuvent ne pas être conjuguées dans $\mathfrak{A}_n$. Plus précisément, les classes de conjugaison de permutations paires de $\mathfrak{S}_n$ peuvent être réunion d'une ou deux classes de conjugaison de $\mathfrak{A}_n$. Observons que pour les permutations ayant au moins deux points fixes, tout se passe « bien » : on peut conjuguer par une transposition pour avoir une conjugaison dans $\mathfrak{A}_n$. À titre d'exemple, décrivons les classes de conjugaison de $\mathfrak{A}_5$. On a $\#\mathfrak{A}_5 = 60$. Les types des éléments de $\mathfrak{S}_5$ sont les suivants (ceux de $\mathfrak{A}_5$ sont en bleue) :

- $(1,1,1,1,1)$ (classe de Id), elle a 1 élément ;
- $(2,1,1,1)$ (classe d'une transposition), elle a $\binom{5}{2} = 10$ éléments ;
- $(2,2,1)$ (classe d'une double transposition), elle a $\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$ éléments ;
- $(3,1,1)$ (classe d'un 3-cycle), elle a $\frac{5 \times 4 \times 3}{3} = 20$ éléments ;

- $(3,2)$, elle a 20 éléments ;
- $(4,1)$ (classe d'un 4-cycle), elle a $\frac{5\times4\times3\times2}{4} = 30$ éléments ;
- (5) (classe d'un 5-cycle), elle a $\frac{5!}{5} = 4! = 24$ éléments.

Les 5-cycles forment deux classes de conjugaison dans $\mathfrak{A}_5$, chacune de cardinal 12 (s'en convaincre en utilisant le fait que 24 ne divise pas 60).

Définition 1.2.2.8. Un groupe G est dit *simple* lorsque ses seuls sous-groupes distingués sont $\{e\}$ et G.

Théorème 1.2.2.9. Si $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple.

Remarque 1.2.2.10. (1) On peut montrer que G est simple abélien si et seulement si G est cyclique d'ordre premier (pour cela, il suffit de penser au groupe $(\mathbf{Z}/p\,\mathbf{Z})$).
(2) Si G est simple et $f\colon G \to G'$ est un morphisme de groupes, alors f est soit injective, soit triviale.

Démonstration. Soit $N \lhd \mathfrak{A}_n$ avec $N \neq \{\mathsf{Id}\}$. On sait que les 3-cycles sont conjugués dans $\mathfrak{A}_n$. Si N contient un 3-cycles, alors il les contient forcément tous, donc $N = \mathfrak{A}_n$ (puisque les 3-cycles engendrent $\mathfrak{A}_n$). Il s'agit donc tout au long de cette preuve de montrer que N contient un 3-cycle. Remarquons d'abord que N est clairement réunion de classe de conjugaison.
• Commençons par le cas $n = 5$. Supposons que N ne contient pas de 3-cycle. Il est clair que $(\mathfrak{A}_5 : N) \geqslant 2$ (sinon, $\mathfrak{A}_5 = N$ et on a une contradiction avec notre hypothèse). On a alors $\#N \leqslant \frac{60}{2} = 30$. D'une part, on a $\mathsf{Id} \in N$. D'autre part, N contient au moins une classe non triviale, donc $\#N \geqslant 1 + 12 > 12$. En outre, $(\mathfrak{A}_5 : N) < \frac{60}{12} = 5$, donc $(\mathfrak{A}_5 : N) = \{2,3,4\}$ *i.e.* $\#N \in \{15,20,30\}$. Si $\#N = 15$, alors $15 - 1 = 14$ devrait s'écrire comme somme d'entiers pris dans la liste $(12,12,15)$, ce qui n'est pas possible. On retrouve cette même impossibilité pour $20 - 1 = 19$ et $30 - 1 = 29$. On a alors une contradiction. Finalement, N contient un 3-cycle et par suite, $N = \mathfrak{A}_5$.
• Revenons maintenant au cas général. Soit $N \neq \{\mathsf{Id}\}$ un sous-groupe distingué de $\mathfrak{A}_n$ ne contenant pas de 3-cycle. On peut choisir $\sigma \in N\backslash\{\mathsf{Id}\}$. Il existe alors $a \in \{1,\dots,n\}$ tel que $b = \sigma(a) \neq a$. On choisit également $c \in \{1,\dots,n\}$ tel que $c \notin \{a, b, \sigma(b)\}$. Posons $\gamma = (a,c,b) \in \mathfrak{A}_n$. Considérons maintenant $\rho = \gamma\sigma\gamma^{-1}\sigma^{-1} = (\gamma\sigma\gamma^{-1})\sigma^{-1} \in N$ car $N \lhd \mathfrak{A}_n$. Mais on a également $\rho = \gamma(\sigma\gamma^{-1}\sigma^{-1}) = (a,c,b)(\sigma(a),\sigma(b),\sigma(c))$ puisque $\gamma^{-1} = (a,b,c)$. On a alors $\rho = (a,c,b)(b,\sigma(b),\sigma(c))$, donc $\mathsf{supp}(\rho) \subset \{a,b,c,\sigma(b),\sigma(c)\}$. En particulier, il existe $X \subset \{1,\dots,n\}$ tel que $\#X = 5$ et $\mathsf{supp}(\rho) \subset X$. Posons $A(X) = \{g \in \mathfrak{A}_n \mid \mathsf{supp}(g) \subset X\}$. On dispose de l'isomorphisme de groupes $A(X) \xrightarrow{\sim} \mathfrak{A}_X \simeq \mathfrak{A}_5$ qui à $g \in A(X)$ associe $g_{|X} \in \mathfrak{A}_X$ (donc l'application est bien définie). On peut remarquer que sa réciproque envoie un élément de $\mathfrak{A}_X$ vers $g(i)$ si $i \in X$ et i sinon. Il est donc clair que $A(X)$ est simple. Considérons maintenant $A(X) \cap N \leqslant \mathfrak{A}_n$. Si $g \in A(X) \cap N$ et $\gamma \in A(X)$, alors $\gamma g\gamma^{-1} \in A(X)$ et de même $\gamma g\gamma^{-1} \in N$, donc $A(X) \cap N \lhd A(X)$. On a $\rho \in A(X) \cap N$. Si on avait $\rho = \mathsf{Id}$, alors $\rho(b) = b$ *i.e.* $[(a,c,b)(b,\sigma(b),\sigma(c))](b) = b$ *i.e.* $(b,\sigma(b),\sigma(c))(b) = (a,b,c)(b)$. Mais comme $(b,\sigma(b),\sigma(c))(b) = \sigma(b)$ et $(a,b,c)(b) = c$ et que par hypothèse, $c \notin \{a,b,\sigma(b)\}$, on a donc que $\rho \in A(X) \cap N\backslash\{\mathsf{Id}\}$. Par simplicité de $A(X)$, on a $A(X) \cap N = A(X) \simeq \mathfrak{A}_5$. On en conclut que N contient un 3-cycle et $N = \mathfrak{A}_n$. □

Remarque 1.2.2.11. Les groupes $\mathfrak{A}_2$ et $\mathfrak{A}_3$ sont simples, mais pas $\mathfrak{A}_4$, qui contient le *groupe de Klein* des doubles transpositions.

Corollaire 1.2.2.12. Si $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathsf{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

Démonstration. Supposons que $G \lhd \mathfrak{S}_n$. Si $G \cap \mathfrak{A}_n \lhd \mathfrak{A}_n$, comme $\mathfrak{A}_n$ est simple, on a $G \cap \mathfrak{A}_n \in \{\mathsf{Id}, \mathfrak{A}_n\}$. Dans le premier cas, on a $\mathfrak{A}_n \subset G$, alors $G = \mathfrak{A}_n$ ou $G = \mathfrak{S}_n$. Dans le deuxième cas, on a $\#G \in \{1,2\}$. Si $\#G = 2$, alors $G = \{\mathsf{Id}, \sigma\}$ avec $\sigma \in \mathsf{Z}(\mathfrak{S}_n)\backslash\{\mathsf{Id}\}$, ce qui est impossible puisque $\mathsf{Z}(\mathfrak{S}_n)$ est trivial pour $n \geqslant 3$. □

Remarque 1.2.2.13. On a un lien avec la résolubilité par radicaux des polynômes.

Exercice 1.2.2.14. Déterminer tous les morphismes de groupes $\mathfrak{S}_n \to \mathbf{C}^\times$.

Solution : Soit $\varphi\colon \mathfrak{S}_n \to \mathbf{C}^\times$ un morphisme de groupes. Soit $\tau \in \mathfrak{S}_n$ une transposition. Comme $\tau^2 = \mathsf{Id}$, on a alors $\varphi(\tau)^2 = 1$, donc $\varphi(\tau) \in \{\pm 1\}$. Comme les transpositions sont conjuguées, elles ont toutes même image par φ. Si cette image est 1, le morphisme est trivial et si cette image est -1, le morphisme est la signature.

Exercice 1.2.2.15. Existe-t-il un morphisme surjectif $\mathfrak{S}_n \to \mathfrak{S}_{n-1}$?

Solution : Un tel morphisme fournit un sous-groupe distingué $G \leqslant \mathfrak{S}_n$ tel que $(\mathfrak{S}_n : G) = n$. Lorsque $n \geqslant 5$, les seuls sous-groupes distingués sont $\{\mathsf{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$ d'indices respectivement $n!$, 2 et 1 : c'est donc impossible. Lorsque $n = 2$, c'est le morphisme trivial et lorsque $n = 3$, on dispose d'un morphisme composé $\mathfrak{S}_3 \xrightarrow{\varepsilon} \{\pm 1\} \xrightarrow{\sim} \mathfrak{S}_2$. Enfin, lorsque $n = 4$, on a $\mathfrak{S}_4/V_4 \simeq \mathfrak{S}_3$.

1.3 Produits semi-directs

1.3.1 Produits semi-directs internes

Soient G un groupe, N et H deux sous-groupes de G.

Lemme 1.3.1.1. Si $N \lhd G$, l'ensemble $NH := \{xy\}_{\substack{x\in N\\ y\in H}}$ est un sous-groupe de G.

Démonstration. Pour $n_1, n_2 \in N$ et $h_1, h_2 \in H$, on a

$$n_1h_1(n_2h_2)^{-1} = n_1h_1h_2^{-1}n_2^{-1} = n_1(h_1h_2^{-1})n_2^{-1}(h_1h_2^{-1})^{-1}(h_1h_2^{-1}) \in NH$$

avec $(h_1h_2^{-1})n_2^{-1}(h_1h_2^{-1})^{-1} \in N$. □

On peut trouver une autre caractérisation sans sous-groupe distingué.

Définition 1.3.1.2. On dit que G est *produit semi-direct interne* de H par N lorsque :
(i) $N \lhd G$;
(ii) $N \cap H = \{e\}$;
(iii) $NH = G$.
On note alors $G = N \rtimes H$.

Proposition 1.3.1.3. Supposons que G soit produit semi-direct interne de H par N. Pour tout $y \in H$, on dispose de l'automorphisme $\varphi_y \in \mathsf{Aut}(N)$ défini par $\varphi_y(x) = yxy^{-1}$.
(i) Pour tout $g \in G$, il existe $x \in N$ et $y \in H$ uniques tels que $g = xy$. (ii) Si $g_1 = x_1y_1$, $g_2 = x_2y_2 \in G$ avec $x_1, x_2 \in N$ et $y_1, y_2 \in H$, on a :

$$g_1g_2 = (x_1\varphi_{y_1}(x_2))(y_1y_2).$$

(iii) L'application $\varphi\colon H \to \mathsf{Aut}(N)$ est un morphisme de groupes.

Démonstration. (i) Pour $x_1, x_2 \in N$ et $y_1, y_2 \in H$, on a :

$$x_1y_1 = x_2y_2 \Leftrightarrow x_2^{-1}x_1 = y_2y_1^{-1} \in N \cap H = \{e\}.$$

On a alors $x_1 = x_2$ et $y_1 = y_2$.
(ii) On a

$$\begin{aligned}(x_1y_1)(x_2y_2) &= x_1y_1x_2(y_1^{-1}y_1)y_2 = x_1(y_1x_2y_1^{-1})y_1y_2\\ &= (x_1\varphi_{y_1}(x_2))(y_1y_2)\end{aligned}$$

et comme $x_1\varphi_{y_1}(x_2) \in N$ et $y_1y_2 \in H$, alors $(x_1\varphi_{y_1}(x_2))(y_1y_2) \in NH$.
(iii) Évident. □

Remarque 1.3.1.4. Supposons G fini, $N \lhd G$ et $N \cap H = \{e\}$. On a alors $\#N\#H = \#G$ si et seulement si $NH = G$. En effet, l'application

$$\begin{aligned}N \times H &\to G\\ (x, y) &\mapsto xy\end{aligned}$$

est injective et son image est NH.

Exemple 1.3.1.5. (1) Soient $N = \mathfrak{A}_3 = \langle(1,2,3)\rangle \lhd G = \mathfrak{S}_3$ et $H = \langle(1,2)\rangle$. Comme $\#N = 3$ et $\#H = 2$, le théorème de Lagrange implique que $N \cap H = \{\mathsf{Id}\}$. Comme $\#N\#H = 6 = \#\mathfrak{S}_3$, on a donc $\mathfrak{S}_3 = N \rtimes H$.
(2) Exemple crucial : le *groupe diédral* d'ordre $2n$. Soient $n \in \mathbf{N}_{>0}$ et $U_n = \{z \in \mathbf{C};\ z^n = 1\}$ (qui est un sous-groupe de $\mathbf{C}^\times$) le groupe des racines n-ièmes de l'unité. Observons que le choix d'une racine primitive n-ième de l'unité fournit un isomorphisme (non canonique) : $\mathbf{Z}/n\,\mathbf{Z} \xrightarrow{\sim} U_n$. Identifions $\mathbf{C}$ au $\mathbf{R}$-espace vectoriel $\mathbf{R}^2$ de la façon habituelle. On note alors D_{2n} le sous-groupe de $\mathsf{O}_2(\mathbf{R})$ constitué des isométries qui préservent U_n. On dispose du morphisme $\mathsf{det}\colon \mathsf{O}_2(\mathbf{R}) \to \{\pm 1\}$ et $\mathsf{Ker}(\mathsf{det}) = \mathsf{SO}_2(\mathbf{R})$. Pour $\theta \in \mathbf{R}$, on dispose de la matrice de rotation

$$R_\theta = \begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix} \in \mathsf{SO}_2(\mathbf{R}).$$

L'application :

$$\begin{aligned}\mathbf{R} &\to \mathsf{SO}_2(\mathbf{R})\\ \theta &\mapsto R_\theta\end{aligned}$$

est un morphisme de groupes, de noyau $2\pi\,\mathbf{Z}$: il induit un isomorphisme

$$\mathbf{R}/2\pi\,\mathbf{Z} \xrightarrow{\sim} \mathsf{SO}_2(\mathbf{R}).$$

De même, l'application $t \mapsto e^{it}$ induit un isomorphisme $\mathbf{R}/2\pi\,\mathbf{Z} \xrightarrow{\sim} U := \{z \in \mathbf{C};\ |z| = 1\}$. On dispose donc d'un isomorphisme $\varepsilon\colon U \xrightarrow{\sim} \mathsf{SO}_2(\mathbf{R})$ tel que pour tout $\theta \in \mathbf{R}$, on ait $\varepsilon(e^{i\theta}) = R_\theta$. Le groupe $D_{2n} \cap \mathsf{Ker}(\mathsf{det}) = D_{2n} \cap \mathsf{SO}_2(\mathbf{R})$ est constitué des rotations qui préservent U_n : l'isomorphisme ε induit un isomorphisme $U_n \xrightarrow{\sim} D_{2n} \cap \mathsf{SO}_2(\mathbf{R})$. Il est distingué dans D_{2n} (c'est le noyau de la restriction de det à D_{2n}). Notons $\sigma \in D_{2n}$ l'élément correspondant à la conjugaison complexe, c'est la symétrie orthogonale par rapport à l'axe des réels dans $\mathbf{C}$. On a $\sigma \notin D_{2n} \cap \mathsf{SO}_n(\mathbf{R})$, donc $(D_{2n} \cap \mathsf{SO}_2(\mathbf{R})) \cap \langle\sigma\rangle = \{\mathsf{Id}_{\mathbf{R}^2}\}$.
Soit $g \in D_{2n}$. Si $g \neq \mathsf{SO}_2(\mathbf{R})$, on a $\mathsf{det}(g) = -1$ et donc $\mathsf{det}(g\sigma) = 1$. On a alors $g = (g\sigma)\sigma \in (D_{2n} \cap \mathsf{SO}_2(\mathbf{R})) \cap \langle\sigma\rangle$. Cela montre que D_{2n} est produit semi-direct de $\langle\sigma\rangle \simeq \mathbf{Z}/2\,\mathbf{Z}$ par $D_{2n} \cap \mathsf{SO}_2(\mathbf{R}) \simeq U_n \simeq \mathbf{Z}/n\,\mathbf{Z}$. En particulier, on a $\#D_{2n} = 2n$ et D_{2n} est engendré par deux éléments ρ (la rotation d'angle $\frac{2\pi}{n}$) et σ (si on peut expliciter les éléments de D_{2n}, on a $D_{2n} = \{\mathsf{Id}, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}$). Ils sont assujettis aux relations $\rho^n = \mathsf{Id}$, $\sigma^2 = \mathsf{Id}$ et

$(\rho\sigma)^2 = \mathsf{Id}$ (puisque $\mathsf{det}(\rho\sigma) = -1$). On remarque également que si $n = 3$, $D_6 \simeq \mathfrak{S}_3$.
(3) Notons V le *groupe de Klein* : le sous-groupe de $\mathfrak{A}_4$ constitué de Id et des trois double-transpositions. On a $V \simeq (\mathbf{Z}/2\,\mathbf{Z})^2$ et $V \lhd \mathfrak{A}_4$. Soient c un 3-cycle (par exemple $c = (1,2,3)$) et $H = \langle c\rangle \simeq \mathbf{Z}/3\,\mathbf{Z}$. On a alors que $\mathfrak{A}_4$ est produit semi-direct interne de H par V.
(4) Soit $(\mathscr{E}, E)$ un espace affine. On dispose du groupe affine $\mathsf{GA}(\mathscr{E})$ des transformations affines et du groupe des translations $\mathscr{T}(\mathscr{E}) \simeq E$. Le choix d'un point $\Omega \in \mathscr{E}$ permet de vectorialiser $\mathscr{E}$ *i.e.* fournit la bijection

$$\begin{aligned} \mathscr{E} &\xrightarrow{\sim} E \\ M &\mapsto \overrightarrow{\Omega M} \end{aligned}$$

Si H_Ω désigne le sous-groupe de $\mathsf{GA}(\mathscr{E})$ constitué des éléments qui fixent Ω, l'application « application linéaire associée » fournit un isomorphisme $H_\Omega \xrightarrow{\sim} \mathsf{GL}(E)$. On vérifie sans peine que $\mathsf{GA}(\mathscr{E})$ est produit semi-direct interne de H_Ω par $\mathscr{T}(\mathscr{E})$.

1.3.2 Produits semi-directs externes

Inspirés par ce qui précède, on peut définir la notion du produit semi-direct « externe »s de deux groupes : cette procédure permet de construire de nouveaux groupes. Soient N et H deux groupes et

$$\begin{aligned} \varphi\colon H &\to \mathsf{Aut}(N) \\ y &\mapsto \varphi_y \end{aligned}$$

un morphisme de groupes.

Définition 1.3.2.1. Le *produit semi-direct externe* de H par N (relativement à φ) est le groupe $N \rtimes_\varphi H$ dont l'ensemble sous-jacent est $N \times H$ (produit direct d'ensembles) et la loi est donnée par

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1\varphi_{y_1}(x_2), y_1y_2).$$

Proposition 1.3.2.2. Ce qui précède définit bien un groupe, d'élément neutre (e_N, e_H).

Démonstration. • Associativité : soient $x_1, x_2, x_3 \in N$ et $y_1, y_2, y_3 \in H$. On a

$$\begin{aligned} (x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3)) &= (x_1, y_1) \cdot (x_2\varphi_{y_2}(x_3), y_2y_3) \\ &= (x_1\varphi_{y_1}(x_2\varphi_{y_2}(x_3)), y_1y_2y_3) \\ &= (x_1\varphi_{y_1}(x_2)\varphi_{y_1y_2}(x_3), y_1y_2y_3) \\ &= (x_1\varphi_{y_1}(x_2), y_1y_2) \cdot (x_3, y_3) \\ &= ((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3). \end{aligned}$$

• Si $x \in N$ et $y \in H$, on a $(x, y) \cdot (e_N, e_H) = (x, y)$ (resp. $(e_N, e_H) \cdot (x, y) = (x, y)$) parce que $\varphi_y(e_N) = e_N$ (resp. $\varphi_{e_H} = \mathsf{Id}_N$).
• Inverse : soient $x \in N$ et $y \in H$. On a $(x, y) \cdot (\varphi_y^{-1}(x), y^{-1}) = (\varphi_y^{-1}(x), y^{-1}) \cdot (x, y) = (e_N, e_H)$. □

Remarque 1.3.2.3. Il est facile de vérifier que $N \rtimes_\varphi H$ est produit semi-direct interne de $\{e_N\} \times H$ par $N \times \{e_H\}$. Pour $x \in N$ et $y \in H$, on a alors

$$(\varphi_y(x), e_H) = (e_N, y) \cdot (x, e_H) \cdot (e_N, y)^{-1}.$$

Proposition 1.3.2.4. Le produit semi-direct $N \rtimes_\varphi H$ est direct (*i.e.* égal à $N \times H$) si et seulement si $\varphi\colon H \to \mathsf{Aut}(N)$ est trivial.

Démonstration. Le produit est direct si et seulement si $(x_1, y_1)\cdot(x_2, y_2) = (x_1x_2, y_1y_2)$ *i.e.* $x_1\varphi_{y_1}(x_2) = x_1x_2$, soit encore si et seulement si $\varphi_{y_1}(x_2) = x_2$ pour tous $x_1, x_2 \in N$ et $y_1, y_2 \in H$. Cela équivaut à $\varphi_y = \mathsf{Id}_N$ pour tout $y \in H$. □

Exemple 1.3.2.5. (1) Si φ est trivial, on a vu que $N \rtimes_\varphi H = N \times H$.
(2) Pour tout $n \in \mathbf{N}_{>0}$, on a $D_{2n} \simeq (\mathbf{Z}/n\,\mathbf{Z}) \rtimes_\varphi (\mathbf{Z}/2\,\mathbf{Z})$ où $\varphi(\overline{1})$ est la multiplication par -1 dans $\mathbf{Z}/n\,\mathbf{Z}$.
(3) Soient $n \in \mathbf{N}_{>1}$ et $\tau \in \mathfrak{S}_n$ une transposition. On a $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes_\varphi \{\pm 1\}$, où $\varphi(-1)$ est la conjugaison par τ.

Remarque 1.3.2.6. On voit que deux morphismes $H \to \mathsf{Aut}(N)$ distincts peuvent produire deux produits semi-directs isomorphes. En général, c'est une question intéressante et un peu délicate de comprendre les classes d'isomorphisme de produits semi-directs d'un groupe par un autre (en faisant varier φ), voire quand deux produits semi-directs sont isomorphes.

1.4 Actions de groupes

1.4.1 Rappels

Dans tout ce qui suit, G désigne un groupe (noté multiplicativement) et X un ensemble non vide. On note e l'élément neutre de G.

Définition 1.4.1.1. Une *action* (à gauche) de G sur X est la donnée d'une application

$$*\colon G \times X \to X$$

ayant les propriétés suivantes :
(i) $(\forall g_1, g_2 \in G)\ (\forall x \in X)\ g_1 * (g_2 * x) = (g_1 g_2) * x$;
(ii) $(\forall x \in X)\ e * x = x$.
On dit aussi que G *agit* sur X.

Remarque 1.4.1.2. On définit de même la notion d'action à droite, en considérant les applications $*\colon X \times G \to X$ vérifiant $(x * g_1) * g_2 = x * (g_1 g_2)$ et $x * e = x$ pour tous $g_1, g_2 \in G$ et $x \in X$. Observons qu'à partir du groupe G, on peut définir le *groupe opposé* G^{op}, dont l'ensemble sous-jacent est G et la loi de groupe est donnée par $(g_1, g_2) \mapsto g_2 g_1$. Il n'est pas très difficile de se convaincre qu'une action à droite de G sur X est la même chose qu'une action à gauche de G^{op} sur X. Dans ce qui suit, on ne considérera que des actions à gauche et quand on parlera d'action, ce sera toujours à gauche.

Si $*\colon G \times X \to X$ est une action et si $g \in G$, on dispose de l'application

$$\begin{aligned} \rho(g)\colon X &\to X \\ x &\mapsto g * x \end{aligned}$$

Les conditions (i) et (ii) se réécrivent :
(i) $(\forall g_1, g_2 \in G)\ \rho(g_1) \circ \rho(g_2) = \rho(g_1 g_2)$;
(ii) $\rho(e) = \mathsf{Id}_X$.

Proposition 1.4.1.3. Pour tout $g \in G$, on a $\rho(g) \in \mathfrak{S}_X$. L'application $\rho\colon G \to \mathfrak{S}_X$ est un morphisme de groupes.

Démonstration. Si $g \in G$, on a $\rho(g) \circ \rho(g^{-1}) = \rho(g^{-1}) \circ \rho(g) = \rho(e) = \mathsf{Id}_X$, ce qui prouve que $\rho(g)$ est une permutation de X et que $\rho(g^{-1}) = \rho(g)^{-1}$. La deuxième partie de la proposition en résulte. □

Si $g \in G$ et $x \in X$, on a $g * x = \rho(g)(x)$. Cela montre que l'action est complètement déterminée par le morphisme associé ρ. Réciproquement, si on se donne un morphisme de groupes $f\colon G \to \mathfrak{S}_X$, on définit une action de G sur X en posant $g * x = f(g)(x)$ pour tout $g \in G$ et $x \in X$. Le morphisme de groupes associé n'est autre que f lui-même. Cet argument montre directement la proposition suivante.

Proposition 1.4.1.4. La donnée d'une action de G sur X équivaut à celle d'un morphisme de groupes $G \to \mathfrak{S}_X$.

Exemple 1.4.1.5. (1) Le groupe G agit sur lui-même par *translation à gauche* : l'action est donnée par $g * x = gx$ pour tous $g, x \in G$. L'action par *translation à droite* est donnée par $(x, g) \mapsto xg^{-1}$.
(2) Plus généralement, si $H \leqslant G$ est un sous-groupe, on dispose de l'ensemble quotient G/H, constitué des classes à gauche modulo H *i.e.* les parties de la forme $\gamma H \subset G$ avec $\gamma \in G$. On fait agir G sur G/H par translation à gauche en posant $g * (\gamma H) = g\gamma H = \{gx\}_{x \in \gamma H}$ (notons que c'est bien défini, *i.e.* que γH ne dépend que de la classe γH et pas du choix d'un représentant γ).
(3) Le groupe $\mathfrak{S}_X$ agit sur X de façon naturelle, par $\sigma * x = \sigma(x)$. Le morphisme de groupes associé n'est autre que l'identité de $\mathfrak{S}_X$. Cas particulier où $X = \{1, \ldots, n\}$.
(4) Tout groupe agit sur lui-même par *conjugaison* en posant $g * x = gxg^{-1}$ pour tous $g, x \in G$.
(5) Plusieurs exemples en algèbre linéaire et en géométrie.

Définition 1.4.1.6. Soit G un groupe agissant sur un ensemble X.
(i) L'*orbite* de $x \in X$ est l'ensemble $G * x = \{g * x\}_{g \in G}$. C'est une partie de X et on la note $\mathsf{orb}(x)$.
(ii) Le *stabilisateur* de $x \in X$ est $\mathsf{stab}_G(x) = \{g \in G \mid g * x = x\}$. C'est un sous-groupe de G.
(iii) On dit que l'action est *fidèle* lorsque le morphisme associé $\rho\colon G \to \mathfrak{S}_X$ est injectif.
(iv) On dit que l'action est *libre* lorsque pour tout $x \in X$, $g * x = x$ implique que $g = e$.
(v) On dit que l'action est *transitive* s'il n'y a qu'une seule orbite. Plus généralement, si $k \in \mathbf{N}_{>0}$, on dit que l'action est k-*transitive* si pour tout k-uplets $(x_1, \ldots, x_k)$ et $(y_1, \ldots, y_k)$ d'éléments distincts de X, il existe $g \in G$ tel que $g * x_i = y_i$ pour tout $i \in \{1, \ldots, k\}$.

Remarque 1.4.1.7. (1) Si $x_1, x_2 \in X$, on pose $x_1 \sim x_2$ lorsqu'il existe $g \in G$ tel que $x_2 = g * x_1$. Cela définit une relation d'équivalence sur X, dont les classes d'équivalence ne sont autres que les orbites. En particulier, les orbites forment une partition de X.
(2) Une action libre est fidèle.
(3) L'action induite de G sur chaque orbite est transitive.

Exemple 1.4.1.8. (1) Si H est un sous-groupe de G, l'action de G sur G/H par translation à gauche est transitive.
(2) L'action naturelle de $\mathfrak{S}_n$ sur $\{1, \ldots, n\}$ est fidèle.
(3) Si G agit sur lui-même par conjugaison, l'orbite de x s'appelle la classe de conjugaison de x. Le stabilisateur de x est le sous-groupe $\mathsf{C}_G(x)$ des éléments de G qui commutent à x : on l'appelle le *centralisateur* de x.
(4) Lorsque G agit sur l'ensemble de ses sous-groupes par conjugaison, le stabilisateur d'un sous-groupe $H \leqslant G$ s'appelle le *normalisateur* de H et se note $\mathsf{N}_G(H)$. On a l'équivalence « $H \lhd G \Leftrightarrow \mathsf{N}_G(H) = G$ » de façon évidente.

Théorème 1.4.1.9 (Caylay)**.** L'action de G sur lui même par translation à gauche est fidèle. Elle permet en particulier de voir G comme un sous-groupe de $\mathfrak{S}_G \simeq \mathfrak{S}_n$, où $n = \#G$.

Démonstration. On dispose du morphisme $G \to \mathfrak{S}_G$. Si $g \in G$ tel que $\rho(g) = \mathsf{Id}_G$, alors on a $gx = x$ pour tout $x \in G$. En particulier, pour $x = e$, on a $g = e$, d'où $\mathsf{Ker}(\rho) = \{e\}$. □

Lemme 1.4.1.10. Soient G un groupe agissant sur un ensemble X, $g \in G$ et $x \in X$. On a

$$\mathsf{stab}_G(g * x) = g\,\mathsf{stab}_G(x)g^{-1}.$$

Démonstration. Si $\gamma \in G$, on a les équivalences :

$$\begin{aligned}\gamma \in \mathsf{stab}_G(g*x) &\Leftrightarrow \gamma * (g*x) = g*x \Leftrightarrow g^{-1}\gamma g * x = x\\ &\Leftrightarrow g^{-1}\gamma g \in \mathsf{stab}_G(x) \Leftrightarrow \gamma \in g\,\mathsf{stab}_G(x)g^{-1}.\end{aligned}$$

□

Théorème 1.4.1.11 (Relation orbite-stabilisateur)**.** Soient G un groupe agissant sur un ensemble X et $x \in X$. L'application

$$\begin{aligned}G/\mathsf{stab}_G(x) &\to \mathsf{orb}_X(x)\\ \overline{g} &\mapsto g \cdot x\end{aligned}$$

est bijective.

Démonstration. Soit

$$\begin{aligned}f\colon G &\to \mathsf{orb}(x)\\ g &\mapsto g \cdot x\end{aligned}$$

une application surjective. On a les équivalences

$$\begin{aligned}f(g_1) = f(g_2) &\Leftrightarrow g_1 \cdot x = g_2 \cdot x \Leftrightarrow (g_2^{-1}g_1)\cdot x = x\\ &\Leftrightarrow g_2^{-1}g_1 \in \mathsf{stab}(x) \Leftrightarrow g_1\,\mathsf{stab}(x) = g_2\,\mathsf{stab}(x)\end{aligned}$$

pour $g_1, g_2 \in G$. On a donc $\mathcal{R}_f = \mathcal{R}_{\mathsf{stab}}$. L'application f induit alors une bijection

$$G/\mathsf{stab}_G(x) \xrightarrow{\sim} \mathsf{orb}(x).$$

□

Remarque 1.4.1.12. La bijection qui précède est en outre G-équivariante *i.e.* compatible aux actions de G.

Corollaire 1.4.1.13. Si G est fini et $x \in X$, on a $\#G = \#\,\mathsf{orb}_X(x)\#\,\mathsf{stab}_G(x)$. En particulier, l'entier

$$\#\,\mathsf{orb}_X(x) = (G : \mathsf{stab}_G(x))$$

divise $\#G$.

Démonstration. Tout découle de la bijection de la proposition précédente. □

Proposition 1.4.1.14 (Équation aux classes)**.** Supposons X fini. Si $\{x_1, \ldots, x_r\}$ est un système complet de représentants des orbites de X, on a

$$\#X = \sum_{i=1}^{r} \#\,\mathsf{orb}_X(x_i) = \sum_{i=1}^{r} (G : \mathsf{stab}_G(x_i)).$$

Démonstration. Cela vient du fait que les orbites forment une partition de X *i.e.* $\#X = \bigsqcup_{i=1}^{r} \mathsf{orb}(x_i)$. □

Corollaire 1.4.1.15. Si G est un p-groupe et X est fini, on a $\#X \equiv \#X^G \bmod p$ (où X^G désigne l'ensemble des points fixes).

Démonstration. Par la proposition 1.4.1.14, on a $\#X = \sum_{i=1}^{r} \#\,\mathsf{orb}(x_i) = \sum_{i=1}^{r} (G : \mathsf{stab}_G(x_i))$. Si $x \in X^G$, alors $\mathsf{orb}(x) = \{x\}$. Si $x \notin X^G$, alors $\#\,\mathsf{orb}(x) > 1$ et comme $\#\,\mathsf{orb}(x) \mid G = p^n$ avec $n \geqslant 1$, alors $p \mid \mathsf{orb}(x)$. En particulier, on a l'égalité

$$\#X = \#X^G + \sum_{x \notin X^G} \#\,\mathsf{orb}(x).$$

□

Corollaire 1.4.1.16. Le centre d'un p-groupe est non trivial (par récurrence, pour tout $k \in \mathbf{N}$ tel que $p^k \mid \#G$, le p-groupe contient un sous-groupe distingué d'ordre p^k).

Démonstration. Soit G un p-groupe non trivial. Faisons agir G sur lui-même par conjugaison. En appliquant le corollaire précédent avec $X^G = \mathsf{Z}(G)$, on a $\#G = \#\,\mathsf{Z}(G) \bmod p$. On sait que $p \mid \#G$ et que G est non trivial, donc $p \mid \#\,\mathsf{Z}(G)$. Mais $e \in \mathsf{Z}(G)$, d'où $\#\,\mathsf{Z}(G) > 0$. On a alors $\#\,\mathsf{Z}(G) \geqslant p \geqslant 2$ *i.e.* $\mathsf{Z}(G)$ contient des éléments non triviaux. □

Proposition 1.4.1.17 (Formule de Burnside)**.** Supposons G et X finis. Pour tout $x \in X$, posons $\mathsf{Fix}(g) = \{x \in X;\ g \cdot x = x\}$ (les points fixes de g dans X). Le nombre d'orbites dans X est

$$\frac{1}{\#G} \sum_{g \in G} \#\,\mathsf{Fix}(g)$$

(c'est le nombre moyen de points fixes).

Démonstration. Posons $\mathscr{E} = \{(g,x) \in G \times X;\ g \cdot x = x\} \subset (G \times X)$. On a donc $\mathscr{E} = \bigsqcup_{g \in G} \{g\} \times \mathsf{Fix}(g)$, alors $\#\mathscr{E} = \sum_{g \in G} \#\,\mathsf{Fix}(g)$. On a également que $\mathscr{E} = \bigsqcup_{x \in X} \mathsf{stab}(x) \times \{x\}$, donc $\#\mathscr{E} = \sum_{x \in X} \#\,\mathsf{stab}_G(x)$. Notons $\Omega_1, \ldots, \Omega_r$ les orbites de X. On a bien sûr

$$X = \bigsqcup_{i=1}^{r} \Omega_i \quad \text{donc} \quad \mathscr{E} = \sum_{i=1}^{r} \sum_{x \in \Omega_i} \#\,\mathsf{stab}_G(x_i).$$

Si $x \in \Omega_i$, alors $\Omega_i = \mathsf{orb}(x)$ et $\#\Omega_i \#\,\mathsf{stab}(x) = \#G$, d'où

$$\#\mathscr{E} = \sum_{i=1}^{r} \sum_{x \in \Omega_i} \frac{\#G}{\#\Omega_i}$$

mais $\sum_{x \in \Omega_i} \frac{\#G}{\#\Omega_i} = \#\Omega_i \frac{\#G}{\#\Omega_i} = \#G$. Finalement,

$$\#\mathscr{E} = \sum_{i=1}^{r} \#G = r\#G \quad \textit{i.e.} \quad r = \frac{1}{\#G} \sum_{g \in G} \#\,\mathsf{Fix}(g).$$

□

Quelques exemples d'utilisation des actions de groupes.

