

Table des matières

1	Groupes	2
1.1	Rappels	2
1.2	Le groupe symétrique	4
1.3	Produits semi-directs	6
1.4	Actions de groupes	8
2	Anneaux et polynômes	10
2.1	Rappels sur les anneaux	10
2.2	Idéaux premiers, idéaux maximaux	14
2.3	Anneaux principaux	15
2.4	Anneaux de séries formelles, anneaux des polynômes	18
2.5	Corps des fractions	20
2.6	Irréductibilité des polynômes	21
3	Extensions de corps	24
3.1	Définitions	24
3.2	Extensions algébriques	25
3.3	Corps algébriquement clos, clôture algébrique	28
3.4	Extensions quadratiques	29
3.5	Extensions cyclotomiques	30
3.6	Corps finis	31

Bibliographie sommaire

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

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

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

J.-P. Serre, *Groupes finis*, *Cours à l'École Normale supérieure de Jeunes Filles 1978/79*, document électronique disponible [en ligne](#)

1 Groupes

1.1 Rappels

1.1.1 Relations d'équivalence et ensembles quotients

Définition 1.1.2. Soit X un ensemble. Une *relation d'équivalence* sur X est une relation binaire \mathcal{R} sur X vérifiant les propriétés suivantes :

- réflexivité $(\forall x \in X) x\mathcal{R}x$;
- symétrie $(\forall x, y \in X) x\mathcal{R}y \Rightarrow y\mathcal{R}x$;
- transitivité $(\forall x, y, z \in X) (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

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 $[x_1] \cap [x_2] = \emptyset$: les classes d'équivalence forment une partition de X . Cette partition détermine entièrement \mathcal{R} : on a $x\mathcal{R}y \Leftrightarrow [x] = [y]$. L'*ensemble quotient* X/\mathcal{R} est la partie de $\mathcal{P}(X)$ constituée par les classes d'équivalences. Si $A \in X/\mathcal{R}$, on a $A = [x]$ pour tout $x \in A$: un tel élément x s'appelle un *représentant* de A .

Exemple 1.1.3. Soit $f : X \rightarrow Y$ 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 préimages non vides des singletons.

Définition 1.1.4. Si \mathcal{R} est une relation d'équivalence sur un ensemble X , on dispose de la *surjection canonique*

$$\begin{aligned} \pi_{\mathcal{R}} : X &\rightarrow X/\mathcal{R} \\ x &\mapsto [x]. \end{aligned}$$

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

Proposition 1.1.5 (Propriété universelle). Soient \mathcal{R} une relation d'équivalence sur un ensemble X et $f : X \rightarrow Y$ une application. Supposons que $x_1\mathcal{R}x_2 \Rightarrow f(x_1) = f(x_2)$. Alors il existe une unique application $\tilde{f} : X/\mathcal{R} \rightarrow Y$ telle que $f = \tilde{f} \circ \pi_{\mathcal{R}}$.

Corollaire 1.1.6 (Décomposition canonique d'une application). Soit $f : X \rightarrow Y$ une application. Il existe une unique application $\tilde{f} : X/\mathcal{R}_f \rightarrow f(X)$ telle que $f = \iota \circ \tilde{f} \circ \pi_{\mathcal{R}_f}$ où $\iota : f(X) \hookrightarrow Y$ est l'inclusion. L'application \tilde{f} est bijective.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \pi_{\mathcal{R}_f} \downarrow & & \uparrow \iota \\ X/\mathcal{R}_f & \xrightarrow{\tilde{f}} & f(X) \end{array}$$

1.1.7 Groupes : définitions et propriétés de base

Définition 1.1.8. Un *groupe* est un couple $(G, *)$ où G est un ensemble, $*$: $G \times G \rightarrow G$ une loi de composition interne, vérifiant les conditions suivantes :

- associativité : on a $(x * y) * z = x * (y * z)$ pour tous $x, y, z \in G$;
- élément neutre : il existe un élément $e \in G$ tel que $e * x = x * e = x$ pour tout $x \in G$;
- inverse : pour tout $x \in G$, il existe un élément $x' \in G$ tel que $x * x' = x' * x = e$.

On dit que G est *abélien* (ou *commutatif*) lorsque $x * y = y * x$ pour tous $x, y \in G$.

Remarques. (0) L'élément neutre est unique. L'inverse d'un élément est unique.

- (1) Dans la pratique, on parle du groupe G , en omettant la loi $*$ dans la notation. Il s'agit d'un abus quasi systématique.
- (2) En général, on note la loi multiplicativement : si $x, y \in G$, on écrit souvent xy voire xy pour $x * y$. L'inverse de x est souvent noté x^{-1} .
- (3) Lorsque le groupe est abélien, la loi est souvent notée additivement, l'élément neutre 0 et l'inverse de x par $-x$.

Exemples 1.1.9. $(\mathbf{Z}, +)$, $(\mathbf{Z}/n\mathbf{Z}, +)$ pour $n \in \mathbf{N}$, le groupe symétrique (\mathfrak{S}_X, \circ) des permutations d'un ensemble X , le groupe $\text{GL}(V)$ où V est un espace vectoriel, d'innombrables exemples en géométrie.

Définition 1.1.10. Comme pour toute « structure algébrique », on a les notions suivantes :

(1) un *morphisme* entre deux groupes $(G, *)$ et (G', \bullet) est une application $f : G \rightarrow G'$ telle que

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

(on a alors $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$, et $f(e)$ est l'élément neutre de G');

(2) Un sous-groupe de G est une partie $H \subset G$ telle que l'inclusion soit un morphisme de groupes (on note alors $H \leq G$). On dit qu'un sous-groupe $H \leq G$ est *distingué*¹ lorsque $(\forall x \in G) xH = Hx$ (soit encore $xHx^{-1} = H$); c'est automatique lorsque G est abélien; on note alors $H \triangleleft G$;
 (3) Le *noyau* (resp. l'*image*) d'un morphisme de groupes $f: G \rightarrow G'$ est $\text{Ker}(f) = f^{-1}(e_{G'})$ (resp. $\text{Im}(f) = f(G)$). C'est un sous-groupe distingué de G (resp. un sous-groupe de G').

Proposition 1.1.11. Soient G un groupe et $H \subset G$. Alors H est un sous-groupe de G si et seulement si $H \neq \emptyset$ et $x, y \in H \Rightarrow xy^{-1} \in H$.

Exemple 1.1.12. Les sous-groupes de \mathbf{Z} sont les parties de la forme $n\mathbf{Z}$ avec $n \in \mathbf{N}$.

Corollaire 1.1.13. Si G est un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition 1.1.14. Soient 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 $\langle X \rangle$.

Exemples 1.1.15. On a $\langle 2, 3 \rangle = \mathbf{Z}$ dans $(\mathbf{Z}, +)$, $\langle (1, 2), (1, 2, 3) \rangle = \mathfrak{S}_3$.

Proposition 1.1.16. Soit $f: G \rightarrow G'$ un morphisme de groupes.

- (1) L'image directe d'un sous-groupe de G est un sous-groupe de G' . En particulier $\text{Im}(f)$ est un sous-groupe de G' .
- (2) L'image réciproque $f^{-1}(H')$ d'un sous-groupe $H' \leq G'$ dans G est un sous-groupe de G . Il est distingué dans G lorsque H' est distingué dans G' .
- (3) f est injective si et seulement si $\text{Ker}(f) = \{e_G\}$.
- (4) Si f est bijective, alors l'application $f^{-1}: G' \rightarrow G$ est un morphisme de groupes (et f est un isomorphisme de groupes).

Remarque. (1) Si $H \leq G$ est un sous-groupe distingué, l'image directe $f(H)$ n'est pas distinguée dans G' en général. 
 (2) On retrouve le fait que $\text{Ker}(f) = f^{-1}(e_{G'})$ est un sous-groupe distingué de G .

Définition 1.1.17. Les *automorphismes* d'un groupe G sont les isomorphismes de G dans lui-même. Ils forment un groupe pour la composition, qu'on note $\text{Aut}(G)$.

On peut raffiner la proposition 1.1.16 de la façon suivante.

Proposition 1.1.18. Soit $f: G \rightarrow G'$ un morphisme de groupes. L'application $H \mapsto f(H)$ induit une bijection de l'ensemble des sous-groupes de G qui contiennent $\text{Ker}(f)$ et l'ensemble des sous-groupes de $\text{Im}(f)$.

1.1.19 Classes modulo un sous-groupe


Définition 1.1.20. Soient G un groupe et $H \leq G$ 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 . Bien entendu, on définit de façon analogue les classes à droite². On note G/H (resp. $H \backslash G$) l'ensemble des classes à gauche (resp. à droite).

Remarque. Si G est un groupe, H un sous-groupe, on a $g_1H = g_2H \Leftrightarrow Hg_1^{-1} = Hg_2^{-1}$ pour tous $g_1, g_2 \in G$ (en passant aux inverses). Cela implique que l'application $gH \mapsto Hg^{-1}$ induit une bijection de l'ensemble G/H sur $H \backslash G$.

Définition 1.1.21 (Indice d'un sous-groupe). Soient G un groupe et $H \leq G$ un sous-groupe. L'*indice* de H dans G est le cardinal³ de l'ensemble quotient G/H . On le note $(G : H) \in \mathbf{N} \cup \{\infty\}$.

Définition 1.1.22. 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.

Théorème 1.1.23 (Lagrange). Si G est un groupe fini et H un sous-groupe, alors $\#G = (G : H)\#H$. On a donc $\#H \mid \#G$. En particulier, l'ordre d'un élément $g \in G$ divise $\#G$.

Remarque. 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 1.1.24. 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.

1. Ou *normal*.
 2. Lorsque H n'est pas distingué dans G , les relations d'équivalence (et donc les partitions) associées ne coïncident pas.
 3. C'est donc aussi celui de $H \backslash G$ en vertu de la remarque qui précède.

Ce qui précède montre en particulier que si H est un sous-groupe distingué de G , l'ensemble quotient G/H (qui est alors égal à $H \backslash G$) et naturellement muni d'une structure de groupe. La loi de groupe est la suivante : si $g_1, g_2 \in G$, on a $(g_1H)(g_2H) = g_1g_2H$ et $(gH)^{-1} = g^{-1}H$ (l'élément neutre est la classe « triviale » H).

Remarque. Dans la pratique, on note \bar{g} la classe gH , lorsque cela ne prête pas à confusion.

Exemple 1.1.25. Si $n \in \mathbf{Z}_{>0}$, on dispose du groupe quotient $\mathbf{Z}/n\mathbf{Z}$.

Corollaire 1.1.26 (propriété universelle). Soient $f: G \rightarrow G'$ un morphisme de groupes et $H \leq G$ un sous-groupe distingué tel que $H \subset \text{Ker}(f)$. Alors il existe un morphisme de groupes $\tilde{f}: G/H \rightarrow G'$ unique tel que $f = \tilde{f} \circ \pi$, où $\pi: G \rightarrow G/H$ est la surjection canonique.

Exemple 1.1.27. (1) Si $f: G \rightarrow G'$ est un morphisme de groupes, alors f induit un isomorphisme

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

Lorsque G est fini, cela implique en particulier que $(G : \text{Ker}(f)) = \#\text{Im}(f)$, et donc $\#G = \#\text{Ker}(f)\#\text{Im}(f)$, égalité qui n'est pas sans rappeler le théorème du rang.

(2) Rappelons que le *centre* d'un groupe G est le sous-groupe $Z(G) = \{g \in G; (\forall x \in G) gx = xg\}$. Si $g \in G$, posons

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

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

$$G/Z(G) \rightarrow \text{Aut}(G).$$

On note $\text{Int}(G)$ son image : ses éléments s'appellent les *automorphismes intérieurs* de G . On a alors $G/Z(G) \xrightarrow{\sim} \text{Int}(G)$. En général, l'inclusion $\text{Int}(G) \subset \text{Aut}(G)$ est stricte.

Théorème 1.1.28 (théorèmes d'isomorphisme). Soit G un groupe.

(1) Soient $H \leq G$ et $N \triangleleft G$. Alors $HN = \{hn\}_{\substack{h \in H \\ n \in N}}$ est un sous-groupe de G , $N \cap H \triangleleft H$ et on a un isomorphisme

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

(2) Soient H et K deux sous-groupes distingués de G . Si $K \leq H$, alors $H/K \triangleleft G/K$ et on a un isomorphisme

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

Proposition 1.1.29. Soit $n \in \mathbf{N}_{>0}$. Pour tout diviseur d de n , il existe un et un seul sous-groupe d'ordre d dans $\mathbf{Z}/n\mathbf{Z}$: c'est le sous-groupe engendré par $\frac{n}{d}$.

1.2 Le groupe symétrique

1.2.1 Généralités, décomposition en produit de cycles à supports disjoints

Définition 1.2.2. 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. Une bijection $f: E \rightarrow E'$ 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 1.2.3. On a $\#\mathfrak{S}_n = n!$.

Définition 1.2.4. (1) Si $\sigma \in \mathfrak{S}_n$, on note $\text{Fix}(\sigma) = \{i \in \{1, \dots, n\}; \sigma(i) = i\}$ l'ensemble des points fixes. L'ensemble $\text{supp}(\sigma) := \{1, \dots, n\} \setminus \text{Fix}(\sigma)$ s'appelle le *support* de σ .

(2) Soient $\ell \in \mathbf{N}_{>1}$ et i_1, \dots, i_ℓ des éléments distincts de $\{1, \dots, n\}$. On note (i_1, \dots, i_ℓ) l'élément de \mathfrak{S}_n qui envoie 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 $\text{supp}(i_1, \dots, i_\ell) = \{i_1, \dots, i_\ell\}$). Une permutation de ce type est appelée *cycle* de longueur ℓ ou ℓ -*cycle*. Un 2-cycle s'appelle une *transposition*.