Proposition 1.4.1.18. Soient G un groupe et $H \leqslant G$ un sous-groupe d'indice n. Il existe un sous-groupe distingué N de G tel que $N \subset H$ et $(G : N) \mid n!$.

Démonstration. Faisons agir G sur l'ensemble G/H par translation à gauche. On en déduit un morphisme de groupes $\varphi \colon G \to \mathfrak{S}_{G/H} \simeq \mathfrak{S}_n$. Posons $N = \mathsf{Ker}(\varphi) \lhd G$. Par passage au quotient, φ induit un morphisme injectif $\widetilde{\varphi} \colon G/N \to \mathfrak{S}_n$, d'où $(G : N) = \#G/N \mid \#\mathfrak{S}_n = n!$. Si $g \in N$, $g\gamma H = \gamma H$ pour tout $\gamma \in G$, ce qui implique en particulier, $\gamma H = H$ *i.e.* $\gamma \in H$ donc $N \subset H$. □

Proposition 1.4.1.19. Soient G un groupe fini, $H \leqslant G$ un sous-groupe et p le plus petit diviseur premier de $\#G$. Si $(G : H) = p$, alors H est distingué dans G.

Démonstration. On fait agir G sur l'ensemble G/H : on en déduit un morphisme de groupes $\rho \colon G \to \mathfrak{S}_{G/H} \simeq \mathfrak{S}_p$. On a $\#\,\mathsf{Im}(\rho) \mid \#G$, donc $\#\,\mathsf{Im}(\rho) \mid \mathsf{pgcd}(p!, \#G) = p$: on a nécessairement $\#\,\mathsf{Im}(\rho) = p$ (car l'action est transitive), *i.e.* $(G : \mathsf{Ker}(\rho)) = (G : H)$. Comme $\mathsf{Ker}(\rho) \leqslant H$, cela implique que $H = \mathsf{Ker}(\rho) \lhd G$. □

Exercice 1.4.1.20. On suppose que $\mathbf{Z}/35\,\mathbf{Z}$ opère sans point fixe sur un ensemble E de cardinal 53. Quel est le nombre d'orbites pour cette action ?

Solution : Les cardinaux des orbites divisent 35 : comme les orbites sont non ponctuelles, ils appartiennent à $\{5, 7, 35\}$. Notons x, y et z le nombre d'orbites à 5, 7 et 35 éléments respectivement : on a $53 = 5x + 7y + 35z$. On a alors $7y \equiv 53 \bmod 5$, *i.e.* $2y \equiv 3 \bmod 5$, soit $y \equiv 2^{-1} \times 3 = 4 \bmod 5$, ce qui implique en particulier que $y \geqslant 4$. De même, on a $5x \equiv 53 \bmod 7$ *i.e.* $5x \equiv 4 \bmod 7$, soit $x \equiv 5^{-1} \times 4 = 5 \bmod 7$, ce qui implique en particulier que $x \geqslant 5$. Comme $5 \times 5 + 4 \times 7 = 53$, on a nécessairement $(x, y, z) = (5, 4, 0)$ et il y a 9 orbites.

Exercice 1.4.1.21. Soit G un groupe d'ordre 33 agissant sur un ensemble de cardinal 19. Montrer qu'il y a au moins un point fixe.

Solution : Le cardinal d'une orbite est un diviseur de 33 : c'est un élément dans $\{1, 3, 11, 33\}$. Supposons qu'il n'y a pas de point fixe : l'équation aux classes est de la forme $19 = 3x + 11y$ (il n'y a pas d'orbite à 33 éléments par cardinalité) avec $x, y \in \mathbf{N}$. On a $y \in \{0, 1\}$ et donc $3x \in \{8, 19\}$, ce qui n'est pas possible. Il y a donc au moins un point fixe.

Lemme 1.4.1.22. Si G est un groupe tel que $G/\mathsf{Z}(G)$ est monogène, alors G est abélien.

Démonstration. Soit $\pi\colon G \to G/\mathsf{Z}(G)$ la surjection canonique. Il existe $x \in G$ tel que $G/\mathsf{Z}(G) = \langle \pi(x) \rangle$. Si $g \in G$, il existe $k \in \mathbf{Z}$ tel que $\pi(g) = \pi(x)^k$ *i.e.* $gx^k \in \mathsf{Ker}(\pi) = \mathsf{Z}(G)$. Il existe $z \in \mathsf{Z}(G)$ tel que $g = zx^k$. Si $g_1, g_2 \in G$, il existe $z_1, z_2 \in \mathsf{Z}(G)$ et $k_1, k_2 \in \mathbf{Z}$ tel que $g_1 = z_1 x^{k_1}$ et $g_2 = z_2 x^{k_2}$. On a alors $g_1 g_2 = z_1 x^{k_1} z_2 x^{k_2} = z_1 z_2 x^{k_1+k_2}$ car $z_2 \in \mathsf{Z}(G)$. De même, $g_2 g_1 = z_2 x^{k_2} z_1 x^{k_1} = z_1 z_2 x^{k_1+k_2}$ car $z_1 \in \mathsf{Z}(G)$. □

Proposition 1.4.1.23. Soit p un nombre premier. Tout groupe de cardinal p^2 est abélien.

Démonstration. Soit G un groupe d'ordre p^2. Son centre $\mathsf{Z}(G)$ n'est pas trivial par le corollaire 1.4.1.16. De plus, $G/\mathsf{Z}(G)$ est d'ordre divisant p, il est alors monogène. On a directement la commutativité de G par le lemme précédent. □

Remarque 1.4.1.24. (1) Soit $G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} ; x, y, z \in \mathbf{Z}/p\mathbf{Z} \right\} \leqslant \mathsf{GL}_3(\mathbf{Z}/p\mathbf{Z})$ le sous-groupe des matrices triangulaires supérieures unipotentes. Il est non abélien de cardinal p^3.
(2) On peut classifier les groupes d'ordre p^2. Si G est cyclique d'ordre p^2, alors $G \simeq \mathbf{Z}/p^2\mathbf{Z}$. Si G n'est pas cyclique, alors il est naturellement muni d'une structure de $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel, on a alors $G \simeq (\mathbf{Z}/p\mathbf{Z})^2$.

Voici une réciproque (très) partielle du théorème de Lagrange.

Théorème 1.4.1.25 (Cauchy)**.** Soient G un groupe fini et p un nombre premier divisant $\#G$. Le groupe G contient alors un élément d'ordre p.

Démonstration. Posons $X = \{(g_1, \dots, g_p) \in G^p;\ g_1 \cdots g_p = e\}$. L'application

$$\begin{aligned} G^{p-1} &\to X \\ (g_1, \dots, g_{p-1}) &\mapsto \left(g_1, \dots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}\right) \end{aligned}$$

est bijective : on a $\#X = \#G^{p-1}$ et en particulier, $p \mid \#X$. Si $x = (g_1, \dots, g_p) \in X$, posons $\delta(x) = (g_p, g_1, \dots, g_{p-1})$ (décalage). On a $\delta^p(x) = x$, ce qui implique qu'on a une action de $\mathbf{Z}/p\mathbf{Z}$ sur X donnée par $k \cdot x = \delta^k(x)$ pour tout $x \in X$ et $k \in \mathbf{Z}/p\mathbf{Z}$. Comme $\mathbf{Z}/p\mathbf{Z}$ est un p-groupe, l'équation aux classes donne $\#X \equiv \#X^G \bmod p\mathbf{Z}$, d'où $p \mid \#X^G$. Mais $X^G = \{(g, \dots, g) \in G^p;\ g^p = e\} \simeq \{e\} \sqcup \Omega_p$ où Ω_p désigne l'ensemble des éléments d'ordre p dans G : on a donc $\#\Omega_p \equiv -1 \bmod p\mathbf{Z}$, en particulier Ω_p n'est pas vide. □

Remarque 1.4.1.26. Signalons que la relation orbite-stabilisateur, l'équation aux classes et la formule de Burnside ont de nombreuses applications en dénombrement.

1.4.2 Les théorèmes de Sylow

Dans tout ce qui suit, p désigne un nombre premier.

Définition 1.4.2.1. (i) Un *p-groupe* est un groupe fini d'ordre une puissance de p.
(ii) Si G est un groupe fini, un *p-sous-groupe de Sylow* (ou simplement p-Sylow) de G est un sous-groupe de G d'ordre $p^{v_p(\#G)}$ (avec $v_p(\#G)$ = la plus grande puissance a de p tel que $p^a \mid \#G$). On note $\mathsf{Syl}_p(G)$ l'ensemble des p-Sylow de G et on pose $n_p(G) = \#\,\mathsf{Syl}_p(G)$.

Remarque 1.4.2.2. Si p ne divise pas $\#G$, alors $\{e\}$ est l'unique p-Sylow de G.

Exemple 1.4.2.3. Si $n \in \mathbf{N}_{>0}$, on a $\#\,\mathsf{GL}_n(\mathbf{Z}/p\mathbf{Z}) = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$ (c'est le nombre de base du $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel $(\mathbf{Z}/p\mathbf{Z})^n$). Cela implique que

$$v_p(\#\,\mathsf{GL}_n(\mathbf{Z}/p\mathbf{Z})) = \sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}.$$

Notons $T_n(\mathbf{Z}/p\mathbf{Z})$ le sous-groupe de $\mathsf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ constitué des matrices triangulaires supérieures dont les coefficients diagonaux valent tous 1. On a $\#T_n(\mathbf{Z}/p\mathbf{Z}) = p^{\frac{n(n-1)}{2}}$ ce qui montre que $T_n(\mathbf{Z}/p\mathbf{Z})$ est un p-Sylow de $\mathsf{GL}_n(\mathbf{Z}/p\mathbf{Z})$.

Théorème 1.4.2.4 (Sylow)**.** On a :
(i) L'entier $n_p \equiv 1 \bmod p$ et en particulier, $\mathsf{Syl}_p(G)$ n'est pas vide ;
(ii) Le groupe G agit transitivement par conjugaison sur $\mathsf{Syl}_p(G)$ (les p-Sylow de G sont conjugués), en particulier $n_p(G) \mid \#G$.

Lemme 1.4.2.5. Si H est un sous-groupe de G et S un p-Sylow de G, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

Démonstration. Le groupe H agit sur G/S par translation à gauche. Le stabilisateur de gS pour cette action est $\{h \in H;\ hgS = gS\} = gSg^{-1} \cap H$: son orbite est de cardinal $(H : gSg^{-1} \cap H)$. Si $p \mid (H : gSg^{-1} \cap H)$ pour tout $g \in G$, les H-orbites de G/S sont toutes de cardinal divisible par p, si bien que $p \mid \#(G/S)$, contredisant le fait que S est un p-Sylow de G. Il existe donc $g \in G$ tel que $p \nmid (H : gSg^{-1} \cap H)$. Comme $gSg^{-1} \cap H$ est un p-groupe (car conjugué d'un sous-groupe de S), c'est un p-Sylow de H. □

Démonstration du théorème 1.4.2.4. • Posons $n = \#G$. D'après le théorème de Caylay (*cf.* théorème 1.4.1.9), on a un morphisme injectif $G \to \mathfrak{S}_n \to \mathsf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ (le deuxième est l'application qui envoie une permutation sur la matrice de permutation associée) : il permet de voir G comme un sous-groupe de $\mathsf{GL}_n(\mathbf{Z}/p\mathbf{Z})$. On dispose dans ce dernier du p-Sylow $T_n(\mathbf{Z}/p\mathbf{Z})$: d'après le lemme 1.4.2.5, il existe $g \in \mathsf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ tel que $gT_n(\mathbf{Z}/p\mathbf{Z})g^{-1} \cap G$ soit un p-sous-groupe de Sylow de G. Cela montre que $\mathsf{Syl}_p(G) \neq \varnothing$.
• Soit S et S' deux p-Sylow de G. Le lemme 1.4.2.5 appliqué à $H = S'$ montre qu'il existe $g \in G$ tel que $gSg^{-1} \cap S'$ soit un p-Sylow de S' *i.e.* soit égal à S' : on a $gSg^{-1} \subset S'$ et donc $gSg^{-1} = S'$ par cardinalité. Cela montre que l'action de G par conjugaison sur l'ensemble de ses p-Sylow est transitive *i.e.* (ii).
• Soit $S \in \mathsf{Syl}_p(G)$. On fait agir S par conjugaison sur $X := \mathsf{Syl}_p(G)\backslash\{S\}$. Si $S' \in X$ est fixe pour cette action, alors $S \subset \mathsf{N}_G(S')$. Cela implique que S et S' sont deux p-Sylow de $\mathsf{N}_G(S')$. Mais comme S' est distingué dans $\mathsf{N}_G(S')$, c'est l'unique p-Sylow de $\mathsf{N}_G(S')$: contradiction. Cela montre que S agit sans point fixe sur X : l'équation aux classes montre que $p \mid \#X$ *i.e.* $n_p(G) \equiv 1 \bmod p\mathbf{Z}$. □

Corollaire 1.4.2.6. Le groupe G admet un unique p-Sylow si et seulement si ce dernier est distingué dans G.

Démonstration. C'est une conséquence directe du fait que les p-Sylow sont conjugués dans G. □

Exercice 1.4.2.7. Si G est un groupe fini et $H \lhd G$ un sous-groupe distingué, on a $H\,\mathsf{N}_G(S) = G$ pour tout $S \in \mathsf{Syl}_p(H)$.

Solution : Si $g \in G$, alors $gSg^{-1} \subset gHg^{-1} = H$ est p-Sylow de H. Comme les p-Sylow de H sont conjugués dans H, il existe $h \in H$ tel que $gSg^{-1} = hSh^{-1}$. On a alors $h^{-1}gS(h^{-1}g)^{-1} = S$, *i.e.* $h^{-1}g \in \mathsf{N}_G(S)$, de sorte que $g \in h\,\mathsf{N}_G(S) \subset H\,\mathsf{N}_G(S)$, d'où $G = H\,\mathsf{N}_G(S)$.

Exercice 1.4.2.8. Soient G un groupe fini et $H \leqslant G$ un sous-groupe tel que H soit un p-groupe. Montrer qu'il existe $S \in \mathsf{Syl}_p(G)$ tel que $H \leqslant S$.

Solution : Soit $S_0 \in \mathsf{Syl}_p(G)$. D'après le lemme 1.4.2.5, il existe $g \in G$ tel que $gS_0g^{-1} \cap H$ soit p-Sylow de H, *i.e.* égal à H (vu que H est un p-groupe). Si $S = gS_0g^{-1}$, on a donc $H \subset S$.

Exercice 1.4.2.9. Soient G un groupe fini, $H \leqslant G$ un sous-groupe et p un nombre premier. Soit Q un p-Sylow de H. Montrer qu'il existe un p-Sylow S de G tel que $Q = S \cap H$.

Solution : Même principe que l'exercice précédent.

Quelques exemples d'utilisation des théorèmes de Sylow.

Proposition 1.4.2.10. Tout groupe d'ordre 35 est cyclique.

Démonstration. Soit G un groupe d'ordre 35. Tout d'abord, $35 = 5 \times 7$. De plus, $n_5 \equiv 1 \bmod 5$ et $n_5 \mid 7$, donc $n_5 = 1$, il y a alors un seul 5-Sylow. Il y a donc 4 éléments d'ordre 5 dans G. De même, $n_7 \equiv 1 \bmod 7$ et $n_7 \mid 5$, donc $n_7 = 1$, il y a alors un seul 7-Sylow. Il y a donc 6 éléments d'ordre 7 dans G. Il y a $35 - 4 - 6 - 1 = 24$ éléments d'ordre 35 dans G, donc il y a au moins un élément d'ordre 35 dans G. Le groupe G est donc cyclique. □

Proposition 1.4.2.11. Tout groupe d'ordre 77 est cyclique.

Démonstration. Soit H l'ensemble des 7-Sylow de G et K l'ensemble des 11-Sylow de G. Il est clair que $H \cap K = \{e\}$. Soit

$$\begin{aligned} f\colon H \times K &\to G \\ (h,k) &\mapsto hk \end{aligned}$$

un morphisme de groupes. Si $(h,k) \in H \times K$, alors $hkh^{-1}k^{-1} \in H \cap K$, donc $hk = kh$. L'application f est alors un isomorphisme. En outre, $H \simeq \mathbf{Z}/7\mathbf{Z}$ et $K \simeq \mathbf{Z}/11\mathbf{Z}$. Par le théorème des restes chinois, on a alors $H \times K \simeq \mathbf{Z}/77\mathbf{Z}$ et on déduit que G est cyclique. □

Proposition 1.4.2.12. Il n'existe pas de groupe simple d'ordre 36.

Démonstration. Tout d'abord, on a $36 = 2^2 \times 3^2$. Soit n_3 le nombre de 3-Sylow de G. On a $n_3 \mid 4$ et $n_3 \equiv 1 \bmod 3$, de sorte que $n_3 \in \{1,4\}$. Si $n_3 = 1$, alors l'unique 3-Sylow est distingué dans G, qui n'est donc pas simple. Si $n_3 = 4$, l'action de G par conjugaison sur l'ensemble de ses 3-Sylow fournit un morphisme de groupes $\rho\colon G \to \mathfrak{S}_4$. Comme l'action est transitive, on a $4 \mid \#\,\mathsf{Im}(\rho)$. On a en outre $\#\,\mathsf{Ker}(\rho)\#\,\mathsf{Im}(\rho) = \#G = 36$, donc $\#\,\mathsf{Im}(\rho) \mid 36$. Comme $\#\,\mathsf{Im}(\rho) \leqslant \mathfrak{S}_4$, on a aussi $\#\,\mathsf{Im}(\rho) \mid 24$. Cela implique que $\#\,\mathsf{Im}(\rho) \in \{4,12\}$, de sorte que $\#\,\mathsf{Ker}(\rho) \in \{3,9\}$. Le sous-groupe distingué $\mathsf{Ker}(\rho)$ est stricte et G n'est pas simple. □

Proposition 1.4.2.13. Il n'existe pas de groupe simple d'ordre 945.

Démonstration. Tout d'abord, on a $945 = 3^3 \times 5 \times 7$. Soit G un groupe d'ordre 945. On a $n_3(G) \mid 5 \times 7$, donc $n_3(G) \in \{1,5,7,35\}$. Mais $n_3(G) \equiv 1 \bmod 3$, donc $n_3(G) \in \{1,7\}$. Si $n_3(G) = 1$, alors l'unique 3-Sylow est distingué dans G, donc G ne peut pas être simple. Si $n_3(G) = 7$, l'action de G sur $\mathsf{Syl}_3(G)$ fournit un morphisme non trivial $\rho\colon G \to \mathfrak{S}_{\mathsf{Syl}_3(G)} \simeq \mathfrak{S}_7$. On sait que $\mathsf{Ker}(\rho)$ est distingué dans G mais différent de G (puisque ρ n'est pas trivial). Si G était simple, on aurait nécessairement $\mathsf{Ker}(\rho) = \{e\}$ *i.e.* ρ est injectif, d'où $3^3 \mid \#G \mid \#\mathfrak{S}_7 = 7!$ mais $3^3 \nmid 7!$. On a donc une contradiction et de nouveau, G ne peut pas être simple. □

Exercice 1.4.2.14. Déterminer le nombre de p-Sylow du groupe symétrique $\mathfrak{S}_p$.

Solution : Un p-Sylow de $\mathfrak{S}_p$ est un sous-groupe d'ordre p. Le nombre n_p de ces sous-groupes est le nombre de p-cycles divisé par $p-1$ (un groupe d'ordre p à $p-1$ générateurs). Or le nombre de p-cycles est $(p-1)!$: on a $n_p = (p-2)!$.

Exercice 1.4.2.15. Soit G un groupe d'ordre 12. On suppose que l'ensemble des 3-Sylow de G est de cardinal 4. Montrer que G est isomorphe à $\mathfrak{A}_4$ (on commencera par construire un morphisme $G \to \mathfrak{S}_4$).

Solution : On fait agir G par conjugaison sur l'ensemble X de ses 3-Sylow : cela fournit un morphisme de groupes $\rho\colon G \to \mathfrak{S}_X \simeq \mathfrak{S}_4$. Le groupe $\mathsf{Im}(\rho)$ agit transitivement sur $\{1,2,3,4\}$. Comme $\#\,\mathsf{Im}(\rho) = \#\,\mathsf{orb}_{\mathsf{Im}(\rho)}(1)\#\,\mathsf{stab}_{\mathsf{Im}(\rho)}(1)$, on a $4 \mid \#\,\mathsf{Im}(\rho)$ et donc $\#\,\mathsf{Ker}(\rho) \mid 3$. Par ailleurs, si $P \in X$, alors $\mathsf{Ker}(\rho) \leqslant \mathsf{stab}_G(P)$. On a bien sûr $P \leqslant \mathsf{stab}_G(P)$ et donc $(G : \mathsf{stab}_G(P)) \mid 3$. Si on avait $\mathsf{stab}_G(P) = \{e\}$, alors P serait distingué dans G et on aurait $X = \{P\}$, ce qui n'est pas. On a donc $\mathsf{stab}_G(P) = P$ et donc $\mathsf{Ker}(\rho) \leqslant P$, d'où $\#\,\mathsf{Ker}(\rho) \mid 4$. Il en résulte que $\#\,\mathsf{Ker}(\rho) \mid \mathsf{pgcd}(3,4) = 1$, ce qui montre que ρ est injectif. On a donc $\#\,\mathsf{Im}(\rho) = 12$, d'où $(\mathfrak{S}_4 : \mathsf{Im}(\rho)) = 2$: on a nécessairement $\mathsf{Im}(\rho) = \mathfrak{A}_4$ et ρ induit un isomorphisme $G \xrightarrow{\sim} \mathfrak{A}_4$.

Exercice 1.4.2.16. Un groupe d'ordre 300 n'est jamais simple.

Solution : Soit G un groupe d'ordre $300 = 2^2 \times 3 \times 5^2$: on a $n_5 \mid 12$ et $n_5 \equiv 1 \bmod 5$, d'où $n_5 \in \{1,6\}$. Si G est simple, alors $n_5 = 6$ (sinon l'unique 5-Sylow serait distingué) et l'action de G par conjugaison sur l'ensemble de ses 5-Sylow fournit un morphisme de groupes $\rho\colon G \to \mathfrak{S}_6$. Comme l'action est transitive, elle est non triviale donc ρ n'est pas trivial. Comme G est simple, on a donc $\mathsf{Ker}(\rho) = \{e\}$ et ρ est injectif. Cela implique que $300 \mid 6! = 720$, ce qui n'est pas : contradiction.

2 Anneaux et polynômes

2.1 Rappels sur les anneaux

2.1.1 Définitions

Définition 2.1.1.1. Un *anneau* est la donnée d'un triplet $(A, +, \cdot)$ où A est un ensemble et $+ \colon A \times A \to A$ et $\cdot \colon A \times A \to A$ sont deux lois de composition interne tels que les propriétés suivantes sont remplies :
(i) le couple $(A, +)$ est un groupe abélien ;
(ii) la loi $\cdot$ est associative, distributive (à droite et à gauche) par rapport à la loi $+$.
On note 0_A l'élément neutre pour la loi $+$. L'anneau est dit *unitaire* s'il existe un élément neutre 1_A (à droite et à gauche) pour la loi $\cdot$, *commutatif* si la loi $\cdot$ est commutative. La loi $+$ est appelée *addition* et la loi $\cdot$ *multiplication*.

Remarque 2.1.1.2. (1) Par abus, on parlera de l'anneau A au lieu de $(A, +, \cdot)$ et on omet le point pour la multiplication *i.e.* on écrit ab pour $a \cdot b$. En outre, on écrit simplement 0 et 1 au lieu de 0_A et 1_A lorsqu'aucune confusion n'est à craindre.
(2) L'anneau nul (*i.e.* réduit à $\{0\}$) est unitaire (on a alors $0 = 1$).
(3) Si A est unitaire, la commutativité de la loi $+$ résulte des autres conditions. Cela résulte de la distributivité : soient $a, b \in A$. Si on développe l'expression $(1 + 1) \cdot (a + b)$ en distribuant le premier et le second facteur, on obtient respectivement $a + a + b + b$ et $a + b + a + b$, d'où $a + b = b + a$ en simplifiant par a à gauche et b à droite.

Exemple 2.1.1.3. (1) $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ et $\mathbf{C}$.
(2) $\mathbf{Z}/n\,\mathbf{Z}$ avec $n \in \mathbf{N}$.
(3) Si K est un corps et V un K-espace vectoriel, $\mathsf{End}_K(V)$ muni de l'addition et de la composition des endomorphismes est un anneau unitaire (non commutatif si $\dim_K(V) > 1$).
(4) Si A est un anneau, l'anneau des polynômes $A[X]$ (*cf.* plus bas), l'anneau des matrices $\mathsf{M}_n(A)$.
(5) Plein d'exemples en analyse.

DANS CE QUI SUIT, TOUS LES ANNEAUX SERONT SUPPOSÉS UNITAIRES.

Remarque 2.1.1.4 (BINÔME DE NEWTON)**.** Si $a, b \in A$ commutent et $n \in \mathbf{N}$, on a :

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Il est important de supposer que $ab = ba$.

Définition 2.1.1.5 (ANNEAUX PRODUITS)**.** (i) Soient A_1 et A_2 deux anneaux. Le produit cartésien $A_1 \times A_2$ est naturellement muni d'une structure d'anneau, les lois étant données par les formules

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$$

pour tous $a_1, b_1 \in A_1$ et $a_2, b_2 \in A_2$. L'élément neutre pour l'addition (resp. la multiplication) est $(0_{A_1}, 0_{A_2})$ (resp. $1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$). Si A_1 et A_2 sont commutatifs, il en est de même de l'anneau produit $A_1 \times A_2$. Bien entendu, cette construction se généralise à un produit quelconque d'anneaux.
(ii) Cas particulier de (i) : soit I un ensemble. On note A^I (resp. $A^{(I)}$) l'ensemble des applications $I \to A$ (resp. des applications $I \to A$ qui sont nulles en dehors d'une partie finie de I). On a bien entendu $A^{(I)} \subset A^I$ avec égalité si et seulement si I est fini. Muni des lois d'addition et de multiplication « composante par composante », A^I est un anneau. Il est commutatif si A l'est.

Remarque 2.1.1.6. Lorsque I est infini, $A^{(I)}$ est un anneau non unitaire.

Définition 2.1.1.7. Soient A un anneau et $a \in A$.
(i) On dit que a est *inversible*, s'il existe $b \in A$ tel que $ab = ba = 1$. L'ensemble des éléments inversibles de A est noté $A^\times$. Muni de la restriction de la multiplication, c'est un groupe, d'élément neutre 1. Bien sûr, on a toujours $1 \in A^\times$. L'anneau A est un *corps* s'il est non nul et tous ses éléments non nuls sont inversibles *i.e.* $A^\times = A \backslash \{0\}$.
(ii) On dit que a est *diviseur de zéro* s'il existe $b \in A \backslash \{0\}$ tel que $ab = 0$ ou $ba = 0$. L'anneau A est dit *intègre* s'il n'a pas de diviseur de zéro autre que 0. En particulier, un corps est un anneau intègre. L'anneau nul n'est pas intègre.
(iii) On dit que a est *nilpotent* s'il existe $n \in \mathbf{N}_{>0}$ tel que $a^n = 0$ (en particulier, c'est un diviseur de zéro). L'anneau A est dit *réduit* s'il n'a pas d'élément nilpotent autre que 0. Bien sûr, un anneau intègre est réduit.

Exemples 2.1.1.8. (1) Les anneaux $\mathbf{Q}, \mathbf{R}$ et $\mathbf{C}$ sont des corps. Il en est de même de $\mathbf{Z}/p\,\mathbf{Z}$ lorsque p est un entier premier. L'anneau $\mathbf{Z}$ est intègre, mais ce n'est pas un corps (2 n'est pas inversible), en fait on a $\mathbf{Z}^\times = \{1, -1\}$.
(2) L'anneau $\mathbf{Z}/6\,\mathbf{Z}$ n'est pas intègre, car $\overline{2} \times \overline{3} = \overline{0}$ alors que $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$. En fait, on a $(\mathbf{Z}/6\,\mathbf{Z})^\times = \{\overline{1}, \overline{5}\}$. Par contre, $\mathbf{Z}/6\,\mathbf{Z}$ est réduit.
(3) L'anneau $\mathbf{Z}/4\,\mathbf{Z}$ n'est pas réduit, car $\overline{2}^2 = \overline{0}$ mais $\overline{2} \neq \overline{0}$.

Comme d'habitude, après avoir défini une structure algébrique, on définit la notion de morphisme entre objets possédant cette structure.

Définition 2.1.1.9. Soient A et B deux anneaux. Un *morphisme d'anneaux* de A vers B est un morphisme $f\colon A \to B$ entre les groupes additifs sous-jacents tel que

$$(\forall a, b \in A) \quad f(ab) = f(a)f(b) \text{ et } f(1_A) = 1_B.$$

Remarque 2.1.1.10. (1) Si $f\colon A \to B$ et $g\colon B \to C$ sont deux morphismes d'anneaux, l'application composée $g \circ f$ est encore un morphisme d'anneaux.
(2) L'application

$$\begin{aligned} i\colon A &\to A \times A \\ a &\mapsto (a, 0) \end{aligned}$$

n'est pas un morphisme d'anneaux, parce que $i(1_A) \neq 1_{A\times A}$.

Exemples 2.1.1.11. (1) Les inclusions $\mathbf{Z} \to \mathbf{Q}$, $\mathbf{Q} \to \mathbf{R}$, $\mathbf{R} \to \mathbf{C}$. Pour $n \in \mathbf{N}_{>1}$, la réduction modulo $n : \mathbf{Z} \to \mathbf{Z}/n\,\mathbf{Z}$.
(2) Il existe un unique morphisme d'anneaux $c_A\colon \mathbf{Z} \to A$. C'est l'application qui à $z \in \mathbf{N}$ associe $c_A(z) = 1_A + \cdots + 1_A$, z fois et telle que $c_A(z) = -c_A(-z)$ si $z \in \mathbf{Z}_{<0}$.

Définition 2.1.1.12. Soit $f\colon A \to B$ un morphisme d'anneaux. Le *noyau* $\{a \in A;\ f(a) = 0_B\}$ et l'*image* $\{f(a);\ a \in A\}$ du morphisme de groupes sous-jacent s'appelle le noyau et l'image de f et est noté $\mathsf{Ker}(f)$ et $\mathsf{Im}(f)$. Rappelons que f est injectif si et seulement si $\mathsf{Ker}(f) = \{0_A\}$. Cependant, $\mathsf{Ker}(f)$ n'est pas un sous-anneau de A.

Définition 2.1.1.13. Soient A et B deux anneaux. On dit que A est un *sous-anneau* de B si $A \subset B$ et si l'inclusion $A \hookrightarrow B$ est un morphisme d'anneaux.

Exemple 2.1.1.14. L'ensemble $\mathcal{C}^0([0,1], \mathbf{R})$ est un sous-anneau de $\mathscr{B}([0,1], \mathbf{R})$

Remarque 2.1.1.15. Pour montrer qu'un ensemble muni de deux lois de composition interne est un anneau, il est souvent judicieux de le voir comme un sous-anneau d'un anneau convenable. Par exemple, $\mathbf{Z}[i] = \{a + ib;\ a, b \in \mathbf{Z}\}$ est un sous-anneau de $\mathbf{C}$.

2.2 Idéaux et quotients

2.2.1 Définitions

Soit A un anneau.

Définition 2.2.1.1. Un *idéal à gauche* de A est un sous-groupe $I \subset A$ pour la loi $+$ tel que

$$(\forall a \in A)\ (\forall x \in I) \quad ax \in I.$$

On définit la notion d'*idéal à droite* de façon analogue. Un *idéal bilatère* est un idéal à gauche qui est aussi un idéal à droite (lorsque A est commutatif, les trois notions coïncident). Un idéal I est dit *strict* si $I \neq A$ (l'anneau A est toujours un idéal, appelé *idéal unité*).

Exemple 2.2.1.2. Les idéaux de $\mathbf{Z}$ sont les $n\,\mathbf{Z}$, avec $n \in \mathbf{N}$ (en particulier, ils coïncident avec les sous-groupes).

Exercice 2.2.1.3. Soient K un corps et V un K-espace vectoriel de dimension finie. Déterminer les idéaux à gauche, à droite et bilatère de $\mathsf{End}_K(V)$.

Proposition 2.2.1.4. Si $f\colon A \to B$ est un morphisme d'anneaux, alors $\mathsf{Ker}(f)$ est un idéal bilatère de A.

Démonstration. Bien entendu, $f\colon A \to B$ est un morphisme entre les groupes additifs sous-jacents : $\mathsf{Ker}(f)$ est un sous-groupe de A. Si $a \in A$ et $x \in \mathsf{Ker}(f)$, on a $f(ax) = f(a)f(x) = 0$, donc $ax \in \mathsf{Ker}(f)$. On a de même $xa \in \mathsf{Ker}(f)$. □

Remarque 2.2.1.5. Si $f\colon A \to B$ est un morphisme d'anneaux et $J \subset B$ un idéal à gauche (resp. à droite), alors $f^{-1}(J)$ est un idéal à gauche (resp. à droite) de A. Si I est un idéal à gauche, $f(I)$ n'est pas un idéal à gauche de B en général (sauf si f est surjectif).

Supposons maintenant A commutatif.

Définition 2.2.1.6. (i) Soit X une partie de A. L'idéal *engendré* par X est l'ensemble des combinaisons A-linéaires d'éléments de X :

$$\left\{ \sum_{i=1}^{n} a_i x_i;\ n \in \mathbf{N}, a_1, \ldots, a_n \in A, x_1, \ldots, x_n \in X \right\}.$$

Si $X = \{x_1, \ldots, x_r\}$ est fini, on note cet idéal $x_1A + \cdots + x_rA$ ou $\langle x_1, \ldots, x_r \rangle$.
(ii) On en déduit immédiatement la notion de *famille génératrice* d'un idéal (bien sûr, il n'y a pas unicité). Un idéal qui peut être engendré par un seul élément est dit *principal* et un anneau intègre dont tous les idéaux sont principaux est dit *principal*.
(iii) Un anneau est dit *nœtherien* si tout idéal est de type fini (*i.e.* admet une famille génératrice finie). C'est une propriété de finitude très importante.

Exemple 2.2.1.7. L'anneau $\mathbf{Z}$ est principal, tout comme l'anneau $\mathbf{Q}[X]$ (on va le prouver plus tard). Par contre, les anneaux $\mathbf{Q}[X,Y]$ et $\mathbf{Z}[X]$ ne sont pas principaux.

Définition 2.2.1.8. Soient A un anneau et $\{I_\lambda\}_{\lambda\in\Lambda}$ une famille d'idéaux de A. On a que

$$\bigcap_{\lambda\in\Lambda} I_\lambda \text{ et } \sum_{\lambda\in\Lambda} I_\lambda$$

sont des idéaux de A (rappelons que $\sum_{\lambda\in\Lambda} I_\lambda$ désigne l'ensemble des sommes finies $x_1+\cdots+x_r$ avec $x_i\in I_{\lambda_i}$ où $\lambda_i\in\Lambda$ pour tout $i\in\{1,\dots,r\}$). En outre, si $\Lambda=\{1,\dots,n\}$ est fini, on note $I_1I_2\cdots I_n$ l'idéal engendré par l'ensemble des produits $x_1x_2\cdots x_n$ avec $x_j\in I_j$ pour tout $j\in\{1,\dots,n\}$.

Exemple 2.2.1.9. Dans $\mathbf{Z}$, on a $6\,\mathbf{Z}\cap 10\,\mathbf{Z}=30\,\mathbf{Z}$, $6\,\mathbf{Z}+10\,\mathbf{Z}=2\,\mathbf{Z}$ et $(6\,\mathbf{Z})(10\,\mathbf{Z})=60\,\mathbf{Z}$.

Définition 2.2.1.10. Rappelons que si A est un anneau unitaire, il existe un unique morphisme unitaire $c_A\colon \mathbf{Z}\to A$. Le noyau de ce morphisme étant un idéal de $\mathbf{Z}$, il est de la forme $\mathsf{car}(A)\,\mathbf{Z}$ avec $\mathsf{car}(A)\in\mathbf{N}$. L'entier $\mathsf{car}(A)$ s'appelle la *caractéristique* de l'anneau A.

Exemple 2.2.1.11. Les corps $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ sont de caractéristique 0, tout comme l'anneau $\mathbf{Z}$. Pour $n\in\mathbf{N}_{>1}$, l'anneau $\mathbf{Z}/n\,\mathbf{Z}$ est de caractéristique n. Si A est un anneau de caractéristique n, il en est de même de l'anneau des polynômes $A[X]$.

Exercice 2.2.1.12. Un anneau fini et intègre est un corps.

Solution : Fixons $a\in A\backslash\{0\}$ et considérons le morphisme de groupes $(A,+)\to(A,+)$ tel que $x\mapsto ax$. Ce morphisme de groupes est injectif, puisque son noyau est réduit à $\{0_A\}$ par intégrité de A. Puisque A est fini, ce morphisme est nécessairement bijectif et il existe alors $x\in A$ tel que $ax=1_A$, donc tout élément a admet un inverse à gauche *i.e.* A est un corps. (Remarquons que nous n'avons pas eu besoin de supposer que A est commutatif)

2.2.2 Quotients

Soit A un anneau.

Proposition 2.2.2.1. Les relations d'équivalence sur A qui sont compatibles avec les lois d'anneaux sont des relations modulo un idéal bilatère.

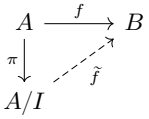
Démonstration. Soit $\mathcal{R}$ une relation d'équivalence sur A. Notons I la classe d'équivalence de l'élément neutre et $\pi\colon A\to A/\mathcal{R}$ la surjection canonique. Supposons $\mathcal{R}$ compatible aux lois d'anneaux. Comme dans la preuve de la proposition 1.1.3.6, cela implique que pour $a_1,a_2\in A$, on peut poser $[a_1]+[a_2]=[a_1+a_2]$ et $[a_1]\cdot[a_2]=[a_1a_2]$ et que ça munit l'ensemble quotient $A/\mathcal{R}$ de deux lois de composition interne qui en font un anneau, tel que π soit un morphisme d'anneaux. Cela montre que $I=\mathsf{Ker}(\pi)$ est un idéal bilatère. Si $a_1,a_2\in A$, on a alors :

$$a_1\mathcal{R}a_2\Leftrightarrow\pi(a_1)=\pi(a_2)\Leftrightarrow a_2-a_1\in\mathsf{Ker}(\pi)=I$$

ce qui montre que $\mathcal{R}$ coïncide avec la relation modulo I (à gauche ou à droite, c'est la même chose). □

Soit $I\subset A$ un idéal bilatère. Comme le groupe additif sous-jacent à A est abélien et I est un sous-groupe de A, on peut former le groupe quotient A/I. Rappelons qu'en tant qu'ensemble, il s'agit des classes $a+I$ avec $a\in A$ (on dit alors que a est un *représentant* de la classe). La loi d'addition est définie par $(a+I)+(b+I)=(a+b)+I$ (cela ne dépend pas des choix des représentants). Par ailleurs, on dispose de la *projection canonique*, c'est l'application $\pi\colon A\to A/I$ qui à l'élément $a\in A$ associe sa classe $a+I$ modulo I. C'est un morphisme surjectif de groupes, de noyau I.

Proposition 2.2.2.2. Le groupe A/I est naturellement muni d'une structure d'anneau pour laquelle la projection canonique π est un morphisme d'anneaux. L'anneau ainsi obtenu s'appelle *l'anneau quotient* de A modulo I. Le couple $(A/I,\pi)$ a la propriété universelle suivante : si $f\colon A\to B$ est un morphisme d'anneaux tel que $I\subset\mathsf{Ker}(f)$, alors il existe un unique morphisme d'anneaux $\widetilde{f}\colon A/I\to B$ tel que $f=\widetilde{f}\circ\pi$.



Démonstration. • Si $a,b\in A$ et $x,y\in I$, on a

$$(a+x)(b+y)=ab+xb+ay+xy\in ab+I$$

puisque I est un idéal bilatère. Cela montre que ab et $(a+x)(b+y)$ appartiennent à la même classe modulo I. Cela implique que la classe modulo I du produit de deux éléments de A ne dépend que de la classe modulo I de ces éléments. On peut donc définir une loi de composition interne sur A/I en posant $(a+I)(b+I)=ab+I$ pour $a,b\in A$. L'associativité, la distributivité et la commutativité de la loi ainsi obtenue se déduisent facilement des propriétés correspondantes de la multiplication de A. Par construction, on a $\pi(ab)=\pi(a)\pi(b)$, ce qui montre la première moitié de l'énoncé.

• Soit $f\colon A \to B$ un morphisme d'anneaux tel que $I \subset \mathsf{Ker}(f)$. Si $\widetilde{f}$ existe, on a nécessairement $\widetilde{f}(a+I) = f(a)$ pour tout $a \in A$, d'où l'unicité. Pour l'existence, il s'agit de vérifier qu'on peut définir une application $\widetilde{f}$ par la formule précédente, *i.e.* que $f(a)$ ne dépend que de la classe $a+I$ de a modulo I. Mais si $x \in I$, on a $x \in \mathsf{Ker}(f)$, d'où $f(a+x) = f(a)$. Le fait que l'application ainsi obtenue est un morphisme d'anneaux résulte du fait que f en est un. Enfin, pour $a \in A$, on a $(\widetilde{f} \circ \pi)(a) = \widetilde{f}(a+I) = f(a)$. □

Remarque 2.2.2.3. (1) Si A est commutatif, il en est de même de A/I.
(2) On a $I = \mathsf{Ker}(\pi\colon A \to A/I)$ et tout idéal bilatère peut être vu comme le noyau d'un morphisme d'anneaux.
(3) Si $f\colon A \to B$ est un morphisme d'anneaux, on dispose de la factorisation canonique $f = \widetilde{f} \circ \pi$ où $\widetilde{f}\colon A/\mathsf{Ker}(f) \to B$ est un morphisme injectif d'anneaux.
Si le morphisme f de départ est surjectif, le morphisme obtenu est alors un isomorphisme. C'est une façon élégante de construire des isomorphismes.

DÉSORMAIS, LES ANNEAUX SERONT TOUS SUPPOSÉS COMMUTATIFS.

Soient A un anneau et $I \subset A$ un idéal. Notons $\pi\colon A \to A/I$ la surjection canonique. Si $J \subset A$ est un idéal contenant I, on dispose de $\pi(J) = J/I$, c'est un idéal de A/I. Réciproquement, si $\overline{J} \subset A/I$ est un idéal, alors $\pi^{-1}(\overline{J})$ est un idéal de A qui contient I.

Proposition 2.2.2.4. Les applications :

$$\begin{aligned} \{\text{idéaux de } A \text{ contenant } I\} &\leftrightarrow \{\text{idéaux de } A/I\} \\ J &\mapsto \pi(J) = J/I \\ \pi^{-1}(\overline{J}) &\mapsfrom \overline{J} \end{aligned}$$

sont des bijections inverses l'une de l'autre. Par ailleurs, si $J \subset A$ est un idéal contenant I et $\overline{J} = J/I$, on a un isomorphisme naturel :

$$A/J \xrightarrow{\sim} (A/I)/\overline{J}.$$

Démonstration. Si $\overline{J} \subset A/I$ est un idéal, on a $\pi(\pi^{-1}(\overline{J})) = \overline{J}$ parce que π est surjective. Si $J \subset A$ est un idéal contenant I et $\overline{J} = J/I$, on dispose du morphisme composé

$$A \xrightarrow{\pi} A/I \to (A/I)/\overline{J}.$$

Il est surjectif, comme composé de deux surjections canoniques. Son noyau est

$$\pi^{-1}(\overline{J}) = \{a \in A;\ a + I \subset J\} = J$$

puisque $I \subset J$. En passant au quotient, cela fournit l'isomorphisme $A/J \xrightarrow{\sim} (A/I)/\overline{J}$. □

2.2.3 Le théorème des restes chinois

Soit A un anneau.

Théorème 2.2.3.1 (DES RESTES CHINOIS)**.** Soient $I_1, \dots, I_n \subset A$ des idéaux tels que pour $j \neq k$, on ait $I_j + I_k = A$. On a alors $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$. En outre, si $\pi_j\colon A \to A/I_j$ désigne la projection canonique, on a un isomorphisme naturel :

$$\begin{aligned} A/I_1 I_2 \cdots I_n &\xrightarrow{\sim} \prod_{j=1}^{n} A/I_j \\ a &\mapsto (\pi_j(a))_{1 \leqslant j \leqslant n} \end{aligned}$$

Démonstration. • On suppose $n > 1$ (sinon c'est trivial). Posons $I = I_1$ et $J = I_2 \cdots I_n$. Pour $j \in \{2, \dots, n\}$, on a $I + I_j = A$: il existe $a_j \in I$ et $b_j \in I_j$ tels que $a_j + b_j = 1$. En développant le produit, on a $(a_2+b_2)(a_3+b_3)\cdots(a_n+b_n) = 1$, donc $a + b_2 b_3 \cdots b_n = 1$ avec $a \in I$ (car a est une somme de termes qui contiennent au moins un a_j). On a donc $I + J = A$: par récurrence (si le théorème est vraie pour I, J et aussi pour $I_2, \dots, I_n$, alors il est vrai pour $I_1, \dots, I_n$), il suffit de traiter le cas $n = 2$.
• On a toujours $I_1 I_2 \subset I_1 \cap I_2$. Comme $I_1 + I_2 = A$, il existe $a_1 \in I_1$ et $a_2 \in I_2$ tels que $a_1 + a_2 = 1$. Si $x \in I_1 \cap I_2$, on a donc $x = xa_1 + xa_2$. Mais comme $x \in I_2$ et $a_1 \in I_1$, on a $xa_1 \in I_1 I_2$. De même, on a $xa_2 \in I_1 I_2$. Ainsi, $I_1 I_2 = I_1 \cap I_2$.
• Notons $\pi_1\colon A \to A/I_1$ et $\pi_2\colon A \to A/I_2$ les projections canoniques et posons

$$\begin{aligned} f\colon A &\to (A/I_1) \times (A/I_2) \\ a &\mapsto (\pi_1(a), \pi_2(a)) \end{aligned}$$

un morphisme d'anneaux. Montrons qu'il est surjectif. Soit $(x, y) \in A^2$. Posons $a = ya_1 + xa_2 \in A$. On a $a_1 \equiv 0 \bmod I_1$ et $a_1 \equiv 1 \bmod I_2$ (puisque $a_1 = 1 - a_2 \in 1 + I_2$), donc $ya_1 \equiv 0 \bmod I_1$ et $ya_1 \equiv y \bmod I_2$. De même, $xa_2 \equiv 0 \bmod I_2$ et $xa_2 \equiv x \bmod I_1$. Ainsi, $a \equiv x \bmod I_1$ et $a \equiv y \bmod I_2$ *i.e.* $f(a) = (x + I_1, y + I_2)$ d'où la surjectivité de f. Comme le noyau de f est $I_1 \cap I_2 = I_1 I_2$, l'application f induit alors un isomorphisme : $A/I_1 I_2 \xrightarrow{\sim} (A/I_1) \times (A/I_2)$. □

Exemple 2.2.3.2. Soient $a_1, \dots, a_n \in \mathbf{Z}$ des entiers non nuls deux à deux premiers entre eux (*i.e.* $a_j\,\mathbf{Z} + a_k\,\mathbf{Z} = \mathbf{Z}$ pour $j \neq k$). On a alors que l'homomorphisme canonique :

$$\mathbf{Z}/(a_1 a_2 \cdots a_n)\,\mathbf{Z} \xrightarrow{\sim} \prod_{j=1}^{n} \mathbf{Z}/a_j\,\mathbf{Z}$$

est un isomorphisme. Bien sûr, dans ce cas, c'est facile à prouver : l'injectivité résulte du lemme de Gauss et la surjectivité suit par cardinalité (les deux anneaux ont même cardinal $|a_1 a_2 \cdots a_n|$). Mais ce théorème des restes chinois sert dans bien d'autres contextes.

Exercice 2.2.3.3. Soient $a, b \in \mathbf{N}_{>0}$. Soient d et m leur pgcd et ppcm respectivement. Montrer que

$$(\mathbf{Z}/a\,\mathbf{Z}) \times (\mathbf{Z}/b\,\mathbf{Z}) \xrightarrow{\sim} (\mathbf{Z}/d\,\mathbf{Z}) \times (\mathbf{Z}/m\,\mathbf{Z}).$$

2.3 Idéaux premiers, idéaux maximaux

Définition 2.3.0.1. Soient A un anneau et $I \subsetneq A$ un idéal strict.
(i) On dit que I est *maximal* si pour tout idéal strict $J \subset A$, on a : $I \subset J \Rightarrow J = I$ (*i.e.* I est maximal pour l'inclusion parmi les idéaux stricts de A).
(ii) On dit que I est *premier* si : $(\forall (a,b) \in A^2)\ ab \in I \Rightarrow (a \in I \text{ ou } b \in I)$.

Proposition 2.3.0.2. Tout idéal maximal est premier.

Démonstration. Soit $I \subsetneq A$ un idéal maximal et $a, b \in A$ tel que $ab \in I$. Si $a \notin I$, alors $I + \langle a \rangle = A$ (par maximalité de I), donc il existe $x \in A$ et $y \in I$ tels que $y + xa = 1$. On a alors $b = xab + yb \in I$, donc I est premier. □

Exemple 2.3.0.3. Les idéaux premiers de $\mathbf{Z}$ sont $\{0\}$ et les $p\,\mathbf{Z}$ avec p premiers.

Proposition 2.3.0.4. Soient A un anneau et $I \subset A$ un idéal. On a les équivalences :
(i) A/I est un corps si et seulement si I est maximal ;
(ii) A/I est intègre si et seulement si I est premier.

Démonstration. (i) Si $a \in A$, alors $a + I$ est inversible dans A/I si et seulement s'il existe $b \in A$ tel que $ab + I = 1 + I$ *i.e.* $1 \in \langle a \rangle + I$ soit encore si et seulement si l'idéal engendré par a et I est A tout entier. Ainsi, l'anneau A/I est un corps si et seulement si pour tout $a \in A$, on a $\langle a \rangle + I = A$ (si $a \notin I$) ou $\langle a \rangle + I = I$ (si $a \in I$). Mais ceci équivaut à la maximalité de l'idéal I.
(ii) Soient $(a,b) \in A^2$, on a $(a+I)(b+I) = I$ dans A/I si et seulement si $ab + I = I$ *i.e.* si et seulement si $ab \in I$. Ainsi, l'anneau A/I est intègre si et seulement si pour tout $(a,b) \in A^2$, on a : $ab \in I \Rightarrow (a + I = I \text{ ou } b + I = I)$ *i.e.* $a \in I$ ou $b \in I$, ce qui veut précisément dire que I est premier. □

Remarque 2.3.0.5. (1) Une autre façon d'exprimer le point (i) de la proposition 2.3.0.4 est de dire qu'un anneau A est un corps si ses seuls idéaux sont $\{0\}$ et A. De ce point de vue, les corps sont les anneaux les plus simples qu'on puisse imaginer.
(2) Il résulte du point précédent que si K est un corps et $f : K \to A$ un morphisme d'anneaux, alors f est automatiquement injectif.
(3) Comme tout corps est intègre, on retrouve le fait que tout idéal maximal est premier.

Proposition 2.3.0.6. Soient A un anneau et $I \subset A$ un idéal. La bijection de la proposition 2.2.2.4 induit des bijections :

$$\{\text{idéaux premiers de } A \text{ contenant } I\} \leftrightarrow \{\text{idéaux premiers de } A/I\}$$
$$\{\text{idéaux maximaux de } A \text{ contenant } I\} \leftrightarrow \{\text{idéaux maximaux de } A/I\}.$$

Exercice 2.3.0.7. Soient $A_1, \dots, A_n$ des anneaux. Montrer que les idéaux premiers de l'anneau produit $A_1 \times \cdots \times A_n$ sont de la forme $A_1 \times \cdots \times A_{k-1} \times \mathfrak{p}_k \times A_{k+1} \times \cdots \times A_n$ où $k \in \{1, \dots, n\}$ et $\mathfrak{p}_k \subset A_k$ est un idéal premier.

Proposition 2.3.0.8. Si A est un anneau principal et I un idéal premier non nul, alors I est maximal.

Démonstration. Soit $\langle a \rangle = I \subsetneq A$ un idéal premier non nul avec $a \in A$. Soit $\langle b \rangle = J \subsetneq A$ un idéal tel que $I + J \subsetneq A$ avec $b \in A$. Il est clair que $\langle a \rangle \subset \langle b \rangle$ si et seulement s'il existe $c \in A$ tel que $a = bc$. On a alors que $bc \in I$, ce qui implique que $b \in I$ ou $c \in I$ par primalité de I, donc $b = \beta a$ avec $\beta \in A$ ou $c = \gamma a$ avec $\gamma \in A$. Supposons $c = \gamma a$, on a alors $a = bc = b\gamma a$. Puisque A est intègre, $1 = b\gamma$ donc $b \in A^\times$ et $J = \langle b \rangle = A$, ce qui est absurde. On a donc $b = \beta a$. Ainsi, $a = bc = \beta ac$, donc $1 = \beta c$ puisque A est intègre *i.e.* $\beta \in A^\times$. On a alors $\langle a \rangle = \langle b \rangle$ *i.e.* $I = J$, donc I est maximal. □

Exemple 2.3.0.9. Soient $A = \mathbf{Q}[X, Y]$ et $I = \langle X \rangle \subset A$. L'anneau $A/I \simeq \mathbf{Q}[Y]$ est intègre, mais ce n'est pas un corps : l'idéal I est donc premier non nul. La proposition précédente implique donc que A n'est pas principal.

2.3.1 Interlude : l'axiome du choix et ses avatars

Les fondements logiques des mathématiques reposent sur les axiomes de la théorie des ensembles de Zermelo-Fraenkel (dont on ignore encore si elle est consistante). L'axiome du choix est le suivant : un ensemble E d'ensembles non vides mutuellement disjoints admet une fonction de choix, c'est-à-dire une application qui à chaque $A \in E$ associe un élément de A. Il est équivalent aux propriétés suivantes :

- toute surjection possède une section ;
- tout produit d'ensemble non vides est non vide.

Cet axiome est indépendant de la théorie ZF, ce qui signifie que si ZF est consistante, il en est de même de ZFC (ZF + axiome du choix) et de ZF « non » C (ZF + négation de l'axiome du choix). Bien entendu, la quasi-totalité des gens utilisent l'axiome du choix, *i.e.* travaillent dans ZFC. Un énoncé équivalent à l'axiome du choix est le suivant.

Définition 2.3.1.1. Un ensemble partiellement ordonné $(E, \leqslant)$ est *inductif* si toute chaîne (*i.e.* partie totalement ordonnée) de E admet un majorant.

Théorème 2.3.1.2 (Zorn)**.** Tout ensemble inductif non vide admet un élément maximal.

Cet énoncé a de très nombreuses conséquences :

- tout ensemble peut être muni d'un bon ordre ;
- le théorème de la base incomplète en dimension quelconque ;
- le théorème de Tychonov (un produit d'espaces compacts et compact) ;
- le théorème de Krull (*cf.* ci-dessous) ;
- le théorème de Hahn-Banach (toute forme linéaire continue sur un sous-espace d'un espace de Banach se prolonge à tout l'espace en une forme linéaire de même norme) ;
- le paradoxe de Banach-Tarski ;
- l'existence de parties de $\mathbf{R}$ non mesurables au sens de Lebesgue ;

et bien d'autres...

Théorème 2.3.1.3 (Krull)**.** Soient A un anneau et $I \subsetneq A$ un idéal strict. Il existe alors un idéal maximal $\mathfrak{m} \subset A$ tel que $I \subset \mathfrak{m}$. En particulier, tout anneau admet au moins un idéal maximal.

Démonstration. Considérons $\mathscr{E} = \{\text{idéaux } J \subsetneq A \text{ qui contiennent } I\}$. Cet ensemble est non vide puisque $I \in \mathscr{E}$. On ordonne $\mathscr{E}$ par l'inclusion *i.e.*

$$J_1 \leqslant J_2 \Leftrightarrow J_1 \subset J_2.$$

Montrons que $(\mathscr{E}, \leqslant)$ est inductif. Soit $(J_\lambda)_{\lambda\in\Lambda}$ une chaîne dans $(\mathscr{E}, \leqslant)$. Posons $J = \bigcup_{\lambda\in\Lambda} J_\lambda \subset A$. C'est un idéal de A. Soit $x, y \in J$ et $a \in A$. Il existe $\lambda, \mu \in \Lambda$ tel que $x \in J_\lambda$ et $y \in J_\mu$. Par hypothèse, $J_\lambda \subset J_\mu$ ou $J_\mu \subset J_\lambda$. Si $J_\lambda \subset J_\mu$, on a $x \in J_\mu$ et comme $y \in J_\mu$, alors $x + ay \in J_\mu \subset J$. De même, si $J_\mu \subset J_\lambda$, on a $x + ay \in J$. Si $J = A$, on a $1 \in J$, donc il existe $\lambda \in \Lambda$ tel que $1 \in J_\lambda$ *i.e.* il existe $\lambda \in \Lambda$ tel que $J_\lambda = A$, ce qui est absurde. On a donc $J \in \mathscr{E}$ et J est un majorant de $(J_\lambda)_{\lambda\in\Lambda}$. D'après Zorn, $\mathscr{E}$ contient un élément maximal $\mathfrak{m}$. Soit $I \subset \mathfrak{m} \subsetneq A$. Par maximalité, $\mathfrak{m}$ est un idéal maximal de A. □

Exercice 2.3.1.4. (1) Soient $f\colon A \to B$ un morphisme d'anneaux et $J \subset B$ un idéal premier. Montrer que $f^{-1}(J)$ est un idéal premier de A. Est-ce encore vrai si on remplace « premier » par « maximal » ?
(2) Soit $I \subsetneq A$ un idéal. Montrer que I est maximal si et seulement si pour tout $a \in A\backslash I$, il existe $b \in A$ tel que $1 - ab \in I$.
(3) Un anneau dans lequel tout idéal strict est premier est un corps.
(4) Soient K un corps et X un ensemble fini. Quels sont les idéaux maximaux de $\mathscr{F}(X, K)$?

2.3.2 Applications : construction de R et de C

Le corps $\mathbf{Q}$ est muni d'une relation d'ordre total $\leqslant$ (si $x = \frac{a}{b}$ et $y = \frac{c}{d}$ avec $a, c \in \mathbf{Z}$ et $b, d \in \mathbf{N}_{>0}$, on a $x \leqslant y$ si et seulement si $ad \leqslant cb$ dans $\mathbf{Z}$). Cette relation est compatible avec l'ordre : si $x \leqslant y$ et $z \in \mathbf{Q}$, on a $x + z \leqslant y + z$ et si en outre $z \geqslant 0$, on a $xz \leqslant yz$. À partir de là, on peut définir la valeur absolue d'un élément $x \in \mathbf{Q}$: on a $|x| = \max\{x, -x\}$ et on peut commencer à faire de la topologie.

Définition 2.3.2.1. Rappelons qu'étant donné un espace métrique (X, d), une suite $(x_n)_{n\in\mathbf{N}}$ à valeurs dans X est dite de *Cauchy* si pour tout $\varepsilon \in \mathbf{Q}_{>0}$, il existe $N \in \mathbf{N}$ tel que pour $n, m \geqslant N$, on ait $d(x_n, x_m) < \varepsilon$. Toute suite convergente est de Cauchy, mais la réciproque est fausse en général. On dit que (X, d) est *complet* si ses suites de Cauchy convergent dans X.

L'espace métrique $(\mathbf{Q}, |\cdot|)$ n'est pas complet (il existe une suite $(x_n)_{n\in\mathbf{N}}$ de rationnels positifs telle que $\lim_{n\to\infty} x_n^2 = 2$, elle est de Cauchy mais ne converge pas, parce que 2 n'est pas un carré dans $\mathbf{Q}$). Pour pouvoir faire de l'analyse, on a besoin de compléter $\mathbf{Q}$. On procède de la façon suivante : notons A l'ensemble des suites de Cauchy à valeurs dans $\mathbf{Q}$. C'est un sous-anneau de l'anneau produit $\mathbf{Q}^{\mathbf{N}}$ (l'addition et la multiplication se font composante par composante). On dispose du morphisme $\iota\colon \mathbf{Q} \to A$ qui à $x \in \mathbf{Q}$ associe la suite constante égale à x. Notons $\mathfrak{m} \subset \mathbf{Q}^{\mathbf{N}}$ l'ensemble des suites qui tendent vers 0. C'est un idéal de A : on pose

$$\mathbf{R} := A/\mathfrak{m}$$

et on note $\pi\colon A \to \mathbf{R}$ la surjection canonique.

Théorème 2.3.2.2. (i) L'idéal $\mathfrak{m} \subset A$ est maximal, donc $\mathbf{R}$ est un corps. Le composé $\pi \circ \iota \colon \mathbf{Q} \to \mathbf{R}$ est injectif : il permet de voir $\mathbf{Q}$ comme un sous-corps de $\mathbf{R}$.
(ii) Si $(x_n)_{n\in\mathbf{N}}, (y_n)_{n\in\mathbf{N}} \in A$ ont pour images x et y dans $\mathbf{R}$, on écrit $x \leqslant y$ si $x = y$ ou s'il existe $\varepsilon \in \mathbf{Q}_{>0}$ tel que $x_n + \varepsilon \leqslant y_n$ pour $n \in \mathbf{N}_{>0}$. Cela définit une relation d'ordre total sur $\mathbf{R}$, qui prolonge celle sur $\mathbf{Q}$. Cela permet en particulier de définir la valeur absolue $|\cdot|$ sur $\mathbf{R}$ (qui prolonge celle sur $\mathbf{Q}$).
(iii) L'espace métrique $(\mathbf{R}, |\cdot|)$ est complet.
(iv) (Propriété universelle). Si $(K, |\cdot|)$ est un corps valué complet contenant $\mathbf{Q}$ et dont la valeur absolue $|\cdot|$ induit la valeur absolue « habituelle » sur $\mathbf{Q}$, alors il existe un unique morphisme de corps valué $\mathbf{R} \to K$.

Remarque 2.3.2.3. Le corps ordonné $\mathbf{R}$ a la propriété de la borne supérieure. En effet, soit $E \subset \mathbf{R}$ une partie non vide et majorée. Soient $x \in E$ et $M \in \mathbf{R}$ un majorant de E. On construit par dichotomie des suites $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\in\mathbf{N}}$ de réels tels que la suite $(x_n)_{n\in\mathbf{N}}$ soit croissante, $(y_n)_{n\in\mathbf{N}}$ décroissante et $x_n \in E$ et y_n est un majorant de E pour tout $n \in \mathbf{N}$. On procède de la façon suivante. On pose $x_0 = x$ et $y_0 = M$. Si $x_0, \dots, x_n$ et $y_0, \dots, y_n$ sont construits, on pose

$$(x_{n+1}, y_{n+1}) = \begin{cases} (x_n, \frac{x_n+y_n}{2}) & \text{si } \frac{x_n+y_n}{2} \text{ est un majorant de } E \\ (\frac{x_n+y_n}{2}, y_n) & \text{sinon} \end{cases}$$

Les suites $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\in\mathbf{N}}$ sont adjacentes : elles sont en particulier de Cauchy. Elles convergent donc dans $\mathbf{R}$ (par complétude) vers une limite commune ℓ, qui est la borne supérieure de E.

Le corps $\mathbf{R}$ est gros et sympathique, mais il a un défaut : certains polynômes non constants n'ont pas de racine (du fait que c'est un corps ordonné, les nombres négatifs ne sont pas des carrés). On pose donc

$$\mathbf{C} = \mathbf{R}[X]/\langle X^2 + 1\rangle.$$

C'est un corps parce que $X^2 + 1$ est irréductible dans $\mathbf{R}[X]$: on l'appelle le corps des *nombres complexes*. Si on note i l'image de X dans le quotient, on a $\mathbf{C} = \mathbf{R} \oplus i\mathbf{R}$ (comme $\mathbf{R}$-espace vectoriel), ce qui implique que $\mathbf{C}$ est complet et $i^2 = -1$. Dans $\mathbf{C}$, on peut donc extraire les racines carrées des réels négatifs et plus généralement, de tout nombre complexe. Les formules bien connues montrent alors que tout trinômes du second degré à coefficients dans $\mathbf{C}$ admet une racine. En fait on a bien mieux : tout polynôme à coefficient dans $\mathbf{C}$ est scindé. C'est le théorème de d'Alembert-Gauss (*cf.* chapitre 3). Le corps ainsi construit a donc de bonnes propriétés algébriques et topologiques.

2.4 Anneaux principaux, anneaux factoriels

Dans toute cette section, A désigne un anneau intègre.

2.4.1 Définitions

Définition 2.4.1.1. Soient $a, b \in A\backslash\{0\}$. On dit que b *divise* a et on note $b \mid a$ s'il existe $c \in A$ tel que $a = bc$ (on dit aussi que b est un *diviseur* de a et que a est un *multiple* de b). Cela équivaut à $\langle a\rangle \subset \langle b\rangle$ (on note $b \nmid a$ dans le cas contraire).

Remarque 2.4.1.2. Cette relation d'ordre n'est pas totale en général. Par exemple, sur $\mathbf{Z}$, c'est la relation de divisibilité habituelle. On a $2 \mid 6$, mais on n'a pas de relation de divisibilité entre 2 et 3.

Définition 2.4.1.3. Soient $a, b \in A\backslash\{0\}$. On dit que a et b sont *associés* si $a \mid b$ et $b \mid a$.

Comme A est intègre, a et b sont associés si et seulement s'il existe $u \in A^\times$ tel que $b = ua$, soit encore si et seulement si $\langle a\rangle = \langle b\rangle$. Il est immédiat que la relation « être associés » est une relation d'équivalence (les classes d'équivalence sont les parties de la forme $\langle a\rangle^\times$ pour $a \in A\backslash\{0\}$) : notons la $\sim$. La relation de divisibilité munit $(A\backslash\{0\})/\sim$ d'une relation d'ordre.

Définition 2.4.1.4. Soit $\pi \in A\backslash\{0\}$.
(i) On dit que π est *irréductible* dans A si $\pi \notin A^\times$ et

$$(\forall a, b \in A)\ (\pi = ab \Rightarrow (a \in A^\times \text{ ou } b \in A^\times))$$

(les seuls diviseurs de π sont les unités et les éléments associés à π).
(ii) On dit que π est *premier* si l'idéal principal $\langle\pi\rangle$ est premier.

Remarque 2.4.1.5. Par convention, 0 n'est pas premier alors que l'idéal nul l'est (rappelons qu'on a supposé A intègre).

Proposition 2.4.1.6. Un élément premier est irréductible.

Démonstration. Supposons π premier et $\pi = ab$ avec $a, b \in A$. Par définition, on a : $ab \in \langle\pi\rangle \Rightarrow (a \in \langle\pi\rangle$ ou $b \in \langle\pi\rangle)$. Supposons $a \in \langle\pi\rangle$, il existe $\alpha \in A$ tel que $a = \pi\alpha$, donc $\pi = ab = \pi\alpha b$ *i.e.* $1 = \alpha b$ (car A intègre et $\pi \neq 0$), d'où $b \in A^\times$. □

Remarque 2.4.1.7. La réciproque est fausse en général.

Exemple 2.4.1.8. Soit $A = \mathbf{Z}[\sqrt{-5}] = \{x + y\sqrt{-5};\ x, y \in \mathbf{Z}\}$. C'est un sous-anneau de $\mathbf{C}$. On dispose du morphisme d'anneaux $f\colon \mathbf{Z}[T] \to \mathbf{C}$ qui envoie T sur $\sqrt{-5}$. On a $\mathsf{Im}(f) = A$ et $T^2 + 5 \in \mathsf{Ker}(f)$. Soient $P(T) \in \mathsf{Ker}(f)$ et $P(T) = (T^2+5)Q(T) + x + yT$ avec $x, y \in \mathbf{Z}$ la division euclidienne de $P(T)$ par T^2+5 dans $\mathbf{Z}[T]$. On a $0 = f(P(T)) = x + y\sqrt{-5}$ de sorte que $x^2 = -5y^2$, ce qui implique $x = y = 0$ et donc $P(T) \in \langle T^2 + 5\rangle$. Il en résulte que $\mathsf{Ker}(f) = \langle T^2 + 5\rangle$ et que f induit un isomorphisme

$$\mathbf{Z}[T]/\langle T^2 + 5\rangle \xrightarrow{\sim} A.$$

On a alors $A/2A \xrightarrow{\sim} (\mathbf{Z}/2\,\mathbf{Z})[T]/\langle T^2 + 5\rangle = (\mathbf{Z}/2\,\mathbf{Z})[T]/\langle T + 1\rangle^2$, ce qui montre que $A/2A$ n'est pas réduit, donc pas intègre : l'élément 2 n'est pas premier dans A. Montrons qu'il est néanmoins irréductible. Posons $z = x + y\sqrt{-5}$ et introduisons l'application

$$\begin{aligned} N\colon A &\to \mathbf{N} \\ z &\mapsto |z|^2 = x^2 + 5y^2 \end{aligned}$$

Si $z_1, z_2 \in A$, on a $N(z_1 z_2) = N(z_1)N(z_2)$. Supposons $2 = ab$ avec $a, b \in A$: on a donc $4 = N(2) = N(a)N(b)$. Cela implique que $N(a), N(b) \in \{1, 2, 4\}$. L'équation $x^2 + 5y^2 = 2$ n'a pas de solution dans $\mathbf{Z}^2$: on a nécessairement $N(a) = 1$ ou $N(b) = 1$, *i.e.* $a \in A^\times$ ou $b \in A^\times$ (si $a = x + y\sqrt{-5} \in A$ vérifie $N(a) = 1$, alors $a \in A^\times$ et $a^{-1} = \overline{a} = x - y\sqrt{-5} \in A$).

Exercice 2.4.1.9. (1) Soient K un corps, T une indéterminée et $A = K + T^2K[T] \subset K[T]$ (on a vu plus haut que $K[X, Y]/\langle Y^2 - X^3\rangle \xrightarrow{\sim} A$). Montrer que T^2 est irréductible mais pas premier dans A.
(2) Soient $a, b \in A$ tels que $a \in A^\times$ ou bien a irréductible et a ne divise pas b. Montrer que $aX + b$ est irréductible dans $A[X]$.

2.4.2 Anneaux factoriels

Les éléments irréductibles sont donc ceux qui ne peuvent s'exprimer comme un produit non trivial, *i.e.* ce sont les « atomes » pour la multiplication.

Les anneaux (intègres) dans lesquels tout élément non nul peut se décomposer de façon « unique » en produit d'éléments irréductibles sont particulièrement agréables.

Définition 2.4.2.1. Soit $a \in A\backslash\{0\}$. Une *factorisation en produit d'éléments irréductibles* de a est une écriture de a sous la forme

$$a = \pi_1 \cdots \pi_r$$

avec $\pi_1, \ldots, \pi_r \in A$ irréductibles. On dit qu'une telle décomposition est unique si pour toute autre factorisation $a = p_1 \cdots p_s$ avec $p_1, \ldots, p_s \in A$ irréductibles, alors $r = s$ et quitte à renuméroter, on a $\langle \pi_i\rangle = \langle p_i\rangle$ (*i.e.* π_i et p_i sont associés) pour tout $i \in \{1, \ldots, r\}$.
On dit que A est *factoriel* si tout élément non nul admet une unique factorisation en produit d'éléments irréductibles.

Remarque 2.4.2.2. Par convention, tout élément inversible admet une unique factorisation en produit d'éléments irréductibles.

Dans la pratique, si A est factoriel, on se fixe une famille de représentants $\mathbf{P} = \{\pi_\lambda\}_{\lambda\in\Lambda}$ des classes des éléments irréductibles modulo la relation « être associé ». Tout élément $a \in A\backslash\{0\}$ s'écrit alors de façon unique

$$a = u \prod_{\lambda\in\Lambda} \pi_\lambda^{n_\lambda}$$

avec $u \in A^\times$ et $(n_\lambda)_{\lambda\in\Lambda}$ une famille d'entiers presque tous nuls (*i.e.* tous nuls sauf un nombre fini).