Remarque. (0) 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.

(1) Un ℓ -cycle est d'ordre ℓ .

(2) Il y a $\frac{n(n-1)\dots(n-\ell+1)}{\ell} = \binom{n}{\ell}(\ell-1)!$ cycles de longueur ℓ .

Lemme 1.2.5. Soient $\sigma_1, \sigma_2 \in \mathfrak{S}_n$. On a $\text{supp}(\sigma_1\sigma_2) \subset \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$. Si en outre on a $\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset$, alors $\text{supp}(\sigma_1\sigma_2) = \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$, les permutations σ_1 et σ_2 commutent.

Théorème 1.2.6. 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 tels que $\sigma = c_1 \cdots c_r$. Une telle décomposition est unique à l'ordre des facteurs près.

Remarque. On a $r = 0 \Leftrightarrow \sigma = \text{Id}$.

Remarque. Les supports des cycles c_1, \dots, c_r ne sont autres que les orbites non ponctuelles de l'action du groupe $\langle \sigma \rangle$ sur $\{1, \dots, n\}$ (cf plus bas).

Corollaire 1.2.7. Le groupe \mathfrak{S}_n admet les parties génératrices suivantes :

- les transpositions ;
- $\{(1, i)\}_{2 \leq i \leq n}$;
- $\{(i, i+1)\}_{1 \leq i \leq n-1}$;
- $\{(1, 2), (1, 2, \dots, n)\}$.

Définition 1.2.8. (1) Le type de $\sigma \in \mathfrak{S}_n$ est la suite $\underline{\ell} = (\ell_1, \dots, \ell_r)$ (ordonnée 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. on a $\ell_1 + \dots + \ell_r = n$).

(2) L'ensemble des partitions de n est en bijection avec les diagrammes de Young : un diagramme de Young est une collection finie de cases, ou cellules, organisée en lignes justifiées à gauche, et telle que les longueurs des lignes décroissent au sens large. Par exemple, le diagramme de Young associé à la partition $(4, 3, 1)$ de l'entier 8 est

.

(3) 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. Par exemple, le produit $(2, 5, 8, 1)(7, 4, 6)$ correspond au tableau

2	5	8	1
7	4	6	
3			

. Le tableau de Young standard (de type $\underline{\ell}$) est celui dont les cases sont remplies dans l'ordre, par exemple

1	2	3	4
5	6	7	
8			

.

Lemme 1.2.9. Soient $c = (i_1, \dots, i_\ell)$ un cycle de longueur ℓ et $\gamma \in \mathfrak{S}_n$. On a

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

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

Théorème 1.2.10. Deux éléments de \mathfrak{S}_n sont conjugués dans \mathfrak{S}_n si et seulement s'ils ont même type.

Remarque. 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 1.2.11. Si $n \geq 3$, le centre de \mathfrak{S}_n est trivial.

Exercice 1.2.12. Montrer que \mathfrak{S}_9 contient un élément d'ordre 20, mais pas d'élément d'ordre 18.

1.2.13 Signature et groupe alterné

Définition 1.2.14. Si $\sigma \in \mathfrak{S}_n$, on pose $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

Remarque. 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 1.2.15. 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 $\tau \in \mathfrak{S}_n$.

Théorème 1.2.16. L'application ε définit un morphisme de groupes $\varepsilon: \mathfrak{S}_n \rightarrow \{\pm 1\}$. Il est surjectif lorsque $n \geq 2$.

Définition 1.2.17. Le groupe alterné est $\mathfrak{A}_n = \text{Ker}(\varepsilon)$. C'est un sous-groupe distingué de \mathfrak{S}_n , d'indice 2 lorsque $n \geq 2$.

Proposition 1.2.18. Le groupe \mathfrak{A}_n admet les parties génératrices suivantes :

- $\{(1, i)(1, j)\}_{2 \leq i < j \leq n}$;
- $\{(1, 2, i)\}_{3 \leq i \leq n}$;
- $\{\sigma^2\}_{\sigma \in \mathfrak{S}_n}$.



Remarque. 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 *a 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 rouge) :

- (1, 1, 1, 1, 1) (classe de **ld**), 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 $\frac{5 \times 4 \times 3 \times 2}{4} = 30$ éléments ;
- (5) (classe d'un 5-cycle), elle a $\frac{5!}{5} = 4! = 24$ éléments.

Les trois premières classes de conjugaison en rouge sont aussi des classes de conjugaison dans \mathfrak{A}_5 . En revanche, 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 1.2.19. Un groupe G est dit *simple* lorsque ses seuls sous-groupes distingués sont $\{e\}$ et G .

Théorème 1.2.20. Si $n \geq 5$, le groupe \mathfrak{A}_n est simple.

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

Corollaire 1.2.21. Si $n \geq 5$, les sous-groupes distingués de \mathfrak{S}_n sont $\{\text{ld}\}$, \mathfrak{A}_n et \mathfrak{S}_n .

Remarque. Lien avec la résolubilité par radicaux des polynômes.

Exercice 1.2.22. Déterminer tous les morphismes de groupes $\mathfrak{S}_n \rightarrow \mathbf{C}^\times$.

Exercice 1.2.23. Existe-t-il un morphisme surjectif $\mathfrak{S}_n \rightarrow \mathfrak{S}_{n-1}$?

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

Définition 1.3.3. On dit que G est *produit semi-direct interne* de H par N lorsque

- $N \triangleleft G$;
- $N \cap H = \{e\}$;
- $NH = G$.

On note alors $G = N \rtimes H$.

Proposition 1.3.4. Supposons que G soit produit semi-direct interne de H par N . Pour tout $y \in H$, on dispose de l'automorphisme $\varphi_y \in \text{Aut}(N)$ défini par $\varphi_y(x) = xyx^{-1}$.

(1) Pour tout $g \in G$, il existe $x \in N$ et $y \in H$ uniques tels que $g = xy$.

(2) 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

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

(3) L'application $\varphi: H \rightarrow \text{Aut}(N)$ est un morphisme de groupes.

Remarque. Supposons G fini, que $N \triangleleft G$ et $N \cap H = \{e\}$. Alors $\#N\#H = \#G$ si et seulement si $NH = G$. En effet, l'application $N \times H \rightarrow G$ donnée par $(x, y) \mapsto xy$ est injective (même argument que l'item (1) de la proposition précédente), et son image est NH .

Exemples 1.3.5. (1) Soient $N = \mathfrak{A}_3 = \langle (1, 2, 3) \rangle \triangleleft G = \mathfrak{S}_3$ et $H = \langle (1, 2) \rangle$. Comme $\#N = 3$ et $\#H = 2$, le théorème de Lagrange implique que $N \cap H = \{\text{ld}\}$. 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 $U_n = \{z \in \mathbf{C}; z^n = 1\} \leq \mathbf{C}^\times$ 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 $O_2(\mathbf{R})$ constitué des isométries qui préservent U_n . On dispose du morphisme $\det: O_2(\mathbf{R}) \rightarrow \{\pm 1\}$ et $\text{Ker}(\det) = SO_2(\mathbf{R})$. Pour $\theta \in \mathbf{R}$, on dispose de la matrice de rotation $R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \in SO_2(\mathbf{R})$. L'application

$$\begin{aligned} \mathbf{R} &\rightarrow SO_2(\mathbf{R}) \\ \theta &\mapsto R_\theta \end{aligned}$$

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

$$\mathbf{R}/2\pi\mathbf{Z} \xrightarrow{\sim} SO_2(\mathbf{R}).$$

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 $\varepsilon: U \xrightarrow{\sim} SO_2(\mathbf{R})$ tel que pour tout $\theta \in \mathbf{R}$, on ait $\varepsilon(e^{i\theta}) = R_\theta$. Le groupe $D_{2n} \cap \text{Ker}(\det) = D_{2n} \cap SO_2(\mathbf{R})$ est constitué des rotations qui préservent U_n : l'isomorphisme ε induit un isomorphisme $U_n \xrightarrow{\sim} D_{2n} \cap SO_2(\mathbf{R})$. 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 $\sigma \notin D_{2n} \cap SO_2(\mathbf{R})$, donc $(D_{2n} \cap SO_2(\mathbf{R})) \cap \langle \sigma \rangle = \{\text{Id}_{\mathbf{R}^2}\}$.

Soit $g \in D_{2n}$. Si $g \notin SO_2(\mathbf{R})$, on a $\det(g) = -1$, et donc $\det(g\sigma) = 1$. On a alors $g = (g\sigma)\sigma \in (D_{2n} \cap SO_2(\mathbf{R}))\langle \sigma \rangle$.

Cela montre que D_{2n} est produit semi-direct de $\langle \sigma \rangle \simeq \mathbf{Z}/2\mathbf{Z}$ par $D_{2n} \cap SO_2(\mathbf{R}) \simeq U_n \simeq \mathbf{Z}/n\mathbf{Z}$. 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). Ils sont assujettis aux relations $\rho^n = \text{Id}$, $\sigma^2 = \text{Id}$ et $(\rho\sigma)^2 = \text{Id}$.

(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 $V \triangleleft \mathfrak{A}_4$. Soient c un 3-cycle (par exemple $c = (1, 2, 3)$) et $H = \langle c \rangle \simeq \mathbf{Z}/3\mathbf{Z}$. Alors \mathfrak{A}_4 est produit semi-direct interne de H par V .

(4) Soit (\mathcal{E}, E) un espace affine. On dispose du groupe affine $GA(\mathcal{E})$ des transformations affines, du groupe des translations $T(\mathcal{E}) \simeq E$. Le choix d'un point $\Omega \in \mathcal{E}$ permet de vectorialiser \mathcal{E} (i.e. fournit la bijection $\mathcal{E} \xrightarrow{\sim} E; M \mapsto \overrightarrow{\Omega M}$). Si H_Ω désigne le sous-groupe de $GA(\mathcal{E})$ constitué des éléments qui fixent Ω , l'application « application linéaire associée » fournit un isomorphisme $H_\Omega \xrightarrow{\sim} GL(E)$. On vérifie sans peine que $GA(\mathcal{E})$ est produit semi-direct interne de H_Ω par $T(\mathcal{E})$.

1.3.6 Produits semi-directs externes

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

$$\begin{aligned} \varphi: H &\rightarrow \text{Aut}(N) \\ y &\mapsto \varphi_y \end{aligned}$$

un morphisme de groupes.

Définition 1.3.7. 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 1.3.8. Ce qui précède définit bien un groupe, d'élément neutre (e_N, e_H) .

Remarque. 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 1.3.9. Le produit semi-direct $N \rtimes_\varphi H$ est direct (i.e. égal au produit cartésien $N \times H$ des groupes N et H) si et seulement si $\varphi: H \rightarrow \text{Aut}(N)$ est trivial.

Exemples 1.3.10. (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 $\varphi(\bar{1})$ est la multiplication par -1 dans $\mathbf{Z}/n\mathbf{Z}$ (exercice).

(3) soient $n \in \mathbf{N}_{\geq 2}$ 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 (exercice).

Remarque. On voit sur le dernier exemple que deux morphismes $H \rightarrow \text{Aut}(N)$ 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 1.4.2. Une *action* (à gauche) de G sur X est la donnée d'une application

$$*: G \times X \rightarrow X$$

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. On définit de même la notion d'action à droite, en considérant les applications $*: X \times G \rightarrow X$ 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 l'action, ce sera toujours à gauche.

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

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

Les conditions (i) et (ii) se réécrivent

- (1) $(\forall g_1, g_2 \in G) \rho(g_1) \circ \rho(g_2) = \rho(g_1 g_2)$;
- (2) $\rho(e) = \text{Id}_X$.

Proposition 1.4.3. Pour tout $g \in G$, on a $\rho(g) \in \mathfrak{S}_X$. L'application $\rho: G \rightarrow \mathfrak{S}_X$ est un morphisme de groupes.

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 $f: G \rightarrow \mathfrak{S}_X$, 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.

Proposition 1.4.4. La donnée d'une action de G sur X équivaut à celle d'un morphisme de groupes $G \rightarrow \mathfrak{S}_X$.

Exemples 1.4.5. (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 $H \leq G$ 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 $g * (\gamma H) = g\gamma H = \{g\gamma x\}_{x \in \gamma H}$ (notons que c'est bien défini, i.e. que $g\gamma H$ 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 la 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 $X = \{1, \dots, n\}$.

(4) Tout groupe agit sur lui-même par conjugaison (en posant $g * x = gxg^{-1}$ pour tout $g, x \in G$).

(5) Exemples en algèbre linéaire et en géométrie.

Définition 1.4.6. Soit G un groupe agissant sur un ensemble X .

- (1) L'*orbite* de $x \in X$ est l'ensemble $G * x = \{g * x\}_{g \in G}$, c'est une partie de X , on la note $\text{orb}(x)$.
- (2) Le *stabilisateur* de $x \in X$ est

$$\text{stab}_G(x) = \{g \in G; g * x = x\}.$$

C'est un sous-groupe de G .

(3) On dit que l'action est *fidèle* lorsque le morphisme associé $\rho: G \rightarrow \mathfrak{S}_X$ est injectif.

(4) On dit que l'action est *libre* lorsque pour tout $x \in X$, on a $g * x = x \Rightarrow g = e$.

(5) On dit que l'action est *transitive* s'il n'y a qu'une seule orbite. Plus généralement, si $k \in \mathbb{N}_{>0}$, on dit que l'action est *k-transitive* si pour tout k -uples (x_1, \dots, x_k) et (y_1, \dots, y_k) d'éléments distincts de X , il existe $g \in G$ tel que $g * x_i = y_i$ pour tout $i \in \{1, \dots, k\}$.