Définition 2.4.2.3. Soit π un élément irréductible de A. Il existe un unique $\lambda \in \Lambda$ tel que $\langle \pi\rangle = \langle \pi_\lambda\rangle$. La multiplicité n_λ s'appelle la *valuation* de a en π. On la note $v_\pi(a)$. On pose $v_\pi(0) = +\infty$.

Proposition 2.4.2.4 (Propriétés des valuations)**.** Soient $a, b \in A$. On a :
(i) d'une part, $v_\pi(ab) = v_\pi(a) + v_\pi(b)$ et d'autre part, $v_\pi(a + b) \geqslant \min\{v_\pi(a), v_\pi(b)\}$ (avec égalité si $v_\pi(a) \neq v_\pi(b)$) pour tout $\pi \in A$ irréductible ;
(ii) $a \mid b$ si et seulement si pour tout $\pi \in A$ irréductible, on a $v_\pi(a) \leqslant v_\pi(b)$;
(iii) $a \in A^\times$ si et seulement si pour tout $\pi \in A$ irréductible, on a $v_\pi(a) = 0$.

Démonstration. Cela résulte immédiatement des définitions et de l'unicité de la factorisation en produit d'éléments irréductibles. □

Exemple 2.4.2.5. (1) Un corps est factoriel (tout élément non nul est inversible).
(2) On sait (mais on va le redémontrer plus loin) que l'anneau $\mathbf{Z}$ est factoriel (les nombres premiers étant un système de représentants des éléments irréductibles). Il en est de même de $A[X]$ si A est factoriel (théorème de transfert, comme vu plus loin).
(3) Le sous-anneau $\mathbf{Z}[\sqrt{-5}]$ de $\mathbf{C}$ n'est pas factoriel, car $2, 3, 1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ sont irréductibles, les unités sont ± 1, mais $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$: on n'a pas unicité de la décomposition de 6 (exercice). De même, si K est un corps et T une indéterminée, le sous-anneau $K + T^2K[T] \subset K[T]$ n'est pas factoriel (parce que $(T^2)^3 = T^6 = (T^3)^2$, exercice).

Proposition 2.4.2.6. Supposons A factoriel. Si $\pi \in A$, alors π est irréductible si et seulement si π est premier, *i.e.* si et seulement si on a,

$$(\forall (a,b) \in A^2) \quad \pi \mid ab \Rightarrow (\pi \mid a \text{ ou } \pi \mid b).$$

Démonstration. Supposons π irréductible et $\pi \mid ab$, on a $v_\pi(a) + v_\pi(b) = v_\pi(ab) \geqslant 1$ et donc $v_\pi(a) \geqslant 1$ ou $v_\pi(b) \geqslant 1$ *i.e.* $\pi \mid a$ ou $\pi \mid b$. La réciproque est la proposition 2.4.1.6. □

Exemple 2.4.2.7. On a vu que $\mathbf{Z}[\sqrt{-5}]$ et $K+T^2K[T]$ (avec K un corps et T une indéterminée) contiennent des éléments irréductibles non premiers : cela redémontre le fait qu'ils ne sont pas factoriels.

L'énoncé qui suit montre que dans la définition d'un anneau factoriel, l'unicité résulte de la condition « irréductible $\Rightarrow$ premier ».

Proposition 2.4.2.8. L'anneau A est factoriel si et seulement si tout élément non nul de A admet une factorisation en produit d'éléments irréductibles et si tout élément irréductible est premier.

Remarque 2.4.2.9. Lorsque A est nœthérien, il admet une factorisation en produits d'éléments irréductibles.

Démonstration. On sait déjà que si A est factoriel, alors tout éléments irréductible est premier (proposition 2.4.2.6). Réciproquement, supposons que tout élément admet une factorisation en produit d'éléments irréductibles et que tout élément irréductible est premier : il s'agit de prouver l'unicité. Supposons donc qu'on a une égalité d'idéaux $\langle a \rangle = \pi_1 \cdots \pi_r A = p_1 \cdots p_s A$ avec $\pi_1, \ldots, \pi_r, p_1, \ldots, p_s$ irréductibles : il s'agit de montrer que $r = s$ et que quitte à renuméroter, on a $\pi_i A = p_i A$. Quitte à échanger les deux écritures, on peut supposer que $r \leqslant s$: on procède par récurrence sur r. Si $r = 0$, alors $a \in A^\times$, ce qui implique $s = 0$. Supposons $r > 0$. On a $\pi_r \mid p_1 \cdots p_s$: comme π_r est premier, il existe $i \in \{1, \ldots, s\}$ tel que $\pi_r \mid p_i$ et donc $\pi_r A = p_i A$ vu que p_i est irréductible. Quitte à renuméroter, on peut supposer que $i = s$ et on a $\pi_1 \cdots p_{r-1} A = p_1 \cdots p_{s-1} A$ et l'hypothèse de récurrence permet de conclure. □

2.4.3 Pgcd, ppcm

Supposons A factoriel.

Définition 2.4.3.1. Soient $a, b \in A$. On appelle *pgcd* (plus grand commun diviseur) -resp. *ppcm* (plus petit commun multiple)- de a et b un plus grand minorant -resp. un plus petit majorant- de $\{a, b\}$ pour la relation de divisibilité. On les note $\mathsf{pgcd}(a,b)$ et $\mathsf{ppcm}(a,b)$ respectivement. On dit que a et b sont *premiers entre eux* si $\mathsf{pgcd}(a,b) = 1$.

Remarque 2.4.3.2. (1) Rigoureusement, $\mathsf{pgcd}(a,b)$ et $\mathsf{ppcm}(a,b)$ sont des classes d'équivalence pour la relation « être associé ». On commettra systématiquement l'abus de noter de la même façon des représentants de ces classes. Dans $\mathbf{Z}$ par exemple, on écrira $\mathsf{pgcd}(6,10) = 2$ au lieu de $\mathsf{pgcd}(6,10) = \{\pm 2\}$. Dans ce qui suit, des égalités impliquant des pgcd et des ppcm doivent donc être comprises à multiplication par une unité près.
(2) Si $a \in A$, on a $\mathsf{pgcd}(a,0) = a$ et $\mathsf{ppcm}(a,0) = 0$.

Comme plus haut, fixons une famille de représentants $\mathbf{P} = \{\pi_\lambda\}_{\lambda \in \Lambda}$ des classes des éléments irréductibles modulo la relation « être associé ». Soient $a, b \in A\backslash\{0\}$. L'anneau A étant factoriel, il existe $u, v \in A^\times$ et des familles $(n_\lambda)_{\lambda\in\Lambda}$ et $(m_\lambda)_{\lambda\in\Lambda}$ dans $\mathbf{N}^{(\Lambda)}$ telles que les factorisations en produits d'éléments irréductibles de a et b soient

$$a = u \prod_{\lambda\in\Lambda} \pi_\lambda^{n_\lambda} \qquad b = v \prod_{\lambda\in\Lambda} \pi_\lambda^{m_\lambda}$$

alors on a

$$\mathsf{pgcd}(a,b) = \prod_{\lambda\in\Lambda} \pi_\lambda^{\min\{n_\lambda, m_\lambda\}} \qquad \mathsf{pgcd}(a,b) = \prod_{\lambda\in\Lambda} \pi_\lambda^{\max\{n_\lambda, m_\lambda\}}.$$

En d'autres termes, pour tout $\pi \in A$ irréductible, on a

$$v_\pi(\mathsf{pgcd}(a,b)) = \min\{v_\pi(a), v_\pi(b)\}$$
$$v_\pi(\mathsf{ppcm}(a,b)) = \max\{v_\pi(a), v_\pi(b)\}.$$

On remarque qu'on a $\mathsf{pgcd}(a,b)\,\mathsf{ppcm}(a,b) = ab$.

Remarque 2.4.3.3. (1) Ce qui précède montre l'existence du pgcd et du ppcm dans un anneau factoriel. Les notions existent dans un anneau quelconque, mais en général, le pgcd et le pccm n'existent pas.
(2) Par induction, on peut facilement étendre la définition et parler du pgcd et du ppcm d'une famille finie d'éléments non nuls.

Définition 2.4.3.4. Si $a, b \in A$, il existe $u, v \in A$ tels que $au + bv = d$: une telle égalité s'appelle *relation de Bézout*. Bien entendu, il n'y a pas unicité en général.

Proposition 2.4.3.5 (Lemme de Gauss)**.** Soient $a, b, c \in A\backslash\{0\}$ tels que $\mathsf{pgcd}(a,b) = 1$. Si $a \mid bc$, alors $a \mid c$.

Démonstration. On donnera ici deux démonstrations du lemme. Une par la relation de Bézout et une avec les valuations.
• Par la relation de Bézout, il existe $u, v \in A$ tel que $1 = au + bv$. Ainsi, on a $c = acu + bcv$, mais $acu, bcv \in \langle a \rangle$, donc $c \in \langle a \rangle$ *i.e.* $a \mid c$.
• Si $\pi \in A$ est irréductible et divise a, on a $v_\pi(b) = 0$ vu que $\pi \nmid b$ (car a et b sont premiers entre eux). On a donc $v_\pi(a) \leqslant v_\pi(bc) = v_\pi(c)$. Comme c'est vrai pour tout π premier divisant a, on a $a \mid c$. □

Exercice 2.4.3.6. Soient A un anneau factoriel et $a, b, c \in A$. Montrer que

$$\mathsf{pgcd}(a,b,c) = \mathsf{pgcd}(a, \mathsf{pgcd}(b,c)).$$

2.4.4 Anneaux principaux

Dans ce numéro, on suppose que A est principal.

Lemme 2.4.4.1. Soit $a \in A$. Les conditions suivantes sont équivalentes :
(i) a est irréductible ;
(ii) $\langle a \rangle$ est un idéal maximal ;
(iii) a est premier.

Démonstration. (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) est évident. Il reste donc à montrer (i) $\Rightarrow$ (ii). Supposons a irréductible : on a $\langle a \rangle \neq A$. Soit $I \subset A$ un idéal propre tel que $\langle a \rangle \subset I$. Il existe $b \in A$ tel que $I = \langle b \rangle$ et on a $b \mid a$. Comme a est irréductible et $b \notin A^\times$ (parce que $I \neq A$), cela implique que a et b sont associés, *i.e.* que $I = \langle a \rangle$. Cela montre que $\langle a \rangle$ est maximal. □

Remarque 2.4.4.2. On retrouve la proposition 2.3.0.8.

Lemme 2.4.4.3. Toute suite croissante d'idéaux de A est stationnaire.

Démonstration. Soit $(I_n)_n$ une suite croissante d'idéaux de A. Posons $I = \bigcup_{n \in \mathbf{N}} I_n$, c'est un idéal de A car $(I_n)_n$ est croissante (ce n'est rien d'autre que la somme des I_n). L'anneau A étant principal, il existe $a \in A$ tel que $I = \langle a \rangle$. Il existe donc $n_0 \in \mathbf{N}$ tel que $a \in I_{n_0}$. Les inclusions $\langle a \rangle \subset I_{n_0} \subset I = \langle a \rangle$ sont donc des égalités et la suite $(I_n)_{n \in \mathbf{N}}$ est stationnaire à partir de n_0. □

Proposition 2.4.4.4. Tout anneau principal est factoriel.

Démonstration. D'après la proposition 2.4.2.8 et le lemme 2.4.4.1, il suffit de montrer que tout élément $a \in A\backslash\{0\}$ admet une factorisation en produit d'éléments irréductibles. Si a est inversible, on a fini. Dans le cas contraire, l'idéal $\langle a \rangle$ est strict : il est contenu dans un idéal maximal. D'après le lemme 2.4.4.1, il existe $\pi_1 \in A$ irréductible tel que $\langle a \rangle \subset \pi_1 A$: on peut écrire $a = \pi_1 a_1$ avec $a_1 \in A\backslash\{0\}$. En itérant ce qui précède, on construit des suites $\pi_1, \dots, \pi_n$ et $a_1, \dots, a_n$ telles que $a_{k-1} = \pi_k a_k$ pour tout $k \in \{1, \dots, n\}$ (avec la convention $a_0 = a$). Si on pouvait continuer indéfiniment, cela fournirait une suite strictement croissante d'idéaux $(a_k A)_{k \in \mathbf{N}}$, contredisant le lemme précédent : le processus s'arrête en un nombre fini d'étapes, *i.e.* il existe $n \in \mathbf{N}$ tel que $a_n \in A^\times$. L'écriture $a = \pi_1 \cdots \pi_n a_n$ est une factorisation en produit d'éléments irréductibles. □

Remarque 2.4.4.5. Si A est un anneau principal, on a une caractérisation importante du pgcd et du ppcm de deux éléments $a, b \in A$. On a $\mathsf{pgcd}(a,b)A = \langle a, b \rangle$ et $\mathsf{ppcm}(a,b)A = \langle a \rangle \cap \langle b \rangle$. Montrons-le pour le pgcd (la preuve pour le ppcm est analogue). Comme A est principal, il existe $d \in A$ tel que $\langle a, b \rangle = \langle d \rangle$. Comme $x \in A$ divise a et b si et seulement si $\langle a \rangle \subset \langle x \rangle$ et $\langle b \rangle \subset \langle x \rangle$ *i.e.* $\langle d \rangle \subset \langle x \rangle$, on a bien $\mathsf{pgcd}(a,b) = d$. En particulier, si $a, b \in A$, il existe $u, v \in A$ tel que $au + bv = d$ (relation de Bézout).
Il ne faut pas croire que cette caractérisation est valable dans tout anneau factoriel. Par exemple, on peut montrer que $\mathbf{Q}[X,Y]$ est factoriel. Comme X et Y sont irréductibles et premiers entre eux, on a $\mathsf{pgcd}(X,Y) = 1$, bien que $\langle X, Y \rangle \neq \mathbf{Q}[X,Y]$ (c'est l'idéal des polynômes qui s'annulent en $(0,0)$). Bien sûr, cela vient du fait que l'anneau $\mathbf{Q}[X,Y]$ n'est pas principal.

Exemple 2.4.4.6. Si K est un corps et $n \in \mathbf{N}_{>1}$, l'anneau $K[X_1, \dots, X_n]$ est factoriel mais pas principal. De même, l'anneau $\mathbf{Z}[X]$ est factoriel mais pas principal (l'idéal engendré par 2 et X n'est pas principal).

Exercice 2.4.4.7. Soit A un anneau factoriel tel que pour tout $a, b \in A$, l'idéal $\langle a, b \rangle$ est principal. Montrer que A est principal.

2.4.5 Anneaux euclidiens

Ici, A est un anneau intègre.

Définition 2.4.5.1. L'anneau A est dit *euclidien* s'il existe une application $\phi\colon A\backslash\{0\} \to \mathbf{N}$ telle que pour tout $(a,b) \in A \times A\backslash\{0\}$, il existe $q, r \in A$ tels que

$$a = bq + r \text{ et } (r = 0 \text{ ou } \phi(r) < \phi(b)).$$

Une telle application ϕ s'appelle alors un *stathme euclidien*. Une écriture $a = bq + r$ s'appelle une *division euclidienne* de a par b, l'élément q s'appelle alors « le » *quotient* et r « le » *reste* de la division.

Remarque 2.4.5.2. (1) Si A est un anneau euclidien, il n'y a pas unicité d'un stathme euclidien sur A. En outre, on ne requiert par l'unicité du quotient et du reste.
(2) Supposons A euclidien et soit $\phi\colon A\backslash\{0\} \to \mathbf{N}$ un stathme euclidien. Pour $a \in A\backslash\{0\}$, posons

$$\psi(a) = \min_{x \in A\backslash\{0\}} \phi(ax).$$

L'application $\psi\colon A\backslash\{0\} \to \mathbf{N}$ est alors un stathme euclidien sur A qui vérifie en outre « $a \mid b \Rightarrow \psi(a) \leqslant \psi(b)$ » (exercice).

Exemples 2.4.5.3. (1) Tout corps est un anneau euclidien. L'anneau $\mathbf{Z}$ est euclidien, avec le stathme donné par $\phi(a) = |a|$ (valeur absolue). Dans ce cas, la division est la division euclidienne habituelle (on a unicité -au signe près- dans ce cas). Si K est un corps, l'anneau de polynômes $K[X]$ est euclidien, avec le stathme donné par $\phi(P) = \deg(P)$. Là encore, on a la division euclidienne habituelle et elle est unique.
(2) L'anneau $\mathbf{Z}[i] = \{a + ib\}_{a,b\in\mathbf{Z}} \subset \mathbf{C}$ des entiers de Gauss est euclidien, muni du stathme $\phi(a + ib) = a^2 + b^2$ (exercice).

Proposition 2.4.5.4. Tout anneau euclidien est principal.

Démonstration. Soient A un anneau euclidien, $\phi\colon A\backslash\{0\} \to \mathbf{N}$ un stathme euclidien et $I \subset A$ un idéal. Montrons que I est principal. On peut supposer $I \neq 0$. Dans ce cas, $\phi(I\backslash\{0\})$ est une partie non vide de $\mathbf{N}$, elle admet donc un plus petit élément : soit $b \in I\backslash\{0\}$ un élément tel que $\phi(b)$ soit minimal. On a bien sûr $\langle b\rangle \subset I$. Réciproquement, soit $a \in I$. Il existe $q, r \in A$ tels que $a = qb + r$ et $r = 0$ ou $\phi(r) < \phi(b)$. Supposons $r \neq 0$: on a $\phi(r) < \phi(b)$. Mais $r = a - qb \in I$ et comme $r \neq 0$, on a $\phi(b) \leqslant \phi(r)$ par minimalité de $\phi(b)$, ce qui est contradictoire. On a donc en fait $r = 0$ et $a = qb \in \langle b\rangle$. Ainsi, $\langle b\rangle$ est principal. □

On a donc les implications :

$$\boxed{\text{corps} \Rightarrow \text{euclidien} \Rightarrow \text{principal} \Rightarrow \text{factoriel} \Rightarrow \text{intègre}}$$

et la remarque suivante.

Remarque 2.4.5.5. Il existe des anneaux qui sont principaux, mais pas euclidiens. Par exemple, $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right] \subset \mathbf{C}$ est principal mais pas euclidien. Ainsi, les implications qui précèdent ont toutes des réciproques fausses.

Corollaire 2.4.5.6. Soit K un corps, les anneaux $\mathbf{Z}$ et $K[X]$ sont principaux, donc factoriels.

Remarque 2.4.5.7. Dans les anneaux euclidiens, on dispose de l'algorithme d'Euclide (étendu), qui permet de calculer le pgcd de deux éléments (de trouver une relation de Bézout).

Exercice 2.4.5.8. (1) Soient $n, m \in \mathbf{N}_{>0}$. Calculer $\mathsf{pgcd}(X^n - 1, X^m - 1)$ dans $\mathbf{Q}[X]$.
(2) Montrer que l'anneau $\mathbf{Z}[j] = \{a + bj\}_{a,b\in\mathbf{Z}} \subset \mathbf{C}$ est euclidien.

2.5 Anneaux de séries formelles, anneaux des polynômes

Soit A un anneau.

Définition 2.5.0.1. L'anneau des *séries formelles* à coefficients dans A est l'ensemble $A^{\mathbf{N}}$ des suites à valeurs dans A muni des deux lois suivantes :

$$(a_n)_{n\in\mathbf{N}} + (b_n)_{n\in\mathbf{N}} = (a_n + b_n)_{n\in\mathbf{N}}$$
$$(a_n)_{n\in\mathbf{N}} \times (b_n)_{n\in\mathbf{N}} = (c_n)_{n\in\mathbf{N}}$$

où $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

Remarque 2.5.0.2. Bien entendu, il ne faut pas le confondre avec l'anneau $A^{\mathbf{N}}$ muni des lois composante par composante défini plus haut.

Notons X l'élément $(0, 1, 0, 0, \ldots) \in A^{\mathbf{N}}$: par définition, on a $X^n = (0, \ldots, 0, 1, 0, \ldots)$ pour tout $n \in \mathbf{N}$ et par linéarité, on a

$$(a_n)_{n\in\mathbf{N}} = \sum_{n=0}^{\infty} a_n X^n$$

c'est sous cette forme qu'on écrit une série formelle dans la pratique.

Définition 2.5.0.3. (i) Avec la notation précédente, X s'appelle l'*indéterminée*. On parle alors de l'*anneau des séries formelles* en l'indéterminée X à coefficients dans A et on le note $A[\![X]\!]$.
(ii) L'*anneau des polynômes* en l'indéterminée X à coefficients dans A est le sous-anneau $A[X]$ de l'anneau $A[\![X]\!]$ constitué des suites à support fini.

Remarque 2.5.0.4. Un polynôme s'écrit donc comme une somme finie

$$P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d.$$

Définition 2.5.0.5. (i) Si $f(X) = \sum_{n=0}^{\infty} a_n X^n \in A[\![X]\!]$, l'élément a_0 s'appelle le *coefficient constant* de $f(X)$.
(ii) Soit $P \in A[X]\backslash\{0\}$. On peut écrire de façon unique $P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$ avec $a_d \neq 0$. L'entier d s'appelle le *degré* de P : on le note $\deg(P)$ (par convention, on a $\deg(0) = -\infty$). L'élément a_d s'appelle le *coefficient dominant* de P. On dit que P est *unitaire* lorsque son coefficient dominant vaut 1.
(iii) Un polynôme dont tous les coefficients sont nuls sauf un seul (*i.e.* de la forme aX^d) s'appelle un *monôme*.

Remarque 2.5.0.6. L'application $A \to A[X]$ qui envoie a sur $(a, 0, \ldots)$ est un morphisme injectif d'anneaux : l'anneau A est donc naturellement un sous-anneau de $A[X]$ (polynômes constants). Idem avec les séries formelles.

Proposition 2.5.0.7. Si $P, Q \in A[X]$, on a :

$$\deg(P+Q) \leqslant \max\{\deg(P), \deg(Q)\}$$
$$\deg(PQ) \leqslant \deg(P) + \deg(Q).$$

Ces inégalités sont strictes en général. La première est une égalité si $\deg(P) \neq \deg(Q)$ et la deuxième si le coefficient dominant de P ou de Q n'est pas un diviseur de zéro (automatique lorsque A est intègre).

Démonstration. Écrivons $P(X) = a_0 + a_1X + \cdots + a_dX^d$ et $Q(X) = b_0 + b_1X + \cdots b_\delta X^\delta$, avec $d = \deg(P)$ et $\delta = \deg(Q)$. On a

$$PQ(X) = a_0b_0 + (a_1b_0 + a_0b_1)X + \cdots + a_db_\delta X^{d+\delta}$$

ce qui montre que $\deg(PQ) \leqslant d + \delta$. Lorsque A est intègre, on a $a_db_\delta \neq 0$ et donc $\deg(PQ) = \deg(P) + \deg(Q)$. □

Exemple 2.5.0.8. Si $P = Q = 1 + 2X \in (\mathbf{Z}/4\,\mathbf{Z})[X]$, alors $PQ = 1$ est de degré 0.

Corollaire 2.5.0.9. Si A est intègre, il en est de même pour $A[X]$.

Démonstration. Si $P, Q \in A[X]\backslash\{0\}$, alors $\deg(PQ) = \deg(P) + \deg(Q) \geqslant 0$ (car A est intègre), d'où $PQ \neq 0$. □

Exercice 2.5.0.10. (1) Montrer que si A est intègre, il en est de même de $A[\![X]\!]$.
(2) Soit A un anneau intègre. Montrer que $A[X]^\times = A^\times$. Décrire $A[\![X]\!]^\times$.

Théorème 2.5.0.11 (Division euclidienne)**.** Soient A un anneau et $P, D \in A[X]$. On suppose que le coefficient dominant de D est inversible. Il existe alors un unique couple $(Q, R) \in A[X]$ tel que

$$\begin{cases} P = QD + R \\ \deg(R) < \deg(D) \end{cases}$$

Le polynôme Q (resp. R) s'appelle le *quotient* (resp. le *reste*) dans la division euclidienne de P par D.

Démonstration. Unicité : Soient (Q_1, R_1) et (Q_2, R_2) tels que $P = Q_1D + R_1 = Q_2D + R_2$ et $\deg(R_1), \deg(R_2) < \deg(D)$. On a donc $R_2 - R_1 = (Q_1 - Q_2)D$, de sorte que $\deg(D) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg(D)$ (l'égalité provient du fait que le coefficient dominant de D n'est pas diviseur de zéro, *cf.* proposition 2.5.0.7). Comme $\deg(D) \in \mathbf{N}$, cela implique $\deg(Q_1 - Q_2) < 0$ et donc $Q_1 - Q_2 = 0$, ce qui montre que $Q_2 = Q_1$ et donc aussi $R_2 = R_1$.
Existence : Si $\deg(D) = 0$, alors D est constant et on a $Q = D^{-1}P$, $R = 0$. Supposons désormais que $\deg(D) > 0$. On procède par récurrence sur $\deg(P)$. Si $0 \leqslant \deg(P) < \deg(D)$, alors $Q = 0$ et $R = P$. Supposons $n := \deg(P) \geqslant d := \deg(D)$. Écrivons $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ et $D = b_dX^d + \cdots + b_0$: on a $b_d \in A^\times$. Posons $\widetilde{P} = P - b_d^{-1}a_nX^{n-d}D$: on a $\deg(\widetilde{P}) < n$. Par hypothèse de récurrence, il existe $\widetilde{Q}, R \in A[X]$ tels que $\widetilde{P} = \widetilde{Q}D + R$ et $\deg(R) < \deg(D)$. Posons alors $Q = b_d^{-1}a_nX^{n-d} + \widetilde{Q} \in A[X]$: on a $P = QD + R$. □

Remarque 2.5.0.12. Si K est un corps, la division euclidienne par un polynôme non nul existe toujours dans $K[X]$. À contrario, si A n'est pas un corps, on n'a pas de division euclidienne pour tout D non nul. Par exemple, il n'existe pas de division euclidienne de X par 2 dans $\mathbf{Z}[X]$.

Proposition 2.5.0.13 (Propriété universelle)**.** Soient $f\colon A \to B$ un morphisme d'anneaux et $b \in B$. Il existe un unique morphisme d'anneaux $\widetilde{f}\colon A[X] \to B$ tel que $\widetilde{f}(a) = f(a)$ pour tout $a \in A$ et $\widetilde{f}(X) = b$.

Démonstration. Si $\widetilde{f}$ existe et $P(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, on a nécessairement $\widetilde{f}(P) = f(a_0) + f(a_1)b + \cdots + f(a_n)b^n$, ce qui montre l'unicité. Il est immédiat que la formule qui précède définit bien un morphisme d'anneaux $A[X] \to B$ ayant les propriétés requises. □

Dans la pratique, si $P \in A[X]$, on note $P(b)$ l'élément $\widetilde{f}(P) \in B$.

Définition 2.5.0.14. Soient A un anneau et $\alpha \in A$. Le morphisme d'*évaluation* en α est l'unique morphisme $\mathsf{ev}_\alpha\colon A[X] \to A$ prolongeant l'identité de A et envoyant X sur α (explicitement, ev_α envoie $a_0 + a_1X + \cdots + a_dX^d$ sur $P(\alpha) = a_0 + a_1\alpha + \cdots + a_d\alpha^d$).

Remarque 2.5.0.15. Un polynôme $P \in A[X]$ fournit donc l'application :

$$A \to A$$
$$\alpha \mapsto P(\alpha)$$

Les fonctions ainsi obtenues sont appelées *fonctions polynomiales*. Il faut néanmoins se garder de confondre un polynôme avec la fonction polynomiale qu'il définit. Par exemple, si $A = \mathbf{Z}/2\,\mathbf{Z}$, le polynôme $X^2 - X$ est non nul, mais ne prend que des valeurs nulles sur $\mathbf{Z}/2\,\mathbf{Z}$. Plus précisément, on dispose du morphisme $A[X] \to \mathscr{F}(A, A)$ qui à un polynôme associe sa fonction polynomiale. Il n'est pas injectif en général. Il l'est lorsque A est un corps infini (exercice).

Exemple 2.5.0.16. Considérons le sous-anneau $A = \mathbf{Z}[i] = \{a+ib;\ a,b \in \mathbf{Z}\}$ de $\mathbf{C}$. On dispose du morphisme $f\colon \mathbf{Z}[X] \to A$ qui envoie X sur i. Il est surjectif et la division euclidienne implique que $\mathsf{Ker}(f) = \langle X^2+1\rangle$. En passant au quotient, on obtient un isomorphisme

$$\mathbf{Z}[X]/\langle X^2+1\rangle \xrightarrow{\sim} \mathbf{Z}[i].$$

De même, on a un isomorphisme $\mathbf{R}[X]/\langle X^2+1\rangle \xrightarrow{\sim} \mathbf{C}$ induit par le morphisme $\mathbf{R}[X] \to \mathbf{C}$ déduit de l'inclusion $\mathbf{R} \subset \mathbf{C}$ et qui envoie X sur i.

Exercice 2.5.0.17. Soient A un anneau, $I \subset A$ un idéal. On dispose dans $A[X]$ de l'idéal $IA[X]$ engendrée par I. Montrer qu'on a un isomorphisme naturel

$$A[X]/IA[X] \xrightarrow{\sim} (A/I)[X].$$

Définition 2.5.0.18. (i) Si A est un anneau, on définit l'anneau des polynômes en les indéterminées $X_1,\dots,X_r$ à coefficients dans A inductivement par

$$A[X_1,\dots,X_r] = (A[X_1,\dots,X_{r-1}])[X_r].$$

Concrètement, un élément de $A[X_1,\dots,X_r]$ est une somme finie :

$$P(X_1,\dots,X_r) = \sum_{\underline{n}\in\mathbf{N}^r} a_{\underline{n}} X_1^{n_1}\cdots X_r^{n_r}$$

où $a_{\underline{n}} \in A$ est nul sauf pour un nombre fini d'indices $\underline{n} = (n_1,\dots,n_r) \in \mathbf{N}^r$.
(ii) Un polynôme $P \in A[X_1,\dots,X_r]$ est dit *homogène* de degré d si c'est une somme de monômes de degré d, *i.e.* si $P(X_1,\dots,X_r) = \sum_{\underline{n}\in\mathbf{N}^r} a_{\underline{n}} X_1^{n_1}\cdots X_r^{n_r}$ avec $a_{\underline{n}} = 0$ dès que $|\underline{n}| := n_1+\cdots+n_r \neq d$. Tout élément $P \in A[X_1,\dots,X_r]$ s'écrit de façon unique $P = P_0 + P_1 + \cdots + P_d$ avec P_i homogène de degré i.

Si on note H_d l'ensemble des polynômes de degré d, on peut même réécrire

$$A[X_1,\dots,X_n] = \bigoplus_{d=0}^{\infty} H_d.$$

Théorème 2.5.0.19 (Propriété universelle)**.** Soient $f\colon A \to B$ un morphisme d'anneaux et $b_1,\dots,b_r \in B$. Il existe un unique morphisme d'anneaux $\widetilde{f}\colon A[X_1,\dots,X_r] \to B$ tel que $\widetilde{f}(a) = f(a)$ pour tout $a \in A$ et $\widetilde{f}(X_i) = b_i$ pour tout $i \in \{1,\dots,r\}$.

Là encore, on note $P(b_1,\dots,b_r)$ l'élément $\widetilde{f}(P)$.

Démonstration. Résulte du théorème 2.5.0.13 par induction sur r. □

Exercice 2.5.0.20. Soient K un corps et X,Y,T des indéterminées.
(1) Montrer que le morphisme d'anneaux $f\colon K[X,Y] \to K[T]$ qui est l'identité sur K et envoie X sur T^2 et Y sur T^3 à l'idéal $\langle Y^2 - X^3\rangle$ pour noyau et $A := K + T^2K[T] \subset K[T]$ pour image.
(2) Montrer que l'idéal engendré par T^2 et T^3 n'est pas principal dans A.

2.5.1 Polynômes symétriques, antisymétriques

Soient A un anneau et $X_1,\dots,X_r$ des indéterminées. Si on prend $P(X_1,\dots X_r) \in A[X_1,\dots,X_r]$ et $\gamma \in \mathfrak{S}_r$, on pose

$$(\gamma, P)(X_1,\dots,X_r) = P(X_{\gamma(1)},\dots,X_{\gamma(r)}).$$

On munit ainsi $A[X_1,\dots,X_r]$ d'une action du groupe $\mathfrak{S}_r$.

Définition 2.5.1.1. (i) Un polynôme $P(X_1,\dots,X_r) \in A[X_1,\dots,X_r]$ est dit *symétrique* si c'est un point fixe sous cette action. On définit de façon analogue la notion de fraction rationnelle symétrique à coefficients dans corps.
(ii) Pour $k \in \{1,\dots,r\}$, on pose

$$\sigma_k = \sigma_k(X_1,\dots,X_r) = \sum_{i_1<\cdots<i_k} X_{i_1}\cdots X_{i_k}$$

(k-ème polynôme symétrique élémentaire).

Exemple 2.5.1.2. On a

$$\begin{aligned}
\sigma_1 &= X_1 + X_2 + \cdots + X_r\\
\sigma_2 &= X_1X_2 + X_1X_3 + \cdots + X_1X_r + X_2X_3 + \cdots + X_2X_r + \cdots + X_{r-1}X_r\\
\sigma_r &= X_1X_2\cdots X_r.
\end{aligned}$$

Proposition 2.5.1.3. On a égalité :

$$\prod_{i=1}^{r}(T - X_i) = T^r - \sigma_1T^{r-1} + \sigma_2T^{r-2} + \cdots + (-1)^k\sigma_kT^{r-k} + \cdots + (-1)^r\sigma_r$$

dans $\mathbf{Z}[T,X_1,\dots,X_r]$.

Théorème 2.5.1.4. Si $P(X_1,\dots,X_r) \in A[X_1,\dots,X_r]$ est symétrique, il existe un unique polynôme $Q(X_1,\dots,X_r) \in A[X_1,\dots,X_r]$ tel que $P(X_1,\dots,X_r) = Q(\sigma_1,\dots,\sigma_r)$.

Corollaire 2.5.1.5. Si K un corps et $R(X_1,\dots,X_n) \in K(X_1,\dots,X_n)$ est symétrique, il existe $Q(Y_1,\dots,Y_n) \in K(Y_1,\dots,Y_n)$ unique telle que $P = Q(\sigma_1,\dots,\sigma_n)$.

Définition 2.5.1.6. Un polynôme $P \in A[X_1,\dots,X_r]$ est dit *antisymétrique* si $\gamma \cdot P = \varepsilon(\gamma)P$ pour tout $\gamma \in \mathfrak{S}_r$ (avec ε la signature).

Exemple 2.5.1.7. Le polynôme
$$\delta(X_1,\dots,X_n) = \prod_{1\leqslant i<j\leqslant r} (X_i - X_j)$$
est antisymétrique (par définition de la signature).

Théorème 2.5.1.8. Supposons 2 inversible dans A. Si $P \in A[X_1,\dots,X_r]$ est antisymétrique, alors il existe $Q \in A[X_1,\dots,X_r]$ symétrique tel que $P = \delta Q$. En particulier, f est de degré supérieur ou égal à $\frac{n(n-1)}{2}$.

2.6 Corps des fractions

2.6.1 Généralités

Soit A un anneau intègre [1]. On construit un corps qui contient A et qui est minimal pour cette propriété de la façon suivante. On munit l'ensemble $A \times (A\backslash\{0\})$ de la relation binaire donnée par :
$$(a_1,s_1) \sim (a_2,s_2) \Leftrightarrow a_1s_2 = a_2s_1.$$

Lemme 2.6.1.1. C'est une relation d'équivalence.