Remarque. (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.

Exemples 1.4.7. (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 $\{1, \dots, n\}$ 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 $C_G(x)$ 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 $H \leq G$ s'appelle le *normalisateur* de H et se note $N_G(H)$. On a bien sûr $H \triangleleft G \Leftrightarrow N_G(H) = G$.

Théorème 1.4.8 (Cayley). *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 $n = \#G$.*

Lemme 1.4.9. *Soient G un groupe agissant sur un ensemble X , $g \in G$ et $x \in X$. On a*

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

Théorème 1.4.10 (Relation orbite-stabilisateur). *Soient G un groupe agissant sur un ensemble X , et $x \in X$. L'application*

$$\begin{aligned} G / \text{stab}_G(x) &\rightarrow \text{orb}_X(x) \\ \bar{g} &\mapsto g \cdot x \end{aligned}$$

est bijective.

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

Corollaire 1.4.11. *Si G est fini et $x \in X$, on a $\#G = \#\text{orb}_X(x) \# \text{stab}_G(x)$, en particulier l'entier*

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

divise $\#G$.

Proposition 1.4.12 (Équation aux classes). *Supposons X fini. Si $\{x_1, \dots, x_r\}$ est un système complet de représentants des orbites de X , on a*

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

Corollaire 1.4.13. *Si G est un p -groupe et X est fini, on a $\#X \equiv \#X^G \pmod{p\mathbf{Z}}$ (où X^G désigne l'ensemble des points fixes).*

Corollaire 1.4.14. *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).*

Proposition 1.4.15. (Formule de Burnside) *Supposons G et X finis. Pour $x \in X$, posons $\text{Fix}(g) = \{x \in X ; g \cdot x = x\}$ (les points fixes de g dans X). Le nombre d'orbites dans X est $\frac{1}{\#G} \sum_{g \in G} \#\text{Fix}(g)$ (c'est le nombre moyen de points fixes).*

Quelques exemples d'utilisation des actions de groupes.

Proposition 1.4.16. *Soient G un groupe et $H \leq G$ un sous-groupe d'indice n . Il existe un sous-groupe distingué N de G tel que $N \subset H$ et $(G : N) \mid n!$.*

Proposition 1.4.17. *Soient G un groupe fini, $H \leq G$ un sous-groupe et p le plus petit diviseur premier de $\#G$. Si $(G : H) = p$, alors H est distingué dans G .*

Exercice 1.4.18. Soit G un groupe d'ordre 33 agissant sur un ensemble de cardinal 19. Montrer qu'il y a au moins un point fixe.

Proposition 1.4.19. *Soit p un nombre premier. Tout groupe de cardinal p^2 est abélien.*

Remarque. Soit $G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} ; x, y, z \in \mathbf{Z}/p\mathbf{Z} \right\} \leq \text{GL}_3(\mathbf{Z}/p\mathbf{Z})$ le sous-groupe des matrices triangulaires supérieures unipotentes. Il est non abélien de cardinal p^3 .

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

Théorème 1.4.20. (Théorème de Cauchy) *Soient G un groupe fini et p un nombre premier divisant $\#G$. Alors G contient un élément d'ordre p .*

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

1.4.21 Les théorèmes de Sylow

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

Définition 1.4.22. (1) Un p -groupe est un groupe fini d'ordre une puissance de p .

(2) 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 $p^{v_p(\#G)}$. On note $\text{Syl}_p(G)$ l'ensemble des p -Sylow de G et on pose $n_p(G) = \#\text{Syl}_p(G)$.

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

Théorème 1.4.23. (Sylow) On a

(i) $n_p \equiv 1 \pmod p$, en particulier $\text{Syl}_p(G)$ n'est pas vide ;

(ii) le groupe G agit transitivement par conjugaison sur $\text{Syl}_p(G)$ (les p -Sylow de G sont conjugués), en particulier $n_p(G) \mid \#G$.

Lemme 1.4.24. Si $r \in \mathbb{N}$ et $m \in \mathbb{N}_{>0}$, on a $\binom{p^r m}{p^r} \equiv m \pmod p$.

Lemme 1.4.25. Soit H un p -sous-groupe de G et S_0 un p -Sylow de G . Alors H est inclus dans un conjugué de S_0 (donc en particulier dans un p -Sylow de G).

Corollaire 1.4.26. Le groupe G admet un unique p -Sylow si et seulement si ce dernier est distingué dans G .

Exercice 1.4.27. Soient G un groupe fini, $H \leq G$ 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 $Q = S \cap H$.

Exercice 1.4.28. Si G est un groupe fini et $H \triangleleft G$ un sous-groupe distingué, on a $H N_G(S) = G$ pour tout $S \in \text{Syl}_p(H)$.

Quelques exemples d'utilisation des théorèmes de Sylow.

Proposition 1.4.29. Tout groupe d'ordre 77 est cyclique.

Proposition 1.4.30. Il n'existe pas de groupe simple d'ordre 945.

Exercice 1.4.31. Déterminer le nombre de p -Sylow du groupe symétrique \mathfrak{S}_p .

Exercice 1.4.32. 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 $G \rightarrow \mathfrak{S}_4$).

Exercice 1.4.33. Un groupe d'ordre 300 n'est jamais simple.

2 Anneaux et polynômes

2.1 Rappels sur les anneaux

2.1.1 Définitions

Définition 2.1.2. Un anneau est la donnée d'un triplet $(A, +, \cdot)$ où A est un ensemble et $+: A \times A \rightarrow A$ et $\cdot: A \times A \rightarrow A$ sont deux lois de composition interne tels que les propriétés suivantes sont remplies :

- le couple $(A, +)$ est un groupe abélien ;
- 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*.

Remarques. (1) Par abus, on parlera souvent 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.

Exemples 2.1.3. (1) Les anneaux \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} .

(2) $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}$.

(3) Si K est un corps et V un K -espace vectoriel, $\text{End}_K(V)$, 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 $M_n(A)$.

(5) Plein d'exemples en analyse.

Dans ce qui suit, tous les anneaux seront supposés *unitaires*.

Remarque (Binôme de Newton). Si $a, b \in A$ commutent et $n \in \mathbf{N}$, on a

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

Mise en garde : il est important de supposer que $ab = ba$.



Définition 2.1.4 (Anneaux produits). (1) 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

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad \text{et} \quad (a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$$

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.

(2) Cas particulier de (1) : soit I un ensemble. On note A^I (resp. $A^{(I)}$) l'ensemble des applications $I \rightarrow A$ (resp. des applications $I \rightarrow A$ 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. Lorsque I est infini, $A^{(I)}$ est un anneau non unitaire.

Définition 2.1.5. Soient A un anneau et $a \in A$.

(1) 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. $A^\times = A \setminus \{0\}$.

(2) On dit que a est *diviseur de zéro* s'il existe $b \in A \setminus \{0\}$ 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.

(3) 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 2.1.6. (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, parce que $2\bar{3} = \bar{0}$ alors que $2 \neq \bar{0}$ et $\bar{3} \neq \bar{0}$. En fait, on a $(\mathbf{Z}/6\mathbf{Z})^\times = \{\bar{1}, \bar{5}\}$. Par contre, $\mathbf{Z}/6\mathbf{Z}$ est réduit.

(3) L'anneau $\mathbf{Z}/4\mathbf{Z}$ n'est pas réduit, car $\bar{2}^2 = \bar{0}$ mais $\bar{2} \neq \bar{0}$.

Remarque. On peut aussi définir les notions d'inversible à gauche et d'inversible à droite. Ces notions sont distinctes en général dans le cas d'un anneau non commutatif (par exemple, dans l'anneau des endomorphismes d'un espace vectoriel de dimension infinie). Par contre, il est immédiat de voir que si un élément est inversible à la fois à gauche et à droite, alors il est inversible (exercice). On peut aussi montrer (exercice) que si un élément admet un *unique* inverse à gauche, alors il est inversible.

Exercice 2.1.7. Un anneau fini et intègre est un corps.

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

Définition 2.1.8. Soient A et B deux anneaux. Un *morphisme d'anneaux* de A vers B est un morphisme $f: A \rightarrow B$ entre les groupes additifs sous-jacents tel que

$$\begin{aligned} (\forall a, b \in A) f(ab) &= f(a)f(b) \\ f(1_A) &= 1_B. \end{aligned}$$

Remarques. (1) Si $f: A \rightarrow B$ et $g: B \rightarrow C$ sont deux morphismes d'anneaux, l'application composée $g \circ f$ est encore un morphisme d'anneaux.

(2) L'application $i: A \rightarrow A \times A; a \mapsto (a, 0)$ n'est pas un morphisme d'anneau, parce que $i(1_A) \neq 1_{A \times A}$.

Exemples 2.1.9. (1) Les inclusions $\mathbf{Z} \rightarrow \mathbf{Q}$, $\mathbf{Q} \rightarrow \mathbf{R}$, $\mathbf{R} \rightarrow \mathbf{C}$. Pour $n \in \mathbf{N}_{>1}$, la réduction modulo $n: \mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z}$.

(2) Il existe un unique morphisme d'anneaux $c_A: \mathbf{Z} \rightarrow A$. C'est l'application qui à $z \in \mathbf{N}$ associe $c_A(z) = \underbrace{1_A + \dots + 1_A}_{z \text{ fois}}$

et telle que $c_A(z) = -c_A(-z)$ si $z \in \mathbf{Z}_{<0}$.

Définition 2.1.10. Soit $f: A \rightarrow B$ un morphisme d'anneaux. Le noyau $\{a \in A, f(a) = 0_B\}$ (resp. l'image $\{f(a)\}_{a \in A}$) du morphisme de groupes sous-jacent s'appelle le *noyau* (resp. l'*image*) de f et est noté $\text{Ker}(f)$ (resp. $\text{Im}(f)$). Rappelons que f est injectif si et seulement si $\text{Ker}(f) = \{0_A\}$.



$\text{Ker}(f)$ n'est pas un sous-anneau de A .

Définition 2.1.11. 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 2.1.12. $\mathcal{C}^0([0, 1], \mathbf{R})$ est un sous-anneau de $\mathcal{B}([0, 1], \mathbf{R})$.

Remarque. Pour montrer qu'un ensemble muni de deux lois de composition interne est un anneau, il est souvent judicieux de 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} .

2.1.13 Idéaux et quotients

2.1.14 Définitions

Soit A un anneau.

Définition 2.1.15. Un *idéal à gauche* de A est un sous-groupe $I \subset A$ pour la loi $+$ tel que

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

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

Exercice 2.1.17. Soient K un corps et V un K -espace vectoriel de dimension finie. Déterminer les idéaux à gauche, à droite, et bilatères de $\text{End}_K(V)$.

Proposition 2.1.18. Si $f: A \rightarrow B$ est un morphisme d'anneaux, alors $\text{Ker}(f)$ est un idéal bilatère de A .

Remarque. Si $f: A \rightarrow B$ 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 $I \subset A$ est un idéal à gauche, $f(I)$ n'est pas un idéal à gauche de B en général (c'en est un lorsque f est surjectif).

Dans la suite de ce numéro, on suppose A commutatif.

Définition 2.1.19. • Soit X une partie de A . L'idéal *engendré* par X est l'ensemble des combinaisons A -linéaires d'éléments de X :

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

Si $X = \{x_1, \dots, x_r\}$ est fini, on note cet idéal $x_1 A + x_2 A + \dots + x_r A$ ou $\langle x_1, \dots, x_r \rangle$.

• 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*.

• Un anneau est dit *noetherien* si tout idéal est de type fini (i.e. admet une famille génératrice finie). C'est une propriété de finitude très importante.

Exemples 2.1.20. 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 (exercice).

Définition 2.1.21. Opérations sur les idéaux. Soient A un anneau et $\{I_\lambda\}_{\lambda \in \Lambda}$ une famille d'idéaux de A . Alors l'intersection $\bigcap_{\lambda \in \Lambda} I_\lambda$ 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* $x_1 + \dots + x_r$ 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 $I_1 I_2 \dots I_n$ l'idéal *engendré* par l'ensemble des produits $x_1 x_2 \dots x_n$ avec $x_j \in I_j$ pour tout $j \in \{1, \dots, n\}$.

Exemple 2.1.22. 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 2.1.23. Rappelons que si A est un anneau unitaire, il existe un unique morphisme unitaire $c_A: \mathbf{Z} \rightarrow A$. Le noyau de ce morphisme étant un idéal de \mathbf{Z} , il est de la forme $\text{car}(A)\mathbf{Z}$ avec $\text{car}(A) \in \mathbf{N}$. L'entier $\text{car}(A)$ s'appelle la *caractéristique* de l'anneau A .

Exemples 2.1.24. 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 de polynômes $A[X]$.

2.1.25 Quotients

Soit A un anneau.

Proposition 2.1.26. *Les relations d'équivalence sur A qui sont compatibles avec les lois d'anneau sont les relations modulo un idéal bilatère.*

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 que 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 $\pi : A \rightarrow A/I$ 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 2.1.27. *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 $f : A \rightarrow B$ est un morphisme d'anneaux tel que $I \subset \text{Ker}(f)$, alors il existe un unique morphisme d'anneaux $\bar{f} : A/I \rightarrow B$ tel que $f = \bar{f} \circ \pi$ i.e. tel qu'on a la factorisation*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow \pi & \nearrow \bar{f} \\ & A/I & \end{array}$$

Remarques. (1) Si A est commutatif, il en est de même de A/I .

(2) On a $I = \text{Ker}(\pi : A \rightarrow A/I)$: tout idéal bilatère peut être vu comme le noyau d'un morphisme d'anneaux.