Démonstration. Elle est symétrique et réflexive de façon évidente. Si $(a_1,s_1) \sim (a_2,s_2)$ et $(a_2,s_2) \sim (a_3,s_3)$, on a $a_1s_2 = a_2s_1$ et $a_2s_3 = a_3s_2$, donc $a_1s_2s_3 = a_2s_1s_3 = a_3s_2s_1$ en multipliant la première égalité (resp. la deuxième) par s_3 (resp. s_1). En simplifiant par s_2 (ce qui est licite vu que A est intègre), on tire $a_1s_3 = a_3s_1$ *i.e.* $(a_1,s_1) \sim (a_3,s_3)$ et la relation est bien transitive. □

On note $\mathsf{Frac}(A)$ l'ensemble quotient de $A \times (A\backslash\{0\})$ par cette relation d'équivalence. Pour tout $(a,s) \in A \times (A\backslash\{0\})$ on note $[(a,s)]$ son image dans $\mathsf{Frac}(A)$. On le munit de deux lois définies par
$$[(a_1,s_1)] + [(a_2,s_2)] = [(a_1s_2 + a_2s_1, s_1s_2)] \qquad \text{et} \qquad [(a_1,s_1)] \cdot [(a_2,s_2)] = [(a_1a_2, s_1s_2)].$$

Proposition 2.6.1.2. Ces lois sont bien définies et munissent $\mathsf{Frac}(A)$ d'une structure de corps. On l'appelle le *corps des fractions* de A. Par ailleurs, l'application
$$\begin{aligned} \iota\colon A &\to \mathsf{Frac}(A) \\ a &\mapsto [(a,1)] \end{aligned}$$
définit un morphisme injectif d'anneaux (de sorte qu'on peut voir A comme un sous-anneau de $\mathsf{Frac}(A)$). En outre, le couple $(\mathsf{Frac}(A),\iota)$ a la propriété universelle suivante : pour tout morphisme d'anneaux $f\colon A \to B$ tel que pour tout $a \in A\backslash\{0\}$, $f(a) \in B^\times$, il existe un unique morphisme d'anneaux $\widetilde{f}\colon \mathsf{Frac}(A) \to B$ tel que $f = \widetilde{f} \circ \iota$.

Démonstration. • Il s'agit de voir que si $(a_1,s_1),(a_2,s_2) \in A \times (A\backslash\{0\})$, les classes de $(a_1s_2 + a_2s_1, s_1s_2)$ et de (a_1a_2, s_1s_2) modulo $\sim$ ne dépendent que des classes de (a_1,s_1) et de (a_2,s_2) modulo $\sim$. Soit donc $(a_1',s_1') \sim (a_1,s_1)$ dans $A \times (A\backslash\{0\})$. On a alors
$$\begin{aligned} (a_1s_2 + a_2s_1)(s_1's_2) &= a_1s_1's_2^2 + a_2s_1s_1's_2 \\ &= a_1's_1s_2^2 + a_2s_1s_1's_2 \quad \text{car } a_1s_1' = a_1's_1 \\ &= (a_1's_2 + a_2s_1')(s_1s_2) \end{aligned}$$
et donc $[(a_1s_2 + a_2s_1, s_1s_2)] = [(a_1's_2 + a_2s_1', s_1's_2)]$. De même, on a
$$(a_1a_2)(s_1's_2) = (a_1s_1')(a_2s_2) = (a_1's_1)(a_2s_2) = (a_1'a_2)(s_1s_2)$$
et donc $[(a_1a_2, s_1s_2)] = [(a_1'a_2, s_1's_2)]$.
• Le fait que ces lois définissent un corps se vérifie simplement, l'élément neutre pour l'addition étant donné par $[(0,1)]$, celui de la multiplication par $[(1,1)]$, on a $-[(a,s)] = [(-a,s)]$ et si $a \in A\backslash\{0\}$, on a $[(a,s)]^{-1} = [(s,a)]$.
• Pour $a_1,a_2 \in A$, on a $\iota(a_1+a_2) = [(a_1+a_2,1)] = [(a_1,1)] + [(a_2,1)] = \iota(a_1) + \iota(a_2)$ et $\iota(a_1a_2) = [(a_1a_2,1)] = [(a_1,1)] \cdot [(a_2,1)] = \iota(a_1)\iota(a_2)$ et $\iota(1) = [(1,1)] = 1_{\mathsf{Frac}(A)}$ donc ι est un morphisme d'anneaux. Comme on a : $[(a,1)] = 0 \Leftrightarrow (a,1) \sim (0,1) \Leftrightarrow a = 0$, alors $\mathsf{Ker}(\iota) = \{0\}$ et ι est injectif.
• Soit $f\colon A \to B$ tel que $f(a) \in B^\times$ pour tout $a \in A\backslash\{0\}$. Soit $(a,s) \in A \times (A\backslash\{0\})$. Si $\widetilde{f}$ existe, on a nécessairement $\widetilde{f}([(s,1)]) = f(s)$ donc $\widetilde{f}([(a,s)])f(s) = \widetilde{f}([(a,s)])[(s,1)] = \widetilde{f}([(a,1)]) = f(a)$ et donc $\widetilde{f}([(a,s)]) = f(a)f(s)^{-1}$ (rappelons que ça a un sens vu que $f(s) \in B^\times$ parce que $s \in A\backslash\{0\}$). Cela prouve l'unicité.
• On définit donc $\widetilde{f}\colon \mathsf{Frac}(A) \to B$ par $\widetilde{f}([(a,s)]) = f(a)f(s)^{-1}$ pour $(a,s) \in A \times (A\backslash\{0\})$. C'est bien défini, parce que si $(a',s') \sim (a,s)$ dans $A \times (A\backslash\{0\})$, on a $as' = a's$, d'où $f(a)f(s') = f(a')f(s)$ soit $f(a)f(s)^{-1} = f(a')f(s')^{-1}$ (en divisant par $f(s)f(s') \in B^\times$). Le fait que $\widetilde{f}$ soit un morphisme d'anneaux résulte immédiatement du fait que f en est un. □

1. Il existe des construction plus générales et sans hypothèse de commutativité ou d'intégrité, dont on ne parlera pas ici.

Remarque 2.6.1.3. (1) L'idée de la construction est de la classe $[(a,s)]$ correspond à la fraction a/s, la relation d'équivalence étant la pour prendre en compte les « simplifications » qui pourraient avoir lieu. Remarquons toutefois qu'à moins d'être dans un anneau factoriel, on n'a pas de notion de « fraction irréductible ».
(2) Grâce à la propriété universelle, on voit que le corps qu'on a construit est « le plus petit » contenant A. En effet, si K est un corps contenant A, on peut factoriser l'inclusion $i\colon A \hookrightarrow K$ en $\widetilde{i}\circ\iota$, et comme $\widetilde{i}\colon \mathsf{Frac}(A) \to K$ est un morphisme d'anneaux entre corps, il est injectif.

Exercice 2.6.1.4. Le corps des fractions de $\mathbf{Z}$ est le corps $\mathbf{Q}$.

2.6.2 Corps des fractions rationnelles

Soit K un corps. L'anneau des polynômes $K[X]$ est intègre : on dispose de son corps des fractions.

Définition 2.6.2.1. Le *corps des fractions rationnelles* (en l'indéterminée X) sur K est

$$K(X) := \mathsf{Frac}(K[X]).$$

Ses éléments peuvent donc s'écrire comme des fractions $\frac{P}{Q}$ avec $P,Q \in K[X]$ et $Q \neq 0$. Cette écriture est unique si on suppose $\mathsf{pgcd}(P,Q) = 1$ et Q unitaire (on parle alors de forme irréductible).

Définition 2.6.2.2. Soient $R \in K(X)$ et $R = \frac{P}{Q}$ sa forme irréductible. Les zéros de P (resp. Q) s'appellent les *zéros* (resp. les *pôles*) de R. Les ordres de multiplicité afférents sont ceux de P et Q respectivement.

Remarque 2.6.2.3. Avec les notations de la définition précédente, la fraction rationnelle R définit l'application

$$\begin{aligned} R\colon K\setminus \mathsf{Z}(Q) &\to K \\ x &\mapsto \frac{P(x)}{Q(x)} \end{aligned}$$

qu'on appelle *fonction rationnelle* associée à R. Comme pour les polynômes, on veillera à ne point confondre fractions et fonctions rationnelles.

Définition 2.6.2.4. (i) Si $R = \frac{P}{Q} \in K(X)$, on pose $\deg(R) = \deg(P) - \deg(Q) \cup \mathbf{Z} \cup \{-\infty\}$, qu'on appelle le *degré* de R (il est immédiat que ça ne dépend que de R et pas de P et Q). Cette fonction jouit des mêmes propriétés que le degré sur $K[X]$.
(ii) Notons $\mathbf{P}$ l'ensemble des polynômes irréductibles et unitaires dans $K[X]$. Si $P \in \mathbf{P}$, on dispose de la valuation P-adique $v_P\colon K[X]\setminus\{0\} \to \mathbf{N}$. Elle se prolonge de façon unique en une application

$$v_P\colon K(X)^\times \to \mathbf{Z}$$

telle que $v_P(\frac{U}{V}) = v_P(U) - v_P(V)$ pour tous $U,V \in K[X]\setminus\{0\}$. On l'appelle encore la *valuation P-adique* et elle vérifie les mêmes propriétés que la valuation P-adique sur $K[X]$.

Remarque 2.6.2.5. On peut interpréter l'application $-\deg\colon K(X) \to \mathbf{Z}\cup\{\infty\}$ comme une valuation de la façon suivante. Posons $Y = \frac{1}{X}$: on a $K(X) = K(Y)$. Si $P(X) = a_0 + a_1X + \cdots + a_dX^d \in K[X]\setminus\{0\}$ avec $d = \deg(P)$, on a

$$P = X^d(a_0Y^d + \cdots + a_{d-1}Y + a_d) = Y^{-d}(a_0Y^d + \cdots + a_{d-1}Y + a_d).$$

Comme $a_d \neq 0$, on a $v_Y(a_0Y^d + \cdots + a_{d-1}Y + a_d) = 0$, de sorte que $v_Y(P) = -d = -\deg(P)$. Il en résulte que $v_Y = -\deg$ sur $K(X)$, de sorte que $-\deg$ est la valuation $1/X$-adique, en d'autre termes, $\deg(R)$ est l'ordre du pôle $+\infty$.

Soit $R \in K(X)^\times$. La décomposition en produit de facteurs irréductibles dans $K[X]$ implique que $(v_P(R))_{P\in\mathbf{P}} \in \mathbf{Z}^{(\mathbf{P})}$ et qu'il existe $u \in K^\times$ unique tel que

$$R = u\prod_{P\in\mathbf{P}} P^{v_P(R)}.$$

Cela donne une description du groupe multiplicatif $K(X)^\times$ (il est isomorphe à $K^\times \times \mathbf{Z}^{(\mathbf{P})}$). Ce qui suit a pour but de comprendre la structure additive de $K(X)$, plus précisément de donner une base de $K(X)$ sur K.

Théorème 2.6.2.6 (Décomposition en éléments simples)**.** La famille

$$\{X^n\}_{n\in\mathbf{N}} \cup \left\{\frac{X^j}{P^k}\right\}_{\substack{P\in\mathbf{P}\\ 0\leqslant j<\deg(P)\\ k\in\mathbf{N}_{>0}}}$$

est une base de $K(X)$ sur K.

Remarque 2.6.2.7. Explicitement, cela signifie que si $R = \frac{P}{Q} \in K(X)$ est écrit sous forme irréductible (avec Q unitaire) et si $Q = \prod_{i=1}^{r} P_i^{m_i}$ est la décomposition en produit de facteurs irréductibles de Q, alors il existe $E \in K[X]$ et des polynômes $(A_{i,j})_{1\leqslant i\leqslant r, 1\leqslant j\leqslant m_i}$ uniques tels que $\deg(A_{i,j}) < \deg(P_i)$ pour tous $i \in \{1,\dots,r\}$ et $j \in \{1,\dots,m_i\}$ et

$$R = E + \sum_{i=1}^{r}\sum_{j=1}^{m_i} \frac{A_{i,j}}{P_i^j}.$$

Le polynôme E s'appelle la *partie entière* de R. Les termes de la somme qui précède s'appellent les *éléments simples* de R.

Lemme 2.6.2.8. Soit $R = \frac{P}{Q} \in K(X)$ tel que $\deg(R) < 0$. Si $Q = Q_1Q_2$ avec $\mathsf{pgcd}(Q_1, Q_2) = 1$, il existe $P_1, P_2 \in K[X]$ uniques tels que $\deg(P_i) < \deg(Q_i)$ et $R = \frac{P_1}{Q_1} + \frac{P_2}{Q_2}$.

Démonstration. Comme $\mathsf{pgcd}(Q_1, Q_2) = 1$, il existe $U, V \in K[X]$ tels que $UQ_1 + VQ_2 = 1$. En multipliant par R, il vient que $R = \frac{VP}{Q_1} + \frac{UP}{Q_2}$. Soit $VP = E_1Q_1 + P_1$ (resp. $UP = E_2Q_2 + P_2$) avec $\deg(P_i) < \deg(Q_i)$ la divison euclidienne de VP (resp. UP) par Q_1 (resp. Q_2). On a $R = E_1 + E_2 + \frac{P_1}{Q_1} + \frac{P_2}{Q_2}$. Comme $\deg(R), \deg(\frac{P_1}{Q_1}), \deg(\frac{P_2}{Q_2}) < 0$, on a $\deg(E_1 + E_2) < 0$, ce qui implique que $E_1 + E_2 = 0$ et donc l'existence de l'écriture.
Montrons l'unicité : supposons que $\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{\tilde{P}_1}{Q_1} + \frac{\tilde{P}_2}{Q_2}$ avec $\deg(P_i), \deg(\tilde{P}_i) < \deg(Q_i)$. On a alors

$$(P_1 - \tilde{P}_1)Q_2 = (\tilde{P}_2 - P_2)Q_1.$$

Comme $\mathsf{pgcd}(Q_1, Q_2) = 1$, cela implique que $Q_i \mid \tilde{P}_i - P_i$: comme $\deg(\tilde{P}_i - P_i) < \deg(Q_i)$, cela implique que $\tilde{P}_i = P_i$ pour $i \in \{1, 2\}$. □

Démonstration du théorème 2.6.2.6. Écrivons $R = \frac{P}{Q}$ sous forme irréductible (avec Q unitaire). Soit $P = QE + \tilde{P}$ avec $\deg(\tilde{P}) < \deg(Q)$ la division euclidienne de P par Q : on a $R = E + \frac{\tilde{P}}{Q}$: cela nous ramène à traiter le cas où $\deg(R) < 0$ (l'unicité de E se prouve comme dans la preuve du lemme précédent en utilisant le degré). Soit

$$Q = \prod_{i=1}^{r} P_i^{m_i}$$

la décomposition de Q en produit de facteurs irréductibles. Le lemme précédent montre qu'il existe $A_1, \dots, A_r \in K[X]$ uniques tels que $\deg(A_i) < m_i \deg(P_i)$ pour tout $i \in \{1, \dots, r\}$ et

$$R = \sum_{i=1}^{r} \frac{A_i}{P_i^{m_i}}$$

ce qui permet de se ramener au cas où $R = \frac{A_i}{P_i^{m_i}}$ avec $\deg(A_i) < m_i \deg(P_i)$. Si on a

$$R = \sum_{j=1}^{m_i} \frac{A_{i,j}}{P_i^j}$$

comme annoncé, on a $A_i = P_i^{m_i} R = \sum_{j=1}^{m_i} A_{i,j} P_i^{m_i - j}$. Cela montre que la suite $(A_{i,j})_{1 \leqslant j \leqslant m_i}$ est obtenue de la façon suivante : on pose $A_i^{(m_i)} = A_i$ et on construit les suites $(A_i^{(j)})_{1 \leqslant j \leqslant m_i}$ et $(A_{i,j})_{1 \leqslant j \leqslant m_i}$ en disant que

$$A_i^{(j)} = A_i^{(j-1)} P_i + A_{i,j}$$

avec $\deg(A_{i,j}) < \deg(P_i)$ est la division euclidienne de $A_i^{(j)}$ par P_i pour $j = m_i, m_i - 1, \dots, 1$. Cela prouve l'existence et l'unicité de $(A_{i,j})_{1 \leqslant j \leqslant m_i}$. □

Remarque 2.6.2.9. On a $\deg(E) = \deg(R)$.

Exemple 2.6.2.10. (1) Ici, $K = \mathbf{C}$. Comme le corps $\mathbf{C}$ est algébriquement clos, on a $\mathbf{P} = \{X - a\}_{a \in \mathbf{C}}$. Si $R = \frac{P}{Q} \in \mathbf{C}(X)$ est sous forme irréductible, $Q(X) = \prod_{i=1}^{r} (X - a_i)^{m_i}$, il existe $E \in \mathbf{C}[X]$, et des éléments $(\alpha_{i,j})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant m_i}}$ dans $\mathbf{C}$ uniques tels que

$$R(X) = E(X) + \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{\alpha_{i,j}}{(X - a_i)^j}.$$

(2) Ici, $K = \mathbf{R}$. On a $\mathbf{P} = \{X - a\}_{a \in \mathbf{R}} \sqcup \{X^2 - sX + p\}_{\substack{s,p \in \mathbf{R} \\ s^2 - 4p < 0}}$. Si $R = \frac{P}{Q} \in \mathbf{R}(X)$ est sous forme irréductible, $Q(X) = \prod_{i=1}^{r} (X - a_i)^{m_i} \prod_{i=1}^{t} (X^2 - s_iX + p_i)^{n_i}$ (avec $s_i^2 - 4p_i < 0$ pour tout $i \in \{1, \dots, t\}$), il existe $E \in \mathbf{R}[X]$ et des éléments $(\alpha_{i,j})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant m_i}}$, $(\beta_{i,j})_{\substack{1 \leqslant i \leqslant t \\ 1 \leqslant j \leqslant n_i}}$, $(\gamma_{i,j})_{\substack{1 \leqslant i \leqslant t \\ 1 \leqslant j \leqslant n_i}}$ dans $\mathbf{R}$ uniques tels que

$$R(X) = E(X) + \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{\alpha_{i,j}}{(X - a_i)^j} + \sum_{i=1}^{t} \sum_{j=1}^{n_i} \frac{\beta_{i,j}X + \gamma_{i,j}}{(X^2 - s_iX + p_i)^j}.$$

Remarque 2.6.2.11. (1) Cela montre par exemple de $\dim(\mathbf{C}(X)) = \#\,\mathbf{R}$ (alors que $\dim(\mathbf{C}[X]) = \#\,\mathbf{N}$).
(2) L'application principale de la décomposition en éléments simples qu'on enseigne en premier cycle est le calcul des primitives et intégrales de fractions rationnelles et rationnelles trigonométriques en utilisant les fonctions « usuelles ».

Exercice 2.6.2.12. (1) Soit $P \in \mathbf{C}[X]$. Les racines de P' sont dans l'enveloppe convexe des racines de P.
(2) Soient $\lambda_1, \dots, \lambda_n \in K$ deux à deux distincts, $Q(X) = \prod_{k=1}^{n} (X - \lambda_k)$ et $P \in K[X]$ tel que $\deg(P) < n$. La décomposition en éléments simples de $\frac{P}{Q}$ est

$$\frac{P}{Q} = \sum_{k=1}^{n} \frac{P(\lambda_k)}{Q'(\lambda_k)(X - \lambda_k)}.$$

2.7 Irréductibilité des polynômes

Soient A un anneau intègre. Dans ce numéro, on va donner des critères d'irréductibilité dans $A[X]$. La détermination de l'irréductibilité d'un polynôme est une question généralement délicate.

Remarque 2.7.0.1. Cette question est bien entendu très sensible à l'anneau de coefficients considéré. Par exemple, le polynôme X^2+1 est irréductible dans $\mathbf{R}[X]$, mais pas dans $\mathbf{C}[X]$. De même, le polynôme $2X$ est irréductible dans $\mathbf{Q}[X]$, mais pas dans $\mathbf{Z}[X]$ (car 2 est irréductible dans $\mathbf{Z}[X]$, mais inversible dans $\mathbf{Q}[X]$). Il convient donc de toujours préciser « irréductible dans $A[X]$ ».

2.7.1 Généralités

Définition 2.7.1.1. Soient $P \in A[X]$ et $\alpha \in A$. On dit que α est une *racine* de P si $P(\alpha)=0$.

Lemme 2.7.1.2. Soient $P \in A[X]$ de degré $\geqslant 1$ et $\alpha \in A$. Si α est racine de P, alors P est divisible par $X-\alpha$. En particulier, P est réductible si $\deg(P) \geqslant 2$.

Démonstration. Résulte de la division euclidienne de P par $X-\alpha$ dans $A[X]$. □

Corollaire 2.7.1.3. Soient K un corps et $P \in K[X]$. Le polynôme P a alors un facteur de degré 1 si et seulement si P a une racine dans K.

Proposition 2.7.1.4. Soient K un corps et $P \in K[X]$.
(i) Si $\deg(P)=1$, alors P est irréductible.
(ii) Si $\deg(P) \in \{2,3\}$, alors P est irréductible si et seulement s'il n'a pas de racine dans K.

Démonstration. (i) Si $P=P_1P_2$ avec $P_1,P_2 \in K[X]$, alors $1=\deg(P_1)+\deg(P_2)$.
(ii) Supposons $\deg(P) \in \{2,3\}$ et P sans racine. Si $P=P_1P_2$ avec $P_1,P_2 \in K[X]$, de nouveau on a $\deg(P)=\deg(P_1)+\deg(P_2)$. Si $\deg(P)=2$, alors P serait réductible si et seulement si $\deg(P_1)=\deg(P_2)=1$, mais P est sans racine, ce qui conclut. On procède de la même manière si $\deg(P)=3$. □

Remarque 2.7.1.5. L'énoncé qui précède est très faux en degré $\geqslant 4$. Par exemple, le polynôme $(X^2+1)^2$ n'a pas de racine dans $\mathbf{R}$, mais il est réductible. De même, il est faux en général sur un anneau qui n'est pas un corps : le polynôme $(2X+1)^2$ est réductible dans $\mathbf{Z}[X]$, mais n'a pas de racine dans $\mathbf{Z}$.

Exercice 2.7.1.6. Supposons A factoriel. Soient $P(X)=a_0+a_1X+\cdots+a_nX^n \in A[X]$ de degré n et $a,b \in A\backslash\{0\}$ premiers entre eux tels que a/b soit une racine de P dans $\mathsf{Frac}(A)$. Montrer que $a \mid a_0$ et $b \mid a_n$. En déduire que si P est unitaire et admet une racine $\alpha \in \mathsf{Frac}(A)$, alors $\alpha \in A$ (on dit que A est *intégralement clos*).

Lemme 2.7.1.7. Si $P \in A[X]\backslash A$ unitaire et réductible, alors il existe $P_1,P_2 \in A[X]$ unitaires tels que $P=P_1P_2$ et $\deg(P_1),\deg(P_2)<\deg(P)$.

Démonstration. On peut écrire $P=Q_1Q_2$ avec $Q_1,Q_2 \in A[X]\backslash(\{0\}\cup A^\times)$. Le terme dominant de Q_1 (resp. Q_2) est de la forme aX^d (resp. bX^{n-d}) où $n=\deg(P)$. On a alors $ab=1$ *i.e.* $a,b \in A^\times$. On pose $P_1=\frac{Q_1}{a}$, $P_2=\frac{Q_2}{b}$ avec $P_1,P_2 \in A[X]$ qui sont unitaires et par construction $P=P_1P_2$. Si on avait $\deg(P_1)=\deg(P)=n$, on aurait $P_2=1$ *i.e.* $Q_2=b \in A^\times$ ce qui est impossible. On a donc $\deg(P_1)<\deg(P)$. □

Remarque 2.7.1.8. L'énoncé qui précède est faux en général sans hypothèse sur le coefficient dominant de P : par exemple, $2X+2=2(X+1)$ est réductible dans $\mathbf{Z}[X]$.

2.7.2 Transfert d'irréductibilité

Supposons A factoriel et posons $K=\mathsf{Frac}(A)$.

Définition 2.7.2.1. (i) Soit $P=a_0+a_1X+\cdots+a_dX^d \in A[X]\backslash\{0\}$. Le *contenu* de P est $\mathsf{c}(P)=\mathsf{pgcd}(a_0,\ldots,a_d)$.
(ii) Un polynôme $P \in A[X]\backslash\{0\}$ est *primitif* si et seulement si $\mathsf{c}(P)=1$.

Remarque 2.7.2.2. (1) Rappelons que rigoureusement parlant, le pgcd est une classe d'équivalence modulo la relation « être associé ». Dans ce qui suit, on commettra l'abus habituel consistant à voir $\mathsf{c}(P)$ comme un élément de A (n'importe quel représentant de la classe) pour ne pas alourdir la rédaction et toutes les égalités faisant intervenir des contenus doivent être lues comme des égalités d'idéaux (*i.e.* modulo la relation « être associé »).
(2) En général (*i.e.* sans supposer A factoriel), on dit qu'un polynôme $P \in A[X]\backslash\{0\}$ est primitif si l'égalité $P=aQ$ avec $a \in A$ et $Q \in A[X]$ implique $a \in A^\times$. Cela signifie que les seuls diviseurs communs aux coefficients de P sont les unités.
(3) Un polynôme unitaire (ou plus généralement à coefficient dominant inversible) est primitif.

Lemme 2.7.2.3. Si $P,Q \in A[X]\backslash\{0\}$, on a :
(i) $\mathsf{c}(aP)=a\cdot\mathsf{c}(P)$ pour tout $a \in A\backslash\{0\}$;
(ii) $P=\mathsf{c}(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ primitif ;
(iii) $\mathsf{c}(PQ)=\mathsf{c}(P)\,\mathsf{c}(Q)$.

Démonstration. (i) Évident.
(ii) Écrivons $P(X) = a_0 + a_1X + \cdots + a_dX^d$ et pour tout $k \in \{0, \ldots, d\}$, on peut écrire $a_k = \mathsf{c}(P)b_k$ avec $b_k \in A$. Posons $\widetilde{P}(X) = b_0 + b_1X + \cdots + b_dX^d \in A[X]$, on a $P = \mathsf{c}(P)\widetilde{P}$ et $\mathsf{c}(\widetilde{P}) = \mathsf{pgcd}(b_0, \ldots, b_d) = 1$ *i.e.* $\widetilde{P}$ est primitif.
(iii) D'après (ii), on a $P = \mathsf{c}(P)\widetilde{P}$ et $Q = \mathsf{c}(Q)\widetilde{Q}$ avec $\widetilde{P}, \widetilde{Q} \in A[X]$ primitifs : on a alors $PQ = \mathsf{c}(P)\,\mathsf{c}(Q)\widetilde{P}\widetilde{Q}$. Quitte à remplacer P et Q par $\widetilde{P}$ et $\widetilde{Q}$ respectivement, il suffit donc de montrer que si P et Q sont primitifs, il en est de même de PQ. Supposons au contraire qu'il existe $\pi \in A$ premier tel que $\pi \mid \mathsf{c}(PQ)$. Si on note $\overline{P}$ et $\overline{Q}$ les images dans $(A/\pi A)[X]$ de P et Q respectivement, cela implique que $\overline{PQ} = 0$ dans $(A/\pi A)[X]$. Mais comme π est premier, l'anneau $A/\pi A$ est intègre : il en est de même de l'anneau $(A/\pi A)[X]$. On a donc $\overline{P} = 0$ ou $\overline{Q} = 0$ et donc $\pi \mid \mathsf{c}(P)$ ou $\pi \mid \mathsf{c}(Q)$, ce qui contredit $\mathsf{c}(P) = 1$ et $\mathsf{c}(Q) = 1$. □

Proposition 2.7.2.4 (Transfert d'irréductibilité)**.** Soit $P \in A[X]$ de degré $\geqslant 1$.
(i) Si P est irréductible dans $A[X]$, alors il est irréductible dans $K[X]$.
(ii) Si P est primitif et irréductible dans $K[X]$, alors il est irréductible dans $A[X]$.

Démonstration. (i) Commençons par observer que $\mathsf{c}(P) = 1$, parce que P est irréductible de degré $\geqslant 1$ dans $A[X]$. Supposons P réductible dans $K[X]$: on peut écrire $P = P_1P_2$ avec $P_1, P_2 \in K[X]$ de degrés $\geqslant 1$. Il existe $a_1, a_2 \in A\backslash\{0\}$ tels que $a_1P_1, a_2P_2 \in A[X]$. On a alors $a_1a_2 = \mathsf{c}(a_1a_2P) = \mathsf{c}(a_1P_1)\,\mathsf{c}(a_2P_2)$ d'après le lemme 2.7.2.3, vu que $\mathsf{c}(P) = 1$. Si on écrit $a_1P_1 = \mathsf{c}(a_1P_1)\widetilde{P}_1$ et $a_2P_2 = \mathsf{c}(a_2P_2)\widetilde{P}_2$ avec $\widetilde{P}_1, \widetilde{P}_2 \in A[X]$ primitifs, on a donc $a_1a_2P = \mathsf{c}(a_1P_1)\,\mathsf{c}(a_2P_2)\widetilde{P}_1\widetilde{P}_2$, soit $P = \widetilde{P}_1\widetilde{P}_2$ en divisant par a_1a_2 (l'anneau A est intègre). Comme P est irréductible dans $A[X]$, on a $\widetilde{P}_1 \in A^\times$ ou $\widetilde{P}_2 \in A^\times$, ce qui contredit $\deg(P_1), \deg(P_2) \geqslant 1$.
(ii) Supposons $P = P_1P_2$ avec $P_1, P_2 \in A[X]$. Comme P est irréductible dans $K[X]$, on peut supposer, quitte à échanger P_1 et P_2, que P_1 est constant, *i.e.* $P_1 = \mathsf{c}(P_1)$. D'après le lemme 2.7.2.3, on a $1 = \mathsf{c}(P) = \mathsf{c}(P_1)\,\mathsf{c}(P_2)$, donc $P_1 \in A^\times$ et P est irréductible dans $A[X]$. □

Exemple 2.7.2.5. (1) Un polynôme non constant et irréductible dans $\mathbf{Z}[X]$ est irréductible dans $\mathbf{Q}[X]$.
(2) Le polynôme $2X + 2$ est irréductible dans $\mathbf{Q}[X]$, mais réductible dans $\mathbf{Z}[X]$.

Remarque 2.7.2.6. Dans l'énoncé qui précède, il est important de supposer A factoriel. Par exemple, soit $A = \mathbf{Z}[\sqrt{-5}] \subset \mathbf{R}$ (on sait déjà que cet anneau n'est pas factoriel). On a $P(X) := X^2 - X - 2 \in A[X]$. Si $K = \mathsf{Frac}(A)$, on a $P(X) = (X - \frac{\sqrt{5}+1}{2})(X - \frac{\sqrt{5}-1}{2})$ dans $K[X]$. Cependant, il est irréductible dans $A[X]$ (exercice).

Exercice 2.7.2.7. (1) Soient $P, Q \in K[X]$ des polynômes unitaires tels que $PQ \in A[X]$. Montrer que $P, Q \in A[X]$.
(2) Soient $a_1, \ldots, a_n \in \mathbf{Z}$ deux à deux distincts. Montrer que $P(X) = (X - a_1)\cdots(X - a_n) - 1$ est irréductible dans $\mathbf{Q}[X]$.

2.7.3 Transfert de la factorialité

Théorème 2.7.3.1 (Transfert de la factorialité)**.** (i) Les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A et les polynômes primitifs non constants qui sont irréductibles dans $K[X]$.
(ii) L'anneau $A[X]$ est factoriel.

Démonstration. (i) Si $\pi \in A$ est irréductible, alors $A[X]/\pi A[X] = (A/\pi A)[X]$ est intègre, de sorte que le polynôme constant π est premier, donc irréductible dans $A[X]$. La proposition 2.7.2.4 (ii) montre que les polynômes primitifs non constants qui sont irréductibles dans $K[X]$ sont irréductibles dans $A[X]$. Réciproquement, soit P un élément irréductible dans $A[X]$. Si $\deg(P) = 0$, on a $P \in A$ et P est à fortiori irréductible dans A. Si $\deg(P) \geqslant 1$, on a $P = \mathsf{c}(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ primitif : comme P est irréductible dans $A[X]$, on a $\mathsf{c}(P) \in A^\times$, donc P est primitif. Par ailleurs, la proposition 2.7.2.4 (i) montre que P est irréductible dans $K[X]$.
(ii) • Si $\pi \in A$ est irréductible, on a vu ci-dessus que π est premier dans $A[X]$. Si $P \in A[X]$ est non constant, primitif et irréductible dans $K[X]$, et si $Q, R \in A[X]$ sont tels que $P \mid QR$ dans $A[X]$, on a à fortiori $P \mid QR$ dans $K[X]$, donc $P \mid Q$ ou $P \mid R$ dans $K[X]$, disons $P \mid Q$. Il existe donc $S \in K[X]$ tel que $Q = PS$. Soit $a \in A\backslash\{0\}$ tel que $aS \in A[X]$: on peut écrire $aS = \mathsf{c}(aS)\widetilde{S}$ avec $\widetilde{S} \in A[X]$ primitif, donc $aQ = \mathsf{c}(aS)P\widetilde{S}$. En prenant les contenus, on a $\mathsf{c}(Q) = \mathsf{c}(aS)$ (parce que $P\widetilde{S}$ est primitif), ce qui montre que $a \mid \mathsf{c}(aS)$: si $\mathsf{c}(aS) = ab$, on a $Q = bP\widetilde{S}$, ce qui montre que $P \mid Q$ dans $A[X]$. Cela prouve que P est premier dans $A[X]$.
• D'après (i), ce qui précède montre que les éléments irréductibles de $A[X]$ sont tous premiers. Pour prouver que $A[X]$ est factoriel, il suffit donc de montrer que tout élément $P \in A[X]\backslash\{0\}$ admet une factorisation en produit d'éléments irréductibles (*cf.* proposition 2.4.2.8). D'après le lemme 2.7.2.3 (ii), on peut écrire $P = \mathsf{c}(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ primitif. Comme A est factoriel, on peut factoriser $\mathsf{c}(P)$ en produit d'éléments irréductibles dans A (donc dans $A[X]$) : il suffit de montrer que $\widetilde{P}$ admet une factorisation. On peut donc se restreindre au cas où P est primitif. Si $P \in A$, on a alors $P = 1$: on peut supposer $\deg(P) \geqslant 1$. Comme l'anneau $K[X]$ est factoriel (*cf.* corollaire 2.4.5.6), on peut écrire $P = P_1P_2\cdots P_r$ avec $P_1, \ldots, P_r$ irréductibles dans $K[X]$. Pour tout $k \in \{1, \ldots, r\}$, choisissons $a_k \in A\backslash\{0\}$ tel que $a_kP_k \in A[X]$: le polynôme $\widetilde{P}_k := \mathsf{c}(a_kP_k)^{-1}(a_kP_k) \in A[X]$ est primitif. Étant irréductible dans $K[X]$, il est irréductible dans $A[X]$ (proposition 2.7.2.4 (ii)). Par ailleurs, on a $a_1\cdots a_rP = \mathsf{c}(a_1P_1)\cdots\mathsf{c}(a_rP_r)\widetilde{P}_1\cdots\widetilde{P}_r$ donc $a_1\cdots a_r = c(a_1P_1)\cdots\mathsf{c}(a_rP_r)$ en prenant le contenu et donc $P = \widetilde{P}_1\cdots\widetilde{P}_r$, ce qui achève la preuve. □

Remarque 2.7.3.2. (1) Réciproquement, il est facile de voir que si $A[X]$ est factoriel, il en est de même de A.
(2) En général, il n'est pas vrai que A factoriel implique $A[\![X]\!]$ factoriel. C'est cependant vrai si A est suffisamment « régulier ». C'est le cas par exemple lorsque A est un corps (exercice).

Corollaire 2.7.3.3. L'anneau $A[X_1, \dots, X_n]$ est factoriel.

Exemple 2.7.3.4. Les anneaux $\mathbf{Z}[X_1, \dots, X_n]$ et $K[X_1, \dots, X_n]$ (où K est un corps) sont factoriels.

Exercice 2.7.3.5. (1) Montrer que les idéaux premiers de $\mathbf{Z}[X]$ sont de trois sortes : $\{0\}$; $\langle P \rangle$ avec $P \in \mathbf{Z}[X]$ irréductible et $\langle p, F \rangle$ avec p premier dans $\mathbf{Z}$ et $F \in \mathbf{Z}[X]$ dont la réduction modulo p est irréductible dans $\mathbf{F}_p[X]$.
(2) Soient A factoriel, $n \in \mathbf{N}_{>0}$ et $\{X_{i,j}\}_{1 \leqslant i,j \leqslant n}$ des indéterminées. Posons $R = A[X_{i,j}]_{1 \leqslant i,j \leqslant n}$ (l'anneau de polynômes en n^2 indéterminées). On dispose de la matrice $M := (X_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(R)$ et du polynôme $D_n := \mathsf{det}(M) \in R$. Montrer que D_n est irréductible dans R (indication : procéder par récurrence sur n en développant D_n par rapport à la première colonne).

2.7.4 Les critères d'irréductibilité

Soit $I \subset A$ un idéal. On dispose de la surjection canonique $A \to A/I$: elle induit un morphisme surjectif $A[X] \to (A/I)[X]$. Si $P \in A[X]$, notons $\overline{P}$ son image dans $(A/I)[X]$. Observons que $\deg(\overline{P}) \leqslant \deg(P)$, avec égalité si et seulement si le coefficient dominant de P n'appartient pas à I.