(3) Si $f : A \rightarrow B$ est un morphisme d'anneaux, on dispose de la factorisation canonique $f = \bar{f} \circ \pi$ où $\bar{f} : A/\text{Ker}(f) \rightarrow B$ est un morphisme *injectif* d'anneaux (cela s'appelle « passer au quotient »). 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 $\pi : A \rightarrow A/I$ 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 $\bar{J} \subset A/I$ est un idéal, alors $\pi^{-1}(\bar{J})$ est un idéal de A qui contient I .

Proposition 2.1.28. *Les applications*

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

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

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

2.1.29 Le théorème des restes chinois

Soit A un anneau.

Théorème 2.1.30 (des restes chinois). *Soient $I_1, \dots, I_n \subset A$ des idéaux tels que pour $i \neq k$, on ait $I_j + I_k = A$. Alors $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$. En outre, si $\pi_j : A \rightarrow A/I_j$ désigne la projection canonique, on a un isomorphisme naturel*

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

Exemple 2.1.31. Soient $a_1, \dots, a_n \in \mathbf{Z}$ des entiers non nuls deux-à-deux premiers entre eux (cela signifie exactement $a_j \mathbf{Z} + a_k \mathbf{Z} = \mathbf{Z}$ pour $j \neq k$). Alors 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 le théorème des restes chinois sert dans bien d'autres contextes.

Exercice 2.1.32. Soient $a, b \in \mathbf{N}_{>0}$ et d et m leur pgcd et leur ppcm respectivement. Montrer que

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

2.2 Idéaux premiers, idéaux maximaux

Définition 2.2.1. Soient A un anneau et $I \subsetneq A$ un idéal strict.

- (1) 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).
- (2) 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 2.2.2. *Tout idéal maximal est premier.*

Exemple 2.2.3. Les idéaux premiers de \mathbf{Z} sont $\{0\}$ et les $p\mathbf{Z}$ avec p premiers.

Proposition 2.2.4. *Soient A un anneau et $I \subset A$ un idéal. Alors*

- (1) A/I est un corps si et seulement si I est maximal ;
- (2) A/I est intègre si et seulement si I est premier.

Remarques. (1) Une autre façon d'exprimer le (1) 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 $f: K \rightarrow A$ 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 (cf proposition 2.2.2).

Proposition 2.2.5. *Soient A un anneau et $I \subset A$ un idéal. La bijection de la proposition 2.1.28 induit des bijections*

$$\begin{aligned} \{\text{idéaux premiers de } A \text{ contenant } I\} &\leftrightarrow \{\text{idéaux premiers de } A/I\} \\ \{\text{idéaux maximaux de } A \text{ contenant } I\} &\leftrightarrow \{\text{idéaux maximaux de } A/I\}. \end{aligned}$$

Exercice 2.2.6. Soient A_1, \dots, A_n des anneaux. Montrer que les idéaux premiers de l'anneau produit $A_1 \times \dots \times A_n$ sont de la forme $A_1 \times \dots \times A_{k-1} \times \mathfrak{p}_k \times A_{k+1} \times \dots \times A_n$ où $k \in \{1, \dots, n\}$ et $\mathfrak{p}_k \subset A_k$ est un idéal premier.

Proposition 2.2.7. *Soient A un anneau principal et I un idéal premier non nul. Alors I est maximal.*

Exemple 2.2.8. 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, non maximal. La proposition précédente implique donc que A n'est pas principal.

Exercices 2.2.9. (1) Soient $f: A \rightarrow B$ 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 $a \in A \setminus I$, 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 $\mathcal{F}(X, K)$?

2.2.10 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'ensembles 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 ZFnoC (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 2.2.11. Un ensemble partiellement ordonné (E, \leq) est *inductif* si toute chaîne (i.e. partie totalement ordonnée) de E admet un majorant.

Théorème 2.2.12 (de 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 est 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 2.2.13 (Krull). *Soient A un anneau et $I \subsetneq A$ un idéal strict. Alors il existe un idéal maximal $\mathfrak{m} \subset A$ tel que $I \subset \mathfrak{m}$. En particulier tout anneau admet au moins un idéal maximal.*

2.2.14 Applications : construction de \mathbf{R} et de \mathbf{C}

Le corps \mathbf{Q} est muni d'une relation d'ordre total \leq (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 $x \leq y$ si et seulement si $ad \leq cb$ dans \mathbf{Z}). Cette relation est compatible avec l'ordre : si $x \leq y$ et $z \in \mathbf{Q}$, on a $x + z \leq y + z$ et si en outre $z \geq 0$, on a $xz \leq yz$. 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 2.2.15. 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 $n, m \geq N \Rightarrow d(x_n, x_m) < \varepsilon$. Toute suite convergente est de Cauchy, mais la réciproque est fautive 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 $\lim_{n \rightarrow \infty} x_n^2 = 2$: 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 $\iota: \mathbf{Q} \rightarrow A$ 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 $\pi: A \rightarrow \mathbf{R}$ la surjection canonique.

Théorème 2.2.16. (1) L'idéal $\mathfrak{m} \subset A$ est maximal, donc \mathbf{R} est un corps. Le composé $\pi \circ \iota: \mathbf{Q} \rightarrow \mathbf{R}$ est injectif : il permet de voir \mathbf{Q} comme un sous-corps de \mathbf{R} .

(2) 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 $x \leq y$ si $x = y$ ou s'il existe $\varepsilon \in \mathbf{Q}_{>0}$ tel que $x_n + \varepsilon \leq y_n$ pour $n \gg 0$. 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}).

(3) L'espace métrique $(\mathbf{R}, |\cdot|)$ est complet.

(4) (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}^4 , alors il existe un unique morphisme de corps valués $\mathbf{R} \rightarrow K$.

4. Il en existe beaucoup d'autres !

Remarque. 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 *nombre 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 trinôme du second degré à coefficients dans \mathbf{C} admet une racine. En fait on a bien mieux : tout polynôme à coefficients dans \mathbf{C} est scindé. C'est le théorème de d'Alembert-Gauss (cf théorème 3.3.2). Le corps ainsi construit a donc de bonnes propriétés algébriques et topologiques.

2.3 Anneaux principaux

Dans toute cette section, A désigne un anneau intègre.

2.3.1 Divisibilité

Définition 2.3.2. Soient $a, b \in A \setminus \{0\}$. 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. 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 2.3.3. Soient $a, b \in A \setminus \{0\}$. 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 $a \in A \setminus \{0\}$) : notons la \sim . La relation de divisibilité munit $(A \setminus \{0\})/\sim$ d'une relation d'ordre.

Définition 2.3.4. Soit $\pi \in A \setminus \{0\}$.

(1) 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).

(2) On dit que π est *premier* si l'idéal principal $\langle \pi \rangle$ est premier.

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

Proposition 2.3.5. *Un élément premier est irréductible.*

Remarque. La réciproque est fautive en général.

Exemple 2.3.6. 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 $f: \mathbf{Z}[T] \rightarrow \mathbf{C}$ qui envoie T sur $\sqrt{-5}$. On a $\text{Im}(f) = A$ et $T^2 + 5 \in \text{Ker}(f)$. Soient $P(T) \in \text{Ker}(f)$ 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 $\text{Ker}(f) = \langle T^2 + 5 \rangle$, 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. Introduisons l'application

$$N: A \rightarrow \mathbf{N} \\ z = x + y\sqrt{-5} \mapsto |z|^2 = x^2 + 5y^2$$

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 $a^{-1} = \bar{a} = x - y\sqrt{-5} \in A$).

Exercices 2.3.7. (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 $a \nmid b$. Montrer que $aX + b$ est irréductible dans $A[X]$.

2.3.8 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 2.3.9. Soit $a \in A \setminus \{0\}$. Une factorisation en produit d'éléments irréductibles de a est une écriture de a sous la forme

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

avec $\pi_1, \dots, \pi_r \in A$ irréductibles. On dit qu'une telle décomposition est *unique* si pour toute autre factorisation $a = p_1 \cdots p_s$ avec $p_1, \dots, p_s \in A$ 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 $i \in \{1, \dots, r\}$. On dit que A est *factoriel* si tout élément non nul admet une unique factorisation en produit d'éléments irréductibles.

Remarque. 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 $\mathbb{P} = \{\pi_\lambda\}_{\lambda \in \Lambda}$ des classes des éléments irréductibles modulo la relation « être associé ». Tout élément $a \in A \setminus \{0\}$ 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 2.3.10. 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 2.3.11 (Propriétés des valuations). Soient $a, b \in A$. On a

- (1) $v_\pi(ab) = v_\pi(a) + v_\pi(b)$ et $v_\pi(a+b) \geq \min\{v_\pi(a), v_\pi(b)\}$ (avec égalité si $v_\pi(a) \neq v_\pi(b)$) pour tout $\pi \in A$ irréductible;
- (2) $a \mid b$ si et seulement si pour tout $\pi \in A$ irréductible, on a $v_\pi(a) \leq v_\pi(b)$;
- (3) $a \in A^\times$ si et seulement si pour tout $\pi \in A$ irréductible, on a $v_\pi(a) = 0$.

Exemples 2.3.12. (1) Un corps est factoriel (tout élément non nul est inversible).

(2) On sait (mais on va le redémontrer plus loin, cf corollaire 2.3.33) 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, non démontré dans ce cours).

(3) Le sous-anneau $\mathbf{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \in \mathbf{C}, x, y \in \mathbf{Z}\}$ de \mathbf{C} n'est pas factoriel, car $2, 3, 1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ sont irréductibles, les unités sont ± 1 , mais $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$: 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 2.3.13. Supposons A factoriel et soit $\pi \in A$. Alors π est irréductible si et seulement si π est premier, i.e. si et seulement si on a

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

Exemples 2.3.14. 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 (cf exemples 2.3.12).

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

Proposition 2.3.15. L'anneau A est factoriel si et seulement si tout élément non nul de A admet une factorisation en produit d'éléments irréductibles⁵ et si tout élément irréductible est premier.

2.3.16 Anneaux principaux, pgcd, ppcm

Définition 2.3.17. Un anneau *principal* est un anneau intègre dont tous idéaux sont principaux, i.e. engendrés par un élément.

Dans ce numéro, on suppose que A est principal.

Lemme 2.3.18. 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.

Remarque. (1) On retrouve la proposition 2.2.7.

(2) L'élément 2 est irréductible mais non premier dans l'anneau $\mathbf{Z}[\sqrt{-5}]$ (cf exemple 2.3.6) : le lemme qui précède montre donc que $\mathbf{Z}[\sqrt{-5}]$ n'est pas principal.

Lemme 2.3.19. Toute suite croissante d'idéaux de A est stationnaire.

Proposition 2.3.20. Soit $a \in A \setminus \{0\}$. Il existe $u \in A^\times$ et $\pi_1, \dots, \pi_r \in A$ irréductibles tels que $a = u\pi_1 \cdots \pi_r$ (factorisation en produit d'éléments irréductibles). Si $a = v\varpi_1 \cdots \varpi_s$ avec $v \in A^\times$ et $\varpi_1, \dots, \varpi_s$ irréductibles est une autre factorisation, alors $r = s$ et quitte à renuméroter, on a $\langle \pi_i \rangle = \langle \varpi_i \rangle$ pour tout $i \in \{1, \dots, r\}$ (unicité de la factorisation)⁶.

Définition 2.3.21. 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 $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$ respectivement. On dit que a et b sont *premiers entre eux* si $\text{pgcd}(a, b) = 1$.



Remarques. (1) Rigoureusement, $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$ 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 $\text{pgcd}(6, 10) = 2$ au lieu de $\text{pgcd}(6, 10) = \{\pm 2\}$. 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 $\text{pgcd}(a, 0) = a$ et $\text{ppcm}(a, 0) = 0$.

Proposition 2.3.22. On a $\text{pgcd}(a, b)A = \langle a, b \rangle$ et $\text{ppcm}(a, b)A = \langle a \rangle \cap \langle b \rangle$.

Remarques. (1) Les notions existent dans un anneau quelconque, mais en général, le pgcd et le ppcm 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.

5. Cette condition est satisfaite lorsque A est noethérien (tout idéal est de type fini).

6. Tout anneau principal est factoriel.

Définition 2.3.23. En particulier, 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.

Proposition 2.3.24 (Lemme de Gauss). Soient $a, b, c \in A \setminus \{0\}$ tels que $\text{pgcd}(a, b) = 1$. Si $a \mid bc$, alors $a \mid c$.

Plus généralement, les pgcd et ppcm existent en supposant seulement A factoriel. Pour le voir, fixons comme plus haut une famille de représentants $\mathbb{P} = \{\pi_\lambda\}_{\lambda \in \Lambda}$ des classes des éléments irréductibles modulo la relation « être associé ».

Soient $a, b \in A \setminus \{0\}$. 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

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

alors on a

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

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

$$\begin{cases} v_\pi(\text{pgcd}(a, b)) = \min\{v_\pi(a), v_\pi(b)\} \\ v_\pi(\text{ppcm}(a, b)) = \max\{v_\pi(a), v_\pi(b)\} \end{cases}$$

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

Remarque. Bien entendu, cette définition est compatible à celle qui a été donnée pour les anneaux principaux. Bien sûr, la définition en termes d'idéaux n'est pas valide en général dans un anneau factoriel mais non principal. Par exemple, on peut montrer que $\mathbf{Q}[X, Y]$ est factoriel. Comme X et Y sont irréductibles et premiers entre eux, on a $\text{pgcd}(X, Y) = 1$, 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.

Proposition 2.3.25. Le lemme de Gauss (cf lemme 2.3.24) est valide dans un anneau factoriel.