Théorème 2.7.4.1 (Critère d'irréductibilité par réduction I)**.** Supposons $P \in A[X]$ non constant et unitaire. Si $\overline{P} \in (A/I)[X]$ ne se factorise pas en un produit de deux polynômes de degrés $< \deg(P)$, alors P est irréductible dans $A[X]$.

Démonstration. Si P est réductible dans $A[X]$, supposons $P = P_1 P_2$ avec $P_1, P_2 \in A[X]$. D'après le lemme 2.7.1.7, on peut supposer P_1 et P_2 unitaires de degré $< \deg(P)$. On a donc $\overline{P} = \overline{P}_1 \overline{P}_2$ et $\deg(P) = \deg(\overline{P}) = \deg(\overline{P}_1) + \deg(\overline{P}_2) \leqslant \deg(P_1) + \deg(P_2) = \deg(P)$. On a alors $\deg(\overline{P}_1) = \deg(P_1)$ et $\deg(\overline{P}_2) = \deg(P_2)$. Quitte à échanger, on peut supposer $\deg(\overline{P}_1) = \deg(\overline{P}) = \deg(P)$ et $\deg(\overline{P}_2) = \deg(P_2) = 0$, donc $P_2 \in A$ et P_2 est unitaire, d'où $P_2 = 1$. □

Exemple 2.7.4.2. (1) Le polynôme $X^2 + X + 1 \in \mathbf{Z}[X]$ est irréductible, parce qu'il est unitaire et que son image modulo 2 est irréductible dans $(\mathbf{Z}/2\,\mathbf{Z})[X]$ (car de degré 2 et sans racine). Remarquons qu'on ne peut pas invoquer la proposition 2.7.1.4 directement, parce que $\mathbf{Z}$ n'est pas un corps.
(2) Soit $P(X, Y) = X^2 + XY + 1 \in \mathbf{Q}[X, Y]$. On prend $A = \mathbf{Q}[Y]$ et $I = Y\,\mathbf{Q}[Y]$ l'idéal engendré par Y. On a $A/I = \mathbf{Q}$ et l'image (modulo I) de P dans $\mathbf{Q}[X]$ est $X^2 + 1$ (qui est irréductible, de degré 2 et n'ayant pas de racine dans le corps $\mathbf{Q}$). Le polynôme P est donc irréductible dans $\mathbf{Q}[X, Y]$.

Remarque 2.7.4.3. (1) L'hypothèse P unitaire est importante : si $P = (1 + X^2)(1 + Y) \in \mathbf{Q}[X, Y]$, alors P est réductible, mais sa réduction modulo Y est irréductible (c'est $X^2 + 1 \in \mathbf{Q}[X]$). C'est parce que le terme dominant de P est $X^2 Y$: il n'est pas unitaire (que ce soit en la variable X ou en la variable Y).
(2) Dans l'énoncé qui précède, l'hypothèse « unitaire » peut être affaiblie en « à coefficient dominant inversible ».

Remarque 2.7.4.4. Un polynôme unitaire (ou plus généralement à coefficient dominant inversible) est primitif.

Théorème 2.7.4.5 (Critère d'irréductibilité par réduction II)**.** Soient $\mathfrak{p} \subset A$ un idéal premier et $P(X) = a_0 + a_1 X + \cdots + a_d X^d \in A[X]$ un polynôme primitif tels que :
(i) $a_d \notin \mathfrak{p}$;
(ii) l'image $\overline{P}$ de P dans $(A/\mathfrak{p})[X]$ est irréductible.
Le polynôme P est alors irréductible dans $A[X]$.

Démonstration. Soit $P = QR$ avec $Q, R \in A[X]$ une factorisation dans $A[X]$: en réduisant modulo $\mathfrak{p}$, on a $\overline{P} = \overline{QR}$ dans $(A/\mathfrak{p})[X]$. Comme $\overline{P}$ est irréductible, l'un des facteurs, disons $\overline{Q}$ est inversible dans $(A/\mathfrak{p})[X]$. Comme $\mathfrak{p}$ est premier, on a $(A/\mathfrak{p})[X]^\times = (A/\mathfrak{p})^\times$ et en particulier, $\deg(\overline{Q}) = 0$. Les inégalités $\deg(\overline{Q}) \leqslant \deg(Q)$ et $\deg(\overline{R}) \leqslant \deg(R)$ donnent

$$\deg(\overline{P}) = \deg(\overline{Q}) + \deg(\overline{R}) \leqslant \deg(Q) + \deg(R) = \deg(P).$$

Comme $\deg(\overline{P}) = \deg(P)$ puisque $a_d \notin \mathfrak{p}$, on a donc $\deg(\overline{Q}) = \deg(Q)$ et $Q \in A$. Comme P est primitif, l'égalité $P = QR$ implique $Q \in A^\times$, ce qui montre que P est irréductible. □

Exemple 2.7.4.6. Le polynôme $P(X) = 7X^3 - 4X^2 + X + 3$ est irréductible dans $\mathbf{Z}[X]$ car primitif et de réduction modulo 2 irréductible (c'est le polynôme $X^3 + X + 1 \in (\mathbf{Z}/2\,\mathbf{Z})[X]$ qui est de degré 3 sans racine).

Remarque 2.7.4.7. Les hypothèses du théorème sont nécessaires. Par exemple, $(2X + 1)X$ est réductible dans $\mathbf{Z}[X]$ bien que primitif et de réduction modulo 2 irréductible, parce que son coefficient dominant est 2.

Théorème 2.7.4.8 (Critère d'Eisenstein)**.** Soient $\mathfrak{p} \subset A$ un idéal premier et $P(X) = a_0 + a_1 X + \cdots + a_d X^d \in A[X]$ un polynôme primitif tels que :
(i) $a_d \notin \mathfrak{p}$;
(ii) $a_0, \dots, a_{d-1} \in \mathfrak{p}$;
(iii) $a_0 \notin \mathfrak{p}^2$.
Le polynôme P est alors irréductible dans $A[X]$.

Démonstration. Supposons P réductible : soit $P = QR$ avec $Q, R \in A[X]$ une factorisation dans $A[X]$ avec $Q, R \notin A^\times$. En réduisant modulo $\mathfrak{p}$, on a

$$\overline{a}_d X^d = \overline{P}(X) = \overline{Q}(X)\overline{R}(X)$$

dans $(A/\mathfrak{p})[X]$. Comme dans la preuve du théorème 2.7.4.5, l'égalité $\deg(\overline{P}) = \deg(P)$ implique que $n := \deg(\overline{Q}) = \deg(Q)$ et $m := \deg(\overline{R}) = \deg(R)$. Le polynôme P étant primitif, cela implique que $n, m > 0$. Dans l'anneau factoriel $\mathsf{Frac}(A/\mathfrak{p})[X]$, l'égalité ci-dessus implique qu'il existe $\alpha, \beta \in A/\mathfrak{p}$ tels que $\overline{Q}(X) = \alpha X^n$ et $\overline{R}(X) = \beta X^m$ avec $\alpha\beta = \overline{a}_d$. Comme $n > 0$, on a donc $\overline{Q}(0) = 0$ *i.e.* $Q(0) \in \mathfrak{p}$. De même on a $R(0) \in \mathfrak{p}$. Cela implique que $a_0 = Q(0)R(0) \in \mathfrak{p}^2$, contredisant l'hypothèse. □

Remarque 2.7.4.9. (1) Bien sûr, l'hypothèse $a_0 \notin \mathfrak{p}^2$ est cruciale, par exemple, le polynôme $X^2-4 = (X-2)(X+2) \in \mathbf{Z}[X]$ n'est pas irréductible (avec $\mathfrak{p} = 2\,\mathbf{Z}$).
(2) Ce critère ne s'applique pas lorsque A est un corps (le seul idéal premier est $\{0\}\ldots$).
(3) À l'inverse du critère par réduction II, le critère d'Eisenstein s'applique quand la réduction $\overline{P}$ est très réductible.

Exemple 2.7.4.10. (1) Le polynôme $X^4 + 4X^3 + 6X^2 + 10$ est irréductible dans $\mathbf{Z}[X]$ (prendre $\mathfrak{p} = 2\,\mathbf{Z}$). Par contre, le critère ne s'applique pas au polynôme $X^5 - 4$ (qui est irréductible dans $\mathbf{Z}[X]$ cependant).
(2) Le polynôme $2X^3+3$ est irréductible dans $\mathbf{Z}[X]$ (prendre $\mathfrak{p} = 3\,\mathbf{Z}$) ; le polynôme $Y^{14}-X(X-1)(X+1)$ est irréductible dans $\mathbf{Q}[X, Y]$ (prendre $A = \mathbf{Q}[X]$ et $\mathfrak{p} = \langle X \rangle$).
(3) Soit p un nombre premier et $\Phi_p(X) = X^{p-1}+X^{p-2}+\cdots+X+1 \in \mathbf{Z}[X]$ (on l'appelle le p-ième polynôme cyclotomique, voir chapitre 3). Le polynôme Φ_p est alors irréductible. Pour le montrer, on remarque que $\Phi_p(X) = \frac{X^p-1}{X-1} \in \mathbf{Q}(X)$ et on effectue le changement de variable $X = Y + 1$. On a alors $\Phi_p(X) = \frac{(Y+1)^p-1}{Y}$, d'où

$$\Phi_p(X) = Y^{p-1} + \tbinom{p}{1}Y^{p-2} + \tbinom{p}{2}Y^{p-3} + \cdots + \tbinom{p}{p-1}.$$

Comme $p \mid \binom{p}{k}$ pour tout $k \in \{1, \ldots, p-1\}$ et $\binom{p}{p-1} = p$ est non divisible par p^2, le critère d'Eisenstein s'applique (avec $\mathfrak{p} = p\,\mathbf{Z}$) et $\Phi_p(Y + 1)$ est irréductible dans $\mathbf{Z}[Y] = \mathbf{Z}[X]$: il en est de même de Φ_p.

Exercice 2.7.4.11. Soit $n \in \mathbf{N}_{>1}$. Montrer que le polynôme $X^n + 5X^{n-1} + 3$ est irréductible dans $\mathbf{Z}[X]$.

Solution : Supposons $X^n + 5X^{n-1} + 3$ réductible sur $\mathbf{Z}$: comme il est primitif (il est unitaire), il peut s'écrire $X^n + 5X^{n-1} + 3 = PQ$ avec $P, Q \in \mathbf{Z}[X]$ non constants. Si a et b désignent les coefficients dominants de P et Q respectivement, on a $ab = 1$, donc $a = b \in \{\pm 1\}$. Quitte à diviser P et Q par leur coefficient dominant, on peut les supposer unitaires. Réduisons modulo 3 : on a

$$\overline{PQ} = X^n - X^{n-1} = X^{n-1}(X - 1)$$

dans $\mathbf{F}_3[X]$. Quitte à échanger P et Q, on peut supposer que c'est $\overline{P}$ qui est divisible par $X-1$: il existe $d \in \{0, \ldots, n-1\}$ tel que $\overline{P} = (X - 1)X^d$ et $\overline{Q} = X^{n-1-d}$. Notons que $0 < \deg(Q) = \deg(\overline{Q}) = n - 1 - d$ puisque Q n'est pas constant. On a donc $\overline{Q}(0) = 0$, ce qui signifie que $3 \mid Q(0)$: écrivons $Q(0) = 3k$ avec $k \in \mathbf{Z}$. Comme $X^n + 5X^{n-1} + 3 = PQ$, on a $P(0)Q(0) = 3$ en évaluant en 0 et donc $3kP(0) = 3$ *i.e.* $kP(0) = 1$, soit encore $k = P(0) \in \{\pm 1\}$. D'après ce qui précède, on peut écrire $P = (X - 1)X^d + 3P_1$ avec $P_1 \in \mathbf{Z}[X]$: si $d > 0$, l'entier $P(0) = 3P_1(0)$ est divisible par 3, contredisant ce qui précède. On a donc nécessairement $d = 1$ *i.e.* $P = X - 1 + 3P_1$. Comme P est unitaire, cela implique que P_1 est une constante et $X^n + 5X^{n-1} + 3$ admet 1 pour racine, ce qui est manifestement faux : contradiction.

3 Extensions de corps

Dans tout ce qui suit, les corps seront supposés commutatifs.

3.1 Définitions

Soit K un corps.

Définition 3.1.0.1. Une *extension* de K est un corps L qui contient K comme sous-corps. On note L/K l'extension. Un *morphisme d'extensions* entre L_1/K et L_2/K est un morphisme $f\colon L_1 \to L_2$ qui induit l'identité sur K. On parle aussi du K-morphisme $f\colon L_1 \to L_2$.

Exemple 3.1.0.2. (1) On a

$$\mathbf{C}/\mathbf{R}, \qquad \mathbf{R}/\mathbf{Q}, \qquad \mathbf{Q}(X)/\mathbf{Q}.$$

(2) $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbf{Q}\}$ est un sous-corps de $\mathbf{C}$. En effet, on dispose du morphisme

$$\begin{aligned} \mathsf{ev}_{\sqrt{2},\mathbf{Q}}\colon \mathbf{Q}[X] &\to \mathbf{C} \\ P &\mapsto P(\sqrt{2}) \end{aligned}$$

Son image est $\mathbf{Q}[\sqrt{2}]$ et son noyau $\langle X^2 - 2\rangle$ (cela résulte du fait que $\sqrt{2} \notin \mathbf{Q}$ et de la division euclidienne) : il induit un isomorphisme $\mathbf{Q}[X]/\langle X^2-2\rangle \xrightarrow{\sim} \mathbf{Q}[\sqrt{2}]$. Comme $X^2 - 2$ est irréductible dans $\mathbf{Q}[X]$, cela montre que $\mathbf{Q}[\sqrt{2}]$ est un corps : c'est donc une extension de $\mathbf{Q}$.

Définition 3.1.0.3. Les corps $\mathbf{Q}$ et $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ avec p premiers sont appelés les *corps premiers*.

Proposition 3.1.0.4. On a les deux possibilités suivantes :
(i) $\mathsf{car}(K) = 0$ donc $\mathbf{Q} \subset K$;
(ii) $\mathsf{car}(K) = p$ est premier et $\mathbf{F}_p \subset K$.

Démonstration. Rappelons qu'il existe un unique morphisme d'anneaux $c_K\colon \mathbf{Z} \to K$ et que la caractéristique de K est l'unique entier $\mathsf{car}(K) \in \mathbf{N}$ tel que $\mathsf{Ker}(c_K) = \mathsf{car}(K)\,\mathbf{Z}$. En passant au quotient, c_K induit un morphisme injectif $\mathbf{Z}/\mathsf{car}(K)\,\mathbf{Z} \to K$: comme K est un corps, l'anneau $\mathbf{Z}/\mathsf{car}(K)\,\mathbf{Z}$ est intègre *i.e.* l'idéal $\mathsf{car}(K)\,\mathbf{Z}$ est premier dans $\mathbf{Z}$. Ce qui signifie que $\mathsf{car}(K) = 0$ ou $\mathsf{car}(K)$ est un nombre premier.
• Si $\mathsf{car}(K) = 0$, le morphisme c_K est injectif, d'où $\mathbf{Z} \subset K$. Comme K est un corps, on a donc $\mathbf{Q} \subset K$ par la propriété universelle du corps des fractions.
• Si $\mathsf{car}(K) = p$ est premier, le morphisme c_K induit un morphisme injectif $\mathbf{F}_p \to K$. □

Exercice 3.1.0.5. Montrer que le seul automorphisme d'un corps premier est l'identité.

Remarque 3.1.0.6. Si L/K est une extension, alors L est naturellement muni d'une structure de K-espace vectoriel (on peut additionner les éléments de L et les multiplier par un élément de K).

Définition 3.1.0.7. Le *degré* de l'extension L/K est l'entier (fini ou infini) $[L : K] := \dim_K(L)$. Si le degré est fini, on dit que l'extension L/K est *finie*.

Exemple 3.1.0.8. On a :

$$[\mathbf{C} : \mathbf{R}] = 2, \qquad [\mathbf{R} : \mathbf{Q}] = \infty, \qquad [\mathbf{Q}(X) : \mathbf{Q}] = \infty, \qquad [\mathbf{Q}[\sqrt{2}] : \mathbf{Q}] = 2.$$

Des exemples d'extensions de K particulièrement importants sont fournis par l'énoncé suivant :

Théorème 3.1.0.9. Si $P \in K[X]$ est irréductible de degré d, le quotient $K[X]/\langle P(X)\rangle$ est une extension de degré d de K. Une base est fournie par $(1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1})$ où $\overline{X}$ désigne l'image de X dans $K[X]/\langle P(X)\rangle$.

Démonstration. Comme $K[X]$ est principal et P irréductible, l'idéal $\langle P(X)\rangle$ est maximal, donc $K[X]/\langle P(X)\rangle$ est un corps. Le morphisme composé $K \to K[X] \xrightarrow{\pi} K[X]/\langle P(X)\rangle$ (où π est la surjection canonique) identifie K à un sous-corps de $K[X]/\langle P(X)\rangle$. Si $Q \in K[X]$, la divison euclidienne de Q par P s'écrit $Q = DP + R$ avec $\deg(R) < d$: on a $\pi(Q) = \pi(R) \in \mathsf{Vect}(1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1})$ et la famille $(1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1})$ engendre le K-espace vectoriel $K[X]/\langle P(X)\rangle$. Elle est libre, car si $a_0 + a_1\overline{X} + \cdots + a_{d-1}\overline{X}^{d-1} = 0$, alors $P(X) \mid a_0 + a_1X + \cdots + a_{d-1}X^{d-1}$, ce qui implique $a_0 = \cdots = a_{d-1} = 0$ pour des raisons de degré. □

Remarque 3.1.0.10. (1) Calcul des inverses dans $K[X]/\langle P(X)\rangle$: Soient $a \in K[X]/\langle P(X)\rangle$ non nul et $Q \in K[X]$ un représentant de a. Comme P est irréductible et Q a une image non nulle modulo $\langle P\rangle$, les polynômes P et Q sont premiers entre eux : il existe une relation de Bézout (qu'on trouve grâce à l'algorithme d'Euclide étendu) $UP + QV = 1$ avec $U, V \in K[X]$. Dans $K[X]/\langle P(X)\rangle$, cette égalité s'écrit $\overline{QV} = 1$: un représentant de a^{-1} dans $K[X]$ est donné par V.
(2) On voit sur cet exemple d'où vient la terminologie de « degré » d'une extension.

Exemple 3.1.0.11. D'après le critère d'Eisenstein, le polynôme $P = X^2 - 2$ est irréductible dans $\mathbf{Z}[X]$: il l'est dans $\mathbf{Q}[X]$. L'extension correspondante est $\mathbf{Q}[\sqrt{2}] = \{x + y\sqrt{2} \mid x, y \in \mathbf{Q}\}$. C'est un corps et on a $[\mathbf{Q}[\sqrt{2}] : \mathbf{Q}] = 2$. Calculons l'inverse de $1 + \sqrt{2}$. Il est représenté par le polynôme $1 + X$ dans $\mathbf{Q}[X]$. On a $X^2 - 2 = (X-1)(X+1) - 1$, en projetant dans $\mathbf{Q}[\sqrt{2}]$, il vient $(1+\sqrt{2})^{-1} = -1 + \sqrt{2}$. En fait, on a trivialement $(x + y\sqrt{2})^{-1} = \frac{x - y\sqrt{2}}{x^2 - 2y^2}$ pour $(x, y) \in \mathbf{Q}^2 \setminus \{(0,0)\}$.

Exercice 3.1.0.12. Soit $P \in K[X]$. Montrer que les propriétés suivantes sont équivalentes :
(1) P est irréductible ;
(2) $K[X]/\langle P(X)\rangle$ est un corps ;
(3) $K[X]/\langle P(X)\rangle$ est intègre.
À quel condition sur P l'anneau $K[X]/\langle P(X)\rangle$ est-il réduit ?

Théorème 3.1.0.13 (de la base télescopique)**.** Si L/K et M/L sont des extensions, alors M/K est une extension et

$$[M : K] = [M : L][L : K].$$

Démonstration. Soient $(x_i)_{i\in I}$ une base de L sur K et $(y_j)_{j\in J}$ une base de M sur L. On a

$$L = \bigoplus_{i\in I} Kx_i \text{ et } M = \bigoplus_{j\in J} Ly_j \quad \text{donc} \quad M = \bigoplus_{j\in J}\left(\bigoplus_{i\in I} Kx_i\right) = \bigoplus_{i\in I, j\in J} Kx_iy_j$$

i.e. $(x_iy_j)_{i\in I, j\in J}$ est une base de M sur K. En particulier, on a : $[M : K] = \mathsf{Card}(I \times J) = \mathsf{Card}(J) \times \mathsf{Card}(I) = [M : L][L : K]$. □

Définition 3.1.0.14. Soit L/K une extension. Une *sous-extension* de L/K est un sous-corps E de L qui contient K.

Exemple 3.1.0.15. $\mathbf{R}$ est une sous-extension de $\mathbf{C}\,/\,\mathbf{Q}$.

Remarque 3.1.0.16. (1) D'après le théorème 3.1.0.13, si E/K est une sous-extension d'une extension finie L/K, alors $[E : K] \mid [L : K]$. Cela implique par exemple que si $[L : K]$ est premier, les seules sous-extensions de L/K sont L et K.
(2) Si L/K est une extension et $(E_i)_{i\in I}$ une famille de sous-extensions, alors $\bigcap_{i\in I} E_i$ est une extension de L/K.

Définition 3.1.0.17. Soient L/K une extension et $S \subset L$. La sous-extension de L/K *engendrée* par S est la plus petite sous-extension de L/K qui contient S. Elle existe et est unique : c'est l'intersection des sous-extensions de L/K qui contiennent S. On la note $K(S)$.
Si L/K est une extension et $S \subset L$, on dit que L est *engendrée* par S sur K si $L = K(S)$. L'extension L/K est dite *de type fini* si L peut être engendré par une famille finie sur K.

Remarque 3.1.0.18. (1) Il est facile de vérifier que l'ensemble sous-jacent à $K(S)$ est constitué des éléments qui peuvent s'écrire sous la forme $R(s_1, \ldots, s_n)$ avec $s_1, \ldots, s_n \in S$ et $R \in K(X_1, \ldots, X_n)$ une fraction rationnelle dont le dénominateur ne s'annule pas en $(s_1, \ldots, s_n)$.
(2) Si L/K est une extension finie, alors c'est une extension de type fini (une partie génératrice étant fournie par une base de L vu comme K-espace vectoriel). La réciproque est fausse : $\mathbf{Q}(X)$ est de type fini sur $\mathbf{Q}$, mais $[\mathbf{Q}(X) : \mathbf{Q}] = \infty$.

Définition 3.1.0.19. Soient L/K une extension et E_1, E_2 deux sous-extensions. Le *compositum* de ces sous-extensions est la sous-extension engendrée par $E_1 \cup E_2$. C'est la plus petite sous-extension de L/K qui contient E_1 et E_2 : on la note E_1E_2.

Remarque 3.1.0.20. (1) Si $E_1 = K(S_1)$ et $E_2 = K(S_2)$, alors $E_1E_2 = K(S_1 \cup S_2)$ (exercice).
(2) En général, $E_1 \cup E_2$ n'est pas une sous-extension de L/K.

3.2 Extensions algébriques

3.2.1 Éléments algébriques

Soient L/K une extension et $\alpha \in L$. On dispose du morphisme d'évaluation en α :

$$\begin{aligned} \mathsf{ev}_{\alpha,K} : K[X] &\to L \\ P &\mapsto P(\alpha) \end{aligned}$$

On note $K[\alpha]$ son image (on peut même remarquer que $K[\alpha] = \mathsf{Vect}(\alpha^k)_{k\in\mathbf{N}} \subset L$). Remarquons que $K(\alpha)$ n'est autre que le corps des fractions de $K[\alpha]$ dans L. On a donc $K[\alpha] \subset K(\alpha)$ et l'inclusion est stricte en général.

Définition 3.2.1.1. (i) On dit que α est *transcendant* sur K si le morphisme $\mathsf{ev}_{\alpha,K}$ est injectif et *algébrique* sur K dans le cas contraire.
(ii) Si α est algébrique sur K, on appelle *polynôme minimal* de α sur K l'unique générateur unitaire de $\mathsf{Ker}(\mathsf{ev}_{\alpha,K})$. On le note $P_{\alpha,K}$. Le *degré* de α sur K est le degré de $P_{\alpha,K}$, on le note $\deg_K(\alpha)$.

Remarque 3.2.1.2. Les notions qui précèdent dépendent très fortement du corps de base. Par exemple, si X est une indéterminée, alors $X \in \mathbf{Q}(X)$ est transcendant sur $\mathbf{Q}$, mais algébrique sur $\mathbf{Q}(X)$, puisque $P_{X,\mathbf{Q}(X)}(T) = T - X$ avec T une indéterminée. L'élément $i \in \mathbf{C}$ est algébrique sur $\mathbf{R}$ et sur $\mathbf{C}$, mais $P_{i,\mathbf{R}}(X) = X^2 + 1$ et $P_{i,\mathbf{C}}(X) = X - i$.

Exemple 3.2.1.3. (1) Si $L = K(X)$ et P est un polynôme non constant, alors P est transcendant sur K. Les nombres π et e sont transcendants sur $\mathbf{Q}$ (mais c'est un peu difficile à prouver).
(2) Si $\alpha \in K$, alors α est algébrique sur K et $P_{\alpha,K}(X) = X - \alpha$.
(3) Les nombres $\sqrt{2}$ et $\sqrt{2}+\sqrt{3}$ sont algébriques sur $\mathbf{Q}$, de polynômes minimaux sur $\mathbf{Q}$ respectifs X^2-2 et X^4-10X^2+1.

Proposition 3.2.1.4. Si L/K est une extension et $\alpha \in L$ est algébrique sur K, alors $P_{\alpha,K}$ est irréductible dans $K[X]$, l'anneau $K[\alpha]$ est un corps isomorphe à $K[X]/\langle P_{\alpha,K}\rangle$. En particulier, on a $K(\alpha) = K[\alpha]$ et $[K(\alpha) : K] = \deg_K(\alpha)$.

Démonstration. La décomposition canonique de $\mathsf{ev}_{\alpha,K} : K[X] \to L$ s'écrit

$$K[X] \to K[X]/\langle P_{\alpha,K}\rangle \xrightarrow{\sim} K[\alpha] \subset L.$$

Comme $K[\alpha] \subset L$, l'anneau $K[\alpha]$ est intègre : il en est de même de $K[X]/\langle P_{\alpha,K}\rangle$ qui lui est isomorphe. Cela implique que $P_{\alpha,K}$ est irréductible dans $K[X]$ et que $K[\alpha] \simeq K[X]/\langle P_{\alpha,K}\rangle$ est un corps. On a $[K[\alpha] : K] = \deg(P_{\alpha,K}) = \deg_K(\alpha)$. □

Remarque 3.2.1.5. Bien sûr, si L/K est une extension, $P \in K[X]$ un polynôme unitaire irréductible dans $K[X]$ et $\alpha \in L$ une racine de P, alors le polynôme minimal de α sur K n'est autre que P *i.e.* $P_{\alpha,K} = P$.

Proposition 3.2.1.6. Soient L/K une extension, E/K une sous-extension et $\alpha \in L$ algébrique sur K. L'élément α est alors algébrique sur E et $P_{\alpha,E} \mid P_{\alpha,K}$ dans $E[X]$.

Démonstration. Comme $P_{\alpha,K} \in \mathsf{Ker}(\mathsf{ev}_{\alpha,E})$, le morphisme $\mathsf{ev}_{\alpha,E}$ n'est pas injectif, *i.e.* α est algébrique sur E. Par définition, on a $\mathsf{Ker}(\mathsf{ev}_{\alpha,E}) = \langle P_{\alpha,E}\rangle$, donc $P_{\alpha,E} \mid P_{\alpha,K}$ dans $E[X]$. □

Exemple 3.2.1.7. (1) Les nombres $\sqrt{2}$ et $\sqrt{2}+\sqrt{3}$ sont algébriques sur $\mathbf{Q}$, donc *a fortiori* sur $E = \mathbf{Q}[\sqrt{2}]$. Les polynômes minimaux sur E sont $X - \sqrt{2}$ et $X^2 - 2\sqrt{2}X - 1$ respectivement.
(2) Si $n \in \mathbf{N}_{>0}$, le polynôme $X^n - 2$ est irréductible dans $\mathbf{Z}[X]$ en vertu du critère d'Eisenstein, donc aussi dans $\mathbf{Q}[X]$. Comme il admet $e^{\frac{2ik\pi}{n}}\sqrt[n]{2}$ comme racine, c'est le polynôme minimal de $e^{\frac{2ik\pi}{n}}\sqrt[n]{2}$ pour tout $k \in \{0,\dots,n-1\}$. Notons que les sous-extensions $\mathbf{Q}(\sqrt[n]{2})$ et $\mathbf{Q}(e^{\frac{2ik\pi}{n}}\sqrt[n]{2})$ de $\mathbf{C}$ sont isomorphes à $\mathbf{Q}[X]/\langle X^n - 2\rangle$, mais pas égales (la première est incluse dans $\mathbf{R}$ mais pas la deuxième).

Dans la pratique, il n'est pas toujours aisé de déterminer si un élément est algébrique sur un corps, *a fortiori* de déterminer son polynôme minimal. Cela dit, on dispose d'un critère (abstrait) d'algébricité très commode.

Proposition 3.2.1.8 (Critère d'algébricité)**.** Soient L/K une extension et $\alpha \in L$. Les conditions suivantes sont équivalentes :
(i) α est algébrique sur K ;
(ii) $K[\alpha]$ est un corps ;
(iii) $K(\alpha)$ est un K-espace vectoriel de dimension finie ;
(iv) il existe une sous-extension finie E de L/K telle que $\alpha \in E$.

Démonstration. • L'implication (i) ⇒ (ii) résulte de la proposition 3.2.1.4.
• Si $K[\alpha]$ est un corps, alors $K[\alpha] = K(\alpha)$ et $\mathsf{Ker}(\mathsf{ev}_{\alpha,K})$ est un idéal maximal de $K[X]$: il est donc engendré par un polynôme irréductible. Cela montre que α est algébrique sur K : la proposition 3.2.1.4 implique que $K(\alpha)$ est un K-espace vectoriel de dimension $\deg_K(P_{\alpha,K})$. On a donc (ii) ⇒ (iii).
• L'implication (iii) ⇒ (iv) est triviale (prendre $E = K(\alpha)$).
• Soit E une sous-extension finie de L/K telle que $\alpha \in E$. La famille $\{1, \alpha, \alpha^2, \dots\}$ est donc liée : il existe $N \in \mathbf{N}$ et $\lambda_0, \dots, \lambda_N \in K$ non tous nuls tels que $\lambda_0 + \lambda_1\alpha + \cdots + \lambda_N\alpha^N = 0$. Le polynôme $\lambda_0 + \lambda_1 X + \cdots + \lambda_N X^N$ est alors un élément non nul de $\mathsf{Ker}(\mathsf{ev}_{\alpha,K})$ et α est algébrique sur K. On a donc (iv) ⇒ (i). □

Exercice 3.2.1.9. Soit A un anneau contenant K comme sous-anneau. Supposons A intègre et de dimension finie comme K-espace vectoriel. Montrer que A est un corps (c'est donc une extension finie de K).

Corollaire 3.2.1.10. Soient L/K une extension et $\alpha, \beta \in L^\times$ algébriques sur K. Les éléments $\alpha-\beta$ et $\alpha\beta^{-1}$ sont algébriques sur K. En particulier, l'ensemble des éléments de L qui sont algébriques sur K forme une sous-extension de L/K.

Démonstration. D'après la proposition 3.2.1.6, l'élément β est algébrique sur $K(\alpha)$. Le K-espace vectoriel $K[\alpha] = K(\alpha)$ et le $K(\alpha)$-espace vectoriel $K(\alpha,\beta)$ sont de dimension finie. D'après le théorème de la base télescopique, le K-espace vectoriel $K(\alpha,\beta)$ est donc de dimension finie. Comme $\alpha-\beta, \alpha\beta^{-1} \in K(\alpha,\beta)$, les éléments $\alpha-\beta$ et $\alpha\beta^{-1}$ sont algébrique sur K en vertu de la proposition précédente. □

Définition 3.2.1.11. On pose

$$\overline{\mathbf{Q}} = \{z \in \mathbf{C};\ z \text{ est algébrique sur } \mathbf{Q}\}.$$

D'après le corollaire qui précède, c'est un sous-corps de $\mathbf{C}$, qu'on appelle le *corps des nombres algébriques*.

Proposition 3.2.1.12. Le corps $\overline{\mathbf{Q}}$ est dénombrable.

Démonstration. Si $P \in \mathbf{Q}[X]$, notons $\mathsf{Z}(P) = P^{-1}(0) \subset \mathbf{C}$ l'ensemble des racines de P. Pour $d \in \mathbf{N}_{>0}$, notons $\mathcal{E}_d$ l'ensemble des polynômes unitaires de degré d à coefficients dans $\mathbf{Q}$. Par définition, on a

$$\overline{\mathbf{Q}} = \bigcup_{d=1}^{\infty} \bigcup_{P\in\mathcal{E}_d} \mathsf{Z}(P).$$

Comme $\mathbf{Q}$ est dénombrable, il en est de même de $\mathcal{E}_d \simeq \mathbf{Q}^d$. Une union dénombrable d'ensembles dénombrables étant dénombrable et $\mathsf{Z}(P)$ étant fini pour tout $P \in \mathcal{E}_d$, l'ensemble $\bigcup_{P\in\mathcal{E}_d} \mathsf{Z}(P)$ est dénombrable pour tout $d \in \mathbf{N}_{>0}$: il en est donc de même de $\overline{\mathbf{Q}}$. □

Donnons-en quelques propriétés.

Corollaire 3.2.1.13. On a $\mathsf{Card}(\mathbf{C}\setminus\overline{\mathbf{Q}}) = \mathsf{Card}(\mathbf{C})$. En particulier, l'ensemble des nombres complexes transcendants sur $\mathbf{Q}$ est non vide (sa cardinalité est celle de $\mathbf{R}$).

Démonstration. On a :
$$\mathsf{Card}(\mathbf{C}) = \mathsf{Card}(\mathbf{R}) = 2^{\mathsf{Card}(\mathbf{N})} > \mathsf{Card}(\mathbf{N}) = \mathsf{Card}(\overline{\mathbf{Q}}).$$
On a donc $\mathsf{Card}(\mathbf{C}\setminus\overline{\mathbf{Q}}) = \mathsf{Card}(\mathbf{C})$. □

Remarque 3.2.1.14. Historiquement, l'existence des nombres transcendants a été prouvée différemment.

Théorème 3.2.1.15 (Liouville)**.** Soient $\alpha \in \overline{\mathbf{Q}} \cap \mathbf{R}$ de degré $d > 1$ sur $\mathbf{Q}$. Il existe alors une constante $c(\alpha) \in \mathbf{R}_{>0}$ telle que pour tout $(p, q) \in \mathbf{Z} \times \mathbf{N}_{>0}$, on a
$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}.$$

Démonstration. Soit $a \in \mathbf{N}_{>0}$ le ppcm des dénominateurs de $P_{\alpha,\mathbf{Q}}$, on a $P = aP_{\alpha,\mathbf{Q}} \in \mathbf{Z}[X]$. C'est le polynôme de degré $d > 1$, irréductible sur $\mathbf{Q}$. En particulier, si $p \in \mathbf{Z}$ et $q \in \mathbf{N}_{>0}$, on a $P(p/q) \neq 0$. Comme $q^d P(p/q) \in \mathbf{Z}$, on a $|q^d P(p/q)| \geqslant 1$ et donc $|P(\alpha) - P(p/q)| \geqslant q^{-d}$ vu que $P(\alpha) = 0$. La formule de Taylor implique qu'il existe $\theta \in [\alpha, p/q]$ tel que $P(\alpha) - P(p/q) = P'(\theta)(\alpha - p/q)$. Si $|\alpha - p/q| \leqslant 1$, on a donc $|P(\alpha) - P(p/q)| < M|\alpha - p/q|$ avec $M = 1 + \max\limits_{|\theta-\alpha|\leqslant 1} |P'(\theta)| \in \mathbf{R}_{\geqslant 1}$. Avec ce qui précède, on a donc $M|\alpha - p/q| > q^{-d}$ *i.e.* $|\alpha - p/q| > \frac{1}{Mq^d}$. Comme $M \geqslant 1$ et $q \geqslant 1$, cette inégalité est encore valable pour $|\alpha - p/q| > 1$. On peut donc prendre $c(\alpha) = M^{-1}$. □

Remarque 3.2.1.16. Le résultat précédent montre que les nombres algébriques s'approchent « mal » par les rationnels. C'est un des premiers résultats d'approximation diophantienne. Il a été raffiné par Baker de la façon suivante : pour tout $\varepsilon \in \mathbf{R}_{>0}$, il n'y a qu'un nombre fini de rationnels p/q avec $p \in \mathbf{Z}$ et $q \in \mathbf{N}_{>0}$ premiers entre eux tels que $\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{2+\varepsilon}}$. Il est facile de voir que ce résultat est optimal : pour tout réel x, il y a une infinité de rationnels p/q avec $p \in \mathbf{Z}$ et $q \in \mathbf{N}_{>0}$ premiers entre eux tels que $\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^2}$.

Corollaire 3.2.1.17. Le nombre $\sum\limits_{n=0}^{\infty} \frac{1}{2^{n!}}$ est transcendant sur $\mathbf{Q}$.

Démonstration. Posons $\alpha = \sum\limits_{n=0}^{\infty} \frac{1}{2^{n!}}$. On a déjà $\alpha \notin \mathbf{Q}$ puisque son développement en base 2 n'est pas périodique. Supposons-le algébrique de degré $d > 1$. Pour $N \in \mathbf{N}_{>0}$, posons $\alpha_N = \sum\limits_{n=0}^{N} \frac{1}{2^{n!}}$, $q_N = 2^{N!}$ et $p_N = \alpha_N q_N \in \mathbf{N}$. D'après le théorème 3.2.1.15, on a
$$\frac{c(\alpha)}{q_N^d} < \alpha - \alpha_N = \sum_{n>N} \frac{1}{2^{n!}}.$$
Pour $n > N$, on a $2^{n!} \geqslant 2^{(N+1)!} 2^{n-N-1}$: on a donc *a fortiori* $\frac{c(\alpha)}{2^{dN!}} < \frac{1}{2^{(N+1)!}} \sum\limits_{n>N} \frac{1}{2^{n-N-1}}$ soit encore $c(\alpha) 2^{(N+1)!-dN!} < 2$. Comme $c(\alpha) > 0$ et $\lim\limits_{N\to\infty} (N+1)! - dN! = +\infty$, on a $\lim\limits_{N\to\infty} c(\alpha) 2^{(N+1)!-dN!} = +\infty$, ce qui est absurde : α est donc transcendant. □

Malheureusement, il est rare qu'on puisse prouver qu'un nombre est transcendant en utilisant le théorème 3.2.1.15. Par exemple, on ne peut pas le faire avec e et π.

3.2.2 Extensions finies, extensions algébriques

Définition 3.2.2.1. Une extension L/K est dite *algébrique* si tous les éléments de L sont algébriques sur K.

Exemple 3.2.2.2. Les extensions $\overline{\mathbf{Q}}/\mathbf{Q}$ et $\mathbf{Q}(X)[\sqrt{2}]/\mathbf{Q}(X)$ sont algébriques, mais $\mathbf{R}/\mathbf{Q}$ et $\mathbf{Q}(X)/\mathbf{Q}$ ne le sont pas.

Proposition 3.2.2.3. Les intersections et les composées d'extensions algébriques sont algébriques. Une sous-extension engendrée par des éléments algébriques est algébrique.

Démonstration. C'est évident pour les intersections et pour les composés, cela résulte du corollaire 3.2.1.10. La dernière assertion résulte elle aussi du corollaire 3.2.1.10. □

Proposition 3.2.2.4. Une extension L/K est finie si et seulement si elle est algébrique et de type fini.

Démonstration. Si L/K est finie, alors elle est algébrique d'après la proposition 3.2.1.8 et de type fini (une partie génératrice étant donnée par une base du K-espace vectoriel L). Réciproquement, supposons L/K algébrique et de type fini : on a $L = K(\alpha_1, \ldots, \alpha_r)$ avec $\alpha_1, \ldots, \alpha_r$ algébriques sur K. Écrivons $L = K(\alpha_1)(\alpha_2)\cdots(\alpha_r)$. Pour tout $i \in \{1, \ldots, r\}$, l'élément α_i est algébrique sur K, donc sur $K(\alpha_1)\cdots(\alpha_{i-1})$ (proposition 3.2.1.6) : on a $[K(\alpha_1)\cdots(\alpha_i) : K(\alpha_1)\cdots(\alpha_{i-1})] < \infty$ et donc
$$[L : K] = \prod_{i=1}^{r} [K(\alpha_1)\cdots(\alpha_i) : K(\alpha_1)\cdots(\alpha_{i-1})] < \infty.$$
□

Remarque 3.2.2.5. (1) Plus précisément, on a montré qu'une extension L/K est finie si et seulement si elle est de la forme $L = K(\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n \in L$ algébriques sur K.
(2) Si K est de caractéristique nulle et L/K est finie, on peut montrer qu'il existe $\alpha \in L$ tel que $L = K(\alpha)$ (théorème de l'élément primitif).
(3) Une extension algébrique n'est pas nécessairement finie. Par exemple, l'extension $\overline{\mathbf{Q}}/\mathbf{Q}$ est algébrique par définition, mais pas de degré fini (car $n = [\mathbf{Q}(\sqrt[n]{2}) : \mathbf{Q}] \leqslant [\overline{\mathbf{Q}} : \mathbf{Q}]$ pour tout $n \in \mathbf{N}_{>0}$).

Exercice 3.2.2.6. Montrer que toute extension algébrique est réunion de ses sous-extensions finies.

Corollaire 3.2.2.7. Soient M/L et L/K deux extensions. L'extension M/K est algébrique si et seulement si M/L et L/K sont algébriques.

Démonstration. L'implication directe est évidente, prouvons la réciproque. Soit $\alpha \in M$: l'élément α est algébrique sur L. Notons L' le sous-corps de L engendrée par les coefficients de $P_{\alpha,L}$. Comme L/K est algébrique, L'/K est algébrique et comme $P_{\alpha,L}$ a un nombre fini de coefficients non nuls, L'/K est de type fini : l'extension L'/K est donc finie en vertu de la proposition 3.2.2.4. Comme $L'(\alpha) = L'[\alpha]$ est fini sur L' (proposition 3.2.1.8), l'extension $L'(\alpha)/K$ est finie et α est algébrique sur K d'après la proposition 3.2.1.8. □

Proposition 3.2.2.8. Soient L/K une extension et L_1/K, L_2/K deux sous-extensions finies. L'extension L_1L_2/K est finie et $[L_1L_2 : K] \leqslant [L_1 : K][L_2 : K]$.

Démonstration. D'après la proposition 3.2.2.4, il existe $\alpha_1, \ldots, \alpha_r \in L$ algébriques sur K tels que $L_2 = K(\alpha_1, \ldots, \alpha_r)$. On a $L_1L_2 = L_1(\alpha_1, \ldots, \alpha_r)$ et les inclusions

$$L_1 \subset L_1(\alpha_1) \subset \cdots \subset L_1(\alpha_1, \ldots, \alpha_{r-1}) \subset L_1L_2.$$

Pour tout $k \in \{1, \ldots, r\}$, l'élément α_k est algébrique sur $K(\alpha_1, \ldots, \alpha_{k-1})$ donc *a fortiori* sur $L_1(\alpha_1, \ldots, \alpha_{k-1})$. Par ailleurs, on a

$$[L_1(\alpha_1, \ldots, \alpha_k) : L_1(\alpha_1, \ldots, \alpha_{k-1})] \leqslant [K(\alpha_1, \ldots, \alpha_k) : K(\alpha_1, \ldots, \alpha_{k-1})]$$

en vertu de la proposition 3.2.1.6. En multipliant ces inégalités et en utilisant le théorème de la base télescopique, on en déduit que $[L_1L_2 : L_1] \leqslant [L_2 : K]$: en multipliant par $[L_1 : K]$ et en utilisant de nouveau le théorème de la base télescopique, il vient $[L_1L_2 : K] \leqslant [L_1 : K][L_2 : K]$. □

Remarque 3.2.2.9. (1) Une autre façon de prouver la proposition 3.2.2.8 est de choisir une base $(x_i)_{1\leqslant i\leqslant n}$ de L_1 sur K et une base $(y_j)_{1\leqslant j\leqslant n}$ de L_2 sur K et de montrer que la famille $(x_iy_j)_{1\leqslant i,j\leqslant n}$ engendre le K-espace vectoriel L_1L_2 (exercice).
(2) L'inégalité précédente peut être stricte. C'est trivialement le cas lorsque $L_1 = L_2 \neq K$. Autre exemple (plus instructif) : $K = \mathbf{Q}$, $L_1 = \mathbf{Q}(\sqrt[3]{2})$ et $L_2 = \mathbf{Q}(j\sqrt[3]{2})$.

Corollaire 3.2.2.10. Soient L/K une extension et L_1, L_2 deux sous-extensions finies telles que $\mathsf{pgcd}([L_1 : K], [L_2 : K]) = 1$, alors $[L_1L_2 : K] = [L_1 : K][L_2 : K]$.

Démonstration. D'après le théorème de la base télescopique, on a $[L_1 : K] \mid [L_1L_2 : K]$ et $[L_2 : K] \mid [L_1L_2 : K]$. Comme $\mathsf{pgcd}([L_1 : K], [L_2 : K]) = 1$, cela implique donc que $[L_1 : K][L_2 : K] \mid [L_1L_2 : K]$, d'où $[L_1L_2 : K] = [L_1 : K][L_2 : K]$ en vertu de la proposition précédente. □

Exercice 3.2.2.11. (1) Calculer les degrés de $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$, $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ sur $\mathbf{Q}$.
(2) Montrer que $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$ et $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbf{Q}(\sqrt{2} + \sqrt[3]{2})$.
(3) Soient L/K une extension et L_1, L_2 deux sous-extensions algébriques. Montrer que L_1L_2/K est algébrique.

3.2.3 Corps de rupture, corps de décomposition

Définition 3.2.3.1. Soient L/K une extension de corps et $P \in K[X]$.
(i) On dit que L est un *corps de rupture* si L est engendré sur K par une racine de P.
(ii) On dit que P est *scindé* sur L si ses facteurs irréductibles dans $L[X]$ sont de degré 1.
(iii) On dit que L est un *corps de décomposition* de P sur K si P est scindé dans $L[X]$ et que L est engendré sur K par les racines de P.

Exemple 3.2.3.2. (1) $\mathbf{C}$ est un corps de rupture (et de décomposition) de $X^2 + 1$ sur $\mathbf{R}$.
(2) Le corps $\mathbf{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2$ sur $\mathbf{Q}$, mais ce n'est pas un corps de décomposition, car il ne contient pas les racines $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$. Le corps $\mathbf{Q}(j, \sqrt[3]{2})$ est un corps de décomposition.

Proposition 3.2.3.3. Si $P \in K[X]$ est irréductible, le corps $K[X]/\langle P(X)\rangle$ est un corps de rupture de P sur K et tout corps de rupture de P sur K est isomorphe à $K[X]/\langle P(X)\rangle$.

Démonstration. Si $\overline{X}$ désigne la classe de X dans $K[X]/\langle P(X)\rangle$, alors $P(\overline{X}) = 0$ et $K[X]/\langle P(X)\rangle = K(\overline{X})$. Si L est un corps de rupture de P sur K, on a $L = K(\alpha)$ et $P(\alpha) = 0$. Le morphisme $\mathsf{ev}_{\alpha,K} \colon K[X] \to L$ est surjectif et son noyau contient P, donc égal à $\langle P(X)\rangle$ (car P est irréductible) : il induit un isomorphisme $K[X]/\langle P(X)\rangle \xrightarrow{\sim} L$. □

Corollaire 3.2.3.4. Tout $P \in K[X]$ admet un corps de décomposition.

Démonstration. On procède par récurrence sur $d = \deg(P)$, le cas $d = 1$ étant évident. Supposons $d > 1$. Comme $K[X]$ est factoriel (même principal), on peut écrire $P = P_1P_2$ avec $P_1, P_2 \in K[X]$ et P_1 irréductible (il suffit de prendre pour P_1 l'un des facteurs irréductibles de P). D'après la proposition 3.2.3.3, P_1 a un corps de rupture K' sur K. Dans $K'[X]$, on peut donc écrire $P = (X - \alpha_1)Q$ où $\alpha_1 \in K'$ est une racine de P_1 et $K' = K(\alpha_1)$. On applique alors l'hypothèse de récurrence à $Q \in K'[X]$: il admet un corps de décomposition L. Le polynôme Q est scindé dans $L[X]$ et $L = K'(\alpha_2, \dots, \alpha_r)$ où $\alpha_2, \dots, \alpha_r$ sont les racines de Q dans L. Le polynôme P est donc scindé dans L et $L = K(\alpha_1, \dots, \alpha_r)$ est engendré sur K par les racines de P. □

Exemple 3.2.3.5. Le polynôme $P(X) = X^3 - 2 \in \mathbf{Q}[X]$ est irréductible sur $\mathbf{Q}$. Un corps de rupture de P est $\mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{C}$. Un corps de décomposition est $\mathbf{Q}(\sqrt[3]{2}, j\sqrt[3]{2}) = \mathbf{Q}(j, \sqrt[3]{2})$ (notons également que $[\mathbf{Q}(j, \sqrt[3]{2}) : \mathbf{Q}] = 6$).

Exercice 3.2.3.6. Si $\deg(P) = d$ et L un corps de décomposition de P sur K, on a $[L : K] \leqslant d!$.

L'énoncé suivant est d'un usage constant pour construire des morphismes entre extensions algébriques.

Théorème 3.2.3.7 (Prolongement des isomorphismes)**.** Soient L_1/K_1 et L_2/K_2 des extensions, $\varphi\colon K_1 \xrightarrow{\sim} K_2$ un isomorphisme et $P \in K_1[X]$ un polynôme irréductible. Notons $\varphi(P) \in K_2[X]$ le polynôme irréductible obtenu en appliquant φ aux coefficients de P. Soient $\alpha \in L_1$ (resp. $\beta \in L_2$) une racine de P (resp. de $\varphi(P)$). Il existe alors un unique isomorphisme

$$\widetilde{\varphi}\colon K_1(\alpha) \xrightarrow{\sim} K_2(\beta)$$

qui prolonge φ et tel que $\widetilde{\varphi}(\alpha) = \beta$.

$$\begin{array}{ccc} L_1 & & L_2 \\ | & & | \\ K_1(\alpha) & \overset{\widetilde{\varphi}}{\dashrightarrow} & K_2(\beta) \\ | & & | \\ K_1 & \xrightarrow[\varphi]{} & K_2 \end{array}$$

Démonstration. On a les isomorphismes :

$$\iota_1\colon K_1[X]/\langle P(X)\rangle \xrightarrow{\sim} K_1(\alpha) \quad \text{et} \quad \iota_2\colon K_2[X]/\langle \varphi(P)(X)\rangle \xrightarrow{\sim} K_2(\beta).$$

Par ailleurs, l'isomorphisme $\varphi\colon K_1 \xrightarrow{\sim} K_2$ induit un isomorphisme $\varphi\colon K_1[X] \xrightarrow{\sim} K_2[X]$ et donc un isomorphisme

$$\varphi\colon K_1[X]/\langle P(X)\rangle \xrightarrow{\sim} K_2[X]/\langle \varphi(P)(X)\rangle.$$

On a également $\varphi\colon K_1[X] \to K_2[X]$ mais $K_1[X] \twoheadrightarrow K_1[X]/\langle P(X)\rangle$ et $K_2[X] \twoheadrightarrow K_2[X]/\langle \varphi(P)(X)\rangle$. L'isomorphisme cherché est alors le composé

$$K_1(\alpha) \xrightarrow{\iota_1^{-1}} K_1[X]/\langle P(X)\rangle \xrightarrow{\varphi} K_2[X]/\langle \varphi(P)(X)\rangle \xrightarrow{\iota_2} K_2(\beta)$$

avec $\widetilde{\varphi} = \iota_2 \circ \varphi \circ \iota_1^{-1}$. □

Le théorème qui précède nous amène naturellement à la définition suivante.

Définition 3.2.3.8. Soient L/K une extension et $\alpha, \beta \in L$ algébriques sur K. On dit que α et β sont *conjugués* sur K s'ils ont même polynôme minimal sur K.

Corollaire 3.2.3.9. D'après le théorème 3.2.3.7 $\alpha, \beta \in L$ sont conjugués sur K si et seulement s'il existe un K-isomorphisme $\sigma\colon K(\alpha) \xrightarrow{\sim} K(\beta)$ tel que $\sigma(\alpha) = \beta$.

Corollaire 3.2.3.10. Si $P \in K[X]$, deux corps de décomposition de P sur K sont isomorphes comme extensions de K.

Démonstration. On montre l'énoncé plus fort suivant : si $\varphi\colon K_1 \to K_2$ est un isomorphisme de corps, $P \in K_1[X]$ non constant et L_1 (resp. L_2) un corps de décomposition de P (resp. de $\varphi(P)$) sur K_1 (resp. sur K_2), alors φ se prolonge en un isomorphisme $L_1 \xrightarrow{\sim} L_2$. On procède par récurrence sur $d = \deg(P)$. Si $d = 1$, il n'y a rien à faire. Si $d > 1$, soit $\alpha \in L_1$ une racine de P : on a $P_{\alpha,K_1} \mid P$, donc $\varphi(P_{\alpha,K_1})$ est un polynôme irréductible qui divise $\varphi(P)$. Soit $\beta \in L_2$ une racine de $\varphi(P_{\alpha,K_1})$. D'après le théorème 3.2.3.7, l'isomorphisme φ se prolonge en un isomorphisme $\varphi' : K_1(\alpha) \xrightarrow{\sim} K_2(\beta)$. Par ailleurs, on peut écrire $P(X) = (X - \alpha)Q(X)$ avec $Q \in K_1(\alpha)[X]$ de degré $d - 1$. On a $\varphi(P)(X) = (X - \beta)\varphi(Q)(X)$ dans $K_2(\beta)[X]$: on conclut en appliquant l'hypothèse de récurrence à φ' et Q (car L_1 est un corps de décomposition de P sur $K_1(\alpha)$ et L_2 de $\varphi'(Q)$ sur $K_2(\beta)$). □

3.3 Corps algébriquement clos, clôture algébrique

Définition 3.3.0.1. Soit K un corps. Les propriétés suivantes sont équivalentes :
(i) Tout polynôme à coefficients dans K est scindé ;
(ii) Tout polynôme non constant à coefficients dans K admet une racine dans K ;
(iii) K n'a pas d'extension algébrique non triviale.
Si elle sont vérifiées, on dit que K est *algébriquement clos.*

Théorème 3.3.0.2 (D'Alembert-Gauss)**.** Le corps $\mathbf{C}$ est algébriquement clos.

Démonstration. Soit $P \in \mathbf{C}[X]\backslash\mathbf{C}$. On a $\lim\limits_{|z|\to\infty} |P(z)| = +\infty$. Il existe donc $r \in \mathbf{R}_{>0}$ tel que $|z| > r \Rightarrow |P(z)| > |P(0)|$. On a donc $\inf\limits_{z\in\mathbf{C}} |P(z)| = \inf\limits_{z\in D_r} |P(z)|$, avec $D_r = \{z \in \mathbf{C};\ |z| \leqslant r\}$. Comme D_r est compact, l'inf est atteint : il existe donc $z_0 \in D_r$ tel que $|P(z)| \geqslant |P(z_0)|$ pour tout $z \in \mathbf{C}$. Supposons $P(z_0) \neq 0$: quitte à remplacer $P(X)$ par $P(z_0)^{-1}P(X+z_0)$, on peut supposer que $z_0 = 0$ et que $P(0) = 1$. On peut donc écrire $P(X) = 1 + aX^n(1 + XQ(X))$ avec $a \in \mathbf{C}^\times$, $n \in \mathbf{N}_{>0}$ et $Q \in \mathbf{C}[X]$. Écrivons $a = \rho e^{i\theta}$ avec $\rho \in \mathbf{R}_{>0}$ et $\theta \in \mathbf{R}$ et posons $z = te^{i\frac{\pi-\theta}{n}}$ avec $t \in \mathbf{R}_{>0}$: on a $P(z) = 1 - \rho t^n + \mathsf{O}(t^{n+1})$ quand t tend vers 0. Cela implique que $|P(z)| < 1$ pour t assez petit : contradiction. □

Corollaire 3.3.0.3. Les polynômes irréductibles dans $\mathbf{R}[X]$ sont :
(i) Les polynômes de degré 1 ;
(ii) Les trinômes du second degré à discriminant strictement négatif.

Démonstration. Soit $P \in \mathbf{R}[X]$ irréductible de degré > 1. Comme $\mathbf{C}$ est algébriquement clos, P admet une racine $\alpha \in \mathbf{C}$. On a $\alpha \notin \mathbf{R}$ vu que $\deg(P) > 1$. Comme $[\mathbf{C} : \mathbf{R}] = 2$, on a nécessairement $\deg(P) = 2$. Par ailleurs, $P(\overline{\alpha}) = \overline{P(\alpha)} = 0$: comme $\alpha \neq \overline{\alpha}$, on a $P(X) = a(X-\alpha)(X-\overline{\alpha})$, dont le discriminant est $a^2(\alpha-\overline{\alpha})^2 \in \mathbf{R}_{<0}$. □

Définition 3.3.0.4. Soit K un corps. Une *clôture algébrique* de K est une extension $\overline{K}/K$ algébrique telle que $\overline{K}$ est algébriquement clos.

Proposition 3.3.0.5. Si C/K est une extension avec C algébriquement clos, alors la sous-extension

$$\overline{K} = \{z \in C;\ z \text{ est algébrique sur } K\}$$

est une clôture algébrique de K.

Démonstration. Commençons par remarquer que $\overline{K}/K$ est algébrique en vertu du corollaire 3.2.1.10. Si $L/\overline{K}$ une extension algébrique, alors L/K est algébrique en vertu du corollaire 3.2.2.4 et donc $L \subset \overline{K}$ *i.e.* $L = \overline{K}$. □

Exemple 3.3.0.6. La proposition précédente et le fait que $\mathbf{C}$ est algébriquement clos impliquent que $\overline{\mathbf{Q}}$ est une clôture algébrique de $\mathbf{Q}$.

Théorème 3.3.0.7 (Steiniz)**.** Tout corps K admet une clôture algébrique. En outre, si $\overline{K}$ est une clôture algébrique et si C/K est une extension avec C algébriquement clos, il existe un K-morphisme $\overline{K} \to C$. En particulier, les clôtures algébriques de K sont deux à deux isomorphes.

Commençons par une construction qui va nous être utile pour prouver l'existence : soit $(P_\lambda)_{\lambda\in\Lambda}$ la famille des polynômes irréductibles unitaires de $K[X]$. Posons $A = K[X_\lambda]_{\lambda\in\Lambda}$ (anneau de polynômes en une infinité de variables) et notons I l'idéal de A engendré par les éléments $P_\lambda(X_\lambda) \in A$. Supposons $I = A$: il existe une égalité de la forme

$$\sum_{i=1}^{n} Q_i P_{\lambda_i}(X_{\lambda_i}) = 1 \qquad (\clubsuit)$$

avec $\lambda_1, \ldots, \lambda_n \in \Lambda$ et $Q_1, \ldots, Q_n \in A$. Soit L/K une extension telle que le polynôme P_{λ_i} admet une racine α_i, dans L pour tout $i \in \{1, \ldots, n\}$ (il suffit d'appliquer n fois la proposition 3.2.3.3). Considérons alors le morphisme d'anneaux K-linéaire $\varphi\colon A \to L$ défini par $\varphi(X_\lambda) = \alpha_i$ si $\lambda = \lambda_i$ pour $i \in \{1, \ldots, n\}$ et 0 sinon. En appliquant φ à l'égalité ($\clubsuit$), il vient que $0 = 1$ ce qui est absurde : l'idéal I est donc strict.

D'après le théorème de Krull, il existe un idéal maximal $\mathfrak{m}$ de A tel que $I \subset \mathfrak{m}$: posons $\widetilde{K} = A/\mathfrak{m}$. C'est un corps et c'est une extension algébrique de K, parce qu'il est engendré sur K par les classes des X_λ pour $\lambda \in \Lambda$ et qu'on a $P_\lambda(X_\lambda) = 0$ dans le quotient $\widetilde{K} = A/\mathfrak{m}$. Par ailleurs, si $P \in K[X]$ est non constant, il admet une racine dans $\widetilde{K}$. En effet, il existe $\lambda \in \Lambda$ tel que P_λ soit un facteur irréductible de P et P_λ a une racine dans $\widetilde{K}$ (la classe de X_λ).

Démonstration. • Montrons l'existence. On définit par récurrence une suite d'extensions de K de la façon suivante : on pose $K_0 = K$ et $K_{n+1} = \widetilde{K}_n$ pour tout $n \in \mathbf{N}$. Posons $\overline{K} = \bigcup\limits_{n=0}^{\infty} K_n$. C'est un corps comme réunion croissante de corps et c'est une extension algébrique de K, car pour tout $n \in \mathbf{N}$, l'extension K_{n+1}/K_n est algébrique d'après ce qui précède (*cf.* corollaire 3.2.2.7). Par ailleurs, le corps $\overline{K}$ est algébriquement clos : si $P \in \overline{K}[X]$, il existe $n \in \mathbf{N}$ tel que $P \in K_n[X]$: si P est non constant, il admet une racine dans $\widetilde{K}_n = K_{n+1}$ et donc dans $\overline{K}$.
• Montrons la deuxième partie du théorème : soit C une extension algébriquement close de K. Notons $\mathcal{E}$ l'ensemble des K-morphismes $f\colon L \to C$ où L est une sous-extension de $\overline{K}/K$. On l'ordonne en posant

$$(f_1\colon L_1 \to C) \leqslant (f_2\colon L_2 \to C) \Leftrightarrow (L_1 \subset L_2 \text{ et } f_{2|L_1} = f_1)$$

Il est immédiat que l'ensemble ordonné $(\mathcal{E}, \leqslant)$ est inductif : d'après le théorème de Zorn, il admet un élément maximal $f_0 \colon L_0 \to C$. Supposons $L_0 \neq \overline{K}$. Soit $\alpha \in \overline{K} \backslash L_0$. Comme C est algébriquement clos, le polynôme $f_0(P_{\alpha,L_0}) \in f_0(L_0)$ admet une racine $\beta \in C$. D'après le théorème 3.2.3.7, il existe un unique prolongement

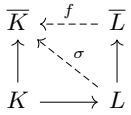
$$\widehat{f_0} \colon L_0[\alpha] \to f_0(L_0)[\beta] \subset C$$

de f_0 tel que $\widehat{f_0}(\alpha) = \beta$. Mais $\widehat{f_0} > f_0$ dans $\mathcal{E}$: contradiction avec la maximalité de f_0. On a donc $L_0 = \overline{K}$, d'où le résultat.

• Soit $\overline{K}'$ une autre clôture algébrique de K. En appliquant ce qui précède à $\overline{K}$ et $\overline{K}'$ respectivement, on dispose de K-morphismes $f \colon \overline{K} \to \overline{K}'$ et $g \colon \overline{K}' \to \overline{K}$. Le composé $g \circ f \colon \overline{K} \to \overline{K}$ est injectif et a pour image une extension algébriquement close $C \subset \overline{K}$ de K. Comme $\overline{K}/K$ est algébrique, il en est de même de $\overline{K}/C$. Comme C est algébriquement clos, on a $C = \overline{K}$ et $g \circ f$ est surjectif. Il en est donc de même pour g, qui est donc un isomorphisme. □

Corollaire 3.3.0.8. Soient L/K une extension algébrique et $\overline{K}$ une clôture algébrique de K. Il existe alors un K-morphisme $L \to \overline{K}$.

Démonstration. Soit $\overline{L}$ une clôture algébrique de L. Comme $\overline{L}/L$ et L/K sont algébriques, il en est de même de $\overline{L}/K$ (corollaire 3.2.2.7). Cela implique que $\overline{L}$ est aussi une clôture algébrique de K. D'après le théorème de Steiniz, on dispose d'un K-morphisme $f : \overline{L} \to \overline{K}$. Le composé de ce dernier avec le morphisme structural $L \to \overline{L}$ fournit l'application σ recherchée.



□

Remarque 3.3.0.9. Il résulte du corollaire 3.3.0.8 qu'on peut toujours prolonger une extension L/K dans une clôture algébrique de K. Il est donc généralement possible (et commode) de travailler avec des sous-corps d'un corps algébriquement clos fixé de K : d'après ce qui précède, ce n'est pas une restriction sérieuse.

3.4 Extensions cyclotomiques

Soit $n \in \mathbf{N}_{>0}$. On pose $\varphi(n) = \mathsf{Card}((\mathbf{Z}/n\,\mathbf{Z})^\times)$ (indicatrice d'Euler). On rappelle que si

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

est la décomposition en facteurs premiers de n, on a $\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{\alpha_i - 1}$ (on se ramène facilement au cas où $r = 1$ grâce au théorème des restes chinois). Posons

$$\mu_n = \{z \in \mathbf{C} \mid z^n = 1\} = \left\{ e^{\frac{2ik\pi}{n}} \right\}_{0 \leqslant k < n}.$$

C'est un sous-groupe cyclique de $\mathbf{C}^\times$. On a même un isomorphisme

$$\begin{aligned} \mathbf{Z}/n\,\mathbf{Z} &\xrightarrow{\sim} \mu_n \\ \overline{k} &\mapsto \zeta^k \end{aligned}$$

Notons μ_n^* le sous-ensemble de μ_n constitué des éléments d'ordre n, *i.e.* des générateurs du groupe μ_n *i.e.*

$$\mu_n^* = \left\{ e^{\frac{2ik\pi}{n}} \right\}_{\substack{0 \leqslant k < n \\ k \wedge n = 1}}$$

(ses éléments sont les *racines primitives n-ièmes de l'unité*). On a même une bijection

$$(\mathbf{Z}/n\,\mathbf{Z})^\times \xrightarrow{\sim} \mu_n^*.$$

On a

$$\mu_n = \bigsqcup_{d \mid n} \mu_d^*$$

(c'est la partition de μ_n suivant l'ordre des éléments). Fixons $\zeta \in \mu_n^*$ une racine n-ième primitive de l'unité. On pose

$$\Phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi) = \prod_{\substack{1 \leqslant k < n \\ k \wedge n = 1}} (X - \zeta^k).$$

C'est un polynôme de degré $\varphi(n)$, unitaire, séparable, à coefficients dans $\mathbf{C}$.

Exemple 3.4.0.1. On a

$$\begin{aligned}
\Phi_1(X) &= X-1\\
\Phi_2(X) &= X+1\\
\Phi_3(X) &= X^2+X+1\\
\Phi_4(X) &= X^2+1\\
\Phi_5(X) &= X^4+X^3+X^2+X+1\\
\Phi_6(X) &= X^2-X+1\\
\Phi_7(X) &= X^6+X^5+X^4+X^3+X^2+X+1\\
\Phi_8(X) &= X^4+1\\
\Phi_9(X) &= X^6+X^3+1.
\end{aligned}$$

Remarque 3.4.0.2. Contrairement aux apparences, les coefficients des polynômes cyclotomiques ne sont pas tous dans $\{0,\pm 1\}$: par exemple, on a

$$\begin{aligned}
\Phi_{105}(X) = X^{48}&+X^{47}+X^{46}-X^{43}-X^{42}-2X^{41}-X^{40}-X^{39}+X^{36}\\
&+X^{35}+X^{34}+X^{33}+X^{32}+X^{31}-X^{28}-X^{26}-X^{24}-X^{22}-X^{20}+X^{17}\\
&+X^{16}+X^{15}+X^{14}+X^{13}+X^{12}-X^9-X^8-2X^7-X^6-X^5+X^2+X+1.
\end{aligned}$$

Proposition 3.4.0.3. Pour tout $n\in\mathbf{N}_{>0}$, on a

$$X^n-1=\prod_{d|n}\Phi_d(X)\quad n=\sum_{d|n}\varphi(d)\quad\text{et}\quad\Phi_n\in\mathbf{Z}[X].$$

Démonstration. • Les racines du polynômes X^n-1 dans $\mathbf{C}$ sont les éléments de μ_n et elles sont toutes simples. La partition des μ_d^* implique donc que

$$X^n-1=\prod_{\xi\in\mu_n}(X-\xi)=\prod_{d|n}\prod_{\xi\in\mu_d^*}(X-\xi)=\prod_{d|n}\Phi_d(X).$$

L'égalité $n=\sum_{d|n}\varphi(d)$ se déduit de la précédente en prenant les degrés.

• Pour voir que $\Phi_n\in\mathbf{Z}[X]$, on procède par récurrence sur $n\in\mathbf{N}_{>0}$. On a $\Phi_1(X)=X-1$. Si $n>1$ et $\Phi_1,\dots,\Phi_{n-1}\in\mathbf{Z}[X]$, alors $Q(X)=\prod_{\substack{d|n\\ d<n}}\Phi_d(X)\in\mathbf{Z}[X]$ est unitaire : on dispose de la division euclidienne de X^n-1 par $Q(X)$ dans $\mathbf{Z}[X]$, ce qui montre que $\Phi_n\in\mathbf{Z}[X]$. □

Exemple 3.4.0.4. Si p est premier et $r\in\mathbf{N}_{>0}$, on a $\Phi_{p^r}(X)=\frac{X^{p^r}-1}{X^{p^{r-1}}-1}$: on a donc en particulier

$$\Phi_p(X)=1+X+\cdots+X^{p-1}$$

et $\Phi_{p^r}(X)=\Phi_p(X^{p^{r-1}})$.

On a vu (*cf.* exemple 2.7.4.10 (3)) que Φ_p est irréductible dans $\mathbf{Q}[X]$. C'est un fait général :

Proposition 3.4.0.5. Si $n\in\mathbf{N}_{>0}$, le polynôme Φ_n est irréductible sur $\mathbf{Q}$. En particulier, c'est le polynôme minimal de ζ sur $\mathbf{Q}$.

On va énoncer un lemme avant de démontrer la proposition 3.4.0.5.

Lemme 3.4.0.6. Soient A un anneau factoriel, $K=\mathsf{Frac}(A)$ et $P,Q\in K[X]$ unitaires tels que $PQ\in A[X]$. On a alors $P,Q\in A[X]$.

Démonstration. Soient $a,b\in A\backslash\{0\}$ tels que $aP,bQ\in A[X]$. D'après le lemme 2.7.2.3, on a $aP=\mathsf{c}(aP)\widetilde{P}$ et $bQ=\mathsf{c}(bQ)\widetilde{Q}$ avec $\widetilde{P},\widetilde{Q}\in A[X]$ primitifs. Comme P est unitaire, on a $\mathsf{c}(aP)\mid a$. De même, on a $\mathsf{c}(bQ)\mid b$. Par ailleurs, on a $abPQ=\mathsf{c}(aP)\,\mathsf{c}(bQ)\widetilde{P}\widetilde{Q}$ et donc $ab=\mathsf{c}(aP)\,\mathsf{c}(bQ)$ en prenant le contenu. Cela implique que a et $\mathsf{c}(aP)$ sont associés dans A, donc $P=\frac{\mathsf{c}(aP)}{a}\widetilde{P}\in A[X]$ et de même $Q\in A[X]$. □

Démonstration de la proposition 3.4.0.5. • Soit P le polynôme minimal de ζ sur $\mathbf{Q}$ (comme ζ est racine de $\Phi_n\in\mathbf{Q}[X]$, c'est un élément algébrique sur $\mathbf{Q}$). Écrivons $\Phi_n=PQ$ avec $Q\in\mathbf{Q}[X]$. Remarquons qu'on a en fait $P,Q\in\mathbf{Z}[X]$ d'après le lemme 3.4.0.6. Il s'agit de montrer que $P=\Phi_n$.

• Soit p un entier premier ne divisant pas n. En réduisant modulo p, on a $\overline{\Phi}_n=\overline{PQ}$. Comme p est premier à n, le polynôme X^n-1 est séparable (sans facteur carré) sur $\mathbf{F}_p$. Il en est donc de même du polynôme $\overline{\Phi}_n$, donc des polynômes $\overline{P}$ et $\overline{Q}$, puis on a $\mathsf{pgcd}(\overline{P},\overline{Q})=1$.