Exercice 2.3.26. Soient A un anneau factoriel et $a, b, c \in A$. Montrer que $\text{pgcd}(a, b, c) = \text{pgcd}(a, \text{pgcd}(b, c))$.

Exemples 2.3.27. Si K est un corps et $n \in \mathbf{N}_{>1}$, l'anneau $K[X_1, \dots, X_n]$ est factoriel mais pas principal (cf remarque précédente). De même, l'anneau $\mathbf{Z}[X]$ est factoriel mais pas principal (l'idéal engendré par 2 et X n'est pas principal).

Exercice 2.3.28. 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.

2.3.29 Anneaux euclidiens

Dans ce numéro, A est un anneau intègre.

Définition 2.3.30. L'anneau A est dit *euclidien* s'il existe une application $\phi: A \setminus \{0\} \rightarrow \mathbf{N}$ telle que pour tout $(a, b) \in A \times A \setminus \{0\}$, 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. (1) Si A est un anneau euclidien, il n'y a pas unicité d'un stathme euclidien sur A . En outre, on ne requiert pas l'unicité du quotient et du reste.

(2) Supposons A euclidien et soit $\phi: A \setminus \{0\} \rightarrow \mathbf{N}$ un stathme euclidien. Pour $a \in A \setminus \{0\}$, posons $\psi(a) = \min_{x \in A \setminus \{0\}} \phi(ax)$.

Alors $\psi: A \setminus \{0\} \rightarrow \mathbf{N}$ est un stathme euclidien sur A qui vérifie en outre $a \mid b \Rightarrow \psi(a) \leq \psi(b)$ (exercice).

Exemples 2.3.31. (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, la division est 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 2.3.32. Tout anneau euclidien est principal.

Remarque. Il existe des anneaux qui sont principaux, mais pas euclidiens.

Corollaire 2.3.33. Soit K un corps, les anneaux \mathbf{Z} et $K[X]$ sont principaux.

Remarque. 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).

Exercices 2.3.34. (1) Soient $n, m \in \mathbf{N}_{>0}$. Calculer $\text{pgcd}(X^n - 1, X^m - 1)$ dans $\mathbf{Q}[X]$.

(2) Montrer que l'anneau $\mathbf{Z}[j] = \{a + bj\}_{a, b \in \mathbf{Z}} \subset \mathbf{C}$ est euclidien.

2.4 Anneaux de séries formelles, anneaux des polynômes

Soit A un anneau.

Définition 2.4.1. L'anneau des *séries formelles* à coefficients dans A est l'ensemble $A^{\mathbb{N}}$ des suites à valeurs dans A muni des deux lois suivantes :

$$\begin{aligned}(a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} &= (a_n + b_n)_{n \in \mathbb{N}} \\ (a_n)_{n \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}} &= (c_n)_{n \in \mathbb{N}}\end{aligned}$$

où $c_n = \sum_{k=0}^n a_k b_{n-k}$.

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

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

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

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

Définition 2.4.2. Avec la notation qui précède, 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 $A[[X]]$.

Définition 2.4.3. 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. Un polynôme s'écrit donc comme une somme finie

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

Définition 2.4.4. (1) Si $f(X) = \sum_{n=0}^{\infty} a_n X^n \in A[[X]]$, l'élément a_0 s'appelle le coefficient constant de $f(X)$.

(2) Soit $P \in A[X] \setminus \{0\}$. On peut écrire de façon unique $P(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_d X^d$ 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.

(3) Un polynôme dont tous les coefficients sont nuls sauf un seul (*i.e.* de la forme aX^d) s'appelle un *monôme*.

Remarque. L'application $A \rightarrow A[X]$ qui envoie a sur $(a, 0, \dots)$ 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 2.4.5. Si $P, Q \in A[X]$, on a

$$\begin{aligned}\deg(P + Q) &\leq \max\{\deg(P), \deg(Q)\} \\ \deg(PQ) &\leq \deg(P) + \deg(Q).\end{aligned}$$

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 diviseur de zéro (c'est automatique lorsque A est intègre).

Exemple 2.4.6. Si $P = Q = 1 + 2X \in (\mathbf{Z}/4\mathbf{Z})[X]$, alors $PQ = 1$ est de degré 0.

Corollaire 2.4.7. Si A est intègre, il est de même de $A[X]$.

Exercices 2.4.8. (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 2.4.9 (Division euclidienne). Soient A un anneau et $P, D \in A[X]$. On suppose que le coefficient dominant de D est inversible. Alors il existe 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 Q .

Remarque. Si K est un corps, la division euclidienne par un polynôme non nul existe toujours dans $K[X]$.

A 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 $\mathbf{Z}[X]$.



Théorème 2.4.10 (Propriété universelle). Soient $f: A \rightarrow B$ un morphisme d'anneaux et $b \in B$. Il existe un unique morphisme d'anneaux $\tilde{f}: A[X] \rightarrow B$ tel que $\tilde{f}(a) = f(a)$ pour tout $a \in A$ et $\tilde{f}(X) = b$.

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

Définition 2.4.11. Soient A un anneau et $\alpha \in A$. Le morphisme d'évaluation en α est l'unique morphisme $\text{ev}_\alpha: A[X] \rightarrow A$ prolongeant l'identité de A et envoyant X sur α (explicitement ev_α envoie $a_0 + a_1X + \dots + a_dX^d$ sur $P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_d\alpha^d$).

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

$$\begin{aligned} A &\rightarrow A \\ \alpha &\mapsto P(\alpha) \end{aligned}$$

Les fonctions ainsi obtenues sont appelées *fonctions polynômiales*. Il faut néanmoins se garder de confondre un polynôme avec la fonction polynômiale 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 $A[X] \rightarrow \mathcal{F}(A, A)$ qui à un polynôme associe sa fonction polynômiale. Il n'est pas injectif en général. Il l'est lorsque A est un corps infini (exercice).

Exemple 2.4.12. Considérons le sous-anneau $\mathbf{Z}[i] = \{a + ib; a, b \in \mathbf{Z}\}$ de \mathbf{C} . On dispose du morphisme $f: \mathbf{Z}[X] \rightarrow \mathbf{C}$ qui envoie X sur i . Il est surjectif, et la division euclidienne implique que $\text{Ker}(f) = \langle X^2 + 1 \rangle$. 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 $\mathbf{R}[X] \rightarrow \mathbf{C}$ déduit de l'inclusion $\mathbf{R} \subset \mathbf{C}$ et qui envoie X sur i .

Exercice 2.4.13. Soient A un anneau, $I \subset A$ un idéal. On dispose dans $A[X]$ de l'idéal $IA[X]$ engendré par I . Montrer qu'on a un isomorphisme naturel

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

Définition 2.4.14. (1) 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 $\underline{n} = (n_1, \dots, n_r) \in \mathbf{N}^r$.

(2) 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 , c'est-à-dire 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 $|\underline{n}| := n_1 + \dots + n_r \neq d$. Tout élément $P \in A[X_1, \dots, X_r]$ s'écrit de façon unique $P = P_0 + P_1 + \dots + P_d$ avec P_i homogène de degré i .

Théorème 2.4.15 (Propriété universelle). Soient $f: A \rightarrow B$ un morphisme d'anneaux et $b_1, \dots, b_r \in B$. Il existe un unique morphisme d'anneaux $\tilde{f}: A[X_1, \dots, X_r] \rightarrow B$ tel que $\tilde{f}(a) = f(a)$ pour tout $a \in A$ et $\tilde{f}(X_i) = b_i$ pour tout $i \in \{1, \dots, r\}$.

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

Exercice 2.4.16. Soient K un corps et X, Y, T des indéterminées.

(1) Montrer que le morphisme d'anneaux $f: K[X, Y] \rightarrow K[T]$ qui est l'identité sur K et envoie X sur T^2 et Y sur T^3 a 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 .

2.4.17 Polynômes symétriques, antisymétriques

Soient A un anneau et X_1, \dots, X_r des indéterminées. Si $P(X_1, \dots, X_r) \in A[X_1, \dots, X_r]$ et $\gamma \in \mathfrak{S}_r$, on pose $(\gamma \cdot P)(X_1, \dots, X_r) = P(X_{\gamma(1)}, \dots, X_{\gamma(r)})$. On munit ainsi $A[X_1, \dots, X_r]$ d'une action du groupe \mathfrak{S}_r .

Définition 2.4.18. (1) 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 un corps.

(2) Pour $k \in \{1, \dots, r\}$, on pose

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

(k -ième polynôme symétrique élémentaire).

Exemple 2.4.19. On a

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

Proposition 2.4.20. On a l'égalité

$$\prod_{i=1}^r (T - X_i) = T^r - \sigma_1 T^{r-1} + \sigma_2 T^{r-2} + \dots + (-1)^k \sigma_k T^{r-k} + \dots + (-1)^r \sigma_r$$

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

Théorème 2.4.21. Si $P(X_1, \dots, X_r) \in A[X_1, \dots, X_r]$ est symétrique, il existe un unique polynôme $Q(X_1, \dots, X_r) \in A[X_1, \dots, X_r]$ unique tel que $P(X_1, \dots, X_r) = Q(\sigma_1, \dots, \sigma_r)$.

Corollaire 2.4.22. Si K est 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 2.4.23. Un polynôme $P \in A[X_1, \dots, X_r]$ est dit antisymétrique si $\gamma.P = \varepsilon(\gamma)P$ pour tout $\gamma \in \mathfrak{S}_r$ (où $\varepsilon : \mathfrak{S}_r \rightarrow \{\pm 1\}$ désigne la signature).

Exemple 2.4.24. Le polynôme

$$\delta(X_1, \dots, X_n) = \prod_{1 \leq i < j \leq n} (X_i - X_j)$$

est antisymétrique (par définition de la signature).

Théorème 2.4.25. 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 $\geq \frac{n(n-1)}{2}$.

2.5 Corps des fractions

2.5.1 Généralités

Soit A un anneau intègre⁷. On construit un corps qui contient A et qui est minimal pour cette propriété de la façon suivante. On munit l'ensemble $A \times (A \setminus \{0\})$ de la relation binaire donnée par :

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1.$$

Lemme 2.5.2. C'est une relation d'équivalence.

On note $\text{Frac}(A)$ l'ensemble quotient de $A \times (A \setminus \{0\})$ par cette relation d'équivalence. Pour tout $(a, s) \in A \times (A \setminus \{0\})$, on note $[(a, s)]$ son image dans $\text{Frac}(A)$. On le munit de deux lois définies par

$$[(a_1, s_1)] + [(a_2, s_2)] = [(a_1 s_2 + a_2 s_1, s_1 s_2)] \quad \text{et} \quad [(a_1, s_1)] \cdot [(a_2, s_2)] = [(a_1 a_2, s_1 s_2)].$$

Proposition 2.5.3. Ces lois sont bien définies, et munissent $\text{Frac}(A)$ d'une structure de corps. On l'appelle le corps des fractions de A . Par ailleurs, l'application

$$\begin{aligned} \iota : A &\rightarrow \text{Frac}(A) \\ a &\mapsto [(a, 1)] \end{aligned}$$

définit un morphisme injectif d'anneaux (de sorte qu'on peut voir A comme un sous-anneau de $\text{Frac}(A)$). En outre, le couple $(\text{Frac}(A), \iota)$ a la propriété universelle suivante : pour tout morphisme d'anneaux $f : A \rightarrow B$ tel que $(\forall a \in A \setminus \{0\}) f(a) \in B^\times$, il existe un unique morphisme d'anneaux

$$\tilde{f} : \text{Frac}(A) \rightarrow B$$

tel que $f = \tilde{f} \circ \iota$.

Remarques. (1) L'idée de la construction est que 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 (voir plus bas), 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 $i : A \hookrightarrow K$ en $\tilde{i} \circ \iota$, et comme $\tilde{i} : \text{Frac}(A) \rightarrow K$ est un morphisme d'anneaux entre corps, il est injectif.

Exemples 2.5.4. Le corps des fractions de \mathbf{Z} est le corps \mathbf{Q} .

2.5.5 Corps des fractions rationnelles

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

Définition 2.5.6. Le corps des fractions rationnelles (en l'indéterminée X) sur K est

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

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 $\text{pgcd}(P, Q) = 1$ et Q unitaire (on parle alors de forme irréductible).

Définition 2.5.7. 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. Avec les notations de la définition 2.5.7, la fraction rationnelle R définit l'application

$$\begin{aligned} R : K \setminus Z(Q) &\rightarrow K \\ x &\mapsto \frac{P(x)}{Q(x)} \end{aligned}$$

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

7. Il existe des constructions plus générales, et sans les hypothèses de commutativité ou d'intégrité, dont on ne parlera pas ici.

Définition 2.5.8. (1) Si $R = \frac{P}{Q} \in K(X)$, on pose $\deg(R) = \deg(P) - \deg(Q) \in \mathbf{Z} \cup \{-\infty\}$, 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 $K[X]$.
 (2) Notons \mathbb{P} l'ensemble des polynômes irréductibles et unitaires dans $K[X]$. Si $P \in \mathbb{P}$, on dispose de la valuation P -adique $v_P : K[X] \setminus \{0\} \rightarrow \mathbf{N}$. Elle se prolonge de façon unique en une application

$$v_P : K(X)^\times \rightarrow \mathbf{Z}$$

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

Remarque. On peut interpréter l'application $-\deg : K(X) \rightarrow \mathbf{Z} \cup \{\infty\}$ comme une valuation de la façon suivante. Posons $Y = \frac{1}{X}$: on a $K(X) = K(Y)$. Si $P(X) = a_0 + a_1 X + \dots + a_d X^d \in K[X] \setminus \{0\}$ avec $d = \deg(P)$, on a

$$P = X^d(a_0 Y^d + \dots + a_{d-d} Y + a_d) = Y^{-d}(a_0 Y^d + \dots + a_{d-d} Y + a_d).$$

Comme $a_d \neq 0$, on a $v_Y(a_0 Y^d + \dots + a_{d-d} Y + a_d) = 0$, 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'autres 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 $(v_P(R))_{P \in \mathbb{P}} \in \mathbf{Z}^{(\mathbb{P})}$ et qu'il existe $u \in K^\times$ unique tel que

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

Cela donne une description du groupe multiplicatif $K(X)^\times$ (il est isomorphe à $K^\times \times \mathbf{Z}^{(\mathbb{P})}$). 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 2.5.9 (Décomposition en éléments simples). *La famille*

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

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

Remarque. 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 $(A_{i,j})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq m_i}}$ 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 2.5.10. Soit $R = \frac{P}{Q} \in K(X)$ tel que $\deg(R) < 0$. Si $Q = Q_1 Q_2$ avec $\text{pgcd}(Q_1, Q_2) = 1$, il existe $P_1, P_2 \in K[X]$ uniques tels que $\deg(P_i) < \deg(Q_i)$ et $R = \frac{P_1}{Q_1} + \frac{P_2}{Q_2}$.

Remarque. Avec les notations de la remarque 2.5.5, on a $\deg(E) = \deg(R)$.

Exemple 2.5.11. • $K = \mathbf{C}$. Comme le corps \mathbf{C} est algébriquement clos, on a $\mathbb{P} = \{X - a\}_{a \in \mathbf{C}}$. 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 $(\alpha_{i,j})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq m_i}}$ dans \mathbf{C} uniques tels que

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

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

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

Remarques. (1) Cela montre par exemple que $\dim_{\mathbf{C}}(\mathbf{C}(X)) = \text{Card}(\mathbf{R})$ (alors que $\dim_{\mathbf{C}}(\mathbf{C}[X]) = \text{Card}(\mathbf{N})$).

(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 2.5.12. (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

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

2.6 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. 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 $A[X]$ ».

2.6.1 Généralités

Définition 2.6.2. Soient $P \in A[X]$ et $\alpha \in A$. On dit que α est une *racine* de P si $P(\alpha) = 0$.

Lemme 2.6.3. Soient $P \in A[X]$ de degré ≥ 1 , et $\alpha \in A$. Si α est racine de P , alors P est divisible par $X - \alpha$. En particulier, P est réductible si $\deg(P) \geq 2$.

Corollaire 2.6.4. Soient K un corps et $P \in K[X]$. Alors P a un facteur de degré 1 si et seulement si P a une racine dans K .

Proposition 2.6.5. Soient K un corps et $P \in K[X]$.

(1) Si $\deg(P) = 1$, alors P est irréductible.

(2) Si $\deg(P) \in \{2, 3\}$, alors P est irréductible si et seulement si il n'a pas de racine dans K .



Remarque. L'énoncé qui précède est très faux en degré ≥ 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 2.6.6. Supposons A principal⁸. Soient $P(X) = a_0 + a_1X + \dots + a_nX^n \in A[X]$ de degré n et $a, b \in A \setminus \{0\}$ premiers entre eux tels que a/b soit une racine de P dans $\text{Frac}(A)$. Montrer que $a \mid a_0$ et $b \mid a_n$. En déduire que si P est unitaire et admet une racine $\alpha \in \text{Frac}(A)$, alors $\alpha \in A$ (on dit que A est *intégralement clos*).

Lemme 2.6.7. Soit $P \in A[X] \setminus A$ unitaire et réductible. Alors il existe $P_1, P_2 \in A[X]$ unitaires tels que $P = P_1P_2$ et $\deg(P_1), \deg(P_2) < \deg(P)$.

Remarque. 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 $\mathbf{Z}[X]$.

2.6.8 Transfert d'irréductibilité

Supposons A principal⁹ et posons $K = \text{Frac}(A)$.

Définition 2.6.9. Soit $P = a_0 + a_1X + \dots + a_dX^d \in A[X] \setminus \{0\}$. Le contenu de P est

$$c(P) = \text{pgcd}\{a_0, \dots, a_d\}.$$

Un polynôme $P \in A[X] \setminus \{0\}$ est *primitif* si $c(P) = 1$.

Remarques. (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 $c(P)$ 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.* en supposant seulement A intègre), on dit qu'un polynôme $P \in A[X] \setminus \{0\}$ 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 2.6.10. Si $P, Q \in A[X] \setminus \{0\}$, on a

(1) $c(aP) = a c(P)$ pour tout $a \in A \setminus \{0\}$;

(2) $P = c(P)\tilde{P}$ avec $\tilde{P} \in A[X]$ primitif ;

(3) $c(PQ) = c(P)c(Q)$.

Proposition 2.6.11. Soit $P \in A[X]$ de degré ≥ 1 .

(1) Si P est irréductible dans $A[X]$, alors il est irréductible dans $K[X]$.

(2) Si P est primitif et irréductible dans $K[X]$, alors il est irréductible dans $A[X]$.

Exemples 2.6.12. (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. Dans l'énoncé qui précède, il est important de supposer A principal¹⁰. Par exemple, soit $A = \mathbf{Z}[\sqrt{-5}] \subset \mathbf{C}$ (on a déjà vu que cet anneau n'est pas factoriel). On a $P(X) := 2X^2 - 2X + 3 \in A[X]$. Si $K = \text{Frac}(A)$, on a $P(X) = 2(X - \frac{1+\sqrt{-5}}{2})(X - \frac{1-\sqrt{-5}}{2})$ dans $K[X]$. Cependant, il est irréductible dans $A[X]$ (exercice).

Exercices 2.6.13. (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 $a_1, \dots, a_n \in \mathbf{Z}$ deux à deux distincts. Montrer que $P(X) = (X - a_1) \cdots (X - a_n) - 1$ est irréductible sur \mathbf{Q} .

2.6.14 Transfert de la factoriabilité

Théorème 2.6.15. (1) Les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A et les polynômes primitifs non constants qui sont irréductibles dans $K[X]$.
(2) L'anneau $A[X]$ est factoriel.

Démonstration. (1) 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 2.6.11 (2) 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 *a fortiori* irréductible dans A . Si $\deg(P) \geq 1$, on a $P = c(P)\tilde{P}$ avec $\tilde{P} \in A[X]$ primitif : comme P est irréductible dans $A[X]$, on a $c(P) \in A^\times$, donc P est primitif. Par ailleurs, la proposition 2.6.11 (1) montre que P est irréductible dans $K[X]$.

(2) • 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 *a 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 $a \in A \setminus \{0\}$ tel que $aS \in A[X]$: on peut écrire $aS = c(aS)\tilde{S}$ avec $\tilde{S} \in A[X]$ primitif, donc $aQ = c(aS)P\tilde{S}$. En prenant les contenus, on a $a c(Q) = c(aS)$ (parce que $P\tilde{S}$ est primitif), ce qui montre que $a \mid c(aS)$: si $c(aS) = ab$, on a $Q = bP\tilde{S}$, ce qui montre que $P \mid Q$ dans $A[X]$. Cela prouve que P est premier dans $A[X]$.

• D'après (1), 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 $P \in A[X] \setminus \{0\}$ admet une factorisation en produit d'éléments irréductibles (cf proposition 2.3.15). D'après le lemme 2.6.10 (2), on peut écrire $P = c(P)\tilde{P}$ avec $\tilde{P} \in A[X]$ primitif. Comme A est factoriel, on peut factoriser $c(P)$ en produit d'éléments irréductibles dans A (donc dans $A[X]$) : il suffit de montrer \tilde{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 $\deg(P) \geq 1$. Comme l'anneau $K[X]$ est factoriel (cf corollaire 2.3.33), on peut écrire $P = P_1P_2 \cdots P_r$ avec P_1, \dots, P_r irréductibles dans $K[X]$. Pour tout $k \in \{1, \dots, r\}$, choisissons $a_k \in A \setminus \{0\}$ tel que $a_k P_k \in A[X]$: le polynôme $\tilde{P}_k := c(a_k P_k)^{-1}(a_k P_k) \in A[X]$ est primitif. Étant irréductible dans $K[X]$, il est irréductible dans $A[X]$ (proposition 2.6.11 (2)). Par ailleurs, on a $a_1 \cdots a_r P = c(a_1 P_1) \cdots c(a_r P_r) \tilde{P}_1 \cdots \tilde{P}_r$, donc $a_1 \cdots a_r = c(a_1 P_1) \cdots c(a_r P_r)$ en prenant le contenu, et donc $P = \tilde{P}_1 \cdots \tilde{P}_r$, ce qui achève la preuve. \square

8. En fait il suffit de le supposer factoriel

9. Tout ce qui suit est valide en supposant seulement A factoriel.

10. En fait factoriel...

Remarques. (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 2.6.16. *L'anneau $A[X_1, \dots, X_n]$ est factoriel.*

Exemple 2.6.17. Les anneaux $\mathbf{Z}[X_1, \dots, X_n]$ et $K[X_1, \dots, X_n]$ (où K est un corps) sont factoriels.

Exercices 2.6.18. (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 $\{X_{i,j}\}_{1 \leq i,j \leq n}$ des indéterminées. Posons $R = A[X_{i,j}\]_{1 \leq i,j \leq n}$ (l'anneau de polynômes en n^2 indéterminées). On dispose de la matrice $M := (X_{i,j})_{1 \leq i,j \leq n} \in M_n(R)$, et du polynôme $D_n := \det(M) \in R$. Montrer que D_n est irréductible dans R [indication : procéder par récurrence sur n et en développant D_n par rapport à la première colonne].


2.6.19 Les critères d'irréductibilité

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

Théorème 2.6.20 (Critère d'irréductibilité par réduction I). *Supposons $P \in A[X]$ non constant et unitaire. Si $\bar{P} \in (A/I)[X]$ ne se factorise pas en un produit de deux polynômes de degrés $< \deg(P)$, alors P est irréductible dans $A[X]$.*

Exemples 2.6.21. (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, cf proposition 2.6.5). Remarquons qu'on ne peut pas invoquer la proposition 2.6.5 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. (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^2Y : 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 ».

Théorème 2.6.22 (Critère d'irréductibilité par réduction II). *Soient $\mathfrak{p} \subset A$ un idéal premier et $P(X) = a_0 + a_1X + \dots + a_dX^d \in A[X]$ un polynôme primitif tels que*

- (i) $a_d \notin \mathfrak{p}$;
- (ii) l'image \bar{P} de P dans $(A/\mathfrak{p})[X]$ est irréductible.

Alors P est irréductible dans $A[X]$ (et donc aussi dans $K[X]$ en vertu de la proposition 2.6.11).


Exemple 2.6.23. 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. 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 2.6.24 (Critère d'Eisenstein). *Soient $\mathfrak{p} \subset A$ un idéal premier et $P(X) = a_0 + a_1X + \dots + a_{d-1}X^{d-1} + a_dX^d \in A[X]$ un polynôme primitif tels que*

- (i) $a_d \notin \mathfrak{p}$;
- (ii) $a_0, a_1, \dots, a_{d-1} \in \mathfrak{p}$;
- (iii) $a_0 \notin \mathfrak{p}^2$.

Alors P est irréductible dans $A[X]$ (et donc aussi dans $K[X]$ en vertu de la proposition 2.6.11).

Remarque. (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 $\{0\}$...)

(3) À l'inverse du critère par réduction 2.6.22, le critère d'Eisenstein s'applique quand la réduction \bar{P} est très réductible.

Exemples 2.6.25. (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 $\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbf{Z}[X]$ (on l'appelle le p -ième polynôme cyclotomique, cf plus bas). Alors Φ_p est irréductible. Pour le montrer, on remarque que $\Phi_p(X) = \frac{X^p - 1}{X - 1} \in \mathbf{Q}(X)$: on effectue le changement de variable $X = Y + 1$. On a alors $\Phi_p(X) = \frac{(Y+1)^p - 1}{Y}$ d'où

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

Comme $p \mid \binom{p}{k}$ pour tout $k \in \{1, \dots, p-1\}$ 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 2.6.26. Soit $n \in \mathbf{N}_{>1}$. Montrer que le polynôme $X^n + 5X^{n-1} + 3$ est irréductible dans $\mathbf{Z}[X]$.

3 Extensions de corps

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

3.1 Définitions

Soit K un corps.

Définition 3.1.1. 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 $f: L_1 \rightarrow L_2$ qui induit l'identité sur K . On parle aussi du K -morphisme $f: L_1 \rightarrow L_2$.

Exemple 3.1.2. (1) \mathbb{C}/\mathbb{R} , \mathbb{R}/\mathbb{Q} , $\mathbb{Q}(X)/\mathbb{Q}$.

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

$$\begin{aligned} \text{ev}_{\sqrt{2}, \mathbb{Q}}: \mathbb{Q}[X] &\rightarrow \mathbb{C} \\ P &\mapsto P(\sqrt{2}) \end{aligned}$$

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

Définition 3.1.3. Les corps \mathbb{Q} et $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ avec p premier sont appelés les *corps premiers*.

Proposition 3.1.4. On a les deux possibilités suivantes :

- $\text{car}(K) = 0$ donc $\mathbb{Q} \subset K$;
- $\text{car}(K) = p$ est premier et $\mathbb{F}_p \subset K$.

Exercice 3.1.5. Montrer que le seul automorphisme d'un corps premier est l'identité.