• Comme ζ^p est racine de Φ_n (car $p\nmid n$), c'est une racine de P ou de Q. Supposons que ce soit une racine de Q, alors ζ est racine de $Q(X^p)$ et P divise $Q(X^p)$. En réduisant modulo p, on a $\overline{P}\mid\overline{Q}(X^p)=\overline{Q}^p$, ce qui est impossible vu que $\mathsf{pgcd}(\overline{P},\overline{Q})=1$. L'élément ζ^p est donc racine de P.

• Comme toute racine n-ième primitive de l'unité est de la forme $\zeta^{p_1p_2\cdots p_r}$ avec $p_1,\dots,p_r$ des nombres premiers (pas forcément distincts) ne divisant pas n, on en déduit que toute les racines n-ièmes primitives de l'unité sont racines de P *i.e.* que $\Phi_n\mid P$. On a bien $P=\Phi_n$. □

3.5 Corps finis

Dans tout ce qui suit, K désigne un corps fini.

3.5.1 Propriétés de base

Proposition 3.5.1.1. (i) $p := \mathsf{car}(K)$ est un nombre premier ;
(ii) on a $\#K = p^d$ avec $d \in \mathbf{N}_{>0}$.

Démonstration. (i) Cela résulte de la proposition 3.1.0.4.
(ii) D'après (i), K est une extension de $\mathbf{F}_p := \mathbf{Z}/p\,\mathbf{Z}$ et $d := [K : \mathbf{F}_p] < +\infty$. On a $K \simeq \mathbf{F}_p^d$ vu comme $\mathbf{F}_p$-espace vectoriel et donc $\#K = p^d$. □

Contrairement à nos conventions, on ne va pas supposer les anneaux commutatifs a priori dans l'énoncé suivant.

Théorème 3.5.1.2 (Wedderburn)**.** Tout corps fini est commutatif.

Démonstration. On fait agir $K^\times$ sur lui-même par conjugaison. Pour $x \in K^\times$, on pose $K_x = \{y \in K;\ xy = yx\}$: c'est un sous-corps de K et si $x \neq 0$, le groupe $K_x^\times$ est le stabilisateur de x dans $K^\times$. On note $F = \bigcap_{x \in K^\times} K_x$ le centre de K. Soit q sont cardinal. Pour $x \in K$, on a $F \subset K_x$, de sorte que K_x soit un F-espace vectoriel, nécessairement de dimension fini vu que K est fini. Si $d_x = \dim_F(K_x)$, on a $\#K_x = q^{d_x}$. Soient $\{x_1, \dots, x_r\} \subset K^\times$ une famille de représentants des orbites non ponctuelles de $K^\times$: on a la partition

$$K^\times = F^\times \sqcup \bigsqcup_{i=1}^{r} \{y^{-1}x_i y;\ y \in K^\times\}$$

(l'union est bien disjointe). Comme $\{y^{-1}x_i y\}_{y \in K^\times} \simeq K^\times / K_{x_i}^\times$ (relation orbite-stabilisateur), l'équation aux classes s'écrit donc

$$q^d - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^d - 1}{q^{d_i} - 1}$$

où $d = \dim_F(K)$ et $d_i = d_{x_i}$ pour $i \in \{1, \dots, r\}$. Supposons K non commutatif, c'est-à-dire $d > 1$. Pour tout δ diviseur de d, on a $\Phi_d(X) \mid \frac{X^d - 1}{X^\delta - 1}$, donc $\Phi_d(q) \mid \frac{q^d - 1}{q^{d_i} - 1}$ pour tout $i \in \{1, \dots, r\}$. On a donc $\Phi_d(q) \mid q - 1$ en vertu de l'équation aux classes. On a donc $|\Phi_d(q)| = \prod_{\substack{1 \leqslant j < d \\ \mathsf{pgcd}(j,d)=1}} |q - \zeta^j| > (q-1)^{\varphi(d)} \geqslant q - 1$ (avec $\zeta = e^{\frac{2i\pi}{d}} \in \mathbf{C}$), ce qui contredit le fait que $\Phi_d(q) \mid q - 1$. □

3.5.2 Existence et unicité des corps finis

On a vu que si K est un corps fini, alors $\#K$ est une puissance d'un nombre premier. Nous allons voir que réciproquement, si p est un nombre premier et $d \in \mathbf{N}_{>0}$, alors il existe un corps de cardinal p^d, unique à isomorphisme près. On va utiliser les deux lemmes suivants.

Lemme 3.5.2.1. Soient A un anneau commutatif de caractéristique p et $a, b \in A$. On a

$$(a + b)^p = a^p + b^p.$$

Démonstration. Comme a et b commutent, on a $(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$ (binôme de Newton). Si $1 \leqslant k < p$, on a $p \mid \binom{p}{k}$: comme A est de caractéristique p, l'image de $\binom{p}{k}$ dans A est donc nulle et $(a + b)^p = a^p + b^p$. □

Remarque 3.5.2.2. Bien entendu, il est important de supposer A commutatif et p premier.

Définition 3.5.2.3. Soient F un corps et $P \in F[X]$. On dit que P est *séparable* si ses racines (prises dans une clôture algébrique de F) sont simples.

Lemme 3.5.2.4. Si F est un corps, un polynôme $P \in F[X]$ est séparable si et seulement si $\mathsf{pgcd}(P, P') = 1$ (où P' désigne le polynôme dérivé).

Démonstration. Soient $\overline{F}$ une clôture algébrique de F et $\alpha \in \overline{F}$ une racine de P : on peut écrire $P(X) = (X - \alpha)^m Q(X)$ avec $m \in \mathbf{N}_{>0}$ (c'est la multiplicité de α) et $Q \in \overline{F}[X]$ tel que $Q(\alpha) \neq 0$. En dérivant, il vient

$$P'(X) = m(X - \alpha)^{m-1} Q(X) + (X - \alpha)^m Q'(X) = (X - \alpha)^{m-1}(mQ(X) + (X - \alpha)Q'(X)).$$

Si P est séparable, on a $m = 1$, donc $P'(\alpha) = Q(\alpha) \neq 0$, donc $X - \alpha \nmid \mathsf{pgcd}(P, P')$: comme c'est vrai pour toute racine α de P, cela implique que $\mathsf{pgcd}(P, P') = 1$. Si P n'est pas séparable, on peut choisir α telle que $m > 1$, alors $X - \alpha \mid \mathsf{pgcd}(P, P')$ et $\mathsf{pgcd}(P, P') \neq 1$: par contraposée, on a la réciproque. □

Remarque 3.5.2.5. Si $\mathsf{car}(F) = p > 0$, il faut prendre garde au phénomène suivant. Le polynôme dérivé de X^p est $pX^{p-1} = 0$: des polynômes non constants peuvent avoir une dérivée nulle. Plus précisément, les polynômes de dérivée nulle sont ceux de la forme $Q(X^p)$ avec $Q \in F[X]$ (exercice).

Exercice 3.5.2.6. (1) Soit $P \in F[X]$ un polynôme irréductible. Montrer que P est séparable si et seulement si $P' \neq 0$. En déduire que tout polynôme irréductible est séparable lorsque $\mathsf{car}(F) = 0$.
(2) Soient p un nombre premier, X et T deux indéterminées. Posons $F = \mathbf{F}_p(T)$. Montrer que le polynôme $P(X) = X^p - T$ est irréductible dans $F[X]$, mais pas séparable. *(Indication : $X^p - T = (X - T^{1/p})^p$.)*

Théorème 3.5.2.7. Soient p un nombre premier, $d \in \mathbf{N}_{>0}$ et $q = p^d$.
(i) Il existe un corps à q éléments ;
(ii) Tout corps à q éléments est un corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$. En particulier, deux corps à q éléments sont isomorphes.

Démonstration. (ii) Commençons par l'unicité : soit K un corps de cardinal q. Le groupe $K^\times$ est d'ordre $q-1$: si $\alpha \in K^\times$, on a $\alpha^{q-1} = 1$ (théorème de Lagrange), donc $\alpha^q = \alpha$. C'est encore vrai lorsque $\alpha = 0$. Il en résulte que les éléments de K sont tous des racines du polynôme $X^q - X$: ce dernier est scindé dans K, à racines simples. Cela montre que K est un corps de décomposition de $X^q - X$ sur $\mathbf{F}_p$.
(i) Montrons l'existence : soit K un corps de décomposition de $P(X) := X^q - X$ sur $\mathbf{F}_p$: c'est une extension finie de $\mathbf{F}_p$, donc un corps fini. Soit $Z := \{\alpha \in K \mid \alpha^q = \alpha\}$ l'ensemble des racines de P. Comme $P'(X) = -1$, le polynôme P est séparable : on a $\#Z = q$. D'après le lemme 3.5.2.1, Z est un sous-anneau de K. C'est donc un sous-corps de K (si $\alpha \in Z \backslash \{0\}$, on a $\alpha^{q-1} = 1$). Par définition d'un corps de décomposition, on a donc $Z = K$ et $\#K = q$. □

Dans la pratique, on fixe une clôture algébrique $\overline{\mathbf{F}}_p$ de $\mathbf{F}_p$ et on pose

$$\mathbf{F}_q = \{\alpha \in \overline{\mathbf{F}}_p;\ \alpha^q = \alpha\}.$$

Corollaire 3.5.2.8. (i) $\mathbf{F}_q$ est l'unique sous-corps de cardinal q dans $\overline{\mathbf{F}}_p$;
(ii) On a : $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n} \Leftrightarrow d \mid n$;
(iii) On a également : $\mathbf{F}_{p^d} \cap \mathbf{F}_{p^n} = \mathbf{F}_{p^{\mathsf{pgcd}(d,n)}}$;
(iv) On a enfin : $\overline{\mathbf{F}}_p = \bigcup_{n=1}^{\infty} \mathbf{F}_{p^n}$.

Démonstration. Le point (i) résulte du théorème précédent. On a $[\mathbf{F}_{p^d} : \mathbf{F}_p] = d$ et $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$: si $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}$, on a $n = d[\mathbf{F}_{p^n} : \mathbf{F}_{p^d}]$ et $d \mid n$. Réciproquement, si $d \mid n$ et $\alpha \in \mathbf{F}_{p^d}$, on a $\alpha^{p^d} = \alpha$, donc $\alpha^{p^{kd}} = \alpha$ pour tout $k \in \mathbf{N}$ et donc $\alpha^{p^n} = \alpha$ *i.e.* $\alpha \in \mathbf{F}_{p^n}$: cela montre (ii). Le point (iii) en découle et (iv) résulte de (i) et de la définition d'une clôture algébrique. □

Remarque 3.5.2.9. (1) On n'a pas $\mathbf{F}_{p^n} \xrightarrow{\sim} \mathbf{Z}/p^n\mathbf{Z}$ dès que $n > 1$ (l'anneau $\mathbf{Z}/p^n\mathbf{Z}$ n'est pas réduit si $n > 1$). De même, on a $\mathbf{F}_{p^n} \xrightarrow{\sim} \mathbf{F}_p^n$ en tant que $\mathbf{F}_p$-espace vectoriel, mais pas en tant qu'anneau si $n > 1$ (l'anneau produit $\mathbf{F}_p^n$ n'est pas intègre si $n > 1$).
(2) On a $\mathbf{F}_4 \not\subset \mathbf{F}_8$ (en fait on a $\mathbf{F}_4 \cap \mathbf{F}_8 = \mathbf{F}_2$).

Exercice 3.5.2.10. Montrer que $\sum_{\alpha \in \mathbf{F}_q} \alpha = 0$. Plus généralement, calculer les polynômes symétriques élémentaires en les q éléments de $\mathbf{F}_q$. Calculer la somme $\sum_{\alpha \in \mathbf{F}_q} \alpha^k$ pour tout $k \in \mathbf{N}_{>0}$.

3.5.3 Structure du groupe multiplicatif

Commençons par rappeler le résultat classique suivant.

Lemme 3.5.3.1. Soit G un groupe abélien (noté multiplicativement).
(i) Soient $x \in G$ d'ordre n et $y \in G$ d'ordre m avec $\mathsf{pgcd}(n, m) = 1$. L'élément xy est d'ordre nm.
(ii) Supposons G fini et notons d le ppcm des ordres des éléments de G (on appelle d *l'exposant* de G). Le groupe G contient un élément d'ordre d.

Démonstration. (i) On a déjà $(xy)^{nm} = (x^n)^m(y^m)^n = 1$. Par ailleurs, si $(xy)^k = 1$, alors *a fortiori* $(xy)^{mk} = x^{mk} = 1$ et donc $n \mid mk$. Comme $\mathsf{pgcd}(n, m) = 1$, on a $n \mid k$. De même, on a $m \mid k$ (en échangeant les rôles de x et de y) et donc $nm = \mathsf{ppcm}(n, m) \mid k$. Ainsi, xy est d'ordre nm.
(ii) Écrivons la décomposition de d en facteurs premiers : $d = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $\alpha_i \in \mathbf{N}_{>0}$ pour $i \in \{1, \ldots, r\}$. Comme d est le ppcm des ordres des éléments de G, pour tout $i \in \{1, \ldots, r\}$, il existe $x_i \in G$ d'ordre divisible par $p_i^{\alpha_i}$. Quitte à remplacer x_i par une puissance convenable de x_i, on peut supposer que x_i est exactement d'ordre $p_i^{\alpha_i}$. L'élément $x = x_1 x_2 \cdots x_r \in G$ est alors d'ordre d d'après (i). □

Théorème 3.5.3.2. Si F est un corps et G un sous-groupe fini de $F^\times$, alors G est cyclique.

Démonstration. Soit d l'exposant de G : par définition, les éléments de G sont racines du polynôme $X^d - 1$. Ce dernier a au plus d racines dans le corps F : on a $\#G \leqslant d$. D'après le lemme 3.5.3.1, G contient un élément x d'ordre d : on a $\#G \geqslant d$, donc $\#G = d$ et $G = \langle x \rangle$ est cyclique. □

En particulier, on a :

Corollaire 3.5.3.3. Le groupe $K^\times$ est cyclique.

Corollaire 3.5.3.4 (Théorème de l'élément primitif pour un corps fini)**.** Si $\mathsf{car}(K) = p$, il existe $\alpha \in K$ tel que $K = \mathbf{F}_p(\alpha)$.

Démonstration. Si $\langle\alpha\rangle = K^\times$, alors $K^\times = \{1, \alpha, \dots, \alpha^{q-2}\}$, donc $\mathbf{F}_p(\alpha) \subset K = \{0, 1, \alpha, \dots, \alpha^{q-2}\} \subset \mathbf{F}_p(\alpha)$. □

Dans la pratique, si p est premier et $d \in \mathbf{N}_{>0}$, pour construire et manipuler le corps $\mathbf{F}_{p^d}$, on le présente sous la forme $\mathbf{F}_p[X]/\langle P(X)\rangle$ avec $P \in \mathbf{F}_p[X]$ irréductible de degré d.

D'après le théorème 3.5.2.7 et le corollaire 3.5.3.4, c'est toujours possible et le résultat ne dépend pas à isomorphisme près du choix de P. Dans le quotient $\mathbf{F}_p[X]/\langle P(X)\rangle$, on dispose de la base canonique $(1, \overline{X}, \overline{X}^2, \dots, \overline{X}^{d-1})$: on peut représenter les éléments dans cette base. Il est alors très facile de les additionner, un peu plus délicat de les multiplier (il faut multiplier des représentants et prendre le reste de la division euclidienne par P).

Exemple 3.5.3.5. (1) On a $\mathbf{F}_4 \simeq \mathbf{F}_2[X]/\langle X^2 + X + 1\rangle$;
(2) On a aussi $\mathbf{F}_8 \simeq \mathbf{F}_2[X]/\langle X^3 + X + 1\rangle \simeq \mathbf{F}_2[X]/\langle X^3 + X^2 + 1\rangle$.

Exercice 3.5.3.6. Soient q une puissance d'un nombre premier et $n \in \mathbf{N}_{>0}$. Posons

$$\begin{aligned}\varphi\colon\ \mathbf{F}_{q^n} &\to \mathbf{F}_{q^n}\\ \alpha &\mapsto \alpha^q\end{aligned}$$

(1) Montrer que $\varphi \in \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q)$ (le groupe des automorphismes de l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$).

Solution : Comme on est en caractéristique p, l'application $x \mapsto x^p$ est un morphisme d'anneaux : il en est de même de φ, qui est son itérée a-ième si $q = p^a$. Étant un morphisme de corps, φ est injectif. C'est un isomorphisme par cardinalité. Par ailleurs, il induit l'identité sur $\mathbf{F}_q$ (les éléments de $\mathbf{F}_q$ sont précisément les éléments $x \in \mathbf{F}_{q^n}$ tels que $x^q = x$)
(2) Soient $P \in \mathbf{F}_q[X]$ de degré d, irréductible dans $\mathbf{F}_q[X]$ et $\alpha \in \mathbf{F}_{q^n}$ une racine de P. Montrer que les racines de P sont $\{\varphi^k(\alpha)\}_{0\leqslant k<d}$ (et donc P est scindé dans $\mathbf{F}_{q^d} \subset \mathbf{F}_{q^n}$).

Solution : Commençons par observer que comme P est irréductible de degré d sur $\mathbf{F}_q$, on a $[F_q(\alpha) : \mathbf{F}_q] = d$: cela implique que $\mathbf{F}_q(\alpha) = \mathbf{F}_{q^d}$. On a donc $\alpha^{q^d} = \alpha$ *i.e.* $\varphi^d(\alpha) = \alpha$. Posons $Q = \prod_{k=0}^{d-1}(X - \varphi^k(\alpha)) \in \mathbf{F}_{q^d}[X]$. On a alors

$$\begin{aligned}\varphi(Q) &= (X - \varphi(\alpha))(X - \varphi^2(\alpha))\cdots(X - \varphi^{d-1}(\alpha))(X - \varphi^d(\alpha))\\ &= (X - \varphi(\alpha))(X - \varphi^2(\alpha))\cdots(X - \varphi^{d-1}(\alpha))(X - \alpha)\\ &= Q\end{aligned}$$

ce qui montre que les coefficients de Q appartiennent à $\{x \in \mathbf{F}_{q^d};\ \varphi(x)\} = \mathbf{F}_q$ *i.e.* $Q \in \mathbf{F}_q[X]$. Comme $Q(\alpha) = 0$, on a $P \mid Q$ (parce que, étant irréductible sur $\mathbf{F}_q$, le polynôme P est le polynôme minimal de α sur $\mathbf{F}_q$). On a donc $P = cQ$ où c est le coefficient dominant de P, pour des raisons de degré.
(3) Montrer que l'application

$$\begin{aligned}\mathbf{Z}/n\mathbf{Z} &\to \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q)\\ k &\mapsto \varphi^k\end{aligned}$$

est un isomorphisme de groupes (indication : pour la surjectivité, appliquer (2) à α tel que $\mathbf{F}_{q^n} = \mathbf{F}_q(\alpha)$).

Solution : L'application $\mathbf{Z} \to \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q)$; $k \mapsto \varphi^k$ est un morphisme de groupes. Son noyau est l'ensemble des $k \in \mathbf{Z}$ tels que $\varphi^k = \mathsf{Id}_{\mathbf{F}_{q^n}}$ *i.e.* tels que $x^{q^k} = x$ pour tout $x \in \mathbf{F}_{q^n}$. Or $\{x \in \overline{\mathbf{F}}_q;\ x^{q^k} = x\} = \mathbf{F}_{q^k}$: la condition qui précède équivaut à $\mathbf{F}_{q^n} \subset \mathbf{F}_{q^k}$. Comme on l'a déjà vu, cela équivaut à $n \mid k$. Le noyau du morphisme est donc $n\mathbf{Z}$: il se factorise en un morphisme de groupes injectif $\mathbf{Z}/n\mathbf{Z} \to \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q)$. Montrons qu'il est surjectif. Choisissons un élément primitif α de l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ et notons P son polynôme minimal sur $\mathbf{F}_q$. Soit $f \in \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q)$. Comme P est à coefficients dans $\mathbf{F}_q$ et f induit l'identité sur $\mathbf{F}_q$, on a $P(f(\alpha)) = f(P(\alpha)) = 0$ *i.e.* $f(\alpha)$ est une racine de P. D'après la question (2), il existe $k \in \{0, \dots, n-1\}$ tel que $f(\alpha) = \varphi^k(\alpha)$. Cela implique que f et φ^k coïncident sur $\mathbf{F}_q$ et en α : comme $\mathbf{F}_{q^n} = \mathbf{F}_q(\alpha)$, ils sont égaux, ce qui conclut.
(4) Montrer que les applications

$$\begin{aligned}\{\text{sous-extension de } \mathbf{F}_{q^n}/\mathbf{F}_q\} &\leftrightarrow \{\text{sous-groupes de } \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q)\}\\ F &\mapsto \{\sigma \in \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q);\ \sigma_{|F} = \mathsf{Id}_F\}\\ \{\alpha \in \mathbf{F}_{q^n};\ (\forall \sigma \in H)\ \sigma(\alpha) = \alpha\} &\hookleftarrow H\end{aligned}$$

sont des bijections décroissantes inverses l'une de l'autre.

Solution : Les applications sont bien définies et clairement décroissantes pour l'inclusion. Soit F une sous-extension de $\mathbf{F}_{q^n}/\mathbf{F}_q$: on a $F = \mathbf{F}_{q^d}$ avec $d \mid n$. Le sous-groupe $H = \{\sigma \in \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q);\ \sigma_{|F} = \mathsf{Id}_F\}$ est alors le sous-groupe engendré par φ^d (ce n'est que la question (3) appliquée à $\mathbf{F}_{q^d}$ à la place de $\mathbf{F}_q$). On a alors

$$\{x \in \mathbf{F}_{q^n};\ (\forall \sigma \in H)\ \sigma(x) = x\} = \{x \in \mathbf{F}_{q^n};\ \varphi^d(x) = x\} = \{x \in \mathbf{F}_{q^n};\ x^{q^d} = x\} = \mathbf{F}_{q^d} = F.$$

De même, soit H un sous-groupe de $\mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q)$. Comme on l'a vu dans la question (3), ce dernier est cyclique d'ordre n, engendré par φ. On connaît les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$: ce sont les $d\mathbf{Z}/n\mathbf{Z}$ avec $d \mid n$. Il existe donc $d \mid n$ tel que $H = \langle\varphi^d\rangle \leqslant \langle\varphi\rangle = \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q)$. On a alors $F := \{x \in \mathbf{F}_{q^n};\ (\forall \sigma \in H)\ \sigma(x) = x\} = \mathbf{F}_{q^d}$ comme on l'a vu ci-dessus et $\{\sigma \in \mathsf{Aut}(\mathbf{F}_{q^n}/\mathbf{F}_q);\ \sigma_{|F} = \mathsf{Id}_F\} = \langle\varphi^d\rangle \leqslant \langle\varphi\rangle = H$ (là encore, on l'a vu ci-dessus). Finalement, on a montré qu'en composant les deux applications dans les deux sens, on obtient l'identité : ce sont des bijections inverses l'une de l'autre.

3.6 Extensions quadratiques

Soit K un corps.

Définition 3.6.0.1. Une extension de K est dite *quadratique* si elle est de degré 2.

Proposition 3.6.0.2. Si $\mathsf{car}(K) \neq 2$ et si L/K est une extension quadratique, il existe $\alpha \in L\backslash K$ tel que $L = K(\alpha)$ et $\alpha^2 \in K$ (*i.e.* L s'obtient à partir de K par adjonction d'une racine carrée). Si en outre $L = K(\beta)$ avec $\beta^2 \in K$, il existe $c \in K^\times$ tel que $\beta = c\alpha$.

Démonstration. • Soit $\alpha_0 \in L\backslash K$: comme $[L : K] = 2$, on a $L = K(\alpha_0)$ et α_0 est de degré 2 sur K. Soit $X^2 + aX + b$ son polynôme minimal : comme $\mathsf{car}(K) \neq 2$, on peut écrire $\left(\alpha_0 + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} = 0$. On a donc $\alpha^2 \in K$ avec $\alpha = \alpha_0 + \frac{a}{2} \in L$. Comme $\frac{a}{2} \in K$, on a aussi $K(\alpha) = K(\alpha_0) = L$.
• Écrivons $\beta = c\alpha + d$ avec $c, d \in K$. Comme $\beta \notin K$, on a $c \neq 0$. Par ailleurs, on a $\beta^2 = c^2\alpha^2 + d^2 + 2cd\alpha$. Comme $(1, \alpha)$ est une K-base de L et $\beta^2 \in K$, on a $2cd = 0$. Comme $\mathsf{car}(K) \neq 2$ et $c \in K^\times$, cela implique $d = 0$, donc $\beta = c\alpha$. □

3.7 Application aux constructions à la règle et au compas

Soit $\mathscr{P}$ le plan affine euclidien. On s'intéresse au problème suivant. Étant données deux points $P_0, P_1 \in \mathscr{P}$ distincts, quels sont les points $P \in \mathscr{P}$ qu'on peut construire avec une règle non graduée et un compas ?

Il s'agit des points $P \in \mathscr{P}$ tels qu'il existe une suite $P_0, P_1, \ldots, P_{n-1}, P_n = P$ telle que pour tout $i \in \{2, \ldots, r\}$, le point P_i s'obtient à partir de

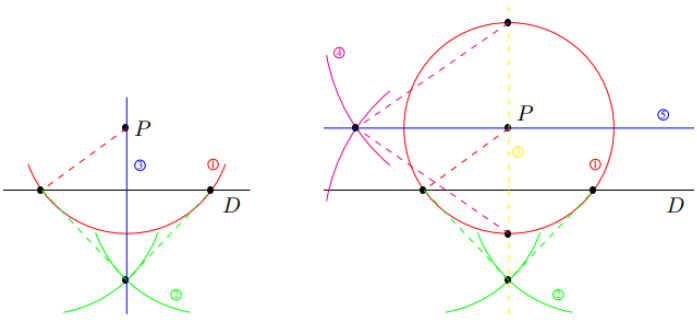
$$\mathscr{E}_i = \{P_0, P_1, \ldots, P_{i-1}\}$$

en effectuant l'une des deux opérations suivantes.

- tracer une droite passant par deux points de $\mathscr{E}_i$;
- tracer un cercle centré en un point de $\mathscr{E}_i$ et passant par un point de $\mathscr{E}_i$;

et en prenant l'intersection des figures ainsi obtenues.

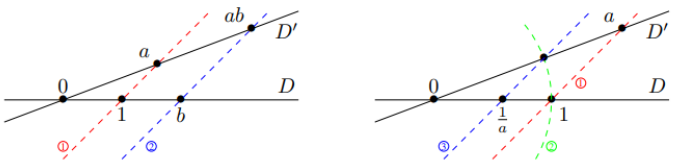
Remarquons déjà que si D est une droite et P un point (qui peut appartenir à D) on sait construire la perpendiculaire à D qui passe par P et donc la projection de P sur D. Par ailleurs, en itérant cette opération, on sait construire la parallèle à D passant par P.



Définition 3.7.0.1. Ainsi, on peut construire la perpendiculaire Δ' à $\Delta := (P_0, P_1)$ passant par P_0. Cela nous donne un repère : si P est un point de $\mathscr{P}$, on peut construire ses projections sur Δ et Δ'. Cela permet de décrire les points constructibles par leurs coordonnées (la longueur P_0P_1 étant l'unité). Tout le problème consiste donc à déterminer quelles sont les nombres réels qui sont coordonnées de points constructibles. On appelle ces réels les *nombres constructibles*.

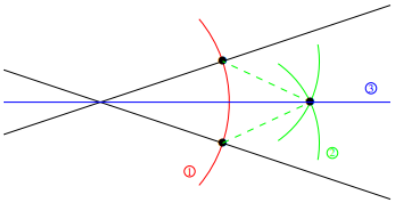
Proposition 3.7.0.2. L'ensemble des nombres constructibles est un sous-corps de $\mathbf{R}$.

Démonstration. Comme on peut reporter des longueurs avec le compas, il est clair que la somme et la différence de deux nombres constructibles est encore constructible. Il s'agit de prouver qu'on peut construire le produit de deux nombres constructibles, ainsi que l'inverse d'un nombre constructible non nul. Cela s'appuie sur le théorème de Thalès.



□

Remarque 3.7.0.3. Rappelons que la bissectrice de deux droites de $\mathscr{P}$ est constructible à la règle et au compas :



Proposition 3.7.0.4. Soit $x \in \mathbf{R}$. L'élément x est constructible si et seulement si il existe une suite d'extensions $\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$ telle que $x \in K_r$ et $[K_i : K_{i-1}] = 2$ pour tout $i \in \{1, \ldots, r\}$. En particulier, il est nécessaire (mais pas suffisant en général) que $[\mathbf{Q}(x) : \mathbf{Q}]$ soit une puissance de 2.

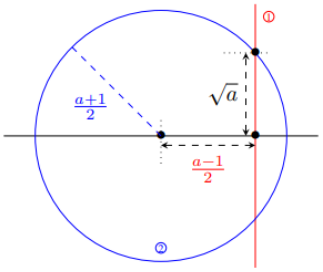
Démonstration. Soit $K/\mathbf{Q}$ une extension constituée de nombres constructibles.
• Les droites (resp. les cercles) que l'on peut tracer à partir des points de $\mathscr{P}$ correspondants on des équations de la forme

$$\alpha x + \beta y + \gamma = 0 \qquad (\text{resp. } x^2 + y^2 + \alpha x + \beta y + \gamma = 0).$$

Les points d'intersections des objets ainsi construits sont solutions de systèmes linéaires ou de la forme

$$\begin{cases} \alpha x + \beta y + \gamma & = 0 \\ x^2 + y^2 + \alpha x + \beta y + \gamma & = 0 \end{cases}$$

(le cas d'une intersection de deux cercles se ramenant à ce dernier système car la différence de deux équations de cercles donne une équation de droite). Par élimination, leurs coordonnées sont solutions d'équations du premier ou deuxième degré. Elles engendrent donc une extension de K de degré 1 (auquel cas K ne change pas) ou 2.
• Réciproquement, si L est une extension quadratique réelle de K, il existe $\alpha \in L \backslash K$ tel que $a := \alpha^2 \in K$: on a $L = K(\sqrt{a})$ et il s'agit de voir que $\alpha = \sqrt{a}$ est constructible. Cela résulte de la construction suivante.



Comme a est constructible, il en est de même de $\frac{a-1}{2}$ et $\frac{a+1}{2}$. On trace la perpendiculaire à (OP) d'abscisse $\frac{a-1}{2}$ et le cercle de centre O et de rayon $\frac{a+1}{2}$. Leurs points d'intersection ont pour coordonnées $\pm\sqrt{a}$. □

Corollaire 3.7.0.5. Les problèmes suivants ne peuvent pas se résoudre à la règle et au compas :
(i) *La quadrature du cercle* (*i.e.* étant donnée un cercle, construire un carré de même aire), ceci parce que π est transcendant.
(ii) *Doubler le volume d'un cube* (*i.e.* étant donné un cube, construire un cube de volume double - c'est dans l'espace et non le plan -), ceci parce que $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$.
(iii) *La trisection de l'angle* (sauf pour des angles particuliers bien sûr). En effet, en vertu de la formule $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$, cela revient à construire une racine du polynôme $4X^3 - 3X - \alpha$ pour $\alpha \in \mathbf{R}$ constructible, mais cela définit des éléments de degré 3 sur $\mathbf{Q}(\alpha)$ en général.

Corollaire 3.7.0.6. Soit p un nombre premier impair. Pour que le polygône régulier à p côtés soit constructible, il faut que $p = 2^{2^r} + 1$ avec $r \in \mathbf{N}_{>0}$ (un tel nombre s'appelle un *nombre premier de Fermat*).

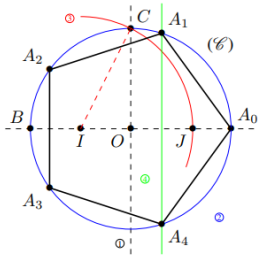
Démonstration. Il s'agit de construire les racines p-ièmes de l'unité. Le polynôme correspondant est le p-ième polynôme cyclotomique $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Il est irréductible et l'extension correspondante est de degré $\varphi(p) = p - 1$: il est donc nécessaire que $p - 1$ soit une puissance de 2. Supposons $p = 2^n + 1$. Si n n'est pas une puissance de 2, on a $n = uv$ avec u impair et alors $p = 2^{uv} + 1 = (2^v + 1)(2^{v(u-1)} - 2^{v(u-2)} + \cdots - 2^v + 1)$ ce qui contredit le fait que p est premier. On a donc $n = 2^r$ avec $r \in \mathbf{N}_{>0}$. □

Remarque 3.7.0.7. (1) Le corollaire 3.7.0.6 fournit une condition nécessaire. En fait, elle est suffisante (mais il est utile de connaître la *théorie de Galois*, qui sera vue en M1, pour le prouver). Pour $r = 0, 1, 2, 3$, on obtient les nombres premiers $3, 5, 17$ et 257 respectivement. Pour $p = 17$, la construction a été donnée par Gauss en 1796 (à l'âge de 19 ans...).
(2) Tout point du plan constructible à la règle et au compas peut être construit en utilisant le compas seul (*théorème de Mohr-Mascheroni*).
(3) Tout point du plan constructible à la règle et au compas peut être construit à la règle seule à condition que soit donné un cercle et son centre (*théorème de Poncelet-Steiner*).

Exemple 3.7.0.8 (Construction du pentagone d'après Ptolémée)**.** Posons $\zeta = e^{\frac{2i\pi}{5}}$. Il s'agit de construire le point $\zeta = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)$, soit encore le réel $\gamma = \cos\left(\frac{2\pi}{5}\right)$. Comme $\zeta \neq 1$ et $(\zeta-1)(\zeta^4+\zeta^3+\zeta^2+\zeta+1) = \zeta^5 - 1 = 0$, on a $\zeta^4+\zeta^3+\zeta^2+\zeta+1 = 0$. Mais $\zeta^3 = e^{\frac{6i\pi}{5}} = e^{\frac{-4i\pi}{5}} = \overline{\zeta}^2$ et $\zeta^4 = e^{\frac{8i\pi}{5}} = e^{\frac{-2i\pi}{5}} = \overline{\zeta}$: on a donc $(\zeta^2+\overline{\zeta}^2)+(\zeta+\overline{\zeta})+1 = 0$ *i.e.* $2\cos\left(\frac{4\pi}{5}\right)+2\cos\left(\frac{2\pi}{5}\right)+1 = 0$. Comme $\cos\left(\frac{4\pi}{5}\right) = 2\cos^2\left(\frac{2\pi}{5}\right)-1$ (car $\cos(2\theta) = 2\cos^2(\theta)-1$), on a donc $(2\gamma)^2+(2\gamma)-1 = 0$. Les racines du polynôme X^2+X-1 étant $\frac{-1\pm\sqrt{5}}{2}$ et comme $\gamma > 0$ (car $\frac{2\pi}{5} \in]0, \frac{\pi}{2}[$), on a $\gamma = \frac{\sqrt{5}-1}{4}$.

Soient O et A_0 deux points distincts du plan $\mathscr{P}$. Construisons le pentagone régulier de centre O et qui admet A_0 comme sommet. On prend la droite (OA_0) comme axe des abscisses et longueur OA_0 comme unité. Il s'agit de construire les points A_1, A_2, A_3 et A_4 de coordonnées respectives ζ, ζ^2, ζ^3 et ζ^4.

On commence par tracer la droite (OA_0) et la perpendiculaire Δ à (OA_0) en O. On trace ensuite le cercle $(\mathscr{C})$ de centre O qui passe par A_0. Il recoupe la droite (OA_0) en B et coupe Δ en C. Notons I le milieu du segment $[OB]$ (on peut construire la médiatrice de $[OB]$). Le cercle de centre I et de rayon $[IC]$ coupe le segment $[OA_0]$ au point J. Comme I est d'abscisse $-\frac{1}{2}$, on a $IC = \frac{\sqrt{5}}{2}$ (Pythagore) et $OJ = \frac{\sqrt{5}-1}{2} = 2\gamma$. La médiatrice du segment $[OJ]$ coupe donc $(\mathscr{C})$ en A_1 et A_4. Le cercle de centre A_1 (resp. A_4) et de rayon $[A_1A_0]$ (resp. $[A_4A_0]$) recoupe le cercle $(\mathscr{C})$ en A_2 (resp. A_3), ce qui achève la construction.



Exercice 3.7.0.9. Montrer qu'un polygone régulier à n côtés peut être construit à la règle et au compas si et seulement si n se décompose sous la forme $n = 2^k p_1 \cdots p_r$ où $k \in \mathbf{N}$ et $p_1, \ldots, p_r$ sont des nombres premiers de Fermat distincts.