Remarque. 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 3.1.6. 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 3.1.7. $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{Q}(X) : \mathbb{Q}] = \infty$ et $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

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

Théorème 3.1.8. 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 $(1, \bar{X}, \bar{X}^2, \dots, \bar{X}^{d-1})$ (où \bar{X} désigne l'image de X dans $K[X]/\langle P(X) \rangle$).

Remarques. (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 $\bar{Q}\bar{V} = 1$: 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 3.1.9. D'après le critère d'Eisenstein, le polynôme $P = X^2 - 2$ est irréductible dans $\mathbb{Z}[X]$: il l'est dans $\mathbb{Q}[X]$. L'extension correspondante est $\mathbb{Q}[\sqrt{2}] = \{x + y\sqrt{2}, x, y \in \mathbb{Q}\}$. C'est un corps, et on a $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. Calculons l'inverse de $1 + \sqrt{2}$. Il est représenté par le polynôme $1 + X$ dans $\mathbb{Q}[X]$. On a $X^2 - 2 = (X - 1)(X + 1) - 1$: en projetant dans $\mathbb{Q}[\sqrt{2}]$, 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 $(x, y) \in \mathbb{Q}^2 \setminus \{(0, 0)\}$.

Exercice 3.1.10. Soit $P \in K[X]$. Montrer que les propriétés suivantes sont équivalentes :

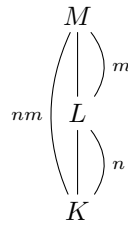
- (i) P est irréductible ;
- (ii) $K[X]/\langle P(X) \rangle$ est un corps ;
- (iii) $K[X]/\langle P(X) \rangle$ est intègre.

À quelle condition sur P l'anneau $K[X]/\langle P(X) \rangle$ est-il réduit ?

Théorème 3.1.11 (de la base télescopique). Si L/K et M/L sont des extensions, alors M/K est une extension, et

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

La proposition précédente se résume simplement par le diagramme suivant :



Définition 3.1.12. Soit L/K une extension. Une *sous-extension* de L/K est un sous-corps E de L qui contient K .

Exemple 3.1.13. \mathbf{R} et une sous-extension de \mathbf{C}/\mathbf{Q} .


Remarques. (1) D'après le théorème 3.1.11, 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 sous-extension de L/K .

Définition 3.1.14. 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 .

Remarques. (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 $R(s_1, \dots, s_n)$ avec $s_1, \dots, s_n \in S$ et $R \in K(X_1, \dots, X_n)$ une fraction rationnelle dont le dénominateur ne s'annule pas en (s_1, \dots, s_n) .

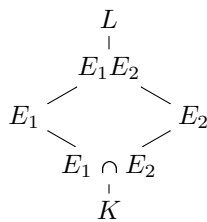
(2) Si L/K est une extension finie, alors c'est une extension de type fini (une partie génératrice étant fournie par une base de L vu comme K -espace vectoriel). La réciproque est fautive : $\mathbf{Q}(X)$ est de type fini sur \mathbf{Q} , mais $[\mathbf{Q}(X) : \mathbf{Q}] = \infty$. 

Définition 3.1.15. 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 $E_1 E_2$.

Remarques. (1) Si $E_1 = K(S_1)$ et $E_2 = K(S_2)$, alors $E_1 E_2 = K(S_1 \cup S_2)$ (exercice).

(2) En général, $E_1 \cup E_2$ n'est pas une sous-extension de L/K . 

Les relations qu'entretiennent ces différentes sous-extensions sont résumées par le diagramme suivant :



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

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

On note $K[\alpha]$ son image. Remarquons que $K(\alpha)$ n'est autre que le corps des fractions de $K[\alpha]$ dans L (cf définition 3.1.14). On a donc $K[\alpha] \subset K(\alpha)$, inclusion stricte en général.

Définition 3.2.2. (1) On dit que α est *transcendant* sur K si le morphisme $\text{ev}_{\alpha, K}$ est injectif, et *algébrique* sur K dans le cas contraire.

(2) Si α est algébrique sur K , on appelle *polynôme minimal* de α sur K l'unique générateur unitaire de $\text{Ker}(\text{ev}_{\alpha, K})$. On le note $P_{\alpha, K}$. Le *degré* de α sur K est le degré de $P_{\alpha, K}$, on le note $\text{deg}_K(\alpha)$.

Remarque. 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 $\mathbf{Q}(X)$. 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 $P_{i, \mathbf{C}}(X) = X - i$.

- Exemples 3.2.3.** (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 $\sqrt{2}$, $\sqrt{2} + \sqrt{3}$ sont algébriques sur \mathbf{Q} , de polynômes minimaux sur \mathbf{Q} respectifs $X^2 - 2$ et $X^4 - 10X^2 + 1$.

Proposition 3.2.4. Soient L/K une extension et $\alpha \in L$ 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 $[K(\alpha) : K] = \deg_K(\alpha)$.

Remarque. 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. $P_{\alpha,K} = P$.

Exemple 3.2.5. 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).

Proposition 3.2.6. Soient L/K une extension, E/K une sous-extension et $\alpha \in L$ algébrique sur K . Alors α est algébrique sur E et $P_{\alpha,E} \mid P_{\alpha,K}$ dans $E[X]$.

Exemple 3.2.7. Les nombres $\sqrt{2}$, $\sqrt{2} + \sqrt{3}$ 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.

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 3.2.8. 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 $\alpha \in E$.

Exercice 3.2.9. 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 3.2.10. Soient L/K une extension et $\alpha, \beta \in L^\times$ algébriques sur K . Alors $\alpha - \beta$ 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 .

Définition 3.2.11. 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*.

Donons-en quelques propriétés.

Proposition 3.2.12. Le corps $\overline{\mathbf{Q}}$ est dénombrable.

Corollaire 3.2.13. On a $\text{Card}(\mathbf{C} \setminus \overline{\mathbf{Q}}) = \text{Card}(\mathbf{C})$. En particulier, l'ensemble des nombres complexes transcendants sur \mathbf{Q} est non vide (sa cardinalité est celle de \mathbf{R}).

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

Théorème 3.2.14 (Liouville). Soit $\alpha \in \overline{\mathbf{Q}} \cap \mathbf{R}$, de degré $d > 1$ sur \mathbf{Q} . Alors il existe une constante $c(\alpha) \in \mathbf{R}_{>0}$ telle que pour tout $(p, q) \in \mathbf{Z} \times \mathbf{N}_{>0}$, on a

$$\left| \alpha - \frac{p}{q} \right| > \frac{c(\alpha)}{q^d}.$$

Remarque. 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 $\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^2}$).

Corollaire 3.2.15. Le nombre $\sum_{n=0}^{\infty} \frac{1}{2^{n!}}$ est transcendant sur \mathbf{Q} .

Malheureusement, il est rare qu'on puisse prouver qu'un nombre est transcendant en utilisant le théorème 3.2.14. Par exemple, on ne peut pas le faire avec e et π .

3.2.16 Extensions finies, extensions algébriques

Définition 3.2.17. Une extension L/K est dite *algébrique* si tous les éléments de L sont algébriques sur K .


Exemples 3.2.18. 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 3.2.19. Les intersection et les composés d'extensions algébriques sont algébriques. Une sous-extension engendrée par des éléments algébriques est algébrique.

Proposition 3.2.20. Une extension L/K est finie si et seulement si elle est algébrique et de type fini.

Remarques. (1) Plus précisément, on a montré qu'une extension L/K est finie si et seulement si elle est de la forme $L = K(\alpha_1, \dots, \alpha_n)$ avec $\alpha_1, \dots, \alpha_n \in L$ algébriques sur K .

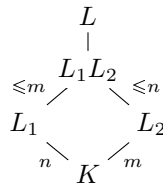
(2) Si K est de caractéristique nulle et L/K est finie, on peut montrer qu'il existe $\alpha \in L$ tel que $L = K(\alpha)$ (théorème de l'élément primitif).

(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 $n = [\mathbf{Q}(\sqrt[n]{2}) : \mathbf{Q}] \leq [\overline{\mathbf{Q}} : \mathbf{Q}]$ pour tout $n \in \mathbf{N}_{>0}$). 


Exercice 3.2.21. Montrer que toute extension algébrique est réunion de ses sous-extensions finies.

Corollaire 3.2.22. Soient M/L et L/K deux extensions. Alors M/K est algébrique si et seulement si M/L et L/K sont algébriques.

Proposition 3.2.23. Soient L/K une extension et $L_1/K, L_2/K$ deux sous-extensions finies. Alors L_1L_2/K est finie et $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$.



Remarques. (1) Une autre façon de prouver la proposition 3.2.23 est de choisir une base $(x_i)_{1 \leq i \leq n}$ de L_1 sur K et une base $(y_j)_{1 \leq j \leq m}$ de L_2 sur K , et de montrer que la famille $(x_i y_j)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ 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 3.2.24. Soient L/K une extension et L_1, L_2 deux sous-extensions finies telles que $\text{pgcd}([L_1 : K], [L_2 : K]) = 1$, alors $[L_1L_2 : K] = [L_1 : K][L_2 : K]$.

Exercices 3.2.25. (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.

3.2.26 Corps de rupture, corps de décomposition

Définition 3.2.27. Soient L/K une extension de corps et $P \in K[X]$.

(1) On dit que L est un *corps de rupture* si L est engendré sur K par une racine de P .

(2) On dit que P est *scindé* sur L si ses facteurs irréductibles dans $L[X]$ sont de degré 1.

(3) On dit que L est un *corps de décomposition* de P sur K si P est scindé dans $L[X]$ et L est engendré sur K par les racines de P .

Exemples 3.2.28. (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 3.2.29. 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 $K[X]/\langle P(X) \rangle$.

Corollaire 3.2.30. Tout $P \in K[X]$ admet un corps de décomposition.

Exemple 3.2.31. 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 que $[\mathbf{Q}(j, \sqrt[3]{2}) : \mathbf{Q}] = 6$).

Exercice 3.2.32. Si $\deg(P) = d$ et L est un corps de décomposition de P sur K , on a $[L : K] \leq d!$.

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

Théorème 3.2.33 (de prolongement des isomorphismes). Soient L_1/K_1 et L_2/K_2 des extensions, $\varphi: K_1 \xrightarrow{\sim} K_2$ 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 $\varphi(P)$). Alors il existe un unique isomorphisme $\tilde{\varphi}: K_1(\alpha) \xrightarrow{\sim} K_2(\beta)$ qui prolonge φ et tel que $\tilde{\varphi}(\alpha) = \beta$.

On peut résumer la proposition précédente par le diagramme suivant :

$$\begin{array}{ccc} L_1 & & L_2 \\ | & & | \\ K_1(\alpha) & \xrightarrow{\tilde{\varphi}} & K_2(\beta) \\ \alpha \longmapsto \beta & & \\ | & & | \\ K_1 & \xrightarrow{\varphi} & K_2 \end{array}$$

La proposition qui précède nous amène naturellement à la définition suivante.

Définition 3.2.34. 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 3.2.35. D'après la théorème 3.2.33, $\alpha, \beta \in L$ sont conjugués sur K si et seulement s'il existe un K -isomorphisme $\sigma: K(\alpha) \rightarrow K(\beta)$ tel que $\sigma(\alpha) = \beta$.

Corollaire 3.2.36. Si $P \in K[X]$, deux corps de décomposition de P sur K sont isomorphes comme extensions de K .

3.3 Corps algébriquement clos, clôture algébrique

Définition 3.3.1. 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 elles sont vérifiées, on dit que K est *algébriquement clos*.

Théorème 3.3.2 (D'Alembert-Gauss). Le corps \mathbf{C} est algébriquement clos.

Corollaire 3.3.3. Les polynômes irréductibles dans $\mathbf{R}[X]$ sont :

- les polynômes de degré 1;
- les trinômes du second degré à discriminant strictement négatif.

Définition 3.3.4. Soit K un corps. Une *clôture algébrique* de K est une extension \bar{K}/K algébrique telle que \bar{K} est algébriquement clos.

Proposition 3.3.5. Si C/K une extension avec C algébriquement clos, alors la sous-extension

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

est une clôture algébrique de K .

Exemple 3.3.6. La proposition précédente et le fait que \mathbf{C} est algébriquement clos impliquent que $\bar{\mathbf{Q}}$ est une clôture algébrique de \mathbf{Q} (cf définition 3.2.11).

Théorème 3.3.7 (Steiniz). Tout corps K admet une clôture algébrique. En outre, si \bar{K} est une clôture algébrique, et si C/K est une extension avec C algébriquement clos, il existe un K -morphisme $\bar{K} \rightarrow C$. En particulier, les clôtures algébriques de K sont deux à deux isomorphes.

Voici une construction 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

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

avec $\lambda_1, \dots, \lambda_n \in \Lambda$ et $Q_1, \dots, Q_n \in A$. Soit L/K une extension telle que le polynôme P_{λ_i} admet une racine α_i dans L pour tout $i \in \{1, \dots, n\}$ (il suffit d'appliquer n fois la proposition 3.2.29). Considérons alors le morphisme d'anneaux K -linéaire $\varphi: A \rightarrow L$ défini par

$$\varphi(X_\lambda) = \begin{cases} \alpha_i & \text{si } \lambda = \lambda_i \text{ pour } i \in \{1, \dots, n\} \\ 0 & \text{sinon} \end{cases}$$

En appliquant φ à l'égalité (*), il vient $0 = 1$, ce qui est absurde : l'idéal I est donc *strict*.

D'après le théorème de Krull (théorème 2.2.13), il existe un idéal maximal \mathfrak{m} de A tel que $I \subset \mathfrak{m}$: posons $\bar{K} = A/\mathfrak{m}$. C'est un corps (proposition 2.2.4), 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 $\bar{K} = A/\mathfrak{m}$. Par ailleurs, si $P \in K[X]$ est non constant, il admet une racine dans \bar{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 \bar{K} (la classe de X_λ).

Corollaire 3.3.8. Soient L/K une extension algébrique et \bar{K} une clôture algébrique de K . Alors il existe un K -morphisme $L \rightarrow \bar{K}$.

Remarque. Il résulte du corollaire 3.3.8 qu'on peut toujours plonger 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 quadratiques

Soit K un corps.

Définition 3.4.1. Une extension de K est dite *quadratique* si elle est de degré 2.

Proposition 3.4.2. Si $\text{car}(K) \neq 2$ et si L/K est une extension quadratique, il existe $\alpha \in L \setminus K$ 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 $\beta = c\alpha$.

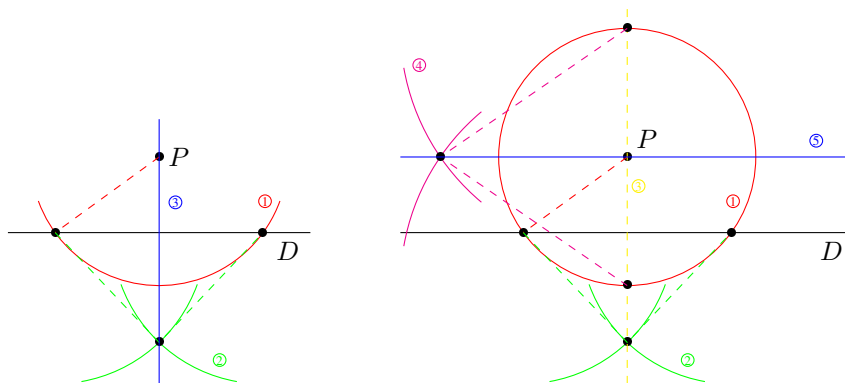
3.4.3 Application aux constructions à la règle et au compas

Soit \mathcal{P} le plan affine euclidien. On s'intéresse au problème suivant. Étant donnés deux points $P_0, P_1 \in \mathcal{P}$ distincts, quels sont les points $P \in \mathcal{P}$ qu'on peut construire avec une règle non graduée et un compas ? Il s'agit des points $P \in \mathcal{P}$ tels qu'il existe une suite $P_0, P_1, \dots, P_{n-1}, P_n = P$ telle que pour tout $i \in \{2, \dots, r\}$, le point P_i s'obtient à partir de $\mathcal{E}_i = \{P_0, P_1, \dots, P_{i-1}\}$ en effectuant l'une des deux opérations suivantes

- tracer une droite passant par deux points de \mathcal{E}_i ;
- tracer un cercle centré en un point de \mathcal{E}_i et passant par un point de \mathcal{E}_i ;

et en prenant l'intersection des figures ainsi obtenues.

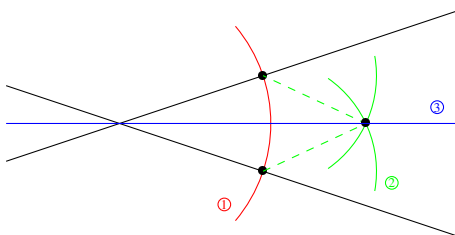
Remarquons déjà que si D est une droite et P un point (qui peut appartenir à D), on sait construire la perpendiculaire à D qui passe par P , et donc la projection de P sur D . Par ailleurs, en itérant cette opération, on sait construire la parallèle à D passant par P .



Définition 3.4.4. 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 \mathcal{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 3.4.5. L'ensemble des nombres constructibles est un sous-corps de \mathbf{R} .

Remarque. Rappelons que la bissectrice de deux droites de \mathcal{P} est constructible à la règle et au compas :



Proposition 3.4.6. Soit $x \in \mathbf{R}$. Alors x est constructible si et seulement si il existe une suite d'extensions $\mathbf{Q} = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_r$ telle que $x \in K_r$ et $[K_i : K_{i-1}] = 2$ pour tout $i \in \{1, \dots, r\}$. En particulier, il est nécessaire (mais pas suffisant en général) que $[\mathbf{Q}(x) : \mathbf{Q}]$ soit une puissance de 2.

Corollaire 3.4.7. Les problèmes suivants ne peuvent pas se résoudre à la règle et au compas :

- (1) La quadrature du cercle (i.e. étant donné un cercle, construire un carré de même aire), ceci parce que π est transcendant.
- (2) Doubler le volume d'un cube (i.e. étant donné un cube, construire un cubule de volume double -c'est dans l'espace et pas le plan-), ceci parce que $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$.
- (3) 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.

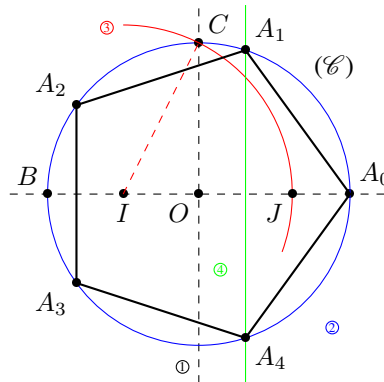
Corollaire 3.4.8. Soit p un nombre premier impair. Pour que le polygone régulier à p côtés soit constructible, il faut que $p = 2^{2^r} + 1$ avec $r \in \mathbf{N}_{>0}$ (un tel nombre s'appelle un nombre premier de Fermat).

Remarque. Le corollaire précédent 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...)

Exemple 3.4.9 (Construction du pentagone (polygone à 5 côtés) 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 $\zeta^3 = e^{\frac{6i\pi}{5}} = e^{-\frac{4i\pi}{5}} = \bar{\zeta}^2$ et $\zeta^4 = e^{\frac{8i\pi}{5}} = e^{-\frac{2i\pi}{5}} = \bar{\zeta}$: on a donc $(\zeta^2 + \bar{\zeta}^2) + (\zeta + \bar{\zeta}) + 1 = 0$ 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 \mathcal{P} . Construisons le pentagone régulier de centre O 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 (\mathcal{C}) 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 (\mathcal{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 (\mathcal{C}) en A_2 (resp. A_3), ce qui achève la construction.



Remarques. (1) Tout point du plan constructible à la règle et au compas peut être construit en utilisant le compas seul (théorème de Mohr-Mascheroni).

(2) 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).

Exercice 3.4.10. 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, \dots, p_r sont des nombres premiers de Fermat distincts.

3.5 Extensions cyclotomiques

Soit $n \in \mathbf{N}_{>0}$. On pose $\varphi(n) = \text{Card}((\mathbf{Z}/n\mathbf{Z})^\times)$ (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 (théorème 2.1.30)).

Posons

$$\mu_n = \{z \in \mathbf{C}; z^n = 1\}.$$

C'est un sous-groupe cyclique de \mathbf{C}^\times . Notons μ_n^* le sous-ensemble de μ_n constitué des éléments d'ordre n , i.e. des générateurs du groupe μ_n (ses éléments sont les racines primitives n -ièmes de l'unité). On a

$$\mu_n = \bigsqcup_{d|n} \mu_d^* \quad (*)$$

(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

$$\Phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi) = \prod_{\substack{1 \leq k < n \\ \text{pgcd}(k,n)=1}} (X - \zeta^k)$$

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

Exemple 3.5.1. 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. Contrairement aux apparences, les coefficients des polynômes cyclotomiques ne sont pas tous dans $\{0, \pm 1\}$: on a

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

Proposition 3.5.2. Pour tout $n \in \mathbf{N}_{>0}$, on a

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \quad \text{et} \quad n = \sum_{d|n} \varphi(d) \quad (\text{C})$$

et $\Phi_n \in \mathbf{Z}[X]$.

Exemple 3.5.3. 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 en particulier

$$\Phi_p(X) = 1 + X + \dots + X^{p-1}$$

et $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.

On a vu (cf exemple 2.6.25 (3)) que Φ_p est irréductible dans $\mathbf{Q}[X]$. C'est un fait général :

Proposition 3.5.4. 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} .

Lemme 3.5.5. Soient A un anneau factoriel, $K = \text{Frac}(A)$ et $P, Q \in K[X]$ unitaires tels que $PQ \in A[X]$. Alors $P, Q \in A[X]$.

3.6 Corps finis

Dans tout ce qui suit, K désigne un corps fini.

3.6.1 Propriétés de base

Proposition 3.6.2. (1) $p := \text{car}(K)$ est un nombre premier ;
(2) on a $\#K = p^d$ avec $d \in \mathbf{N}_{>0}$.

Contrairement à nos conventions, on ne va pas supposer les anneaux commutatifs *a priori* dans l'énoncé suivant.

Théorème 3.6.3 (Wedderburn). Tout corps fini est commutatif.

3.6.4 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 3.6.5. Soient A un anneau commutatif de caractéristique p et $a, b \in A$. On a

$$(a + b)^p = a^p + b^p.$$

Remarque. Bien entendu, il est important de supposer A commutatif et p premier.



Définition 3.6.6. 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 3.6.7. Si F est un corps, un polynôme $P \in F[X]$ est séparable si et seulement si $\text{pgcd}(P, P') = 1$ (où P' désigne le polynôme dérivé).



Remarque. Si $\text{car}(F) = p > 0$, 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).

Exercices 3.6.8. (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 $\text{car}(F) = 0$.

(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.

Théorème 3.6.9. Soient p un nombre premier, $d \in \mathbf{N}_{>0}$ et $q = p^d$.

(1) Il existe un corps à q éléments.

(2) 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 (cf corollaire 3.2.36).

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 3.6.10. (1) \mathbf{F}_q est l'unique sous-corps de cardinal q dans $\overline{\mathbf{F}}_p$;

(2) $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n} \Leftrightarrow d \mid n$;

(3) $\mathbf{F}_{p^d} \cap \mathbf{F}_{p^n} = \mathbf{F}_{p^{\text{pgcd}(d,n)}}$;

(4) $\overline{\mathbf{F}}_p = \bigcup_{n=1}^{\infty} \mathbf{F}_{p^n}$.



Remarques. (1) On n'a pas $\mathbf{F}_{p^n} \simeq \mathbf{Z}/p^n\mathbf{Z}$ dès que $n > 1$ (l'anneau $\mathbf{Z}/p^n\mathbf{Z}$ n'est pas réduit si $n > 1$). De même, on a $\mathbf{F}_{p^n} \simeq \mathbf{F}_p^n$ 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 3.6.11. 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 $k \in \mathbf{N}_{>0}$.

3.6.12 Structure du groupe multiplicatif

Commençons par rappeler le résultat classique suivant.

Lemme 3.6.13. Soit G un groupe abélien (noté multiplicativement).

(1) Soient $x \in G$ d'ordre n et $y \in G$ d'ordre m avec $\text{pgcd}(n, m) = 1$. Alors xy est d'ordre nm .

(2) Supposons G fini, et notons d le ppcm des ordres des éléments de G (on appelle d l'exposant de G). Alors G contient un élément d'ordre d .

Proposition 3.6.14. Si F est un corps et G un sous-groupe fini de F^\times , alors G est cyclique.

En particulier, on a :

Corollaire 3.6.15. Le groupe K^\times est cyclique.

Corollaire 3.6.16 (théorème de l'élément primitif pour un corps fini). Si $\text{car}(K) = p$, il existe $\alpha \in K$ tel que $K = \mathbf{F}_p(\alpha)$.

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 3.6.9 et le corollaire 3.6.16, 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 par la division euclidienne par P).

Exemple 3.6.17. (1) $\mathbf{F}_4 \simeq \mathbf{F}_2[X]/\langle X^2 + X + 1 \rangle$;

(2) $\mathbf{F}_8 \simeq \mathbf{F}_2[X]/\langle X^3 + X + 1 \rangle \simeq \mathbf{F}_2[X]/\langle X^3 + X^2 + 1 \rangle$.

Exercice 3.6.18. Soient q une puissance qu'un nombre premier et $n \in \mathbf{N}_{>0}$. Posons

$$\begin{aligned} \varphi: \mathbf{F}_{q^n} &\rightarrow \mathbf{F}_{q^n} \\ \alpha &\mapsto \alpha^q \end{aligned}$$

- (1) Montrer que $\varphi \in \text{Aut}(\mathbf{F}_{q^n} / \mathbf{F}_q)$ (le groupe des automorphismes de l'extension $\mathbf{F}_{q^n} / \mathbf{F}_q$).
 (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 $\{\varphi^k(\alpha)\}_{0 \leq k < d}$ (et donc P est scindé dans $\mathbf{F}_{q^d} \subset \mathbf{F}_{q^n}$).
 (3) Montrer que l'application

$$\begin{aligned} \mathbf{Z} / n\mathbf{Z} &\rightarrow \text{Aut}(\mathbf{F}_{q^n} / \mathbf{F}_q) \\ k &\mapsto \varphi^k \end{aligned}$$

est un isomorphisme de groupes [indication : pour la surjectivité, appliquer (2) à α tel que $\mathbf{F}_{q^n} = \mathbf{F}_q(\alpha)$].

- (4) Montrer que les applications

$$\begin{aligned} \{\text{sous-extensions de } \mathbf{F}_{q^n} / \mathbf{F}_q\} &\leftrightarrow \{\text{sous-groupes de } \text{Aut}(\mathbf{F}_{q^n} / \mathbf{F}_q)\} \\ F &\mapsto \{\sigma \in \text{Aut}(\mathbf{F}_{q^n} / \mathbf{F}_q); \sigma|_F = \text{Id}_F\} \\ \{\alpha \in \mathbf{F}_{q^n}; (\forall \sigma \in H) \sigma(\alpha) = \alpha\} &\leftrightarrow H \end{aligned}$$

sont des bijections décroissantes inverses l'une de l'autre.